Intro to Algebra W3-1

fat

March 6, 2024

13.1 Basics of field extensions

Definition 1. The **characteristic** of a ring R (denoted by $char(R)$) with 1 is the smallest positive integer n s.t. $n \cdot 1 = 0$. If no such integer exists, we define the characteristic of R to be 0.

Example 1.
- $char(\mathbb{Z}/n\mathbb{Z}) = n$.
- $char(\mathbb{Q}) = char(\mathbb{R}) = char(\mathbb{Z}) = 0$.

Proposition 1. Let D be an integral domain. Then $char(D)$ is either 0 or a prime P.

Proof.

Assume $char(D) = n \neq 0$. If n is not a prime, say $n = ab$, where $a, b > 1$, we consider

$$(a \cdot 1)(b \cdot 1) = n \cdot 1 = 0$$

Since n is the smallest positive integer s.t. $n \cdot 1 = 0$, we have $a \cdot 1, b \cdot 1 \neq 0$. This contradicts to the assumption that D is an integral domain. □

Proposition 2. Let F be a field. If $char(F) = 0$, then F contains a subfield isomorphic to $\mathbb{Q}$. If $char(F) = p$, then F contains a subfield isomorphic to $\mathbb{Z}/p\mathbb{Z}$.

Proof.

Assume $char(F) = 0$. Define a ring homomorphism $\phi : \mathbb{Q} \to F$ by $\phi(m/n) = m \cdot 1/n \cdot 1$. It is easy to see that it's injective $\Rightarrow \mathbb{Q} \simeq Im(\phi) \subseteq F$. If $char(F) = p$, we consider $\phi : \mathbb{Z}/n\mathbb{Z} \to F$ defined by $\phi(m) = m \cdot 1$ instead. □

Definition 2. The field $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ in the proposition is called the **prime subfield** of F.

Remark 1. The proposition also shows that every field of p elements is isomorphic to $\mathbb{Z}/p\mathbb{Z}$. ϕ in this case is both injective and surjective, so ϕ is an isomorphism. That is, up to isomorphisms, there is only 1 field of p elements. We often denote the field by $\mathbb{F}_p$.

Definition 3. If K is a field containing a subfield F, we say K is a **extension field** of F. Sometimes we call F the **base field** or the **ground field** in the extension K/F. (Note that the meaning of K/F differs from that of quotient rings or quotient groups.)

Definition 4. Let K/F be a field extension. Let $\alpha, \beta, \gamma, ... \in K$. The smallest subfield of K containing $F, \alpha, \beta, \gamma, ...$ is called the **subfield generated by** $\alpha, \beta, \gamma, ...$ **over** F and is denoted by

$$F(\alpha, \beta, \gamma, ...) = \left\{ \frac{f(\alpha, \beta, \gamma, ...)}{g(\alpha, \beta, \gamma, ...)} : g \neq 0, f \in F[\alpha, \beta, \gamma, ...] \right\}$$

If $K = F(\alpha)$ for some $\alpha \in K$, then we say K/F is a **simple extension** and α is a **primitive element** in the extension K/F.

Example 2. For example, $\mathbb{C} = \mathbb{R}(i)$ is a simple extension of $\mathbb{R}$ and i (or any $a + bi$ with $a, b, \in \mathbb{R}, b \neq 0$) is a primitive element.

Observation: If K is an extension field of F, then K is is a vector space over F.

Definition 5. The **degree** of K/F is defined to be the dimension of K as a vector space over F. The degree of K/F will be denoted by $[K : F]$. (i.e. $[K : F] := dim_F(K)$) (For example, $[\mathbb{C} : \mathbb{R}] = 2$.) If $[K : F] < \infty$, then we say K/F is a **finite extension**.

Remark 2. Thus, for example, if K is a finite extension of $\mathbb{F}_p$, then $|K| = p^{[K:\mathbb{F}_p]}$ is a prime power. (Say $\{\alpha_1, ..., \alpha_n\}$ is a basis, then $K = \{a_1\alpha_1 + \ldots + a_n\alpha_n : a_j \in \mathbb{F}_p\} \Rightarrow |K| = p^n$) This, together with an earlier proposition shows that the cardinality of a finite field must be a prime power.

Proposition 3. Let F, F' be 2 fields and $\phi : F \to F'$ is a ring homomorphism. Then either ϕ is identically 0, or ϕ is injective.

Proof.

$ker\phi$ is an ideal of F. A field F has only 2 ideals $\{0\}, F$. If $ker\phi = \{0\}, \phi$ is injective, else $\phi = 0$. □

Recall that one motivation to introduce $\mathbb{C}$ is to solve the equation $x^2 + 1 = 0$.

Theorem 1. Let $p(x)$ be an irreducible polynomial in $F[x]$. Then $\exists$ an extension field K s.t. $p(x)$ has a root in K.

Proof.

Let $K = F[x]/(p(x))$. By Prop 15 of Chapter 9, K is a field. It contains F as a subfield. (To be more rigorous, K contains a subfield $\{a + (p(x)) : a \in F\}$ which is isomorphic to F.) It's clear $\alpha = x + (p(x)) \in K$ is a root of $p(x)$. $(p(\alpha) = p(x) + (p(\alpha)) = 0 + (p(x)))$ □

Definition 6. Let K/F be a field extension. An element $\alpha \in K$ is said to be **algebraic over** F is α is a root of some nonzero polynomial over F. If no such polynomials exist, then we say α is **transcendental** over F. If every element of K is algebraic over F, then we say K is an **algebraic extension of** F. In the case of $\mathbb{Q}$, a number $\alpha \in \mathbb{C}$ is an **algebraic number/transcendental number** if α is algebraic/transcendental over $\mathbb{Q}$.

Example 3. (1) $\sqrt{2}$ is an algebraic number. (i.e. $\sqrt{2}$ is algebraic over $\mathbb{Q}$.)

(2) π is transcendental over $\mathbb{Q}$. (Lindemann)

(3) $\sqrt{\pi}$ is transcendental over $\mathbb{Q}$, but is algebraic over $\mathbb{Q}(\pi)$. ($\sqrt{\pi}$ is a root of $x^2 - \pi \in \mathbb{Q}(\pi)[x]$.)

Proposition 4. Assume α is algebraic over F. Then $\exists!$ monic irredubcible polynomial $m_{\alpha,F}(x) \in F[x]$ s.t.

$$\begin{cases} \alpha \text{ is a root of } m_{\alpha,F}(x) \\ \text{a polynomial } f(x) \text{ has } \alpha \text{ as a root } \Leftrightarrow m_{\alpha,F}(x)|f(x) \end{cases}$$

Proof.

Let $I_\alpha := \{f(x) \in F[x], f(\alpha) = 0\}$. It's straightforward to check that I is an ideal of $F[x]$. By the assuumption that α is algebraic over F, $I_\alpha \neq \{0\}$. Let $p(x)$ be a polynomial s.t. $I_\alpha = (p(x))$. Check $p(x)$ is irreducible. Assume $p(x) = a(x)b(x), a(x), b(x) \in F[x]$. We want to show that one of $a(x), b(x)$ is a unit, i.e. one of $a(x), b(x)$ is a nonzero constant polynommial. Now we have

$$a(\alpha)b(\alpha) = p(\alpha) = 0$$

$$\Rightarrow a(\alpha) = 0 \text{ or } b(\alpha) = 0$$

If $a(\alpha) = 0$, then $a(x) \in I_\alpha = (p(x))$

$$\Rightarrow p(x)|a(x)$$

$$deg(a(x)) \geq deg(p(x)) \geq deg(a(x))$$

$$\Rightarrow deg(a(x)) = deg(p(x)) = deg(b(x)) = 0$$

$\Rightarrow b(x)$ is a nonzero constant polynomial, i.e. $b(x) \in F[x]^\times$. Likewise, if $b(\alpha) = 0$, then $a(x) \in F[x]^\times$. This proves that $p(x)$ is irreducible. Set

$$m_{\alpha,F}(x) = \frac{1}{(\text{leading coefficients of } p(x))} p(x)$$

Then $m_{\alpha,F}(x)$ is the polynomial with the claimed properties. $\square$

Definition 7. The polynomial $m_{\alpha,F}(x)$ is called the **minimal polynomial** of α over F. We define the **degree** of α over F to be $deg(m_{\alpha,F}(x))$.

Theorem 2. Assume that α is algebraic over F. Let $n = deg(m_{\alpha,F}(x))(= deg_F(\alpha))$. Then

(1) $F[\alpha] = F(\alpha) \left(= \frac{f(\alpha)}{g(\alpha)}\right) \simeq F[x]/(m_{\alpha,F}(x))$.

(2) $[F(\alpha) : F] = n$.

(3) $\{1, \alpha, ..., \alpha^{n-1}\}$ is a basis of $F(\alpha)$ over F.