Field Theory

Boran Erol

April 2024

1 Definitions and Basic Properties

Definition 1. If L, K are fields with $K \subseteq L$, L is said to be a **field extension of** K.

Notice that L can be given the structure of a vector space over K. The reason we study a pair of fields when we study fields is that we often consider a chain of fields $L_0 \subseteq L_1 \subseteq ... = L$, which helps us prove facts about L is itself.

Definition 2. The **degree of an extension** L/K is the dimension of L as a vector space over K. This is also denoted $[L : K]$.

Definition 3. L/K is **finite dimensional** if $[L : K]$ is finite.

Definition 4. Let L/K and $\alpha \in L$. α is **algebraic** over K if $\exists f \in K[x] : f(\alpha) = 0$. Otherwise, α is called **transcendental**.

Example 1.1. Here's a silly example. Consider $\mathbb{Q} \subseteq \mathbb{Q}(x)$, where $\mathbb{Q}(x)$ is the field of rational functions over $\mathbb{Q}$. Then, $x \in \mathbb{Q}(x)$ is transcendental over $\mathbb{Q}$.

Example 1.2. e and π are transcendental over $\mathbb{Q}$, but the proof is complicated.

In fact, proving that $e+\pi$ and $e\pi$ are transcendental is an open problem. However, it's incredibly simple to prove that one of them is transcendental.

Lemma 1.3. Let L/K and let $p \in K[x]$ a polynomial with algebraic coefficients and assume $p(\alpha) = 0$. Then, α is algebraic.

Proof. Let $p = a_0 + a_1x + ... + a_nx^n$ □

Theorem 1.4. Either $e + \pi$ or $e\pi$ is transcendental.

Proof. Consider $p(x) = x^2 = (e + \pi)x + e\pi$. The roots of this polynomial are e and π. If $e + \pi$ and $e\pi$ are both algebraic, the roots would also be algebraic, which is a contradiction. Therefore, at least one of them needs to be transcendental. □

Definition 5. L/K is **algebraic** if $\forall \alpha \in E : \alpha$ is algebraic over K.

Lemma 1.5. If E/K is finite, E/K is algebraic.

Proof. We prove the contrapositive. If E/K is not algebraic, there's some $\alpha \in E$ that's not algebraic over K. Then, the powers of α are K-independent and therefore E/K is not finite. □

Lemma 1.6. Let $K \subseteq L \subseteq E$ be finite field extensions. Then, $[E : K] = [E : L][L : K]$.

Proof. Let $x_1, ..., x_n$ be a basis for E/L and $y_1, ..., y_k$ be a basis for L/K. We will prove that x_iyi is a basis for E/K.

Let's first show that it spans. Let $\alpha \in E$. Then,

$$\alpha = \sum_{i=1}^{n} a_i x_i$$

, where $a_i \in L$. Then,

$$\alpha = \sum_{i=1}^{n} \sum_{j=1}^{k} b_{i,j} x_i y_j$$

, where $b_{i,j} \in K$.

Thus, $x_i yi$ spans E/K.

Let's now prove independence.

Assume

$$\exists c_{i,j} \in K : \sum_{i=1}^{n} (\sum_{j=1}^{k} c_{i,j} y_j) x_i$$

.

Using the fact that x_i is a basis followed up by the fact that y_j is a basis concludes the proof. □

Nathan suggests seeing this through a functional lens. The spanning step is surjectivity and the linear independence is injectivity.

Example 1.7. Let's now show that $[\mathbb{Q}[\sqrt{2}, \sqrt[3]{3}] : \mathbb{Q}] = 6$.

Let $E = \mathbb{Q}[\sqrt{2}, \sqrt[3]{3}]$, $L = \mathbb{Q}[\sqrt{2}], K = \mathbb{Q}$. Notice that $[L : K] = 2$.

Now, let $L' = \mathbb{Q}[\sqrt[3]{3}]$. Notice that $[L' : K] = 3$.

Thus, 2 and 3 divide $[E : K]$ so $[E : K] \geq 6$.

$[E : K] \leq 6$ as well since

Let's now solve another example using brute force.

Example 1.8. Let's now show that $[\mathbb{Q}[\sqrt{2}, \sqrt{3}] : \mathbb{Q}] = 4$.

Let $E = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$, $L = \mathbb{Q}[\sqrt{2}], K = \mathbb{Q}$.

We'll show that $\forall a, b \in Q : \sqrt{3} \neq a\sqrt{2} + b$, therefore proving that $[E : L] > 1$.

Assume by contradiction that $\exists a, b \in Q : \sqrt{3} \neq a\sqrt{2} + b$.

...

Justify the existence of $m_\alpha(x)$.

Let E/K be a field extension and $\alpha \in E$. Let $K(\alpha)$ be the smallest subfield in E containing α. Notice that $K(\alpha)$ will contain $\frac{f(\alpha)}{g(\alpha)}$ for any $f, g \in K[x]$.

Lemma 1.9. Let E/K be a field extension and $\alpha \in E$ be algebraic over K. Then, $K(\alpha) = K[\alpha]$.

Proof. Let's first show that $K[\alpha]$ is a field. Let $0 \neq f \in K[\alpha]$.

Since $m_\alpha(x)$ is an irreducible polynomial, f and m_α are relatively prime. Then, by Bezout's Identity, $\exists g, h \in K[x]$:

$$g(x)p(x) + h(x)f(x) = 1$$

Since $p(\alpha) = 0$, $h(\alpha)f(\alpha) = 1$ and $h = f^{-1}$.

Let's now show that $K[\alpha]$ is the smallest subfield of E that contains α.

... □

Let's now demonstrate how this gives us an algorithm for finding inverses in $K[\alpha]$.

Let $f(x) = ax + b$ and $p(x) = x^2 - d$.

One goal of Galois Theory is to understand the following: Given a field extension $F \subset K$, how many fields are between F and K? In other words, how many E are there such that $F \subset E \subset K$?

Let $F \subset K$ be a field extension and $\alpha \in K$. The evaluation map at α produces a map $eval_\alpha : F[X] \to K$ with $p(x) \mapsto p(\alpha)$. We denote by $F[\alpha]$ the image of this map. In other words, $F[\alpha]$ is the F-linear span of $\{1, \alpha, \alpha^2, ...\}$.

$F[\alpha]$ is a subring of K. In general, however, it's not a subfield.

Example 1.10. Consider $\mathbb{R} \subset \mathbb{C}$ and $\alpha = i$. Then, $\mathbb{R}[i] = \mathbb{C}$.

Example 1.11. Consider $\mathbb{Q} \subset \mathbb{C}$ and let α be transcendental. Then, $\mathbb{Q}[\alpha] =$. WHO KNOWS FIGURE THIS OUT?

Notice that the definition of algebraicity can be reformulated as requiring that $dim_F(F[\alpha]) < \infty$.

It's difficult to figure out whether a number is transcendental over $\mathbb{Q}$.

Example 1.12. Let $\mathbb{Q} \subset \mathbb{C}$ and $\alpha = \sqrt{2}$. Notice that $\mathbb{Q}[\alpha]$ is spanned by 1 and $\sqrt{2}$.

Let F, F' be fields and $F \xrightarrow{\phi} F'$ be an isomorphism.

We can extend ϕ to be a ring isomorphism between $F[X]$ and $F'[X]$ that applies ϕ to the coefficients.

Let $p \in F[X]$ be a non-constant polynomial and let $p' = f(p) \in F'[X]$.

2 Algebraic Closure

Definition 6. Let F be a field. F is **algebraically closed** if every polynomial in f can be factored into linear factors.

Notice that a polynomial $f \in F[x]$ is irreducible if and only if $deg(f) = 1$.

Definition 7. Let K/F be a field extension. We say that K is an **algebraic closure of** F if $F \subset K$, K is algebraically closed and K is minimal with these properties. In other words, if E is algebraically closed and $F \subset E \subset K$, $E = K$.

Lemma 2.1 (Fundamental Theorem of Algebra)**.** $\mathbb{C}$ is algebraically closed.

You can also prove this using analytical techniques.

Example 2.2. $\bar{\mathbb{Q}} \subseteq \mathbb{C}$ is algebraically closed.

Example 2.3. Puiseux series with cool complex analysis stuff.

Theorem 2.4 (Uniqueness of Algebraic Closures)**.**

There's no unique isomorphism between algebraic closures. This is a problem for category theorists.

This problem is related to defining the fundamental group of a topological space X.