Przykłady

Wielomiany rozkładu koła (cyklotomiczne)

$$W_m(X) = X^m - 1 \in \mathbb{Q}[X]$$

- pierwiastki jednokrotne (m punktów na okręgu)
- $\mu_m(\mathbb{C})$ cykliczna,

$\varepsilon \in \mu_m$ generator $\Rightarrow$ ε^k generuje $\mu_m(\mathbb{C})$ $\Leftrightarrow$ $NWD(k,m)=1$

Niech $\varphi(m) = |\{k \in \mathbb{N} : 0 < k < m \text{ i } (k,m)=1\}|$ funkcja Eulera

$\mu_m(\mathbb{C})$ ma $\varphi(m)$ generatorów:

$$\varepsilon^{m_1}, \varepsilon^{m_2}, \ldots, \varepsilon^{m_{\varphi(m)}}$$

$m_1 = 1$.

Niech $F_m(X) = (X-\varepsilon^{m_1})(X-\varepsilon^{m_2})\ldots(X-\varepsilon^{m_{\varphi(m)}})$

m-ty wielomian cyklotomiczny

Uwaga 5.3 (1) $W_m(X) = F_m(X) \cdot \underbrace{\left(\prod_{\substack{d|m \\ d<m}} F_d(X)\right)}_{V_m(X)}$

(2) $F_m(X) \in \mathbb{Z}[X]$.

D-d (1) $W_m(X) = \prod_{\alpha \in \mu_m(\mathbb{C})} (X - \alpha)$

$\alpha \in \mu_m(\mathbb{C}) \Rightarrow \alpha^d = 1$ dla $d = ord(\alpha)$, $d \mid m$

Wtedy α: pierwotny pierw. z 1 stopnia d.

$$F_d(X) = \prod_{\substack{\alpha \in \mu_m(\mathbb{C}) \\ ord(\alpha) = d}} (X - \alpha)$$

(2) Indukcja względem m:

(a) $m = 1$, OK: $F_m(X) = X - 1$.

(b) Zał, że dla $d < m$ $F_d(X) \in \mathbb{Z}[X]$.

$$\underset{\mathbb{Z}[X]}{\underset{\cap}{W_m(X)}} = \underset{\mathbb{C}[X]}{\underset{\cap}{F_m(X)}} \cdot \underset{\mathbb{Z}[X]}{\underset{\cap}{V_m(X)}} \leftarrow \text{zał. indukc.}$$

w $\mathbb{C}[X]$: $V_m(X) \mid W_m(X)$, V_m, W_m: unormowane

Stąd $F_m(X) \in \mathbb{Z}[X]$.

Uwaga 5.4. $F_m(X)$ nierozkładalny w $\mathbb{Q}[X]$

(równoważnie: w $\mathbb{Z}[X]$, bo: $\mathbb{Q}$: ciało ułamków $\mathbb{Z}$, lemat Gaussa)

D-d nie wprost. A2R/3 4

Załóżmy, że w $\mathbb{Z}[X]$: $F_m = G_1 \cdot G_2$, G_1: nierozkładalny

$$0 < \deg G_i < \varphi(m) = \deg F_m.$$

(*) Istnieje ε': pierwiastek G_1 i liczba pierwsza $p \nmid m$ t. że ~~$G_2((\varepsilon')^p) = 0$~~. $G_2((\varepsilon')^p) = 0$.

bo:

Niech ε: jakiś pierwiastek G_1

Niech τ: —//— G_2.

$\tau \in \mu_m(\mathbb{C}) \Rightarrow \tau = \varepsilon^l$ dla pewnego l t. że $(l,m)=1$,
pierwotny stopnia m

$l = p_1 \cdots p_t$
iloczyn liczb pierwszych $\nmid m$

$$\underset{\substack{\uparrow \\ \text{pierwiastek } G_1}}{\varepsilon}, \ \varepsilon^{p_1}, \ \varepsilon^{p_1 \cdot p_2}, \ldots, \ \underset{\substack{\uparrow \\ \text{pierwiastek } G_2}}{\varepsilon^{p_1 \cdots p_t}}$$

$\Downarrow$

Istnieje $i < t$ t. że dla $\varepsilon' = \varepsilon^{p_1 \cdots p_i}$

ε': pierw. G_1 $\varepsilon^{p_1 \cdots p_i \cdot p_{i+1}} = (\varepsilon')^{p_{i+1}}$: pierw. G_2.

$p = p_{i+1} \nmid m$. $\square_{(*)}$

AZR/4 (4)

Tzn. ε': pierwiastek wielomianów

$\underbrace{G_1(X)}_{\text{nierozkładalny}}$ i $G_2(X^p)$ w $\mathbb{Q}[X]$

$\Rightarrow G_1(X) \mid G_2(X^p)$ w $\mathbb{Q}[X]$

i w $\mathbb{Z}[X]$

$$(+) \quad G_2(X^p) = G_1(X) \cdot H(X)$$

dla pewnego $H(X) \in \mathbb{Z}[X]$.

Niech $j : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}_p$ ilorazowe.

$$j(F_m) = j(G_1) \cdot j(G_2)$$

$$[j(G_2(X))]^p = [j(a_u)X^u + \ldots + j(a_1)X + j(a_0)]^p =$$

$G_2(X) = a_u X^u + \ldots + a_1 X + a_0$, $a_i \in \mathbb{Z}$

$$\underset{\uparrow}{=} j(a_u)^p (X^p)^u + \ldots + j(a_1)^p X^p + j(a_0)^p \underset{\uparrow}{=} j(G_2(X^p)) =$$

w $\mathbb{Z}_p(X)$ ciało char $= p$

dla $a \in \mathbb{Z}_p$ $a^p = a$

$j(a_i)^p = j(a_i)$

$$\overset{(+)}{=} j(G_1(X)) \cdot j(H(X))$$

w pierścieniu $\mathbb{Z}_p[X]$: $j(G_1)$ i $j(G_2)$ nie są względnie pierwsze, bo: $j(G_1) \mid (j(G_2))^p$.

$\Rightarrow$ w pewnym rozszerzeniu ciała $\mathbb{Z}_p$, $W_m(X)$ ma pierwiastek wielokrotny i $p \nmid m$ $\lightning$ z Uwagi 3.3(2)

Wn. 5.5.

Zał, że $\varepsilon \in \mathbb{C}$ pierwiastek pierwotny z 1 stopnia m.
Wtedy $[\mathbb{Q}[\varepsilon] : \mathbb{Q}] = \varphi(m)$. $F_m(X)$: wielomian minimalny $\varepsilon / \mathbb{Q}$.

Liczby przestępne Liouville'a:

Lemat 5.6 (Liouville) Jeśli $a \in \mathbb{R}$ algebraiczna, stopnia $N > 1$ (nad $\mathbb{Q}$), to $\exists C = C(a) > 0 \; \forall r = \frac{p}{q} \in \mathbb{Q}$

$$\left| a - \frac{p}{q} \right| \geq \frac{C}{q^n}$$

$p, q \in \mathbb{Z}$
$q \neq 0$

D-d $N > 1 \Rightarrow a \notin \mathbb{Q}$.

Niech $f(X) \in \mathbb{Z}[X]$, $f(a) = 0$, $\deg(f) = \deg(a/\mathbb{Q})$.

dla każdego $x \in \mathbb{R}$:

$\hat{f}(x) = \hat{f}(x) - \hat{f}(a) = \hat{f}'(t)(x-a)$ dla pewnego t między x i a. (tw. o wartości średniej)

Niech $\varepsilon > 0$ t. że $a \in (a-\varepsilon, a+\varepsilon)$ to jedyny pierwiastek f w tym przedziale. BSO: $f'(a) > 0$,

$C = C(a) := \min\{\varepsilon, \frac{1}{d}\}$, gdzie $d = \sup f'$ na przedziale $I := (a-\varepsilon, a+\varepsilon)$,

C: dobra

Niech $r = \frac{p}{q}$, $p, \overset{o}{\hat{q}} \in \mathbb{Z}$ $\quad f(X) = \sum_{k=0}^{N} a_k X^k$

$a_N \neq 0$

1°, $r \notin I \Rightarrow |a - p/q| > \varepsilon \geq \frac{\varepsilon}{q^n} \geq \frac{C}{q^N}$

$a_k \in \mathbb{Z}$

2°, $r \in I \Rightarrow |a - (\frac{p}{q})| = \frac{|f(\frac{p}{q})|}{|f'(t)|} \geq \frac{|f(\frac{p}{q})|}{d} \geq \frac{C}{q^n}$,

$\overset{\shortparallel}{x}$

dla pewnego
$t \in (a-\varepsilon, a+\varepsilon)$

bo: $0 \neq |f(\frac{p}{q})| = |\sum_{k=0}^{N} a_k \frac{p^k}{q^k}| = \frac{\overbrace{|\sum a_k p^k q^{N-k}|}^{\geq 1}}{q^N} \geq \frac{1}{q^N}$

i $\frac{1}{d} \geq C$

Def. 5.7. $L \supset K$ jest algebraicznym domknięciem ciała K, gdy:

(1) L jest algebraicznie domknięte i

(2) Rozszerzenie $K \subset L$ jest algebraiczne
($\forall a \in L$ a algebraiczny nad K).

L oznaczamy przez $\hat{K}$, K^{alg}.

Wn. 5.8. $\hat{K}$ istnieje.

<u>D-d</u> Niech $K_\infty \supset K$ ciało algebraicznie domknięte, rozszerzenie ciała K (tw. 2.3)

$$\hat{K} = K_{alg}(K_\infty) = \{a \in K_\infty : a \text{ algebraiczny}/K\}$$

(a) $\hat{K}$ algebraicznie domknięte

(bo: $f(X) \in \hat{K}[X]$, $\deg > 0$ $\Rightarrow$ f ma pierwiastek a w K_∞ $\overset{5.2}{\Rightarrow}$ $a \in \hat{K}$)

b) $K \subset \hat{K}$ algebraiczne rozszerzenie ciał: z definicji

Tw. 5.9. Algebraiczne domknięcie ciała K jest jedyne z dokł. do $\cong_K$. Tzn: $L_1, L_2 \supset K$ algebr. domknięcia K $\Rightarrow$

$$\exists f : L_1 \cong_K L_2$$

<u>D-d.</u> Niech $\mathcal{K} = \{(K', f') : K \subseteq K' \subseteq L_1$ i $f' : K' \to L_2$ monomorfizm t. że $f'\restriction_K = id_K\}$

Porządek na $\mathcal{K}$: $(K', f') \leq (K'', f'') \Leftrightarrow K' \subseteq K''$ & $f' \subseteq f''$.

$\mathcal{K}$ spełnia założenia lematu Zorna.

Niech $(K_1, f_1) \in \mathcal{K}$: element maksymalny.

Pokażemy, że $K_1 = L_1$.

nie wprost:

$a_1 \in L_1 \setminus K_1$ $\quad$ $W_1(X) \in K_1[X]$ wielomian minimalny a/K_1

$$\cong_K \downarrow f_1 \qquad \downarrow f_1$$

$L_2 \supseteq K_2 = f_1[K_1]$ $\quad$ $W_2(X) \in K_2[X]$ wiel. nierozkładalny

Niech $a_2 \in L_2$ pierw. W_2.

$$K_1(a_1) = K_1[a_1] \cong K_1[X]/(W_1) \cong K_2[X]/(W_2) \cong$$

$$\cong K_2[a_2] = K_2(a_2).$$

Dostajemy $f_2 \supseteq f_2' : K_1(a_1) \xrightarrow[\cong_K]{} K_2(a_2)$ $\not$ z maksymalności (K_1, f_1),

---

$K_1 = L_1 \Rightarrow K_1 \subseteq K_2 \subset L_2$

$K_1 \cong_K K_2$ $\qquad$ K_1: alg. domknięte $\Rightarrow$

K_2: alg. domknięte i

$K_2 \subset L_2$: algebraiczne $\Rightarrow K_2 = L_2$

(bo: $a \in L_2 \setminus K_2 \Rightarrow$ wiel. minimalny $f_a(X) \in K_2[X]$ a/K_2 nierozkładalny $\Rightarrow$ $\deg f_a = 1 \Rightarrow a \in K_2$.

Wn. 5.10 $K \underset{f}{\cong} L$ ciała $\Rightarrow \hat{K} \cong \hat{L}$ ($f \subseteq f'$)

Wn. 5.11. Jeśli $K \underset{alg}{\subset} L$, to $\exists f : L \longrightarrow \hat{K}$ $f|_K = id$.
zanurzenie ciał

Rozszerzenia algebraiczne.

K ciało $K \subset \hat{K}$ alg. domknięcie K.

$K \subset L$: rozszerzenie algebraiczne ciał.

Def. $G(L/K) = \{ f \in Aut(L) : f|_K = id_K \} < Aut(L)$

grupa Galois rozszerzenia $K \subset L$

$Gal(L/K)$

$(Aut(L/K))$

Idea: badać rozszerzenia $K \subset L$ przez badanie $G(L/K)$.

Przykład. (1) K ciało proste $\Rightarrow G(L/K) = Aut(L)$

(bo: $f \in Aut(L) \Rightarrow f|_K = id_K$)

(2) $G(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = Aut(\mathbb{Q}(\sqrt{2})) = \{f_0, f_1\} \cong \mathbb{Z}_2$

$f_0 = id$, $f_1 : \mathbb{Q}[\sqrt{2}] \longrightarrow \mathbb{Q}[\sqrt{2}]$

$f_1(\sqrt{2}) = -\sqrt{2}$

Def. $G(\hat{K}/K)$ = „absolutna grupa Galois ciała K".

Problem. (Odwrotny problem Galois)
(inverse Galois problem)

Czy każda grupa skończona jest $\cong G(L/\mathbb{Q})$?
dla $\mathbb{Q} \underset{alg}{\subset} L$?

(Otwarty, główny problem teorii Galois)

Uwaga 6.1 (jednorodność $\hat{K}$).

$a, b \in \hat{K}$, $I(a/K) = I(b/K) \Longrightarrow \exists f \in G(\hat{K}/K)$
$f(a) = b$

D-d

$$\begin{tikzcd}
K[a] \arrow[r, "f", "\cong_K"'] \arrow[d, phantom, "\cap"] & K[b] \arrow[d, phantom, "\cap"] \\
\hat{K} \arrow[r, "f'", "\cong"'] & \hat{K}
\end{tikzcd}$$

na mocy Wn. 5.10

$\hat{K} = \widehat{K[a]} = \widehat{K[b]}$.

$\hat{K}$: "największe" algebraiczne rozszerzenie ciała K:

$K \underset{alg}{\subset} L \overset{5.11}{\Longrightarrow} \exists f : L \longrightarrow \hat{K}$ ~~zanu~~ monomorfizm ciał, $(f|_K = id)$ $(*)$

Def. Rozszerzenie algebraiczne ciał $K \subset L$ jest **normalne**, gdy w $(*)$: $f[L] \subseteq \hat{K}$ to samo dla wszystkich f.

Przykład $K \subset \hat{K}$ jest normalne.

Uwaga 6.2. ($K \subset L \subset \hat{K}$).

$K \subset L$ normalne $\iff \forall f \in G(\hat{K}/K)\ f[L] = L$.

D-d. $\Rightarrow$ z definicji $\Leftarrow$: też.

Wn. $K \subseteq L_1 \subseteq L$, $\underset{\text{normalne}}{K \subseteq L} \Rightarrow \underset{\text{normalne}}{L_1 \subseteq L}$.

TW. 6.3. $K \underset{\text{alg.}}{\subset} L$ jest normalne $\iff$

$\forall b \in L$ $\underset{\text{wiel. minimalny } b/K}{W_b(X) \in K[X]}$ ~~nie~~ rozkłada się w $L[X]$ na iloczyn czynników liniowych

D-d.

Bso $K \subset L \subset \hat{K}$.

$\Rightarrow$ nie wprost. $b \in L$ i $W_b(X)$ ma pierwiastek $a \in \hat{K} \setminus L$.

Uwaga 6.1 $\rightsquigarrow$ $\exists f \in G(\hat{K}/K)$
$f(b) = a$ $\Rightarrow f[L] \neq L$ $\because$
$\quad\ \ \ni a \qquad \not\ni a$

$\Leftarrow$ nie wprost.

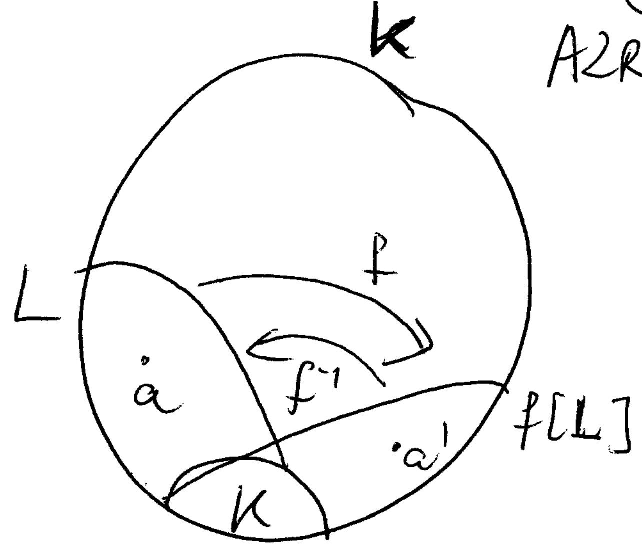
Niech $f \in G(\hat{K}/K)$, (t. że) $f[L] \neq L$.

Niech $a \in L \setminus f[L]$ (symetrycznie: $a' \in f[L] \setminus L$, analogiczne rozumowanie)

Niech $W_a(X)$: wiel. minimalny a/K

$\Downarrow$ $f|_K = id_K$

$W_a(X) = f(W_a(X))$: wiel minimalny b/K (dla $b = f(a)$)



$K \subset L$ normalne

$\Updownarrow$

$K \subset f[L]$ normalne

~~$L/K \cong$~~

$L \overset{f}{\cong}_K f[L]$

$\Downarrow$

$W_a(X)$ rozkłada się nad $f[L]$ na czynniki liniowe,

sprzeczność, bo: a pierwiastek $W_a(X)$, $a \notin f[L]$.