Algebraic Closure and Infinite Galois Theory

Tristan Wylde-LaRue

Algebraic Extensions

Definition:
A field extension L/F (of potentially infinite degree) is algebraic if every $\alpha \in L$ is a root of some $f \in F[x]$.

Algebraic Extensions

Definition:
A field extension L/F (of potentially infinite degree) is algebraic if every $\alpha \in L$ is a root of some $f \in F[x]$.

Examples:

- $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$
- The splitting field of $x^5 - x - 1$ over $\mathbb{Q}$.
- $\mathbb{C}/\mathbb{R}$

Algebraically Closed Fields

Definition:
A field L is algebraically closed if it has no nontrivial algebraic extensions.

Definition:
A field extension $\overline{F}/F$ is an algebraic closure if it is algebraic and algebraically closed.

Which fields have an algebraically closed extension?
Which fields have an algebraic closure?

Existence of Algebraic Closures

Theorem

For every field F, there is an algebraic extension $\overline{F}/F$ that is algebraically closed.

Existence of Algebraic Closures

Lemma
Let F be a field. There exists an extension L/F such that every nonconstant polynomial $f(x) \in F[x]$ has at least one root in L.

Proof of Lemma

Take the polynomial ring $F[x]$.

Proof of Lemma

Take the polynomial ring $F[x]$.
Let $\mathscr{F} \subseteq F[x]$ be the set of nonconstant, monic polynomials.

Proof of Lemma

Take the polynomial ring $F[x]$.
Let $\mathscr{F} \subseteq F[x]$ be the set of nonconstant, monic polynomials.
Construct a new ring $R = F[x_f]_{f \in \mathscr{F}}$

Proof of Lemma

Take the polynomial ring $F[x]$.
Let $\mathscr{F} \subseteq F[x]$ be the set of nonconstant, monic polynomials.
Construct a new ring $R = F[x_f]_{f \in \mathscr{F}}$

Consider the subset of R obtained by evaluating each $f \in \mathscr{F}$ at its corresponding symbol:

$$\{f(x_f) \mid f \in \mathscr{F}\}$$

Proof of Lemma

Take the polynomial ring $F[x]$.
Let $\mathscr{F} \subseteq F[x]$ be the set of nonconstant, monic polynomials.
Construct a new ring $R = F[x_f]_{f \in \mathscr{F}}$

Consider the subset of R obtained by evaluating each $f \in \mathscr{F}$ at its corresponding symbol:

$$\left\{ f(x_f) \mid f \in \mathscr{F} \right\}$$

Let $I \subseteq R$ be the ideal generated by this set.

Proof of Lemma (cont.)

Claim: I is a proper ideal of R.

Assume that $I = R$. Then it must contain 1 and so

$$1 = \sum_{i=1}^{n} r_i \cdot f_i(x_{f_i})$$

for some $\{f_1, ..., f_n\} \subseteq \mathscr{F}$ and $\{r_1, ..., r_n\} \subseteq R$.

Proof of Lemma (cont.)

Claim: I is a proper ideal of R.

Assume that $I = R$. Then it must contain 1 and so

$$1 = \sum_{i=1}^{n} r_i \cdot f_i(x_{f_i})$$

for some $\{f_1, ..., f_n\} \subseteq \mathscr{F}$ and $\{r_1, ..., r_n\} \subseteq R$.

For each $1 \leq i \leq n$, there is a field K_i that contains a root of f_i.

Proof of Lemma (cont.)

Claim: I is a proper ideal of R.

Assume that $I = R$. Then it must contain 1 and so

$$1 = \sum_{i=1}^{n} r_i \cdot f_i(x_{f_i})$$

for some $\{f_1, ..., f_n\} \subseteq \mathscr{F}$ and $\{r_1, ..., r_n\} \subseteq R$.

For each $1 \leq i \leq n$, there is a field K_i that contains a root of f_i. Thus we can apply the evaluation maps $x_{f_i} \mapsto \alpha_i$ to both sides

$$1 = \sum_{i=1}^{n} r_i \cdot f(\alpha_i) = \sum_{i=1}^{n} r_i \cdot 0 = 0$$

Proof of Lemma (cont.)

Since I is proper, by Zorn's Lemma, it is contained in a maximal ideal $I \subseteq \mathfrak{m} \subset R$.

The quotient ring $R/\mathfrak{m}$ must be a field. Moreover, $\mathfrak{m}$ and F are disjoint, hence we can identify F as a subset of $R/\mathfrak{m}$.

Thus $R/\mathfrak{m}$ is a field extension of F. $\square$

Existence of Algebraic Closures

Theorem

For every field F, there is an algebraic extension $\overline{F}/F$ that is algebraically closed.

Proof of Existence

We apply the Lemma to construct a field extension K_1/F in which every polynomial $f \in F[x]$ has a root.

Proof of Existence

We apply the Lemma to construct a field extension K_1/F in which every polynomial $f \in F[x]$ has a root. Apply this iteratively to get

$$\dots K_3/K_2/K_1/F$$

Proof of Existence

We apply the Lemma to construct a field extension K_1/F in which every polynomial $f \in F[x]$ has a root. Apply this iteratively to get

$$\ldots K_3/K_2/K_1/F$$

Define

$$K := \bigcup_{i=1}^{\infty} K_i$$

This is an algebraically closed extension of F.

Proof of Existence

We apply the Lemma to construct a field extension K_1/F in which every polynomial $f \in F[x]$ has a root. Apply this iteratively to get

$$\dots K_3/K_2/K_1/F$$

Define

$$K := \bigcup_{i=1}^{\infty} K_i$$

This is an algebraically closed extension of F. Now take

$$\overline{F} = \{\alpha \mid \alpha \text{ is a root of some } f \in F[x]\}$$

This extension is clearly algebraic. It is slightly less obvious that it is algebraically closed, but it follows from some case checking. $\square$

Uniqueness

Is this construction unique? Or are there fields with multiple distinct algebraic closures?

Uniqueness

Is this construction unique? Or are there fields with multiple distinct algebraic closures?

Theorem: Algebraic Closures are unique up to isomorphism, but this isomorphism is not unique.

Examples of Algebraic Closures

- $\overline{\mathbb{R}} = \mathbb{C}$
- The algebraic closure of the rationals $\overline{\mathbb{Q}} \subseteq \mathbb{C}$
- The algebraic closure of $\mathbb{F}_p$

Algebraic closures can be very complicated objects. We can study them by looking at how fields sit inside their algebraic closure.

The finite Galois Correspondence

Recall the fundamental theorem establishes a correspondence for finite Galois extensions:

$$\{\text{intermediate fields } E : \ L/E/F\} \longleftrightarrow \{\text{subgroups of } G\}$$

The infinite Galois Correspondence

With the correct choice of topology, the correspondence generalizes to infinite Galois extensions as

$$\{\text{intermediate fields } E : \ L/E/F\} \Longleftrightarrow \{\text{closed subgroups of } G\}$$

With enough work one can show that the entire fundamental theorem extends exactly the same by replacing subgroup with closed subgroup

Topological Groups

A topological group is a group G equipped with a Hausdorff topology such that

(1) The group operation $G \times G \to G$ is continuous

(2) The inverse map $g \mapsto g^{-1}$ is continuous.

For a finite group, the only possible Hausdorff topology is the discrete topology.

Limits

Let $\{A_1, A_2, ...\}$ be a family of topological groups. Suppose we have a chain of surjective homomorphisms

$$A_1 \twoheadleftarrow A_2 \twoheadleftarrow A_3 \twoheadleftarrow \cdots$$

Then we can define the limit

$$\lim_{i \in I} A_i := \prod_{i \in I} A_i$$

Limits (cont.)

In full generality, this satisfies the universal property:

$$
\begin{tikzcd}
 & Y \arrow[ddl, bend right, "\psi_i"'] \arrow[ddr, bend left, "\psi_j"] \arrow[d, dashed, "u"] & \\
 & X \arrow[dl, "\pi_i"'] \arrow[dr, "\pi_j"] & \\
A_j \arrow[rr, "f_{ij}"'] & & A_i
\end{tikzcd}
$$

Some Examples

A not so interesting, but perhaps illustrative example:

$$\lim_{n\in\mathbb{N}} (\mathbb{Z}/2\mathbb{Z})^n = \prod_{n\in\mathbb{N}} (\mathbb{Z}/2\mathbb{Z})^n$$

A more interesting one, for any prime p we have:

$$\lim_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} = \prod_{n\in\mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} \overset{\text{def}}{=} \mathbb{Z}_p$$

Connecting back to Galois Theory

Theorem: If L/F is Galois, then

$$\mathrm{Gal}(L/F) \cong \lim_{\substack{L/E/F \\ E/F \text{ finite}}} \mathrm{Gal}(E/F)$$

Finite Fields

Finite fields:

$$\mathrm{Gal}(\overline{\mathbb{F}}_p/\mathbb{F}_p) = \hat{\mathbb{Z}}$$

where $\hat{\mathbb{Z}}$, the profinite integers, can be defined as the limit

$$\hat{\mathbb{Z}} = \lim_{n \in \mathbb{Z}} \mathbb{Z}/n\mathbb{Z} \; = \lim_{p \text{ prime}} \mathbb{Z}_p$$

The group generated by the Frobenious map is dense in $\hat{\mathbb{Z}}$.

Absolute Galois Group of the Rationals

What is $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$?

This turns out to be in incredibly difficult problem. J.S. Milne refers to it as the "most important object in mathematics."

Some properties of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$:

- It is conjectured that it admits every finite group as a quotient group (proven for all simple groups and all sporadic groups except M_{23}).
- When $\overline{Q}$ is viewed as subset of $\mathbb{C}$, the only Borel measurable function in $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ is complex conjugation.