Chapter 13  Field Theory

13.1  Basic Theory of Field Extensions

First, let's recall an old result that will be useful in our investigations.

Euclidean Algorithm (Finds \( \gcd(a, b) \) for \( a, b \) in a Euclidean Domain)

\[
a = q_0 b + r_0 \quad \leftarrow \text{division alg.}
\]
\[
b = q_1 r_0 + r_1 \quad \leftarrow \text{division alg.}
\]
\[
r_0 = q_2 r_1 + r_2 \quad \leftarrow \text{division alg}
\]
\[
r_1 = q_3 r_2 + r_3 \quad \leftarrow \text{division alg}
\]
\[\vdots\]
\[
r_n = q_n r_{n-1} + r_{n} \quad \leftarrow \gcd(a, b)
\]
\[
r_{n+1} = q_{n+1} r_n + 0
\]

It works by applying the following simple fact iteratively:

\[a = qb + r \Rightarrow \gcd(a, b) = \gcd(q, r)\]

Working backwards from last step, we can find \( x, y \) for which

\[ax + by = \gcd(a, b)\]

The characteristic of a field \( F \)

\[\text{char}(F) = \text{smallest } p \in \mathbb{N} \text{ for which } 1 + 1 + \ldots + 1 = 0 \text{ or }
\]
\[\text{char}(F) = 0 \text{ if no such } p \text{ exists.}\]

Examples

\[
\text{Ch}(\mathbb{Z}/3\mathbb{Z}) = 3 \quad \text{Ch}(\mathbb{R}) = 0 \quad \text{Ch}(\mathbb{Q}) = 0
\]

Field with 9 elements.

Proposition 1: \( \text{Ch}(F) \) is either prime or 0. If \( \text{Ch}(F) = p \), then

\[pa = a + a + \ldots + a = 0 \quad \text{for all } a \in F\]

Ring homomorphism \( \Phi: \mathbb{Z} \rightarrow F \) has kernel \( \text{ch}(F) \mathbb{Z} \).

By 1st isomorphism Theorem

If \( \text{Ch}(F) = p \), get injection \( \mathbb{Z}/p\mathbb{Z} \rightarrow F \)

If \( \text{Ch}(F) = 0 \), get injection \( \mathbb{Z}/0\mathbb{Z} = \mathbb{Z} \rightarrow F \)

Notation \( F_p = \mathbb{Z}/p\mathbb{Z} \).

Proposition 2

Given homomorphism \( \Phi: F \rightarrow F \), between fields, then \( \ker(\Phi) = 0 \) or \( \ker(\Phi) = F \), that is, \( \Phi \) is either injective or the zero map.
Field Extensions

Field $K$ is an extension of field $F$ if $F \subseteq K$. Expressed $K/F$ or $F \subset K$.

Examples:

- $\mathbb{R} \subset \mathbb{C}$
- $\mathbb{Q} \subset \mathbb{R}$
- $\mathbb{R}/\mathbb{Q}$ denotes extension, not quotient. (No such quotient anyway.)

Example: $[\mathbb{F}_3[x]/(x^2+1) = \mathbb{F}_3 \cup \{0, 1, 2, 1 + x, 1 + x, 2 + x, 1 + 2x, 2 + x, 2x\}$

$\mathbb{F}_3 = \{0, 1, 2\}$

Basis $B = \{1, x\}$

Note: $[\mathbb{F}_3[x]/(x^2+1)$ is a two-dimensional vector space over field $\mathbb{F}_3$.

Observation: If $K/F$ then $K$ is a vector space over $F$. The dimension of this space is called the degree of the extension, denoted $[K:F] = \dim(K)$. Extension is finite if $[K:F]$ is finite.

Theorem 4: Suppose $F$ is a field and $p(x) \in F[x]$ is irreducible, deg $n$, then $K = F[x]/(p(x))$, so $K$ is a vector space over $F$, $K/F$. Then $B = \{1, x, x^2, \ldots, x^{n-1}\}$ is a basis for $K$.

Thus $[K:F] = \deg(p(x))$.

Multiplication in $K = F[x]/(p(x))$:

If $a(x), b(x) \in K$, then $a(x)b(x) = r(x)$ where $a(x)b(x) = q(x)p(x) + r(x)$ by division algorithm.

Inverses in $K$: What is the inverse of $a(x)$?

Answer: Note $\gcd(p(x), a(x)) = 1$ because $p(x)$ irreducible.

Use Euclidean Alg to get $p(x)f(x) + a(x)g(x) = 1$.

Then $a(x)g(x) = 1 + p(x)f(x)$, i.e., $a(x)g(x) = 1, a(x) = g(x)$

Ex: In $K = \mathbb{F}_3[x]/(x^2+1)$, find $(2x+2)^{-1}$

Euclidean Alg:

$x^2 + 1 = 2x(2x+2) + (2x+1)$

$2x+2 = 1(2x+1) + 1 \leftarrow \gcd \quad 1 = (2x+2) - (2x+1)$

$1 = (2x+2) - (x^2+1 - 2x(2x+2))$

$1 = (x^2+1)(-1) + (2x+2)(1+2x)$

$\Rightarrow (2x+2)^{-1} = (1+2x)$
Roots of Polynomials

**Basic Question** If \( \varphi(x) \in F[x] \) has no roots in \( F \), is there an extension \( K/F \) for which \( \varphi(x) \) has a root in \( K \)?

**Example** \( \varphi(x) = x^2 - 2 \in \mathbb{Q}[x] \) has no root in \( \mathbb{Q} \) but has root \( \sqrt{2} \in \mathbb{R} \), \( \mathbb{R} \cap \mathbb{Q} \)

**Theorem 3** Suppose \( F \) is a field and \( \varphi(x) \in F[x] \) is irreducible. (In particular \( \varphi(x) \) has no root in \( F \)). Then there is an extension

\[
K = \frac{F[x]}{(\varphi(x))}
\]

\( \cong F \)

and \( \varphi(x) \in K[x] \) has root \( \alpha = \sqrt{2} \in K \)

\( \varphi(\sqrt{2}) = \varphi(x) = 0 \)

**Ungshot:** Given any field \( F \) and irreducible \( \varphi(x) \in F[x] \), there is an extension \( K/F \) containing a root of \( \varphi(x) \).

**Definitions** Given \( K/F \) and \( A = \{ a_1, a_2, \ldots, a_i \} \subseteq K \) then field generated by \( A \) over \( F \) is

\[
F(a_1, a_2, \ldots) = \bigcap_{J \subseteq K} \bigcap_{F \in J} F^J \cup F \mu A
\]

\( \varphi(\alpha) = 0 \) is called a simple extension; \( \alpha \) is its primitive element

**Theorem 6** Suppose \( K/F \) and \( \varphi(x) \in F[x] \) is irreducible and has a root \( a \in K \). Then \( F(a) \cong F[x]/(\varphi(x)) \)

**Proof** Show \( F[x] \rightarrow F(a) \) has kernel \( (\varphi(x)) \). Use F.L.T.

**Consequence** If \( \varphi(x) \) has roots \( a_1, a_2, \ldots, a_k \), then

\[
F(a_1) \cong F(a_2) \cong F(a_3) \cong \cdots \cong F(a_k)
\]

**Example** \( x^3 - 2 \in \mathbb{Q}[x] \)

has roots \( \sqrt[3]{2} \in \mathbb{R} \) and \( \sqrt[3]{2} \left( \frac{-1 \pm i \sqrt{3}}{2} \right) \in \mathbb{C} \)

Then \( \mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q} \left( \sqrt[3]{2} \left( \frac{-1 \pm i \sqrt{3}}{2} \right) \right) \)

\[
1 \quad \mathbb{R} \quad \mathbb{C}
\]