Field Theory, Part 1: Basic Theory and Algebraic Extensions

Jay Havaldar

1.1 Introduction

Recall that a field is a commutative ring in which every nonzero element has a multiplicative inverse.

Definition: The **characteristic** of a field is the additive order of 1. For example, if $1+1+1=0$, then we say the field has characteristic 3. If $1+1+\ldots$ is never equal to 0, we say the field has characteristic 0. The characteristic of a field is either 0 or a prime.

Denote $1+1+\cdots+1$, added n times, we denote this element $n \cdot 1$. For each field F, we have a natural homomorphism $\mathbb{Z} \to F$, which maps n to $n \cdot 1$. Note that a homomomorphism into a field is either zero identically or an isomorphism; thus the image of this map can be realized as a subfield of F.

The kernel of this homomorphism is exactly $(\text{char}F)\mathbb{Z}$. By the isomorphism theorems, then, F contains either a subring isomorphic to $\mathbb{Z}$ (in which case F contains $\mathbb{Q}$) or else F contains a subring isomorphic to $\mathbb{Z}/p\mathbb{Z}$ (in which case $\mathbb{F}_p$, the finite field of p elements, is a subfield).

Definition: The prime subfield of a field F is the subfield generated by 1 additively. It is either $\mathbb{Q}$ or $\mathbb{F}_p$, the finite field of p elements.

Definition: If K is a field containing a subfield F, then K is an extension of F. The prime subfield is called the base field of an extension.

Definition: The degree of K/F, the extension K over F, is the dimension of K as a vector space over F.

Definition: Let K be an extension of F. Then for $\alpha \in K$, $F(\alpha)$ denotes the smallest subfield of K which contains F and α. This is called a simple extension of F; a simple extension is not, in general, simply an extension of degree 2 over F.

Theorem 1

> Let F be a field and $p(x) \in F[x]$ an irreducible polynomial. Then there exists a field K containing F such that $p(x)$ has a root.

We can prove this by considering the field:

$$K = \frac{F[x]}{(p(x))}$$

Since p is irreducible, and $F[x]$ is a PID, p spans a maximal ideal, and thus K is indeed a field. Furthermore, we have the canonical projection:

$$\pi : F[x] \to K$$

When restricted to F, this map is an isomorphism. Since it sends 1 to 1, it is an isomorphism and therefore an image of F lies in K. Thus, since π is a homomorphism, denoting the image in the quotient with a bar, we have:

$$\overline{p(x)} = p(\overline{x}) = 0$$

And thus, $\bar{x}$ is a root of p. In particular, let:

$$p(x) = a_n x^n + \cdots + a_1 x + a_0$$

Then if $\theta = \bar{x}$, then the above proof gives us a basis for K:

$$1, \theta, \ldots, \theta^{n-1}$$

And thus, $[K : F] = n$, i.e. K is a vector space over F of dimension n. It remains to check that this is indeed a basis, i.e. that it is linearly independent; this follows from the fact that p is irreducible.

Theorem 2

Let F be a field and $p(x) \in F[x]$ an irreducible polynomial. Suppose that K is an extension of F containing a root α of $p(x)$ such that $p(\alpha) = 0$. Let $F(\alpha)$ denote the subfield of K generated over F by α. Then:

$$F(\alpha) \cong \frac{F[x]}{(p(x))}$$

This theorem tells us that any field over F in which $p(x)$ contains a root contains a subfield isomorphic to the extension we considered in Theorem 1. The natural homomorphism that allows us to prove this identity is:

$$\varphi : F[x] \to F(\alpha) \subseteq K f(x) \mapsto f(\alpha)$$

This homomorphism is exactly evaluation. With some work, we can prove that this is a nontrivial ring homomorphism; thus the quotient ring is indeed a field.

Indeed, we can totally describe $F(\alpha)$ using this theorem:

Corollary

Suppose that $p(x)$ has degree n. Then:

$$F(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}\} \subseteq K$$

Where $a_i \in F$.

Describing the fields which are generated by more than element is a little more complicated.

Note that Theorem 2 tells us that the roots of an irreducible polynomial are, in a sense, indistinguishable; adjoining any root of an irreducible polynomial yields an isomorphic field. We extend this result.

Theorem 3

Let $\varphi : F \to \tilde{F}$ be an isomorphism of fields. Let $p(x) \in F[x]$ be an irreducible polynomial and let $p'(x) = \varphi(p(x))$ (we simply map each coefficient under φ). Then $p'(x)$ is irreducible.

Let α be a root of $p(x)$ and β be a root of $p'(x)$ in some extension of F'. Then there is an isomorphism:

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

$$\sigma : a \mapsto \beta$$

And such that σ restricted to F is exactly φ.

Thus, we can extend any isomorphism of fields to an isomorphism of simple extensions which maps roots to roots. In particular, if $F = F'$ and φ is the identity, then this tells us that $F(\alpha) \cong F(\beta)$, where β is another root of $p(x)$. This will be vital to understanding Galois theory.

Theorem 4 (Eisenstein's Criterion)

Suppose that we have a polymial in $\mathbb{Q}[x]$ given by:

$$a_n x^n + \cdots + a_1 x + a_0$$

Then if there exists a prime p such that: - $p \mid a_i$ for each $i \neq n$ - $p \nmid a_n$ - $p^2 \nmid a_0$ Then, this polynomial is irreducible over $\mathbb{Q}$ and equivalently over $\mathbb{Z}$.

1.2 Algebraic Extensions

Definition: The element $\alpha \in K$ is said to be **algebraic** over F if α is a root of some nonzero polynomial with coefficients in F. Otherwise, α is said to be transcendental over F. The extension K/F is algebraic if every element of K is algebraic over F.

From the Euclidean algorithm, we get:

Definition: Let α be algebraic over F. Then there exists a unique monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ which has α as a root. This polynomial is called the **minimal polynomial** of α and we say the degree of α is the degree of this polynomial.

Proposition 1

Let α be algebraic over F, and let $F(\alpha)$ be the field generated by α over F. Then:

$$F(\alpha) \cong \frac{F[x]}{(m_\alpha(x))}$$

This proves that in particular:

$$[F(\alpha) : F] = \text{deg } \alpha$$

Thus, the degree of a simple extension is exactly the degree of the minimal polynomial, and we have an explicit way of computing simple extensons corresponding to algebraic elements.

Proposition 2

The element α is algebraic over F iff the simple extension $F(\alpha)/F$ is finite.

This tells us that the property that α is algebraic over F is equivalent to the property that $[F(\alpha) : F]$ is finite. In particular, we have the corollary:

Proposition 3

If an extension K/F is finite, then it is algebraic.

A simple algebraic extension is finite, but in general the converse is not true, since there are infinite algebraic extensions.

Example Let F be a field of characteristic 2, and K an extension of degree 2 (called a quadratic extension). Let $\alpha \in K$ be an element not in F. It must be algebraic. Its minimal polynomial cannot be degree 1 (since $\alpha \notin F$); and so it is quadratic. It looks like:

$$m_\alpha(x) = x^2 + bx + c$$

For some $b, c \in F$. Furthermore, $K = F(\alpha)$. The roots are given by:

$$\alpha = \frac{-b \pm \sqrt{b^2 - 4c}}{2}$$

And $b^2 - 4c$ is not a square in F, since if it were then $\alpha \in F$.

Now, $F(\alpha) \subset F(\sqrt{b^2 - 4c})$ since α is an element of the field on the right. Conversely, $\sqrt{b^2 - 4c} = \pm(b + 2\alpha)$ so we have the reverse inclusion.

We have just shown that any quadratic extension is of the form $F(\sqrt{D})$ where D is an element of F which is not a square in F; conversely, every such extension has degree 2.

Theorem 5

Let $F \subseteq K \subseteq L$ be fields. Then:

$$[L : F] = [L : K][K : F]$$

This is an analogous theorem to the one for groups; indeed this connection is deeper than it appears.

Corollary

> Suppose L/F finite extension, and K a subfield of L containing F. Then $[K : F]$ divides $[L : F]$.

Definition: An extension K/F is **finitely generated** if there are element $\alpha_1, \ldots, \alpha_k$ in K such that:

$$K = F(\alpha_1, \ldots, \alpha_k)$$

As expected, we can obtain this field by recursively compounding a series of simple extensions, i.e.:

$$(F(\alpha))(\beta) = F(\alpha, \beta)$$

Where $F(\alpha, \beta)$ is the smallest field containing F, α, and β.

Theorem 6

> The extension K/F is finite iff K is generated by a finite number of algebraic elements over F. If these elements have degrees $n_1, \ldots, n_k$ then, K is algebraic of degree at most $n_1 n_2 \ldots n_k$.

To see this, notice that if K/F is finite of degree n, then say $\alpha_1, \ldots, \alpha_n$ is a basis for K as a vector space over F. Then:

$$[F(\alpha_i) : F] \mid [K : F] = n$$

Therefore, by Proposition 2 each α_i is algebraic. Conversely, if K is generated by a finite number of algebraic elements, then it is generated as a vector space by polynomials of those elements.

Corollary

> Let L/F be an arbitrary extension. Then the collection of elements of L that are algebraic over F forms a subfield K of L.

Suppose that α, β are algebraic over F. Then, note that $\alpha \pm \beta, \alpha\beta, \alpha/\beta, \alpha^{-1}$ are all algebraic, and lie in the finite extension $F(\alpha, \beta)$; and since this extension is finite, these elements are algebraic. Thus, the collection of algebraic elements is closed under addition, multiplication, and inverses.

Theorem 7

> If K is algebraic over F and L is algebraic over K, then L is algebraic over F.

We also ask about ``intersections'' of fields.

Definition: Let K_1, K_2 be subfields of K. The composite field of K_1, K_2, denoted $K_1 K_2$, is the smallest subfield of K containing both K_1, K_2. It is equivalently the intersection of all subfields of K containing both K_1 and K_2.

Indeed, if K_1, K_2 are finite extensions, then if we combine their bases, we can construct a set of generators for $K_1 K_2$. From this discussion, we can see:

Proposition 4

Let K_1, K_2 be two finite extensions of a field F contained in K. Then:

$$[K_1K_2 : F] \leq [K_1 : F][K2 : F]$$

Corollary

Suppose that $[K_1 : F] = n$, and $[K_2 : F] = m$, then if n, m are relatively prime then:

$$[K_1K_2 : F] = [K_1 : F][K_2 : F] = nm$$