13.4 Splitting Field and Closures

Earlier we showed:

For \( f(x) \in F[x] \) of degree \( n \), there is an extension \( K/F \) of degree \( \leq n \) containing a root \( \alpha \) of \( f(x) \).

Thus, \( f(x) = (x-\alpha)g(x) \) for some \( g(x) \in K[x] \) of degree \( \leq n-1 \).

Repeating this process with \( g(x) \) eventually proves:

\[ \text{monic} \]

Theorem: For \( f(x) \in F[x] \) of degree \( n \), there is an extension \( K/F \) of degree \( \leq n \) such that \( f(x) = (x-\alpha_1)(x-\alpha_2) \cdots (x-\alpha_n) \) with \( \alpha_1, \ldots, \alpha_n \in K \).

The smallest extension \( K/F \) with this property is called a splitting field of \( f(x) \).
In fact, \( K = F(\alpha_1, \ldots, \alpha_n) \).

Prop: Any two splitting fields of \( f(x) \) over \( F \) are isomorphic over \( F \).

(We'll omit the proof in this course)

Ex: The splitting field of \( x^3 - 2 \) over \( \mathbb{Q} \) is \( \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2} \omega, \sqrt[3]{2} \omega^2) \).

where \( \omega = \frac{-1 + \sqrt{-3}}{2} \).

This is the same as \( \mathbb{Q}(\sqrt[3]{2}, \sqrt{-3}) \).

which has degree 6 over \( \mathbb{Q} \).

\[ [K : \mathbb{Q}] = 9 \]

\[ [K_1 : \mathbb{Q}] = 3 \]

\[ [K_2 : \mathbb{Q}] = 3 \]

\[ [K_3 : \mathbb{Q}] = 3 \]

\[ [K_4 : \mathbb{Q}] = 2 \]
Ex: The splitting field of $x^n - 1$ over $\mathbb{Q}$.

There are $n$ roots in $\mathbb{C}$ given by

Euler's formula: $e^{2\pi i k/n}$, $0 \leq k \leq n - 1$.

(derived from $e^{i\theta} = \cos \theta + i \sin \theta$.)

If we set $\zeta = e^{2\pi i/n}$ (or any primitive $n$-th root of 1), these are

$1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$

Thus, all are in $\mathbb{Q}(\zeta)$.

What is $[\mathbb{Q}(\zeta): \mathbb{Q}]$?

Theorem: $[\mathbb{Q}(\zeta): \mathbb{Q}] = \varphi(n)$ (Euler phi function).

If $n = p$ is prime, we showed earlier that

Example (4)

$p = 310$

$$\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1$$

is irreducible.

It's hard to prove the general case!
Any extension $K/F$ that is the splitting field of a polynomial $f(x) \in F[x]$ is called a normal extension.

(There is a relation to normal subgroup to be explained later!)

Ex: Splitting field of $(x^2 - 2)(x^2 - 3)$ over $\mathbb{Q}$

$$= \mathbb{Q}(\sqrt{2}, \sqrt{3})$$

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) \quad \mathbb{Q}(\sqrt{2}) \quad \mathbb{Q}(\sqrt{3}) \quad \mathbb{Q}(\sqrt{6})$$

How do we know these are the only intermediate fields?

Galois Theory.
Closure:

Suppose we adjoin all roots of all polynomials $f(x) \in F[x]$ to $F$.
The resulting field $\bar{F}$ is called the algebraic closure of $F$.

Theorem: 1) $\bar{F}/F$ is an algebraic extension.
2) $\bar{F}/F$ is algebraically closed: any polynomial $f(x) \in \bar{F}[x]$ has a root in $\bar{F}$.
3) Any field $K/F$ which is both algebraic and algebraically closed is isomorphic to $\bar{F}$.

Proof: (1) by definition.

(2) Given $f(x) \in F[x]$, let $K/F$ be a finite extension containing a root $\alpha$ of $f(x)$.
Then $K/F$ is algebraic and since $\bar{F}/F$ is algebraic, by our earlier theorem, we see $K/F$ is algebraic.
Hence, $a$ satisfies a polynomial equation $g(x) = 0$ for some nonconstant $g(x) \in F[x]$. Then by definition of $E$, $a \in F$. QED

Proved later.

The Fundamental Theorem of Algebra

$\mathbb{C}$ is algebraically closed.

The closure of $\mathbb{Q}$ is $\overline{\mathbb{Q}}$, the subfield of $\mathbb{C}$ consisting of all algebraic numbers.

Cantor: 1) $\overline{\mathbb{Q}}$ is countable.

2) $\mathbb{R}$ and $\mathbb{C}$ are uncountable.