Contents

Chapter 1

Field Extensions

1.1 Fields

A **field** is a tuple $(F, +, \cdot)$ such that $(F, +)$ and $(F^\times, \cdot)$ are abelian groups and multiplication distributes over addition, where $F^\times \doteq F - \{0\}$.

Equivalently, a field is a commutative ring with unity (i.e. has a multiplicative identity) where every nonzero elt has a multiplicative inverse (i.e. is a unit). Since units can't be zero divisors, fields have no zero divisors.

$$\text{Fields} \subset \text{Euclidean Domains} \subset \text{PIDs} \subset \text{UFDs} \subset \text{Integral Domains}.$$

Proposition 1. *Any nonzero field homomorphism is injective.*

Proof. Let φ be a field homomorphism with domain F. Now $\ker\varphi$ is an ideal of F, but the only ideals of a field are 0 and itself. Since φ is nonzero, $\ker\varphi = 0$, so φ is injective. □

Definition 1. The **characteristic** $\mathrm{ch}(F)$ of a field F is the smallest positive integer p such that $p \cdot 1_F = 0$. If no such p exists, we say $\mathrm{ch}(F) = 0$.

Proposition 2. *The characteristic of a field is either 0 or prime.*

Proof. If n is composite and $n \cdot 1 = 0$, then we can decompose this into its prime factorization and get that its smallest prime factor is the characteristic. □

Fields don't have interesting ideals (it's either 0 or the entire field), so instead we study subfields and field extensions.

Definition 2. The **prime subfield** of a field F is the subfield generated by $1 \in F$.

Proposition 3. *The prime subfield of a field F is isomorphic to $\mathbb{Q}$ if $ch(F) = 0$ and isomorphic to $\mathbb{F}_p$ if $ch(F) = p$.*

Definition 3. A field K is a **(field) extension** of F if F is a subfield of K. Denote this by $K \nwarrow F$.

Definition 4. If K is an extension of F, then the **degree** $[K : F]$ of K over F is the dimension of K as an F-vector space. An extension is **finite** if its degree is finite, and its **infinite** otherwise.

Example 1. $[\mathbb{C} : \mathbb{R}] = 2$ because $\{1, i\}$ is a basis for $\mathbb{C}$ over $\mathbb{R}$.

Field of fractions (DF sec 7.5). Since $\mathbb{Q}$ is the field of fractions of $\mathbb{Z}$, any field containing $\mathbb{Z}$ must also contain $\mathbb{Q}$.

1.2 Polynomial Rings over Fields

Many field extensions arise from trying to solve polynomial equations, so we gotta review that.

Theorem 1. *Let F be a field, then $F[x]$ is a Euclidean Domain.*

This means that any polynomial ring over a field has a division algorithm, i.e. for all $f(x)$ and nonzero $g(x)$, there exist *unique* $q(x), r(x)$ such that

$$f(x) = q(x)g(x) + r(x),$$

where $\deg r(x) < \deg g(x)$. Here, we take the degree of the zero polynomial to be 0. It should also be clear that degree is the norm of $F[x]$.

Corollary 1. *$F[x]$ is also a principal ideal domain (PID) and a unique factorization domain (UFD).*

If $E \nwarrow F$ and $f(x), 0 \neq g(x) \in F[x]$, then the result of the division algorithm in $F[x]$ is the same in $E[x]$ by the uniqueness bit. paragraph at end of sec 9.2.

Often, even if R is not a field (but *is* a UFD), then we can say something about factorization in R by looking at its field of fractions (the smallest field containing R, see sec 7.5, think $\mathbb{Z}$ to $\mathbb{Q}$).

Lemma 1 (Gauss' Lemma)**.** *Let R be a UFD with field of fractions F. Let $p(x) \in R[x]$ have coefficients with $\gcd$ 1, then $p(x)$ is irreducible in $R[x]$ if and only if it's irreducible in $F[x]$.*

Note that this works for all monic polynomials.

Proposition 4. *Let $p(x) \in F[x]$, where F is a field. Then $p(x)$ has a root $a \in F$ if and only if $(x - a)$ divides $p(x)$.*

Proof. Do this. □

Corollary 2. *Any $p(x) \in F[x]$ has at most $\deg p$ roots in F (including with multiplicity).*

Proof. Use induction on the proposition above. □

Corollary 3. *If $p(x) \in F[x]$ has degree 2 or 3, then it's reducible if and only if it has a root in F.*

The above corollary should be relatively obvious, but note that it doesn't hold in 4 dimensions or higher because a reducible polynomial could reduce into two other polynomials that have dimension 2+.

Example 2. We claim that $p(x) = x^3 + x + 1$ is irreducible in $\mathbb{F}_2[x]$. Using Corollary 3, we check that $p(0)$ and $p(1)$ are nonzero, so p has no roots in $\mathbb{F}_2$.

Proposition 5. *Let R be a UFD and let $p(x) = \sum_i a_i x^i \in R[x]$. If c and d are relatively prime with d nonzero and $p(c/d) = 0$, then $c \mid a_0$ and $d \mid a_n$.*

This is very useful in limiting the candidates for the roots of a particular polynomial.

Example 3. We claim that $p(x) = x^3 - x - 1$ is irreducible in $\mathbb{Z}[x]$. By Gauss' Lemma and Corollary 3, it suffices to show that p has no rational roots. By the above proposition, the only possibilities of rational roots are ± 1. But $p(1)$ and $p(-1)$ are both nonzero, so p is irreducible.

Theorem 2 (Eisenstein's Criterion)**.** *Let R be a UFD with field of fractions F and let $f(x) = \sum_i a_i x^i \in R[x]$ with $n \geq 1$ (i.e. non-constant) and $a_n \neq 0$. If there is some irreducible $p \in R$ such that*

1. *p does not divide a_n,*
2. *p divides a_i for all $i < n$, and*
3. *p^2 does not divide a_0,*

then $f(x)$ is irreducible in $F[x]$.

This is usually used when $R = \mathbb{Z}$ (so the field of fractions is $\mathbb{Q}$) and p is prime.

Example 4. $x^{12} - 10x^4 + 4x - 6$ is irreducible in $\mathbb{Q}[x]$ by Eisenstein's criterion for $p = 2$.

Theorem 3. *The multiplicative group of any finite field is cyclic.*

Proof. Let F be a finite field, then $(F^\times, \cdot)$ is a finite abelian group. By the fundamental theorem of finitely generated abelian groups, there exist positive integers $m_1 \mid m_2 \mid \cdots \mid m_k$ such that

$$F^\times \cong \mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_k}.$$

In particular, every element of $F^\times$ has order dividing m_k, i.e. $\alpha^{m_k} = 1$ for all $\alpha \in F^\times$. Thus every element of $F^\times$ is a root of $x^{m_k} - 1$. Since this polynomial can have at most m_k roots, $|F^\times| \leq m_k$; however, if $F^\times$ is isomorphic to $\mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_k}$, then $|F^\times| = m_1 \cdots m_k$. But this is only true if $k = 1$, so $F^\times \cong \mathbb{Z}_{m_1}$, so it is cyclic. $\square$

1.3 Constructing Field Extensions with Polynomials

The main idea of all this is to take an irreducible polynomial $p(x)$ over a field F, take its (maximal) ideal $(p(x))$, and use that to create the field $F[x]/(p(x))$.

As it turns out, this field will contain a root of p, so we can use this technique to construct field extensions that contain the roots of certain polynomials.

Definition 5. Suppose $K \nwarrow F$, and let $a_1, \dots, a_n \in K$. Then the extension $F(a_1, \dots, a_n)$ is the smallest subfield of K containing F and all the a_i.

Let R be a subring of K, then $R[a_1, \dots, a_n]$ is the smallest subring of K containing R containing R and all the a_i.

If we have a set A, we might denote the extension that it generates over F by $F(A)$.

We say K is a **simple extension** of F if $K = F(\alpha)$ for some $\alpha \in K$.

Definition 6. Let $K \nwarrow F$. We say $\alpha \in K$ is **algebraic** over F if it's the root of *some* polynomial over F. Otherwise it's **transcendental** over F.

K is an **algebraic extension** of F if every element of K is algebraic over F.

Example 5. $\mathbb{C}$ is algebraic over $\mathbb{R}$, but $\mathbb{R}$ is not algebraic over $\mathbb{Q}$.

Example 6. Every element α of a field F is algebraic over F since $(x - \alpha)$ is a polynomial over F.

Let $K \nwarrow F$ with $\alpha \in K$ algebraic over F, and consider the "evaluation at α" map $\phi_\alpha : F[x] \to K$ given by $F \overset{\text{id}}{\mapsto} F$, $x \mapsto \alpha$, and ϕ_a a ring homomorphism.

Definition 7. The **minimal polynomial** $m_{\alpha,F}(x)$ of α over F is the unique irreducible monic generator of $\ker \phi_a \subset F[x]$, i.e. it generates all the polynomials over F that have α as a root.

The **degree** of α over F is the degree of $m_{\alpha,F}(x)$.

Minimal polynomials are handy because they allow us to construct field extensions that contain one of their roots. If we take $F[x]$ and mod out everything generated by $m_\alpha(x)$, then what we get is a field where everything "related to" α becomes 0. Replace this with actual good intuition. Use the theorem about the form of elements of $F(\alpha_1, \dots)$ to show this.

Theorem 4. *If $K \nwarrow F$ and $\alpha \in K$ is algebraic over F with minimal polynomial $m_\alpha(x)$, then*

1. $F(\alpha) = F[\alpha]$,

2. *$F(\alpha) \cong F[x]/m_\alpha(x)$,*
3. *$[F(\alpha) : F] = \deg m_\alpha(x)$, and*
4. *$\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis for $F(\alpha)$ over F, where $n = \deg m_\alpha(x)$.*

Proof. Do this. □

Example 7. If $\alpha \in \mathbb{C}$ has minimal polynomial $x^3 + x + 3$ over $\mathbb{Q}$, then $\mathbb{Q}(\alpha)$ has basis $\{1, \alpha, \alpha^2\}$ over $\mathbb{Q}$.

We can use this theorem to construct any field of order p^n, where p is a prime. If we take a monic irreducible polynomial $f(x)$ of degree n over the finite field $\mathbb{F}_p$, then the extension $\mathbb{F}_p[x]/(f(x))$ as a vector space over $\mathbb{F}_p$ has degree n, so there are p^n elements of the extension.

GO OVER SECTION 13.1 FOR ALL THE PROOFS.

The roots of an irreducible polynomial $p(x)$ are algebraically indistinguishable in the sense that they generate the same extensions. If α, β are roots of $p(x)$ over F, then

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

We can extend this idea slightly by considering field extensions generated by isomorphcially related polynomials. In this case, the field extensions are themselves isomorphic.

Note 1. If we have a map $\phi : F \to E$ and I write something like $\phi(f(x))$, this means we're applying ϕ to each coefficient of $f(x)$ and returning a new polynomial over E.

Theorem 5. *Suppose $\phi : F \to E$ is a field isomorphism. Let α be the root of minimal polynomial $f(x)$ over F, and let β be a root of $\phi(f(x))$. Then we can extend ϕ to an isomorphism $\hat{\phi} : F(\alpha) \to E(\beta)$ such that $\hat{\phi}(\alpha) = \beta$.*

Proof. Do this. □

This theorem can be represented with the following diagram.

$$\begin{tikzcd}
\hat{\phi}: & F(\alpha) \arrow[r, "\cong"] \arrow[d, dash] & E(\beta) \arrow[d, dash] \\
\phi: & F \arrow[r, "\cong"] & E
\end{tikzcd}$$

1.4 Algebraic Extensions

Definition 8. $K \nwarrow F$ is **finitely generated** if $K = F(\alpha_1, \ldots, \alpha_N)$.

Note 2. A field extension might be finitely generated without being a finite extension. Consider $\mathbb{Q}(\pi)$, which is clearly finitely generated. Since π is transcendental over $\mathbb{Q}$, $\mathbb{Q}(\pi)$ is an infinite extension over $\mathbb{Q}$.