Efektywne Metody
Rzeczywistej Geometrii Algebraicznej

Literatura Pomocnicza:

1. S.Basu, R.Pollack, M.-F.Roy, *Algorithms in Real Algebraic Geometry*
2. R.Benedetti, J.-J.Risler, *Real Algebraic and Semi-Algebraic Sets*
3. J.Bochnak, M.Coste, M.-F.Roy, *Real Algebraic Geometry*
4. J.Browkin, *Teoria ciał*
5. D.Cox, J.Little, D.O'Shea, *Ideals, varieties and Algorithms*
6. D.Cox, J.Little, D.O'Shea, *Using Algebraic Geometry*
7. M.Dumnicki, T.Winiarski, *Bazy Gröbnera – Efektywne metody w układach równań wielomianowych*
8. G.-M.Greuel, G.Pfister, and H.Schönemann, `Singular` 3.0.2. *A Computer Algebra System for Polynomial Computations.* `http://www.singular.uni-kl.de`
9. A.Mostowski, M.Stark, *Elementy Algebry Wyższej*

1 Oznaczenia

$\mathbb{K}$ – ciało, na ogół $\mathbb{R}$, $\mathbb{C}$, niektóre pojęcia są też zdefiniowane dla ciała $\mathbb{Q}$ lub $\mathbb{Z}_p$

$\mathbb{K}^n = \underbrace{\mathbb{K} \times \cdots \times \mathbb{K}}_{n}$

Punkty: $\mathbb{K}^n \ni p = (p_1, \ldots, p_n)$, $p_1, \ldots, p_n \in \mathbb{K}$

Początek układu: $\mathbf{0} = (0, \ldots, 0)$

$$p, q \in \mathbb{K}^n : \quad |p| = \sqrt{|p_1|^2 + \cdots + |p_n|^2}$$
$$d(p, q) = |p - q| = \sqrt{|p_1 - q_1|^2 + \cdots + |p_n - q_n|^2},$$

i-ta współrzędna x_i : $\quad x_i(p) = p_i$, więc

$$x_i : \ \mathbb{K}^n \to \mathbb{K}$$

(Gdy $\mathbb{K} = \mathbb{C}$ to używa się często symbolu z_i zamiast x_i.)

$(\mathbb{K}^n, d)$ – jest przestrzenią metryczną, izometryczną z $\mathbb{R}^n$ lub z $\underbrace{\mathbb{R}^2 \times \cdots \times \mathbb{R}^2}_{n} = \mathbb{R}^{2n}$, ze standardową metryką euklidesową.

Niech $U \subset \mathbb{K}^n$ będzie zbiorem otwartym, $p \in U$, oraz $f : U \to \mathbb{K}$. Definiujemy pochodną cząstkową $\frac{\partial f}{\partial x_i}(p) = D_i f(p)$ jako

$$\lim_{h \to 0} \frac{f(p_1, \ldots, p_i + h, \ldots, p_n) - f(p_1, \ldots, p_i, \ldots, p_n)}{h} \ ,$$

o ile ta granica istnieje.

- $\mathbb{N} = \{0, 1, 2, \ldots\}$
- *Wielowskaźnik:* $\alpha = (\alpha_1, \ldots, \alpha_n), \ \alpha_i \in \mathbb{N}$
- $|\alpha| = \alpha_1 + \cdots + \alpha_n$ – norma wielowskaźnika
- $\alpha\,! = \alpha_1! \cdots \alpha_n!$ – silnia wielowskaźnika
- $D^\alpha f = \partial^{|\alpha|} f / \partial x^\alpha = \partial^{|\alpha|} f / \partial x_1^{\alpha_1} \ldots \partial x_n^{\alpha_n}$
- $x^\alpha = x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ – jednomian stopnia $|\alpha|$
- Przyjmujemy, że $D^{(0,\ldots,0)} f = f$, $(0, \ldots, 0)! = \mathbf{0}! = 0$, $x^{\mathbf{0}} = 1$

2 Wielomiany jednej zmiennej

Wielomian jednej zmiennej X o współczynnikach w ciele $\mathbb{K}$, to napis:

$$f = f(X) = a_0 + a_1 X + \cdots + a_n X^n, \quad a_i \in \mathbb{K}$$

- *współczynniki*: $a_0, a_1, \ldots, a_n$
- *wyraz wolny*: a_0
- *jednomian stopnia k*: X^k (przyjmujemy, że $X^0 = 1$)
- *składnik stopnia k*: $a_k X^k$

- Jeżeli $a_n \neq 0$, *stopień wielomianu* $\deg(f) = n$
- *współczynnik wiodący*: a_n
- *składnik wiodący*: $a_n X^n$

Funkcje stałe są wielomianami stopnia 0, wielomianowi $f = 0$ można przypisać dowolny stopień.

Zbiór wielomianów $\mathbb{K}[X]$ zmiennej X o współczynnikach w ciele $\mathbb{K}$ z naturalnymi działaniami dodawania i mnożenia jest pierścieniem przemiennym z jedynką.

- Jeżeli ciało $\mathbb{K}$ jest nieskończone oraz $f(x) = 0$ dla każdego $x \in \mathbb{K}$, to $f = 0$.
- $\deg(f \pm g) \leq \max(\deg(f), \deg(g))$
- Jeżeli $f \neq 0$, $g \neq 0$, to $fg \neq 0$ oraz $\deg(fg) = \deg(f) + \deg(g)$
- Jeżeli $fg = 0$, to $f = 0$ lub $g = 0$, czyli $\mathbb{K}[X]$ jest pierścieniem bez dzielników zera
- Jeżeli $h \neq 0$ oraz $hf = hg$, to $f = g$
- f jest *dzielnikiem* g jeżeli istnieje h taki, że $g = fh$. Wielomian g jest wtedy *wielokrotnością* f. Piszemy: $f \mid g$.
- Jeżeli f nie jest dzielnikiem g, to piszemy $f \nmid g$
- Każdy wielomian jest dzielnikiem wielomianu 0
- Jeżeli $f \mid g$ oraz $g \mid h$, to $f \mid h$
- Jeżeli $f \mid g$ oraz $g \mid f$, to istnieje niezerowa liczba $c \in \mathbb{K}$ taka, że $f = cg$

Twierdzenie 2.1 (Algorytm Dzielenia) *Dla każdej pary wielomianów f, g, gdzie* $\deg(f) > 0$, *istnieje dokładnie jedna para wielomianów h, r, dla których $g = hf + r$ oraz* $\deg(r) < \deg(f)$.

Wielomian r nazywamy resztą z dzielenia *g przez f.*

Fakt 2.2 *Resztą z dzielenia g przez $(X - a)$ jest $g(a)$. W szczególności $g(a) = 0$ wtedy i tylko wtedy, gdy $(X - a) \mid g$.*

Wielomian g nazywamy *największym wspólnym dzielnikiem* wielomianów f_1, f_2 (ozn. $g = \gcd(f_1, f_2)$), jeżeli $g \mid f_1$, $g \mid f_2$, oraz jeżeli $h \mid f_1$, $h \mid f_2$ to $h \mid g$.

Największy wspólny dzielnik można obliczyć używając *Algorytmu Euklidesa.*

Wielomiany f_1, f_2 są *względnie pierwsze*, gdy $\gcd(f_1, f_2) = 1$.

Wielomiany f_1, f_2 są względnie pierwsze wtedy i tylko wtedy, gdy f_1, f_2 nie mają wspólnych pierwiastków zespolonych.

Fakt 2.3 *Wielomian f ma wyłącznie jednokrotne pierwiastki zespolone wtedy i tylko wtedy, gdy* $\gcd(f, f') = 1$.

Fakt 2.4 *Niech $Q = f/\gcd(f, f')$. Wielomiany f, Q mają te same pierwiastki zespolone, wszystkie pierwiastki Q są jednokrotne.*

Ilość zespolonych pierwiastków wielomianu f jest równa

$$\deg(Q) = \deg(f) - \deg(\gcd(f, f')).$$

Przykład. SINGULAR

```
> ring r=0,x,lp;
> poly f=x9-13x8+67x7-173x6+243x5-255x4+409x3-603x2+432x-108;
> poly df=diff(f,x);
> poly g=gcd(f,df);
> g;
x3-8x2+21x-18
> list L=division(f,g);
> L;
x6-5x5+6x4-2x3+11x2-17x+6
0
1
poly Q=f/g;
Q;
x6-5x5+6x4-2x3+11x2-17x+6
> exit;
Auf Wiedersehen.
```

Wielomian f ma dokładnie 6 parami różnych pierwiastków zespolonych.

Fakt 2.5 *Niech $f \in \mathbb{Q}[X]$, niech $0 \neq c \in \mathbb{Z}$ będzie takie, że $h = cf \in \mathbb{Z}[X]$. Jeżeli $f(a) = 0$ dla $a \in \mathbb{Q}$, to $a = \frac{p}{q} \in \mathbb{Q}$, gdzie $p, q \in \mathbb{Z}$, p dzieli wyraz wolny wielomianu h oraz q dzieli współczynnik wiodący wielomianu h.*

Przykład. SINGULAR

```
> ring r=0,x,lp;
> poly f=2x11-8x10+6x9-14x7+60x6-58x5+12x4-2x3+10x2-14x+6;
> subst(f,x,1);
0
> subst(f,x,-1);
160
> subst(f,x,2);
-638
> subst(f,x,-2);
-7590
> subst(f,x,3);
0
> subst(f,x,-3);
-855168
> subst(f,x,6);
300775530
> subst(f,x,-6);
-1262603790
> subst(f,x,1/2);
1045/1024
> subst(f,x,-1/2);
19803/1024
> subst(f,x, 3/2);
7815/1024
> subst(f,x,-3/2);
629865/1024
```

Wielomian f ma więc dwa pierwiastki wymierne: 1 oraz 3.

W podręczniku A.Mostowski, M.Stark – *Elementy Algebry Wyższej* – podane są wzory pozwalające znaleźć wszystkie pierwiastki wielomianu stopnia 3 (Wzory Cardano) oraz wielomianu stopnia 4. Wiadomo też, że dla wielomianów stopnia większego niż 4 nie istnieją ogólne wzory pozwalające obliczać pierwiastki.

Istnieją metody znajdowania przybliżonych rozwiązań:

Przykład. SINGULAR

```
> ring r=0,x,lp;
> LIB ''solve.lib'';
> poly a=x5-2x3+3x2-x+4;
> def A= solve(a);
-2.04356833
(-0.18082745+i*0.94258812)
(-0.18082745-i*0.94258812)
(1.20261162+i*0.82376372)
(1.20261162-i*0.82376372)
```

Przykład przedstawiony przez Wilkinsona pokazuje, jak duże błędy mogą się pojawić gdy posługujemy się przybliżonymi wartościami:

Przykład. SINGULAR

```
> ring r=0,x,lp;
> LIB ''solve.lib'';
> poly f=x*(x+1)*(x+2)*(x+3)*(x+4)*(x+5)*(x+6)*(x+7)
*(x+8)*(x+9)*(x+10)*(x+11)*(x+12)*(x+13)*(x+14)*(x+15)
*(x+16)*(x+17)*(x+18)*(x+19)*(x+20);
> poly g=f+1/100000*x19;
> def G=solve(g);
-7.93695027
-7.00367647
-5.999903
-5.00000122
-4
-3
-2
-1
(-20.99405821+i*1.34421008)
(-20.99405821-i*1.34421008)
(-18.49088339+i*3.24042337)
(-18.49088339-i*3.24042337)
(-15.31073486+i*3.5589746)
(-15.31073486-i*3.5589746)
```

```
(-12.61151323+i*2.82711482)
(-12.61151323-i*2.82711482)
(-10.57923379+i*1.73129676)
(-10.57923379-i*1.73129676)
(-9.04331107+i*0.62692384)
(-9.04331107-i*0.62692384)
0
```

3 Wielomiany w $\mathbb{R}[X]$

$\underline{a} = (a_1, \ldots, a_n)$ – ciąg liczb rzeczywistych

Definicja. *Liczbą zmian znaku w ciągu* $\underline{a}$ nazywamy liczbę par $(i, i+k)$ $(k \geq 1)$ takich, że

- $a_i a_{i+k} < 0$,
- $a_{i+r} = 0$ dla $0 < r < k$.

Oznaczamy ją symbolem $Var(\underline{a})$.

Przykład. $\underline{a} = (-1, 0, 0, 2, 0, 4, 0, 0, -5, 6)$, $Var(\underline{a}) = 3$

Twierdzenie 3.1 (Sturm) *Niech* $f \in \mathbb{R}[X]$. *Niech* $f_0 = f$, $f_1 = f', \ldots$

$$f_{i-2} = f_{i-1} g_{i-1} - f_i \quad (\deg(f_i) < \deg(f_{i-1})), \ldots$$

tak długo, aż $f_{s-1} = f_s g_s$, *tzn. gdy* $f_s = \pm \gcd(f, f')$.

Jeżeli $a < b$ *oraz* $f(a) \neq 0$, $f(b) \neq 0$, *to liczba pierwiastków (bez krotności)*

$$\# f^{-1}(0) \cap [a, b] = Var(f_0(a), \ldots, f_s(a)) - Var(f_0(b), \ldots, f_s(b)).$$

Wniosek 3.2 *Niech* $\underline{A}$ *będzie ciągiem wiodących współczynników wielomianów* $f_0(-X), \ldots, f_s(-X)$, *niech* $\underline{B}$ *będzie ciągiem wiodących współczynników wielomianów* $f_0(X), \ldots, f_s(X)$. *Wtedy liczba wszystkich pierwiastków rzeczywistych*

$$\# f^{-1}(0) = Var(\underline{A}) - Var(\underline{B}).$$

Stosując Twierdzenie Sturma obliczymy liczbę rzeczywistych pierwiastków w danym przedziale, oraz liczbę wszystkich rzeczywistych pierwiastków.

Przykład. SINGULAR

```
> ring r=0,x,lp;
> LIB ''rootsur.lib'';
> poly f=x9-7x8+3x5+4x4-5x2+2x-5;
> sturm(f,1,7);
1
> sturm(f,-5,5);
0
> nrroots(f);
1
```

Definicja. $z_+(f)$ – liczba dodatnich pierwiastków f (liczonych z krotnościami)

Twierdzenie 3.3 (Lemat Kartezjusza) *Niech* $f = a_0 + \cdots + a_n X^n \in \mathbb{R}[X]$. *Wtedy*

$$z_+(f) \leq Var(a_0, \ldots, a_n),$$
$$z_+(f) \equiv Var(a_0, \ldots, a_n) \mod 2 \ .$$

Ćwiczenie. Oszacuj liczbę rzeczywistych pierwiastków wielomianu $X^{80} - 9X^{11} + 7$.

4 Wielomiany wielu zmiennych

Definicja. Wielomianem zmiennych $X_1, \ldots, X_n$ nazywamy skończoną kombinację:

$$f = \sum a_\alpha X_1^{\alpha_1} \cdots X_n^{\alpha_n} = \sum_\alpha a_\alpha X^\alpha \ \ , \ \alpha \in \mathbb{N}^n, \ a_\alpha \in \mathbb{K} \ .$$

Zbiór wszystkich wielomianów oznaczamy symbolem $\mathbb{K}[X_1, \ldots, X_n]$, lub krócej $\mathbb{K}[X]$ jeżeli jest jasne które zmienne rozpatrujemy. Zbiór $\mathbb{K}[X]$ z naturalnymi działaniami dodawania i mnożenia jest przemiennym pierścieniem z jedynką.

Wielomian $f \in \mathbb{K}[X]$ definiuje funkcję $f : \mathbb{K}^n \to \mathbb{K}$:

$$f(x) = f(x_1, \ldots, x_n) = \sum_\alpha a_\alpha x^\alpha = \sum_\alpha a_\alpha x_1^{\alpha_1} \cdots x_n^{\alpha_n} \ .$$

Fakt 4.1 *Jeżeli ciało $\mathbb{K}$ jest nieskończone to $f = 0$ (tzn. wszystkie współczynniki $a_\alpha = 0$) wtedy i tylko wtedy, gdy funkcja $f : \mathbb{K}^n \to \mathbb{K}$ jest funkcją zerową.*

Wtedy również dwa wielomiany $f, g \in \mathbb{K}[X]$ są równe wtedy i tylko wtedy, gdy funkcje $f, g : \mathbb{K}^n \to \mathbb{K}$ są równe.

Definicja. Niech $f_1, \ldots, f_s \in \mathbb{K}[X]$. Definiujemy zbiór

$$V(f_1, \ldots, f_s) = \{x = (x_1, \ldots, x_n) \in \mathbb{K}^n \mid f_i(x) = 0 \text{ dla } 1 \leq i \leq s\},$$

który nazywamy *(afinicznym) zbiorem algebraicznym* zdefiniowanym przez $f_1, \ldots, f_s$. Jest to zbiór rozwiązań układu równań:

$$\begin{cases} f_1(x) = 0 \\ \quad\vdots \\ f_s(x) = 0 \end{cases}$$

Przykłady:

- $f = 0$ to $V(f) = \mathbb{K}^n$
- $V(X^2 + Y^2 - 1)$ jest okręgiem jednostkowym na płaszczyźnie
- $V(XY, XY + 3) = \emptyset$
- $V(Y - f(X))$ jest wykresem wielomianu f
- $V(X^2 + Y^2 + (Z - 1)Z^4)$ (Kiss)
- Każdy skończony podzbiór $\mathbb{K}^n$ jest zbiorem algebraicznym
- $[0, 1]$, $\mathbb{Q}$, $\mathbb{N}$ nie są zbiorami algebraicznymi

Twierdzenie 4.2 *Skończona suma zbiorów algebraicznych jest zbiorem algebraicznym.*

Przekrój dowolnej rodziny zbiorów algebraicznych jest zbiorem algebraicznym

5 Ideały w $\mathbb{K}[X]$

Definicja. Podzbiór $I \subset \mathbb{K}[X]$ jest *ideałem*, jeżeli

- $0 \in I$,
- $f, g \in I \;\Rightarrow\; f \pm g \in I$,
- $f \in I,\; h \in \mathbb{K}[X] \;\Rightarrow\; hf \in I$.

Fakt 5.1 *Jeżeli $f_1, \ldots, f_s \in \mathbb{K}[X]$, to zbiór*

$$\langle f_1, \ldots, f_s \rangle = \left\{ \sum_{i=1}^{s} h_i f_i \mid h_1, \ldots, h_s \in \mathbb{K}[X] \right\}$$

jest ideałem. Nazywamy go ideałem generowanym *przez $f_1, \ldots, f_s$.*

Zauważmy, że

- jeżeli $f_1(x) = \ldots = f_s(x) = 0$ oraz $h \in \langle f_1, \ldots, f_s \rangle$, to $h(x) = 0$,
- jeżeli $\langle f_1, \ldots, f_s \rangle = \langle g_1, \ldots, g_r \rangle$, to $V(f_1, \ldots, f_s) = V(g_1, \ldots, g_r)$,
- $f_1, \ldots, f_s$ należą do ideału I wtedy i tylko wtedy, gdy $\langle f_1, \ldots, f_s \rangle \subset I$,
- w pierścieniu wielomianów <u>jednej zmiennej</u> ($n = 1$) każdy ideał jest generowany przez jeden element. W szczególności,

$$\langle f_1, \ldots, f_s \rangle = \langle \gcd(f_1, \ldots, f_s) \rangle \;.$$

Z ideałem I można stowarzyszyć pierścień ilorazowy $\mathbb{K}[X]/I$, z naturalnymi działaniami dodawania i mnożenia (mod I).

Ponieważ ideał I jest w szczególności podprzestrzenią liniową przestrzeni $\mathbb{K}[x]$, więc można zdefiniować wymiar $\dim_K \mathbb{K}[x]/I$.

Jeżeli $I \subset J$ są ideałami, to $\dim_K \mathbb{K}[X]/I \geq \dim_K \mathbb{K}[X]/J$.

6 Porządek jednomianów

Definicja. Niech $'' < ''$ będzie porządkiem w zbiorze $\{X^\alpha \mid \alpha \in \mathbb{N}^n\}$ spełniającym trzy warunki:

- porządek jest liniowy, tzn. dla każdych dwóch jednomianów X^α, X^β jest spełniona jedna z relacji: $X^\alpha < X^\beta$ lub $X^\alpha = X^\beta$ lub $X^\alpha > X^\beta$,
- jeżeli $X^\alpha < X^\beta$ to dla każdego jednomianu X^γ spełniona jest nierówność $X^\alpha X^\gamma = X^{\alpha+\gamma} < X^{\beta+\gamma} = X^\beta X^\gamma$,
- $'' < ''$ jest dobrym porządkiem, tzn. każdy niepusty zbiór złożony z jednomianów posiada element najmniejszy. Warunek ten jest równoważny z warunkiem, że każdy malejący ciąg jednomianów $X^{\alpha(1)} > X^{\alpha(2)} > X^{\alpha(3)} > \ldots$ jest skończony.

Fakt 6.1 *W przypadku jednej zmiennej, tzn. gdy $n = 1$, jedynym porządkiem jednomianów jest*

$$1 = X^0 < X^1 < X^2 < X^3 < \ldots \ .$$

Niech $X^\alpha = X_1^{\alpha_1} \cdots X_n^{\alpha_n}$, $X^\beta = X_1^{\beta_1} \cdots X_n^{\beta_n}$.

Przykład. Porządek *leksykograficzny*: $X^\alpha >_{lex} X^\beta$ jeżeli pierwsza niezerowa współrzędna z lewej strony różnicy $\alpha - \beta$ jest dodatnia, np.

$$X_1^3 X_2^5 X_3^1 \ >_{lex} \ X_1^3 X_2^3 X_3^8 \ ,$$

jest porządkiem jednomianów.

Weźmy zmienne $X_1 = x$, $X_2 = y$, $X_3 = z$, oraz ciało $\mathbb{K} = \mathbb{Q}$.
SINGULAR:

```
> ring r=0, (x,y,z),lp ;
```

Przykład. Porządek *leksykograficzny z gradacją*: $X^\alpha >_{grlex} X^\beta$ jeżeli $|\alpha| > |\beta|$, lub $|\alpha| = |\beta|$ oraz $X^\alpha >_{lex} X^\beta$, np.

$$X_1^3 X_2^5 X_3^1 \ <_{grlex} \ X_1^3 X_2^3 X_3^8 \ , \ X_1^2 X_2^2 X_3^2 >_{grlex} X_1^2 X_2^1 X_3^3$$

jest porządkiem jednomianów.

Weźmy zmienne $X_1 = x$, $X_2 = y$, $X_3 = z$ oraz ciało $\mathbb{K} = \mathbb{Q}[\sqrt{5}]$.
SINGULAR:

```
> ring r=(0,p), (x,y,z), Dp ;
> minpoly = p2-5;
```

Przykład. Porządek *odwrotny leksykograficzny z gradacją*:
$X^\alpha >_{grevlex} X^\beta$ jeżeli $|\alpha| > |\beta|$, lub $|\alpha| = |\beta|$ oraz pierwsza niezerowa współrzędna z prawej strony różnicy $\alpha - \beta$ jest ujemna, np.

$$X_1^3 X_2^5 X_3^1 <_{grevlex} X_1^3 X_2^3 X_3^8 \quad , \quad X_1^2 X_2^3 X_3^2 <_{grevlex} X_1^3 X_2^2 X_3^2$$

jest porządkiem jednomianów.

Weźmy zmienne $X_1 = x$, $X_2 = y$, $X_3 = z$, oraz ciało $\mathbb{K} = \mathbb{Q}[i]$.
SINGULAR:

```
> ring r=(0,i), (x,y,z), dp ;
> minpoly = i2+1;
```

Fakt 6.2 *W każdym z trzech powyższych porządków:* $X_1 > X_2 > \ldots > X_n$.

Porządek jednomianów pozwala jednoznacznie uporządkować składniki wielomianu:

Przykład. Niech $f = 4XY^2Z + 4Z^2 - 5X^3 + 7X^2Z^2 \in \mathbb{K}[X, Y, X]$:

- $f = -5X^3 + 7X^2Z^2 + 4XY^2Z + 4Z^2$, (lex)
- $f = +7X^2Z^2 + 4XY^2Z - 5X^3 + 4Z^2$, (grlex)
- $f = +4XY^2Z + 7X^2Z^2 - 5X^3 + 4Z^2$, (grevlex)

Definicja. Z niezerowym wielomianem $f = \sum a_\alpha X^\alpha$ w pierścieniu $\mathbb{K}[X]$ z wybranym porządkiem jednomianów $'' >''$ można stowarzyszyć

- *wielostopień* multideg(f) będący wykładnikiem pierwszego składnika w uporządkowanej postaci f
- *wiodący współczynnik* $LC(f) = a_{\text{multideg}(f)} \in \mathbb{K}$
- *wiodący jednomian* $LM(f) = X^{\text{multideg}(f)}$
- *wiodący składnik* $LT(f) = LC(f) \cdot LM(f)$

Przykład. Niech $f = 4XY^2Z + 4Z^2 - 5X^3 + 7X^2Z^2 \in \mathbb{K}[X, Y, X]$ z porządkiem leksykograficznym.

$$\text{multideg}(f) = (3, 0, 0)$$

$$LC(f) = -5$$

$$LM(f) = X^3$$
$$LT(f) = -5X^3$$

Własności:

- jeżeli $X^\alpha | X^\beta$, to $X^\alpha \leq X^\beta$
- jeżeli $X^\alpha \leq X^\beta$ oraz $X^\gamma \leq X^\delta$, to $X^\alpha \cdot X^\gamma \leq X^\beta \cdot X^\delta$
- $LC(fg) = LC(f)LC(g)$
- $LM(fg) = LM(f)LM(g)$
- $LT(fg) = LT(f)LT(g)$
- $LM(f \pm g) \leq \max\{LM(f), LM(g)\}$
- jeżeli $LM(f) < LM(g)$, to $LT(f+g) = LT(g)$
- jeżeli $LM(f) \leq LM(g)$, to $LM(fh) \leq LM(gh)$
- $\forall\ \alpha \in \mathbb{N}^n \ : \quad 1 \leq X^\alpha$

7 Algorytm dzielenia w $\mathbb{K}[X]$

Jeżeli w $\mathbb{K}[X]$ jest wybrany porządek jednomianów, to każdy wielomian $f \in \mathbb{K}[X]$ można podzielić (z resztą) przez skończony ciąg wielomianów $f_1, \ldots, f_s \in \mathbb{K}[X]$.

Przykład. Podzielimy $f = xy^2 + 1$ przez $f_1 = xy + 1$, $f_2 = y + 1$. Przyjmujemy w $\mathbb{R}[x, y]$ porządek `lex` taki, że $x > y$.

$$f = xy^2 + 1 = y \cdot xy + 1 = y(xy + 1) - y + 1 =$$
$$y \cdot f_1 - (y + 1) + 1 + 1 = y \cdot f_1 + (-1) \cdot f_2 + 2\ .$$

Przykład. Podzielimy $f = x^2y + xy^2 + y^2$ przez $f_1 = xy - 1$, $f_2 = y^2 - 1$. Przyjmujemy w $\mathbb{R}[x, y]$ porządek `lex` taki, że $x > y$.

$$f = x^2y + xy^2 + y^2 = x \cdot xy + xy^2 + y^2 = x(xy - 1) + x + xy^2 + y^2 =$$

$$x\cdot f_1+y\cdot xy+x+y^2 = x\cdot f_1+y(xy-1)+y+x+y^2 = (x+y)\cdot f_1+1\cdot(y^2-1)+x+y+1 =$$
$$(x+y)\cdot f_1+1\cdot f_2+x+y+1\ .$$

Zauważmy, że w obu przypadkach żaden składnik reszty nie dzieli się przez $LT(f_1), LT(f_2)$.

Twierdzenie 7.1 (Algorytm Dzielenia) *Wybierzmy w $\mathbb{K}[X]$ porządek jednomianów $''>''$. Niech $(f_1,\ldots,f_s)$ będzie skończonym ciągiem wielomianów z $\mathbb{K}[X]$. Wtedy*

$$\forall\ f\in\mathbb{K}[X] \quad \exists\ a_1,\ldots,a_s,r\in\mathbb{K}[X]:$$

$$f = a_1f_1+\cdots+a_sf_s+r\ ,$$

gdzie $r=0$ lub r jest kombinacją liniową jednomianów z których żaden nie dzieli się przez $LT(f_1),\ldots,LT(f_s)$. Wielomian r nazywamy resztą.

Ponadto, jeżeli $a_if_i\neq 0$, to

$$\mathrm{multideg}(f)\geq\mathrm{multideg}(a_if_i)\ .$$

Jeżeli $r\neq 0$ to $\mathrm{multideg}(f)\geq\mathrm{multideg}(r)$.

Przykład. Jeżeli podzielimy $f=x^2y+xy^2+y^2$ przez $f_1=y^2-1$, $f_2=xy-1$, to otrzymamy: $f=(x+1)\cdot f_1+x\cdot f_2+2x+1$.

Zauważmy, że w szczególności reszta z dzielenia jest inna niż poprzednio. Przykład ten pokazuje, że wynik Algortymu Dzielenia zależy od kolejności w jakiej występują wielomiany $f_1,\ldots,f_s$.

Fakt 7.2 *Jeżeli $r=0$ to $f\in\langle f_1,\ldots,f_s\rangle$.*

Przykład. Zastosujemy Algorytm Dzielenia aby podzielić $f=xy^2-x$ przez $f_1=xy+1$, y^2-1. Otrzymamy

$$xy^2-x = y\cdot(xy+1)+0\cdot(y^2-1)-x-y\ ,$$

więc otrzymamy niezerową resztę. Z drugiej strony

$$xy^2-x = 0\cdot(xy+1)+x\cdot(y^2-1)\ ,$$

więc $xy^2-x\in\langle f_1,f_2\rangle$.

8 Ideały jednomianowe

Definicja. Ideał $J \subset \mathbb{K}[X]$ nazywamy*ideałem jednomianowym*, jeżeli istnieje zbiór $\mathcal{A} \subset \mathbb{N}^n$ (być może nieskończony) taki, że

$$J = \left\{ f = \sum_{\alpha \in \mathcal{A}} h_\alpha X^\alpha \right\},$$

gdzie $h_\alpha \in \mathbb{K}[X]$, oraz $h_\alpha = 0$ z wyjątkiem skończonej ilości wielowskaźników α.

Piszemy wtedy $J = \langle X^\alpha \mid \alpha \in \mathcal{A} \rangle$, i mówimy że jednomiany $\{X^\alpha \mid \alpha \in \mathcal{A}\}$ generują ideał J.

Przykłady ideałów jednomianowych.

- $\left\langle X^4Y^2, X^3Y^2, X^2Y^5 \right\rangle \subset \mathbb{K}[X,Y]$
- $\left\langle (k-1)XY^k \mid k \geq 3 \right\rangle = \left\langle XY^k \mid k \geq 3 \right\rangle \subset \mathbb{K}[X,Y]$
- $\left\langle k\ell X^{2k}Y^{2\ell} \mid k, \ell \geq 2 \right\rangle = \left\langle X^{2k}Y^{2\ell} \mid k, \ell \geq 2 \right\rangle \subset \mathbb{K}[X,Y]$

Dla dowolnego zbioru $\{a_\alpha \in \mathbb{K} \setminus \{\mathbf{0}\} \mid \alpha \in \mathcal{A}\}$:

Lemat 8.1 $\langle a_\alpha X^\alpha \mid \alpha \in \mathcal{A} \rangle = \langle X^\alpha \mid \alpha \in \mathcal{A} \rangle$, *więc* $\langle a_\alpha X^\alpha \mid \alpha \in \mathcal{A} \rangle$ *jest ideałem jednomianowym.*

Lemat 8.2 *Niech* $J = \langle a_\alpha X^\alpha \mid \alpha \in \mathcal{A} \rangle$. *Wtedy składnik* cX^β *należy do* J *wtedy i tylko wtedy, gdy istnieje taki wielowskaźnik* $\alpha \in \mathcal{A}$, *że* $X^\alpha \mid X^\beta$.

Twierdzenie 8.3 (Lemat Dicksona) *Ideał jednomianowy* $J = \langle a_\alpha X^\alpha \mid \alpha \in \mathcal{A} \rangle$ *może być przedstawiony w postaci*

$$J = \left\langle a_{\alpha(1)} X^{\alpha(1)}, \ldots, a_{\alpha(s)} X^{\alpha(s)} \right\rangle ,$$

gdzie $\alpha(1), \ldots, \alpha(s) \in \mathcal{A}$.

W szczególności ideał jednomianowy J *jest zawsze skończenie generowany.*

Ćwiczenie. $f \in \left\langle a_{\alpha(1)} X^{\alpha(1)}, \ldots, a_{\alpha(s)} X^{\alpha(s)} \right\rangle$ wtedy i tylko wtedy, gdy reszta z dzielenia f przez $(a_{\alpha(1)} X^{\alpha(1)}, \ldots, a_{\alpha(s)} X^{\alpha(s)})$ jest równa zero.

9 Bazy Gröbnera

Definicja. Niech $I \subset \mathbb{K}[X]$ będzie niezerowym ideałem.

- $LT(I) = \{LT(f) \mid f \in I \setminus \{0\}\}$
- $LM(I) = \{LM(f) \mid f \in I \setminus \{0\}\}$
- $\langle LT(I)\rangle = \langle LM(I)\rangle$ - ideał jednomianowy generowany przez elementy zbioru $LT(I)$

Uwaga. Jeżeli $I = \langle f_1, \ldots, f_s\rangle$, to ideały $\langle LT(f_1), \ldots LT(f_s)\rangle$ oraz $\langle LT(I)\rangle$ nie muszą być równe. Ponieważ

$$f_i \in I \;\Rightarrow\; LT(f_i) \in \langle LT(I)\rangle \;,$$

więc zawsze spełniona jest inkluzja:

$$\langle LT(f_1), \ldots LT(f_s)\rangle \subset \langle LT(I)\rangle \;.$$

Przykład. $f_1 = X^2 - X$, $f_2 = X^2 + X$, $I = \langle f_1, f_2\rangle$. Ponieważ $\gcd(f_1, f_2) = X$, więc $I = \langle X\rangle$ oraz $X \in \langle LT(I)\rangle$.

Z drugiej strony

$$\langle LT(f_1), LT(f_2)\rangle = \left\langle X^2, X^2\right\rangle = \left\langle X^2\right\rangle \;,$$

i oczywiście $\left\langle X^2\right\rangle$ nie jest równy $\langle X\rangle$.

Fakt 9.1 *Istnieją $g_1, \ldots, g_s \in I$ takie, że*

$$\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_s)\rangle \;.$$

Twierdzenie 9.2 (Twierdzenie Hilberta o Bazie) *Jeżeli $\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_s)\rangle$ dla $g_1, \ldots, g_s \in I$, to $I = \langle g_1, \ldots, g_s\rangle$.*

Więc każdy ideał $I \subset \mathbb{K}[X]$ jest skończenie generowany, tzn. istnieją $g_1, \ldots, g_s \in I$ takie, że $I = \langle g_1, \ldots, g_s\rangle$.

Definicja. Skończony zbiór $G = \{g_1, \ldots, g_s\} \subset I$ nazywamy *bazą Gröbnera* (lub *bazą standardową*) ideału I, jeżeli

$$\langle LT(I)\rangle = \langle LT(g_1), \ldots, LT(g_s)\rangle \;.$$

(Definicja bazy Gröbnera zależy więc od porządku jednomianów.)

Wniosek 9.3 *Każdy niezerowy ideał $I \subset \mathbb{K}[X]$ posiada bazę Gröbnera. Elementy bazy Gröbnera generują I.*

Uwaga ! Jeżeli wybierzemy jakiś porządek jednomianów to z każdym ideałem można stowarzyszyć wiele różnych baz Gröbnera. Można wprowadzić pojęcie tzw. *zredukowanej bazy Gröbnera*, która jest jednoznacznie zdeterminowana przez ideał.

Istnieją implementacje pozwalające liczyć bazy Gröbnera.

Przykład. `SINGULAR`

```
> ring r=0,(x,y),dp;
> ideal I=x3+y3-xy+1,x2y+xy2-x+y;
> ideal G=groebner(I); (Można też: > ideal G=std(I);)
> G;
G[1]=x2y+xy2-x+y
G[2]=x3+y3-xy+1
G[3]=y4-5xy2+2y3+x2-3xy+2x-y+1
G[4]=xy3+y4-xy2+x2-2xy+y2+y
```

Definicja. Pierścień przemienny P nazywamy *pierścieniem noetherowskim*, jeżeli spełniony jest jeden z równoważnych warunków

(i) każdy ideał w P jest skończenie generowany

(ii) każdy wstępujący ciąg ideałów $I_1 \subset I_2 \subset \ldots$ w pierścieniu P stabilizuje się, tzn. istnieje N takie, że $I_N = I_{N+1} = \ldots$

Wniosek 9.4 *Pierścień wielomianów $\mathbb{K}[X] = \mathbb{K}[X_1, \ldots, X_n]$ jest pierścieniem noetherowskim.*

Fakt 9.5 *Niech*

$$V(I) = V_K(I) = \{x \in \mathbb{K}^n \mid \forall\ f \in I\ :\ f(x) = 0\}\ .$$

Wtedy istnieją $f_1, \ldots, f_s \in I$ takie, że $V(I) = V(f_1, \ldots, f_s)$. Więc $V(I)$ jest zbiorem algebraicznym.

Fakt 9.6 *Niech $f \in \mathbb{K}[X]$. Istnieje dokładnie jeden element $r \in \mathbb{K}[X]$ taki, że*

(i) żaden składnik r nie dzieli się przez żaden składnik z $\langle LT(I)\rangle$,

(ii) istnieje $h \in I$ taki, że $f = h + r$.

Jak widać element r zależy od porządku jednomianów, ale nie zależy od wyboru bazy Gröbnera ideału I. Jeżeli wybierzemy już jakąś bazę Gröbnera $G = \{g_1, \ldots, g_s\}$, to warunek (i) możemy zastapić przez jeden z warunków:

(iii) żaden składnik r nie dzieli się przez żaden składnik z $\langle LT(g_1), \ldots, LT(g_s)\rangle$,

(iv) wielomian r jest resztą z dzielenia f przez G z użyciem Algorytmu Dzielenia

(Wybór bazy Gröbnera oraz wybór kolejności elementów w G nie wpływa na wartość r.) Czasem r nazywa się postacią normalną f *(*normal form*). Resztę będziemy oznaczać symbolem $NF(f)$.*

Przykład. SINGULAR

```
> ring r=0,(x,y),dp;
> ideal I=x3+y3-xy,x2-y2+1;
> ideal G=groebner(I);
> poly f=xy-x5+2y-3;
> poly a=NF(f,G);
> a;
2xy-y2+2y-5/2
> poly b=x3+y3-xy+x*(x2-y2+1);
> poly c=NF(b,G);
> c;
0
```

Niech $G = \{g_1, \ldots, g_s\}$ będzie bazą Gröbnera ideału I.

Ćwiczenie.

(i) $f = NF(f) \pmod I$,

(ii) $f \in I$ wtedy i tylko wtedy, gdy $NF(f) = 0$,

(iii) $NF(f \pm g) = NF(f) \pm NF(g)$,

(iv) $f = g \pmod I$ wtedy i tylko wtedy, gdy $NF(f) = NF(g)$,

(v) $NF(fg) = NF(NF(f) \cdot NF(g))$

Niech $\Delta \subset \mathbb{N}^n$ będzie zbiorem tych wielowskaźników α, że jednomian X^α nie dzieli się przez żaden z jednomianów $LM(g_1), \ldots, LM(g_s)$. Wtedy

$$NF(f) = \sum_{\alpha \in \Delta} a_\alpha X^\alpha \ .$$

Więc jednomiany $X^\alpha, \alpha \in \Delta$, rozpinają przestrzeń liniową $\mathbb{K}[X]/I$.

Ćwiczenie. Jeżeli skończona suma $\sum_{\alpha \in \Delta} a_\alpha X^\alpha = 0 \pmod I$, to wszystkie współczynniki $a_\alpha = 0$, więc jednomiany $X^\alpha, \alpha \in \Delta$, są liniowo niezależne w $\mathbb{K}[X]/I$.

Wniosek 9.7 *Jednomiany $X^\alpha, \alpha \in \Delta$, są bazą przestrzeni $\mathbb{K}[X]/I$, a więc $\dim_K \mathbb{K}[x]/I$ jest równy mocy zbioru Δ.*

Przykład.SINGULAR

```
> ring r=0,(x,y),dp;
> ideal I=x2+y3,xy;
> ideal G=groebner(I);
> G;
G[1]=xy
G[2]=y3+x2
G[3]=x3
> vdim(G);
5
> kbase(G);
y2
y
x2
x
1
> ideal J=xy, x2+xy2;
> ideal H=groebner(J);
> H;
H[1]=xy
```

```
H[2]=x2
> vdim(H);
-1
```

Jednomiany $Y^2, Y, X^2, X, 1$ są bazą $\mathbb{K}[X]/I$, więc $\dim_K \mathbb{K}[X]/I = 5$.

$\dim_K \mathbb{K}[X]/J = \infty$.

10 Twierdzenie Hilberta o Zerach

Sformułujemy bez dowodu tzw. Słabe Twierdzenie Hilberta o Zerach (Nullstellensatz).

Twierdzenie 10.1 $\mathbb{K}$ – *ciało algebraicznie domknięte, np.* $\mathbb{K} = \mathbb{C}$. *Niech* $I \subset \mathbb{K}[X]$ *będzie ideałem.*

Wtedy $V_K(I) = \emptyset$ *wtedy i tylko wtedy, gdy* $1 \in I$ *czyli* $I = \mathbb{K}[X]$.

Uwaga. jeżeli $\mathbb{K} = \mathbb{R}$ to twierdzenie nie jest prawdziwe. Np. weźmy ideał $I = \langle 1 + X^2 \rangle \subset \mathbb{R}[X]$, $n = 1$. Wtedy $V_R(I) = \emptyset$, ale $1 \notin \langle 1 + X^2 \rangle$.

Wniosek 10.2 *Niech* G *będzie bazą Gröbnera ideału* $I \subset \mathbb{K}[X]$, $\mathbb{K}$ – *ciało algebraicznie domknięte.*

Wtedy $V_K(I) = \emptyset$ *wtedy i tylko wtedy, gdy* $1 \in G$.

Przykład. SINGULAR

```
> ring r=0,(x,y),dp;
> ideal I1=x3+y3-x+y-2,x2-2y2+5x-4;
> ideal I2=x3+y3-x+y-2,x2-2y2+5x-4, xy+3y;
> ideal G1=groebner(I1);
> ideal G2=groebner(I2);
> G1;
G1[1]=x2-2y2+5x-4
G1[2]=2xy2+y3-10y2+28x+y-22
G1[3]=7y4+30y3-26xy-73y2+236x+42y-216
> G2;
G2[1]=1
```

Więc $V_C(I_1) \neq \emptyset$, $V_C(I_2) = \emptyset$.

Sformułujemy teraz Twierdzenie Hilberta o Zerach (Nullstellensatz)

Twierdzenie 10.3 $\mathbb{K}$ – *ciało algebraicznie domknięte. Jeżeli* $f, f_1, \ldots f_s \in \mathbb{K}[X]$ *oraz wielomian* f *przyjmuje wartość zero we wszystkich punktach zbioru algebraicznego* $V_K(f_1, \ldots, f_s)$*, wtedy*

$$\exists\ m \geq 1\ :\quad f^m \in \langle f_1, \ldots, f_s \rangle\ .$$

Definicja. Zbiór

$$\sqrt{I} = \mathrm{rad}(I) = \{f \in \mathbb{K}[X] \mid \exists\ m \geq 1\ :\quad f^m \in I\}$$

jest ideałem. Nazywamy go *radykałem* ideału I. Łatwo sprawdzić, że

- $I \subset \sqrt{I}$
- $V_K(\sqrt{I}) = V_K(I)$
- $\dim_K \mathbb{K}[X]/\sqrt{I} \leq \dim_K \mathbb{K}[X]/I$

Twierdzenie Hilberta o Zerach można sformułować następująco

Twierdzenie 10.4 $\mathbb{K}$ – *ciało algebraicznie domknięte. Jeżeli* $J \subset \mathbb{K}[X]$ *jest ideałem, to zbiór* $I(V_K(J))$ *wszystkich wielomianów przyjmujących wartość zero w punktach zbioru* $V_K(J)$ *jest równy* $\sqrt{J}$*, czyli*

$$I(V_K(J)) = \sqrt{J}\ .$$

Definicja. Ideał J jest *radykalny*, jeżeli $J = \sqrt{J}$.

Fakt 10.5 *Ideał* $\sqrt{I}$ *jest radykalny.*

Fakt 10.6 $\mathbb{K}$ – *ciało algebraicznie domknięte. Jeżeli ideał* $J \subset \mathbb{K}[X]$ *jest radykalny, to wielomian* f *zeruje się we wszystkich punktach zbioru algebraicznego* $V_K(J)$ *wtedy i tylko wtedy, gdy* $f \in J$.

11 Skończone zbiory algebraiczne w $\mathbb{C}^n$

Niech $I \subset \mathbb{K}[X]$ będzie ideałem, niech

$$\mathcal{A} = \mathcal{A}_K = \mathbb{K}[X]/I$$

oznacza pierścień ilorazowy stowarzyszony z ideałem I. (Symbolu $\mathcal{A}_K$ używa się aby podkreślić jakie ciało K rozpatrujemy.)

Twierdzenie 11.1 *(i)* $\dim_K \mathcal{A} = 0 \quad \Rightarrow \quad V(I) = \emptyset$,

(ii) $\dim_K \mathcal{A} < \infty \quad \Rightarrow \quad V(I)$ *jest zbiorem skończonym,*

(iii) $K = \mathbb{C}$ *oraz* $V(I)_C = \emptyset \quad \Rightarrow \quad \dim_C \mathcal{A}_C = 0$,

(iv) $V(I)_C$ *– skończony* $\quad \Rightarrow \quad \dim_C \mathcal{A}_C < \infty$.

Definicja. Algebra $\mathcal{A}$ jest *skończenie wymiarowa*, jeżeli

$$\dim_K \mathcal{A}_K < \infty.$$

Fakt 11.2 *Jeżeli* $\mathbb{K}$ *jest podciałem ciała* $\mathbb{C}$ *(np.* $\mathbb{K} = \mathbb{Q}$ *lub* $\mathbb{K} = \mathbb{R}$*) oraz ideał* I *jest generowany przez wielomiany ze współczynnikami z ciała* $\mathbb{K}$*, to*

$$\dim_K \mathcal{A}_K = \dim_C \mathcal{A}_C \ .$$

Ćwiczenia.

1. Załóżmy, że $X^3 - XY$ oraz $Y^2 + X - Y$ należą do ideału $I \subset \mathbb{K}[X, Y]$. Pokaż, że $\dim_K \mathcal{A} \leq 6$.

2. Niech $f_i \in \mathbb{K}[X] = K[X_1, \ldots, X_n]$ będą takimi wielomianami, że

$$f_i = X_i^{k(i)} + p_i \quad (1 \leq i \leq n)$$

gdzie wielomian p_i ma stopień $< k(i)$. Niech

$$f_1, \ldots, f_n \in I \subset \mathbb{K}[X], \quad \mathcal{A} = \mathbb{K}[X]/I \ .$$

Pokaż, że $\dim_K \mathcal{A} < \infty$.

3. Niech $I = \langle X^2 + Y, XY - 1 \rangle \subset \mathbb{C}[X, Y]$. Pokaż, że $\dim_C \mathbb{C}[X, Y]/I < \infty$.

Przykład. SINGULAR

```
> ring r=0,(x,y,z,w),dp;
> poly f1=2-x+3y-xy-zw+xyzw;
> poly f2=-1+z-2w+yz+x3-y4;
> poly f3=x2-y2+3z3-w3-xyzw;
> poly f4=2-z2-w3+xz-yzw+z4+w4;
```

```
> ideal I=f1,f2,f3,f4;
> ideal G=groebner(I);
> vdim(G);
148
```

Więc układ równań $f_1 = 0, \ldots, f_4 = 0$ ma skończenie wiele rozwiazań w $\mathbb{C}^4$.

Twierdzenie 11.3 *Niech $f_1, \ldots, f_r \in \mathbb{K}[X]$. Jeżeli*

$$0 < \dim_K \mathbb{K}[X]/\langle f_1, \ldots, f_r \rangle < \infty$$

to $r \geq n$.

Ćwiczenia.

- $f = X^2 + Y^2 \in \mathbb{R}[X, Y]$, $I = \langle f \rangle$. Wtedy $\dim_R \mathbb{R}[X, Y]/I = \infty$ ale $V_R(I) = \{(0, 0)\}$ jest skończony.
- $I = \langle 1 \rangle = \mathbb{K}[X] = \mathbb{K}[X_1, \ldots, X_n]$, $0 = \dim_K \mathbb{K}[X_1, \ldots, X_n]/\langle 1 \rangle < \infty$, a liczba generatorów ideału I jest równa 1.

Definicja. Wielomian h jest *jednorodny* (*stopnia k*), jeżeli wszystkie składniki tego wielomianu mają ten sam stopień (równy k).

Fakt 11.4 *Jeżeli h jest jednorodny oraz $h(x_0) = 0$, to $h(t \cdot x_0) = 0$ dla dowolnego $t \in \mathbb{K}$.*

Jeżeli $x_0 \neq \mathbf{0}$, to h przyjmuje wartość zero na całej prostej $\mathbb{K} \cdot x_0$.

Twierdzenie 11.5 (Bézout I) *Jeżeli $h_1, \ldots, h_n \in \mathbb{C}[X] = \mathbb{C}[X_1, \ldots, X_n]$ są jednorodne stopni $k_1, \ldots, k_n$ to poniższe warunki są równoważne:*

(i) $h_1^{-1}(0) \cap \ldots \cap h_n^{-1}(0)$ *jest skończony (tzn. $= \{\mathbf{0}\}$),*

(ii) $\dim_C \mathbb{C}[X]/\langle h_1, \ldots, h_n \rangle < \infty$,

(iii) $\dim_C \mathbb{C}[X]/\langle h_1, \ldots, h_n \rangle = k_1 \cdots k_n$.

Definicja. Jeżeli f jest wielomianem stopnia k, to symbolem $(f)_k$ oznaczymy wielomian jednorodny będący sumą składników stopnia k:
Np. jeżeli $f = 2 - X + Y + XY^2 - 3Y^3$ to $(f)_3 = XY^2 - 3Y^3$.

Twierdzenie 11.6 (Bézout II) *Niech* $g_1, \ldots, g_n \in \mathbb{K}[X] = \mathbb{K}[X_1, \ldots, X_n]$ *będą stopnia* $k_1, \ldots, k_n$ *(*$\mathbb{K} = \mathbb{C}$ *lub* $\mathbb{K} = \mathbb{R}$*). Niech* $h_1 = (g_1)_{k_1}, \ldots, h_n = (g_n)_{k_n}$.

Jeżeli $\{z \in \mathbb{C}^n \mid h_1(z) = \cdots = h_n(z) = 0\}$ *jest skończony (tzn.* $= \{\mathbf{0}\}$*), to*

$$\dim_K \mathbb{K}[X]/\langle g_1, \ldots, g_n\rangle = k_1 \cdots k_n.$$

Przykład. Niech $f_1 = 3 - X + 2Y^4 + X^5 + Y^5$, $f_2 = X^2 + Y^2 - X^4Y^4 \subset \mathbb{K}[X, Y]$, niech $\mathcal{A}_K = \mathbb{K}[X, Y]/\langle f_1, f_2\rangle$. Wtedy (nie używając komputera) można sprawdzić, że $\dim_K \mathcal{A} = 5 \cdot 8 = 40$.

W dalszej części tego rozdziału zajmiemy się oszacowaniem mocy zbioru $V_K(I)$, którą oznaczymy symbolem $\# V_K(I)$. Oczywiście zawsze moc $\# V_R(I)$ zbioru rozwiązań w $\mathbb{R}^n$ jest ograniczona przez moc $\# V_C(I)$ zbioru rozwiązań w $\mathbb{C}^n$, czyli $\# V_R(I) \leq \# V_C(I)$.

Ćwiczenie. Jeżeli $p_1, \ldots, p_s \in \mathbb{K}^n$ są parami różne, to istnieją $f_1, \ldots, f_s \in \mathbb{K}[X]$ takie, że

$$f_i(p_i) = 1, \quad f_i(p_j) = 0 \ \text{ dla } i \neq j \ .$$

Twierdzenie 11.7 *Niech* I *będzie ideałem w* $\mathbb{C}[X]$*, niech* $V_C(I) \subset \mathbb{C}^n$ *będzie zbiorem zer ideału* I *oraz* $\mathcal{A}_C = \mathbb{C}[X]/I$*. Wtedy*

(i) $\# V_C(I) \leq \dim_C \mathcal{A}_C$,

(ii) jeżeli $I = \sqrt{I}$ *(tzn.* I *jest ideałem radykalnym), to*

$$\# V_C(I) = \dim_C \mathcal{A}_C \ .$$

Przykład. Układ równań

```
f1=2-x+3y-xy-zw+xyzw=0
f2=-1+z-2w+yz+x3-y4=0
f3=x2-y2+3z3-w3-xyzw=0
f4=2-z2-w3+xz-yzw+z4+w4=0
```

ma co najwyżej 148 rozwiazań w $\mathbb{C}^4$.

12 Skończone zbiory algebraiczne w $\mathbb{R}^n$

Definicja. Baza Gröbnera $G = \{g_1, \ldots, g_s\}$ jest *zredukowana*, jeżeli

(1) $LC(g_k) = 1$ dla $1 \leq k \leq s$,

(2) żaden ze składników wielomianu g_k nie dzieli się przez żaden $LT(g_i)$, gdzie $i \neq k$.

Twierdzenie 12.1 *Każdy ideał posiada dokładnie jedną zredukowaną bazę Gröbnera.*

Przykład.SINGULAR

```
> ring r=0,(x,y,z),dp;
> poly f1=x2-2y3+z2-xyz+2;
> poly f2=xz-x3+2y-1;
> poly f3=z3-xy+2y+1;
> ideal I=f1,f2,f3;
> option(redSB);
> ideal G=std(I);
> vdim(G);
27
> ring s=0,(z,y,x),lp;
> ideal J=fglm(r,G);
> J;
J[1]=2x27+18x24+10x22+58x21-51x20+92x19-42x18-84x17+
191x16+14x15- 130x14+740x13-220x12+157x11+1177x10-
1644x9+2341x8+368x7-228x6+2940x5- 674x4+248x3-
636x2-864x-1198
J[2]=109369648916254332540601141761608334858542y+
119885499570528142122365070054722315 20x26-
....+356876776188511619520716753007003857308 08x-
322984951078200406999185405394099363820 16
J[3]=109369648916254332540601141761608334858542z-
747456739576197848760668792700975994 90x26+....
...+202300457748961858458344330033439137545546x2+
253606226192392279324467245742781101159 72x-
390852240880105768376824587567186084819 36
```

Zbiór $\{J[1]/LC(J[1]), J[2]/LC(J[2]), J[3]/LC(J[3])\}$ jest zredukowaną bazą Gröbnera ideału $\langle f_1, f_2, f_3 \rangle$.

Jak widać, rozwiązania w $\mathbb{K}^3$ układu równań $f_1 = 0,\ f_2 = 0,\ f_3 = 0$

są jednoznacznie wyznaczone przez pierwiaski wielomianu jednej zmiennej $J[1](x) = 0$. W szczególności rozwiązaniom w $\mathbb{R}^3$ odpowiadają rzeczywiste pierwiastki tego wielomianu, które można badać używając klasycznych metod dla jednej zmiennej (np. Lemat Kartezjusza, Twierdzenie Sturma). Najprostsza jest obserwacja, że układ równań ma co najmniej jedno rozwiazanie w $\mathbb{R}^3$, bo stopień wielomianu $J[1]$ równy $27 = \dim_K \mathcal{A}$ jest liczbą nieparzystą.

Kolejne twierdzenie wyjaśni, dlaczego otrzymaliśmy zredukowaną bazę Gröbnera takiej postaci.

Twierdzenie 12.2 *Niech $J \subset \mathbb{R}[X_1, \ldots, X_n]$ będzie ideałem radykalnym takim, że*

$$1 \leq m = \dim_R \mathcal{A}_R = \dim_C \mathcal{A}_C < \infty \ ,$$

gdzie $\mathcal{A}_K = \mathbb{K}[X_1, \ldots, X_n]/J$ dla $\mathbb{K} = \mathbb{R}$ lub $\mathbb{K} = \mathbb{C}$.
(Na mocy Twierdzenia 11.7, zbiór $V_C(J) \subset \mathbb{C}^n$ ma m elementów, tzn. $V_C(J) = \{p_1, \ldots, p_m\}$.) Oznaczmy $p_i = (x_{i1}, \ldots, x_{in})$.

Niech G będzie zredukowaną bazą Gröbnera ideału J w takim porządku leksykograficznym, że $X_1 > \ldots > X_n$. Załóżmy, że n-te współrzędne $x_{1n}, \ldots, x_{mn}$ punktów z $V_C(J)$ są parami różne.

Wtedy istnieją wielomiany $h_1, \ldots, h_n \in \mathbb{R}[X_n]$ takie,że

(i) $h_n(X_n) = (X_n - x_{1n}) \cdots (X_n - x_{mn})$ jest stopnia m,

(ii) wielomiany $h_1(X_n), \ldots, h_{n-1}(X_n)$ mają stopień $\leq m - 1$,

(iii) $G = \{X_1 + h_1(X_n), \ldots, X_{n-1} + h_{n-1}(X_n), h_n(X_n)\}$.

Uwaga. Jeżeli $\dim \mathcal{A} < \infty$ to zawsze możemy dokonać takiej liniowej zmiany układu współrzędnych aby założenie, że n-te współrzędne są różne, było spełnione.

Dowód przedstawimy w przypadku, gdy $n = 3$, oraz ideał zredukowany $J \subset \mathbb{R}[X, Y, Z]$.

Ponieważ J jest ideałem radykalnym oraz $\dim \mathcal{A} = m$, $m \neq 0$, więc $V_C(J) \subset \mathbb{C}^3$ jest skończony, i składa się z punktów

$$p_i = (x_i, y_i, z_i) \in \mathbb{C}^3, \quad 1 \leq i \leq m \ .$$

Ponieważ wielomiany generujące J mają współczynniki w $\mathbb{R}$, więc dla każdego p_i pewien p_j ma postać $p_j = (\overline{x_i}, \overline{y_i}, \overline{z_i})$.

Na mocy założeni, ostatnie współrzedne $z_1, \ldots, z_m$ są parami różne. Zdefiniujmy

$$h_3(Z) = (Z - z_1) \ldots (Z - z_m) \in \mathbb{R}[Z].$$

Ponieważm $h_3(x_i, y_i, z_i) = 0$ dla $1 \leq i \leq m$, więc h_3 przyjmuje wartość zero w każdym punkcie zbioru $V_C(J)$. Ideał J jest radykalny, więc $h_3 \in J \cap \mathbb{R}[Z]$.

Lemat 12.3 *Jeżeli $h(Z) \in J \cap \mathbb{R}[Z]$ jest niezerowy, to $h_3 \,|\, h$, więc* $\deg(h) \geq m$.

Fakt 12.4 *Istnieją wielomiany $f_1, f_2 \in \mathbb{R}[Z]$ stopnia $\leq m-1$ takie, że $X + f_1(Z)$, $Y + f_2(Z)$ przyjmują wartości zero w $V_C(J)$, więc*

$$X + f_1(Z) \in J, \quad Y + f_2(Z) \in J \ .$$

Wniosek 12.5 *Niech $J \subset \mathbb{R}[X_1, \ldots, X_n]$ będzie ideałem radykalnym spełniającym założenia Twierdzenia 12.2.*

Ilość zer $V_R(J) \subset \mathbb{R}^n$ jest równa ilości rzeczywistych pierwiastków wielomianu $h_n(X_n)$.

Jeżeli $\dim_R \mathcal{A}_R$ *jest nieparzysty, to $V_R(J) \neq \emptyset$.*

Niektóre z powyższych faktów będą spełnione również wtedy, jeżeli opuścimy założenie o radykalności ideału:

Fakt 12.6 *Niech $I \subset \mathbb{K}[X_1, \ldots, X_n]$ będzie ideałem. Jeżeli* $\dim_K \mathbb{K}[X_1, \ldots, X_n]/I < \infty$, *to*

$$\# V_C(I) \leq \dim_K \mathbb{K}[X_1, \ldots, X_n]/I \ .$$

Fakt 12.7 *Niech $I \subset \mathbb{R}[X_1, \ldots, X_n]$ będzie ideałem. Jeżeli* $\dim_R \mathbb{R}[X_1, \ldots, X_n]/I < \infty$ *jest nieparzysty, to $V_R(I) \neq \emptyset$.*

Fakt 12.8 *Niech $f \in \mathbb{K}[X]$ będzie wielomianem jednej zmiennej. Jeżeli $\langle f, f' \rangle = \mathbb{K}[X]$, to wszystkie zespolone pierwiastki wielomianu f są jednokrotne oraz ideał $\langle f \rangle$ jest radykalny.*

Definicja. Niech $I = \langle f_1, \ldots, f_k \rangle \subset \mathbb{K}[X_1, \ldots, X_n]$, $k \geq n$. Niech I' będzie ideałem generowanym przez $f_1, \ldots, f_k$ oraz wszystkie minory

$$\frac{\partial(f_{i_1}, \ldots, f_{i_n})}{\partial(X_1, \ldots, X_n)}, \text{ gdzie } 1 \leq i_1 < \ldots < i_n \leq k \ .$$

Powiemy, że *wszystkie zespolone zera ideału I są regularne*, jeżeli $I' = \mathbb{K}[X_1, \ldots, X_n]$.

Twierdzenie 12.9 *Załóżmy, że* $\dim_K \mathbb{K}[X]/I < \infty$. *Jeżeli wszystkie zespolone zera ideału* I *są regularne, to* I *jest ideałem radykalnym.*

Przykład. SINGULAR

```
> ring r=0,(x,y),dp;
> poly f1=x2-2xy2+y3+x-3;
> poly f2=y2-xy-y+1;
> poly f3=-2x2y2+xy3+x3+xy2-y3+x2+y2-3x-y;
> ideal I=f1,f2,f3;
> matrix A=jacob(I);
> ideal B=minor(A,2);
> ideal C=I,B;
> std(C);
1
> option(redSB);
> ideal G=std(I);
> vdim(G);
5
> ring s=0,(y,x),lp;
> ideal J=fglm(r,G);
> J;
J[1]=x5+x4-6x3+16x-16
J[2]=8y+x4+3x3-4x2-12x+8
> LIB ''rootsur.lib'';
> nrroots(J[1]);
1
```

Więc ideał I jest radykalny, układ równań $f_1 = 0, f_2 = 0, f_3 = 0$ ma dokładnie pięć różnych rozwiązań w $\mathbb{C}^2$, w tym dokładnie jedno rozwiązanie w $\mathbb{R}^2$.

Niech $I \subset \mathbb{K}[X_1, \ldots, X_n]$ będzie takim ideałem, że $\dim_K \mathbb{K}[X_1, \ldots, X_n]/I < \infty$. Tak jak w dowodzie Twierdzenia 12.2, i korzystając z Twierdzenia Hilberta o Zerach, można pokazać, że istnieją niezerowe wielomiany od jednej zmiennej:

$$Q_1(X_1), \ldots, Q_n(X_n) \in I \ .$$

Więc jeżeli $p = (x_1, \ldots, x_n) \in V_C(I)$, to $Q_1(x_1) = 0, \ldots, Q_n(x_n) = 0$. Niech

$$P_1 = \frac{Q_1}{\gcd\left(Q_1, \frac{\partial Q_1}{\partial X_1}\right)}, \ldots, P_n = \frac{Q_n}{\gcd\left(Q_n, \frac{\partial Q_n}{\partial X_n}\right)} .$$

Wprawdzie $P_1, \ldots, P_n$ niekoniecznie należą do I, ale jeżeli $p = (x_1, \ldots, x_n) \in V_C(I)$, to

$$P_i(p) = P_i(x_i) = 0, \qquad \frac{\partial P_i}{\partial X_i}(p) = \frac{\partial P_i}{\partial X_i}(x_i) \neq 0 ,$$

oraz $\frac{\partial P_i}{\partial X_j} \equiv 0$ dla $i \neq j$. Więc

$$\frac{\partial(P_1, \ldots, P_n)}{\partial(X_1, \ldots, X_n)}(p) = \frac{\partial P_1}{\partial X_1}(p) \cdots \frac{\partial P_n}{\partial X_n}(p) \neq 0 .$$

Twierdzenie 12.10 *Niech* $I = \langle f_1, \ldots, f_k \rangle \subset \mathbb{K}[X_1, \ldots, X_n]$ *będzie takim ideałem, że* $\dim_K \mathbb{K}[X_1, \ldots, X_n]/I < \infty$. *Niech*

$$J = \langle f_1, \ldots, f_k, P_1, \ldots, P_n \rangle .$$

Wtedy $J = \sqrt{I}$.

Jako wniosek otrzymujemy mocniejszą wersję twierdzenia 12.9:

Twierdzenie 12.11 *Załóżmy, że* $\dim_K \mathbb{K}[X]/I < \infty$. *Wtedy wszystkie zespolone zera ideału* I *są regularne wtedy i tylko wtedy, gdy* I *jest ideałem radykalnym.*

Przykład. SINGULAR

```
> ring r=0,(x,y,z),dp;
> poly f1=x2-xyz+y3;
> poly f2=z4-xy+3x3;
> poly f3=x2y+y4-5x2z;
> ideal I=f1,f2,f3;
> matrix A=jacob(I);
> ideal B=minor(A,3);
> ideal C=I,B;
> groebner(C);
y3-xyz+x2
z4+3x3-xy
xy2z-5x2z
```

```
x2yz
219284129587644x3z+...
> vdim(groebner(I));
39
> LIB "primdec.lib";
> ideal J=radical(I);
> option(redSB);
> ideal GJ=std(J);
> vdim(GJ);
11
> ring s=0,(y,z,x),lp;
> ideal H=fglm(r,GJ);
> H;
H[1]=151875x11+4050x10+3037527x9+63318375x8+19411875x7-
210937350x6+6591909376x5+2345125x4+718750x3-7812500x2+244140625x

H[2]=294838423698850016660424881229532145877705566406 25z-
246213224351615540270326095121468454177625 0x10-...-
772277932998982240043094027135011939628906 25x

H[3]=117935369479540006664169952491812858351082226 5625y+
394516586078582537412298136291260309852500x10+...-
129742990787426340883968430328194082149218 7500x
> LIB ''rootsur.lib'';
> nrroots(H[1]);
1
```

Ideał $I = \langle f_1, f_2, f_3 \rangle$ nie musi być radykalny, ideał $J = \sqrt{I}$ jest radykalny z definicji. Układ równań $f_1 = 0, f_2 = 0, f_3 = 0$ ma dokładnie 11 różnych rozwiązań w $\mathbb{C}^3$, w tym dokładnie jedno rozwiązanie (w punkcie $\mathbf{0}$) należące do $\mathbb{R}^3$.

W programie SINGULAR istnieje użyteczny sposób sprawdzania, ile jest takich zer w $\mathbb{R}^n$ które leżą w zbiorze

$$\{(x_1, \ldots, x_n) \mid x_1 > 0, \ldots, x_n > 0\} :$$

Przykład. SINGULAR

```
> ring r=0,(x,y,z),dp;
> poly f1=x3+y3+z3-3;
```

```
> poly f2=xy+xz+yz-3;
> poly f3=xyz-1;
> ideal i=f1,f2,f3;
> ideal I=std(i);
> vdim(I);
18
> LIB ''signcond.lib'';
> firstoct(I);
1
```

13 Ślad odwzorowania liniowego

- V - $\mathbb{R}$-liniowa przestrzeń wektorowa skończonego wymiaru
- $L : V \to V$ - odwzorowanie $\mathbb{R}$-liniowe
- $M(L)$ - macierz (kwadratowa) L w dowolnej bazie przestrzeni V
- $\mathbb{R} \ni \mathrm{Tr}(L) =$ suma elementów na przekątnej macierzy $M(L)$
- wartość $\mathrm{Tr}(L)$ nie zależy od wyboru bazy w V, nazywamy ją *śladem* L
- $\mathrm{Tr}(L_1 + L_2) = \mathrm{Tr}(L_1) + \mathrm{Tr}(L_2)$
- $\mathrm{Tr}(\alpha \cdot L) = \alpha \cdot \mathrm{Tr}(L)$ dla $\alpha \in \mathbb{R}$
- jeżeli $L' : W \to W$ oraz $(L, L') : V \times W \to V \times W$, to

$$\mathrm{Tr}((L, L')) = \mathrm{Tr}(L) + \mathrm{Tr}(L')$$

14 Formy dwuliniowe

- V - $\mathbb{R}$-przestrzeń wektorowa skończonego wymiaru
- $\Phi : V \times V \to \mathbb{R}$ - odwzorowanie dwuliniowe symetryczne
- $\Phi^2 : V \to \mathbb{R}$: $\quad \Phi^2(v) = \Phi(v, v)$ - forma kwadratowa

- istnieją podprzestrzenie liniowe $V_1, V_2 \subset V$ maksymalnego wymiaru spełniające:
$$\forall \ v \in V_1 \setminus \{\mathbf{0}\} \qquad \Phi^2(v,v) > 0$$
$$\forall \ v \in V_2 \setminus \{\mathbf{0}\} \qquad \Phi^2(v,v) < 0$$
- $$\sigma(\Phi^2) = \dim_R V_1 - \dim_R V_2 \ \in \mathbb{Z}$$
Liczbę $\sigma(\Phi^2)$ nazywamy *sygnaturą* formy kwadratowej Φ^2
- jeżeli $\Psi : W \times W \to \mathbb{R}$ dwuliniowa symetryczna, $\Psi^2 : W \to \mathbb{R}$, oraz $(\Phi^2 + \Psi^2) : V \times W \to \mathbb{R}$, to
$$\sigma(\Phi^2 + \Psi^2) = \sigma(\Phi^2) + \sigma(\Psi^2)$$

Przykład. $\Phi^2(x,y,z) = x^2 - xy + z^2 =$
$$x^2 - 2x(\frac{1}{2}y) + \frac{1}{4}y^2 - \frac{1}{4}y^2 + z^2 = (x - \frac{1}{2}y)^2 - \frac{1}{4}y^2 + z^2 \ .$$
Więc $\qquad \sigma(\Phi^2) = 1 - 1 + 1 = 1.$

15 Formy dwuliniowe na pierścieniach

- A - pierścień przemienny będący również $\mathbb{R}$-przestrzenią wektorową skończonego wymiaru
- $h \in A$ - ustalony element

Dla $f \in A$ niech $L_h(f) : A \to A$ będzie odwzorowaniem liniowym zdefiniowanym wzorem:
$$A \ni a \mapsto h \cdot f \cdot a \in A \ .$$
Wtedy $\qquad t_h(f) := \mathrm{Tr}(L_h(f)) \in \mathbb{R} \ . \qquad$ Ponieważ
$$t_h(f+g) = \mathrm{Tr}(L_h(f+g)) = \mathrm{Tr}(L_h(f) + L_h(g)) =$$
$$\mathrm{Tr}(L_h(f)) + \mathrm{Tr}(L_h(g)) = t_h(f) + t_h(g),$$
$$t_h(\alpha \cdot f) = \mathrm{Tr}(L_h(\alpha \cdot f)) = \mathrm{Tr}(\alpha \cdot L_h(f)) =$$
$$\alpha \cdot \mathrm{Tr}(L_h(f)) = \alpha \cdot t_h(f), \ \text{gdzie } \alpha \in \mathbb{R} \ ,$$
więc $t_h : A \to \mathbb{R}$ jest liniowe.

Ponieważ pierścień A jest przemienny, więc

$$T_h : A \times A \to \mathbb{R} \ : \ T_h(f,g) = t_h(f \cdot g) \ ,$$

jest dwuliniową formą symetryczną.

$$T_h^2 : A \to \mathbb{R} \ : \ T_h^2(f) = T_h(f,f) = t_h(f^2)$$

jest formą kwadratową. Jest więc zdefiniowana sygnatura formy T_h^2:

$$\sigma(T_h^2) \in \mathbb{Z} \ .$$

Jak widać, każdemu elementowi h pierścienia A można w sposób kanoniczny przyporządkować liczbę całkowitą $\sigma(T_h^2)$.

Ćwiczenie. Jeżeli $A = A_1 \times \cdots \times A_s$ jest produktem kartezjańskim pierścieni oraz

$$h = (h_1, \cdots, h_s) \in A_1 \times \cdots \times A_s \ , \quad \text{to}$$

$$\sigma(T_h^2) = \sigma(T_{h_1}^2) + \cdots + \sigma(T_{h_s}^2) \ .$$

Macierz każdej formy $T_{h_i}^2$ jest nieosobliwa wtedy i tylko wtedy, gdy macierz formy T_h^2 jest nieosobliwa.

Więc w takim wypadku, aby obliczyć $\sigma(T_h^2)$ wystarczy znać sygnatury stowarzyszone z $h_1, \ldots, h_s$ w każdym składniku.

Fakt 15.1 *Niech $A = \mathbb{R}$, $h \in \mathbb{R}$. Wtedy*

$$\sigma(T_h^2) = \mathit{znak}(h) \ .$$

Jeżeli T_h^2 jest nieosobliwa, to $h \neq 0$.

Fakt 15.2 *Niech $A = \mathbb{C}$, $h \in \mathbb{C}$. Wtedy*

$$\sigma(T_h^2) = 0 \ .$$

Jeżeli T_h^2 jest nieosobliwa, to $h \neq 0$.

16 Znaki wielomianu na zbiorze algebraicznym

Weźmy $f_1, \ldots, f_s \in \mathbb{R}[X]$. Zdefiniujmy

- $J_R = \langle f_1, \ldots, f_s \rangle \subset \mathbb{R}[X]$

- $J_C = \langle f_1, \ldots, f_s \rangle \subset \mathbb{C}[X]$
- $\mathcal{A}_R = \mathbb{R}[X]/J_R$
- $\mathcal{A}_C = \mathbb{C}[X]/J_C$

Fakt 16.1 $\dim_R \mathcal{A}_R = \dim_C \mathcal{A}_C$.

Będziemy zakładać, że J_C jest takim ideałem, że

(A) $J_C \neq \mathbb{C}[X]$,

(B) $J_C = \sqrt{J_C}$,

(C) $1 \leq m = \dim_C \mathcal{A}_C < \infty$.

Z Twierdzenia o Zerach wynika, że $f \in J_C$ wtedy i tylko wtedy, gdy f przyjmuje wartość zero we wszystkich punktach zbioru $V_C(J_C)$. Z Twierdzenia 11.7, $V_C(J_C)$ jest zbiorem skończonym złożonym z m punktów.

Oznaczmy:

- $V_C(J_C) = \{p_1, \ldots, p_k, q_1, \overline{q_1}, \ldots, q_\ell, \overline{q_\ell}\} \subset \mathbb{C}^n$, gdzie $m = k + 2\ell$
- $V_R(J_R) = \{p_1, \ldots, p_k\} \subset \mathbb{R}^n$
- $V_C(J_C) \setminus V_R(J_R) = \{q_1, \overline{q_1}, \ldots, q_\ell, \overline{q_\ell}\} \subset \mathbb{C}^n \setminus \mathbb{R}^n$
- jeżeli $q_i = (z_1, \ldots, z_n)$, to $\overline{q_i} = (\overline{z_1}, \ldots, \overline{z_n})$

Definicja.

$$\mathcal{B}_C = \underbrace{\mathbb{C} \times \cdots \times \mathbb{C}}_{m=k+2\ell}$$

$$\mathcal{B}_R = \underbrace{\mathbb{R} \times \cdots \times \mathbb{R}}_{k} \times \underbrace{\mathbb{C} \times \cdots \times \mathbb{C}}_{\ell}$$

Ćwiczenie. Z naturalnymi działaniami dodawania i mnożenia na współrzędnych:

- $\mathcal{B}_C$ jest $\mathbb{C}$-przestrzenią wektorową, $\dim_C \mathcal{B}_C = m$
- $\mathcal{B}_R$ jest $\mathbb{R}$-przestrzenią wektorową, $\dim_R \mathcal{B}_R = m$
- $\mathcal{B}_C$ oraz $\mathcal{B}_R$ są pierścieniami

Fakt 16.2 *Niech* $\xi_C : \mathbb{C}[X] \to \mathcal{B}_C$ *będzie surjektywnym homomorfizmem pierścieni zdefiniowanym wzorem:*

$$\mathbb{C}[X] \ni f \mapsto \xi_C(f) = (f(p_1), \ldots, f(p_k), f(q_1), f(\overline{q_1}), \ldots, f(q_\ell), f(\overline{q_\ell})) \in \mathcal{B}_C \ .$$

Wtedy $\operatorname{Ker} \xi_C = J_C \subset \mathbb{C}[X]$. *Więc*

$$\mathcal{A}_C = \mathbb{C}[X]/J_C = \mathbb{C}[X]/\operatorname{Ker} \xi_C \simeq \mathcal{B}_C \ .$$

Fakt 16.3 *Niech* $\xi_R : \mathbb{R}[X] \to \mathcal{B}_R$ *będzie surjektywnym homomorfizmem pierścieni zdefiniowanym wzorem:*

$$\mathbb{R}[X] \ni f \mapsto \xi_R(f) = (f(p_1), \ldots, f(p_k), f(q_1), \ldots, f(q_\ell)) \in \mathcal{B}_R \ .$$

Wtedy $\operatorname{Ker} \xi_R = J_R \subset \mathbb{R}[X]$. *Więc*

$$\mathcal{A}_R = \mathbb{R}[X]/J_R = \mathbb{R}[X]/\operatorname{Ker} \xi_R \simeq \mathcal{B}_R \ .$$

Możliwość rozkładu pierścienia $\mathcal{A}_R$ na bardzo proste składniki pozwala charakteryzować sygnatury form kwadratowych na $\mathcal{A}_R$ przez sygnatury na tych składnikach.

Kolejne twierdzenie zostało udowodnione przez E.Beckera, T.Wörmanna oraz P.Pedersena, M.-F.Roy, A.Szpirglas.

Twierdzenie 16.4 *Niech* $h \in \mathbb{R}[X]$, *niech* $T_h^2 : \mathcal{A}_R \to \mathbb{R}$ *będzie formą kwadratową stowarzyszoną z* h. *Wtedy*

$$\sigma(T_h^2) = \sum_{i=1}^{k} \operatorname{znak}(h(p_i)) \ .$$

Jeżeli T_h^2 *jest niezdegenerowana, to* $h(p_i) \neq 0$ *dla* $1 \leq i \leq k$.

(Można udowodnić to Twierdzenie jeżeli tylko $\dim_R \mathcal{A}_R < \infty$, *bez założenia, że ideał* J_C *jest radykalny.)*

Wniosek 16.5

$$\sigma(T_h^2) = \#\{p \in V_R(I) \mid h(p) > 0\} \ - \ \#\{p \in V_R(I) \mid h(p) < 0\} \ .$$

Wniosek 16.6

$$\sigma(T_1^2) = \#V_R(I) \ .$$

Przykład. SINGULAR

```
> ring r=0,(x,y,z),dp;
> poly f1=x3-yz+z2-3;
> poly f2=y3-xyz+z-y+2;
> poly f3=z4-y2z+y+1;
> poly h=x2-y2+z3-x+2;
> LIB ''rootsmr.lib'';
> ideal i=f1,f2,f3;
> ideal I=groebner(i);
> vdim(I);
36
> ideal b=qbase(I);
> matrix m=matbil(1,b,I);
> det(m);
-4920981729178573025.....
> symsignature(m);
2
> matrix n=matbil(h,b,I);
> det(n);
-3373102853138801001......
> symsignature(n);
2
```

Więc $\sigma(T_1^2) = 2$ oraz $\sigma(T_h^2) = 2$. Łatwo można teraz sprawdzić, że $V_R(I)$ składa się z dwóch punktów. W obu tych punktach wielomian h przyjmuje dodatnie wartości.

Ćwiczenie. Układ $x^3 - xy + y^3 = 1$, $x^3 - y^2 + x - y = 0$ ma rozwiązanie w punkcie $(1, 1)$. Czy układ $x^3 - xy + y^3 = 1.01$, $x^3 - y^2 + x - y = -0.01$ ma rzeczywiste rozwiązanie w kole o środku $(1, 1)$ i promieniu $\frac{1}{10}$.

17 Stopień topologiczny

Niech $B \subset \mathbb{R}^n$ będzie zbiorem zwartym o niepustym wnętrzu.

Niech $F = (f_1, \ldots, f_n) : B \to \mathbb{R}^n$ będzie takim odwzorowaniem ciągłym, że $F^{-1}(\mathbf{0}) \subset \mathrm{int}(B)$.

Można wtedy zdefiniować *stopień topologiczny* $\mathrm{DEG}(F, B) \in \mathbb{Z}$ odwzo-

rowania F na B.

Twierdzenie 17.1 *Jeżeli* $\mathrm{DEG}(F, B) \neq 0$, *to* $F^{-1}(\mathbf{0}) \cap \mathrm{int}(B) \neq \emptyset$.

Jeżeli F jest klasy C^1, $p \in \mathrm{int}(D)$, to symbolem

$$\mathrm{Jac}(p) = \frac{\partial(f_1, \ldots, f_n)}{\partial(X_1, \ldots, X_n)}(p)$$

będziemy oznaczać Jacobian w punkcie p, tzn. wyznacznik

$$\det \left[\frac{\partial f_i}{\partial X_j}(p) \right]_{i,j=1}^{n}$$

macierzy pochodnej $DF(p) : \mathbb{R}^n \to \mathbb{R}^n$ w punkcie p.

Definicja. Odwzorowaninie $F : B \to \mathbb{R}^n$ ma *regularne zera*, jeżeli $\mathrm{Jac}(p) \neq 0$ dla $p \in F^{-1}(\mathbf{0})$.

Jeżeli $\mathrm{Jac}(p) > 0$, to $DF(p) : \mathbb{R}^n \to \mathbb{R}^n$ *zachowuje orientację* przestrzeni $\mathbb{R}^n$.

Jeżeli $\mathrm{Jac}(p) < 0$, to $DF(p) : \mathbb{R}^n \to \mathbb{R}^n$ *zmienia orientację* przestrzeni $\mathbb{R}^n$.

Twierdzenie 17.2 *Jeżeli F ma regularne zera, to*

$$\mathrm{DEG}(F, B) = \sum_{p \in F^{-1}(\mathbf{0})} \mathrm{znak}\ (\mathrm{Jac}(p)) \ .$$

Jeżeli B jest podzbiorem płaszczyzny $\mathbb{R}^2$ którego brzeg $\partial B = B \setminus \mathrm{int}(B)$ jest sumą skończonej rodziny rozłącznych zamkniętych krzywych, to ∂B można kanonicznie zorientować.

W takim wypadku $F(\partial B)$ "nawija się" skończenie wiele razy wokół $\mathbf{0} \in \mathbb{R}^2$.

Fakt 17.3 *Jeżeli ∂B jest sumą skończonej rodziny zamkniętych rozłącznych krzywych na płaszczyźnie $\mathbb{R}^2$, oraz $F : B \to \mathbb{R}^2$, to*

$$\mathrm{DEG}(F, B) = \textit{ilość nawinięć } F(\partial B) \textit{ wokół } \mathbf{0} \ .$$

18 Stopień topologiczny odwzorowań wielomianowych

Załóżmy, że $f_1, \ldots, f_n, u \in \mathbb{R}[X] = \mathbb{R}[X_1, \ldots, X_n]$. Zdefiniujmy

$$F = (f_1, \ldots, f_n) : \mathbb{R}^n \to \mathbb{R}^n \ ,$$

$$B = \{x \in \mathbb{R}^n \mid u(x) \geq 0\} \ .$$

Załóżmy, że B jest zbiorem zwartym. Łatwo jest sprawdzić, że $\partial B = u^{-1}(0)$.

Niech $I = \langle f_1, \ldots, f_n \rangle$ oraz $\mathcal{A}_R = \mathbb{R}[X]/I$. Załóżmy, że $\dim_R \mathcal{A}_R < \infty$. Oczywiście

$$h_1 = \mathrm{Jac} \ , \ h_2 = \mathrm{Jac} \cdot u$$

są wielomianami, więc można zdefiniować formy kwadratowe $T^2_{h_1}, T^2_{h_2}$ na $\mathcal{A}_R$

Twierdzenie 18.1 *Jeżeli* $\dim_R \mathcal{A}_R < \infty$*, to* F *ma skończenie wiele zer.*

(i) Jeżeli $\langle f_1, \ldots, f_n, u \rangle = \mathbb{R}[X]$*, to* F *nie ma zer na* ∂B*, więc stopień topologiczny* $\mathrm{DEG}(F, B)$ *jest określony.*

(ii) Jeżeli forma $T^2_{h_1}$ *jest niezdegenerowana, to* F *ma regularne zera.*

(iii) Jeżeli obie formy $T^2_{h_1}$ *oraz* $T^2_{h_2}$ *są niezdegenerowane, to*

$$\mathrm{DEG}(F, B) = \frac{1}{2}\left(\sigma(T^2_{h_1}) + \sigma(T^2_{h_2})\right) \ .$$

Przykład. SINGULAR

```
> ring r=0,(x,y),dp;
> poly f1=-y+7xy+5x2y-5x5;
> poly f2=x-x2+6y2-x2y2+8x4;
> poly u=1-x2-y2;
> ideal i=f1,f2;
> matrix A=jacob(i);
> poly Jac=det(A);
> poly h1=Jac;
> poly h2=Jac*u;
> ideal I=std(i);
> vdim(I);
```

```
12
> ideal j=f1,f2,u;
> ideal J=std(j);
> J;
1
> LIB ''rootsmr.lib'';
> ideal b=qbase(I);
> matrix m=matbil(h1,b,I);
> det(m);
933500003619188878016....
> symsignature(m);
0
> matrix n=matbil(h2,b,I);
> det(n);
2453554908481340652.....
> symsignature(n);
0
```

Więc $\mathrm{DEG}(F, B) = 0$. Warto zauważyć, że $F^{-1}(\mathbf{0}) \cap B$ musi mieć co najmniej dwa elementy.

Uwaga. Jeżeli odwzorowanie F ma nieregularne zera, to nie można liczyć stopnia topologicznego używając powyższego twierdzenia. Istnieje inny algorytm (również oparty na formach kwadratowych), pozwalający liczyć stopień tylko przy założeniu, że $\dim_R \mathcal{A}_R < \infty$ oraz $\langle f_1, \ldots, f_n, u\rangle = \mathbb{R}[X]$. Jego opis można znaleźć na stronie
$http://mat.ug.edu.pl/\sim szafran/szafraniec\_chambery.pdf$.

19 Charakterystyka Eulera

Definicja. Podzbiór przestrzeni $\mathbb{R}^n$ nazywamy *hiperpłaszczyzną* (odp. *otwartą półprzestrzenią*) jeżeli istnieje funkcja linowa $L : \mathbb{R}^n \to \mathbb{R}$ oraz stała $c \in \mathbb{R}$ taka, że ten podzbiór ma postać $\{x \in \mathbb{R}^n \mid L(x) = c\}$ (odp. $\{x \in \mathbb{R}^n \mid L(x) < c\}$).

Zbiór $S \subset \mathbb{R}^n$ nazywamy *ścianą*, jeżeli jest przekrojem skończonej rodziny złożonej z hiperpłaszczyzn oraz otwartych półprzestrzeni.

Fakt 19.1 *Ściana jest zbiorem wypukłym, jej wymiar jest równy wymiarowi najmniejszej podprzestrzeni afinicznej w której ściana jest za-*

warta.

Fakt 19.2 *Jeżeli S jest ścianą, to domknięcie $\overline{S}$ oraz brzeg $\partial S = \overline{S} \setminus S$ jest sumą skończonej rodziny rozłącznych ścian.*

Definicja. Domknięty zbiór $W \subset \mathbb{R}^n$ nazywamy *wielościanem*, jeżeli istnieje taka skończona rodzina $\{S_i\}$ parami rozłącznych ścian, że

- $W = \bigcup_i S_i$,
- dla każdej sciany S_j : $\overline{S_j}$ oraz ∂S_j są sumami pewnych ścian z rodziny $\{S_i\}$.

Definicja. *Charakterystyką Eulera* wielościanu W nazywamy liczbę całkowitą:

$$\chi(W) = \sum_i (-1)^{\dim(S_i)} \ .$$

Przykłady.

$$\chi(\emptyset) = 0$$

$$\chi(\{x_0\}) = 1$$

$$\chi(\mathbb{R}^n) = \begin{cases} -1 & \text{gdy } n \text{ jest nieparzyste} \\ +1 & \text{gdy } n \text{ jest parzyste} \end{cases}$$

$$\chi(\{(x,y) \mid x \geq 0\}) = 0$$

$$\chi(\{(x,y) \mid x \geq 0,\ y \geq 0,\ x+y \leq 1\}) = 1$$

Twierdzenie 19.3 *Charakterystyka Eulera $\chi(W)$ nie zależy od tego, jak wybierzemy ściany z których składa się W.*

Fakt 19.4 *Jeżeli $W_1, W_2 \subset \mathbb{R}^n$ są wielościanami, to $W_1 \cup W_2$ oraz $W_1 \cap W_2$ są wielościanami, oraz:*

$$\chi(W_1 \cup W_2) = \chi(W_1) + \chi(W_2) - \chi(W_1 \cap W_2) \ .$$

Twierdzenie 19.5 *Jeżeli wielościany $W_1 \subset \mathbb{R}^n$, $W_2 \subset \mathbb{R}^m$ są homeomorficzne, to*

$$\chi(W_1) = \chi(W_2) \ .$$

Definicja. Niech X będzie zbiorem homeomorficznym z pewnym wielościanem W. Liczbę

$$\chi(X) := \chi(W)$$

nazywamy *charakterystyką Eulera* zbioru X.

Twierdzenie 19.6 *Każdy zbiór algebraiczny, jak również każdy zbiór postaci* $\{x \in \mathbb{R}^n \mid f(x) \geq c\}$ $(f \in \mathbb{R}[X],\ c \in \mathbb{R})$, *jest homeomorficzny z pewnym wielościanem, więc charakterystyka Eulera takich zbiorów jest określona.*

20 Zbiory $f \geq c$

Niech $f : \mathbb{R}^n \to \mathbb{R}$ będzie funkcją klasy C^2. Zdefiniowany jest *gradient*

$$\nabla f = \left(\frac{\partial f}{\partial X_1}, \ldots, \frac{\partial f}{\partial X_n}\right) : \mathbb{R}^n \to \mathbb{R}^n$$

Definicja. $p \in \mathbb{R}^n$ nazywamy punktem *regularnym* (odp. *krytycznym*) funkcji f jeżeli $\nabla f(p) \neq \mathbf{0}$ (odp. $\nabla f(p) = \mathbf{0}$).

Hesjan funkcji f jest zdefiniowany jako

$$\mathrm{Hess}(f)(p) = \mathrm{Jac}(\nabla f)(p) = \det\left[\frac{\partial^2 f}{\partial X_i\, \partial X_j}(p)\right] .$$

Punkt krytyczny p jest *niezdegenerowany* jeżeli $\mathrm{Hess}(f)(p) \neq 0$.

Twierdzenie 20.1 *Niech* $f : \mathbb{R}^n \to \mathbb{R}$ *będzie takim wielomianem, że zbiór* $B = \{x \in \mathbb{R}^n \mid f(x) \geq c\}$ *jest ograniczony (a więc zwarty), oraz wszystkie punkty należące do zbioru* $\{x \in \mathbb{R}^n \mid f(x) = c\}$ *są punktami regularnymi funkcji* f. *Wtedy*

(i) $\chi(B) = (-1)^n \,\mathrm{DEG}(\nabla f, B)$.

(ii) Liczba składowych zbioru B *jest ograniczona przez*

$$\#\{x \in B \mid \nabla f(x) = \mathbf{0}\} .$$

(iii) Jeżeli $n = 2$, *to* $\partial B = \{x \in \mathbb{R}^n \mid f(x) = c\}$ *jest sumą skończonej rodziny zamkniętych owali, których liczba przystaje* (mod 2) *do* $\mathrm{DEG}(\nabla f, B)$.

Przykład. SINGULAR

```
> ring r=0,(x,y,z),dp;
> poly f=-2+x2+5y2+3z2-3xyz+x2y-2y3+4y2z-x4-3y4-2z4;
> ideal F=f;
> ideal grad=jacob(F);
> ideal GRAD=std(grad);
> vdim(GRAD);
27
> matrix hess=jacob(grad);
> poly Hess=det(hess);
> ideal p1=grad,Hess;
> std(p1);
1
> poly u=f+1;
> ideal p2=grad,u;
> std(p2);
1
> poly h1=Hess;
> poly h2=Hess*u;
> LIB ''rootsmr.lib'';
> ideal b=qbase(GRAD);
> matrix k=matbil(1,b,GRAD);
> det(k);
145533517569821042617.....
> symsignature(k);
15
> matrix l=matbil(u,b,GRAD);
> det(l);
-22862037364712617987.....
> symsignature(l);
5
> matrix m=matbil(h1,b,GRAD);
> det(m);
211800047362454101101.....
> symsignature(m);
-1
> matrix n=matbil(h2,b,GRAD);
> det(n);
```

```
-33271927164993089574......
> symsignature(n);
1
```

Więc charakterystyka Eulera zbioru $\{x \in \mathbb{R}^3 \mid f(x) \geq -1\}$ jest równa zero. Funkcja f ma w tym zbiorze 10 punktów krytycznych.

21 Szeregi formalne

Definicja. Każdy napis

$$\sum_{\alpha} a_\alpha \, X^\alpha = \sum_{\alpha} a_\alpha X_1^{\alpha_1} \cdots X_n^{\alpha_n},$$

gdzie $\alpha = (\alpha_1, \ldots, \alpha_n) \in \mathbb{N}^n$ oraz $a_\alpha \in \mathbb{R}$, nazywamy *formalnym szeregiem potęgowym* (o współczynnikach rzeczywistych).

Zbiór szeregów potęgowych oznaczać będziemy jednym z symboli:

$$\mathbb{R}[[X]] = \mathbb{R}[[X_1, \ldots, X_n]].$$

$\mathbb{R}[[X]]$ z naturalnymi działaniami dodawania i mnożenia jest pierścieniem, i przestrzenią wektorową nad $\mathbb{R}$.

Istnieje naturalny injektywny homomorfizm $\mathbb{R}[X] \hookrightarrow \mathbb{R}[[X]]$.

Uwaga. Formalne szeregi potęgowe nie muszą być zbieżne poza $\mathbf{0}$.

Twierdzenie 21.1 $\mathbb{R}[[X]]$ *jest pierścieniem noetherowskim i lokalnym, tzn. posiada dokładnie jeden ideał maksymalny* $\mathbf{m}$ *składający się z tych szeregów, których wyraz wolny jest równy zero.*

W pierścieniu $\mathbb{R}[[X]]$ można wprowadzić pojęcie *bazy standardowej ideału* analogicznie jak w $\mathbb{R}[X]$. Jeżeli ideał w $\mathbb{R}[[X]]$ był generowany przez wielomiany, to używając takich programów jak `SINGULAR`, można obliczać bazy standarowe w $\mathbb{R}[[X]]$.

Przykład. `SINGULAR`

```
> ring r=0,(x,y),dp;
> poly f1=x2-y2+x2y2;
```

```
> poly f2=xy-x4;
> ideal i=f1,f2;
> ideal I=std(i);
> vdim(I);
10
> I;
I[1]=x3-xy2+y3
I[2]=xy3+x2+xy-y2
I[3]=x2y2+x2-y2
I[4]=y5+x2y+xy2
```

```
> ring s=0,(x,y),ds;
> poly g1=x2-y2+x2y2;
> poly g2=xy-x4;
> ideal j=g1,g2;
> ideal J=std(j);
> vdim(J);
4
> J;
J[1]=x2-y2
J[2]=xy
J[3]=y3
```

Jak pokazuje ten przykład, te same wielomiany generują istotnie różne ideały w pierścieniu wielomianów oraz w pierścieniu szeregów formalnych.

22 Lokalny stopień topologiczny

Niech $F = (f_1, \ldots, f_n) : (\mathbb{R}^n, \mathbf{0}) \to (\mathbb{R}^n, \mathbf{0})$ będzie takim odwzorowaniem wielomianowym, że $F(\mathbf{0}) = \mathbf{0}$.

Załóżmy, że $\mathbf{0}$ jest punktem izolowanym zbioru $F^{-1}(\mathbf{0})$.

Definicja. *Lokalnym stopniem topologicznym* w punkcie $\mathbf{0}$ nazywamy liczbę całkowitą

$$\mathrm{DEG}_0(F) = \mathrm{DEG}(F, B(r)) \ ,$$

gdzie $B(r) = \{x \in \mathbb{R}^n \mid \ \| x \| \leq r\}$ oraz $\{\mathbf{0}\} = F^{-1}(\mathbf{0}) \cap B(r)$.

Zdefiniujmy: $Q := \mathbb{R}[[X_1, \ldots, X_n]] / \langle f_1, \ldots, f_n \rangle$,

$\mathcal{J}$ – warstwa Jacobianu Jac w Q .

Twierdzenie 22.1 (Eisenbud-Levine, Khimshiashvili) .

(i) $\dim_R Q < \infty \quad \Rightarrow \quad \mathbf{0}$ *jest izolowany w* $F^{-1}(\mathbf{0})$

(ii) Niech $\theta : Q \to \mathbb{R}$ *będzie takim liniowym funkcjonałem, że* $\theta(\mathcal{J}) > 0$. *Zdefiniujmy dwuliniową formę symetryczną*

$$\Theta : Q \times Q \to \mathbb{R} \ : \qquad \Theta(a, b) = \theta(a \cdot b) \ ,$$

oraz stowarzyszoną z nią formę kwadratową

$$\Theta^2 : Q \to \mathbb{R} \ : \qquad \Theta^2(a) = \Theta(a, a) = \theta(a^2) \ .$$

Forma Θ^2 *jest niezdegenerowana, oraz*

$$\mathrm{DEG}_0(F) = \sigma(\Theta^2) \ .$$

Przykład. $F(X_1, X_2) = (X_1^2 - X_2^2, 2X_1X_2)$

$$I = \left\langle X_1^2 - X_2^2, 2X_1X_2 \right\rangle \subset \mathbb{R}[[X_1, X_2]]$$

$$X_2^3 = -X_2(X_1^2 - X_2^2) + (\frac{1}{2}X_1) \cdot 2X_1X_2 \in I$$

$$Q = \mathbb{R}[[X_1, X_2]]/I \simeq \mathbb{R}[[X_1, X_2]] / \left\langle X_1^2 - X_2^2, X_1X_2, X_2^3 \right\rangle$$

$$X_1^2 \equiv X_2^2, \quad X_1X_2 \equiv 0, \quad X_2^3 \equiv 0$$

$$Q = \{b_1 \cdot 1 + b_2 \cdot X_1 + b_3 \cdot X_2 + b_4 \cdot X_2^2\}$$

$$\mathcal{J} = \det \begin{bmatrix} 2X_1 & -2X_2 \\ 2X_2 & 2X_1 \end{bmatrix} = 4(X_1^2 + X_2^2) \equiv 8X_2^2$$

$$\theta(b_1 \cdot 1 + b_2 \cdot X_1 + b_3 \cdot X_2 + b_4 \cdot X_2^2) = b_4$$

$$\theta(\mathcal{J}) = 8 > 0$$

$$\text{macierz formy } \Theta^2 = \begin{bmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}$$

$$\sigma(\Theta) = 2$$

$$\mathrm{DEG}_0(F) = 2\ .$$

Przykład. `Program A.Łęckiego`

```
4 4
x1^5-x1*x2*x3*x4+2*x1^2*x3^2:
x2^4+3*x2*x3^2-4*x1^2*x3:
x3^4-x2^2*x4+5*x2*x3*x4:
x4^5+3*x1*x3^2+2*x2^2*x3-x4^7:

Local complex degree = 186
Computations in real case
Rank of matrix = 186
Signature = 0
```

`Czas: ok. 1.5 min.` Więc $\mathrm{DEG}_0(F) = 0$.

23 Punkty osobliwe hiperpowierzchni

Niech $f : (\mathbb{R}^n, \mathbf{0}) \to (\mathbb{R}, 0)$ będzie wielomianem. Oznaczmy

$$S(r) = \{x \in \mathbb{R}^n \mid \ \| x \| = r\}$$

$$L(r) = S(r) \cap f^{-1}(0)$$

$$A_-(r) = S(r) \cap \{f \leq 0\}, \quad A_+(r) = S(r) \cap \{f \geq 0\}\ .$$

Jeżeli $r > 0$ jest dostatecznie małym promieniem, to topologia zbiorów $L(r)$, $A_+(r)$, $A_-(r)$ jest dobrze zdefiniowana z dokładnością do homeomorfizmu.

Twierdzenie 23.1 (Sullivan) *Charakterystyka Eulera $\chi(L(r))$ jest zawsze parzysta.*

Twierdzenie 23.2 (Khimshiashvili) *Jeżeli f ma izolowany punkt krytyczny w punkcie $\mathbf{0}$, tzn. $\mathbf{0}$ jest punktem izolowanym w zbiorze $\{x \in \mathbb{R}^n \mid \nabla f(x) = \mathbf{0}\}$, to*

$$\chi(A_-(r)) = 1 - \mathrm{DEG}_0(\nabla f)$$

$$\chi(A_+(r)) = 1 + (-1)^{n+1}\,\mathrm{DEG}_0(\nabla f)$$

$$\chi(L(r)) = \begin{cases} 0 & \textit{jeżeli } n \textit{ jest nieparzyste} \\ 2(1 - \mathrm{DEG}_0(\nabla f)) & \textit{jeżeli } n \textit{ jest parzyste} \end{cases}$$

Przykład. Niech $f(X_1, X_2) = \frac{1}{3}X_1^3 - X_1X_2^2$. Wtedy

$$\nabla f = (X_1^2 - X_2^2, -2X_1X_2) : \mathbb{R}^2\mathbf{0} \to \mathbb{R}^2, \mathbf{0}),$$

$$\mathrm{DEG}_0(\nabla f) = -2\ ,$$

$$\chi(A_-(r)) = \chi(A_+(r)) = 3, \quad \chi(L(r)) = 6\ .$$

Przykład. `Program A. Łęckiego`

```
3 3
d(1;x1^5-x2^6+x1*x2*x3+4*x2*x3^7-5*x1^2*x2^2*x3^2):
d(2;x1^5-x2^6+x1*x2*x3+4*x2*x3^7-5*x1^2*x2^2*x3^2):
d(3;x1^5-x2^6+x1*x2*x3+4*x2*x3^7-5*x1^2*x2^2*x3^2):

Local complex degree = 40
Computations in real case
Rank of matrix = 40
Signature = 2
```

`Czas: 1 sek.` Więc dla $f = X_1^5 - X_2^6 + X_1X_2X_3 + 4X_2X_3^7 - 5X_1^2X_2^2X_3^2$:

$$\chi(A_-(r)) = -1,\ \chi(A_+(r)) = 3,\ \chi(L(r)) = 0\ .$$

Jeżeli $f : (\mathbb{R}^n, \mathbf{0}) \to (\mathbb{R}, 0)$ jest wielomianem jednorodnym, to topologia zbiorów $S(r)$, $L(r)$, $A_+(r)$, $A_-(r)$ nie zależy od wyboru promienia r. W szczególności te zbiory są homeomorficzne odpowiednio ze zbiorami:

$$S(1) = S^{n-1}$$

$$L(1) = S^{n-1} \cap f^{-1}(0)$$
$$A_-(1) = S^{n-1} \cap \{f \leq 0\}, \quad A_+(1) = S^{n-1} \cap \{f \geq 0\} \ .$$

Twierdzenie 23.3 (Sz., Bruce) *Niech $f : \mathbb{R}^n \to \mathbb{R}$ będzie wielomianem jednorodnym stopnia d, niech k będzie dowolną nieparzystą liczbą naturalną $> \ d-1$. Zdefiniujmy:*

$$H_1 = \left(\frac{\partial f}{\partial X_1} - X_1^k, \ldots, \frac{\partial f}{\partial X_n} - X_n^k \right) : (\mathbb{R}^n, \mathbf{0}) \to (\mathbb{R}^n, \mathbf{0}) \ ,$$

$$H_2 = \left(-\frac{\partial f}{\partial X_1} - X_1^k, \ldots, -\frac{\partial f}{\partial X_n} - X_n^k \right) : (\mathbb{R}^n, \mathbf{0}) \to (\mathbb{R}^n, \mathbf{0}) \ .$$

Wtedy punkt $\mathbf{0}$ jest izolowany w $H_1^{-1}(\mathbf{0})$, $H_2^{-1}(\mathbf{0})$, oraz

$$\chi(A_-(1)) = 1 - \mathrm{DEG}_0(H_1) \ ,$$

$$\chi(A_+(1)) = 1 - \mathrm{DEG}_0(H_2) \ ,$$

$$\chi(L(1)) = 1 + (-1)^n - \mathrm{DEG}_0(H_1) - \mathrm{DEG}_0(H_2) \ .$$

Przykład. `Program A.Łęckiego`

```
3 3
d(1;x1*x2*x3)-x1^3:
d(2;x1*x2*x3)-x2^3:
d(3;x1*x2*x3)-x3^3:

Local complex degree = 11
Computations in real case
Rank of matrix = 11
Signature = 3

3 3
-d(1;x1*x2*x3)-x1^3:
-d(2;x1*x2*x3)-x2^3:
-d(3;x1*x2*x3)-x3^3:

Local complex degree = 11
Computations in real case
Rank of matrix = 11
Signature = 3
```

Więc dla $f = X_1X_2X_3$:

$$\chi(A_1(1)) = -2,\ \chi(A_+(1)) = -2,\ \chi(L(1)) = -6\ .$$

24 Charakterystyka Eulera hiperpowierzchni

Niech $f : (\mathbb{R}^n, \mathbf{0}) \to (\mathbb{R}, 0)$ będzie wielomianem stopnia $d \geq 2$:

$$f = \sum_\alpha a_\alpha X^\alpha =$$

$$\underbrace{\sum_{|\alpha|=0} a_\alpha X^\alpha}_{f_0} + \underbrace{\sum_{|\alpha|=1} a_\alpha X^\alpha}_{f_1} + \cdots + \underbrace{\sum_{|\alpha|=d} a_\alpha X^\alpha}_{f_d}\ .$$

Zdefinujmy wielomiany od n oraz $n+1$ zmiennych:

$$g(X_1, \ldots, X_n) = f_d\ ,$$

$$h(X_1, \ldots, X_n, X_{n+1}) = X_{n+1}^d f_0 + X_{n+1}^{d-1} f_1 + \cdots + X_{n+1} f_{d-1} + f_d\ .$$

Przykład. Niech $f = 3 - X_1 + X_1X_2 + X_1^3 - X_2^3$. Wtedy

$$g = X_1^3 - X_2^3\ ,$$

$$h = 3X_3^3 - X_3^2X_1 + X_3X_1X_2 + X_1^2 - X_2^2\ .$$

Wielomiany h, g są jednorodne stopnia d. Niech k będzie naturalną nieparzystą liczbą $>\ d-1$. Zdefiniujmy:

$$G_1 = \left(\frac{\partial g}{\partial X_1} - X_1^k, \ldots, \frac{\partial g}{\partial X_n} - X_n^k\right) : (\mathbb{R}^n, \mathbf{0}) \to (\mathbb{R}^n, \mathbf{0})\ ,$$

$$G_2 = \left(-\frac{\partial g}{\partial X_1} - X_1^k, \ldots, -\frac{\partial g}{\partial X_n} - X_n^k\right) : (\mathbb{R}^n, \mathbf{0}) \to (\mathbb{R}^n, \mathbf{0})\ ,$$

$$H_1 = \left(\frac{\partial h}{\partial X_1} - X_1^k, \ldots, \frac{\partial h}{\partial X_{n+1}} - X_{n+1}^k\right) : (\mathbb{R}^{n+1}, \mathbf{0}) \to (\mathbb{R}^{n+1}, \mathbf{0})\ ,$$

$$H_2 = \left(-\frac{\partial h}{\partial X_1} - X_1^k, \ldots, -\frac{\partial h}{\partial X_{n+1}} - X_{n+1}^k\right) : (\mathbb{R}^{n+1}, \mathbf{0}) \to (\mathbb{R}^{n+1}, \mathbf{0})\ .$$

Twierdzenie 24.1 (Sz.) *Odwzorowania G_1, G_2, H_1, H_2 mają izolowane zero w* $\mathbf{0}$.

Niech W będzie hiperpowierzchnią w $\mathbb{R}^n$ złożoną z zer wielomianu f:

$$W = \{x \in \mathbb{R}^n \mid f(x) = 0\} \ .$$

Wtedy charakterystyka Eulera $\chi(W)$ jest równa

$$\frac{1}{2}\left(\mathrm{DEG}_0(G_1) + \mathrm{DEG}_0(G_2) - \mathrm{DEG}_0(H_1) - \mathrm{DEG}_0(H_2)\right) + (-1)^{n+1} \ .$$

Na stronach
`http://homepage.univie.ac.at/herwig.hauser/bildergalerie/gallery.html`
`http://wims.unice.fr/gallery/`
`http://mathworld.wolfram.com/AlgebraicSurface.html`
można znaleźć liczne przyklady algebraicznych powierzchni w $\mathbb{R}^3$. Jedną z nich jest *powierzchnia Nordstranda*:
`http://mathworld.wolfram.com/NordstrandsWeirdSurface.html`.
Jej równanie ma postać

$$25\left[X^3(Y+Z) + Y^3(X+Z) + Z^3(X+Y)\right] + 50(X^2Y^2 + X^2Z^2 + Y^2Z^2) -$$
$$125(X^2YZ + Y^2XZ + Z^2XY) + 60XYZ - 4(XY + XZ + YZ) = 0 \ .$$

Używając programu A. Łęckiego można obliczyć, że

$$\mathrm{DEG}_0(G_1) = -1, \quad \mathrm{DEG}_0(G_2) = +7 \ ,$$
$$\mathrm{DEG}_0(H_1) = 19, \quad \mathrm{DEG}_0(H_2) = -9 \ .$$

Więc charakterystyka Eulera powierzchni Nordstranda jest równa -1.

Inny przykład to *powierzchnia Clebscha*:
`http://mathworld.wolfram.com/ClebschDiagonalCubic.html`.
Jej równanie ma postać

$$81(X^3 + Y^3 + Z^3) - 189(X^2Y + X^2Z + Y^2X + Y^2Z + Z^2X + Z^2Y) + 54XYZ +$$
$$126(XY + XZ + YZ) - 9(X^2 + Y^2 + Z^2) - 9(X + Y + Z) + 1 = 0 \ .$$

Używając programu A. Łęckiego można obliczyć, że

$$\mathrm{DEG}_0(G_1) = 0, \quad \mathrm{DEG}_0(G_2) = 0 \ ,$$
$$\mathrm{DEG}_0(H_1) = 6, \quad \mathrm{DEG}_0(H_2) = 6 \ .$$

Więc charakterystyka Eulera powierzchni Clebscha jest równa -5.

Niech $W_- = \{x \in \mathbb{R}^n \mid f(x) \leq 0\}$, $W_+ = \{x \in \mathbb{R}^n \mid f(x) \geq 0\}$.

Twierdzenie 24.2 *Jeżeli d jest liczbą parzystą, to*

$$\chi(W_-) = \frac{1}{2}\left(\mathrm{DEG}_0(G_1) - \mathrm{DEG}_0(H_1)\right) \ ,$$

$$\chi(W_+) = \frac{1}{2}\left(\mathrm{DEG}_0(G_2) - \mathrm{DEG}_0(H_2)\right) \ .$$

Przykład. Jeżeli f jest takie, jak w definicji powierzchni Nordstranda, to $\chi(W_-) = -10$, $\chi(W_+) = +8$.

Jeżeli liczba d jest nieparzysta, to trzeba zdefiniować odwzorowania:

$$h' = X_{n+1} \cdot h \ ,$$

$$H_1' = \left(\frac{\partial h'}{\partial X_1} - X_1^{d+2}, \ldots, \frac{\partial h'}{\partial X_{n+1}} - X_{n+1}^{d+2}\right) : (\mathbb{R}^{n+1}, \mathbf{0}) \to (\mathbb{R}^{n+1}, \mathbf{0}) \ ,$$

$$H_2' = \left(-\frac{\partial h'}{\partial X_1} - X_1^{d+2}, \ldots, -\frac{\partial h'}{\partial X_{n+1}} - X_{n+1}^{d+2}\right) : (\mathbb{R}^{n+1}, \mathbf{0}) \to (\mathbb{R}^{n+1}, \mathbf{0}) \ .$$

Twierdzenie 24.3 *Odwzorowania H_1', H_2' mają izolowane zero w $\mathbf{0}$, oraz*

$$\chi(W_-) = \frac{1}{2}\left((-1)^n - \mathrm{DEG}_0(H_1')\right) \ ,$$

$$\chi(W_+) = \frac{1}{2}\left((-1)^n - \mathrm{DEG}_0(H_2')\right) \ .$$

Przykład. Jeżeli f jest takie, jak w definicji powierzchni Clebscha, to $\chi(W_-) = \chi(W_+) = -3$.

25 Lokalna liczba łuków krzywej

Niech $H = (h_1, \ldots, h_{n-1}) : (\mathbb{R}^n, \mathbf{0}) \to (\mathbb{R}^{n-1}, \mathbf{0})$ będzie odwzorowaniem wielomianowym. Załóżmy, że w pobliżu $\mathbf{0}$ zbiór $H^{-1}(\mathbf{0})$ jest skończoną

sumą łuków mających jeden punkt wspólny w $\mathbf{0}$. Niech b będzie liczbą tych łuków. Oznaczmy

$$\Omega = \det \begin{bmatrix} X_1 & \cdots & X_n \\ \frac{\partial h_1}{\partial X_1} & \cdots & \frac{\partial h_1}{\partial X_n} \\ \vdots & \vdots & \vdots \\ \frac{\partial h_{n-1}}{\partial X_1} & \cdots & \frac{\partial h_{n-1}}{\partial X_n} \end{bmatrix}$$

$$F = (\Omega, h_1, \ldots, h_{n-1}) : (\mathbb{R}^n, \mathbf{0}) \to (\mathbb{R}^n, \mathbf{0}) \ .$$

Twierdzenie 25.1 (Aoki, Fukuda, Nishimura,Sun) *Jeżeli* $\mathbf{0}$ *jest izolowany w zbiorze* $F^{-1}(\mathbf{0})$*, to w pobliżu* $\mathbf{0}$ *zbiór* $H^{-1}(0)$ *jest skończoną sumą łuków mających jeden punkt wspólny w* $\mathbf{0}$*, oraz*

$$b = 2 \cdot \mathrm{DEG}_0(F) \ .$$

Przykład. Niech $H = (h_1, h_2) : (\mathbb{R}^3, \mathbf{0}) \to (\mathbb{R}^2, \mathbf{0})$, gdzie:

$$h_1 = X_1^5 - X_1X_2X_3 + X_2^3 + 4X_3^4 \ ,$$

$$h_2 = X_1^3X_2 - X_2X_3^3 - X_1^4X_3 \ .$$

Używając programu A.Łęckiego można sprawdzić, że $\mathbf{0}$ jest izolowany w zbiorze $F^{-1}(\mathbf{0})$ oraz $\mathrm{DEG}_0(F) = +6$. Więc w pobliżu $\mathbf{0}$ zbiór $H^{-1}(0)$ jest sumą dwunastu łuków mających jeden punkt wspólny w $\mathbf{0}$.