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)

$$
\begin{aligned}
a &= q_0 b + r_0 && \leftarrow \text{division alg.} \\
b &= q_1 r_0 + r_1 && \leftarrow \text{division alg.} \\
r_0 &= q_2 r_1 + r_2 && \leftarrow \text{division alg} \\
r_1 &= q_3 r_2 + r_3 && \leftarrow \text{division alg} \\
&\ \vdots \quad\ \vdots \quad\ \vdots && \quad\ \vdots \\
r_{n-2} &= q_n r_{n-1} + r_n && \longleftarrow \gcd(a,b) \\
r_{n-1} &= q_{n+1} r_n + 0
\end{aligned}
$$

It works by applying the following simple fact iteratively:

$a = qb + r \Rightarrow$
$\gcd(a,b) = \gcd(a,r)$

Working backwards from last step, we can find x, y for which
$ax + by = \gcd(a,b)$

The characteristic of a field F

$\mathrm{ch}(F) =$ smallest $p \in \mathbb{N}$ for which $\overbrace{1+1+1+\cdots+1}^{p \text{ times}} = 0$ or
$\mathrm{ch}(F) = 0$ if no such p exists.

Examples $\mathrm{Ch}(\mathbb{Z}/3\mathbb{Z}) = 3$ $\mathrm{Ch}(\mathbb{R}) = 0$ $\mathrm{Ch}\left(\underbrace{\mathbb{Z}/3\mathbb{Z}[x]/(x^2+1)}_{\text{field with 9 elements.}}\right) = 3$

$\mathrm{Ch}(\mathbb{Z}/5\mathbb{Z}) = 5$ $\mathrm{Ch}(\mathbb{Q}) = 0$

Proposition 1: $\mathrm{Ch}(F)$ is either prime or 0. If $\mathrm{Ch}(F) = p$, then
$pa = a + a + \cdots + a = 0$ for all $a \in F$

Ring homomorphism $\varphi: \mathbb{Z} \longrightarrow F$ has kernel $\mathrm{ch}(F)\mathbb{Z}$.
$x \longmapsto x \cdot 1$

By 1st isomorphism Theo:

If $\mathrm{Ch}(F) = p$, get injection $\mathbb{Z}/p\mathbb{Z} \longrightarrow F$ $\quad \mathbb{Z}/p\mathbb{Z} \subseteq F$

If $\mathrm{Ch}(F) = 0$, get injection $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z} \longrightarrow F$ $\quad \mathbb{Z} \subseteq \mathbb{Q} \subseteq F$

prime subfields of F

Notation $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$.

Proposition 2

Given homomorphism $\varphi: F \longrightarrow F'$ between fields, then $\ker(\varphi) = 0$ or $\ker(\varphi) = F$, that is, φ 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 $\begin{array}{c} K \\ | \\ F \end{array}$

Examples $\begin{array}{c} \mathbb{R} \\ | \\ \mathbb{Q} \end{array}$ $\begin{array}{c} \mathbb{C} \\ | \\ \mathbb{R} \end{array}$ $\begin{array}{c} \mathbb{C} \\ | \\ \mathbb{Q} \end{array}$ $\mathbb{C} - \mathbb{R} - \mathbb{Q}$

$\mathbb{R}/\mathbb{Q}$ denotes extension not quotient. (No such quotient anyway!)

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

$|$

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

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

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. Let $K = F[x]/(p(x))$, so K is a vector space over F, K/F. Then $\mathcal{B} = \{\bar{1}, \bar{x}, \overline{x^2}, \ldots, \overline{x^{n-1}}\}$ is a basis for K. Thus $[K:F] = \deg(p(x))$.

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

If $\overline{a(x)}, \overline{b(x)} \in K$ then $\overline{a(x)}\,\overline{b(x)} = \overline{r(x)}$

where $a(x)b(x) = q(x)p(x) + r(x)$ by division algorithm.

Inverses in K What is inverse of $\overline{a(x)}$?

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. $\overline{a(x)}\,\overline{g(x)} = 1$, $\overline{a(x)}^{-1} = \overline{g(x)}$

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

Euclidean Alg:

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

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

$1 = 1 \cdot 1 + 0$

$\rightsquigarrow 1 = (2x+2) - (2x+1)$

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

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

$\Rightarrow \overline{(2x+2)}^{-1} = \overline{(1+2x)}$

Roots of Polynomials

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

Ex $p(x) = x^2 - 2 \in \mathbb{Q}[x]$ has no root in $\mathbb{Q}$ but has root $\sqrt{2} \in \mathbb{R}$, $\mathbb{R}/\mathbb{Q}$

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

$$\begin{array}{c} K = F[x]/(p(x)) \\ | \\ F \end{array}$$

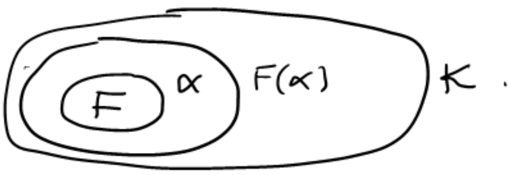
and $p(x) \in K[x]$ has root $\theta = \bar{x} \in K$ $\quad$ $\{ p(\bar{x}) = \overline{p(x)} = 0 \}$

Upshot: Given any field F and irreducible $p(x) \in F[x]$ there is an extension K/F containing a root of $p(x)$

Definitions Given K/F and $A = \{a_1, a_2, \cdots\} \subseteq K$ then field generated by A over F is

$$F(a_1, a_2, \cdots) = \bigcap_{\substack{F \subseteq J \subseteq K \\ A \subseteq J}} J = \left(\begin{array}{l} \text{intersection of all subfields} \\ J \text{ of } F \text{ containing } F \cup A \end{array} \right)$$

$F(a)$ is called a simple extension; a is its primitive element



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

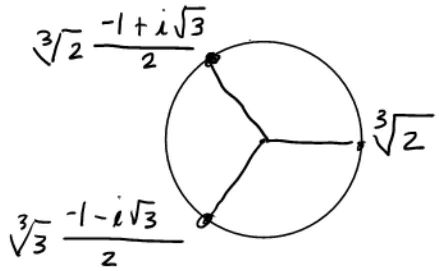
Proof Show $\begin{array}{ccc} F[x] & \longrightarrow & F(a) \\ f(x) & \longmapsto & f(a) \end{array}$ has kernel $(p(x))$. Use F.I.T. ∎

Consequence If $p(x)$ has roots $a_1, a_2, \cdots, a_k$, 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

$$\begin{array}{ccc} \mathbb{Q}(\sqrt[3]{2}) & \cong & \mathbb{Q}\left(\sqrt[3]{2}\left(\frac{-1+i\sqrt{3}}{2}\right)\right) \\ | & & | \\ \mathbb{R} & & \mathbb{C} \end{array}$$