Field Theory

TRISCT

Contents

Part I
Field Theory

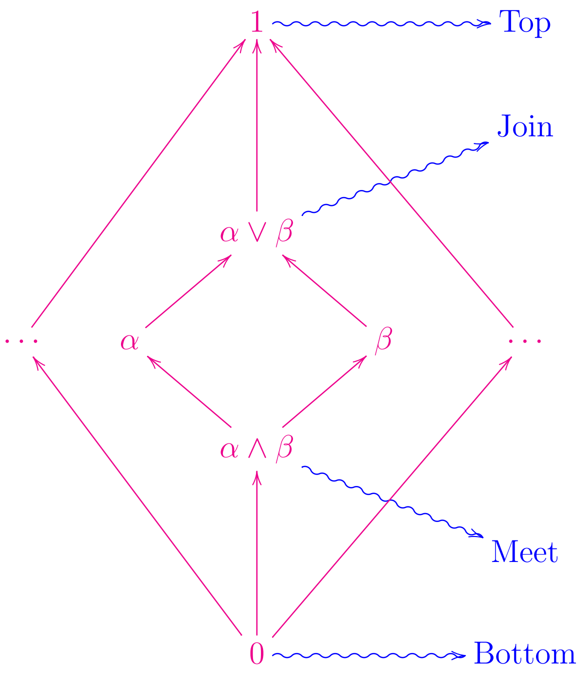
1 Field Extensions

1.1 Definitions and Properties

Poset A **poset** is a nonempty set P together with a binary relation $\leqslant$ satisfying reflexivity, antisymmetry and transitivity. An **upper bound** (resp. **lower bound**) $a \in P$ for a subset $S \subset P$ is such that $\forall x \in S,\ x \leqslant a$ (resp. $a \leqslant x$). The **least upper bound** is an upper bound which is also the lower bound of all upper bounds, and the **greatest lower bound** is defined similarly. A **maximal element** (resp. **minimal**) in P is one such that there is no other element strictly large (resp. smaller) than it. A **top element** (resp. bottom) is such that every element is smaller (resp. larger) than or equal to it, which is usually denoted by 1, and the bottom element is usually denoted by 0.

Lattice A poset L becomes a **lattice** if we require that any pair of elements a, b has a least upper bound, called **join**, denoted by $\alpha \vee \beta$, in P, and a greatest lower bound, called **meet**, denoted by $\alpha \wedge \beta$, in P. If every nonempty subset of L has a join and a meet, then L is called a complete lattice. A **sublattice** is a subset of a lattice which is closed under the taking of join and meet in the sense that the join and meet are the same if taken in the original lattice.

Note 1.1. An illustration is as follows (arrows mean "going to the larger element"). In short, $\vee$ always denotes something like "larger" or "union".



The following criterion tells us when a subset becomes a complete lattice. Let L be a complete lattice and $\varepsilon \neq S \subset L$. If $1 \in S$ and S is closed under arbitrary intersection, then S is itself a complete lattice, but not necessarily a sublattice because the join of a subset in S may not be identical if taken in L.

Lattice of subfields Let K be a field. For the subfields $E, F < K$, we can define the operations

(i) (**Intersection**) The intersection $E \cap F$ of E, F is also a subfield of K. More generally, the intersection of an arbitrary family of subfields is a subfield. One can see that the intersection is the meet.

(ii) (**Composite**) The composite EF of E, F is the smallest subfield containing E, F, i.e., the intersection of all subfields containing E, F, or again, the field generated by E, F. More generally, the composite $\bigvee E_i$ of a family of subfields is the smallest subfield containing every E_i. One can see that the composite is the join.

The collection of all subfields of a field form a complete lattice, with the join being composite and the meet being intersection. It has top $1 = K$ and bottom $0 = K_p$ (the prime subfield of K, either $\mathbb{Z}_p$ or $\mathbb{Q}$).

Types of extensions Let $F < E$ be a field extension. We shall define some descriptors for elements in E first. An element $a \in E$ is called

(i) **algebraic** over F if a satisfies some polynomial over F.

(ii) **transcendental** if it is not algebraic.

(iii) **separable** if it is algebraic, and its minimal polynomial is separable.

A field extension $F < E$ is called

(i) **algebraic** if every $a \in E$ is algebraic over F.

(ii) **transcendental** if some $a \in E$ is transcendental over F.

(iii) **simple** if $E = F(a)$ for some $a \in E$, and such a is called a **primitive element** of E.

(iv) **finite** if $[E : F]$ is finite.

(v) **finitely generated** if $E = F(S)$ for some finite set $S \subset E$.

(vi) **separable** if every $s \in E$ is separable.

(vii) **normal** if E is the splitting field of a family of polynomials over F.

(viii) **Galois** if it is both separable and normal.

(ix) **distinguished** if it satisfies the **tower property**, the **lifting property** and is **closed under finite compositions**.

The following illustrations show the mutual implications of different kinds of extensions.

$$\begin{tikzcd}
\text{finitely generated algebraic} \arrow[d, Leftrightarrow] \\
\text{finite} \arrow[d, shift left, "\text{char}=0"] \\
\text{simple algebraic} \arrow[u, Rightarrow, shift left]
\end{tikzcd}$$

Embedding An **embedding** of a field F into a ring R is ring monomorphism $f : F \hookrightarrow R$. Since F contains no nontrivial ideal, f is an embedding as long as it is nonzero. Let $F < E$ be an extension and let $\sigma : F \hookrightarrow L$ and $\overline{\sigma} : E \hookrightarrow L$ be two embeddings. If $\overline{\sigma}|_F = \sigma$, then $\overline{\sigma}$ is called an **extension** of σ. If $\overline{\sigma}$ is an extension of id_F, the $\overline{\sigma}$ is called an **embedding over** F or an F**-embedding**. The set of all embeddings form E to L is denoted by $\mathrm{Hom}(E, F)$. We also use the following notations as well.

(i) Let $\sigma : F \hookrightarrow L$ be an embedding and $F < E$. Define $\mathrm{Hom}_\sigma(E, L) = \{\tau \in \mathrm{Hom}(E, L) : \tau|_F = \sigma\}$ to be all possible extensions of σ.

(ii) Let $F < E$. Define $\mathrm{Hom}_F(E, L) = \{\tau \in \mathrm{Hom}(E, L) : \tau|_F = \mathrm{id}_F\}$ to be all embeddings over F.

An embedding $\sigma : F \hookrightarrow L$ naturally gives rise to a mapping between polynomials. If $p(x) = a_0 + a_1x + \cdots + a_nx^n \in F[x]$, then $(\sigma p)(x) = p^\sigma(x) = (\sigma a_0) + (\sigma a_1)x + \cdots + (\sigma a_n)x^n$ is a polynomial in $L[x]$. If x is an indeterminant, then σ does not have any effect on it; if x is an element in F, then we have $\sigma(p(x)) = p^\sigma(x^\sigma)$. Embeddings have the following properties.

(i) (**Preserving factorization and roots**) Let $\sigma : F \hookrightarrow L$ be an embedding, $f, p, q \in F[x]$ and $\alpha \in F$.

$$f(x) = p(x)q(x) \iff f^\sigma(x) = p^\sigma(x)q^\sigma(x)$$

$$f(\alpha) = 0 \iff f^\sigma(\alpha^\sigma) = 0$$

(ii) (**Preserving the lattice structure**)

(iii) (**Preserving the adjoining**)

(iv) (**Preserving algebraicness**)

(v) (**Preserving algebraic closures**)

2 Topics

2.1 Embeddings

The question to find all possible extensions of an embedding from a field is of vital importance in the field theory, for these embeddings provide a good view of the structure of the field. Let $\sigma : F \hookrightarrow L$ be an embedding. In order not to let the possibilities be limited by L, we assume that L is algebraically closed.

Simple case First we consider the simple case. Let $\sigma : F \hookrightarrow L$ be an embedding where L is algebraically closed. From some extension E of F we choose an algebraic element $\alpha \in E$. The following theorem describes all possible extensions of $\sigma : F \hookrightarrow L$ to $F(\alpha)$.

Theorem 2.1. *Let $\sigma : F \hookrightarrow L$ be an embedding. Choose an algebraic element α over F and denote its minimal polynomial by $p_\alpha = \min(\alpha, F)$. Then*

$$\tau \in \mathrm{Hom}_\sigma(F(\alpha), L) \iff \tau(\alpha) \textit{ is a root of } p^\sigma_\alpha(x)$$

And therefore there are exact as many extensions of σ to $F(\alpha)$ as the number of distinct roots of $\min(\alpha, F)$.

Proof. A more precise way to state the theorem is that, any mapping $\tau : F \cup \{\alpha\} \to L$ such that

$$\tau|_F = \sigma, \quad \tau(\alpha) \text{ is a root of } p_\alpha^\sigma(x)$$

can be extended to an embedding $\tau : F(\alpha) \hookrightarrow L$. Conversely, any embedding that extends σ is such an extension of mapping. We shall prove this now.

(i) Since α is algebraic, we have

$$F(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} : p_\alpha(\alpha) = 0\} \cong F[x]/(p_\alpha(x))$$

where $n = \deg p_\alpha$. If β is any root of p_α^σ, and we set $\tau(\alpha) = \beta$, then for any $a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \in F(\alpha)$, its image under τ is uniquely determined (by the tentative property of τ being a homomorphism):

$$\begin{aligned} \tau(a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}) &= \tau(a_0) + \tau(a_1)\tau(\alpha) + \cdots + \tau(a_{n-1})\tau(\alpha^{n-1}) \\ &= \sigma(a_0) + \sigma(a_1)\beta + \cdots + \sigma(a_{n-1})\beta^{n-1} \end{aligned}$$

For this to be well-defined, τ must not contradict with the only other restriction that $p_\alpha(\alpha) = 0$, i.e., it must hold that

$$0 = \tau(0) = \tau(p_\alpha(\alpha)) = p_\alpha^\tau(\alpha^\tau) = p_\alpha^\sigma(\beta)$$

But this is true by our assumption that β is a root of p_α^σ.

Note 2.1. Another way to see why this is the only other restriction is to think of τ as an embedding from $F[x]/(p_\alpha(x))$ such that $\tau(\overline{x}) = \beta$. The embedding, defined on the quotient ring of polynomials, is well-defined if the image of an equivalence class does not depend on the choice of the representative, i.e., τ maps $p_\alpha(x)$ to 0.

(ii) Conversely, any embedding $\tau \in \mathrm{Hom}_\sigma(F(\alpha), L)$ satisfies

$$0 = \tau(0) = \tau(p_\alpha(\alpha)) = p_\alpha^\sigma(\alpha^t au)$$

i.e., α^τ is a root of p_α^σ.

The proof above says that there is a one-to-one correspondence from all extensions $\mathrm{Hom}_\sigma(F(\alpha), L)$ of $\sigma : F \hookrightarrow L$ to all distinct roots of $\min(\alpha, F)$, hence the two sets have the same cardinality.

The following is an illustration of extending an embedding. Let $\sigma : F \hookrightarrow L$ be an embedding. Let $p(x)$ be the minimal irreducible polynomial of α over F, and write $p^\sigma(x) = (x-\beta_1)^{m_1} \cdots (x-\beta_k)^{m_k}$ where $\beta_1, \cdots, \beta_k$ are distinct (if p^σ is separable, then $m_i = 1$).

$$\begin{tikzcd}
 & & F \arrow[d] & & & \\
 & & \alpha \arrow[d, dash] \arrow[dr, dash] \arrow[drrr, dash] & & & \\
p^\sigma(x) & = & (x-\beta_1)^{m_1} \arrow[d] & (x-\beta_2)^{m_2} \arrow[d] & \cdots & (x-\beta_k)^{m_k} \arrow[d] \\
 & & \tau_1 & \tau_2 & \cdots & \tau_k
\end{tikzcd}$$

Embeddings of an algebraic number field In the algebraic number theory, we are most concerned about embeddings of an algebraic number field. Such embeddings are of the form $\sigma : K \hookrightarrow \mathbb{C}$ where $K/\mathbb{Q}$ is an algebraic number field. Any embedding, as a ring homomorphism, must preserve 1 and hence the prime field ($\mathbb{Q}$ in this case). Therefore, we may think of σ as an extension of the identity mapping $\mathrm{id}_{\mathbb{Q}}$ on $\mathbb{Q}$. We can then apply Theorem.2.1. to this.

Let $\sigma : K \hookrightarrow \mathbb{C}$ be an embedding of an algebraic number field K. Since $\mathrm{char}\mathbb{Q} = 0$, the primitive element theorem says $K = \mathbb{Q}(\alpha)$ for some algebraic element $\alpha \in K$. We suppose α has the minimal polynomial $p_\alpha(x) = \min(\alpha, \mathbb{Q})(x) \in \mathbb{Q}[x]$ with $\deg p_\alpha = n = [K : \mathbb{Q}]$. Also, $\mathrm{char}\mathbb{Q} = 0$ implies that p_α is separable, hence it has exactly n roots in $\mathbb{C}$, and Theorem.2.1. says there are exactly n embeddings $\sigma : K \hookrightarrow L$ over $\mathbb{Q}$, mapping α to the n distinct roots of p_α.

Example 2.1. Consider the field extension $\mathbb{Q} < \mathbb{Q}(\zeta)$ where $\zeta = e^{2\pi i/3}$. We have $p(x) = \min(\zeta, \mathbb{Q}) = x^2 + x + 1 = (x-\zeta)(x-\zeta^2)$. Then the only possible embeddings are

$$\sigma_1 : \mathbb{Q}(\zeta) \to \mathbb{C},\ \zeta \mapsto \zeta \quad \text{and} \quad \sigma_2 : \mathbb{Q}(\zeta) \to \mathbb{C},\ \zeta \mapsto \zeta^2$$

□

Note that the complex roots of $p_\alpha(x)$ appear in pairs. Suppose

$$p_\alpha(x) = (x-r_1)\cdots(x-r_s)(x-r_{s+1})(x-\overline{r}_{s+1})\cdots(x-r_{s+t})(x-\overline{r}_{s+t})$$

where r_i $(1 \leqslant i \leqslant s)$ are real roots and $r_{s+j}, \overline{r}_{s+j}$ $(1 \leqslant j \leqslant t)$ are nonreal complex roots. Let $\sigma_i : K \hookrightarrow \mathbb{C}$ be the embedding such that $\alpha \mapsto r_i$ $(1 \leqslant i \leqslant s+t)$

and $\overline{\sigma}_i : K \hookrightarrow \mathbb{C}$ the embedding such that $\alpha \mapsto \overline{r}_i$ $(s+1 \leqslant i \leqslant s+t)$. We claim that $\sigma_1, \cdots, \sigma_s$ are **real embeddings**, i.e., $\sigma_i(K) \subset \mathbb{R}$, because they map the primitive elements to a real number, and hence the image of $K = \mathbb{Q}(\alpha)$ under each σ_i $(1 \leqslant i \leqslant s)$ is contained in $\mathbb{R}$. Similarly, the other embeddings are **complex embeddings**.

For further applications of these embeddings see the algebraic number theory part.

Index