

„Teoria rugownika i wyróżnik ciała”. Projekt zaliczeniowy: Algebraiczna Teoria Liczb I

Bazyli Klockiewicz

22 czerwca 2014

1 Rugownik pary wielomianów oraz wyróżnik wielomianu.

Poniższe stwierdzenia opisują ideę rugownika pary wielomianów.

Stwierdzenie 1. *Niech F będzie ciałem i niech $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ oraz $g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$ będą wielomianami z $F[x]$, $a_n \neq 0$, $b_m \neq 0$. Wówczas $f(x)$ i $g(x)$ mają wspólny nietrywialny dzielnik w $F[x]$ wtedy i tylko wtedy, gdy istnieją: niezerowy wielomian $a(x) \in F[x]$ stopnia co najwyżej $m-1$ oraz niezerowy wielomian $b(x) \in F[x]$ stopnia co najwyżej $n-1$ takie, że $a(x)f(x) = b(x)g(x)$.*

Dowód. Załóżmy, że $f(x)$ i $g(x)$ mają wspólny nietrywialny dzielnik $w(x) \in F[x]$. Innymi słowy, w $F[x]$ zachodzą równości $f(x) = w(x)b(x)$ oraz $g(x) = w(x)a(x)$ dla pewnych $a(x), b(x) \in F[x]$ przy czym $\deg w(x) \geq 1$. Wtedy, $\deg a(x) = m - \deg w(x) \leq m-1$ oraz $\deg b(x) = n - \deg w(x) \leq n-1$ (bo $F[x]$ jest dziedziną całkowitości) i mamy $f(x)a(x) = w(x)b(x)a(x) = g(x)b(x)$.

Na odwrót, niech $f(x)a(x) = g(x)b(x)$ dla $a(x), b(x) \in F[x]$ w treści stwierdzenia. Gdyby $f(x)$ i $g(x)$ nie miały wspólnego nietrywialnego dzielnika, to ponieważ $F[x]$ jest dziedziną z jednoznacznością rozkładu, otrzymalibyśmy $f(x)|b(x)$ (analogicznie $g(x)|a(x)$) w $F[x]$. Jest to sprzeczność, ponieważ $\deg b(x) \leq n-1 < \deg f(x)$. $\square$

Równoważnie można powiedzieć, że istnienie wyżej opisanych wielomianów $a(x)$ i $b(x)$ jest warunkiem koniecznym i dostatecznym na to, aby wielomiany $f(x)$ i $g(x)$ miały wspólny pierwiastek w $\bar{F}$ (albo po prostu w pewnym rozszerzeniu F).

Stwierdzenie 2 (Rugownik wielomianów f i g). Niech F będzie ciałem i niech $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$ oraz $g(x) = b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0$ będą wielomianami z $F[x]$. Wówczas $f(x)$ i $g(x)$ mają wspólny nietrywialny dzielnik w $F[x]$ (równoważnie - wspólny pierwiastek w $\bar{F}$) wtedy i tylko wtedy, gdy wyznacznik

$$R(f, g) = \begin{vmatrix} a_n & a_{n-1} & \dots & a_0 & 0 & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_0 & 0 & \dots \\ & 0 & a_n & a_{n-1} & \dots & a_0 & 0 \\ & & & \ddots & & & 0 \\ & & 0 & a_n & a_{n-1} & a_{n-2} & \dots & a_0 \\ b_m & b_{m-1} & \dots & b_0 & 0 & \dots & 0 \\ 0 & b_m & b_{m-1} & \dots & b_0 & 0 & \dots \\ & 0 & b_m & b_{m-1} & \dots & b_0 & 0 \\ & & & \ddots & & & 0 \\ & & & 0 & b_m & b_{m-1} & \dots & b_0 \end{vmatrix}$$

jest równy zero.

Dowód. Korzystając z Stwierdzenia 1. istnienie wspólnego nietrywialnego dzielnika wielomianów $f(x)$ oraz $g(x)$ jest równoważnie istnieniu niezerowych wielomianów $a(x) = c_{m-1} x^{m-1} + c_{m-2} x^{m-2} + \dots + c_1 x + c_0$ oraz $b(x) = d_{n-1} x^{n-1} + d_{n-2} x^{n-2} + \dots + d_1 x + d_0$ z $F[x]$ takich, że $f(x)a(x) = (a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0)(c_{m-1} x^{m-1} + c_{m-2} x^{m-2} + \dots + c_1 x + c_0) = (b_m x^m + b_{m-1} x^{m-1} + \dots + b_1 x + b_0)(d_{n-1} x^{n-1} + d_{n-2} x^{n-2} + \dots + d_1 x + d_0) = g(x)b(x)$. Porównując współczynniki przy potęgach x , otrzymujemy zatem następujący układ równań liniowych jednorodnych, w którym współczynniki c_i, d_i są zmiennymi:

$$\begin{aligned} a_n c_{m-1} - b_m d_{n-1} &= 0 \\ a_{n-1} c_{m-1} + a_n c_{m-2} - b_{m-1} d_{n-1} - b_m d_{n-2} &= 0 \\ &\dots \\ a_0 c_0 - b_0 d_0 &= 0 \end{aligned}$$

Podstawiając $-d_i$ w miejsce d_i oraz transponując macierz powyższego jednorodnego układu równań liniowych (co może skutkować jedynie zmianą znaku wyznacznika) stwierdzamy, że układ ten ma nietrywialne rozwiązanie dokładnie wtedy, gdy $R(f, g)$ się zeruje.

□

Z dowodów stwierdzeń wynika, że zamiast rozważać wielomiany nad ciałem, można ogólniej wymagać tylko, by $f(x), g(x) \in A[x]$, gdzie $A[x]$ jest dziedziną z jednoznacznością rozkładu.

Definicja 1. (*Rugownik pary wielomianów*) Wyznacznik $R(f, g)$ z powyższego stwierdzenia nazywamy rugownikiem wielomianów f oraz g .

Zauważmy, że rugownik jest wyznacznikiem macierzy $(n+m) \times (n+m)$, w której pierwszych n wierszy pochodzi ze współczynników wielomianu f , a kolejnych m wierszy pochodzi od współczynników wielomianu g . Samą macierz nazywamy *macierzą Sylvestera*.

Zachodzi następujące kluczowe:

Twierdzenie 1. *Przy dotychczasowych oznaczeniach, niech $x_1, x_2, \dots, x_n$ będą pierwiastkami $f(x)$ oraz $y_1, y_2, \dots, y_m$ niech będą pierwiastkami $g(x)$ (niekoniecznie różnymi i ogólnie zawartymi w $\bar{F}$). Wówczas*¹

$$R(f, g) = a_n^m b_m^n \prod_{i,j} (x_i - y_j) = a_n^m \prod_i g(x_i) = (-1)^{nm} \cdot b_m^n \prod_j f(y_j)$$

Dowód. Ponieważ $f(x) = a_n(x-x_1) \cdots (x-x_n)$ oraz $g(x) = b_m(x-y_1) \cdots (x-y_m)$, ze wzorów Viete'a wnioskujemy, że $a_k = \pm a_n \sigma_k(x_1, \dots, x_n)$, gdzie σ_k jest elementarną funkcją symetryczną. Podobnie $b_k = \pm b_m \sigma_k(y_1, \dots, y_m)$. Rozwijając wyznacznik definiujący rugownik stwierdzamy, że jest on wielomianem jednorodnym stopnia m względem współczynników a_i oraz stopnia n względem współczynników b_i (na przykład dla a_i rozwijając wyznacznik zawsze względem pierwszego wiersza). Stąd:

$$R(f, g) = a_n^m b_m^n P(x_1, x_2, \dots, x_n, y_1, \dots, y_m),$$

gdzie P jest wielomianem symetrycznym, który - z własności rugownika - zeruje się, jeśli $x_i = y_j$ dla pewnych i, j . Z tożsamości:

$$x_i^k = (x_i - y_j)x_i^{k-1} + y_j x_i^{k-1}$$

zastosowanej k razy wynika, że wielomian P możemy zapisać następująco:

$$P(x_1, x_2, \dots, x_n, y_1, \dots, y_m) = (x_i - y_j)Q(x_1, \dots, y_m) + U(x_1, \dots, \hat{x}_i, \dots, y_m),$$

gdzie wielomian U nie zawiera współczynnika x_i . Podstawiając $x_i = y_j$ wnioskujemy, że wielomian U jest zerowy. Stosując podobny argument dla każdej z

¹W książce Prasolova brakuje wyrażenia $(-1)^{nm}$, pewnie dlatego, że autor zadowolili się w dowodzie frazą "the arguments are similar...".

par x_i, y_j stwierdzamy, że $R(f, g)$ dzieli się przez $S = a_n^m b_m^n \prod (x_i - y_j)$. Chcemy pokazać, że zachodzi równość $R(f, g) = S$. Ponieważ $g(x) = b_m \prod_{j=1}^m (x - y_j)$, więc $\prod_{i=1}^n g(x_i) = b_m^n \prod (x_i - y_j)$. Zatem:

$$S = a_n^m \prod_{i=1}^n g(x_i) = a_n^m \prod_{i=1}^n (b_m x_i^m + b_{m-1} x_i^{m-1} + \dots + b_0).$$

Z postaci tej widać (stosując znów wzory Viete'a), że zarówno $R(f, g)$ oraz S są wielomianami stopnia nm względem x_i, y_j , a ponieważ $S|R$, stąd $R(f, g) = \lambda S$ dla pewnego $\lambda \neq 0$, przy czym λ nie zależy od współczynników a_i ani b_i (bo możemy podzielić obustronnie przez $a_n^m b_m^n$). Zauważamy teraz, że współczynnik przy $\prod_{i=1}^n x_i^m$ w wielomianie S jest równy $a_n^m b_m^n$, podobnie w wielomianie $R(f, g)$ stąd $\lambda = 1$, a więc $S = R(f, g)$. Pozostaje dowieść drugą z równości. Otóż mamy $f(x) = a_n \prod_{i=1}^n (x - x_i)$, więc $\prod_{i=1}^m f(y_i) = a_n^m \prod (y_j - x_i) = (-1)^{nm} \cdot a_n^m \prod (x_i - y_j)$ i stwierdzamy, że

$$S = (-1)^{nm} \cdot b_m^n \prod_{j=1}^m f(y_j) = (-1)^{nm} \cdot b_m^n \prod_{j=1}^m (a_n y_j^n + a_{n-1} y_j^{n-1} + \dots + a_0).$$

□

Pojęcie rugownika jest ściśle związane z wyróżnikiem wielomianu.

Definicja 2. (*Wyróżnik wielomianu*) Niech $x_1, x_2, \dots, x_n$ będą pierwiastkami wielomianu $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_0 \in F[x]$, gdzie $a_n \neq 0$. Wyróżnikiem wielomianu f nazywamy liczbę:

$$D(f) = a_n^{2n-2} \prod_{i < j} (x_i - x_j)^2$$

Czasami wyróżnik definiuje się za pomocą rugownika wielomianu oraz jego pierwszej pochodnej. Zachodzi bowiem następujące:

Twierdzenie 2. *Dla wielomianu powyżej zachodzi*

$$R(f, f') = (-1)^{n(n-1)/2} a_n^{2n-1} D(f)$$

Dowód. Z Twierdzenia 1. otrzymujemy $R(f, f') = a_n^{n-1} \prod_{i=1}^n f'(x_i)$. Ponadto, różniczkując f łatwo zauważyć, że $f'(x_i) = a_n \prod_{j \neq i} (x_i - x_j)$. Stąd:

$$R(f, f') = a_n^{2n-1} \prod_{i=1}^n \prod_{j \neq i} (x_i - x_j) = (-1)^{n(n-1)/2} a_n^{2n-1} \prod_{i < j} (x_i - x_j)^2.$$

Współczynnik $(-1)^{n(n-1)/2}$ pochodzi stąd, że każda para x_i, x_j dla $i \neq j$, "występuje" dwa razy: raz jako $(x_i - x_j)$, a drugi raz jako $(x_j - x_i)$. □

Wyróżnik wielomianu znajduje zastosowanie przy obliczaniu wyróżników ciała liczbowego, o których traktuje następna część pracy.

2 Wyróżnik ciała liczbowego.

Przypomnijmy definicję (bezwzględnego) wyróżnika ciała liczbowego.

Definicja 3. (Bezwzględny wyróżnik ciała liczbowego) Niech K będzie ciałem liczbowym stopnia n i niech $\mathcal{O}_K$ będzie pierścieniem jego liczb algebraicznych całkowitych. Niech $\alpha_1, \alpha_2, \dots, \alpha_n$ będzie bazą całkowitą $\mathcal{O}_K$ oraz niech $\sigma_1, \sigma_2, \dots, \sigma_n$ będzie zbiorem zanurzeń zespolonych ciała K . Wyróżnikiem ciała K nazywamy liczbę:

$$\Delta_K = \left(\det \begin{bmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \dots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \dots & \sigma_2(\alpha_n) \\ \vdots & & \ddots & \vdots \\ \sigma_n(\alpha_1) & \sigma_n(\alpha_2) & \dots & \sigma_n(\alpha_n) \end{bmatrix} \right)^2$$

Definicja jest poprawna, bowiem można łatwo pokazać, że wyróżnik ciała nie zależy od wyboru bazy całkowitej $\mathcal{O}_K$ (i taka baza zawsze istnieje). Co ważne, wyróżnik jest liczbą całkowitą.

Twierdzenie 3. W przypadku, gdy $\mathcal{O}_K$ posiada potęgową bazę całkowitą $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$, wyróżnik Δ_K jest równy wyróżnikowi wielomianu minimalnego elementu α :

$$\Delta_K = D(\min_{\mathbb{Q}}(\alpha))$$

Dowód. Niech $x_1, x_2, \dots, x_n$ będą pierwiastkami wielomianu minimalnego f elementu α . Oczywiście z założenia wynika w szczególności, że $K = \mathbb{Q}(\alpha)$. Możemy przyjąć, że $\sigma_i(\alpha) = x_i$ oraz σ_i są homomorfizmami pierścieni, a więc w tym przypadku macierzą definiującą Δ_K jest macierz typu Vendermonde'a:

$$\Delta_K = \left(\det \begin{bmatrix} 1 & x_1 & \dots & x_1^{n-1} \\ 1 & x_2 & \dots & x_2^{n-1} \\ \vdots & & \ddots & \vdots \\ 1 & x_n & \dots & x_n^{n-1} \end{bmatrix} \right)^2,$$

której kwadrat wyznacznika jest równy:

$$\Delta_K = \prod_{i < j} (x_i - x_j)^2 = D(f) = D(\min_{\mathbb{Q}}(\alpha))$$

(bo wielomian f jest unormowany).

□

Wyróżnik ciała zajmuje niezwykle ważne miejsce w Algebraicznej Teorii Liczb. Głównym celem niniejszego krótkiego opracowania będzie udowodnienie następującego twierdzenia:

Twierdzenie 4. *Niech K i L będą ciałami liczbowymi stopni m i n odpowiednio takimi, że $(\Delta_K, \Delta_L) = 1$. Wówczas $\Delta_{KL} = \Delta_K^n \Delta_L^m$.*

Powyższe twierdzenie pozwala na przykład wyrazić wyróżnik ciała cyklotomicznego w jawnej postaci. Przypomnijmy, że:

Definicja 4. *Niech ciała K i L będą podciałami ciała M . Wówczas iloczyn ciał KL to z definicji najmniejsze podciało ciała M zawierające zarówno K oraz L .*

Dla ciał liczbowych bierzemy $M = \bar{\mathbb{Q}}$.

Definicja 5. *(Iloczyn Kroneckera macierzy) Niech będą dane macierze kwadratowe $A = [a_{ij}] \in M_{m,m}(K)$ oraz $B = [b_{ij}] \in M_{n,n}(K)$ o współczynnikach w ciele K . Definiujemy iloczyn tensorowy (Kroneckera) $A \otimes B \in M_{mn,mn}(K)$ macierzy A i B jako macierz blokową:*

$$\begin{bmatrix} Ab_{11} & Ab_{12} & \dots & Ab_{1n} \\ Ab_{21} & Ab_{22} & \dots & Ab_{2n} \\ \vdots & & \ddots & \vdots \\ Ab_{n1} & Ab_{n2} & \dots & Ab_{nn} \end{bmatrix}$$

Lemat 1. $\det(A \otimes B) = (\det A)^n (\det B)^m$

Dowód. Przeprowadzamy proces eliminacji Gaussa traktując bloki wierszy:

$$\begin{bmatrix} Ab_{i1} & Ab_{i2} & \dots & Ab_{in} \end{bmatrix}$$

jak pojedyncze wiersze. Otrzymamy macierz blokową:

$$\begin{bmatrix} Ax_{11} & 0 & \dots & 0 \\ 0 & Ax_{22} & \dots & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & Ax_{nn} \end{bmatrix}$$

w której współczynniki x_{ii} są elementami macierzy diagonalnej otrzymanej z B za pomocą metody eliminacji Gaussa (a więc w szczególności $\det B = \prod_{i=1}^n x_{ii}$). Z twierdzenia Cauchy'ego dla macierzy blokowych:

$$\det(A \otimes B) = \prod_{i=1}^n \det(Ax_{ii}) = (\det A)^n \prod_{i=1}^n (x_{ii})^m = (\det A)^n (\det B)^m$$

□

W dalszym ciągu będziemy potrzebowali kilku nowych definicji (spolszczenia angielskich terminów należą do autora tekstu i mogą nie odpowiadać ogólnie przyjętym).

Definicja 6. (*Relatywny ślad elementu*) Niech K/F będzie rozszerzeniem ciał liczbowych stopnia n oraz niech σ_i dla $i = 1, 2, \dots, n$ będą wszystkimi F –liniowymi zanurzeniami ciała K w $\bar{F}$ (inaczej F -izomorfizmami K). Relatywnym śladem w K/F elementu $\alpha \in K$ nazywamy liczbę:

$$T_{K/F}(\alpha) := \sum_{i=1}^n \sigma_i(\alpha)$$

Definicja 7. (*Relatywny stopień ideału*) Niech K/F będzie rozszerzeniem ciał liczbowych, $\mathfrak{p}$ będzie ideałem pierwszym w $\mathcal{O}_F$, który w $\mathcal{O}_K$ rozkłada się następująco:

$$\mathfrak{p} = \prod_{j=1}^g \mathcal{P}_j^{e_j},$$

gdzie $\mathcal{P}_j$ są różnymi ideałami pierwszymi w $\mathcal{O}_K$ (mówimy, że $\mathcal{P}_j$ leżą nad $\mathfrak{p}$). Liczbę

$$f_{K/F}(\mathcal{P}_j) := |\mathcal{O}_K/\mathcal{P}_j : \mathcal{O}_F/\mathfrak{p}|$$

nazywamy relatywnym stopniem $\mathcal{P}_j$ w $\mathcal{O}_K$.

Definicja 8. (*Relatywna norma ideału*) Niech K/F będzie rozszerzeniem ciał liczbowych i niech $\mathcal{P}$ będzie ideałem pierwszym w $\mathcal{O}_K$ leżącym nad (jednoznacznie wyznaczonym, co można udowodnić) ideałem pierwszym w $\mathcal{O}_F$, a więc $\mathfrak{p} = \mathcal{P} \cap \mathcal{O}_F$. Definiujemy relatywną normę ideału $\mathcal{P}$ następująco:

$$N^{K/F}(\mathcal{P}) = \mathfrak{p}^{f_{K/F}(\mathcal{P})}.$$

Definicję tę przedłużamy na ideały ułamkowe I następująco:

$$N^{K/F}(I) := \prod_{j=1}^n \mathfrak{p}_k^{f_{K/F}(\mathcal{P}_j)},$$

gdzie $I = \prod_{j=1}^n \mathcal{P}_j^{a_j}$ jest iloczynem potęg różnych ideałów pierwszych w $\mathcal{O}_K$ takich, że $\mathcal{P}_j \cap \mathcal{O}_F = \mathfrak{p}_j$.

W szczególności

$$N^{K/\mathbb{Q}}(I) = (N(I))$$

jako ideał główny w $\mathbb{Z}$ generowany przez klasyczną normę ideału.

Definicja 9. (Kodyfrent) Niech K/F będzie rozszerzeniem ciał liczbowych i niech I będzie ideałem ułamkowym w $\mathcal{O}_F$. Kodyfrentem nazywamy zbiór:

$$I^* = \{\beta \in K : T_{K/F}(\beta I) \subseteq \mathcal{O}_F\},$$

gdzie $T_{K/F}(\beta I) \subseteq \mathcal{O}_F$ oznacza, że $T_{K/F}(\beta \alpha) \in \mathcal{O}_F$ dla każdego $\alpha \in I$.

Można wykazać, że I^* jest ideałem ułamkowym.

Definicja 10. (Dyfrent) Niech K/F będzie rozszerzeniem ciał liczbowych i niech I będzie ideałem ułamkowym w $\mathcal{O}_K$. Ideał $(I^*)^{-1}$ nazywamy dyfrentem I nad F i oznaczamy $\mathcal{D}_{K/F}(I)$. W przypadku, gdy $I = \mathcal{O}_K$, dyfrent $\mathcal{D}_{K/F}(I)$ nazywamy dyfrentem rozszerzenia K/F i oznaczamy $\mathcal{D}_{K/F}$.

Definicja 11. (Relatywny wyróżnik rozszerzenia ciał)

Niech K/F będzie rozszerzeniem ciał liczbowych. Wyróżnikiem relatywnym rozszerzenia K/F nazywamy:

$$\Delta_{K/F} = N^{K/F}(\mathcal{D}_{K/F})$$

W szczególności, $\Delta_{K/\mathbb{Q}} = (\Delta_K)$ jako ideał w $\mathbb{Z}$.

Uwzględniając powyższe definicje, można wykazać następujące własności, które będą kluczowe w dowodzie głównego twierdzenia.

Lemat 2. Jeśli $F \subseteq K \subseteq L$ jest wieżą rozszerzeń ciał liczbowych, wówczas:

$$\Delta_{L/F} = \Delta_{K/F}^{[L:K]} N^{K/F}(\Delta_{L/K}).$$

Lemat 3. Niech $F \subseteq K \subseteq L$ będzie wieżą rozszerzeń ciał liczbowych, gdzie L jest najmniejszym rozszerzeniem ciała F zawierającym K takim, że L jest rozszerzeniem normalnym nad F . Wówczas $\Delta_{K/F}$ oraz $\Delta_{L/F}$ mają te same dzielniki (ideały) pierwsze.

Przytoczymy ponadto następujące lematy, które okażą się przydatne.

Lemat 4. Jeśli F jest podciałem ciała liczbowego K , to $\Delta_F | \Delta_K$.

Lemat 5. (Twierdzenie Minkowskiego) Jeśli K jest ciałem liczbowym, $K \neq \mathbb{Q}$, to $|\Delta_K| > 1$.

Lemat 6. Dziedzina całkowitości będąca skończeniem wymiarową przestrzeni liniowej nad ciałem także jest ciałem.

Dowód. Niech R będzie taką skończoną wymiarową dziedziną całkowitości nad ciałem F . Niech $x \in R$ będzie niezerowym elementem. Z założenia istnieje najmniejsza liczba naturalna t taka, że zbiór $\{1, x, x^2, \dots, x^t\}$ jest liniowo zależny. Niech $a_0 + a_1x + \dots + a_tx^t = 0$, gdzie $a_i \in F$ nie wszystkie są równe 0. Gdyby $a_0 = 0$ lub $a_t = 0$, to mielibyśmy odpowiednio $x(a_1 + a_2x + \dots + a_tx^{t-1}) = 0$ lub $a_0 + a_1x + \dots + a_{t-1}x^{t-1} = 0$, co przy $x \neq 0$ przeczy minimalności t . Stąd $x^{-1} = (-a_0)^{-1}(a_1 + a_2x + \dots + a_tx^{t-1})$. $\square$

W końcu możemy przystąpić do dowodu głównego twierdzenia:

Twierdzenie 5. *Niech K i L będą ciałami takimi, że $[K : \mathbb{Q}] = n$, $[L : \mathbb{Q}] = m$ oraz $\{\alpha_1, \alpha_2, \dots, \alpha_n\}$ i $\{\beta_1, \beta_2, \dots, \beta_m\}$ są bazami całkowitymi odpowiednio $\mathcal{O}_K$ i $\mathcal{O}_L$. Jeżeli $(\Delta_K, \Delta_L) = 1$, to dla ciała $M = KL$ zachodzą następujące fakty:*

- a) $[M : \mathbb{Q}] = nm$,
- b) $\mathcal{O}_M = \mathcal{O}_K \mathcal{O}_L$ oraz $\{\alpha_i \beta_j\}_{1 \leq i \leq n, 1 \leq j \leq m}$ jest bazą całkowitą $\mathcal{O}_M$,
- c) $\Delta_M = \Delta_K^m \Delta_L^n$.

Dowód. Z mnożliwości stopnia rozszerzenia:

$$[M : \mathbb{Q}] = [M : L][L : \mathbb{Q}] = [M : L]m$$

Założmy, że $[M : \mathbb{Q}] < nm$. Wówczas $[M : L] < n$ (*). Niech α będzie takim elementem, że $K = \mathbb{Q}(\alpha)$ (taki element zawsze istnieje z twierdzenia o elemencie prymitywnym). Z (*) wynika, że wtedy $\min_L(\alpha) \mid \min_{\mathbb{Q}}(\alpha)$ w sposób właściwy oraz, że jeśli F jest podciałem L generowanym przez współczynniki wielomianu $\min_L(\alpha)$, to $F \neq \mathbb{Q}$ (i stąd z Twierdzenia Minkowskiego $|\Delta_F| > 1$ (**)). Z lematu 4 mamy $\Delta_F \mid \Delta_L$. Ponieważ (ze wzorów Viete'a) współczynniki $\min_L(\alpha)$ są wartościami elementarnych funkcji symetrycznych na pierwiastkach tego wielomianu, więc $\min_L(\alpha) \in N[x]$, gdzie N jest najmniejszym rozszerzeniem Galois ciała $\mathbb{Q}$ zawierającym K . Stąd, $F \subseteq N$ i znów otrzymujemy $\Delta_F \mid \Delta_N$. Jeśli $p \mid \Delta_F$ jest liczbą pierwszą, to mamy teraz $p \mid \Delta_L$ oraz $p \mid \Delta_N$. Z lematu 2. wnioskujemy, że także $p \mid \Delta_K$. Ponadto z (**) wynika, że taka liczba pierwsza p zawsze istnieje, co przeczy założeniu, że $(\Delta_K, \Delta_L) = 1$. Z drugiej strony zauważmy, że na mocy Lematu 6., $M = \text{span}_{\mathbb{Q}}\{\alpha_k \beta_l\}$, bo ciało to zawiera zarówno K jak i L , a więc $[M : \mathbb{Q}] \leq nm$. To dowodzi a).

Z definicji, $\mathcal{O}_K \mathcal{O}_L$ to najmniejszy podpierścień $\mathcal{O}_M$ zawierający zarówno $\mathcal{O}_K$ jak $\mathcal{O}_L$. Zatem $\{\alpha_k \beta_l\}$ dla $1 \leq k \leq n, 1 \leq l \leq m$ jest bazą całkowitą $\mathcal{O}_K \mathcal{O}_L$. Ponadto:

$$\Delta_{M/\mathbb{Q}}(\{\alpha_k\beta_l\}) = \det(\sigma_i(\alpha_k)\theta_j(\beta_l))^2 \quad (1)$$

gdzie po lewej mamy wyróżnik układu elementów algebraicznych, σ_i są zanurzeniami zespolonymi ciała K , a θ_j są zanurzeniami zespolonymi ciała L . Zatem jest to poprawne, ponieważ każde z nm zanurzeń τ ciała M indukuje zanurzenia $\tau|_K = \sigma_i$ oraz $\tau|_L = \theta_j$ oraz wartość zanurzenia na dowolnym elemencie ciała M jest wyznaczona jednoznacznie przez wartości na $\{\alpha_k\beta_l\}$, zbiorze generatorów $M/\mathbb{Q}$. Powyższy wyróżnik jest kwadratem wyróżnika macierzy Kroneckera:

$$\begin{bmatrix} A\theta_1(\beta_1) & A\theta_1(\beta_2) & \dots & A\theta_1(\beta_m) \\ A\theta_2(\beta_1) & A\theta_2(\beta_2) & \dots & A\theta_2(\beta_m) \\ \vdots & & \ddots & \vdots \\ A\theta_m(\beta_1) & A\theta_m(\beta_2) & \dots & A\theta_m(\beta_m) \end{bmatrix},$$

gdzie $A = [\sigma_i(\alpha_k)]_{1 \leq i \leq n, 1 \leq k \leq n}$. Na mocy lematu 1 otrzymujemy

$$\Delta_{M/\mathbb{Q}}(\{\alpha_k\beta_l\}) = \Delta_K^m \Delta_L^n. \quad (2)$$

Z lematu 2 oraz mnożliwości stopnia rozszerzeń ciał:

$$\Delta_{M/\mathbb{Q}} = \Delta_{K/\mathbb{Q}}^{[M:K]} N^{K/\mathbb{Q}}(\Delta_{M/K}) = \Delta_{K/\mathbb{Q}}^m N^{K/\mathbb{Q}}(\Delta_{M/K})$$

i podobnie:

$$\Delta_{M/\mathbb{Q}} = \Delta_{L/\mathbb{Q}}^n N^{L/\mathbb{Q}}(\Delta_{M/L}).$$

Są to równości ideałów głównych w $\mathbb{Z}$, a zatem zarówno Δ_L^n jak i Δ_K^m dzielą Δ_M , a ponieważ z założenia $(\Delta_K, \Delta_L) = 1$, więc w $\mathbb{Z}$ zachodzi podzielność:

$$\Delta_K^m \Delta_L^n \mid \Delta_M.$$

Zauważmy jednak, że z (2) wynika podzielność odwrotna:

$$\Delta_M \mid \Delta_K^m \Delta_L^n = \Delta_{M/\mathbb{Q}}(\{\alpha_k\beta_l\}).$$

Z tych dwóch faktów wynika po pierwsze, że $\{\alpha_j\beta_k\}$ jest bazą całkowitą $\mathcal{O}_M$ oraz, że $\Delta_M = \Delta_K^m \Delta_L^n$, co kończy dowód podpunktów b) i c) oraz całego twierdzenia. □

Literatura

- [1] David S. Dummit, Richard M. Foote, *Abstract Algebra. Second Edition*, John Wiley & Sons, Inc., 2003.
- [2] Victor V. Prasolov, *Polynomials*, Springer, 2001.
- [3] C. Musili, *Algebraic Geometry for Beginners*, Hindustan Book Agency, 2000.
- [4] Richard A. Mollin, *Algebraic Number Theory*, CHAPMAN & HALL/CRC, 1999.
- [5] Juergen Neukirch, *Algebraic Number Theory*, Springer, 1999.
- [6] James Milne, *Algebraic Number Theory*, Version 3.06, May 28, 2014.
<http://www.jmilne.org/math/CourseNotes/ANT.pdf>
- [7] David Hilbert, *The Theory of Algebraic Number Fields*, Springer, 1998.