Wybrane Zagadnienia Algebry

Rafał Włodarczyk

INA 6, 2026

Contents

1 Lecture I

1.1 Grupa

Magmą nazywamy parę $(X, +)$, gdzie $+ : X \times X \to X$.

- Magma + łączność = półgrupa
- Półgrupa + el. neutralny 0 = monoid
- Monoid + elementy odwrotne = grupa
- Grupa + przemienność = grupa abelowa

1.2 Pierścień

Pierścieniem nazywamy $R = (X, +, \cdot, 0)$, gdy:

- $(X, +, 0)$ jest grupą abelową
- $(X, \cdot)$ jest półgrupą
- $(\forall a, b, c \in X) \quad a \cdot (b + c) = a \cdot b + a \cdot c$
- $(\forall a, b, c \in X) \quad (a + b) \cdot c = a \cdot c + b \cdot c$

Jeśli $(X, \cdot)$ jest przemienne, to pierścień R nazywamy przemiennym.
Jeśli $1 \in X : (X, \cdot, 1)$ jest monoidem, to R nazywamy pierścieniem z jedynką.

Operacje na pierścieniach $R = (X, +, \cdot, 0)$ - pierścień, $\alpha, \beta \in X$ to:

$$\alpha A + \beta B = \{\alpha \cdot a + \beta \cdot b : a \in A, b \in B\}$$

Przykład $(2\mathbb{Z}, +, \cdot, 0)$ - pierścień przemienny bez 1.
Przykład $(M_{2\times 2}, +, \cdot, 0, 1_2)$ - pierścień macierzy rzeczywistych 2×2 odwracalne - pierścień z jedynką, ale nie przemienny.

1.3 Ciało

Jeśli $(X - \{0\}, \cdot, 1)$ jest grupą abelową to nazywamy to **ciałem**.
Jeśli p-pierwsza to $(\mathbb{Z}_p, +_p, \cdot_p, 0, 1)$ jest ciałem.
Jeśli $R = (X, +, \cdot, 0)$ oraz A niepusty taki, że $A \cap X = \emptyset$. Określamy rozszerzenie R o A:

$$R[A] \text{ - najmniejszy pierścień który zawiera } R \cup A$$

Jeśli $|A| = n \in \mathbb{N}$ to dla $A = \{a_1, a_2, \ldots, a_n\}$:

$$R[A] = R[a_1, a_2, \ldots, a_n]$$

Pierścień Gaussa $(\mathbb{Z}[i], +, \cdot, 0, 1)$, $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$
Liczby Dualne $\mathbb{R}[\varepsilon] = (D, +, \cdot, 0, 1)$, $D = \{a + b\varepsilon : a, b \in \mathbb{R}\}, \varepsilon \notin \mathbb{R}, \varepsilon^2 = 0$
Liczby Podwójne $(P, +, \cdot, 0, 1), P = \{a + bj : a, b \in \mathbb{R}\}, j \notin \mathbb{R}, j^2 = 1$

Liczby Zespolone $\mathbf{C} = \mathbf{R}[i] = (\mathbf{C}, +, \cdot, 0, 1)$
Pierścień wielomianów o zm. x : $x \notin K$, $K[x] = \{\sum_{i=0}^{n} a_i x^i : n \in \mathbb{N}\,(\forall i = 0, 1 \ldots n)\,, a_i \in K\}$
Pierścień wielomianów w zm. zm. x, y $K[x, y] = \{\sum_{i=0}^{n} \sum_{j=0}^{m} a_{ij} x^i y^j : a_{ij} \in K\}$

Def. $R = (X, +, \cdot)$ - pierścień. $A \subseteq X$. Określamy ideał:

$$\langle A \rangle = \{\sum_{i=1}^{n \in \mathbb{N}} r_i \cdot a_i : r_i \in X, a_i \in A\}$$

A - może być nieskończony. Jeśli $A = \{a_1, \ldots a_k\}$ to $\langle A \rangle = \{\sum_{i=1}^{k} r_i \cdot a_i : r_i \in X\}$
$\langle 2 \rangle$ w $\mathbb{Z}$: $\langle 2 \rangle = 2\mathbb{Z}$
$\langle x - 1 \rangle$ w $\mathbb{R}[x]$: $\langle x - 1 \rangle = \{(x - 1)w(x) : w(x) \in \mathbb{R}[x]\}$
$R = (X, +, \cdot, 0)$ - pierścień. $d|a \equiv (\exists b \in X)\, d \cdot b = a$
$d \in \mathrm{NWD}(a, b) \equiv (d|a \wedge d|b) \wedge (\forall x)\,((x|a \wedge x|b) \implies x|d)$
$d \in \mathrm{NWW}(a, b)$ ćwiczenia
$a, b \in \mathbb{Z}[i] \langle a, b \rangle = \langle c \rangle \equiv c \in \mathrm{NWD}(a, b)$
$\langle a \rangle \cap \langle b \rangle = \langle c \rangle \equiv c \in \mathrm{NWW}(a, b)$

1.4 Ideał

$R = (X, +, \cdot, 0)$ - pierścień przemienny. $\emptyset \neq I \subseteq X$. I nazywamy ideałem w R, gdy:

1. $(\forall a, b \in I)\ a - b \in I$
2. $(\forall r \in X)\,(\forall a \in I)\, r \cdot a \in I$

$I = \{0\}$ - ideał trywialny, $I = X$ - ideał niewłaściwy.
$\langle A \rangle$ - najmniejszy ideał w R zawierający A.

1.5 Relacja Równoważności

Niech R - pierścień, a $I \in \mathrm{ID}(R)$, $a, b \in R$

$$a \equiv b \iff (a - b) \in I$$

Gdzie $\equiv$ jest relacją równoważności.

1.6 Pierścień Ilorazowy

$R/_{\equiv}$ nazywamy pierścieniem ilorazowym z działaniami i el neutralnym określonymi naturalnie.

1.7 Dziedzina Całkowitości

Pierścień R to dziedzina całkowitości gdy $(\forall u, v \in R)\, u \cdot v = 0 \implies (u = 0 \vee v = 0)$
$\mathbb{Z}_7[x] \implies w(x) = x^7 - x$ (MTF) $(\forall x \in \mathbb{Z}_7)\, w(x) = 0$

1.8 Dziedzina Euklidesowa

Nazywamy dziedzinę całkowitości $(X, +, \cdot, 0)$, że $\exists N : X \to \mathbb{N}$, $N(0) = 0$, takie, że

1. $(\forall a, b \in X)\,(b \neq 0) \implies [(\exists q, r \in X)a = q \cdot b + r \wedge (r = 0 \vee N(r) < N(b))]$
2. $(\forall a, b \in X)\,(b \neq 0) \implies N(a) \leqslant N(a \cdot b)$

Uwaga. Jeśli istnieje n które spełnia 1 to istnieje $\tilde{N}$, które spełnia 1,2.
Uwaga. N, N które spełnia 1, 2 nazywamy normą dziedziny euklidesowej $R \in$ EUCL

Przykład: w $\mathbb{Z}$: $N(k) = |k|$
Przykład: w $\mathbb{Z}[i] : N(a + bi) = a^2 + b^2$

2 Wykład II

by Michał Waluś

Fakt:

$$\mathbb{C} \backsimeq \left\{ \begin{bmatrix} a & -b \\ b & a \end{bmatrix} : a, b \in \mathbb{R} \right\}$$

Przykład: $< a + bi >$ w $\mathbb{Z}[i]$

$$< a + bi >= \{(a + bi)(x + yi) : x, y \in \mathbb{Z}\} = \left\{ (a + bi)\sqrt{N(x + y)} \cdot O_\varphi : x, y \in \mathbb{Z} \right\}$$

gdzie O_φ to obrót o jakiś kąt φ, $\tan\varphi = \frac{y}{x}$.

2.1 Wielomiany

Przykład. $K[x]$, K - ciało. $f \in K[x] \implies N(f) = deg(f)$.

Jak sprawdzić kiedy $f \in K[x]$ spełnia $f \equiv 0$?

Fakt: $f \equiv 0 \iff (\exists A \in K)(|A| > deg(f) \wedge (\forall x \in A)f(x) = 0)$

Def. Jeśli $f \in K[x]$, $f = \sum_{i=0}^{n} a_i x^i$, $a_n \neq 0$, to określamy wiodący jednomian $LT(f) = a_n x^n$. $(LT(0) = 0)$

2.2 Ideały

Def. Dziedzinę całkowitości $\mathcal{R}$ nazywamy dziedziną ideałów głównym (*PID - Perfect Ideal Domain*), jeśli

$$(\forall \mathcal{I} \in ID(\mathcal{R}))(\exists a)\mathcal{I} =< a >$$

Fakt: W dziedzinach euklidesowych $< a, b >=< c >\equiv c \in NWD(a, b)$

Fakt: $d|a \iff < a > \subseteq < d >$
Wniosek: $(d|a \wedge d|b) \iff < a, b > \subseteq < d >$

Fakt: w $\mathcal{R} \in EUCL$, dla $b \neq 0$, $a = b \cdot q + r$ mamy $< a, b > = < b, r >$

2.3 Algorytm Euklidesa

Tw. (Euklides) Jeśli $NWD(n, m) = d$, to

$$(\exists a, b \in \mathbb{Z}) d = an + bm \text{ } \textit{(tożsamość Bézouta)}$$

$< a, b > = < d > \equiv d = X \cdot b + Y \cdot r \equiv d = X \cdot b + Y \cdot (a - b \cdot q) = a \cdot Y + b(X - q \cdot Y)$

Roszerzony algorytm Euklidesa:

```
EXT_NWD(a, b) {
    if (b = 0) { return (a, 1, 0)}
    else {
        (q, r) = div(a b)
        (d, X, Y) = EXT_NWD(b, r)
        return (d, Y, b * (X - q * Y)
    }
}
div(f, q) {
    q = 0, p = f
    while (p != 0 && LT(g) | LT(f)) {
        q += LT(f)/LT(g)
        p -= g * (LT(f) / LT(g))
    }
    return (q, p)
}
```

2.4 Częściowy porządek

Def. w $\mathbb{N}^k$

$$(x_1, \ldots, x_k) \leqslant (y_1, \ldots, y_k) \equiv \bigwedge_{i=1}^{k} x_i \leqslant y_i$$

Lemat Dicksona
Niech $\overline{x_n} = (x_1^{(n)}, \ldots, x_k^{(n)}) \in \mathbb{N}^k$. Wtedy istnieje podciąg $i_1, i_2, \ldots$ taki, że $(\overline{x_{i_j}})_{j \in \mathbb{N}}$ jest niemalejący.

D-d
$A_n = \overline{x}[\mathbb{N}]$.

1. Jeśli $|A_0| < \aleph_0$, to istnieje $\overline{z} \in \mathbb{N}^k$, taki że $|\overline{x}^{-1}[\overline{z}]| = \aleph_0$. Wystarczy wziąć podciąg składający się z samych $\overline{z}$.

2. Indukcja ze względu na k.

   (a) ($k = 1$) Kładziemy $\overline{x_{i_1}} = \min A_0$, $i_1 \in \{n \in \mathbb{N} : x_n = \min A_0\}$. $A_1 = A_0 \backslash \{\overline{x_{i_1}}\}$. Dalej $\overline{x_{i_2}} = \min A_1$, $A_j = A_j \backslash \{\overline{x_{i_j}}\}$.
   Oczywiście $(\overline{x_n})_{n\in\mathbb{N}}$ ma podciąg niemalejący.

   (b) ($k \implies k+1$) $\overline{x_k} = (x_1^{(n)}, \dots, x_k^{(n)})$. Ciąg $(x_{k+1}^{(n)})_n$ ma podciąg niemalejący $(x_k^{(n_j)})_j$.
   Z założenia indukcyjnego $y_j = (x_1^{(i_j)}, \dots, x_k^{(i_j)})$, istnieje $(y_{j_l})_l$ - niemalejący w $\mathbb{N}^k$.
   Zatem $(x_1^{(i_{j_l})}, \dots)$ jest niemalejący.

3 Wykład III

again by Rafał Włodarczyk

3.1 Multiindeksy

Multiindeksem nazywamy $\alpha = (\alpha_1, \alpha_2, \dots, \alpha_n) \in \mathbf{N}^n$.
Długość multiindeksu α to $|\alpha| = \sum_{i=1}^n \alpha_i$.

$$\alpha + \beta = (\alpha_1 + \beta_1, \alpha_2 + \beta_2, \dots, \alpha_n + \beta_n)$$
$$\alpha \leqslant \beta \iff \wedge_{i=1}^n \alpha_i \leqslant \beta_i$$
$$\alpha! = \prod_{i=1}^n (\alpha_i)!$$

Gdy $k = |\alpha|$, to określamy $\binom{k}{\alpha} = \frac{k!}{\alpha!}$. Rozważamy $K[x_1, x_2, \dots, x_n]$, ozn. $x = (x_1, x_2, \dots, x_n)$:

$$x^\alpha = \prod_{i=1}^n x_i^{\alpha_i}$$

P. x^3yz^2 - $\bar{x} = (x, y, z)$, $\bar{x}^{(3,1,2)} = x^3yz^2$
$\alpha = (3, 1, 2) \quad |\alpha| = 3 + 1 + 2 = 6, \beta = (1, 1, 0) \quad \beta \leqslant \alpha$

3.2 Współczynniki multimianowe

Twierdzenie o współczynnikach multimianowych.

$$\left(\sum_{i=0}^n x_i\right)^k = \sum_{|\alpha|=k} \binom{k}{\alpha} x^\alpha$$

P. $(x+y+z)^3 = \binom{3}{(3,0,0)}x^3y^0z^0+\binom{3}{(2,1,0)}x^2yz^0+\binom{3}{(2,0,1)}x^2y^0z+\binom{3}{(1,2,0)}xy^2z^0+\binom{3}{(1,1,1)}xyz+\binom{3}{(1,0,2)}xy^0z^2+\binom{3}{(0,3,0)}x^0y^3z^0+\binom{3}{(0,2,1)}x^0y^2z+\binom{3}{(0,1,2)}x^0yz^2+\binom{3}{(0,0,3)}x^0y^0z^3 = x^3+y^3+z^3+\cdots+6xyz$
Def. Stopień całkowity jednomianu ax^α w $K[x_1,x_2,\ldots,x_n]$, gdzie $a\in K$, $x=(x_1,x_2,\ldots,x_n)$, $\alpha=(\alpha_1,\alpha_2,\ldots,\alpha_n)$ określamy jako $|\alpha|$ i piszemy $\mathrm{tdeg}(ax^\alpha)=|\alpha|$.
Dla wielomianu $f(x)=\sum_{\alpha\in A_f}a_\alpha\cdot x^\alpha$, gdzie $A_f=\{\alpha\in\mathbb{N}^n : a_\alpha\neq 0\}$. Określamy $\mathrm{tdeg}(f)=\max_\alpha\{|\alpha|\}$.
P. $f(x,y,z)=x^3z+3y^2z^3+y+2\to A_f=\{(3,0,1),(0,2,3),(0,1,0),(0,0,0)\}, a_{(0,2,3)}=3, \mathrm{tdeg}(f)=5$
Fakt $\mathrm{tdeg}(f\cdot g)=\mathrm{tdeg}(f)+\mathrm{tdeg}(g),\quad f,g\in K[\bar{x}]-\{0\}$ P. $K[x,y]$, $\langle x,y\rangle=\{a(x,y)\cdot x+b(x,y)\cdot y : a,b\in K[x,y]\}=$
$=\{f\in K[x,y] : f(0,0)=0\}$. $\langle x,y\rangle$ - nie jest ideałem głównym $\langle f\rangle=\langle x,y\rangle$ wtedy $x=af$, $\mathrm{tdeg}(x)=1=\mathrm{tdeg}(a)+\mathrm{tdeg}(f)$.
Jeśli $\mathrm{tdeg}(a)=1$ to $f=$ const., czy $c\in\langle x,y\rangle$ - tylko jeśli $c=0$, a to nie może wygenerować nam przestrzeni.
Jeśli $\mathrm{tdeg}(f)=1$ to $\mathrm{tdeg}(a)=0$, $f=c'x$ - nie da się wygenerować $y=a'f$.
Fakt Jeśli $d=\deg(f)$, dla $f\in K[x]$ oraz $(\exists A)\,|A|>d\wedge(\forall a\in A)\,f(a)=0, tof\equiv 0$.
Tw. Niech $d=\mathrm{tdeg}(f)$, $f\in K[x_1,\ldots,x_n]$ oraz $(\exists A\subseteq K)\,|A|>d\wedge(\forall\bar{a}\in A^n)\,f(\bar{a})=0$, to $f\equiv 0$
P. $f(x,y)=x^2+y^2-1, \mathrm{tdeg}(f)=2, K=\mathbb{R}$
D-d. $n=1$ KO Zał, że $f ß K[x_1,\ldots,x_n,x_{n+1}]$

$$f=\sum_{i=0}^{k}g_i(x_1,\ldots,x_n)\cdot x_{n+1}$$
$$f(a_1,a_2,\ldots,a_n,x_{n+1})=\sum_{i=0}^{k}g_i(a_1,\ldots,a_k)\cdot x_{n+1}$$
$$a_i\in A, |A|>\mathrm{tdeg}(f)\to |A|>\mathrm{tdeg}(g_i)$$
$$\text{Przypuśćmy, że} g_i(a_1,\ldots,a_n)\equiv 0 \text{ dla wszystkich } i=0,1,\ldots k$$
$$\text{Wtedy} f(\bar{(}a),x_{n+1})=0$$

P. $f(x,y)=x^2+y^2+2xy$, $\varepsilon(x,y)=(x+y)^2$ Czy $f-g\equiv 0$. Wystarczy sprawdzić w 9 punktach czy zgadza się wynik. **Rozmaitość Algebraiczna.** Niech $F\subseteq K[x_1,\ldots,x_n]$. Rozmaitość V nazywamy:

$$V(F)=\{\bar{a}\in K^n : (\forall f\in F)f(\bar{a})=0\}$$

P. $V(\{x^2+y^2-2, x^2-y^2\})=\{(-1,-1),(1,-1),(-1,1),(1,1)\}$
P. $F,G\subseteq K[x_1,\ldots,x_n]$.
P. $V(F\cup G)=V(F)\cap V(G)$.
P. $V(F)\cup V(G)=V(\{f\cdot g : f\in F, g\in G\})$
P. $V(F)=V(\langle F\rangle)$
P. $V(\{x^2+y^2-2, x^2-y\})=V(\langle x^2+y^2-2, x^2-y\rangle)=V(\langle 2x^2-2, x^2-y^2\rangle)=V(\langle x^2-1, x^2-y^2\rangle)=V(\langle x^2-1\rangle)\cap V(\langle x^2-y^2\rangle)=[V(\langle x-1\rangle)\cup V(\langle x+2\rangle)]\cap[V(\langle x-y\rangle)\cup V(\langle x+y\rangle)]$

4 Wykład IV

Rozmaitością algebraiczną rodziny $\mathcal{F}\subseteq\mathcal{K}[x_1,\ldots,x_n]$ to zbiór:

$$V(\mathcal{F}) = \{(a_1, a_2, \ldots, a_n) \in \mathcal{K}^n : (\forall f \in \mathcal{F})\, f(\bar{a}) = 0\} \tag{4.0.1}$$

P. $V(\{0\}) = \mathcal{K}^n$
P. $V(F) \cup V(G) = V(\{fg : f \in F, g \in G\})$
P. $V(F) \cap V(G) = V(F \cup G)$
P. $V(x^2 + y^2 - 1)$

$$x(t) = \frac{1-t^2}{1+t^2} \wedge y(t) = \frac{2t}{1+t^2}$$
$$x(1+t^2) + t^2 - 1 = 0 \wedge y(1+t^2) - 2t = 0$$

P. $V(x(1+t^2) + t^2 - 1, y(1+t^2) - 2t)$
P. $V(x^2 - y^2 - 9, (u-x)^2 + (v-y)^2 - 1)$ - Równanie ramienia robota, gdzie pierwszy segment ma długość 3, a następny 1. Ale super!! Ruch kamery przymocowanej do drona itd.

Definition. Ideał Generowany. Niech $A \subseteq \mathcal{K}^n$. Wtedy:

$$I(A) = \{f \in K[x_1, \ldots, x_k] : (\forall \bar{a} in A)\, f(\bar{a}) = 0\}$$

Fakt. $I(A)$ - ideał Fakt. $I \subseteq I(V(I))$ - rozmaitość na ideale to ideał.

Przykład $V(\langle x^2, y^2\rangle) = \{(0,0)\}$, $I(V(\langle x^2, y^2\rangle)) = \{\alpha(x,y)x + \beta(x,y)y : a, b \in K[x,y]\} = \langle x, y\rangle$

Def. Dobry porządek $\leqslant$ na $\mathbb{N}^n$ (obcinamy do długości n) nazywamy porządkiem jednomianowym (Monomial Order), jeśli $(\forall \alpha, \beta, \gamma \in \mathbb{N}^n)\, \alpha < \beta \to \alpha + \gamma < \beta + \gamma$, gdzie $a < b \iff (a \leqslant b \wedge a \neq b)$. P $\leqslant_{\text{lex}}$ na $\mathbb{N}^n$ jest MO.

Def. Przy pomocy porządku MO można wprowadzić dobry porządek na jednomianach $\mathbb{K}[x_1, \ldots, x_n]$ następująco:

$$\bar{x}^\alpha \leqslant \bar{x}^\beta \iff \alpha \leqslant \beta$$

P. Dla $\leqslant_{\text{lex}}$ na $\mathbb{N}^2$, $y < x$

$$1 < y < y^2 < \cdots < x < xy < xy^2 < \cdots < x^2 < x^2 y < \ldots$$

Def **Graded Lex.** na $\mathbb{N}^n$

$$\alpha \leqslant_{\text{GL}} \beta \to (|\alpha| < |\beta| \vee (|\alpha| = |\beta|^\alpha \leqslant_{\text{lext}} \beta))$$

Polynomial Quotient Reduce $f_1, g_1, g_2, \ldots, g_n \in \mathcal{K}[x_1, \ldots, x_n]$
PQR$(f, \{g_1, \ldots, g_k\})$ $f(\bar{(x)}) = \sum_{i=1}^k g_i(\bar{x}) \cdot q_i(\bar{x}) + r(\bar{x})$
P PQR$(1, \{x^2, x^2+1\}) = ((0,0), 1)$
P PQR$(1, \{x^2, x^2+1\}) = ((-1, 1, 0))$