# Algebra 2R

a voyage into the unknown

koteczek

~

## SYLABUS:

### I. Podstawy teorii równań algebraicznych

1. Rozszerzenia ciał. Rozszerzenia o pierwiastek wielomianu nierozkładalnego. Ciało rozkładu wielomianu: istnieje, jedyność.

2. Ciało algebraicznie domknięte: definicja. Każde ciało zawiera się w ciele algebraicznie domkniętym (konstrukcja). Podciało proste: istnienie, jedyność. Ciała proste.

3. Pierwiastki z jedności, pierwiastki pierwotne. Grupa pierwiastków z jedności w ciele: każda jej skończona podgrupa jest cykliczna. Wielomiany podziału koła. Funkcja Frobeniusa. Ciała skończone: własności.

### II. Teoria Galois

1. Rozszerzenia [elementy] algebraiczne, przestępne: definicja. Stopień rozszerzenia. Warunki równoważne algebraiczności. Wielomian minimalny elementu ciała nad podciałem, własności.

2. Algebraiczne domknięcie ciała: definicja, istnienie, jedyność, własności (jednorodność). Istnienie rzeczywistych liczb przestępnych, liczby Liouville'a.

3. Rozszerzenia normalne: definicja, własności. Rozszerzenia [elementy, wielomiany] rozdzielcze. Twierdzenie Abela o elemencie pierwotnym. Rozszerzenia czysto nierozdzielcze (radykalne): definicja, własności. Stopień rozdzielczy [radykalny] rozszerzenia: definicja, własności.

# Contents

# 1. Teoria równań algebraicznych

## 1.1. Ciała

Dla $K \subseteq L$ ciał i $a_1, \ldots, a_n = \bar{a} \in L$ definiujemy ideał $I(\bar{a}/L)$ w $K[X_1, \ldots, X_n]$ jako:

$$I(\bar{a}/L) := \{f(X_1, \ldots, X_n) \in K[\bar{X}] : f(\bar{a}) = 0\},$$

to znaczy generujemy ideał w wielomianach nad K zawierający wszystkie wielomiany (niekoniecznie tylko jednej zmiennej) zerujące się w $\bar{a}$.

**Przykład:**

Dla $K = \mathbb{Q}, L = \mathbb{R}, n = 1, a_1 = \sqrt{2}$ mamy

$$I(\sqrt{2}/\mathbb{Q}) = \{f(x^2 - 2) \ : \ f \in \mathbb{Q}[X]\} = (x^2 - 2) \triangleleft \mathbb{Q}[X]$$

Dalej, definiujemy

$$K[\bar{a}] := \{f(\bar{a}) \ : \ f \in K[X]\}$$

czyli podpierścień L generowany przez $K \cup \{\bar{a}\}$ oraz $K(\bar{a})$, czyli podciało L generowane przez $K \cup \{\bar{a}\}$:

$$K(\bar{a}) := \{f(\bar{a}) \ : \ f \in K(X_1, \ldots, X_n) \text{ i } f(\bar{a}) \text{ dobrze określone}\}.$$

Tutaj $K(X_1, \ldots, X_n)$ to *ciało ułamków pierścienia* $K[\bar{X}]$ (czyli najmniejsze ciało, że pierścień może być w nim zanurzony).

**Przykład:**

Dla $K = \mathbb{Q}, L = \mathbb{R}$ zachodzi:

$$K[\sqrt{2}] = \mathbb{Q}[\sqrt{2}] = \{q + p\sqrt{2} \ : \ q, p \in \mathbb{Q}\}$$
$$K[\sqrt{2}, \sqrt{3}] = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$$
$$K(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$$

to ostatnie to usuwanie niewymierności z mianownika.

**Twierdzenie:** Niech $K \subseteq L_1, K \subseteq L_2$ będą ciałami. Wybieramy $\{a_1, \ldots, a_n\} \in L_1$ i $\{b_1, \ldots, b_n\} \in L_2$. Wtedy następujące warunki są równoważne:

- $\hookrightarrow$ istnieje izomorfizm $\phi : K[a_1, \ldots, a_n] \to K[b_1, \ldots, b_n]$ taki, że $\phi \restriction K = id_K$ oraz $\phi(a_i) = b_i$.
- $\hookrightarrow$ $I(\bar{a}/K) = I(\bar{b}/K)$.

**Dowodzik:**

$K[\bar{a}] \cong K[\bar{b}] \implies I(\bar{a}/K) = I(\bar{b}/K)$

Niech $\omega \in K[\bar{X}]$. Wtedy $\omega \in I(\bar{a}/K)$ wtedy i tylko wtedy, gdy $\omega(\bar{a}) = 0$, to mamy z definicji $I(\bar{a}/K)$. Wiemy też, że $\phi(a) \in K[\bar{X}]$ wtedy, gdy $\omega(\phi(\bar{a})) = 0$, a ponieważ $\phi(\bar{a}) = \bar{b}$, to również $\omega(\bar{b}) = 0$ i mamy, że $\omega \in I(\bar{b}/K)$. Czyli izomorfizm między $K[\bar{a}] = K[\bar{b}]$ implikuje, że $I(\bar{a}/K) = I(\bar{b}/K)$.

$K[\bar{a}] \cong K[\bar{b}] \impliedby I(\bar{a}/K) = I(\bar{b}/K)$

Spróbujmy zdefiniować izomorfizm $\phi$ tak, że dla $\omega \in K[\bar{X}]$ mamy $\phi(\omega(\bar{a})) = \omega(\bar{b})$

1. $\phi$ jest homomorfizmem:

$$\phi(\omega(\bar{a}) \cdot v(\bar{a})) = f((\omega \cdot v)(\bar{a})) = (\omega \cdot v)(\bar{b}) = \omega(\bar{b}) \cdot v(\bar{b}) = \phi(\omega(\bar{a})) \cdot \phi(v(\bar{a}))$$

2. $\phi$ jest różnowartościowe:

$$\phi(\omega(\bar{a})) = \phi(v(\bar{a})) \iff \omega(\bar{b}) = v(\bar{b}) \iff (\omega - v)(\bar{b}) = 0 \iff \omega - v \in I(\bar{b}/K) = I(\bar{a}/K) \iff (\omega - v)(\bar{a}) = 0 \iff \omega(\bar{a}) = v(\bar{a})$$

3. $\phi$ jest dobrze zdefiniowane (czyli przyjmuje tylko jedną wartość dla jednego argumentu):

$$\omega(\bar{a}) - v(\bar{a}) = 0 \iff (\omega - v)(\bar{a}) = 0 \iff \omega - v \in I(\bar{a}/K) \iff \omega - v \in I(\bar{b}/K) \iff (\omega - v)(\bar{b}) = 0 \iff \omega(\bar{b}) - v(\bar{b}) = 0$$

Możemy teraz zapytać, czy każdy ideał w pierścieniu wielomianów $K[X]$ jest postaci $I(\bar{a}/K)$ dla pewnego $\bar{a} \in L \supset K$? Albo ogólniej, czy dla pierścienia przemiennego $R$ z $1_R \neq 0_R$ oraz ideału $I = (f_1, \dots, f_m) = I(\bar{a}/R) \triangleleft R[X]$, czy istnieje nadpierścień $S$ taki, że $1_S = 1_R$ i $0_S = 0_R$ oraz układ

$$f_1(\bar{x}) = \dots = f_m(\overline{m}) = 0$$

ma rozwiązanie w $S$? Takie rozwiązanie spełniałoby $\bar{a} \in S \iff (\forall\, g \in (f_1, \dots, f_m))\ g(\bar{a}) = 0$.