PIERWIASTNIKI I ROZSZERZENIA PIERWIASTNIKOWE

Najpierw dwa-trzy ogólne fakty algebraiczne:

(A) Rozszerzenie ciała liczbowego K o element algebraiczny nad K

<u>Def.</u> Liczbę a nazywamy <u>elementem algebraicznym nad ciałem liczbowym</u> K jeśli a jest pierwiastkiem wielomianu $f(x) = \alpha_n x^n + \ldots + \alpha_1 x + \alpha_0$ o współczynnikach $\alpha_0, \alpha_1, \ldots, \alpha_n$ z ciała K.

UWAGI:

1. Elementy algebraiczne nad $\mathbb{Q}$ to po prostu liczby algebraiczne.

2. Każdy element algebraiczny u nad ciałem K posiada <u>wielomian minimalny nad K</u>, czyli wielomian najmniejszego stopnia o współczynnikach z K, dla którego u jest pierwiastkiem; taki wielomian minimalny nad K jest jednoznaczny z dokładnością do czynnika z K. Jest też prawdą, że wielomian nad K, którego pierwiastkiem jest u, jest wielomianem minimalnym dla u $\Longleftrightarrow$ jest wielomianem nierozkładalnym nad K, czyli nie wyraża się jako iloczyn wielomianów mniejszego stopnia o współczynnikach z K.

   Dowody tych wszystkich faktów są identyczne jak poznane przez nas dowody dla liczb algebraicznych (nad $\mathbb{Q}$).

3. <u>Stopień</u> elementu algebraicznego u nad K, oznaczany $st_K(u)$, to stopień wielomianu minimalnego u nad K.

PRZYKŁAD. Liczba zespolona $i\pi$ jest elementem algebraicznym nad ciałem $\mathbb{R}$, gdyż jest pierwiastkiem wielomianu $f(x) = x^2 + \pi$. Jest to wielomian minimalny nad $\mathbb{R}$ dla tej liczby, a zatem $st_{\mathbb{R}}(i\pi) = 2$.

Def. Rozszerzeniem ciała K o element algebraiczny u nad K nazywamy najmniejsze ciało liczbowe zawierające zarówno K jak i liczbę u. OZNACZAMY je przez $K(u)$.

PRZYKŁAD. $\mathbb{R}(i\pi) = \mathbb{C}$.

TWIERDZENIE. Niech u będzie elementem algebraicznym stopnia k nad ciałem liczbowym K, i niech $f(x) = \alpha_k x^k + \dots + \alpha_1 x + \alpha_0$ będzie wielomianem minimalnym dla u nad K ($\alpha_0, \dots, \alpha_k \in K$).
Wówczas ciało rozszerzone $K(u)$ składa się z liczb postaci

$$(*) \qquad a_{k-1}u^{k-1} + a_{k-2}u^{k-2} + \dots + a_1 u + a_0$$

gdzie $a_0, a_1, \dots, a_{k-1}$ należą do K. Ponadto, przedstawienie dowolnej liczby $z \in K(u)$ w postaci $(*)$ jest jednoznaczne.

WNIOSKI.

(1) Z jednoznaczności przedstawienia liczb z $K(u)$ w postaci $(*)$ wynika, że układ elementów $1, u, \dots, u^{k-1}$ jest bazą $K(u)$ jako przestrzeni wektorowej nad K (o zbiorze skalarów K). Zatem ta przestrzeń wektorowa ma wymiar k.

(2) Z definicji, oznacza to że stopień rozszerzenia $(K(u):K)$ wynosi k, czyli $(K(u):K) = \mathrm{st}_K(u)$.

Dowód TWIERDZENIA:

Jasne jest, że liczby postaci (*) należą do najmniejszego ciała zawierającego K i u. Wystarczy więc pokazać, że liczby te tworzą ciało. W tym celu wystarczy pokazać, że suma, różnica, iloczyn i iloraz liczb takiej postaci jest też liczbą takiej postaci.

Dla sumy i różnicy jest to oczywiste.

Pokażemy tą własność dla iloczynu, a potem dla odwrotności (co razem z iloczynem oznacza zamkniętość na dzielenie).

ILOCZYN. $z = a_{k-1}u^{k-1} + \ldots + a_1 u + a_0$, $z' = b_{k-1}u^{k-1} + \ldots + b_1 u + b_0$

gdzie a_j i b_j należą do K. Ich iloczyn $z \cdot z'$, po wymnożeniu i uporządkowaniu, będzie miał postać

$$z \cdot z' = c_{2k-2}u^{2k-2} + c_{2k-3}u^{2k-3} + \ldots + c_1 u + c_0$$

gdzie współczynniki c_j wyrażają się przez a_j i b_j a więc także należą do ciała K.

Rozważmy wielomian $g(x) = c_{2k-2}x^{2k-2} + \ldots + c_1 x + c_0$.

Dzieląc go przez wielomian minimalny $f(x)$ dostaniemy iloraz $q(x)$ oraz resztę $r(x)$, które są wielomianami także o współczynnikach z K, przy czym:

- $g(x) = q(x) \cdot f(x) + r(x)$,
- stopień $r(x)$ jest $\leq k-1$, czyli $r(x) = \rho_{k-1}x^{k-1} + \ldots + \rho_1 x + \rho_0$. (bo stopień $f(x)$ to k), gdzie $\rho_0, \rho_1, \ldots, \rho_{k-1} \in K$.

Zauważmy, że wówczas

$$z \cdot z' = g(u) = q(u) \cdot \underbrace{f(u)}_{=0} + r(u) = r(u) =$$

$$= \rho_{k-1} u^{k-1} + \dots + \rho_1 u + \rho_0$$

a to jest właśnie postać (*) dla iloczynu $z \cdot z'$.

ODWROTNOŚĆ.

- Najpierw (na rozgrzewkę) pokażmy, że $\frac{1}{u}$ ma postać (*).

Skoro u jest pierwiastkiem wielomianu minimalnego $f(x)=\alpha_{k-1}x^{k-1}+\ldots+\alpha_0$,

zachodzi
$$\alpha_{k-1}u^{k-1}+\alpha_{k-2}u^{k-2}+\ldots+\alpha_1 u+\alpha_0=0. \quad (**)$$

Dzieląc obie strony przez u otrzymujemy

$$\alpha_{k-1}u^{k-2}+\alpha_{k-2}u^{k-3}+\ldots+\alpha_2 u+\alpha_1+\alpha_0\frac{1}{u}=0.$$

Współczynnik α_0 w wielomianie minimalnym jest niezerowy

(bo inaczej, dzieląc wyrażenie (**) przez u, dostalibyśmy
$$\alpha_{k-1}u^{k-2}+\ldots+\alpha_2 u+\alpha_1=0$$
i wielomian $f'(x)=\alpha_{k-1}x^{k-2}+\ldots+\alpha_2 x+\alpha_1$ miałby pierwiastek u

i stopień mniejszy od minimalnego, co jest niemożliwe).

Skoro $\alpha_0\neq 0$, wyliczamy $\frac{1}{u}$:

$$\frac{1}{u}=-\frac{\alpha_{k-1}}{\alpha_0}u^{k-2}-\frac{\alpha_{k-2}}{\alpha_0}u^{k-3}-\ldots-\frac{\alpha_2}{\alpha_0}u-\alpha_1$$

a to jest postać (*) dla $\frac{1}{u}$.

- Zauważmy, że również potęgi $\frac{1}{u^j}$ wyrażają się wtedy w postaci (*), (jako iloczyny kilku sztuk liczby $\frac{1}{u}$).

Przechodzimy do odwrotności dla ogólnej liczby $z \neq 0$

postaci $z = a_{k-1} u^{k-1} + \ldots + a_1 u + a_0$.

Skoro $z \neq 0$, przynajmniej jeden spośród współczynników a_j jest niezerowy.

Wówczas wielomian $h(x) = a_{k-1} x^{k-1} + \ldots + a_1 x + a_0$ jest wielomianem

niezerowym.

Ponieważ wielomian $f(x)$, jako minimalny, jest nierozkładalny, wielomiany $f(x)$ i $h(x)$ nie mają wspólnych dzielników, a więc są względnie pierwsze. Z algebry wielomianów wiadomo, że wówczas istnieją wielomiany $s(x)$ i $t(x)$ o współczynnikach z K takie, że

$$f(x) \cdot s(x) + h(x) \cdot t(x) = 1.$$

Podstawiając $x = u$ dostajemy

$$1 = \underbrace{f(u)}_{0} \cdot s(u) + h(u) \cdot t(u) = h(u) \cdot t(u).$$

Zatem $\frac{1}{z} = \frac{1}{h(u)} = t(u)$.

Jeśli stopień $t(x)$ jest $\leq k-1$, to $\frac{1}{z} = t(u)$ jest szukaną postacią (*) dla odwrotności $\frac{1}{z}$.

Jeśli stopień $t(x)$ jest $\geq k$, wykonujemy dzielenie $t(x)/f(x)$:

$$t(x) = q(x) \cdot f(x) + r(x), \text{ gdzie stopień } r(x) \leq k-1$$

(bo mniejszy od stopnia $f(x)$ równego k).

Wtedy $\frac{1}{z} = t(u) = q(u) \cdot \underbrace{f(u)}_{0} + r(u) = r(u)$

i $\frac{1}{z} = r(u)$ jest postacią (*) dla $\frac{1}{z}$. □

Pozostało pokazać jednoznaczność wyrażenia w postaci (*).

Załóżmy nie wprost, że pewna liczba z ma 2 różne wyrażenia w postaci (*):

$$z = a_{k-1}u^{k-1} + \dots + a_1 u + a_0 = b_{k-1}u^{k-1} + \dots + b_1 u + b_0$$

Postacie są różne, czyli dla conajmniej jednego j mamy $a_j \neq b_j$.

Wtedy:

$$0 = z - z = (a_{k-1}-b_{k-1})u^{k-1} + \dots + (a_1-b_1)u + (a_0-b_0).$$

A więc liczba u jest pierwiastkiem niezerowego wielomianu

$$(a_{k-1}-b_{k-1})x^{k-1} + \dots + (a_1-b_1)x + (a_0-b_0)$$

mającego stopień conajwyżej $k-1$, czyli mniejszy niż k.

Ale to jest niemożliwe, bo $st_K(u) = k$. (wielomian minimalny ma stopień k).

Stąd jednoznaczność postaci (*). $\square$

(B) DRUGI OGÓLNY FAKT.

OZNACZENIE. Jeśli K jest ciałem liczbowym, zaś $a_1, \ldots, a_n$ są dowolnymi liczbami zespolonymi, oznaczamy przez $K(a_1, \ldots, a_n)$ najmniejsze ciało liczbowe zawierające K oraz wszystkie liczby $a_1, \ldots, a_n$.

Z kolei, przez $K(a_1)(a_2)\cdots(a_n)$ oznaczamy ciało uzyskane przez kolejne rozszerzenia

$$K \subset K(a_1) \subset \big(K(a_1)\big)(a_2) \subset \cdots \subset \Big(\big(\big(K(a_1)\big)(a_2)\big)\cdots\Big)(a_n)$$

(kolejność przy tym jest ważna!).

LEMAT. $K(a_1, \ldots, a_n) = K(a_1)(a_2)\cdots(a_n)$.

Dowód: ciało $K(a_1)\cdots(a_n)$ niewątpliwie zawiera K, oraz wszystkie liczby $a_1, \ldots, a_n$ i dlatego jest większe niż najmniejsze ciało $K(a_1, \ldots, a_n)$ zawierające K i te liczby. Tzn.: $K(a_1, \ldots, a_n) \subset K(a_1)\cdots(a_n)$.

Dla dowodu zawierania w drugą stronę, zauważmy że skoro $K(a_1, \ldots, a_n)$ zawiera K i a_1, zachodzi $K(a_1) \subset K(a_1, \ldots, a_n)$. Skoro $K(a_1, \ldots, a_n)$ zawiera $K(a_1)$ i a_2, zachodzi $K(a_1)(a_2) \subset K(a_1, \ldots, a_n)$. Kontynuując to rozumowanie dochodzimy (w końcu) do ostatniego kroku: skoro $K(a_1, \ldots, a_n)$ zawiera $K(a_1)\cdots(a_{n-1})$ oraz a_n, zachodzi też $K(a_1)\cdots(a_{n-1})(a_n) \subset K(a_1, \ldots, a_n)$. $\square$

• rozszerzenie o pierwiastek

K ciało, $a \in K$, $p \notin K$, $p^n = a$ $(p = \sqrt[n]{a})$, $L = K(a)$

• rozszerzenie pierwiastnikowe ciała Q

$$Q = F_0 \subset F_1 \subset \dots \subset F_n = K$$

$F_i \subset F_{i+1}$ - rozszerzenia o pierwiastek

Wówczas $Q \subset K$ nazywamy rozszerzeniem pierwiastnikowym

FAKT. Liczba u wyraża się za pomocą liczb wymiernych, działań arytmetycznych i pierwiastników $\Longleftrightarrow$ u należy do (pewnego) pierwiastnikowego rozszerzenia K ciała Q.

Dowód FAKTU (szkic):

Jeśli u wyraża się poprzez liczby wymierne, działania arytmetyczne, i operacje pierwiastków, to jest dość jasne, że należy do pełnego rozszerzenia pierwiastkowego.

Np. liczba $u = \dfrac{\sqrt[4]{2} + 1/(\sqrt{3+\sqrt[3]{7}})}{2+i}$

należy do rozszerzenia pierwiastkowego

$$\mathbb{Q}(\sqrt[3]{7})(\sqrt{3+\sqrt[3]{7}})(\sqrt[4]{2})(\sqrt{-1}).$$

Z kolei, jeśli u należy do rozszerzenia pierwiastkowego,

np. $u \in \mathbb{Q}(\sqrt[k]{b})(\sqrt[m]{c})$, to:

1. $u = \alpha_{m-1}(\sqrt[m]{c})^{m-1} + \ldots + \alpha_1 \cdot \sqrt[m]{c} + \alpha_0$

gdzie $\alpha_0, \alpha_1, \ldots, \alpha_{m-1} \in \mathbb{Q}(\sqrt[k]{b})$.

2. Każdy spośród współczynników α_j jest postaci

$$\alpha_j = \beta_{j,k-1}(\sqrt[k]{b})^{k-1} + \ldots + \beta_{j,1} \cdot \sqrt[k]{b} + \beta_{j,0}$$

gdzie $\beta_{j,i-1} \in \mathbb{Q}$

3. Wstawiając wyrażenie dla α_j do wyrażenia na u z punktu 1 dostajemy:

$$u = \left(\beta_{m-1,k-1}(\sqrt[k]{b})^{k-1} + \ldots + \beta_{m-1,1} \cdot \sqrt[k]{b} + \beta_{m-1,0}\right)(\sqrt[m]{c})^{m-1} +$$

$$+ \ldots\ldots +$$

$$+ \beta_{0,k-1}(\sqrt[k]{b})^{k-1} + \ldots + \beta_{0,1} \cdot \sqrt[k]{b} + \beta_{0,0}.$$

I widać, że u wyraża się (za pomocą liczb wymiernych) przez pierwiastki. $\square$

PYTANIE. Czy każda liczba algebraiczna u wyraża się za pomocą liczb wymiernych, działań arytmetycznych i pierwiastników? Odpowiedź musiałaby być twierdząca, gdyby istniały ~~wzory za~~ pierwiastnikowe wzory na pierwiastki wielomianu dowolnego stopnia. Jeśli więc odpowiedź jest negatywna, to nie ma też pierwiastnikowych wzorów na pierwiastki dowolnych wielomianów.

ODP. JEST NEGATYWNA.

TW (Niels Henrik ABEL, 1824). Dla każdego $n \geq 5$ istnieją równania stopnia n o wymiernych współczynnikach, których pierwiastki nie wyrażają się przez pierwiastniki.

($\Longleftrightarrow$ $\forall n \geq 5$ istnieją liczby algebraiczne stopnia n nie dające się wyrazić przez pierwiastniki)

Istnieją takie równania, których pierwiastki wyrażają się przez pierwiastniki

Np. $x^n - 2 = 0$ ma pierwiastki

$$\varepsilon_n^i \cdot \sqrt[n]{2} \quad i = 0, 1, \ldots, n-1.$$

wszystkie należą do $\mathbb{Q}(\varepsilon_n)(\sqrt[n]{2})$.

Evariste GALOIS, w 1832, w pełni wyjaśnił dla jakich wielomianów nad $\mathbb{Q}$ ich pierwiastki są wyrażalne przez pierwiastniki, a dla jakich nie są.

Odpowiedź zależała od tego jak wygląda zbiór tzw. „algebraicznych symetrii" zbioru pierwiastków, zwany też „grupą algebraicznych symetrii", a jeszcze krócej, grupą Galois wielomianu.

TW (Galois). Pierwiastki wielomianu nierozkładalnego

$a_n x^n + \dots + a_0 x \in \mathbb{Q}[x]$ wyrażają się przez pierwiastniki

$\Longleftrightarrow$ grupa Galois tego wielomianu (grupa „algebraicznych symetrii" zbioru pierwiastków tego wielomianu) jest grupą „piętrowo abelową" (= rozwiązalną).

Algebraiczne symetrie zbioru pierwiastków ?

(1) pierwiastki nierozkładalnego parami różne

(2)

Algebraiczne symetrie – te permutacje zbioru pierwiastków, które zachowują algebraiczne związki pomiędzy nimi:

$v_1, \dots, v_n$ pierwiastki:

$F(x_1, \dots, x_n)$ – pewne formuły arytmetyczne n zmiennych

$\sigma \in \Sigma(v_1, \dots, v_n)$ jest algebraiczną symetrią zbioru pierwiastków

gdy dla każdej formuły F

jeśli $F(v_1 \dots v_n) = 0$ to $F(v_{\sigma(1)}, \dots, v_{\sigma(n)}) = 0$.

PRZYKŁAD. $x^n - 2 = 0$, $v_i = \varepsilon_n^i \sqrt[n]{2}$ $i = 0, 1, \dots, n-1$.

PRZYKŁADOWA FORMUŁA: $\frac{x_1}{x_0} = \frac{x_2}{x_1}$, $\frac{x_1}{x_0} - \frac{x_2}{x_1} = 0$

$$\boxed{F(x_1, \dots, x_n, \dots x_n) = \frac{x_1}{x_0} - \frac{x_2}{x_1}}$$