Wykład 9.

Przykład. 1) $S_n := \mathrm{Sym}(\{X_1, \dots, X_n\})$

$L := K(X_1, \dots, X_n)$

$M = K(X_1, \dots, X_n)^{S_n}$, $S_n < \mathrm{Aut}(L)$ skończona.

z tw. Artina:

$M \subset L$: rozszerzenie Galois oraz $S_n = G(L/M)$

- gdy $n \geq 5$, S_n nie jest rozwiązalna, więc:

$M \subset L$ też nie jest rozwiązalne.

L: ciało rozkładu wielomianu

$$M[T] \ni W(T) = (T - X_1)(T - X_2) \dots (T - X_n) =$$

$$= T^n - \sigma_1(\bar{X}) T^{n-1} + \sigma_2(\bar{X}) T^{n-2} + \dots + (-1)^{n-1} \sigma_{n-1}(\bar{X}) T + (-1)^n \sigma_n(\bar{X}),$$

gdzie $\sigma_i(\bar{X}) = \sum_{1 \leq j_1 < \dots < j_i \leq n} X_{j_1} X_{j_2} \dots X_{j_i}$

(wzory Viete'a). $\sigma_i(\bar{X}) \in M = L^{S_n}$.

$\sigma_i(\bar{X})$: bazowe funkcje symetryczne.

2) Gdy $K \subset L$ rozszerzenie ciał ~~rozz~~ oraz

L: ciało rozkładu nad K wielomianu $W(X)$ stopnia ≤ 4,

to $G(L/K) \hookrightarrow S_4$; rozwiązalna.

[<u>Fakt</u>. Podgrupa grupy rozwiązalnej jest rozwiązalna

więc wtedy równanie "$W(X)=0$" jest rozwiązalne przez pierwiastniki

bo: Niech $M = L^{G(L/K)}$. Wtedy z tw. Artina:

$$K \subset M \subset L, \quad G(L/M) = G(L/K)$$

↑ ↑ radykalne Galois (z faktu 7.4)

$$\Downarrow$$

$$\cancel{G(M/K) = \{id_K\}}$$

$$\Downarrow$$

oraz $M \subset L$: rozszerzenie ~~przez~~ pierwiastnikowe,

tzn. $L \subseteq L_0 \supseteq L_1 \supseteq \ldots \supseteq L_k = M$

rozszerzenia o pierwiastki

(*) $X^n - a$ $(p \nmid n)$

(**) $X^p - X - a$

<u>Więc</u> wszystkie pierwiastki $W(X)$ dają się wyrazić nad K poprzez stosowanie działań ciała (włączając dzielenie, odejmowanie) oraz "pierwiastkowanie", tj. branie rozwiązań (*), (**)

- Gdy ~~det~~ $\deg W = 5$, tak być nie musi (Zadanie z listy 6 ? lub 7 ?)

<u>Fakt</u> $K(\sigma_1, \ldots, \sigma_n) = K(X_1, \ldots, X_n)^{S_n}$.

<u>D-d</u> $\subseteq$: jasne

$\supseteq$: $K(\vec{\sigma}) \subseteq K(\vec{X})^{S_n} \subseteq K(\vec{X})$

$$n! = [K(\bar{X}) : K(\bar{X})^{S_n}] \leq [K(\bar{X}) : K(\vec{\sigma})] \leq n!$$

bo $K(\bar{X})$: ciało rozkładu wielomianu $W(T) = (T - X_1) \ldots (T - X_n)$ nad $K(\sigma)$.

stąd $=$ i $K(\vec{\sigma}) = K(\bar{X})^{S_n}$.

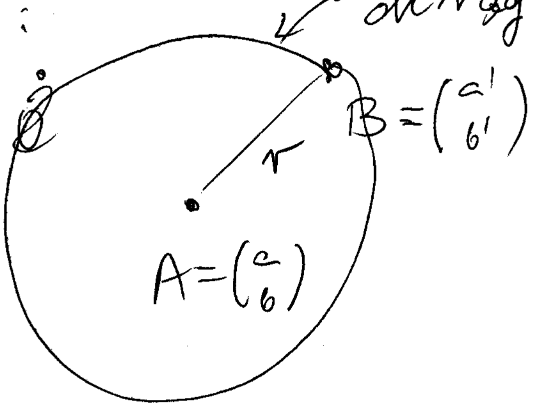
<u>Uwaga.</u> Można pokazać, że $K[\sigma_1, \ldots, \sigma_n] = K[X_1, \ldots, X_n]^{S_n}$. (podstawowe tw. o wielomianach symetrycznych).

Zastosowanie: Konstrukcje przy pomocy cyrkla i linijki:

• ~~cyrkiel~~ Dane punkty $A \neq B \in \mathbb{R}^2$

cyrkiel: okrąg : $\left\{ \binom{x}{y} : (x-a)^2+(y-b)^2=r^2 \right\}$,

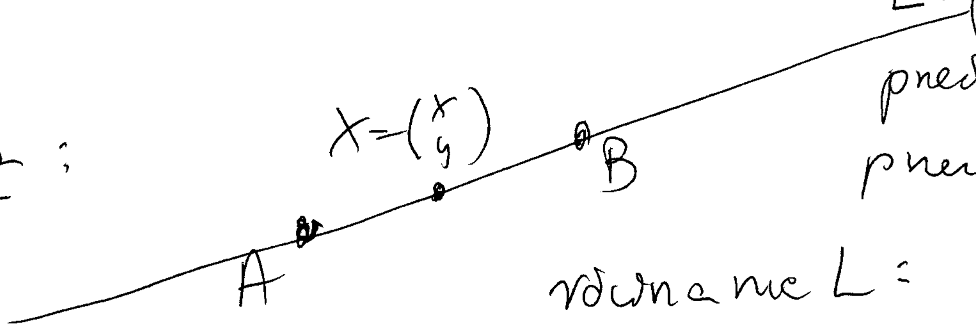
school compass



$$r=\sqrt{(a'-a)^2+(b'-b)^2}$$

• linijka : ruler

L: prosta przechodząca przez A i B



równanie L:

$$\begin{vmatrix} x-a & a'-a \\ y-b & b'-b \end{vmatrix}=0$$

Niech $(a_1,b_1),\dots,(a_n,b_n)\in\mathbb{R}^2$.

<u>Fakt</u> Punkt $(a,b)\in\mathbb{R}^2$ jest konstruowalny (przy pomocy cyrkla i linijki) na płaszczyźnie $\mathbb{R}^2$ z punktów $(a_1,b_1),\dots,(a_n,b_n)$ i punktów $(0,1)$, $(1,0)$ $\iff$ rozszerzenie ciał $K\subset K(a,b)$ ~~R~~ jest rozszerzeniem przez pierwiastniki stopnia ≤ 2 $(X^2-\alpha)$

tu: $K=\mathbb{Q}(a_1,b_1,\dots,a_n,b_n)$.

(a) Kwadratura koła:

Dane koło o promieniu 1 : punkt $(0,1)$.

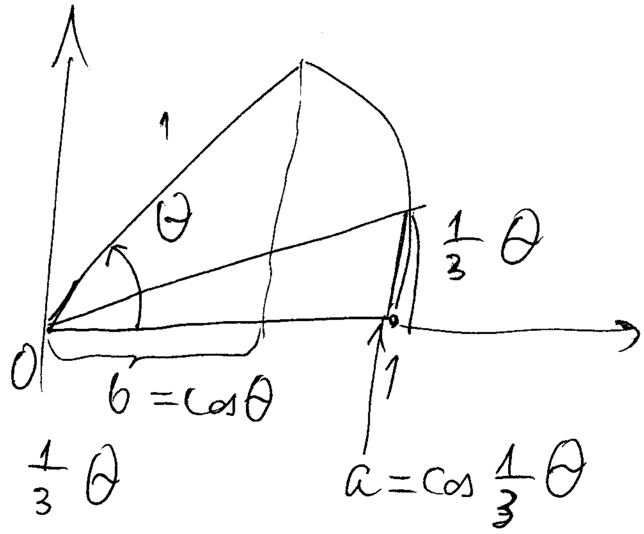
szukany : kwadrat o polu π = polu tego koła

równoważnie : punkt $(0,\sqrt{\pi})$.

Ale : π : przestępna, więc $\sqrt{\pi}$ też : niemożliwe.

(b) Trysekcja kąta:

Dany kąt $0 < \theta < \pi$



Cel: skonstruować kąt $\frac{1}{3}\theta$

a algebraiczne nad $\mathbb{Q}(b)$:

$$4a^3 - 3a - b = 0$$

Niemożliwe, gdy $[\mathbb{Q}(a,b) : \mathbb{Q}(b)] = 3$.

(c) Podwojenie sześcianu o krawędzi jednostkowej :

równoważnie : skonstruowanie $(0,a)$, gdzie $a^3 = 2$

też niemożliwe...

Rozszerzenia przestępne ciał.

$K \subset L$ rozszerzenie ciał

Def (1) $K \subset L$: przestępne, gdy

$\exists a \in L$ a przestępny nad K (tzn. $I(a/K) = \{0\}$)

(2) $K \subset L$: czysto przestępne, gdy $\forall a \in L \setminus K$

a/K : przestępny

Uwaga 10.1. a/K : przestępny $\iff K(a) \cong K(X)$

D-d ćw.

Niech $U = \hat{U}$: (duże) ciało, oraz : $K \subset U$ podciało

$F \subset K$ podciało proste

Def (1) $acl_K : P(U) \longrightarrow P(U)$: operator algebraicznego domknięcia nad K

$U \supseteq A \rightsquigarrow acl_K(A) = K(A)^{alg} \subseteq U$.

(2) $A \subseteq U$ jest algebraicznie domknięty nad K, gdy

$$A = acl_K(A)$$

Własności

1. $acl_K(\emptyset) = \hat{K}$

2 (i) $A \subseteq B \Rightarrow acl_K(A) \subseteq acl_K(B)$ (monotoniczność)

(ii) $A \subseteq acl_K(A)$

(iii) (idempotentność) $acl_K(acl_K(A)) = acl_K(A)$.

tzn: acl_K operator domknięcia.

3. $acl_K(A) = \bigcup_{A_0 \subset A \text{ skońn.}} acl_K(A_0)$ (skończony charakter)

4. (własność wymiany)

$a \in acl_K(A \cup \{b\}) \setminus acl_K(A) \Rightarrow b \in acl_K(A \cup \{a\})$.

<u>D-d</u> 3. $acl_K(A) = K(A)^{alg} = \bigcup_{A_0 \subset_{sk} A} K(A_0)^{alg}$

$\subseteq$:

$b \in K(A)^{alg} \Rightarrow$ istnieje $W(X) \in K(A)[X]$
t.że $W(b)=0$ i $W \neq 0$

W ma współczynniki w $K(A_0)$ dla pewnego skończonego $A_0 \subset A$

Wtedy $b \in K(A_0)^{alg}$.

4. • $a \notin \underbrace{K(A)^{alg}}_{=L} \Rightarrow b \notin K(A)^{alg}$ (bo: $b \in K(A)^{alg}$

$\Downarrow$

$a \in K(A,b)^{alg} = K(A)^{alg}$)

• $a \in K(A,b)^{alg} = L(b)^{alg}$.

tzn: b przestępny / L
i $L(b) \cong L(Y)$

tzn. istnieje $W(X) \in L[X]$, $W(a)=0$ i ~~deg~~ $\deg W > 0$, AlZR/9

bzo: $W(X) \in L[b][X]$

(bo: $L(b)$: ciało ułamków pierścienia $L[b]$)

$W(X) = \underset{\neq 0}{c_n} X^n + \ldots + c_1 X + c_0$,

~~$c_i \in$~~ $c_i \in L[b]$, tzn. $c_i = V_i(b)$, $V_i \in L[y]$

Niech $V(y) = V_n(y) \cdot a^n + \ldots + V_1(y) \cdot a + V_0(y)$

$\cap$

$L[a](y)$.

- $V(b) = 0$
- $V \neq 0$ (ćwiczenie)

$\Rightarrow b \in ad_K(A \cup \{a\}) = L(a)^{alg}$,

<u>Def.</u> (1) $A \subset U$ jest algebraicznie niezależny nad K, ~~g~~

gdy $\forall a \in A \quad a \notin ad_K(A \setminus \{a\})$

[równoważnie: $\forall_n \forall \, a_1, \ldots, a_n \in A$ różnych $\forall \, \underset{\neq 0}{W(X_1, \ldots, X_n)} \in K[\bar{X}]$ $W(\bar{a}) \neq 0$] (zadanie)

(2) A jest bazą przestępną zbioru $B \subset U_k$ nad K,

gdy $\begin{cases} A \text{ jest algebraicznie niezależny nad } K \\ A \subseteq B \subseteq ad_K(A). \end{cases}$

(3) $\underbrace{\operatorname{trdeg}_K(B)}$ = moc jakiejkolwiek bazy przestępnej zbioru B nad K,
wymiar przestępny B nad K.

• gdy $K = F$ ~~p~~ ciało proste, pomijamy je
w ~~acl~~ acl_K, trdeg_K, "baza przestępna nad K"
"algebraicznie niezależny nad K"

TW. 10.2. (1) Jeśli $A \subseteq B \subseteq U$ i A jest algebraicznie niezależny nad K, to $\exists A'$: baza przestępna B nad K, $A \subseteq A' \subseteq B$.

(2) Każde dwie bazy przestępne zbioru B nad K są równoliczne.

D-d ćwiczenie (patrz dowód dla operatora Lin w przestrzeni liniowej)

Przykład 1) Niech K ciało, X_i, $i \in I$: zmienne, oraz $U = K(X_i : i \in I)^{alg}$. Wtedy $\{X_i : i \in I\} \subseteq U$ algebraicznie niezależny /K i $\operatorname{trdeg}_K(U) = |I|$.

(2) Jeśli $K \subset L \subset U$ oraz $\{a_i : i \in I\}$: baza przestępna L/K,
to : (a) $K(a_i : i \in I) \underset{K}{\cong} K(X_i, i \in I)$

(b) $K \subseteq K(a_i, i \in I) \subseteq L$.
czysto przestępne, algebraiczne