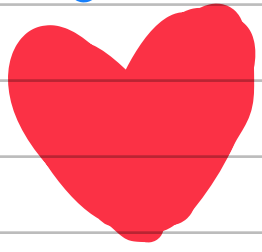
13.1 Basic Theory of Field Extensions



Characteristics

Def (Characteristic)
The Characteristic of a field F, denoted $ch(F)$, is the least positive integer p s.t. $p \cdot 1_F = 0$ if such p exists.
$ch(F)$ is defined to be 0 otherwise.

#1 Prop. $ch(F)$ is either 0 or a prime p. If $ch(F) = p$ then for any $\alpha \in F$,

$$p \cdot \alpha = \overbrace{\alpha + \alpha + \alpha + \dots + \alpha}^{p\ \alpha\text{'s}} = 0.$$

We only need to show that

Proof. (1) $ch(F) = p$.

By definition of a field: if $m, n \in \mathbb{Z}^+$, then

$$n \cdot 1_F + m \cdot 1_F = (m+n) \cdot 1_F \quad \text{and} \quad (n \cdot 1_F)(m \cdot 1_F) = mn \cdot 1_F.$$

Descent Argument!

If n is composite ($n = ab$) w/ $n \cdot 1_F = 0$, then $ab \cdot 1_F = (a \cdot 1_F) \cdot (b \cdot 1_F) = 0$
So one of $(a \cdot 1_F)$ and $(b \cdot 1_F)$ must necessarily be 0. If we keep reducing, the smallest such integer is a prime.

※ Also if $n \cdot 1_F = 0$, then $p \mid n$.

(2) $p \cdot \alpha$ part

$$p \cdot \alpha = \overbrace{\alpha + \alpha + \alpha + \dots + \alpha}^{p\ \alpha\text{'s}} = 0$$

(α: guaranteed by definition of a field; 0: ①)

① $p \cdot \alpha = p \cdot (\alpha \cdot 1_F) = (p \cdot 1_F) \cdot \alpha = 0 \cdot \alpha = 0$.

#2 Prop. There is a homomorphism $\varphi: \mathbb{Z} \to F$ given by

$$\varphi(n) = n \cdot 1_F.$$

Proof. $\varphi(m+n) = m \cdot 1_F + n \cdot 1_F = \varphi(m) + \varphi(n)$.

※ Note that the kernel of the action $\ker(\varphi) = ch(F)$ in $\mathbb{Z}$.
(in this case, $\ker(\varphi)$ maps to the additive identity 0_F).

Prime Subfield

Def. The <u>prime subfield</u> of F is the field generated by 1_F.

It is isomorphic to $\begin{cases} \mathbb{Q}, & ch(F) = 0 \\ \mathbb{F}_p, & ch(F) = p \end{cases}$

* Should be pretty easy to see.

Field Extension & Related topics.

#1 Def. (Field extension)

If K is a field containing subfield F, then K is an extension of F, denoted K/F or $\overset{K}{|}F$.

※ Every field is an extension of its prime subfield.

#2 Def. (Degree of Extension)

The degree of extension K/F, written $[K:F]$, is the dimension of K as a vector space over F.

Ex. (1) $[F:F]=1$ for all F.

(2) $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$: the two basis vectors are 1 and $\sqrt{2}$.

(3) $[\mathbb{Q}(\sqrt{2},\sqrt[3]{2}):\mathbb{Q}]=6$: the basis vectors are

$(2^{\frac{1}{6}}, 2^{\frac{1}{3}}, 2^{\frac{1}{2}}, 2^{\frac{2}{3}}, 2^{\frac{5}{6}}, 1)$

Th. (Field extension containing root exists)

Statement. Let F be a field & let $p(x)\in F[x]$ be an irreducible polynomial. Then there exists field K containing an isomorphic copy of F such that $p(x)$ has a root in K.

※ We assume that $p(x)$ irred. since for reducible $a(x)$, we can reduce it to irreducible $p(x)$ by taking $p(x)\mid a(x)$.

Proof: We can find this field extension K & prove that it contains a root of $p(x)$.

① Identify K.

Consider $K=F[x]/(p(x))$.

② Prove that K is a field.

We know that $F[x]/(a(x))$ is a ring for all $a\in F$. We only need to show that with the condition that $p(x)$ is irred, $F(x)/(p(x))$ is a field (i.e. show the multiplicative inverse law).

③ There exists an isomorphic copy of F in K.

Construct a map series by

$$F \overset{\cong}{\underset{\text{☺}}{}} F_1 \subset F[x] \cong F_1[x]/(p(x)) \subset F[x]/p(x).$$

④ $p(x)$ has a root in k.

Let φ denote the isomorphism $F \to F' \subset K$.

$$p(\varphi(x)) = \varphi(p(x)) = p(x) \pmod{p(x)} = 0.$$

Therefore $\varphi(x)$ is a root of p in K.

Follow-ups.

☺ It's pretty easy to see that there exists a copy of F in $F[x]$ (in fact, there are a lot of copies of F in $F[x]$). Note that numerically, $F \subset F[x]$.

Note: there is a version of this theorem that is slightly easier to prove:

Alternative Version:

If $p(x)$ irred. over F & a is a root of $p(x)$, then

$$F(a) \cong F[x]/(p(x)).$$

Will prove this later.

(When you see Wilbur, this means that this is an important result for the research topic.)

Th. (What does K look like?)

Let $p(x) \in F[x]$ irred. of degree n & $K = F[x]/p(x)$.

Let $\alpha = x \pmod{p(x)} \in K$. Then the elements

$$1, \alpha, \alpha^2, \dots, \alpha^{n-1}$$

form a basis for the vector field of K/F. Therefore $[K/F] = n$.

※ Saying $\alpha = x \pmod{p(x)}$ is equivalent to saying $p(\alpha) = 0$.

This gives that all elements in the field extension K can be written as

$$K = \{a_0 + a_1\theta + a_2\theta^2 + \dots + a_{n-1}\theta^{n-1} \mid a_0, a_1, \dots, a_{n-1} \in F\}.$$

Ex: (1) $\mathbb{R}[x]/(x^2+1) \cong \mathbb{R}[i] = \mathbb{C}$.

For $z \in \mathbb{C}$, z can be written as $a+bi$ for $a, b \in \mathbb{R}$.

(2) $\mathbb{Q}[x]/(x^2-2) \cong \mathbb{Q}[\sqrt{2}]$.

For $m \in \mathbb{Q}[\sqrt{2}]$, $m = a + b\sqrt{2}$ for some $a, b \in \mathbb{Q}$.

(The fact that $\mathbb{Q}[\sqrt{2}]$ is a field could be proven with arithmetic.)

(3) $\mathbb{Q}[x]/(x^3-2) \cong \mathbb{Q}[\sqrt[3]{2}, \sqrt[3]{4}]$.

For $\theta \in \mathbb{Q}[x]/(x^3-2)$, $\theta = a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2$ for $a, b, c \in \mathbb{Q}$.

Cor. (Euclidean Algorithm & Inverses)

If $\theta \in K$ is a root of the irred. poly $p(x) = p_n x^n + \dots + p_1 x + p_0$,

then we can find $\theta^{-1} \in K$:

$$\theta(p_n\theta^{n-1} + \dots + p_1) = -p_0$$

$$\theta^{-1} = -\frac{1}{p_0}(p_n\theta^{n-1} + p_{n-1}\theta^{n-2} + \dots + p_1) \in K.$$

Def. (Simple Extensions)

If field K is generated by a single element α over F ($K = F(\alpha)$), then K is said to be a simple extension.

Conversely, if $K = F(\alpha, \beta, \dots)$, then K is not simple.

Th. $(F(\alpha) \cong F[x]/p(x))$

Let $p(x)$ be a deg n irred. poly over F and α be a root of $p(x)$. Then

$$F(\alpha) \cong F[x]/p(x).$$

Proof Consider the map $\varphi: F[x]/p(x) \to F(\alpha)$

$$\varphi(c_0 + c_1x + c_2x^2 + \cdots + c_{n-1}x^{n-1}) = c_0 + c_1\alpha + \cdots + c_{n-1}\alpha^{n-1}$$

① φ is a homomorphism.

$$\varphi(f_1(x)f_2(x)) = f_1(\alpha)f_2(\alpha) = \varphi(f_1(x))\varphi(f_2(x)).$$

② φ is a bijection.

Injectivity: Both $F[x]/p(x)$ and $F(\alpha)$ are fields, and φ is not the 0 map, so φ is necessarily injective.

Surjectivity: Apparently.

$\Rightarrow$ φ is an isomorphism.

※ This tells us that $F(\alpha)$ is the same field regardless of which α is adjoined, i.e. the roots of $p(x)$ are algebraically equivalent.

We can prove it:

Th. (Roots of $p(x)$ are algebraically equivalent.)

Let $\varphi: F \to F'$ be an isomorphism of fields. Let $p(x) \in F[x]$ be irred. & let the polynomial obtained by applying φ to the coefs of $p(x)$ be $p'(x) \in F'[x]$. Let α be a root of $p(x)$ in some extension of F & let β be a root of $p'(x)$ in some extension of F'. Then there is an isomorphism σ:

$$\sigma: F(\alpha) \longrightarrow F'(\beta)$$

that ① maps α to β and ② fixes $\varphi: F \to F'$.

Proof. Some lemmas on ideals:

Lemma #1. An isomorphism (of any Principal Ideal Domain) maps the maximal ideal to another maximal ideal.

Lemma #2. $p(x) \in F[x]$ is irreducible $\Leftrightarrow (p(x))$ is the maximal ideal of $F[x]$.

Anyway:

There exists a natural isomorphism $F[x] \cong F'[x]$ obtained by applying φ to all the coefs of $F'[x]$. This isomorphism maps the maximal ideal $(p(x))$ to $(p'(x))$, so $(p'(x))$ is also maximal, and $p'(x)$ is irred. over $F'[x]$.

We can therefore take the quotients of the ideals:

$$F[x]/(p(x)) \xrightarrow{\sim} F'[x]/(p'(x))$$

(Both $p(x)$ & $p'(x)$ are irred. so $F[x]/(p(x))$, $F'[x]/(p'(x))$ are fields.)

Since $F[x]/(p(x)) \cong F(\alpha)$ & $F'[x]/(p'(x)) \cong F(\beta)$,

$$\boxed{F(\alpha) \cong F(\beta).}$$

※ This isomorphism restricted to F is exactly $\varphi: F \xrightarrow{\sim} F'$.

This theorem will be incredibly useful in Galois Theory:

it can be represented by the (familiar) diagram

$$\begin{array}{ccc} \sigma: & F(\alpha) & \xrightarrow{\sim} F(\beta) \\ & | & | \\ \varphi: & F & \xrightarrow{\sim} F' \end{array}$$