

Wybrane zagadnienia Algebry

Lista zadań

Jacek Cichoń
WIT, PWR, 2023/24

1 Wstęp

Lab. 1

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

1. Napisz algorytm dzielenia z resztą w pierścieniu liczb Gaussa $\mathbb{Z}[i]$, czyli algorytm, który dla danych $x, y \in \mathbb{Z}[i]$, $y \neq 0$ wyznaczy $q, r \in \mathbb{Z}[i]$ takie, że $x = q \cdot y + r$ oraz $N(r) < N(y)$.
2. Największym wspólnym dzielnikiem liczb $u, v \in \mathbb{Z}[i]$ nazywamy takie $d \in \mathbb{Z}[i]$, że $(d|u) \wedge (d|v)$ oraz

$$(\forall x \in \mathbb{Z}[i])(x|u \wedge x|v \rightarrow x|d) .$$

Oprogramuj algorytm wyznaczania NWD dla $\mathbb{Z}[i]$.

3. Oprogramuj funkcję wyznaczającą $NWW(x, y)$ dla $x, y \in \mathbb{Z}[i]$.
4. Ideał generowany przez liczby a_1, \dots, a_k oznaczamy przez (a_1, \dots, a_k) . Korzystając z poprzednich dwóch podpunktów znajdź takie c i d , że $(3 + 4i, 1 + 3i) = (c)$ oraz $(3 + 4i) \cap (1 + 3i) = (d)$.

Lab. 2

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

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 $NWW(x, y)$ 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 $(1 + x^2) \cap (1 + 2x + x^2) = (d)$.

Ćwic. 1

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

Ćwic. 2

Rozważ prostą przechodzącą przez punkt $(-1, 0)$ o współczynniku kierunkowym $t \in \mathbb{R}$. Znajdź drugi punkt przecięcia tej prostej z hiperbolą $x^2 - y^2 = 1$. Wyraż 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 $f_1, \dots, f_k \in k[x_1, \dots, x_n]$ przez $V(f_1, \dots, f_k)$ oznaczamy zbiór

$$V(f_1, \dots, f_k) = \{(a_1, \dots, a_n) \in k^n : (\forall i \in \{1, \dots, k\})(f_i(a_1, \dots, a_n) = 0)\} .$$

Zbiór ten nazywamy **rozmaitością algebraiczną** generowaną przez wielomiany f_1, \dots, 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 działaniom na wielomianach (np. `PolynomialQuotientRemainder`) oraz generowania krzywych i powierzchni zadawanych równaniami parametrycznymi.

2 Wielomiany i rozmaitości

Ćwic. 3

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

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

Ćwic. 4

Ustalmy ciało k liczbę $n \geq 1$. 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

$$(x_1, \dots, x_k) \leq (y_1, \dots, y_k) \iff \bigwedge_{i=1}^k (x_i \leq y_i)$$

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

Ćwic. 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 $n, m \geq 1$.

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 $\langle X^2, y^2 \rangle$ 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 $n, m \geq 1$.

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. $\text{GCD}(x^4 + x^2 + 1, x^4 - x^2 - 2x - 1, x^3 - 1)$
2. $\text{GCD}(x^3 + x^2 - 4x - 4, x^3 - x^2 - 4x + 4, x^3 - 2x^2 - x + 2)$

Ćwicz. 11

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

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

Lab. 8

Napisz pseudokod procedury, która dla danych wielomianów $f, g \in k[x]$ znajduje takie $A, B \in k[x]$, że $\text{nwd}(f, g) = A \cdot f = B \cdot g$.

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 $f, \dots, f_k \in \mathbb{C}[x]$. Pokaż, że $V(f_1, \dots, f_k) = \emptyset$ wtedy i tylko wtedy, gdy $1 \in \langle f_1, \dots, f_k \rangle$
3. Opisz procedurę rozstrzygającą, czy dla danych wielomianów $f, \dots, f_k \in \mathbb{C}[x]$ rozmaitość $V(f_1, \dots, f_k)$ 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, \dots, 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 $V(f) = \{a_1, \dots, a_k\}$.
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 \sqsubseteq będzie porządkiem jednomianowym na \mathbb{N}^k . Niech

$$\alpha \sqsubseteq \beta \iff (\forall i)(\alpha_i \leq \beta_i) .$$

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

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

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

Ćwicz. 17

Pokaż, że

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

jest jedynym porządkiem monomialnym na \mathbb{N} .

Ćwicz. 18

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

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

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

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

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

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

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

Ćwic. 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 $r_1 - r_2 \in \langle g_1, g_2 \rangle$.

Ćwic. 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 :

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

Ćwic. 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

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

Ćwicz. 25

Założmy, 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, że jest $N \in \mathbb{N}$ takie, że $(\forall n > N)(V_n = V_N)$.

Ćwicz. 26

Założmy, 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 metody mnożników Lagrange'a. Znajdź bazę Grobnera dla porządku leksykograficznego w którym $\lambda > x > y > z$.

Ćwicz. 28

Niech $G = \langle xy + 1, y^2 + 1 \rangle$ oraz $f = xy^2 - x$.

1. Podziel f przez ciąg $(xy + 1, y^2 + 1)$.
2. Pokaż, że $f \rightarrow_G 0$.

c.d.n.
Powodzenia,
Jacek Cichoń