MATERIAŁY XIV KONFERENCJI SZKOLENIOWEJ
Z TEORII ZAGADNIEŃ EKSTREMALNYCH

1993 **Łódź** **str. 59**

ZASTOSOWANIE BAZ GRÖBNERA W TEORII ODWZOROWAŃ WIELOMIANOWYCH

T.Winiarski (Kraków)*

Wstęp

Pojęcie bazy standardowej, wraz z dowodem jej istnienia, pojawiło się po raz pierwszy w słynnej pracy H.Hironaki [HH] o usuwaniu osobliwości, opublikowanej w 1964 roku. Hironaka podał również algorytm dzielenia, który ma wiele ciekawych zastosowań zarówno czysto teoretycznych, jak również w algebrze komputerowej.

Nieco później, tzn. już w 1965 roku B. Buchberger wprowadził nową nazwę dla bazy standardowej - nazwał ją *bazą Gröbnera* (p. [BB]). Dwadzieścia lat później, w pracy [BB1 s.185] Buchberger napisał : "...the author introduced the name *Gröbner bases*, because Prof. W.Gröbner, the thesis advisor of [BB] stimulated the research on the subject by asking how a multiplication table for the associative algebra, which is formed by the residue ring modulo a polynomial ideal, can be constructed algorithmically, and by presenting a first sketch of an algorithm ..." Wyjaśniając dalej napisał : "In retrospect, it seems that the concept of *Gröbner bases* under the name *standard bases* appeared already one year earlier (1964) in Hironaka's fa-

*Badania finansowane przez grant KBN Nr 2 1077 91 01

mous paper [HH]. However, Hironaka only gave an inconstructible existence proof for these bases, whereas in [BB], together with the concept of such bases, we also presented an algorithm for constructing the bases and only this algorithm allows an algorithmic solution to the various problems ... ".

Obecnie w literaturze matematycznej używane są dwie nazwy: *baza standardowa* oraz *baza Gröbnera*. Ponieważ, w niniejszym opracowaniu, algorytmy odgrywają istotną rolę , używać będziemy nazwy zaproponowanej przez B. Buchbergera.

Począwszy od 1965 roku (tzn. od pracy [BB] B.Buchbergera) rozpoczął się szybki rozwój teorii baz Gröbnera. Bardzo mocno udoskonalono algorytm, powstały i nadal powstają coraz to lepsze programy komputerowe oraz odkrywane są dalsze możliwości zastosowania. W prezentowanym opracowaniu przedstawimy jedynie kilka, niedawno odkrytych, zastosowań baz Gröbnera w teorii odwzorowań wielomianowych. Pierwszą pracą z tego zakresu była praca A. van den Essena [AvdE] z 1986 roku.

§ 1. Oznaczenie i uwagi wstępne.

1. Przez $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}, \mathbb{N}$ oznaczać będziemy odpowiednio : ciało liczb zespolonych, rzeczywistych, wymiernych, pierścień liczb całkowitych i zbiór liczb naturalnych (całkowitych nieujemnych). Przez $\Bbbk$ oznaczać będziemy dowolne ciało nieskończone. O pierścieniach zakładamy stale, że są pierścieniami przemiennymi z jedynką.

Dowolnemu $\alpha = (\alpha_1, \dots, \alpha_n) \in \mathbb{N}^n$ odpowiada dokładnie jeden jednomian

$$X^\alpha = {X_1}^{\alpha_1} \dots {X_n}^{\alpha_n} \quad \text{stopnia} \quad |\alpha| \ = \alpha_1 + \dots + \alpha_n \, .$$

W powyższej odpowiedniości dodawaniu w $\mathbb{N}^n$ odpowiada mnożenie jednomianów.[1] W szczególności podzbiór $\emptyset \neq E \subset \mathbb{N}^n$ będziemy utożsamiać z podzbiorem

$$J(E) := \{X^\alpha \mid \alpha \in E\} \tag{i}$$

pierścienia $\Bbbk[X_1, \dots, X_n]$. Dla zbioru

$$\widehat{E} := \bigcup_{\alpha \in E} (\alpha + \mathbb{N}^n) \tag{ii}$$

zbiór $J(\widehat{E})$ jest zbiorem złożonym ze wszystkich jednomianów z ideału $< J(E) >$ generowanego przez zbiór $J(E)$. Zauważmy jeszcze, że układ jednomianów $X^{\alpha^{(1)}}, \dots, X^{\alpha^{(r)}}$ jest bazą ideału $< J(E) >$ wtedy i tylko wtedy, gdy

$$\widehat{E} = \bigcup_{j=1}^{r} (\alpha^{(j)} + \mathbb{N}^n) \, . \tag{iii}$$

Jeśli (iii), to układ $\mathfrak{A} = \{\alpha^{(1)}, \dots, \alpha^{(r)}\}$ nazywać będziemy *bazą* $\widehat{E}$.

[1] Fakt ten był już wykorzystywany przez G.Hermanna (p. [GH]) w latach trzydziestych.

Wielomian $P = \sum_{\alpha\in\mathbb{N}^n} c_\alpha X^\alpha$ o współczynnikach c_α należących do ciała $\Bbbk$ utożsamiamy z odwzorowaniem

$$\Phi_P : \mathbb{N}^n \ni \alpha \longrightarrow c_\alpha \in \Bbbk,$$

dla którego co najwyżej skończona ilość wartości jest różna od zera. Zbiór wielomianów o współczynnikach z ciała $\Bbbk$, wraz z naturalnymi działaniami dodawania i mnożenia, jest pierścieniem. Pierścień ten oznaczamy przez $\Bbbk[X_1, \dots, X_n]$ lub krótko przez $\Bbbk[X]$.

2. Niech $<$ będzie porządkiem w $\mathbb{N}^n$ spełniającym następujące dwa warunki

$$(\star) \qquad \forall\, \alpha \in \mathbb{N}^n \setminus \{0\}, \quad 0 < \alpha;$$

$$(\star\star) \qquad \forall\, \alpha, \beta, \gamma \in \mathbb{N}^n, \quad (\alpha < \beta \Longrightarrow \alpha + \gamma < \beta + \gamma).$$

Warunki $(\star), (\star\star)$ i następujące dwa są równoważne

$$(\sharp) \qquad \forall\, \alpha, \beta \in \mathbb{N}^n, \quad \beta \neq 0 \Longrightarrow \alpha < \alpha + \beta,$$

$$(\sharp\sharp) \qquad \forall\, \alpha, \beta, \gamma \in \mathbb{N}^n, \quad \alpha < \beta \Longleftrightarrow \alpha + \gamma < \beta + \gamma.$$

Przyjmujemy umowę:

$$\alpha \leq \beta \Longleftrightarrow \alpha < \beta \quad \text{ lub } \quad \alpha = \beta.$$

Mówiąc o porządku w $\mathbb{N}^n$ będziemy mieli na myśli porządek spełniający warunki $(\star)$, $(\star\star)$.

Lemat 1. *1. Najmniejszym elementem zbioru*

$$\alpha + \mathbb{N}^n := \{\alpha + \gamma \mid \gamma \in \mathbb{N}^n\}$$

jest α. W szczególności, jeśli X^α dzieli X^β, to $\alpha \leq \beta$.

2. Każdy silnie malejący ciąg w $\mathbb{N}^n$ jest skończony. W szczególności, każdy niepusty podzbiór $\mathbb{N}^n$ ma element najmniejszy.

3. (Lemat Dicksona [LED]) Jeśli $\emptyset \neq E \subset \mathbb{N}^n$, to istnieje dokładnie jeden podzbiór $\mathfrak{A} = \{\alpha^{(1)}, \dots, \alpha^{(r)}\} \subset E$, który jest minimalną bazą $\widehat{E}$.

Dowód. 1. jest natychmiastową konsekwencją $(\sharp\sharp)$.

Niech $\alpha^{(1)} > \alpha^{(2)} > \dots$ będzie malejącym ciągiem w $\mathbb{N}^n$. Ciągowi temu odpowiada wstępujący ciąg ideałów

$$< X^{\alpha^{(1)}} > \subset < X^{\alpha^{(1)}}, X^{\alpha^{(1)}} > \subset \dots,$$

który jest skończony, gdyż pierścień $\Bbbk[X_1 \dots, X_n]$ jest noetherowski, co kończy dowód 2.

Dla wykazania 3 wystarczy udowodnić, że jeśli $\mathfrak{B} = \{\beta^{(1)}, \dots, \beta^{(s)}\}$ jest bazą $\widehat{E}$ oraz $\mathfrak{A} = \{\alpha^{(1)}, \dots, \alpha^{(r)}\}$ bazą minimalną, to $\mathfrak{A} \subset \mathfrak{B}$. Możemy założyć że $\mathfrak{B}$ jest bazą uproszczoną tzn., że

$$\beta^{(i)} \notin \bigcup_{j\neq i} (\beta^{(j)} + \mathbb{N}^n), \quad \text{dla } i = 1, \dots, s,$$

gdyż w przeciwnym przypadku $\mathfrak{B} \setminus \{\beta^{(i)}\}$ też jest bazą. Gdyby istniało $j \in \{1, \dots, r\}$ takie, że $\alpha^{(i)} \notin \mathfrak{B}$, to istniałoby $i \in \{1, \dots, s\}$ takie, że $\alpha^{(j)} - \beta^{(i)} = \gamma \in \mathbb{N}^n \setminus \{0\}$. Zatem istniałoby $k \neq i$ takie, że $\beta^{(i)} - \alpha^{(k)} = \delta \in \mathbb{N}^n$. Stąd

$$\alpha^{(j)} = \beta^{(i)} + \gamma = \alpha^{(k)} + \delta + \gamma \in \alpha^{(k)} + \mathbb{N}^n,$$

co przeczy minimalności bazy $\mathfrak{A}$. □

3. Podamy teraz **przykłady ważne dla dalszych zastosowań.**

1. Porządek *leksykograficzny* :

$$\alpha <_l \beta \iff \exists\, j \in \{1, \dots, n\} \quad \text{takie, że} \quad \alpha_k = \beta_k \quad \text{gdy} \quad k < j \quad \text{oraz} \quad \alpha_j < \beta_j .$$

2. Porządek *leksykograficzny z gradacją* :

$$\alpha <_{lg} \beta \iff (\sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i) \quad \text{lub} \quad ((\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i) \quad \text{oraz} \quad \alpha <_l \beta) .$$

3. Porządek *odwrotnie leksykograficzny z gradacją* :

$$\alpha <_{ol} \beta \iff (\sum_{i=1}^{n} \alpha_i < \sum_{i=1}^{n} \beta_i) \quad \text{lub} \quad ((\sum_{i=1}^{n} \alpha_i = \sum_{i=1}^{n} \beta_i) \quad \text{oraz}$$
$$\exists\, j \in \{1, \dots, n\} \quad \text{takie, że} \quad \alpha_k = \beta_k \quad \text{dla} \quad k > j \quad \text{oraz} \quad \alpha_j > \beta_j) .$$

4. Porządek *indukowany przez formę* L.
Niech

$$L = \sum_{i=1}^{n} c_i X_i$$

będzie formą liniową o współczynnikach $c_i \geq 0$, dla $i = 1, \dots, n$.

$$\alpha <_L \beta \iff L(\alpha) < L(\beta) \quad \text{lub} \quad (L(\alpha) = L(\beta) \quad \text{oraz} \quad \alpha <_l \beta) .$$

W szczególności, gdy L jest formą zerową, to porządek indukowany przez L jest porządkiem leksykograficznym. Jeżeli $L = \sum_{i=1}^{n} X_i$, to indukowany przez nią porządek jest porządkiem leksykograficznym z gradacją.

5. Porządek *wyznaczony przez macierz* A. Niech

$$A := \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$

będzie macierzą o wyrazach rzeczywistych taką, że odwzorowanie $\mathbb{N}^n \ni \alpha \longrightarrow A\alpha \in \mathbb{N}^n$ jest bijektywne.[2]

[2]Dla celów praktycznych używa się jedynie macierzy o wyrazach z $\mathbb{N}$.

Mówimy, że $\alpha <_A \beta$ *w uporządkowaniu wyznaczonym przez macierz* A, *jeśli*
$A\alpha < A\beta$ *w uporządkowaniu leksykograficznym.*

Dla przykładu zauważmy, że macierz jednostkowa wyznacza porządek leksykograficzny, zaś macierz

$$\begin{pmatrix} 1 & 1 & \dots & 1 & 1 \\ 1 & 0 & \dots & 0 & 0 \\ 0 & 1 & \dots & 0 & 0 \\ \dots & \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 1 & 0 \end{pmatrix}$$

porządek leksykograficzny z gradacją w $\mathbb{N}^n$.

Przykłady.

$$\begin{aligned} &(0,2,0) <_l (1,0,0) <_l (1,0,1) \\ &(1,0,0) <_{lg} (0,2,0) <_{lg} (1,0,1)\,, \\ &(1,0,0) <_{ol} (1,0,1) <_{ol} (0,2,0)\,. \end{aligned}$$

Przy ustalonym porządku w $\mathbb{N}^n$, dla niezerowego wielomianu $P = \sum_\alpha c_\alpha X^\alpha$, definiujemy :

$$\begin{aligned} \deg(P) &:= \max\{\alpha \in \mathbb{N}^n \mid c_\alpha \neq 0\} && \text{(stopień P)} \\ \mathrm{lc}(P) &:= c_{\deg(P)} && \text{(współczynnik wiodący)} \\ \mathrm{in}(P) &:= \mathrm{lc}(P) X^{\deg(P)} && \text{(forma początkowa)}\,. \end{aligned}$$

Dla niepustego podzbioru $I \subset \Bbbk[X]$ definiujemy

$$\deg(I) := \{\deg(P) \mid P \in I \setminus \{0\}\}, \quad \mathrm{in}(I) := \{\mathrm{in}(P) \mid P \in I \setminus \{0\}\}\,.$$

Uwaga. Jeżeli P,Q są wielomianami niezerowymi, to

$$\deg(PQ) = \deg(P)\deg(Q) \quad \text{oraz} \quad \mathrm{in}(PQ) = \mathrm{in}(P)\,\mathrm{in}(Q)\,.$$

Przykład. Dla wielomianu

$$P = 3X_1^2X_2^4 + 5X_1^3X_2^3 + 7X_1^4X_2 + 8X_1^5$$

jest

$$\begin{aligned} &\text{(porządek leksykograficzny)} && \Longrightarrow \deg(P) = (5,0)\,, && \mathrm{in}(P) = 8X_1^5\,, \\ &\text{(porz. leksykograficzny z gradacją)} && \Longrightarrow \deg(P) = (3,3)\,, && \mathrm{in}(P) = 5X_1^3X_2^3 \\ &\text{(porz. odwrotnie leksykograficzny)} && \Longrightarrow \deg(P) = (2,4)\,, && \mathrm{in}(P) = 3X_1^2X_2^4\,. \end{aligned}$$

Przy uporządkowaniu leksykograficznym mamy

$$(2,4) < (3,3) < (4,1) < (5.0)\,.$$

Dzięki wzajemnie jednoznacznej odpowiedniości pomiędzy punktami $\alpha \in \mathbb{N}^n$ a jednomianami X^α, porządek leksykograficzny w $\mathbb{N}^2$ daje nierówności :

$$X_1^2X_2^4 < X_1^3X_2^3 < X_1^4X_2 < X_1^5 .$$

Przy porządku leksykograficznym z gradacją jest

$$X_1^4X_2 < X_1^5 < X_1^2X_2^4 < X_1^3X_2^3 .$$

Leksykograficzne uporządkowanie jednomianów, zmiennych X_1, X_2, jest następujące :

$$1 < X_2 < X_2^2 < \cdots < X_1 < X_1X_2 < X_1X_2^2 < \cdots < X_1^2 < X_1^2X_2 < X_1^2X_2^2 < \cdots \\ < X_1^3 < X_1^3X_2 < X_1^3X_2^2 < \cdots .$$

§ 2. Operacja $S(P,Q)$ i algorytm dzielenia

1. Niech "<"będzie porządkiem w $\mathbb{N}^n$. Zacznijmy od prostej obserwacji. Niech $\lambda = (\lambda_1, \dots, \lambda_n)$, $\mu = (\mu_1, \dots, \mu_n)$. Wtedy

$$\gamma = \gamma(\lambda, \mu) := (\gamma_1, \dots, \gamma_n) := (\max\{\lambda_1, \mu_1\}, \dots, \max\{\lambda_n, \mu_n\})$$

jest najmniejszym elementem zbioru

$$(\lambda + \mathbb{N}^n) \cap (\mu + \mathbb{N}^n) .$$

Niech $P, Q \in \Bbbk[X_1, \dots, X_n] \setminus \{0\}$. Niech

$$\alpha = \gamma(\deg(P), \deg(Q)) - \deg(P) , \qquad \beta = \gamma(\deg(P), \deg(Q)) - \deg(Q)$$

i niech liczby $a, b \in \Bbbk$ będą tak dobrane aby $a \cdot \mathrm{lc}(P) = b \cdot \mathrm{lc}(Q)$. Wielomian

$$S(P,Q) := aX^\alpha P - bX^\beta Q ,$$

nazywamy S-wielomianem od P, Q.

Wielomian $S(P,Q)$ jest wyznaczony jednoznacznie, z dokładnością do czynnika stałego.

Przykład. Ustalmy porządek leksykograficzny w $\mathbb{N}^2$. Dla wielomianów

$$P = 1 + X_1^3X_2 , \quad Q = 2X_1X_2 + 3X_1^2 + 4X_1^2X_2^3 \in \mathbb{Q}[X_1, X_2] ;$$

$$\deg(P) = (3,1),\ \deg(Q) = (2,3),\ \gamma = (3,3),\ \alpha = (0,2),\ \beta = (1,0) ,$$
$$S(P,Q) = 2X_2^2 \cdot P - 3X_1 \cdot Q = 2X_2^2 - 6X_1^2X_2 - 9X_1^3 .$$

Dla dowolnego podzbioru $F \subset \Bbbk[X]$, zbiór

$$< F > := \{P \in \Bbbk[X] \mid \exists Q_1, \dots, Q_l \in F; h_1, \dots h_l \in \Bbbk[X] \\ \text{takie,że} \quad P = h_1Q_1 + \cdots + h_lQ_l \}$$

jest ideałem pierścienia $\Bbbk[X]$.

Interesującym nas przypadkiem jest podzbiór $F = \{F_1, \dots, F_l\}$ złożony ze skończonej ilości wielomianów $F_1, \dots, F_l$. Ponieważ każdy ideał pierścienia $\Bbbk[X]$ jest skończenie generowany, założenie skończoności zbioru F nie zmniejsza ogólności rozważań.

2. Algorytm dzielenia. Niech $F = \{F_1, \dots, F_l\}$ będzie układem l wielomianów, n zmiennych $X_1, \dots, X_n$, o współczynnikach z ciała $\Bbbk$. Rozpoczniemy od kilku obserwacji dotyczących ideału

$$< \mathrm{in}(F) > = < \mathrm{in}(F_1), \dots, \mathrm{in}(F_l) > .$$

Ideał $< \mathrm{in}(F) >$ jest ideałem jednorodnym.

Zauważmy, że

$$(P = \sum_{\alpha \in \mathbb{N}^n} c_\alpha X^\alpha \in < \mathrm{in}(F) >) \iff (c_\alpha \neq 0 \Longrightarrow \alpha \in \bigcup_{i-1}^{l} (\deg(F_i) + \mathbb{N}^n)) .$$

Zatem zbiór

$$\text{(i)} \qquad \bigcup_{i=1}^{l} (\deg(F_i) + \mathbb{N}^n) , \qquad$$

w pełni charakteryzuje ideał $< \mathrm{in}(F) >$.

To wszystko ma sens przy założeniu, że w $\mathbb{N}^n$ został ustalony jakiś porządek.

Uwaga 1. Zmieniając, w razie potrzeby, F_j na $\frac{1}{\mathrm{lc}(F_j)} F_j$ możemy założyć, że $\mathrm{lc}(F_j) = 1$ dla $j = 1, \dots, l$.

Uwaga 2. Jeżeli istnieje $j \neq i$ takie, że

$$\deg(F_i) \in (\deg(F_j) + \mathbb{N}^n) ,$$

to

$$< \mathrm{in}(F \setminus \{F_i\}) > = < \mathrm{in}(F) > .$$

Definicja 1. Mówimy, że układ F jest uproszczony, jeśli

$$\text{(*)} \qquad \begin{aligned} &\mathrm{lc}(F_j) = 1 , \qquad \text{dla } j = 1, \dots, l , \\ &\deg(F_i) \in (\deg(F_j) + \mathbb{N}^n) \Longrightarrow (i = j) . \end{aligned}$$

Układ F nazywamy zredukowanym[3] gdy jest on uproszczony oraz dla $F_i = \sum_{\alpha \in \mathbb{N}^n} c_\alpha^i X^\alpha$ jest

$$\text{(**)} \qquad (\alpha < \deg(F_i) , \alpha \in \bigcup_{j=1}^{l} (\deg(F_j) + \mathbb{N}^n)) \Longrightarrow (c_\alpha^i = 0) .$$

[3]To czy układ jest zredukowany lub uproszczony zależy od porządku w $\mathbb{N}^n$.

Definicja 2. Wielomian

$$L := \sum_{\alpha\in\mathbb{N}^n, P\in F} c_{\alpha,P} X^\alpha P\,,$$

o współczynnikach $c_{\alpha,P} \in \Bbbk$, nazywamy dopuszczalną kombinacją dla F, jeżeli

$$\deg(L) = \max\{\deg(X^\alpha P) \mid c_{\alpha,P} \neq 0\}\,.$$

Twierdzenie A. *(Pierwsze twierdzenie o dzieleniu.) Dla dowolnego* $Q \in \Bbbk[X]\setminus\{0\}$ *istnieją wielomiany* L , $\widetilde{Q}$ *takie, że:*

(a) *jeśli* $\mathrm{in}(Q) \notin <\mathrm{in}(F)>$, *to* $L = 0, \widetilde{Q} = Q$,
(b) *jeśli* $\mathrm{in}(Q) \in <\mathrm{in}(F)>$, *to* L *jest dopuszczalną kombinacją dla* F *taką, że* $\mathrm{in}(L) = \mathrm{in}(Q)$, *oraz albo* $\widetilde{Q} = 0$ *albo* $\mathrm{in}(\widetilde{Q}) \notin <\mathrm{in}(F)>$.

Dowód. Podamy algorytm przy pomocy którego znajdujemy L , $\widetilde{Q}$. Jeśli

$$\mathrm{in}(Q) \notin <\mathrm{in}(F)>,$$

to sprawa jest oczywista. Załóżmy więc, że $\mathrm{in}(Q) \in <\mathrm{in}(F)>$.

Opis algorytmu i dowód jego skończoności:

Krok 1:
a) Kładziemy $Q_0 := Q$,
b) Wybieramy takie $j \in \{1,\dots,l\}$, aby $\deg(Q_0) \in (\deg(F_j) + \mathbb{N}^n)$. Mamy teraz

$$\deg(Q_0) = \deg(F_j) + \beta\,, \quad \text{gdzie}\, \beta \in \mathbb{N}^n\,,$$

c) Kładziemy

$$L_0 := \frac{\mathrm{lc}(Q_0)}{\mathrm{lc}(F_j)} X^\beta F_j\,.$$

Przy tak zdefiniowanym L_0 jest : $\mathrm{in}(L_0) = \mathrm{in}(Q_0)$. Teraz kładziemy

$$Q_1 := Q_0 - L_0$$

d) Jeśli $Q_1 = 0$ lub $\mathrm{in}(Q_1) \notin <\mathrm{in}(F)>$, to $L = L_0$ oraz $\widetilde{Q} = Q_1$. Jeśli $\mathrm{in}(Q_1) \in <\mathrm{in}(F)>$, to powtarzamy **Krok 1.**, tzn. konstruujemy L_1 dla Q_1 tak samo jak L_0 dla Q_0. Potem kładziemy

$$Q_2 := Q_1 - L_1$$

i powtarzamy postępowanie.

Krok 2:
Kontynuując postępowanie indukcyjne przypuśćmy, że Q_k zostało już skonstruowane. Wtedy, tak jak w kroku pierwszym, konstruujemy L_k i kładziemy

$$Q_{k+1} := Q_k - L_k\,.$$

Postępowanie kończymy, gdy $Q_k = 0$ lub $Q_k \notin < \mathrm{in}(F) >$. Jeśli tak jest, to wystarczy przyjąć

$$L := \sum_{j=0}^{k-1} L_j \qquad \text{oraz} \qquad \widetilde{Q} := Q_k \,.$$

Fakt, że L jest dopuszczalną kombinacją dla F jest prosty do zauważenia.

Krok 3:
Dowodzimy skończoności algorytmu. W tym celu zauważmy, że

$$\deg(Q_0) > \deg(Q_1) > \dots \,.$$

Zatem ciąg $\deg(Q_1), \deg(Q_2), \dots$ jest malejącym ciągiem w $\mathbb{N}^n$, a więc, na mocy lematu 1, pkt 2, §1 musi być skończony. Zatem istnieje $k \in \mathbb{N}$ takie, że albo $Q_k = 0$ albo $Q_k \notin < \mathrm{in}(F) >$.

Definicja. Wielomian $\widetilde{Q}$ nazywamy resztą z dzielenia Q przez $F_1, \dots, F_l$.

W pierwszym twierdzeniu o dzieleniu wielomiany L, $\widetilde{Q}$ nie są wyznaczone jednoznacznie. Niejednoznaczna jest konstrukcja wielomianów $L_0, L_1, \dots, L_k$. Istotnym jest jedynie to, aby wielomian L był dopuszczalną kombinacją dla F taką, że $\mathrm{in}(L) = \mathrm{in}(Q)$. Fakt ten jest prosty do sprawdzenia.

W następnym twierdzeniu o dzieleniu uzyskamy jednoznaczność, z dokładnością do kolejności w jakiej występują $F_1, \dots, F_l$. Rozpoczniemy od oznaczeń:

$$\Delta_1 := \deg(F_1) + \mathbb{N}^n, \dots, \Delta_i := (\deg(F_i) + \mathbb{N}^n) \setminus \bigcup_{j<i} \Delta_j \,, \text{ dla } i = 2, \dots, l \,,$$

$$\widetilde{\Delta} := \mathbb{N}^n \setminus \bigcup_{i=1}^{l} \Delta_i \,.$$

Twierdzenie B. *(O dzieleniu z jednoznacznością). Dla dowolnego $Q \in \Bbbk[X]$ istnieją $P_1, \dots, P_l$ i $\widetilde{Q} \in \Bbbk[X]$ takie, że*

(i) $$Q = P_1F_1 + \ldots + P_lF_l + \widetilde{Q} \,,$$

(ii) *jeśli* $P_i = \sum_\alpha c_\alpha^i X^\alpha, \quad c_\alpha^i \neq 0 \Longrightarrow \deg(F_i) + \alpha \in \Delta_i \,, \quad$ *dla* $i = 1, \dots, l \,,$

(iii) $$\text{jeśli} \quad \widetilde{Q} = \sum_\alpha b_\alpha X^\alpha, \text{ to} \quad b_\alpha \neq 0 \Longrightarrow \alpha \in \widetilde{\Delta} \,.$$

Ponadto

(iv) $$\begin{aligned} &(Q \neq 0,\, \widetilde{Q} \neq 0) \Longrightarrow \deg(\widetilde{Q}) \leq \deg(Q) \,, \\ &(Q \neq 0,\, P_i \neq 0) \Longrightarrow \deg(P_i) + \deg(F_i) \leq \deg(Q) \,. \end{aligned}$$

Warunki $(i),(ii),(iii)$ *wyznaczają* $P_1,\dots,P_l,\widetilde{Q}$ *jednoznacznie*[4]. *Wielomian* $\widetilde{Q}$ *nie zależy od kolejności w jakiej występują* $F_1,\dots,F_l$.

Dowód. Polega na konstrukcji algorytmu.

Jeśli $Q=0$, to kładąc $P_1=\ldots=P_l=\widetilde{Q}=0$ otrzymujemy szukane wielomiany. Jeśli $Q\neq 0$, to rozpoczynamy algorytm.

Krok 1:

Dla $Q\neq 0$ mogą się zdarzyć dwa przypadki:

1^0. $\deg(Q)\in\widetilde{\Delta}$. Wtedy kładziemy

$$\widetilde{Q}^{(1)}:=\mathrm{in}(Q),\ \ P_j^{(1)}:=0,\quad \text{dla}\quad j=1,\dots,l$$

oraz

$$(*)\qquad Q^{(1)}:=Q-\sum_{j=1}^{l}P_j^{(1)}F_j-\widetilde{Q}^{(1)}.$$

2^0. $\exists\, i\in\{1,\dots,l\}$ takie, że $\deg(Q)\in\Delta_i$. Oznacza to, że

$$\exists\,\beta\in\mathbb{N}^n \text{ takie, że } \deg(Q)=\deg(F_i)+\beta.$$

Teraz kładąc

$$\widetilde{Q}^{(1)}:=0\,,P_j^{(1)}:=0 \text{ dla } j\neq i\,,P_i^{(1)}:=\frac{\mathrm{lc}(Q)}{\mathrm{lc}(F_i)}X^{\beta}$$

definiujemy $Q^{(1)}$ wzorem (*).

Jeśli $Q^{(1)}=0$, to $P_j=P_j^{(1)}$, dla $j=1,\dots,l$, oraz $\widetilde{Q}=\widetilde{Q}^{(1)}$ są szukanymi wielomianami i "Krok 1" kończy algorytm.

Jeśli $Q^{(1)}\neq 0$, to przechodzimy do kroku następnego.

Krok 2:

Polega na powtórzeniu kroku 1 z $Q=Q^{(1)}$, tzn definiujemy $P_j^{(2)}$, dla $j=1,\dots,l$, $\widetilde{Q}^{(2)}$ oraz $Q^{(2)}$ tak samo jak $P_j^{(1)}$, dla $j=1,\dots,l$, $\widetilde{Q}^{(1)}$ oraz Q^1 w "Kroku 1".

Jeśli $Q^{(2)}=0$, to szukanymi wielomianami są:

$$P_j:=P_j^{(1)}+P_j^{(2)}\quad \text{dla } j=1,\dots,l\,,$$
$$\widetilde{Q}:=\widetilde{Q}^{(1)}+\widetilde{Q}^{(2)}.$$

Natomiast jeśli $Q^{(2)}\neq 0$, to przechodzimy do kroku następnego.

. . . . . .

Krok k**:**

[4]Zależą one jedynie od kolejności w jakiej występują wielomiany $F_1,\dots,F_l$.

W kroku $k-1$ otrzymaliśmy wielomiany:

$$P_1^{(k-1)}, \dots, P_l^{(k-1)}, \widetilde{Q}^{(k-1)} \text{ oraz } Q^{(k-1)}\,.$$

Zgodnie z poprzednią uwagą, "Krok k" wykonujemy gdy $Q^{(k-1)} \neq 0$, ponieważ $Q^{(k-1)} = 0$ kończy procedurę. Krok ten, podobnie jak "Krok 2", jest powtórzeniem "Kroku 1" z $Q = Q^{(k-1)}$. Po przeprowadzeniu odpowiednich rachunków otrzymamy wielomiany: $P_1^{(k)}, \dots, P_l^{(k)}, \widetilde{Q}^{(k)}$ oraz

$$Q^{(k)} := Q^{(k-1)} - \sum_{j=1}^{l} P_j^{(k)} F_j - \widetilde{Q}^{(k)}\,.$$

Ciąg $\deg(Q), \deg(Q^{(1)}), \deg(Q^{(2)}), \dots$ jest silnie malejący. Na mocy lematu 1, §1 jest on skończony. Zatem istnieje $k \in \mathbb{N}$ takie, że $Q^{(k)} = 0$. Mamy teraz równości:

$$\begin{cases} Q^{(1)} & := Q - \sum_{j=1}^{l} P_j^{(1)} F_j - \widetilde{Q}^{(1)} \\ Q^{(2)} & := Q^{(1)} - \sum_{j=1}^{l} P_j^{(2)} F_j - \widetilde{Q}^{(2)} \\ \vdots & \quad \vdots \quad \vdots \\ Q^{(k-1)} & := Q^{(k-2)} - \sum_{j=1}^{l} P_j^{(k-1)} F_j - \widetilde{Q}^{(k-1)} \\ 0 & := Q^{(k-1)} - \sum_{j=1}^{l} P_j^{(k)} F_j - \widetilde{Q}^{(k)}\,. \end{cases}$$

Po dodaniu stronami otrzymamy, że

$$\begin{aligned} P_j &:= P_j^{(1)} + P_j^{(2)} + \ldots + P_j^{(k)}\,, \quad \text{dla } j = 1, \dots, l\,, \\ \widetilde{Q} &:= \widetilde{Q}^{(1)} + \widetilde{Q}^{(2)} + \ldots + \widetilde{Q}^{(k)} \end{aligned}$$

są szukanymi wielomianami.

Dowód jednoznaczności pominiemy, gdyż nie odgrywa ona istotnej roli w dalszych rozważaniach (szczegóły można znaleźć w [ML-J]).

Dla podania przykładu weźmy $n = 2$ i porządek leksykograficzny w $\mathbb{N}^2$.

Przykład. Dla

$$F_1 = X_1^3, \quad F_2 = X_1^2 X_2 - X_2^3, \quad Q = X_1^3 X_2$$

mamy

$$\mathrm{in}(F_1) = X_1^3,\ \mathrm{in}(F_2) = X_1^2 X_2,\ \mathrm{in}(Q) = X_1^3 X_2,$$
$$\deg(Q) \in \Delta_1,\ \deg(F_1) + (0,1) = \deg(Q)\,.$$

Z "kroku 1" mamy

$$\widetilde{Q}^{(1)} = 0 = \widetilde{Q},\ P_1 = X_2,\ P_2 = 0,\ Q^{(1)} = 0$$

Jeśli natomiast

$$F_1 = X_1^2 X_2 - X_2^3,\ F_2 = X_1^3,\ Q = X_1^3 X_2\,,$$

to po dwóch krokach otrzymamy:

$$P_1 = X_1,\ P_2 = 0,\ \widetilde{Q} = X_1 X_2^3\,.$$

§ 3. Bazy Gröbnera

1. Przy ustalonym porządku w $\mathbb{N}^n$, ideałowi I pierścienia $\Bbbk[X_1,\dots,X_n]$ odpowiada ideał jednorodny $<\mathrm{in}(I)>$. Ideał ten jest generowany przez skończony układ jednomianów. Jednomiany te są formami początkowymi wielomianów z ideału I. Zatem istnieją wielomiany $G_1,\dots,G_k$ należące do ideału I takie, że

$$(*) \qquad <\mathrm{in}(I)>=<\mathrm{in}(G_1),\dots,\mathrm{in}(G_k)>\ .$$

Definicja. Skończony układ $G=\{G_1,\dots,G_k\}$ wielomianów ideału I nazywamy jego bazą Gröbnera[5], jeśli zachodzi równość $(*)$.

Bazę Gröbnera G nazywamy uproszczoną bazą Gröbnera, gdy układ G jest uproszczony[6], natomiast zredukowaną bazą Gröbnera, gdy układ G jest zredukowany.

Baza Gröbnera zawsze istnieje, ale nie jest wyznaczona jednoznacznie.

Uproszczona baza Gröbnera jest minimalną bazą[7] i nie jest wyznaczona jednoznacznie (z wyjątkiem bardzo szczególnych przypadków.) Uwaga 2 (§2,2.) pozwala z bazy Gröbnera otrzymać uproszczoną bazę Gröbnera.

Zredukowana baza Gröbnera jest wyznaczona jednoznacznie.

Twierdzenie 1. *Jeżeli $G=\{G_1,\dots,G_k\}$ jest bazą Gröbnera ideału I, to $I=<G_1,\dots,G_k>$.*

Dowód. Inkluzja $<G_1,\dots,G_k>\subset I$ jest oczywista. Dla wykazania inkluzji przeciwnej weźmy dowolny wielomian $Q\in I$. Dzieląc Q przez $G_1,\dots,G_k$ otrzymamy:

$$Q=H_1G_1+\ldots+H_kG_k+\widetilde{Q}\,,$$

gdzie $H_1,\dots,H_k,\widetilde{Q}$ są wielomianami. Ponieważ $Q\in I$, więc $\widetilde{Q}\in I$. Stąd $\mathrm{in}(\widetilde{Q})\in<\mathrm{in}(G)>$, co daje $\widetilde{Q}=0$. Zatem $Q\in<G_1,\dots,G_k>$.

Niech $F=\{F_1,\dots,F_l\}$ będzie układem l wielomianów n zmiennych, o współczynnikach z ciała $\Bbbk$. Ideał $I=<F_1,\dots,F_l>$ pierścienia $\Bbbk[X_1,\dots,X_n]$ ma wiele innych układów generatorów. Każde dwa układy generatorów mają bardzo ważną[8] cechę wspólną: jeśli $G_1,\dots,G_l$ jest innym układem generatorów ideału I, to

$$\{x\in\Bbbk^n \mid F_1(x)=\ldots=F_l(x)=0\}=\{x\in\Bbbk^n \mid G_1(x)=\ldots=G_l(x)=0\}\,.$$

W szczególności na bazę Gröbnera możemy patrzeć jak na układ równań równoważny układowi: $F_1(x)=\ldots=F_l(x)=0$. Baza Gröbnera zależy od porządku w $\mathbb{N}^n$. Pojawiają się dwa naturalne pytania:

1. Który porządek w $\mathbb{N}^n$ jest "dobry" dla rozwiązywania wielomianowych układów równań ?
2. Jak znaleźć bazę Gröbnera ?

Przy rozwiązywaniu wielomianowych układów równań "dobrym" okazuje się porządek leksykograficzny. Mamy bowiem następujące twierdzenie.

---

[5] Dla zmiennych w kolejności : $X_1,\dots,X_n$ względem ustalonego porządku w $\mathbb{N}^n$.

[6] W sensie definicji 1, pkt2., §1.

[7] Tzn. nie zawiera "zbędnych" wielomianów.

[8] Dla wielomianowych układów równań.

Twierdzenie 2. *Niech G będzie bazą Gröbnera ideału I, przy porządku leksykograficznym w $\mathbb{N}^n$.*

Jeśli $I \cap \Bbbk[X_s, \dots, X_n] \neq \{0\}$, to

$$G_s := G \cap \Bbbk[X_s, \dots, X_n]$$

jest bazą Gröbnera ideału

$$I_s := I \cap \Bbbk[X_s, \dots, X_n].$$

Dowód tego twierdzenia można znaleźć w [FPaMP].

Aby odpowiedzieć na drugie pytanie. podamy algorytm polegający na skończonej ilości operacji wymiernych na współczynnikach wielomianów $F_1, \dots, F_l$, prowadzący do bazy Gröbnera ideału $< F_1, \dots, F_l >$.

2. Konstrukcja algorytmu. Niech $F^0 := F = \{F_1, \dots, F_l\}$.

Krok 1. Dla $P, Q \in F^0$ obliczamy $S(P,Q)$ i następnie obliczamy resztę $\widetilde{S(P,Q)}$ z dzielenia wielomianu $S(P,Q)$ przez układ F^0. Teraz tworzymy

$$F^1 := F^0 \cup (\{\widetilde{S(P,Q)} \mid P, Q \in F^0\} \setminus \{0\}).$$

Po i-tym kroku wykonujemy :

Krok i+1. Jest on powtórzeniem kroku 1, z tą tylko różnicą, że rolę F^0 pełni teraz F^i, tzn. wyznaczamy

$$F^{i+1} := F^i \cup (\{\widetilde{S(P,Q)} \mid P, Q \in F^i\} \setminus \{0\}),$$

gdzie $\widetilde{S(P,Q)}$, podobnie jak w kroku 1, jest resztą z dzielenia wielomianu $S(P,Q)$ przez układ F^i.

Postępowanie kończymy gdy $F^i = F^{i+1}$. Jeśli tak jest, to F^i jest bazą Gröbnera ideału $< F >$. Dowód tego faktu można znaleźć w cytowanej literaturze. Skończoność algorytmu jest dość prostą konsekwencją tego, że pierścień $\Bbbk[X_1, \dots, X_n]$ jest pierścieniem noetherowskim.

Po wykonaniu powyższego algorytmu przystępujemy do uproszczenia otrzymanej bazy. Robimy to w oparciu o uwagę 2, §3. Po uproszczeniu otrzymamy uproszczoną bazę Gröbnera, którą następnie redukujemy. Dla otrzymania bazy zredukowanej należy wykonać skończoną ilość operacji $S(\cdot, \cdot)$.

§ 4. Zastosowania baz Gröbnera w teorii odwzorowań wielomianowych.

Dobrym, dla zastosowań w teorii odwzorowań wielomianowych, jest porządek n–rozdzielający zmienne $X = (X_1, \dots, X_n)$, $Y = (Y_1, \dots, Y_m)$.

Definicja. Mówimy, że $<$ jest porządkiem n– rozdzielającym zmienne X, Y, jeśli

(1) $<$ jest porządkiem w $\mathbb{N}^{n+m}$,
(2) dla dowolnego $\alpha \in \mathbb{N}^n \setminus \{0\}$ oraz $\beta \in \mathbb{N}^m$ zachodzi nierówność : $Y^\beta < X^\alpha$.

Niech $P = (P_1, \dots, P_m) \colon \Bbbk^n \longrightarrow \Bbbk^m$ będzie odwzorowaniem wielomianowym. Odwzorowanie to utożsamiamy z jego wykresem, zaś wykres z ideałem

$$\mathfrak{a}_P := < Y_1 - P_1(X_1, \dots, X_n), \dots, Y_m - P_m(X_1, \dots, X_n) >$$

pierścienia $\Bbbk[X_1, \dots, X_n, Y_1, \dots, Y_m] = \Bbbk[X, Y]$, który jest ideałem wykresu odwzorowania P. Jeśli V jest algebraicznym podzbiorem $\Bbbk^n$, którego ideał jest generowany przez wielomiany $H_1(X), \dots, H_r(X)$, to

$$\mathfrak{a}_{P|V} := < H_1(X), \dots, H_r(X), Y_1 - P_1(X_1, \dots, X_n), \dots, Y_m - P_m(X_1, \dots, X_n) >$$

jest ideałem wykresu odwzorowania $P|V$. Dla ideału $\mathfrak{a} = \mathfrak{a}_P$ lub $\mathfrak{a}_{P|V}$ definiujemy

$$(*) \qquad \begin{aligned} \mathfrak{a}(X) &= \mathfrak{a} \cap \Bbbk[X_1, \dots, X_n] \\ \mathfrak{a}(Y) &= \mathfrak{a} \cap \Bbbk[Y_1, \dots, Y_m] \\ \mathfrak{a}(X, Y) &= \mathfrak{a} \setminus (\mathfrak{a}(X) \cup \mathfrak{a}(Y)) \end{aligned}$$

1. $\mathfrak{a}(X)$ jest ideałem pierscienia $\Bbbk[X_1, \dots, X_n]$. Jest to ideał zbioru V.

2. Wielomian $G(Y_1, \dots, Y_m) \in \mathfrak{a}(Y)$ wtedy i tylko wtedy gdy $G(Y_1, \dots, Y_m)$ znika na obrazie P. Zatem

(a) $\mathfrak{a}(Y) = \{0\}$ wtedy i tylko wtedy, gdy P jest odwzorowaniem dominującym.

(b) (M. Kwieciński, [MK]) $\mathfrak{a}(Y)$ jest ideałem zbioru $P(V)$.

3. $\mathfrak{a}(X, Y)$ decyduje o własnościach odwzorowania P.

(a) (A. van den Essen, [AvdE]) Jeśli $m = n$, to odwzorowanie P jest wielomianowym automorfizmem $\Bbbk^n$ wtedy i tylko wtedy, gdy $\mathfrak{a}_P(X, Y)$ zawiera wielomiany postaci

$$(**) \qquad X_1 - G_1(Y_1, \dots, Y_n), \dots, X_n - G_n(Y_1, \dots, Y_n)$$

Wtedy układ $(**)$ jest zredukowaną bazą Gröbnera ideału $\mathfrak{a}_P$, względem dowolnego porządku n– rozdzielającego zmienne X, Y. Ponadto $G|P(V) := (G_1, \dots, G_n)|P(V)$ jest odwrotne do $P|V$.

(b) (M. Kwieciński, [MK], m, n dowolne) $P|V : V \longrightarrow P(V)$ jest izomorfizmem[9] wtedy i tylko wtedy, gdy $\mathfrak{a}_{P|V}(X, Y)$ zawiera wielomiany postaci

$$(***) \qquad X_1 - G_1(Y_1, \dots, Y_m), \dots, X_n - G_n(Y_1, \dots, Y_m)$$

[9]Tzn. P jest różnowartościowe na V, $P(V)$ jest algebraicznym podzbiorem $\mathbb{C}^m$, oraz $(P|V)^{-1} : P(V) \longrightarrow V$ jest wielomianowe.

Wtedy układ $(***)$ zawiera się w zredukowanej bazie Gröbnera ideału $\mathfrak{a}_{P|V}$, względem dowolnego porządku n–rozdzielającego zmienne X, Y.

(c) Jeśli $\Bbbk = \mathbb{C}$ i $m \leq n$, to P jest odwzorowaniem właściwym wtedy i tylko wtedy, gdy $\mathfrak{a}_P(X, Y)$ zawiera wielomiany postaci

$$X_j^{k_j} + c_1^{(j)}(Y)X_j^{k_j-1} + \ldots + c_{k_j}^{(j)}(Y)\,, \text{dla} \quad j = 1, \ldots, n\,,$$

gdzie $c_i^{(j)}(Y) \in \mathbb{C}[Y_1, \ldots, Y_m]$. Wynika to z faktu, że P jest właściwe wtedy i tylko wtedy, gdy $\mathbb{C}[X]$ jest całkowitym rozszeniem pierscienia $P^\star(\mathbb{C}[Y])$, gdzie $P^\star$ jest dane wzorem

$$P^\star(H)(X) = H(P(X)) \qquad \text{dla} \quad H \in \mathbb{C}[Y]\,.$$

W takim przypadku zredukowana baza Gröbnera ideału $\mathfrak{a}_P$, względem porządku leksykograficznego, przy zmiennych w kolejności $X_1, \ldots, X_n$, $Y_1, \ldots, Y_m$, zawiera wielomiany postaci

$$(\sharp) \qquad \begin{array}{l} X_1^{k_1} + c_1^{(1)}(Y)X_1^{k_1-1} + \ldots + c_{k_1}^{(1)}(Y)\,, \\ X_2^{k_2} + c_1^{(2)}(X_1, Y)X_2^{k_2-1} + \ldots + c_{k_2}^{(2)}(X_1, Y)\,, \\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ X_n^{k_n} + c_1^{(n)}(X_1, \ldots, X_{n-1}, Y)X_n^{k_n-1} + \ldots + c_{k_n}^{(n)}(X_1, \ldots, X_{n-1}, Y)\,. \end{array}$$

Podamy teraz kilka przykładów baz Gröbnera. Obliczenia zostały wykonane na komputerze IBM PT (AT 386), przy użyciu programu "FELIX", którego autorami są: J.Apel, U.Klaus z Uniwersytetu w Lipsku.

Przykład 1. Niech

$$h :=< X + Y^2 - 2YZ + Z^2 - U, -XZ + Y - V, -X^2 + Z - W >$$

będzie ideałem pierscienia $\mathbb{C}[X, Y, Z, U, V, W]$.

(a) Jeśli w $\mathbb{N}^6$ ustalimy porządek leksykograficzny oraz zmienne w kolejności: X, Y, Z, U, V, W, to zredukowana baza Gröbnera ideału h składa się z 7 następujących wielomianów:

$G_1 = U^2 - 2UV^2 + V^4 + W - Z + 4UVZ - 4V^3Z + 4VWZ - 2UZ^2 - 4VZ^2 + 6V^2Z^2 - 4WZ^2 + 2UWZ^2 + 2V^2WZ^2 + 4Z^3 - 2UZ^3 - 4VZ^3 - 2V^2Z^3 - 4VWZ^3 + Z^4 + 4VZ^4 + 2WZ^4 + W^2Z^4 - 2Z^5 - 2WZ^5 + Z^6$,

$G_2 = \frac{U^2}{4} - \frac{V}{8} + UV - \frac{3U^2V}{2} - \frac{5V^2}{4} + UV^2 + \frac{U^2V^2}{2} + 2UV^3 - \frac{9V^4}{4} - \frac{V^5}{2} - \frac{V^6}{2} + \frac{W}{4} - UVW - \frac{U^2VW}{2} + \frac{3V^2W}{4} + 2V^3W + \frac{V^5W}{2} - \frac{3VW^2}{4} + \frac{Y}{8} - UY + U^2Y + \frac{5VY}{4} - \frac{3UVY}{2} - UV^2Y + \frac{5V^3Y}{2} - UV^3Y + V^5Y - \frac{WY}{2} + UWY - \frac{VWY}{4} - 2V^2WY + UV^2WY - V^4WY + \frac{W^2Y}{4} - \frac{Z}{4} - \frac{UZ}{8} + \frac{U^2Z}{2} + \frac{VZ}{2} - \frac{UVZ}{4} + \frac{U^2VZ}{2} - \frac{3V^2Z}{8} - 2UV^2Z + \frac{V^3Z}{4} + \frac{3V^4Z}{2} - \frac{V^5Z}{2} - \frac{WZ}{2} + \frac{3UWZ}{2} - \frac{U^2WZ}{2} + \frac{VWZ}{2} + \frac{UVWZ}{4} - \frac{5V^2WZ}{2} + \frac{3V^3WZ}{4} + \frac{V^4WZ}{2} + \frac{W^2Z}{2} - \frac{UW^2Z}{4} - \frac{3V^2W^2Z}{4} + \frac{Z^2}{2} - \frac{3UZ^2}{2} + \frac{U^2Z^2}{2} - \frac{VZ^2}{4} + \frac{5UVZ^2}{4} + V^2Z^2 - \frac{UV^2Z^2}{2} - \frac{9V^3Z^2}{4} - WZ^2 + \frac{UWZ^2}{2} + VWZ^2 + UVWZ^2 - V^2WZ^2 + \frac{UV^2WZ^2}{2} - V^3WZ^2 - \frac{V^4WZ^2}{2} + \frac{3VW^2Z^2}{2} - \frac{UVW^2Z^2}{2} + \frac{V^3W^2Z^2}{2} + \frac{5Z^3}{8} - \frac{3UZ^3}{4} + \frac{VZ^3}{4} - UVZ^3 + \frac{9V^2Z^3}{4} -$

$\frac{UV^2Z^3}{2}+V^3Z^3+\frac{V^4Z^3}{2}+\frac{3WZ^3}{8}-UWZ^3-\frac{3VWZ^3}{2}+UVWZ^3+V^2WZ^3-V^3WZ^3-\frac{W^2Z^3}{4}-\frac{UW^2Z^3}{2}+\frac{VW^2Z^3}{4}+\frac{V^2W^2Z^3}{2}-\frac{W^3Z^3}{4}-\frac{5Z^4}{8}+UZ^4-\frac{UVZ^4}{2}-V^2Z^4+\frac{V^3Z^4}{2}+UWZ^4-\frac{VWZ^4}{2}-V^2WZ^4+\frac{W^2Z^4}{2}+\frac{Z^5}{4}-\frac{UZ^5}{2}+\frac{VZ^5}{4}+\frac{V^2Z^5}{2}-\frac{WZ^5}{4}$,

$G_3=\frac{-V}{2}+UV-\frac{V^2}{2}-V^3+\frac{VW}{2}+\frac{Y}{2}-UY+\frac{VY}{2}+V^2Y-\frac{WY}{2}-\frac{UZ}{2}-\frac{VZ}{2}-\frac{UVZ}{2}+\frac{3V^2Z}{2}-\frac{V^3Z}{2}-WZ+\frac{UWZ}{2}+\frac{V^2WZ}{2}+\frac{YZ}{2}-VYZ+V^2YZ-VWYZ+Z^2-\frac{UZ^2}{2}-VZ^2-\frac{V^2Z^2}{2}-VWZ^2+\frac{Z^3}{2}+\frac{3VZ^3}{2}+WZ^3-\frac{VWZ^3}{2}+\frac{W^2Z^3}{2}-Z^4+\frac{VZ^4}{2}-WZ^4+\frac{Z^5}{2}$,

$G_4=\frac{U^2}{2}-\frac{V}{4}+UV-\frac{3V^2}{2}-V^3-\frac{V^4}{2}+\frac{W}{2}+\frac{VW}{2}+\frac{Y}{4}-UY+\frac{3VY}{2}-UVY+V^2Y+V^3Y-\frac{WY}{2}-\frac{Z}{2}-\frac{UZ}{4}-\frac{UVZ}{2}+\frac{7V^2Z}{4}-\frac{V^3Z}{2}-WZ+\frac{UWZ}{2}+\frac{VWZ}{2}+\frac{V^2WZ}{2}+UYZ-\frac{3VYZ}{2}+\frac{WYZ}{2}-VWYZ+Z^2-UZ^2-\frac{3VZ^2}{2}-WZ^2+\frac{UWZ^2}{2}-VWZ^2-\frac{V^2WZ^2}{2}+\frac{5Z^3}{4}-\frac{UZ^3}{2}+\frac{3VZ^3}{2}+\frac{V^2Z^3}{2}+\frac{5WZ^3}{4}-\frac{VWZ^3}{2}+\frac{W^2Z^3}{2}-\frac{5Z^4}{4}+\frac{VZ^4}{2}-WZ^4+\frac{Z^5}{2}$,

$G_5=\frac{V}{2}-\frac{Y}{2}+\frac{UZ}{2}+\frac{V^2Z}{2}-VYZ+YZ^2-\frac{Z^3}{2}+\frac{WZ^3}{2}-\frac{Z^4}{2}$,

$G_6=V^2-2VY+Y^2+WZ^2-Z^3$,

$G_7=-U-V^2+X+2VY-2YZ+Z^2-WZ^2+Z^3$.

Zgodnie z twierdzeniem 2 jest :
$\{G_1\}$ jest bazą Gröbnera ideału $h\cap\mathbb{C}[Z,U,V,W]$,
$\{G_2,\dots,G_6\}$ jest bazą ideału $h\cap\mathbb{C}[Y,Z,U,V,W]$.

(b) Przy ustawieniu zmiennych w kolejności : Z,Y,X,U,V,W ; baza Gröbnera jest następująca :
$G_1=X^6-2X^5+2X^4W+X^4+2X^3V-4X^3W-2X^2V+X^2W^2+2X^2W+2XVW-2XW^2+X-U+V^2-2VW+W^2$,
$G_2=Y-X^3-XW-V$,
$G_3=Z-X^2-W$.

(c) Przy ustawieniu zmiennych w kolejności: X,Z,Y,U,V,W ; rachunków nie udało się przeprowadzić do końca.

Przykład 2. Ideał

$$\mathfrak{I}:=<a^2X^2+2abXY+X+b^2Y^2-U,c^2X^2+2cdXY+d^2Y^2+Y-V>$$

jest ideałem wykresu odwzorowania

$$(\flat)\qquad F\colon\mathbb{C}^2\ni(x,y)\longrightarrow(u,v)=(x+(ax+by)^2,y+(cx+dy)^2)\in\mathbb{C}^2\,.$$

Dla zmiennych w kolejności: X,Y,U,V ; jego baza Gröbnera $\{H_1,\dots,H_k\}$ względem porządku leksykograficznego jest :

(1) gdy $ad-bc\neq0$, $a\neq0$, $c\neq0$, to

$$H_1=Y^4-\frac{2VY^2a^2}{b^2c^2-2abcd+a^2d^2}-\frac{2UY^2c^2}{b^2c^2-2abcd+a^2d^2}+\frac{Y^3\left(2a^2-2cd\right)}{b^2c^2-2abcd+a^2d^2}+\frac{V^2a^4}{b^4c^4-4ab^3c^3d+6a^2b^2c^2d^2-4a^3bcd^3+a^4d^4}-\frac{Vc^2}{b^4c^4-4ab^3c^3d+6a^2b^2c^2d^2-4a^3bcd^3+a^4d^4}+\frac{Yc^2}{b^4c^4-4ab^3c^3d+6a^2b^2c^2d^2-4a^3bcd^3+a^4d^4}-\frac{2UVa^2c^2}{b^4c^4-4ab^3c^3d+6a^2b^2c^2d^2-4a^3bcd^3+a^4d^4}+\frac{U^2c^4}{b^4c^4-4ab^3c^3d+6a^2b^2c^2d^2-4a^3bcd^3+a^4d^4}+\frac{VY\left(-2a^4-4abc^2+2a^2cd\right)}{b^4c^4-4ab^3c^3d+6a^2b^2c^2d^2-4a^3bcd^3+a^4d^4}+\frac{UY\left(2a^2c^2+2c^3d\right)}{b^4c^4-4ab^3c^3d+6a^2b^2c^2d^2-4a^3bcd^3+a^4d^4}+\frac{Y^2\left(a^4+4abc^2-2a^2cd+c^2d^2\right)}{b^4c^4-4ab^3c^3d+6a^2b^2c^2d^2-4a^3bcd^3+a^4d^4},$$

$$H_2 = UX - \frac{VXa^2}{c^2} + \frac{UY(-(bc)+3ad)}{2ac} + \frac{VY\left(-3abc+a^2d\right)}{2c^3} + \frac{U\left(-2a^3-bc^2-acd\right)}{-4a^2bc^2+4a^3cd} + \frac{X\left(2a^3+bc^2+acd\right)}{-4a^2bc^2+4a^3cd} + \frac{V\left(2a^3+5bc^2-3acd\right)}{-4bc^4+4ac^3d} + \frac{Y\left(-2a^3-5bc^2+3acd\right)}{-4bc^4+4ac^3d} + \frac{Y^2\left(4a^3bc-b^2c^3-4a^4d-2abc^2d+3a^2cd^2\right)}{4a^2c^3} + \frac{Y^3\left(b^3c^3-3ab^2c^2d+3a^2bcd^2-a^3d^3\right)}{2ac^3},$$

$$H_3 = XY + \frac{Y^2(bc+ad)}{2ac} + \frac{Uc}{-2abc+2a^2d} - \frac{Xc}{-2abc+2a^2d} - \frac{Va}{-2bc^2+2acd} + \frac{Ya}{-2bc^2+2acd},$$

$$H_4 = X^2 - \frac{Y^2bd}{ac} - \frac{Ud}{-(abc)+a^2d} + \frac{Xd}{-(abc)+a^2d} + \frac{Vb}{-(bc^2)+acd} - \frac{Yb}{-(bc^2)+acd},$$

(2) gdy $a = rc$, $b = rd$, $cr^2 + d \neq 0$, $r \in \mathbb{C}$, to

$$H_1 = Y^2 + \frac{2UYc}{d+cr^2} - \frac{2VYcr^2}{d+cr^2} - \frac{V}{d^2+2cdr^2+c^2r^4} + \frac{Y}{d^2+2cdr^2+c^2r^4} + \frac{U^2c^2}{d^2+2cdr^2+c^2r^4} - \frac{2UVc^2r^2}{d^2+2cdr^2+c^2r^4} + \frac{V^2c^2r^4}{d^2+2cdr^2+c^2r^4},$$

$$H_2 = -U + X + Vr^2 - Yr^2,$$

(3) gdy $a = rc$, $b = rd$, $cr^2 + d = 0$, $cr \neq 0$, to

$$H_1 = Y^4 - \frac{Y^2}{(4c^4r^8)} + \frac{Y}{(16c^6r^12)},$$

$$H_2 = X - 16c^4r^{10}Y^3 - 4c^2r^6Y^2 + 3r^2Y.$$

Jeśli $c = 0$, to $H_1 = Y - V$, $H_2 = X - U$. Jeśli natomiast $c \neq 0$, $r = 0$, to $H_1 = Y + c^2U^2 - V$, $H_2 = X - U$.

(4) gdy $c = ra$, $d = rb$, $r \neq 0$, $br^2 + a \neq 0$, to

$$H_1 = Y^2 + \frac{2ar^2YU}{br^2+a} - \frac{(2a)YV}{(br^2+a)} + \frac{r^2Y}{(b^2r^4+2abr^2+a^2)} + \frac{a^2r^4U^2}{b^2r^4+2abr^2+a^2} - \frac{2a^2r^2UV}{b^2r^4+2abr^2+a^2} + \frac{a^2V^2}{b^2r^4+2abr^2+a^2} - \frac{r^2V}{b^2r^4+2abr^2+a^2},$$

$$H_2 = X - \frac{Y}{r^2} - U + \frac{V}{r^2}.$$

Jeśli $b = 0$, to $H_1 = Y - V$, $H_2 = X - U$. Jeśli natomiast $b \neq 0$, $r = 0$, to $H_1 = Y - V$, $H_2 = X + b^2V^2 - U$.

(5) gdy $c = 0$, $d = 0$, to

$$H_1 = Y - V,$$

$$H_2 = X^2 + \frac{2bXV}{a} + \frac{X}{a^2} - \frac{U}{a^2} + \frac{b^2V^2}{a^2}.$$

(6) gdy $a = 0$, $bc \neq 0$, to

$$H_1 = Y^4 - \frac{2dY^3}{(b^2c)} - \frac{2Y^2U}{b^2} + \frac{d^2Y^2}{b^4c^2} + \frac{2dYU}{b^4c} + \frac{Y}{b^4c^2} + \frac{U^2}{b^4} - \frac{V}{b^4c^2},$$

$$H_2 = X + b^2Y^2 - U.$$

(7) gdy $a = 0$, $c = 0\, d \neq 0$, to

$$H_1 = Y^2 + \frac{Y}{d^2} - \frac{V}{d^2},$$

$$H_2 = X - \frac{b^2Y}{d^2} - U + \frac{b^2V}{d^2}.$$

(8) gdy $c = 0$, $ad \neq 0$, to

$$H_1 = Y^2 + \frac{Y}{d^2} - \frac{V}{d^2},$$

$$H_2 = X^2 + \frac{2bXY}{a} + \frac{X}{a^2} - \frac{b^2Y}{a^2d^2} - \frac{U}{a^2} + \frac{b^2V}{a^2d^2}.$$

Obserwując uzyskane wyniki zauważamy że odwzorowanie (♭) jest właściwe, niezależnie od wybory stałych a, b, c, d. Tylko w bardzo szczególnych przypadkach jest ono wielomianowym automorfizmem[10]

[10] Tę samą obserwację można, bez większego trudu, uzyskać bez użycia komputera.

Przykład 3. Ustalmy w $\mathbb{C}^5$ zmienne w kolejności: U, V, X, Y, Z. Ideał $\mathfrak{m} :=< X - U^2 + V, Y + UV - 2V, Z - 3V^3 + U >$, przy porządku w $\mathbb{N}^5$ zadanym macierzą:

$$\begin{pmatrix} 1 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \end{pmatrix}$$

ma bazę Gröbnera złożoną z 11 następujących wielomianów:

$G_1 = \frac{-190X}{27} + \frac{16X^2}{3} - \frac{4X^3}{3} + \frac{X^4}{9} - \frac{95Y}{27} + \frac{64XY}{9} - \frac{14X^2Y}{9} + \frac{20Y^2}{9} - \frac{4XY^2}{9} + 8XY^3 + \frac{2X^2Y^3}{3} + \frac{10Y^4}{3} + Y^6 + \frac{XZ}{27} + \frac{16YZ}{9} - \frac{8XYZ}{9} + \frac{X^2YZ}{9} - \frac{8Y^2Z}{9} - \frac{16Y^3Z}{3} - 4XY^3Z - Y^4Z + \frac{190Z^2}{27} - \frac{16XZ^2}{3} + \frac{4X^2Z^2}{3} - \frac{X^3Z^2}{9} - \frac{16YZ^2}{3} + \frac{4XYZ^2}{3} + \frac{Y^2Z^2}{3} - \frac{Z^3}{27}$,

$G_2 = \frac{-95V}{3} + \frac{X}{3} + 16VX - 2VX^2 + 16Y + 16VY - 2VXY - X^2Y - 4Y^2 + 12VY^3 - 3Y^4 + 16VZ - 8VXZ + VX^2Z - 16YZ - 4VYZ + 4XYZ + 2Y^2Z - \frac{Z^2}{3}$,

$G_3 = \frac{4X}{9} - \frac{VX}{9} - \frac{X^2}{9} + \frac{2Y}{9} - \frac{16VY}{3} + \frac{VX^2Y}{3} + \frac{8Y^2}{3} + \frac{4VY^2}{3} + 2XY^2 + \frac{Y^3}{3} + VY^4 - \frac{YZ}{9} + \frac{16VYZ}{3} - \frac{4VXYZ}{3} - 4Y^2Z - \frac{2VY^2Z}{3} - \frac{XY^2Z}{3} - \frac{4Z^2}{9} + \frac{VZ^2}{9} + \frac{XZ^2}{9}$,

$G_4 = \frac{16X}{3} - \frac{4VX}{3} - \frac{8X^2}{3} + \frac{VX^2}{3} + \frac{X^3}{3} + \frac{8Y}{3} - \frac{2VY}{3} - 2XY - \frac{Y^2}{3} - 8VY^2 - 6VXY^2 + 4Y^3 - VY^3 + XY^3 - \frac{4YZ}{3} + \frac{VYZ}{3} + \frac{XYZ}{3} + 12VY^2Z + VXY^2Z - 4Y^3Z - \frac{16Z^2}{3} + \frac{4VZ^2}{3} + \frac{8XZ^2}{3} - \frac{VXZ^2}{3} - \frac{X^2Z^2}{3} + \frac{4YZ^2}{3}$,

$G_5 = \frac{-190V}{9} + 16VX - 4VX^2 + \frac{VX^3}{3} + \frac{95Y}{9} + \frac{40VY}{3} - \frac{16XY}{3} - \frac{10VXY}{3} + \frac{2X^2Y}{3} - \frac{16Y^2}{3} - \frac{VY^2}{3} + \frac{2XY^2}{3} + 12VY^3 + VXY^3 - 4Y^4 + \frac{VZ}{9} - \frac{16YZ}{3} + \frac{4VYZ}{3} + \frac{8XYZ}{3} - \frac{VXYZ}{3} - \frac{X^2YZ}{3} + \frac{4Y^2Z}{3}$,

$G_6 = -16V + 4V^2 + V^2X + VX^2 + 8Y + 2VY + 6XY + Y^2 + 3VY^3 + 16VZ - 4V^2Z - 4VXZ - 12YZ - VYZ - XYZ$,

$G_7 = -16V + 4V^2 + 4VX + 8Y + 3VY - \frac{V^2Y}{4} + 3XY - \frac{VXY}{2} - \frac{X^2Y}{4} + \frac{9VY^3}{2} - \frac{3Y^4}{4} + 16VZ - 4V^2Z - 4VXZ - 12YZ - VYZ - XYZ - \frac{3VY^3Z}{4} - 4VZ^2 + V^2Z^2 + VXZ^2 + 3YZ^2 + \frac{VYZ^2}{4} + \frac{XYZ^2}{4}$,

$G_8 = \frac{V}{3} - \frac{V^2}{12} + \frac{X}{3} - \frac{VX}{6} - \frac{X^2}{12} - 2V^2Y + \frac{3VY^2}{2} - \frac{Y^3}{4} + V^2YZ - \frac{VY^2Z}{4} - \frac{Z^2}{3} + \frac{VZ^2}{12} + \frac{XZ^2}{12}$,

$G_9 = \frac{-8V}{3} + \frac{2V^2}{3} + \frac{2VX}{3} + \frac{4Y}{3} + \frac{VY}{3} + \frac{XY}{3} + V^2Y^2 + \frac{4VZ}{3} - \frac{V^2Z}{3} - \frac{VXZ}{3} - \frac{4YZ}{3}$,

$G_{10} = 16V - 8V^2 + V^3 - VX^2 - 8Y + 2VY - 6XY - 2Y^2 - 3VY^3 - 16VZ + 4V^2Z + 4VXZ + 12YZ + VYZ + XYZ$,

$G_{11} = U + 48V - 24V^2 - 3VX^2 - 24Y + 6VY - 18XY - 6Y^2 - 9VY^3 + Z - 48VZ + 12V^2Z + 12VXZ + 36YZ + 3VYZ + 3XYZ$.

Jest to baza zredukowana.

Przykład 4.

$$\begin{aligned} J = {} & (9a^3c^2d - 9a^2bc^3)X^4 + (18a^3cd^2 - 18ab^2c^3)X^3Y \\ & + (9a^3d^3 + 27a^2bcd^2 - 27ab^2c^2d - 9b^3c^3)X^2Y^2 + (3c^2d + 3a^3)X^2 \\ & + (18a^2bd^3 - 18b^3c^2d)XY^3 + (6cd^2 + 6a^2b)XY \\ & + (9ab^2d^3 - 9b^3cd^2)Y^4 + (3d^3 + 3ab^2)Y^2 + 1 \end{aligned}$$

jest jakobianem odwzorowania

$$\mathbb{C}^2 \ni (x, y) \longrightarrow (x + (ax + by)^3, y + (cx + dy)^3) \in \mathbb{C}^2.$$

Niech $\mathfrak{I}$ będzie ideałem pierścienia $\mathbb{C}[x, y, u, v, a, b, c, d]$ generowanym przez 10 następujących wielomianów:

$9a^3c^2d - 9a^2bc^3$, $18a^3cd^2 - 18ab^2c^3$, $9a^3d^3 + 27a^2bcd^2 - 27ab^2c^2d - 9b^3c^3$, $3c^2d + 3a^3$, $18a^2bd^3 - 18b^3c^2d$, $6cd^2 + 6a^2b$, $9ab^2d^3 - 9b^3cd^2$, $3d^3 + 3ab^2$, $x + (ax + by)^3 - u$, $y + (cx + dy)^3 - v$.

Zerowanie się pierwszych ośmiu wielomianów jest równoważne temu, że $J = 1$.

Jeśli w $\mathbb{N}^8$ ustalimy porządek leksykograficzny oraz zmienne w kolejności: x, y, u, v, c, d, a, b, to zredukowana baza Gröbnera ideału $\mathfrak{I}$ składa się z ośmiu następujących wielomianów:

$d^3 + ab^2$, $cab^2 - da^2b$, $ca^2b - da^3$, $cd^2 + a^2b$, $c^2d + a^3$, $c^3b^3 + a^4b^2$, $Y + U^3c^3 - 3U^2Va^3 - 3UV^2a^2b - V^3ab^2 - V$, $X + U^3a^3 + 3U^2Va^2b + 3UV^2ab^2 - U + V^3b^3$.

Ostatnie dwa wielomiany dają wzory na odwzorowanie odwrotne.

SPIS LITERATURY

[BB] B. Buchberger, *An algorithm for finding a basis for the residue class ring of a zero-dimensional polynomial ideal (German)*, Univ. of Innsbruck (Austria), Math. Inst.

[BB1] ———, *An algorithmic method in polynomial ideal theory*, in: Multidimensional System Theory by N. Bose, Reidel Publ. Comp., Dortrecht 1985, 184-232.

[LED] L.E. Dickson, *Finitness of the odd perfect and primitive abundant numbers with n distinct prime factors*, Am.J.of Math. **35** (1913), 413-426.

[AvdE] A. van den Essen, *A criterion to decide if a polynomial map is invertible and to compute the inverse*, Communications in Algebra **18 (10)** (1990), 3183-3186.

[WF] W. Fulton, *Algebraic Curves*, The Benjamin /Cummings Publishing Company, 1969.

[GH] G. Hermann, *The question of finitely many steps in polynomial Ideal Theory (German)*, Math. Ann. **95** (1926), 736-738.

[HH] H. Hironaka, *Resolution of singularities of an algebraic variety over a field of characteristic zero: I,II*, Annals of Math. **79** (1964), 109-326.

[MK] M. Kwieciński, *A Gröbner basis criterion for isomorphisms of algebraic varieties*, Journ. of Pure and Appl. Alg. (to appear).

[MK1] ———, *Automorphisms from face polynomials*, Report 9105 (1991), Catholic University Nijmegen.

[ML-J] M. Lejeune-Jalabert, *Effectivité de Calculs Polynomiaux*, Cours de D.E.A.,Université de Grenoble, 140 pages, Grenoble 1986.

[SŁ] S. Łojasiewicz, *Introduction to Complex Analytic Geometry*, Birkhäuser, 1991.

[FPaMP] F. Pauer and M. Pheifhofer, *The theory of Gröbner bases*, L'Enseignement Mathématique **34** (1988), 215-232.

[TW] T. Winiarski, *Inverse of polynomial automorphisms of* $\mathbb{C}^n$, Bull. Polon. Ac. Sci. **27** (1979), no. 9, 673-674.

[KRaTW] K. Rusek and T. Winiarski, *Polynomial automorphisms of* $\mathbb{C}^n$, Univ. Iag. Acta Math. **24** (1984), 143-149.

[CoAl] *Commutative Algebra*, from a special issue of the Journ of Symbolic Computation, edited by Dr Lorenzo Robbiano, Academic Press INC., San Diego, CA 92101, 1989.

[EBaPM] E. Bierstone and P. Milman, *The local geometry of analytic mappings*, Dottorato di Ricerca in Matematica, Dipartamento di Matematica dell'Universita di Pisa, 1988.

Application of Gröbner bases in the theory of polynomial mappings

Summary. In the paper, a detailed introduction into the concept of Gröbner bases is given. Moreover, recent applications of Gröbner bases in the theory of polynomial mappings are presented.

Bronisławów, 11–15 stycznia 1993 r.