Wybrane zagadnienia Algebry
Lista zadań

Jacek Cichoń
WIT, PWr, 2023/24

1 Wstęp

Lab. 1

Liczbami Gaussa nazywamy pierścień $\mathbb{Z}[\imath] = \{a+b\imath : a, b \in \mathbb{Z}\}$ z dodawaniem i dzieleniem odziedziczonym z liczb zespolonych. Na $\mathbb{Z}[\imath]$ określamy funkcję (zwaną normą) $N(a+b\imath) = a^2+b^2$. Dla $x, y \in \mathbb{Z}[\imath]$ określamy $x|y \longleftrightarrow (\exists z \in \mathbb{Z}[\imath])(y = x \cdot z)$

1. Napisz algorytm dzielenia z resztą w pierścieniu liczb Gaussa $\mathbb{Z}[\imath]$, czyli algorytm, który dla danych $x, y \in \mathbb{Z}[\imath]$, $y \neq 0$ wyznaczy $q, r \in \mathbb{Z}[\imath]$ takie, że $x = q \cdot y + r$ oraz $N(r) < N(y)$.
2. Największym wspólnym dzielnikiem liczb $u, v \in \mathbb{Z}[\imath]$ nazywamy takie $d \in \mathbb{Z}[\imath]$, że $(d|u) \wedge (d|v)$ oraz
$$(\forall x \in \mathbb{Z}[\imath])(x|u \wedge x|v \rightarrow x|d) \ .$$
Oprogramuj algorytm wyznaczania NWD dla $\mathbb{Z}[\imath]$.
3. Oprogramuj funkcję wyznaczającą $NWW(x, y)$ dla $x, y \in \mathbb{Z}[\imath]$.
4. Ideał generowany przez liczby $a_1, \ldots, a_k$ oznaczamy przez $(a_1, \ldots, a_k)$. Korzystając z poprzednich dwóch podpunktów znajdź takie c i d, że $(3 + 4\imath, 1 + 3\imath) = (c)$ oraz $(3 + 4\imath) \cap (1 + 3\imath) = (d)$.

Lab. 2

Wielomian $a_0 + a_1 \cdot x + \ldots + a_n x^n \in \mathbb{R}[x]$ interpretujemy jako ciąg $[a_0, \ldots, a_n]$.

1. Napisz algorytm dzielenia z resztą w pierścieniu wielomianów $\mathbb{R}[x]$.
2. Oprogramuj algorytm wyznaczania NWD dla $\mathbb{R}[x]$.
3. Oprogramuj funkcję wyznaczającą $\mathrm{NWW}(x, y)$ dla $x, y \in \mathbb{R}[x]$.
4. Korzystając z poprzednich dwóch podpunktów znajdź takie $c(x), d(x) \in \mathbb{R}[x]$, że $(1 + x^2, 1 + 2x + x^2) = (c)$ oraz $(1 + x^2) \cap (1 + 2x + x^2) = (d)$.

Ćwicz. 1

Rozważ prostą przechodzącą przez punkt $(-1, 0)$ o współczynniku kierunkowym $t \in \mathbb{R}$. Znajdź drugi punkt przecięcia tej prostej z okręgiem $x^2 + y^2 = 1$. Wyraź otrzymane rozwiązanie jako funkcję $p(t) = (x(t), y(t))$ oraz wyznacz obraz $\{p(t) : t \in \mathbb{R}\}$.

Ćwicz. 2

Rozważ prostą przechodzącą przez punkt $(-1, 0)$ o współczynniku kierunkowym $t \in \mathbb{R}$. Znajdź drugi punkt przecięcia tej prostej z hiperbolą $x^2 - y^2 = 1$. Wyraź otrzymane rozwiązanie jako funkcję $p(t) = (x(t), y(t))$ oraz wyznacz obraz $\{p(t) : t \in \mathbb{R}\}$.

Niech k będzie ciałem. Dla wielomianów $f_1, \ldots, f_k \in k[x_1, \ldots, k_n]$ przez $V(f_1, \ldots, f_k)$ oznaczamy zbiór
$$V(f_1, \ldots, k_k) = \{(a_1, \ldots, a_n) \in k^n : (\forall i \in \{1, \ldots, k\})(f_i(a_1, \ldots, a_n) = 0)\} \ .$$
Zbiór ten nazywamy **rozmaitością algebraiczną** generowaną przez wielomiany $f_1, \ldots, f_k$ w **przestrzeni afinicznej** k^n.

Lab. 3

Skorzystaj z jakiejś biblioteki (np. `mplot3d` z `Matplotlib`) do wyświetlenia następujących rozmaitości algebraicznych w $\mathbb{R}^3$:

1. $V(z - x^2 - y^2)$
2. $V(z^2 - x^2 - y^2)$
3. $V(z - x^2 + y^2)$
4. $V(xz, yz)$

Lab. 4

Krzywą czterolistną nazywaną krzywą zadaną następującym równaniem

$$r(\theta) = \sin(2\theta)$$

we współrzędnych biegunowych.

1. Narysuj wykres tej krzywej na płaszczyźnie.
2. Spróbuj znaleźć wielomian $w(x, y)$ taki, że $r[\mathbb{R}] = V(w)$.

Lab. 5

Zapoznaj się poleceniami systemu Wolfram Alpha służącymi go działań na wielomianach (np. PolynomialQuotientRemainder) oraz generowania krzywych i powierzchni zadawanych równaniami parametrycznymi.

2 Wielomiany i rozmaitości

Ćwicz. 3

Które z następujących podzbiorów $\mathbb{R}^2$ są rozmaitościami algebraicznymi:

1. skończony podzbiór $\mathbb{R}^2$
2. $\mathbb{Z} \times \mathbb{Z}$
3. $\mathbb{R} \times [0, \infty)$?

Ćwicz. 4

Ustalmy ciało k liczbę $n \geqslant 1$. Pokaż, że rodzina rozmaitości algebraicznych w k^n jest domknięta na skończone sumy oraz skończone przekroje. Czy jest ona domknięta na operację dopełnienia?

Lab. 6

Zaproponuj algorytm który wyznacza punkty minimalne dla skończonych podzbiorów $A \subseteq \mathbb{N}^k$ dla porządku

$$(x_1, \dots, x_k) \leqslant (y_1, \dots, y_k) \longleftrightarrow \bigwedge_{i=1}^{k} (x_j \leqslant y_i)$$

1. Ile jest punktów minimalnych w zbiorze $\{n, k) \in \mathbb{N}^2 : n \cdot k \geqslant 11\}$?
2. Ile jest punktów minimalnych w zbiorze $\{n, k) \in \mathbb{N}^2 : (n - 10)^2 + (y - 10)^2 \leqslant 25\}$?

Ćwicz. 5

Załóżmy, że k jest ciałem oraz $A \subseteq k^n$. Niech

$$I(A) = \{f \in k[x_1, \dots, x_n] : (\forall a \in A)(f(a) = 0)\} .$$

Pokaż, że $I(A)$ jest ideałem.

Ćwicz. 6

Pokaż, że $I(V(x^n, x^m)) = \langle x, y \rangle$ dla dowolnych $n, m \geqslant 1$.

Ćwicz. 7

Ideał I nazywamy radykalnym, jeśli z tego, że $x^n \in I$ wynika, że $x \in I$.

1. Pokaż, że ideały postaci $I(A)$ są radykalne.
2. Pokaż, że ideał $\left\langle X^2, y^2 \right\rangle$ nie jest radykalny.

Ćwicz. 8

Niech k będzie dowolnym nieskończonym ciałem.

1. Pokaż, że dowolny wielomian $f \in k[x, y]$ można zapisać w postaci

$$f = g(x) + (x - y)h(x, y)$$

   dla pewnego wielomianu $g \in k[x]$ oraz $h \in k[x, y]$.
2. Pokaż, że $I(V(x - y)) = \langle x - y \rangle$.

Ćwicz. 9

Pokaż, że $I(V(x^n, x^m)) = \langle x, y \rangle$ dla dowolnych $n, m \geqslant 1$.

Ćwicz. 10

Niech $\mathcal{R} = (R, +, \cdot)$ będzie pierścieniem. Załóżmy, że $a, b, c, q \in R$ oraz $a = q \cdot b + c$. Pokaż, że

$$\langle a, b \rangle = \langle b, c \rangle \ .$$

Lab. 7

Wyznacz za pomocą dowolnego systemu obliczeń algebraicznych

1. GCD $\left(x^4 + x^2 + 1, x^4 - x^2 - 2x - 1, x^3 - 1\right)$
2. GCD $\left(x^3 + x^2 - 4x - 4, x^3 - x^2 - 4x + 4, x^3 - 2x^2 - x + 2\right)$

Ćwicz. 11

Czy wielomian $x^2 - 2$ należy do następującego ideału

$$\left\langle x^3 + x^2 - 4x - 4, x^3 - x^2 - 4x + 4, x^3 - 2x^2 - x + 2 \right\rangle ?$$

Lab. 8

Napisz pseudokod procedury, która dla danych wielomianów $f, g \in k[x]$ znajduje takie $A, B \in k[x]$, że $nwd(f, g) = A \cdot f = B \cdot g$.
Wskazówka: Wzoruj się na algorytmie wyznaczania największego wspólnego dzielnika dla liczb całkowitych

Ćwicz. 12

W zadaniu tym zajmujemy wielomianami z pierścienia $\mathbb{C}[x]$.

1. Niech $f \in \mathbb{C}[x]$ będzie niezerowym wielomianem. Pokaż, że $V(f) = \emptyset$ wtedy i tylko wtedy, gdy f jest wielomianem stałym.
2. Załóżmy, że $f, \ldots, f_k \in \mathbb{C}[x]$. Pokaż, że $V(f_1, \ldots, f_k) = \emptyset$ wtedy i tylko wtedy, gdy $1 \in \langle f_1, \ldots, f_k \rangle$

3. Opisz procedurę rozstrzygającą, czy dla danych wielomianów $f, \ldots, f_k \in \mathbb{C}[x]$ rozmaitość $V(f_1, \ldots, f_k)$ jest niepusta.

Ćwicz. 13

Załóżmy, że $f \in \mathbb{C}[x]$ jest wielomianem postaci

$$f = c(x-a_1)^{r_1}(x-a_2)^{r_2}\cdots(x-a_k)^{r_k} \ ,$$

gdzie $a_1,\ldots,a_k$ są parami różne oraz $c \neq 0$. Niech

$$f_{red} = (x-a_1)(x-a_2)\cdots(x-a_k) \ .$$

1. Pokaż, że $V(f) = \{a_1,\ldots,a_k\}$.
2. Pokaż, że I jest ideałem oraz, że $I(V(f)) = \langle f_{red} \rangle$.
3. Pokaż, że

$$f_{red} = \frac{f}{gcd(f,f')} \ ,$$

gdzie f' oznacza formalną pochodną wielomianu f.

3 Porządki jednomianowe i dzielenie wielomianów

Ćwicz. 14

Niech $\prec$ będzie porządkiem jednomianowym. Pokaż, że jeśli $\alpha \prec \beta$ oraz $\gamma \prec \delta$ to

$$\alpha + \gamma \prec \beta + \delta \ .$$

Ćwicz. 15

Niech $\preceq$ będzie porządkiem jednomianowym na $\mathbb{N}^k$. Niech

$$\alpha \sqsubseteq \beta \longleftrightarrow (\forall i)(\alpha_i \leqslant \beta_i) \ .$$

Pokaż, że jeśli $\alpha \sqsubseteq \beta$ to $\alpha \preceq \beta$ (czyli, że $\sqsubseteq \subseteq \preceq$).

Ćwicz. 16

Dla $\alpha, \beta \in \mathbb{N}^k$ określamy

$$lcm(\alpha,\beta) = (\max(\alpha_1,\beta_1), \max(\alpha_2,\beta_2),\ldots,\max(\alpha_k,\beta_k)) \ .$$

1. Pokaż, że $lcm(\alpha, lcm(\beta,\gamma)) = lcm(lcm(\alpha,\beta),\gamma)$.
2. Pokż, że jeśli $\alpha \sqsubseteq \gamma$ i $\beta \sqsubseteq \gamma$ to $lcm(\alpha,\beta) \sqsubseteq \gamma$.

Ćwicz. 17

Pokaż, że

$$1 \prec x \prec x^2 \prec x^3 \prec x^4 \prec \ldots$$

jest jedynym porządkiem monomialnym na $\mathbb{N}$.

Ćwicz. 18

Ciąg liczb $(u_1,\ldots,u_k)$ jest liniowo niezależny nad ciałem liczb wymiernych $\mathbb{Q}$ jeśli dla dowolnych $\lambda_1,\ldots,\lambda_k \in \mathbb{Q}$ mamy

$$\left(\sum_{i=1}^{k} \lambda_i u_i = 0\right) \rightarrow (\lambda_1 = \lambda_2 = \ldots = \lambda_k = 0) \ .$$

1. Pokaż, że ciąg $(1, \sqrt{2}, \sqrt{3})$ jest niezależny nad $\mathbb{Q}$.

2. Załóżmy, że $(u_1, \ldots, u_k)$ jest niezależnym nad $\mathbb{Q}$ ciągiem liczb dodatnich. Na $\mathbb{N}^k$ definiujemy porządek

$$(\alpha \prec \beta) \longleftrightarrow \left(\sum_{i=1}^{k} \alpha_i u_i < \sum_{i=1}^{k} \beta_i u_i \right)$$

Pokaż, że $\prec$ jest porządkiem monomialnym na $\mathbb{N}$.

Ćwicz. 19

Rozstrzygnij, czy podane wielomiany należą do podanego idealu $I \subseteq \mathbb{R}[x]$:

1. $f(x) = x^2 - 2x + 1$, $I = \langle\, x - 1 \,\rangle$
2. $f(x) = x^3 - 1$, $I = \left\langle\, x^9 - 1, x^5 + x^3 - x^2 - 1 \,\right\rangle$
3. $f(x) = x^3 + 1$, $I = \left\langle\, x^2 - 1, x^2 - 3x + 2 \,\right\rangle$.

Ćwicz. 20

Rozważmy GradedLex porządek. Niech $f = x^3 - x^2y - x^2z$ oraz $g_1 = x^2y - z$ oraz $g_2 = xy - 1$.

1. Podziel f przez (g_1, g_2) i oznacz resztę przez r_1
2. Podziel f przez (g_2, g_1) i oznacz resztę przez r_2

Obliczenia te, niestety, wykonaj ręcznie.

3. Sprawdź, czy $r_1 - r_2 \in \langle\, g_1, g_2 \,\rangle$.

Ćwicz. 21

Znajdź parametryzację rozmaitości algebraicznych wyznaczonych przez następujące układy równań:

1. W przestrzeni $\mathbb{R}^3$ lub $\mathbb{C}^3$:

$$\begin{aligned} 2x + 3y + z &= 3 \\ x + 2y &= 2 \\ -x + y + z &= 1 \end{aligned}$$

2. W przestrzeni $\mathbb{R}^4$ lub $\mathbb{C}^4$:

$$\begin{aligned} x + y + u + z &= 1 \\ x - y + u &= 2 \end{aligned}$$

3. W przestrzeni $\mathbb{R}^3$ lub $\mathbb{C}^3$:

$$\begin{aligned} y &= x^2 \\ z &= x^4 \end{aligned}$$

Ćwicz. 22

Wyznacz reprezentację niejawną rozmaitości algebraicznych sparametryzowanych w następujący sposób:

1. W przestrzeniach $\mathbb{R}^3$ lub $\mathbb{C}^3$:

$$\begin{aligned} x &= t + 1 \\ y &= 2t + 1 \\ z &= -t + 1 \end{aligned}$$

2. W przestrzeni $\mathbb{R}^4$ lub $\mathbb{C}^4$:

$$\begin{aligned} x_1 &= t+u \\ x_2 &= t-u \\ x_3 &= 2t+u \\ x_4 &= t-3u \end{aligned}$$

3. W przestrzeni $\mathbb{R}^3$ lub w $\mathbb{C}^3$:

$$x_1 = t^2, \quad x_2 = t^3, \quad x_3 = t^6$$

Ćwicz. 23

Ustalmy liczby $n, m \in \mathbb{N}$. Niech $V = \{(t, t^n, t^m) : t \in \mathbb{R}\}$. Pokaż, że V jest rozmaitością algebraiczną oraz wyznacz $I(V)$.

Ćwicz. 24

Załóżmy, że $f \in k[x_1, \ldots, x_n]$ oraz $f \notin \langle x_1, \ldots, x_n \rangle$. Pokaż, że $\langle x_1, \ldots, x_n, f \rangle = k[x_1, \ldots, x_n]$.

Ćwicz. 25

Załóżmy, że $(V_n)_{n\in\mathbb{N}}$ jest nieskończonym ciągiem rozmaitości algebraicznych takich, że $(\forall n \in \mathbb{N})(V_{n+1} \subseteq V_n)$. Pokaż, ze jest $N \in \mathbb{N}$ takie, że $(\forall n > N)(V_n = V_N)$.

Ćwicz. 26

Załóżmy, że

$$\begin{aligned} a+b+c &= 1 \\ a^2+b^2+c^2 &= 2 \\ a^3+b^3+c^3 &= 1 \end{aligned}$$

Jaką wartość ma $a^5 + b^5 + c^5$?

Ćwicz. 27

Jaka jest odległość punktu $P = (2, 1, 1)$ od sfery $S = \{(x, y, z) \in \mathbb{R}^3 : x^2 + y^2 + z^2 = 1\}$?
Wskazówka: Użyj metodę mnożników Lagrange'a. Znajdź bazę Grobnera dla porządku leksykograficznego w którym $\lambda > x > y > z$.

Lab. 9

Narysuj wykresy następujących krzywych algebraicznych oraz wyznacz ich punkty osobliwe

1. $\left(x^2 + y^2 + 4y\right)^2 - 16\left(x^2 + y^2\right) = 0$
2. $2\left(x^2 + 9\right)\left(y^2 - 16\right) + \left(x^2 - 9\right)^2 + \left(y^2 - 16\right)^2 = 0$
3. $350x^2y^2 - 15^2\left(x^2 + y^2\right) + 12^2\left(x^4 + y^4\right) + 81 = 0$

Ćwicz. 28

Pokaż, że każde ciało algebraicznie domknięte jest nieskończone.

Ćwicz. 29

Załóżmy, że k jest nieskończonym ciałem. Niech $f_1, \ldots, f_k$ będą elementami $k[x] \setminus \{0\}$. Pokaż, że jest $a \in k$ takie, że $f_i(a) \neq 0$ dla wszystkich $i = 1, \ldots, k$.

Lab. 10

Parasolka Whitney'a zadana jest równaniami parametrycznymi

$$x = u \cdot v$$
$$y = v$$
$$z = u^2$$

1. Wyznacz bazę Groebnera dla monomialnego porządku leksykograficeźznego gdzie $u > v > x > y > z$ i sprawdź, że trzecim ideałem eliminacyjny I_2 jest

$$\left\langle x^2 - y^2 z \right\rangle \ .$$

2. Pokaż, że w ciele $\mathbb{C}$ każde częściowe rozwiązanie $(a, b, c) \in \mathbb{C}^3$ równania $x^2 - y^2 z = 0$ rozszerza się pełnego rozwiązania w $\mathbb{C}^5$.
3. Co się dzieje w ciele $\mathbb{R}$?
4. Narysuj wykres równania $x^2 - y^2 z = 0$ (w $\mathbb{R}^3$).
5. Wyznacz punkty osobliwe rozmaitości $V(x^2 - y^2 z)$.

Lab. 11

Przeprowadź proces implicityzacji parametrycznego generowania okręgu

$$x(t) = \frac{1 - t^2}{1 + t^2}$$
$$y(t) = \frac{2t}{1 + t^2}$$

oraz wyznacz czym się różni otrzymana rozmaitość algebraiczna (okrąg jednostkowy) od obrazu $\{x(t), y(t)) : t \in \mathbb{R}\}$.

Ćwicz. 30

Załóżmy, że $f, g \in \mathbb{Z}[x]$. Pokaż, że $Res(f, g) \in \mathbb{Z}$.

Ćwicz. 31

Niech $f, g \in k[x]$ będą niezerowymi wielomianami, $k = deg(f)$, $l = deg(g)$.

1. Pokaż, że

$$Res(f, g, x) = (-1)^{k \cdot l} Res(g, f, x) \ .$$

   Zwróć uwagę na przypadek $l = 0$ lub $l = 0$.
2. Załóżmy, że $\kappa \neq 0$ oraz $\lambda \neq 0$. Pokaż, że

$$Res(\kappa f, \lambda g) = \kappa^{deg(g)} \lambda^{\deg(f)} Res(f, g, x) \ .$$

Lab. 12

Conchoida Slusa jest zadana we współrzędnych biegunowych równaniem parametrycznym

$$r = \frac{1}{\cos(t)} + a \cos(t)$$

(a jest parametrem tej krzywej).

1. Korzystając z baz Grobnera wyznacz najmniejszą rozmaitość algebraiczną zawierającą tą krzywą. Otrzmać masz krzywą algebraiczną stopnia trzeciego.
2. Narysuj wykresy tych krzywych dla $a \in \{-4, -2, 0, 1, 2, 3\}$.

Ćwicz. 32

Pracujemy z ciałem $\mathbb{R}$. Pokaż, że dla dowolnej rodziny wielomianów $w_1, \ldots, w_k$ z $k[x_1, \ldots, x_n]$ istnieje wielomian $w \in k[x_1, \ldots, x_n]$ taki, że $V(w_1, \ldots, w_k) = V(w)$.

Ćwicz. 33

1. Wyznacz w ciałach $\mathbb{R}$ oraz $\mathbb{C}$ rozmaitość $V(x, y)$.
2. Czy istnieje wielomian $w(x, y) \in \mathbb{C}[x, y]$ takie, że $V(w) = \{(0, 0)\}$?

Ćwicz. 34

Niech I będzie ideałem w pierścieniu R. Niech

$$\sqrt{I} = \{a \in R : (\exists m \geqslant 1)(a^m \in I)\} \ .$$

Pokaż, że $\sqrt{I}$ jest ideałem.

Ćwicz. 35

Załóżmy, że $G = \{g_1, \ldots, g_k\} \subseteq k[x_1, \ldots, x_n]$ oraz $f \in G$ oraz, że $LM(f)$ i $LM(g)$ są względnie pierwsze. Pokaż, że istnieją wielomiany $A_1, \ldots, A_k$ takie, że

$$S(f, g) = \sum_{i=1}^{k} A_i g_i$$

oraz $multdeg(A_i g_i) \leqslant multdeg(f)$.

Ćwicz. 36

Załóżmy, że $G = \{g_1, \ldots, g_k\} \subseteq k[1_1, \ldots, x_n]$ oraz $f, g \in G$ oraz, że $LM(f)$ i $LM(g)$ są względnie pierwsze. Pokaż, że istnieją wielomiany $A_1, \ldots, A_k$ takie, że

$$S(f, g) = \sum_{i=1}^{k} A_i g_i$$

oraz $multdeg(A_i g_i) \leqslant multdeg(S(f, g))$.

Ćwicz. 37

Pokaż, że z NullStellenSatz wynika słabe NullStellenSatz.

c.d.n.
Powodzenia,
Jacek Cichoń