Field Theory and Galois Theory.

Alec Zabel-Mena

January 12, 2023

Contents

1 Fields. **5**
1.1 Field Extensions. 5

Chapter 1

Fields.

1.1 Field Extensions.

Definition. We define the **characteristic** of a field F to be the smallest positive integer p, such that $p \cdot 1 = 0$, where 1 is the identity of F. We write $\operatorname{char} F = p$, and if no such p exists, then we write $\operatorname{char} F = 0$.

Lemma 1.1.1. *Let F be a field, then $\operatorname{char} F$ is either 0, or a prime integer.*

Proof. Let $\Gamma F = p$. If $p = 0$, then we are done. Now suppose that $p = mn$, with $m, n \in \mathbb{Z}^+$. Then $p \cdot 1 = (mn)1 = (n \cdot 1)(m \cdot 1) = mn = 0$, which makes m and n 0 divisors. Since F is a field, and hence an integral domain, this is impossible, and hence p must be prime. ■

Corollary. *If $\operatorname{char} F = p$, then for all $a \in F$, $pa = \underbrace{a + \cdots + a}_{p \text{ times}}$.*

Proof. We have $pa = p(a \cdot 1) = (p \cdot 1)a$. ■

Example 1.1. (1) Both $\mathbb{Q}$ and $\mathbb{R}$ have char $= 0$. Similarly, $\operatorname{char} \mathbb{Z} = 0$, even though $\mathbb{Z}$ is just an integral domain.

(2) $\operatorname{char} \mathbb{Z}/p\mathbb{Z} = p$ and $\operatorname{char} \mathbb{Z}/p\mathbb{Z}[x] = p$ for any prime p.

Definition. We define the **prime subfield** of a field F to be the subfield of F generated by 1.

Example 1.2. (1) The prime subfields of $\mathbb{Q}$ and $\mathbb{R}$ is $\mathbb{Q}$.

(2) Let $\mathbb{Z}/p\mathbb{Z}(x)$ the field of rational functions over $\mathbb{Z}/p\mathbb{Z}$. Then the prime subfield of $\mathbb{Z}/p\mathbb{Z}(x)$ is $\mathbb{Z}/p\mathbb{Z}$. Similarly, the prime subfield for $\mathbb{Z}/p\mathbb{Z}[x]$ is also $\mathbb{Z}/p\mathbb{Z}$.

Definition. If K is a field containing a field F, then we call K **field extension** over F, and write K/F (not the quotient field!) or denote it by the diagram

$$\begin{array}{c} K \\ | \\ F \end{array}$$

Lemma 1.1.2. *Every field is a field extension of its prime subfield.*

Lemma 1.1.3. *Let K an extension over a field F. Then K is a vector space over F.*

Definition. Let K/F a field extension. We define the **degree** of K over F, $[K:F]$ to be the dimension of K/F as a vector space.

Definition. Let F be a field, and $f \in F[x]$ a polynomial. We call am element $\alpha \in R$ a **root** (or **zero**) of f if $f(\alpha) = 0$.

Lemma 1.1.4. *Let $\phi : F \to L$ a field homomorphism. Then either $\phi = 0$, or ϕ is 1–1.*

Lemma 1.1.5. *Let F be a field, and $p \in F[x]$ an irreducible polynomial. Then there exists a field K containing an embedding of F, such that p has a root in K.*

Proof. Consider $K = F[x]/(p)$. Siince p is irreducible in a principle ideal domain, (p) is a maximal idea, and hence K is a field. Now consider the canonical map $\pi : F[x] \to K$ taking $f \to f \mod (p)$ and let $\phi = \pi|_F$. Then $\phi \neq 0$, since $\pi : 1 \to 1$. Then ϕ is 1–1. And so $\phi(F) \simeq F$.

Now, consider F as a subfield of K. Then $p(x \mod (p)) \equiv p(x) \mod (p) \equiv 0 \mod (p)$, so that $x \mod (p)$ is a root of p in K. ■

Corollary. *There exists a field extension of F containing a root of p.*

Theorem 1.1.6. *Let F be a field, and let $p \in F[x]$ an irreducible polynomial of degree n, and let $K = F[x]/(p)$, and $\theta = x \mod (p)$. Then $\{1, \theta, \dots, \theta^{n-1}\}$ forms a basis for K as a vector space over F and $[K:F] = n$.*

Proof. Let $a \in F[x]$, since $F[x]$ is Euclidean domain, there exist $q, r \in F[x]$, $q \neq 0$ for which

$$a(x) = q(x)p(x) + r(x) \text{ where } \deg r < n$$

Now, since $pq \in (p)$, $a(x) \equiv r(x) \mod (p)$, and every element of K is a polynomial of degree less than n. Then the elements $\{1, \theta, \dots, \theta^{n-1}\}$ span K.

Now, suppose that there are $b_0, \dots, b_{n-1} \in F$ not all 0 for which

$$b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1} = 0$$

Then

$$b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1} \equiv 0 \mod (p)$$

so that $p|(b_0 + b_1\theta + \cdots + b_{n-1}\theta^{n-1})$ in F. But $\deg p = n$ and p divides a polynomial of degree $n-1$, which is a contradiction. Therefore we are left with $b_0 = \cdots = b_{n-1} = 0$. ■

Corollary. $K = \{\alpha_0 + a_1\theta + \cdots + a_{n-1}\theta^{n-1} : a_i \in F \textit{ for all } 1 \leq i \leq n-1\}$

Corollary. *If $a(\theta), b(\theta) \in K$, are elements of degree less than n, and the operations of polynomial addition, and polynomial multiplication mod (p) are defined, then K forms a field.*

Example 1.3. (1) Consider the polynomial x^2+1 over $\mathbb{R}$. Then one has the field

$$\mathbb{C} = \mathbb{R}[x]/(x^2+1)$$

an extension of $\mathbb{R}$ of degree $[\mathbb{C} : \mathbb{R}] = 2$. Let i be a root of x^2+1 in this field, then $i^2 = -1$, and the elements of $\mathbb{C}$ are of the form $a + ib$ where $a, b \in \mathbb{R}$. Then we have described the field of complex numbers, and the addition and multiplication (mod x^2+1) of these elements are the addition and multiplication of complex numbers.

One might also construct $\mathbb{C}$ differently by defining the isomorphism

$$\mathbb{R}[x]/(x^2+1) \to \mathbb{C} \text{ taking } a + xb \to a + ib$$

(2) Consider again x^2+1 over $\mathbb{Q}$. Then we get the field

$$\mathbb{Q}(i) = \mathbb{Q}[x]/(x^2+1)$$

of degree $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, and where i is a root of x^2+1, so that $i^2 = -1$. Then the elements of $\mathbb{Q}(i)$ are of the form $a + ib$ where $a, b \in \mathbb{Q}$, i.e. it is isomorphic to the set of all complex numbers with rational components.

(2) Consider x^2-2 over $\mathbb{Q}$. by Eisenstein's criterion for $p = 2$, x^2-2 is irreducible over $\mathbb{Q}$. Let α a root of x^2-2, so that $\alpha^2 = 2$. Then we have the field

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[x]/(x^2-2)$$

of degree $[Q(\sqrt{2}) : \mathbb{Q}] = 2$, and whose elements are of the form $a + b\sqrt{2}$. One can define an isomorphism between $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{2})$ by taking $\sqrt{2} \to i$.

(3) The polynomial x^3-2 over $\mathbb{Q}$ gives us the field

$$\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}[x]/(x^3-2)$$

of degree $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ over 2. Here the elements are of the form $a + b\xi + c\xi^2$ where $\xi^3 = 2$.

(4) Denote $\mathbb{F}_2$ to be a finite field of 2 elements. Consider the polynomial x^2+x+1 over $\mathbb{F}_2$ which is irreducible. Then the field

$$\mathbb{F}_2(\alpha) = \mathbb{F}_2[x]/(x^2+x+1)$$

is a field of degree 2 over $\mathbb{F}_2$, whose elements are of the form $a + b\alpha$, where $\alpha^2 = \alpha + 1$. In fact, one can generate this field using the fact that $\alpha^2 = \alpha + 1$.

(5) Let $F = K(t)$ the field of rational functions in t over a field K. Let $p(x) = x^2 - t \in F[x]$, then by Eisenstien's criterion with the ideal (t), p is irreducible over $F[x]$. Let θ be a root for p, that is $\theta = \sqrt{t}$, then we get the field $K(t, \sqrt{t})$ of degree $[K(t, \sqrt{t}) : K] = 2$, whose elements are of the form $a(t) + b(t)\sqrt{t}$.

Lemma 1.1.7. *Let F be a subfield of a field K, and let $\alpha \in K$. Then there exists a unique minimal subfield of K containing F and α; more preciesly, it is the intersection of all subfields of K containing F and α.*

Definition. Let K be any extension of a field F, and let $\alpha, \beta, \dots \in K$. Then we define the subfield **generated** by $\alpha, \beta, \dots$ over F to be the unique minimal subfield containing all $\alpha, \beta, \dots$ and F and we denote it $F(\alpha, \beta, \dots)$. Moreover, we call K a **simple extension** of F if $K = F(\alpha, \beta, \dots)$. If $K = (F\alpha_1, \dots, a_n)$ for $\alpha_1, \dots, a_n \in K$, then it is a **finitely generated** simple extension.

Theorem 1.1.8. *Let F be a field, and $p \in F[x]$ irreducible, and let K an extension of F containing a root α of p. Then*

$$F(\alpha) \simeq {}^{F[x]}\!\big/_{(p)}$$

Proof. Consider the homomorphism $F[x] \to F(\alpha)$ taking $a(x) \to a(\alpha)$. Since $p(\alpha) = 0$, p is in the kernel of this homomorphism, and we get an induced homomorphsim from ${}^{F[x]}\!\big/_{(p)} \to F(\alpha)$. Now, since p is irreducible, ${}^{F[x]}\!\big/_{(p)}$ is a field, and since the homomorphsim takes $1 \to 1$, it is 1–1. Then by the first isomorphsim theorem for ring homomorphsims these two fields are isomorphic. ■

Corollary. *If $\deg p = n$, then $F(\alpha) = \{a_0 + a_1\alpha + \dots a_{n-1}\alpha^{n-1} : a_i \in F \text{ for all } 1 \leq i \leq n-1\}$ and $[F(\alpha) : F] = n$.*

Example 1.4. (1) The polynomial $x^2 - 2$ over $\mathbb{Q}$ also has the root $-\sqrt{2}$ in $\mathbb{R}$, so that $\mathbb{Q}(-\sqrt{2})$ is of degree 2 over $\mathbb{Q}$ with elements of the form $a - b\sqrt{2}$. Notice however that $\mathbb{Q}(-\sqrt{2}) \simeq \mathbb{Q}(\sqrt{2})$ by taking $a - b\sqrt{2} \to a + b\sqrt{2}$.

(2) The polynomial $x^3 - 2$ only has the solution $\xi = \sqrt[3]{2}$ in $\mathbb{R}$. However, in $\mathbb{Q}$ it has the solutions given by

$$\sqrt[3]{2}\left(\frac{-1 \pm i\sqrt{3}}{2}\right)$$

So that the subfields generated by either of these three elements (over $\mathbb{C}$) are isomorphic.

Theorem 1.1.9. *Let $\phi : F \to L$ a field isomorphism and $p \in F[x]$, $q \in L[x]$ irreducible polynomials, where q is obtained by applying ϕ to the coefficients of p. Let α a root of p, and β a root of q. Then there exists an isomorphism $F(\alpha) \to L(\beta)$ taking $\alpha \to \beta$ and extending ϕ. That is, we have the following diagram*

$$\begin{array}{ccc} F(\alpha) & \longrightarrow & L(\beta) \\ | & & | \\ F & \xrightarrow[\phi]{} & E \end{array}$$

Proof. Notice that ϕ induces a ring homomorphism between $F[x]$ and $L[x]$, so that (p) is maximal. Since q is obtained from p, (q) is also maximal, so that $F[x]/(p)$ and $L[x]/(q)$ are fields. Then we have an isomorphsism

$$F[x]/(p) \simeq L[x]/(q)$$

Then, if α is a root of p, and β a root of q, we obtain the isomorphism

$$F(\alpha) \simeq L(\beta)$$

moreover, this isomorphism takes $\alpha \to \beta$. ■

1.2 Algebraic Extensions.

Bibliography

[1] D. Dummit, *Abstract algebra.* Hoboken, NJ: John Wiley & Sons, Inc, 2004.

[2] I. N. Herstein, *Topics in algebra.* New York: Wiley, 1975.