Wykład 2.

<u>Def.</u> Ciało L jest <u>algebraicznie domknięte</u>, gdy każdy $f \in L[X]$ stopnia >0 ma pierwiastek w L.

<u>Przykład</u> $\mathbb{C}$ tak, $\mathbb{R}$ nie, bo: x^2+1 nie ma pierwiastka w $\mathbb{R}$.

$\mathbb{Q}$ też nie

$\mathbb{Q}[i]$ nie, bo: X^2-2 nie ma pierwiastka w $\mathbb{Q}[i]$.

TW. 2.3. Każde ciało K zawiera się w pewnym ciele algebraicznie domkniętym.

<u>D-d</u>

$(*)$ $\forall K\ \exists L \supset K\ \forall f \in K[X]$, $\deg f > 0$, f ma pierwiastek w L

<u>d-d</u>.

Niech $\{f_\alpha : \alpha < \varkappa\} = \{f \in K[X] : \deg f > 0\}$

Konstruujemy rosnący łańcuch ciał K_α, $\alpha < \varkappa$ t.że:

(1) $K \subseteq K_\alpha \subseteq K_\beta$ dla $\alpha < \beta < \varkappa$

(2) f_α ma pierwiastek w ciele $K_{\alpha+1}$.

Konstrukcja przez indukcję pozaskończoną.

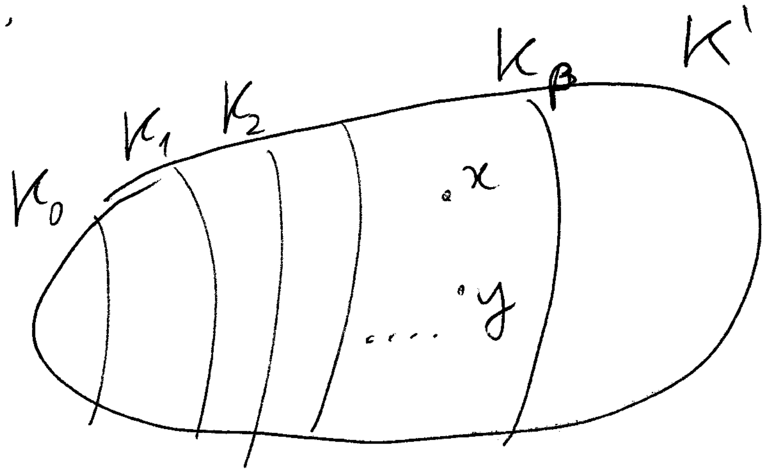
- $K_0 = K$
- krok indukcyjny: Załóżmy, że $\alpha < \varkappa$ i mamy już K_β dla wszystkich $\beta < \alpha$.

Niech $K' = \bigcup_{\beta<\alpha} K_\beta$. K': ciało, bo:

Przypadek (a) $\underline{\alpha = \beta + 1}$. Wtedy $K' = K_\beta$ OK.

Przyp. (b) α: graniczna l. porządkowa (np. $\alpha = \omega$ lub $\alpha = 2\omega^2 + \omega$)

$K' = \bigcup_{\beta<\alpha} K_\beta$ jako zbiór.



działania w K':
niech $x, y \in K'$.
Istnieje $\beta < \alpha$ t. że $x, y \in K_\beta$.

Określamy: $x + y$ = "$x+y$ liczone w K_β"
$x \cdot y$ = "$x \cdot y$ liczone w K_β".

- wynik nie zależy od wyboru β
- $(K', +, \cdot)$: ciało t. że $K_\beta \subset K'$ rozszerzenie ciał dla każdego $\beta < \alpha$

definiujemy
$K_\alpha := K'$ (w przypadku (b)).

Powrót do przypadku (a): $\alpha = \beta + 1$

$K' = K_\beta$. Na mocy Wniosku 1.7

istnieje ciało $K_\alpha \supset K_\beta$ t. że

f_β ma pierwiastek w K_α. $\cancel{(*)}$

$L := \bigcup_{\alpha < \varkappa} K_\alpha$

szukane ciało $\square_{(*)}$

d-d tw. 2.3.

Konstruujemy rosnący ciąg ciał L_n, $n = 0, 1, 2, \dots$

z $(*)$

(a) $L_0 = K$

(b) $L_{n+1} \supseteq L_n$ t. że $\forall f \in L_n[X]$, $\deg f > 0$, f ma pierwiastek w L_{n+1}.

Niech $L_\infty = \bigcup_{n<\omega} L_n$.

ciało algebraicznie domknięte, $K \subseteq L_\infty$

bo: niech $f \in L_\infty[X]$, $\deg f > 0$.

$\Rightarrow$ $f \in L_n[X]$ dla pewnego $n \in N$

$\underset{(b)}{\Longrightarrow}$ f ma pierwiastek w $L_{n+1} \subseteq L_\infty$.

Elementarz ciał:

$K \subseteq L$ rozszerzenie ciał.

Uwaga 3.0. (1) $0_K = 0_L$, $1_K = 1_L$ (bo: $(K,+) < (L,+)$
$(K^*,\cdot) < (L^*,\cdot)$)

(2) dla $x \in K$: $\underset{\text{w } K}{-x} = \underset{\text{w } L}{-x}$, $\underset{\text{w } K}{x^{-1}} = \underset{\text{w } L}{x^{-1}}$, gdy $x \neq 0$.

Def. Ciało K jest <u>proste</u>, gdy nie zawiera podciał właściwych.

Przykład: $\mathbb{Q}$, (char $=0$), $\mathbb{Z}_p$ (p: l. pierwsza, char $=p$).

Uwaga 3.1. (1) Każde ciało zawiera jedyne podciało proste.

(2) $\mathbb{Q}$, $\mathbb{Z}_p$ (p pierwsze) to wszystkie (z dokł. do $\cong$) ciała proste.

<u>Przykład</u>. Zał., że K: skończone. Wtedy K^* też, rzędu n $(=p^k-1)$ $\Rightarrow \forall x \in K^*\ x^n = 1$

pierwiastek z 1 !

Pierwiastki z 1:

Def. (1) $a \in R$ jest pierwiastkiem z 1 (stopnia $n>0$), gdy $a^n = 1$.

(2) $\mu_n(R) = \{a \in R : a^n = 1\}$

(3) $\mu(R) = \{a \in R : \exists n>0\ a^n = 1\} = \bigcup_{n>0} \mu_n(R)$.

(4) a jest pierwiastkiem pierwotnym (primitive) stopnia n z 1, gdy $a^n = 1$ i n najmniejsze takie >0.

Uwaga 3.2. (1) $\mu_n(R) < R^*$ (2) $\mu(R) < R^*$ (tzn. to są podgrupy grupy R^*).

(3) $\mu(R)$: torsyjna grupa abelowa.

Przykład.

$$\mu(\mathbb{C}) = \bigcup_{n>0} \mu_n(\mathbb{C}) < \{z \in \mathbb{C} : |z| = 1\} < \mathbb{C}^*$$

nieskończona

$$\mu(\mathbb{R}) = \{\pm 1\} \cong \mathbb{Z}_2 .$$

$$\mu_8(\mathbb{C}) = \{\cos\frac{2k\pi}{8} + i\sin\frac{2k\pi}{8} : k = 0, \dots, 7\}$$

$$\vee$$

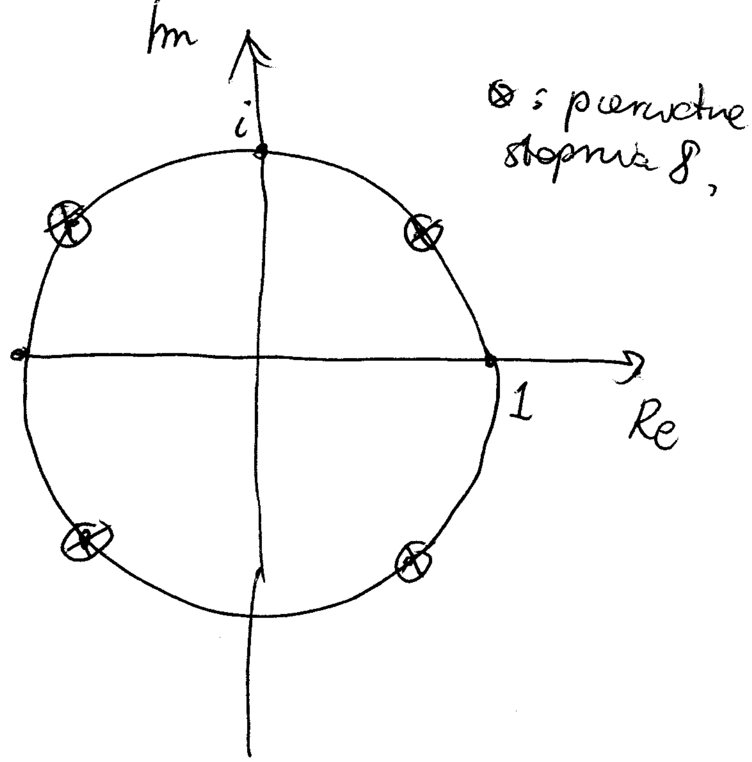
$$\mu_4(\mathbb{C}) = \{\pm 1, \pm i\}$$

$$\vee$$

$$\mu_2(\mathbb{C}) = \{\pm 1\}$$

$$\vee$$

$$\mu_1(\mathbb{C}) = \{1\}$$



$\mu_n(K) = \{$zera wielomianu $\underbrace{X^n - 1}_{W_n(X)}\}$

Uwaga 3.3. (1) $\operatorname{char} K = 0 \Rightarrow W_n(X)$ ma tylko pierwiastki jednokrotne,

(2) $\operatorname{char} K = p$, $n = p^l \cdot n_1$, $p \nmid n_1 \Rightarrow$ wszystkie pierwiastki $W_n(X)$ mają krotność p^l.

D-d. (1) Zał. że $a \in K$ pierwiastek $W_n(X)$.

$$W_n(X) = X^n - 1 = X^n - a^n = (X - a)(\underbrace{X^{n-1} + aX^{n-2} + \dots + a^{n-2}X + a^{n-1}}_{V_n(X)})$$

$V_n(a) = n \cdot a^{n-1} \neq 0$ (char $K \neq 0$),

więc a: jednokrotny.

(2) $W_n(X) = X^n - 1 = X^n - 1^n = (X^{n_1})^{p^l} - (1^{n_1})^{p^l} =$

$\boxed{n = p^l \cdot n_1}$ $= (X^{n_1} - 1)^{p^l} = \underbrace{W_{n_1}(X) \cdot \ldots \cdot W_{n_1}(X)}_{p^l}$

char $= p$

Zał, że $a \in K$ pierwiastek $W_n(X)$. Wtedy a: pierw. $W_{n_1}(X)$.

$W_{n_1}(X) = (X-a)\, V_{n_1}(X)$ (jak w (1))

$\cancel{V_{n_1}(X)}$ $V_{n_1}(a) = n_1 a^{n-1} \neq 0$, bo $p \nmid n_1$

Dlatego: a: 1-krotny pierw. $W_{n_1}(X) \Rightarrow p^l$-krotny pierw. $W_n(X)$.

TW. 3.4. Zał, że $G < \mu(K)$ grupa skończona rzędu n. Wtedy $G = \mu_n(K)$, G: cykliczna i $p \nmid n$ (gdy char $K = p$).

<u>D-d.</u> • dla $x \in G$, $x^n = 1$, więc $G \subseteq \mu_n(K)$.

• $|\mu_n(K)| \leq n$ (bo $W_n(X)$ ma $\leq n$ pierwiastków)

$\Downarrow$

$G = \mu_n(K) \Rightarrow W_n(X)$ ma n różnych pierw. w K

$\Rightarrow$ wszystkie jednokrotne $\overset{}{\underset{3.3}{\Rightarrow}} p \nmid n$.

Wystarczy pokazać, że $\cancel{\forall}$ $\exists x \in G$ $\operatorname{ord}(x) = n$.

<u>nie wprost</u>

Zał. że $\forall x \in G$ $ord(x) < n$.

Niech $k = \max\{ord(x) : x \in G\}$ Niech $x \in G$ t. że $ord(x) = k$

(*) $\forall y \in G$ $ord(y) \mid k$.

bo: jeśli dla pewnego $y \in G$, $\underset{\overset{\parallel}{l}}{ord(y)} \nmid k$, to niech

$w = NWD(l, k)$

wtedy $ord(y^w) = \frac{l}{w} > 1$ i $\frac{l}{w}, k$: względnie pierwsze.

Stąd: $ord(y^w \cdot x) = \frac{l}{w} \cdot k > k$ ↯

(*) $\Rightarrow$ $\forall y \in G$ $y^k = 1$, więc $G \subseteq \mu_k(K)$ i $|G| \leq k$ ↯.

Wn. 3.5. Niech $a \in \mu_n(K)$, wtedy:

~~Jeśli~~ a : pierwiastek pierwotny stopnia $n \geq 1$ $\Rightarrow$

a : generuje $\mu_n(K)$.

<u>D-d.</u> $\Rightarrow$: $|\mu_n(K)| \leq n$

$\langle a \rangle = \{\underbrace{1, a, \dots, a^{n-1}}_{\text{parami } \neq}\} \subseteq \mu_n(K) \Rightarrow \mu_n(K) = \langle a \rangle$.

Tw. 3.6. (K : ciało skończone)

(1) $|K| = p^n$ dla pewnego $n > 0$, gdzie $p = char\, K$,

(2) Dla każdego $n > 0$ istnieje dokładnie jedno ciało K mocy p^n (z dokł. do $\cong$).

D-d (1) $K \supseteq K_0 \cong \mathbb{Z}_p$
podciało proste

K: przestrzeń liniowa nad $\mathbb{Z}_p$, $\dim_{\mathbb{Z}_p} K = n < \infty$

$\Rightarrow K \cong (\mathbb{Z}_p)^n \Rightarrow |K| = p^n$.

(2) Niech $L \supseteq \mathbb{Z}_p$: ciało rozkładu wielomianu $W_{p^n-1}(X)$ nad $\mathbb{Z}_p$

$p \nmid p^n - 1 \Rightarrow W_{p^n-1}(X)$ ma tylko pierwiastki 1-krotne, w liczbie p^n-1 w L.

$K = \{0\} \cup \{\text{pierwiastki } W_{p^n-1}(X) \text{ w } L\}$
$\cap|$
L

- $|K| = p^n$
- K podciało ciała L

bo: dla $x \in L$:

$x \in K \Leftrightarrow x = 0 \lor x^{p^n-1} = 1$

$\Leftrightarrow x^{p^n} = x$

$\Leftrightarrow x \in Fix(Fr^n)$, gdzie $Fr: L \to L$ funkcja Frobeniusa $Fr(x) = x^p$.

Ćw:
Jeśli F: ciało i $\overset{\neq 0}{\varphi}: F \to F$ endomorfizm, to $Fix(\varphi) = \{x \in F : \varphi(x) = x\}$: podciało.

Stąd: $\underset{K}{\overset{\shortparallel}{Fix(Fr^n)}}$ ciało więc $|L| = p^n$.

Jedyność. Zał., że L': ciało mocy p^n.

Stąd: $char\, L' = p$ oraz $(\forall x \in L')$
bso $\mathbb{Z}_p \subseteq L'$ $(x = 0 \lor x^{p^n - 1} = 1)$

stąd $L' = \{0\} \cup \{$pierwiastki $W_{p^n-1}(X)$ w $L'\}$

więc L': ciało rozkładu wielomianu $W_{p^n-1}(X)$ nad $\mathbb{Z}_p$.

$\Downarrow$ Wn. 2.1(2)

$L \cong L'$.