Lecture 12b: Algebraic Closure

MAT205 Abstract Algebra II

Ma, Jia-Jun

Xiamen University Malaysia

Definition: Algebraically Closed Field

Definition. A field K is *algebraically closed* if every nonconstant $f \in K[x]$ has a root in K.

Equivalent form. Every nonconstant $f \in K[x]$ factors into linear factors over K:

$$f = c \prod_{i=1}^{\deg f} (x - \alpha_i), \qquad c \in K^{\times},\ \alpha_i \in K.$$

- **Example.** $\mathbb{C}$ is algebraically closed (Fundamental Theorem of Algebra; analytic proof outside this course).
- **Non-examples.** $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{F}_p$ — each has an irreducible polynomial of degree ≥ 2 (e.g. $x^2 + 1$ over $\mathbb{R}$).

Definition: Algebraic Closure

Definition. An *algebraic closure* of a field F is a field $\overline{F}$ with:

1. $F \subseteq \overline{F}$;
2. $\overline{F}/F$ algebraic (every element of $\overline{F}$ is algebraic over F);
3. $\overline{F}$ algebraically closed.

So $\overline{F}$ contains a root of every nonconstant $f \in F[x]$, and adds nothing beyond what algebraicity over F forces.

Example. $\overline{\mathbb{Q}} := \{\, \alpha \in \mathbb{C} : \alpha \text{ algebraic over } \mathbb{Q} \,\}$, the algebraic numbers, is an algebraic closure of $\mathbb{Q}$. It is a field (the algebraic elements form a subfield), and algebraically closed since $\mathbb{C}$ is and a root of a polynomial over $\overline{\mathbb{Q}}$ is algebraic over $\mathbb{Q}$ (transitivity of algebraicity).

Steinitz's Theorem (Existence and Uniqueness)

Theorem (Steinitz, 1910). Every field F has an algebraic closure $\overline{F}$. Any two algebraic closures of F are isomorphic as extensions of F (an F-isomorphism fixing F pointwise).

- Existence uses **Zorn's lemma** directly.
- Uniqueness follows from the universal property of $\overline{F}$.
- Both rest on the Axiom of Choice.

Historical note. Steinitz's 1910 paper *Algebraische Theorie der Körper* systematized field theory by transfinite methods — one of the earliest serious uses of choice principles in algebra.

Partial and Total Orders

Partial order. A relation $\leq$ on a set P that is

- reflexive: $a \leq a$;
- antisymmetric: $a \leq b$ and $b \leq a \Rightarrow a = b$;
- transitive: $a \leq b$ and $b \leq c \Rightarrow a \leq c$.

Then $(P, \leq)$ is a *partially ordered set* (poset). Some pairs may be *incomparable* — neither $a \leq b$ nor $b \leq a$.

Total order. A partial order in which any two elements are comparable: for all a, b, $a \leq b$ or $b \leq a$ (also: linear order). A *chain* is exactly a totally ordered subset.

Examples. $(\mathcal{P}(X), \subseteq)$ is partial, not total once $|X| \geq 2$ ($\{1\}, \{2\}$ incomparable); $(\mathbb{Z}, \leq)$ is total; divisibility $(\mathbb{N}, |)$ is partial, not total ($2, 3$ incomparable).

Here the objects are fields ordered by inclusion $\subseteq$ — a partial order on Ω; a chain is a tower $K_1 \subseteq K_2 \subseteq \cdots$.

Zorn's Lemma

Vocabulary. Let $(\mathcal{P}, \leq)$ be a partially ordered set.

- A *chain* is a totally ordered subset $\mathcal{C} \subseteq \mathcal{P}$.
- An *upper bound* of $\mathcal{C}$ is $u \in \mathcal{P}$ with $c \leq u$ for all $c \in \mathcal{C}$.
- m is *maximal* if $m \leq x \Rightarrow x = m$.

Zorn's Lemma. If $\mathcal{P} \neq \varnothing$ and every chain has an upper bound in $\mathcal{P}$, then $\mathcal{P}$ has a maximal element. (Equivalent to the Axiom of Choice.)

In the existence proof, $\mathcal{P}$ is the set of fields K with $F \subseteq K \subseteq \Omega$ and K/F algebraic, ordered by inclusion.

Proof Skeleton: The Zorn Argument

- **Step 1 (ambient set).** Every algebraic extension of F has cardinality $\leq \max(|F|, \aleph_0)$. Fix a set $\Omega \supseteq F$ of this cardinality.
- **Step 2 (poset).** Let $\mathcal{P}$ be all fields K with $F \subseteq K \subseteq \Omega$ and K/F algebraic, ordered by inclusion.
- **Step 3 (Zorn).** Every chain has the union as upper bound (a field, algebraic over F). Zorn gives a maximal $\overline{F} \in \mathcal{P}$.
- **Step 4 (maximal $\Rightarrow$ closed).** If $f \in \overline{F}[x]$ had no root in $\overline{F}$, build $\overline{F}(\alpha) \supsetneq \overline{F}$ with $f(\alpha) = 0$ (Kronecker's theorem). Then α is algebraic over F (transitivity of algebraicity), so $\overline{F}(\alpha)$ embeds in Ω — contradicting maximality.

So $\overline{F}$ is algebraically closed and algebraic over F: an algebraic closure of F. $\square$

Universal Property of the Algebraic Closure

Theorem. Let $\overline{F}/F$ be an algebraic closure. For any algebraic extension E/F there is an F-embedding

$$\sigma : E \hookrightarrow \overline{F}, \qquad \sigma|_F = \mathrm{id}_F.$$

So $\overline{F}$ contains a copy of every algebraic extension of F.

- **Count.** For $E = F(\alpha)$ with α a root of irreducible $p \in F[x]$, the F-embeddings $E \hookrightarrow \overline{F}$ correspond to the roots of p in $\overline{F}$ — generally not unique.
- **Uniqueness of $\overline{F}$.** Embed one algebraic closure into another; by maximality the image is everything, giving an F-isomorphism (not canonical).

Proof (Zorn again). Order pairs (K, σ_K), $F \subseteq K \subseteq E$, $\sigma_K : K \hookrightarrow \overline{F}$ an F-embedding, by extension. A maximal pair has $K = E$: otherwise send some $\beta \in E \setminus K$ to a root of its minimal polynomial in $\overline{F}$. $\square$