16: Spis definicji i ważniejszych twierdzeń

Rozwiązanie ogólne układu $U = (f_1, ..., f_m)$ to $\bar{a} = (a_1, ..., a_n)$ takie, że $I(\bar{a}/R) = (f_1, ..., f_m)$, gdzie $f_i \in R[x_1, ..., x_n]$ oraz $\bar{a} \in S^n$, gdzie $S \supseteq R$.

Niech $\bar{a}_i \in L_i \supseteq K$ $(i = 1, 2)$. Wtedy $I(\bar{a}_1/K) = I(\bar{a}_2/K) \iff (\exists\ \phi : K[\bar{a}_i] \to K[\bar{a}_2])\ \phi \restriction K = id_K$ i $\phi(\bar{a}_1) = \bar{a}_2$.

Ciała L_1 i L_2 są izomorficzne nad K, gdzie $K \subseteq L_i$, wtw. istnieje izomorfizm $f : L_1 \to L_2$ taki, że $f \restriction K = id_K$.

$L \supseteq K$ jest ciałem rozkładu nad K wielomianu $f \in K[x]$ jeśli:

1. f rozkłada się w L[x] na czynniki liniowe
2. L jest rozszerzeniem K o wszystkie pierwiastki f.

Ciało rozkładu wielomianu jest *jedyne z dokładnością do izomorfizmu nad K*.

Ciało algebraicznie domknięte to ciało L takie, że każdy $f \in L[x]$ o stopniu > 0 posiada w L pierwiastek (każdy wielomian rozkłada się na czynniki liniowe).

Ciało proste nie zawiera żadnego właściwego podciała.

Pierwiastki z jedności:

1. $a \in R$ jest pierwiastkiem z jedności stopnia n jeśli $a^n - 1 = 0$
2. $\mu_n(R) = \{a \in R : a^n - 1 = 0\}$ jest **grupą pierwiastków z 1 stopnia n**
3. $\mu(R) = \{a \in R : (\exists\ n) a^n - 1 = 0\} = \bigcup \mu_n(R)$ jest grupą pierwiastków z 1. Jest to torsyjna grupa abelowa i jest podgrupą R^*
4. a jest **pierwiastkiem pierwotnym** stopnia n z 1 jeśli $a \in \mu_n(R)$ i dla każdego $k < n$ $a \notin \mu_k(R)$.

Element a jest algebraiczny jeśli istnieje $f \in K[x]$ taki, że $f(a) = 0$.

Jeśli a jest algebraiczny nad K, to $K[a] = K(a)$, tzn. K[a] jest ciałem.

Element a jest przestępny jeśli dla każdego $f \in K[x]$ $f(a) \neq 0$.

Rozszerzenie algebraiczne składa się z samych elementów algebraicznych.

Niech $K \subseteq L \subseteq M$, wtedy $K \subseteq M$ jest algebraiczne $\iff$ $K \subseteq L$ oraz $L \subseteq M$ są algebraiczne.

Stopień rozszerzenia: jeśli $K \subseteq L$ jest rozszerzeniem ciała, to L możemy traktować jako *przestrzeń liniową* nad K. Definiujemy wtedy stopień rozszerzenia $[L : K] = \dim_K(L)$ jako rozmiar bazy L nad K.

Algebraiczne domknięcie K w L : $K_{alg}(L) = \{a \in L : a \text{ jest algebraiczny}\}$

Mówimy, że K jest *relatywnie algebraicznie domknięte w L* jeśli $K_{alg}(L) = K$.

Funkcja Eulera: $\phi(m) = |\{k \in \mathbb{N} : 0 \leq k < m : NWD(k, m) = 1\}|$.

m-ty wielomian cyklotoniczny: zdefiniujmy $\{k \in \mathbb{N} : NWD(k, m) = 1\} = \{m_1, ..., m_{\phi(m)}\}$ i niech $a \in \mu_m(R)$ będzie generatorem tej grupy. Wtedy wielomian

$$F_m(x) = (x - a^{m_1})...(x - a^{m_{\phi(m)}})$$

nazywamy m-tym wielomianem cyklotonicznym.

Wiemy, że $w_m(x) = x^m - 1 = F_m(x) \prod_{\substack{d<m \\ d|m}} F_d(x)$.

Lemat Liouville'a: jeśli $a \in \mathbb{R}$ jest liczbą algebraiczną stopnia $N > 1$, to istnieje $c = c(a) \in \mathbb{R}$ takie, że dla każdego $r = \frac{p}{q} \in \mathbb{Q}$ zachodzi

$$\left| a - \frac{p}{q} \right| \geq \frac{c}{q^N}$$

Jeśli liczba nie spełnia tego lematu, to jest liczbą przestępną.

Domknięcie algebraiczne $\widehat{K} = K^{alg}$ to ciało $L \subseteq K$, które jest algebraicznie domkniętym rozszerzeniem algebraicznym K (każdy $a \in L$ jest pierwiastkiem wielomianu z $K[x]$).

Jest to najmniejsze algebraicznie domknięte ciało zawierające K.

Domknięcie algebraiczne jest *jedyne z dokładnością do izomorfizmu nad K*

Izomorfizm ciał przenosi się na izomorfizm ich domknięć algebraicznych dokładniej, jeśli $f : K \xrightarrow{\cong} L$, to istnieje $h : \widehat{K} \xrightarrow{\cong} \widehat{L}$ taki, że $h \restriction K = f$.

Grupa Galois rozszerzenia $K \subseteq L$ to grupa $Gal(L/K) = \{f \in Aut(L) : f \restriction K = id_K\} = Aut(L/K)$. Jest to podgrupa wszystkich automorfizmów ciała L.

Grupa $Gal(\widehat{K}/K)$ jest nazywana **absolutną grupą Galois** ciała K.

Rozszerzenie normalne to rozszerzenie algebraiczne $K \subseteq L$ takie, że dla wszystkich $f : L \to K$ zachodzi $f[L] \subseteq \widehat{K}$ oraz $f[L]$ jest jedno dla wszystkich takich f.

Rozszerzenie jest normalne $\iff$ dla każdego $f \in Gal(\widehat{K}/K)$ mamy $f[L] = L$.

Rozszerzenie algebraiczne $K \subseteq L$ jest normalne $\iff$ dla każdego $b \in L$ wielomian minimalny $f \in K[x]$ rozkłada się w $L[x]$ na iloczyn czynników liniowych.

Rozszerzenie skończone i normalne $L \subseteq K \iff$ L jest ciałem rozkładu pewnego wielomianu.

Normalne domknięcie ciała: niech $K \subseteq L$ i niech L_1 będzie generowane przez $\bigcup\{f[L] : f \in Gal(\widehat{K}/K)\}$. Wtedy

1. L_1 jest normalnym domknięciem ciała L w $\widehat{K}$
2. rozszerzenie $K \subseteq L_1$ jest normalne
3. $K \subseteq L_2$ i $L \subseteq L_2$ są normalne, to istnieje monomorfizm $L_1 \to L_2$ który po obcięciu do K jest id_K.

Element rozdzielczy: $a \in \widehat{K}$ jest rozdzielczy nad K gdy wielomian minimalny $w_a(x) \in K[x]$ ma jedynie pierwiastki pojedyncze. Wielomian taki nazywamy **wielomianem rozdzielczym** .

Rozszerzenie rozdzielcze to rozszerzenie algebraiczne którego wszystkie elementy są rozdzielcze nad K.

Wielomian $w(x)$ **jest nierozdzielczy** $\iff w \in K[x^p]$.

Jeśli $a \in \widehat{K}$, to $|\{f(a) : f \in Gal(\widehat{K}/K)\}| \leq deg(a)$, a jeśli a jest rozdzielczy to zamiast $\leq$ jest $=$.

Element pierwotny $L \supseteq K$ to $a \in L$ takie, że $L = K(a)$.

Jeśli $K \subseteq L$ jest rozszerzeniem skończonym takim, że $L = K(a_1, ..., a_n)$ i a_i są rozdzielcze nad K, to istnieje $a \in L$ rozdzielczy nad K taki, że $L = K(a)$.

Rozszerzenia radykalne: $K \subseteq L$

1. $a \in L$ jest czysto nierozdzielczy [**radykalny**] nad K gdy wielomian minimalny w_a ma tylko jeden pierwiastek w K
2. $K \subseteq L$ jest **rozszerzeniem radykalnym** gdy każdy $a \in L$ jest radykalny.

a jest radykalne nad K $\iff$ dla każdego $f \in \mathrm{Gal}(\widehat{K}/K)$ $f(a) = a$. Jeśli z kolei $\mathrm{char}(K) = p$, to a radykalne $\iff$ istnieje n takie, że $a^{p^n} \in K$.

Domknięcie rozdzielcze K w L $\mathrm{sep}_L(K) = \{a \in L : a \text{ rozdzielcze nad } K\}$. Oznaczamy $\widehat{K}^s = \mathrm{sep}_{\widehat{K}}(K)$ jako **rozdzielcze domknięcie** K.

Domknięcie radykalne K w L $\mathrm{rad}_L(K) = \{a \in L : a \text{ radykalne nad } K\}$. Oznaczamy $\widehat{K}^r = \mathrm{rad}_{\widehat{K}}(K)$ jako **radykalne domknięcie** K.

Stopień rozdzielczy rozszerzenia L nad K definiujemy $[L : K]_s = [\mathrm{sep}_L(K) : K]$.

Stopień radykalny rozszerzenia L nad K to z kolei $[L : K]_r = [\mathrm{rad}_L(K)]$.

Rozszerzenie Galois to rozszerzenie algebraiczne $K \subseteq L$ takie, że dla każdego $a \in L \setminus K$ istnieje $f \in \mathrm{Gal}(L/K)$ taki, że $f(a) \neq a$.

$K \subseteq L$ jest Galois $\iff$ $K \subseteq L$ jest rozdzielcze i normalne.

Niech $K \subseteq L \subseteq M$. Wtedy $K \subseteq M$ jest Galois $\iff$ $L \subseteq M$ jest Galois.

Twierdzenie Artina: jeśli $G < \mathrm{Aut}(L)$, to $L^G = \{a \in : : (\forall f \in G)\ f(a) = a\} \subseteq L$ jest rozszerzeniem Galois i $[L : L^G] = |G|$.

Stopień rozszerzenia Galois jeśli $K \subseteq L$ jest skończonym rozszerzeniem Galois, to $[L : K] = |\mathrm{Gal}(L/K)|$.

Dla $K \subseteq L$ skończonego i Galois oraz $H \leq \mathrm{Gal}(L/K)$ mamy $H \triangleleft \mathrm{Gal}(L/K) \iff K \subseteq L^H$ jest normalne.

Rozszerzenie abelowe to skończone rozszerzenie Galois dla którego grupa Galois jest cykliczna.

Rozszerzenie rozwiązywalne to rozszerzenie Galois dla którego grupa Galois jest rozwiązywalna.

Rozszerzenie ciała przez pierwiastki $K \subseteq L$ to rozszerzenie dla którego istnieje k oraz $L \subseteq L_0 \supseteq L_1 \supseteq \ldots \supseteq L_k = K$ takie, że dla każdego $i < k$ ciało L_i jest ciałem rozkładu nad L_{i+1} wielomianu

1. $x^{n_i} - b_i$ dla $b_i \in L_{i+1}$ lub
2. $x^p - x - b_i$ dla $b_i \in L_{i+1}$.

$K \subseteq L$ jest skończonym rozszerzeniem przez pierwiastki $\iff$ istnieje $L' \supseteq L$ takie, że $K \subseteq L'$ jest rozwiązywalna.

Rozszerzenie przestępne posiada element a przestępny nad K (tzn. $I(a/K) = 0$). **Rozszerzenie czysto przestępne** składa się wyłącznie z elementów przestępnych.

a jest elementem przestępnym, jeśli $K(a) \cong K(x)$.

Domknięcie algebraiczne $U = \widehat{U}$ jest dużym ciałem, $F \subseteq K \subseteq U$, gdzie F jest ciałem prostym, wtedy

1. $\mathrm{acl}_K : \mathscr{P}(U) \to \mathscr{P}(U)$ jest operatorem domknięcia algebraicznego który podzbiór $A \subseteq U$ przekształca na $K(A)^{alg}$
2. $A \subseteq U$ jest algebraicznie domknięty nad K gdy $A = \mathrm{ack}_K(A)$.

Podzbiór algebraicznie niezależny spełnia $(\forall a \in A)\ a \notin \mathrm{acl}_K(A \setminus \{a\})$.

Równoważnie, dla każdego n oraz $a_1, \ldots, a_n \in A$ parami różnych dla każdego $w(x_1, \ldots, x_n) \in K[\bar{x}]$ $w(\bar{a}) \neq 0$.

Baza przestępna to algebraicznie niezależny podzbiór $B \subseteq A$ taki, że $B \subseteq A \subseteq \mathrm{acl}_K(B)$. **Wymiar przestępny** A nad K to moc jego bazy przestępnej.

Lemat Schura: jeśli M jest R-modułem prostym, to $\mathrm{End}_R(M)$ jest pierścieniem z dzieleniem (prawie ciało, ale niekoniecznie jest przemienny)

Podzbiór liniowo niezależny w R-module $\{m_i\} \subseteq M$ znaczy, że jeśli $\sum r_i m_i = 0$, to $r_i = 0$ dla każdego i.

Baza modułu spełnia:

1. jest liniowo niezależna
2. generuje M jako R-moduł (czyli dowolny $M \ni m = \sum r_i b_i$ dla $r_i \in R$ oraz b_i z bazy)
3. $\mathrm{Lin}_R(B) = M$

Suma prosta modułów to $\bigsqcup M_i = \bigoplus M_i = \{f \in \prod M_i \ : \ \{i \in I \ : \ f(i) \neq 0\}$ jest skończony$\}$ (skończenie wiele współrzędnych jest niezerowych).

Moduł wolny posiada bazę.

Każdy R-moduł M jest obrazem pewnego R-modułu wolnego przez homomorfizm.

Niech M, N będą R-modułami i N jest wolny. Niech $f : M \to N$ będzie epimorfizmem, wtedy $M \cong \ker(f) \oplus N$.

Moduł projektwyny N dla każdego epimorfizmu $f : M \to N$ ma $M = \ker(f) \oplus M'$ dla $M' \subseteq M$.

Równoważnie isnieje $g : N \to M$ takie, że $fg = \mathrm{id}_N$ [f *rozszczepia się*].

Moduł injektywny M to taki, że dla każdego N i każdego monomorfizmu $g : M \to N$ istnieje $N' \subseteq N$ taki, że $N = \mathrm{Im}(g) \oplus N'$, tzn. obraz g jest *składnikiem prostym* N.

Moduł cykliczny jest generowany przez pojedynczy element, tzn. $M = Ra$ dla pewnego $a \in M$.

Torsje

1. a jest **torsyjny** gdy istnieje $r \neq 0$ takie, że $ra = 0$
2. M jest **modułem torsyjnym** gdy każdy element jest torsyjny. Jeśli każdy element jest beztorsyjny to M jest modułem **beztorsyjnym**
3. $M_t = \{a \in M \ : \ a$ jest torsyjny$\}$ jest **częścią torsyjną** M i jest jego podmodułem.