Algebraiczna teoria liczb

Karol Janowicz

February 2020

1 Pierścienie całkowite. Dziedziny Dedekinda

Jednym z najważniejszych obiektów naszych badań będą skończone rozszerzenia ciała liczb wymiernych $\mathbb{Q} \subset K$. Nazywać je będziemy **ciałami algebraicznymi**.

Definicja 1.1. *Niech $\mathbb{Q} \subset K$ będzie skończonym rozszerzeniem ciała liczb wymiernych.* ***Pierścieniem całkowitym*** *ciała algebraicznego K nazywamy zbiór:*

$$O_K := \{x \in K \mid x \text{ jest pierwiastkiem unormowanego wielomianu nad } \mathbb{Z}\}$$

Jak można się domyśleć, zbiór O_K z działaniami dodawania i mnożenia jak w K, jest istotnie pierścieniem. Nie jest to jednak zupełnie trywialne; naszym celem jest udowodnienie ogólniejszego faktu.

Definicja 1.2. *Niech $A \subset B$ będzie rozszerzeniem pierścieni. Powiemy, że element $x \in B$ jest* ***całkowity nad A****, wtedy i tylko wtedy, gdy jest on pierwiastkiem unormowanego wielomianu nad A. Pierścień B nazywa się* ***całkowity nad A****, jeśli każdy element $x \in B$ jest całkowity nad A.*

Przypomnijmy teraz podstawowe twierdzenie algebry liniowej, które posłuży nam do scharakteryzowania elementów całkowitych.

Twierdzenie 1.3. *Niech $A = (a_{ij})$ będzie macierzą kwadratową o n wierszach i o współczynnikach w pierścieniu R. Niech A^* oznacza macierz dołączoną do A, to znaczy $A^* = \left((-1)^{i+j} A_{ij}\right)^T$, gdzie A_{ij} jest wyznacznikiem macierzy powstałej z macierzy A przez usunięcie i-tego wiersza i j-tej kolumny. Wówczas $A^*A = \det A \cdot \mathrm{Id}$. W szczególności*

$$Av = 0 \implies \det A \cdot v = 0$$

dla $v \in R^n$.

Dowód powyższego twierdzenia polega na banalnym rachunku, dlatego go pozostawiamy. Udowodnimy wreszcie kluczowe twierdzenie.

Twierdzenie 1.4. *Niech $A \subset B$ będzie rozszerzeniem pierścieni. Elementy $b_1, b_2, \ldots, b_n \in B$ są całkowite nad A wtedy i tylko wtedy, gdy pierścień $A[b_1, \ldots, b_n]$ jest skończenie generowanym A-modułem.*

Dowód. Dowodzimy twierdzenia przez indukcję po n. Załóżmy, że $b \in B$ jest całkowity nad A. Wówczas $b^n = a_{n-1}b^{n-1} + \ldots + a_0$, gdzie $a_i \in A$, a więc A-moduł $A[b]$ jest istotnie skończenie generowany. Załóżmy, że teza jest prawdziwa dla $n-1 \in \mathbb{N}$ i niech $b_1, \ldots, b_n \in B$ będą całkowite nad A. Wówczas A-moduł $A[b_1, \ldots, b_{n-1}]$ jest skończenie generowany z założenia indukcyjnego. Wówczas oczywiście $A[b_1, \ldots, b_{n-1}][b_n]$ jest także skończenie generowany nad A, tj. $A[b_1, \ldots, b_n]$ jest skończenie generowany, co kończy dowód implikacji w jedną stronę. Załóżmy zaś, że moduł $A[b_1, \ldots, b_n]$ jest skończenie generowany i niech $\omega_1 \ldots, \omega_k$ będą jego generatorami. Wtedy dla każdego $b \in A[b_1, \ldots, b_n]$ mamy

$$b\omega_i = \sum_{i=1}^{k} c_{ij}\omega_j$$

dla $i = 1, \ldots, k$ i $c_{ij} \in A$. Innymi słowy mamy, że $(b\,\mathrm{Id} - C)[\omega_i] = 0$ gdzie $C = (c_{ij})$. Co więcej $1 = a_1\omega_1 + \ldots a_k\omega_k$, więc z twierdzenia 2.3 wynika, że $\det(b\,\mathrm{Id} - C) = 0$. To kończy dowód, bowiem b było wybrane dowolnie z $A[b_1, \ldots, b_n]$. ■

Uwaga 1.5. *Nietrudno wykazać, że element $x \in B$ jest całkowity nad A wtedy i tylko wtedy, gdy istnieje niezerowy, skończenie generowany A-moduł M o tej własności, że $xM \subset M$. Jeśli x jest całkowity, kładziemy $M := A[x]$. W drugą stronę postępujemy podobnie jak wyżej.*

Wniosek 1.6. *Niech $A \subset B$ będzie rozszerzeniem pierścieni, zaś elementy $b_1, b_2 \in B$ będą całkowite nad A. Wówczas elementy $b_1 + b_2$ i $b_1 b_2$ są całkowite nad A. Zatem, zbiór elementów całkowitych nad A stanowi podpierścień zawarty między A i B i nazywamy go* ***całkowitym domknięciem pierścienia A w B****; oznaczamy go przez $\bar{A}$.*

Z twierdzenia 2.2 wynika ponadto, że jeśli mamy pierścienie $A \subset B \subset C$, przy czym B jest całkowity nad A, zaś C jest całkowity nad B, to wówczas C jest całkowity nad A. Jeśli bowiem $c \in C$ jest taki, że $c^n = b_{n-1}c^{n-1} + \ldots + b_1 c + b_0$, gdzie $b_i \in B$, to przyjmując $R := A[b_1, \ldots, b_{n-1}]$, wiemy że $R[c]$ jest skończenie generowanym R-modułem. Ponadto, R jest skończenie generowanym A-modułem, toteż $R[c]$ jest także skończenie generowanym A-modułem. To oczywiście oznacza, że c jest całkowity nad A.

Niech dana będzie dziedzina A. Powiemy, że jest ona **całkowicie domknięta** wtedy i tylko wtedy, gdy jej domknięcie w ciele ułamków K jest równe A. **Normalizacją** dziedziny A nazywamy jej domknięcie w ciele ułamków. Jest niemal natychmiastowym następujący fakt:

Twierdzenie 1.7. *Każda dziedzina z jednoznacznym rozkładem jest całkowicie domknięta.*

Przypuśćmy teraz, że mamy całkowicie domkniętą dziedzinę A z ciałem ułamków K. Niech dane będzie ponadto skończone rozszerzenie ciał $K \subset L$ oraz niech B oznacza całkowite domknięcie A w L. Zobaczmy, że każdy element $\beta \in L$ jest postaci:

$$\beta = \frac{b}{a}$$

gdzie $b \in B$ i $a \in A$. Rzeczywiście, niechaj β będzie pierwiastkiem wielomianu

$$f(X) = a_n X^n + \ldots + a_1 X + a_0$$

gdzie $a_i \in A$. Wtedy element $a_n\beta \in L$ jest całkowity nad A, toteż $a_n\beta \in B$. Co więcej, element $\beta \in L$ jest całkowity nad A wtedy i tylko wtedy, gdy wielomian minimalny $p_\beta \in K[X]$ ma współczynniki w A. Istotnie, niech β będzie pierwiastkiem wielomianu unormowanego $g \in A[X]$ (a więc

β jest całkowity nad A). Wówczas wielomian minimalny $p_\beta \in K[X]$ dzieli wielomian g, toteż zera wielomianu p_β są zerami unormowanego wielomianu g nad A, a więc są całkowite nad A. Ponieważ A jest całkowicie domknięta, musi być $p_\beta \in A[X]$. Odnotujmy ten przyjemny i ważny fakt.

Twierdzenie 1.8. *Niech A będzie całkowicie domkniętą dziedziną, zaś K - jej ciałem ułamków. Niech też $K \subset L$ będzie skończonym rozszerzeniem i niech $\beta \in L$ będzie całkowity nad A. Wówczas wielomian minimalny elementu β ma współczynniki w pierścieniu A.*

Przypomnijmy w tym miejscu dwa bardzo ważne pojęcia związane ze skończonym rozszerzeniem ciał $K \subset L$.

Definicja 1.9. *Niech $K \subset L$ będzie skończonym rozszerzeniem ciał. Dla elementu $\alpha \in L$ definiujemy K-liniowy endomorfizm $\varphi_\alpha : L \longrightarrow L$ zadany wzorem*

$$\varphi_\alpha(x) := \alpha \cdot x$$

*Wielomian charakterystyczny endomorfizmu φ_α oznaczać będziemy przez $f_\alpha(t) := \det(t\,\mathrm{Id} - \varphi_\alpha)$. **Śladem** elementu $\alpha \in L$ nazywamy $T_{L|K}(\alpha) := \operatorname{Tr} \varphi_\alpha \in K$, zaś **normą** – liczbę $N_{L|K}(\alpha) := \det \varphi_\alpha$.*

Natychmiast odnotujmy, że jeśli mamy całkowicie domkniętą dziedzinę A z ciałem ułamków K oraz dane jest skończone, rozdzielcze rozszerzenie $K \subset L$, to norma i ślad elementu $\alpha \in L$ całkowitego nad A jest elementem pierścienia A. Wynika to z lematu znanego z teorii Galois.

Lemat 1.10. *Niech $K \subset L$ będzie skończonym rozszerzeniem rozdzielczym. Wówczas, dla $\alpha \in L$ mamy*

1. $f_\alpha(t) = \prod_\sigma (t - \sigma\alpha)$,
2. $N_{L|K}(\alpha) = \prod_\sigma \sigma\alpha$,
3. $T_{L|K}(\alpha) = \sum_\sigma \sigma\alpha$

gdzie $\sigma : L \longrightarrow \overline{K}$ przebiega K-zanurzenia ciała L w ustalone algebraiczne domknięcie $\overline{K}$.

Dowód. Jest jasne, że wielomian charakterystyczny f_α jest potęgą wielomianu minimalnego elementu $\alpha \in L$: $f_\alpha(t) = p_\alpha(t)^d$. gdzie $d := |L : K(\alpha)|$. Wynika to z faktu, że endomorfizm φ_α ma w odpowiedniej bazie postać klatkowo-diagonalną, z taką samą macierzą cykliczną na przekątnej:

$$\begin{bmatrix} 0 & 0 & \dots & -c_0 \\ 1 & 0 & \dots & -c_1 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & -c_{m-1} \end{bmatrix}$$

gdzie $p_\alpha(t) = t^m + c_{m-1}t^{m-1} + \ldots + c_1 t + c_0$, $m = |K(\alpha) : K|$.

Mamy m parami różnych K-zanurzeń ciała $K(\alpha)$ w $\overline{K}$, z których każde może zostać przedłużone do zanurzenia $L \longrightarrow \overline{K}$ na d istotnie różnych sposobów. Wystarczy napisać, że $L = K(\alpha)(\beta)$ dla

pewnego $\beta \in L$, $|K(\alpha)(\beta) : K(\alpha)| = d$. Możemy więc podzielić zbiór homomorfizmów $L \longrightarrow \overline{K}$ nad K przez relację

$$\sigma \equiv \tau \iff \sigma\alpha = \tau\alpha$$

Niech $\sigma_1, \ldots, \sigma_m$ będą reprezentantami klas abstrakcji tej relacji. Jest jasne, że $p_\alpha(t) = \prod_{i=1}^{m}(t - \sigma_i\alpha)$, toteż

$$f_\alpha(t) = p_\alpha(t)^d = \prod_{i=1}^{m}(t - \sigma_i\alpha)^d = \prod_{i=1}^{m}\prod_{\sigma\equiv\sigma_i}(t - \sigma\alpha) = \prod_{\sigma}(t - \sigma\alpha)$$

Z tego dalej już łatwo wynika 2. i 3. ■

Zatem istotnie, jeśli tylko $\alpha \in L$ jest całkowity nad A (to znaczy α należy do domknięcia A w L), to dla każdego K-zanurzenia $\sigma : L \longrightarrow \overline{K}$ element $\sigma\alpha$ jest całkowity nad A, czyli $f_\alpha \in A[X]$. W konsekwencji $N_{L|K}(\alpha)$, $T_{L|K}(\alpha) \in A$. Można też powiedzieć, że wielomian minimalny elementu całkowitego $\alpha \in L$ ma współczynniki w A, toteż wielomian charakterystyczny f_α będący potęgą wielomianu minimalnego należy do pierścienia $A[X]$. Mamy natychmiast wniosek

Wniosek 1.11. *Niech $K \subset L \subset M$ będą skończonymi rozszerzeniami oraz niech $K \subset M$ będzie rozdzielcze. Wówczas*

$$T_{L|K} \circ T_{M|L} = T_{M|K}$$
$$N_{L|K} \circ N_{M|L} = N_{M|K}$$

Dowód. Tak jak w dowodzie lematu, dzielimy zbiór homomorfizmów $M \longrightarrow \overline{K}$ przez relację:

$$\sigma \equiv \tau \iff \sigma|_L = \tau|_L$$

Ta relacja ma $m = |L : K|$ klas abstrakcji; niech $\sigma_1, \ldots, \sigma_m$ będą ich reprezentantami, to znaczy

$$Hom(L, \overline{K}) = \{\sigma_1|_L, \ldots, \sigma_m|_L\}$$

Liczymy

$$T_{M|K}(\alpha) = \sum_{i=1}^{m}\sum_{\sigma\equiv\sigma_i}\sigma\alpha = \sum_{i=1}^{m}T_{\sigma_i M|\sigma_i L}(\sigma_i\alpha) = \sum_{i=1}^{m}\sigma_i T_{M|L}(\alpha) = T_{L|K}(T_{M|L}(\alpha))$$

dla dowolnego $\alpha \in M$. Analogicznie dla normy. ■

Powyższy rezultat jest prawdziwy w przypadku ogólnym, dla dowolnych skończonych rozszerzeń $K \subset L \subset M$. Nie będzie nam on jednak potrzebny. Wprowadzimy teraz niezwykle ważną definicję.

Definicja 1.12. *Niech $K \subset L$ będzie skończonym rozszerzeniem rozdzielczym z bazą $\{\alpha_1, \ldots, \alpha_n\}$.* ***Wyróżnikiem bazy*** *$\{\alpha_i \mid i = 1, \ldots, n\}$ nazywamy liczbę*

$$d(\alpha_1, \ldots, \alpha_n) = \det\left((\sigma_i\alpha_j)\right)^2$$

gdzie σ_i są parami różnymi zanurzeniami $L \longrightarrow \overline{K}$ w ustalone algebraiczne domknięcie ciała K.

Zauważmy, że $T_{L|K}(\alpha_i\alpha_j) = \sum_k (\sigma_k\alpha_i)(\sigma_k\alpha_j)$. Wynika stąd, że macierz $(T_{L|K}(\alpha_i\alpha_j))$ jest iloczynem macierzy $(\sigma_k\alpha_i)^T(\sigma_k\alpha_j)$. Wynika stąd, że

$$d(\alpha_1, \ldots, \alpha_n) = \det\left(T_{L|K}(\alpha_i\alpha_j)\right)$$

Jeśli ciało L ma bazę potęgową $\{1, \vartheta, \ldots, \vartheta^{n-1}\}$, to można łatwo policzyć, że

$$d(1, \vartheta, \ldots, \vartheta^{n-1}) = \prod_{i<j}(\vartheta_j - \vartheta_i)^2$$

gdzie $\vartheta_i := \sigma_i\vartheta$. Istotnie, mamy bowiem

$$d(1, \ldots, \vartheta^{n-1}) = \det\begin{bmatrix} 1 & \vartheta_1 & \ldots & \vartheta_1^{n-1} \\ 1 & \vartheta_2 & \ldots & \vartheta_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \vartheta_n & \ldots & \vartheta_n^{n-1} \end{bmatrix}^2$$

a to jest macierz Vandermonde'a. Warto to w tym miejscu odnotować, gdyż każde skończone, rozdzielcze rozszerzenie $K \subset L$ ma bazę potęgową. Udowodnimy obecnie kluczowe

Twierdzenie 1.13. *Jeśli rozszerzenie $K \subset L$ jest skończone, rozdzielcze z bazą $\{\alpha_1, \ldots, \alpha_n\}$, to*

$$d(\alpha_1, \ldots, \alpha_n) \neq 0$$

Co więcej, funkcja

$$(x, y) := T_{L|K}(xy)$$

jest niezdegenerowaną formą dwuliniową na K-liniowej przestrzeni L.

Dowód. Wykażemy, że forma $(x, y) = T_{L|K}(xy)$ jest niezdegenerowana. Niech $L = K(\vartheta)$. Wówczas L ma bazę potęgową $\{1, \vartheta, \ldots, \vartheta^{n-1}\}$ oraz

$$d(1, \vartheta, \ldots, \vartheta^{n-1}) = \det\begin{bmatrix} 1 & \vartheta_1 & \ldots & \vartheta_1^{n-1} \\ 1 & \vartheta_2 & \ldots & \vartheta_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & \vartheta_n & \ldots & \vartheta_n^{n-1} \end{bmatrix}^2$$

a więc wyznacznik

$$\det\left(T_{L|K}(\vartheta^i\vartheta^j)\right) = \prod_{i<j}(\vartheta_j - \vartheta_i)^2 \neq 0$$

dla $i, j = 0, 1, \ldots, n-1$, czyli nasza forma jest niezdegenerowana. Wynika stąd natychmiast, że dla dowolnej innej bazy $\{\alpha_1, \ldots, \alpha_n\}$ ciała L nad K mamy $d(\alpha_1, \ldots, \alpha_n) \neq 0$, gdyż jest to wyznacznik macierzy tej formy w bazie $\{\alpha_1, \ldots, \alpha_n\}$. ■

Z lematu 2.1 wynika także proste kryterium odwracalności elementu całkowitego $x \in L$. Mianowicie

$$x \in B^* \iff N_{L|K}(x) \in A^*$$

Wiemy już, że norma obcięta do domknięcia A w L (oznaczanego dalej przez B) ma wartości w pierścieniu A. Jeśli $xy = 1$ dla pewnego $y \in B$, to rzecz jasna $N_{L|K}(x) \in A^*$. Na odwrót, jeśli $aN_{L|K}(x) = 1$ dla pewnego $a \in A$, to mamy $1 = a\prod_{\sigma}\sigma x = yx$ dla pewnego $y \in B$ (bowiem sprzężenia elementu całkowitego są całkowite nad A). Wprowadzone pojęcia wyróżnika pozwala nam sformułować, jak się okaże, użyteczny

Lemat 1.14. *Niech $\alpha_1, \ldots, \alpha_n$ stanowią bazę L nad K, przy czym zakładamy, że każdy element α_i jest całkowity nad A. Jeśli $d = d(\alpha_1, \ldots, \alpha_n)$ jest wyróżnikiem tej bazy, to*

$$dB \subset A\alpha_1 + \ldots A\alpha_n$$

Dowód. Jeśli element $\alpha = a_1\alpha_1 + \ldots + a_n\alpha_n \in B$ (jest całkowity nad A), gdzie $a_i \in K$, to wówczas $(a_1, \ldots, a_n)$ jest rozwiązaniem układu równań liniowych:

$$T_{L|K}(\alpha\alpha_j) = \sum_{i=1}^{n} T_{L|K}(\alpha_i\alpha_j)x_i \quad \text{dla } j = 1, \ldots, n$$

Skoro zaś $T_{L|K}(\alpha\alpha_j) \in A$, to a_i jest równy ilorazowi elementu z A przez wyznacznik macierzy $(T_{L|K}(\alpha_i\alpha_j))$ równy d. Zatem $da_i \in A$, czyli $d\alpha \in A\alpha_1 + \ldots + A\alpha_n$. ■

Jeśli istnieją elementy $\omega_1, \ldots, \omega_n \in B$ takie, że każdy element $b \in B$ możemy zapisać **w sposób jednoznaczny** jako kombinację $b = a_1\omega_1 + \ldots + a_n\omega_n$, $a_i \in A$, to mówimy, że te elementy stanowią **bazę całkowitą** B nad A. Innymi słowy, pierścień B jest **wolnym *A*-modułem**. Zauważmy, że jeśli baza całkowita istnieje, to jest ona mocy $n = |L : K|$, bowiem elementy tej bazy rozpinają też przestrzeń L nad K. W przypadku ogólnym, baza całkowita istnieć nie musi. Jednak jeżeli dziedzina A jest dostatecznie przyzwoita, to baza całkowita istnieje.

Twierdzenie 1.15. *Niech A będzie dziedziną ideałów głównych, zaś rozszerzenie $K \subset L$ będzie skończone i rozdzielcze. Wówczas każdy, skończenie generowany B-podmoduł $M \neq 0$ ciała L jest wolnym A-modułem rangi $n = |L : K|$. W szczególności, B ma bazę całkowitą.*

Dowód. Niech $M \neq 0$ będzie tak jak powyżej i niech $\alpha_1, \ldots, \alpha_n$ będzie bazą L nad K. Bez straty ogólności możemy założyć, że $\alpha_i \in B$. Zatem, na mocy lematu 2.2 mamy $dB \subset A\alpha_1 + \ldots + A\alpha_n =: M_0$; w szczególności A-moduł dB jest wolny, rangi co najwyżej $n = |L : K|$. To oznacza, że B jest wolny, rangi co najwyżej $|L : K|$ (zauważmy bowiem, że A-moduł B jest oczywiście beztorsyjny). Stąd jednak wynika, że ranga A-modułu B musi być równa $|L : K|$, bowiem generatory B nad A rozpinają L nad K. Niech wreszcie $\{\mu_i\}_{i=1,\ldots,m}$ będzie zbiorem generatorów B-modułu M. Możemy wybrać $a_i \in A$, $i = 1, \ldots, m$ tak, by $a_i\mu_i \in B$. Wtedy istnieje $a \in A$ taki, że $a\mu_i \in B$ i w konsekwencji

$$daM = da(B\mu_1 + \ldots + B\mu_m) \subset dB \subset A\alpha_1 + \ldots + A\alpha_n = M_0$$

wobec czego daM jest wolny i M jest wolny rangi co najwyżej n. Zatem

$$|L : K| = r(B) \leqslant r(M) = r(adM) \leqslant r(M_0) = |L : K|$$

Nierówność $r(B) \leqslant r(M)$ wynika z faktu, że dla $m \in M$, $m \neq 0$, elementy $\alpha_i m \in M$ dla $i = 1, \ldots, n$ są liniowo niezależne nad A, toteż Bm jest podmodułem M rangi $n = r(B)$. m ■

Odnotujmy co wynika z twierdzenia 2.6. Jesteśmy szczególnie zainteresowani sytuacją, gdzie naszą dziedziną całkowitości A jest pierścień liczb całkowitych $\mathbb{Z}$ z ciałem ułamków $\mathbb{Q}$. Niech ponadto będzie dane dowolne, skończone rozszerzenie $\mathbb{Q} \subset K$. Wówczas pierścień liczb całkowitych O_K ma bazę całkowitą $\omega_1, \ldots, \omega_n$, gdzie $n = |L : K|$. Możemy ponadto zdefiniować poprawnie **wyróżnik ciała liczbowego K**:

$$d_K = d(O_K) = d(\omega_1, \ldots, \omega_n)$$

a także wyróżnik dowolnego, skończenie generowanego O_K-podmodułu α w K (a więc w szczególności także ideału $I \triangleleft O_K$)

$$d(\alpha) = \det\left((\sigma_i \alpha_j)\right)^2$$

gdzie $\alpha_1, \ldots, \alpha_n \in \alpha$ stanowią bazę modułu α. To jest dobrze określone, bowiem dla każdego $A \in GL_n(\mathbb{Z})$ mamy $|\det A| = 1$. Mamy ponadto

Twierdzenie 1.16. *Niech $I \triangleleft O_K$ będzie niezerowym ideałem w pierścieniu liczb całkowitych ciała K. Wówczas zachodzi równość*

$$d(I) = |O_K : I|^2 \cdot d_K$$

(w szczególności indeks $|O_K : I|$ jest skończony)

Dowód. To twierdzenie wynika wprost z faktu, że jeśli dana jest dowolna macierz A wymiarów $n \times n$ nad $\mathbb{Z}$, przy czym $\det A \neq 0$, to wówczas indeks obrazu przekształcenia $A : \mathbb{Z}^n \longrightarrow \mathbb{Z}^n$ w $\mathbb{Z}^n$ jest równy $|\det A|$:

$$|\mathbb{Z}^n : \operatorname{im} A| = |\det A|$$

■