Field Theory and Galois Theory.

Alec Zabel-Mena

January 11, 2023

Contents

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. ■

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

Bibliography

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

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