Euler Circle Chapter 6: Fields

Albert Ye

May 13, 2020

§1 Fields

§1.1 Notes

§1.1.1 Fields

Definition 1.1. A **field** is a set F together with two binary operations $+$ and $\cdot$ s.t.

- F forms an abelian group under $+$
- $F^\times = F \setminus \{0\}$ forms an abelian group under $\cdot$.
- F is distributive, i.e. for $a, b, c \in F$, $a(b+c) = ab + ac$

Examples of fields include $\mathbb{Q}, \mathbb{R}, \mathbb{C}$. $\mathbb{Z}$ is not a field because $\mathbb{Z} \setminus \{0\}$ is not an abelian group.

There are other fields, such as $\mathbb{F}_2$, which is the field of two numbers s.t. $a+b = (a+b)\%2$.

Note 1.2. There are no fields with just one element since if F has one element, then $F^\times = \varnothing$ which isn't multiplicative.

Some of the most interesting fields are those that are like $\mathbb{Q}$, but are a bit bigger. For example, $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2}\}$.

Most of the axioms are clear but we need to prove $\sqrt{\not{F}}^\times$ is a group under multiplication. To do this we just find $\dfrac{1}{a+b\sqrt{2}}$ rationalize the denominator.

§1.1.2 Homomorphisms

Definition 1.3. Let F, K be two fields. A **homomorphism** between them is a function $\phi : F \to K$ s.t. ϕ is a homomorphism of additive and multiplicative groups. For all $a, b \in F$, we have

- $\phi(a+b) = \phi(a) + \phi(b)$.
- $\phi(ab) = \phi(a)\phi(b)$.
- $\phi(1_F) = 1_K$.

Proposition 1.4

All field homomorphisms are injective.

Proof. Suppose that $\phi(a) = \phi(b)$, where $a \neq b$. We have $\phi(\dfrac{1}{a-b}) \cdot \phi(a-b) = \phi(1) = 1$, but $\phi(a-b) = 0$. So this means that 1 is a multiple of 0, which is false. □

§1.1.3 Field Extension

If we have a homomorphism $\phi : F \to K$, we can consider F as beinga subfield of K, or K being an extension of F. We write K/F to mean that K is an extension of F.

To construct field extensions, let F be a field and $\alpha \notin F$. Let $F(\alpha)$ be the smallest field containing both F and α. More generally, if $\alpha_1, \alpha_2, \dots$ are elements, then $F(\alpha_1, \alpha_2, \cdots)$ is the smallest field containing F and all α.

Example: $\mathbb{Q}(\sqrt{2})$ is an extension of $\mathbb{Q}$. It contains $\mathbb{Q}, \sqrt{2}$, and everything build out of them. This is just $\{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$, because the set's already closed under nonzero inverses.

Example: Let x be a variable. Then $\mathbb{Q}(x)$ consists of all rational functions in x with coefficients in $\mathbb{Q}$, i.e. expressions of the form $f(x)/g(x)$ where f, g are polynomials with rational coeffs.

We often consider extensions of the form $F(x)$, where x is a root of a nonzero polynomial with coefficients in F, i.e.

$$a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0 = 0 (*)$$

for some $a_0, a_1, \dots, a_n \in F$, not all 0. We can assume that $a_n \neq 0$, then divide by a_n s.t. F is now monic.

Then a typical element of $F(x)$ has the form $b_0 + b_1 x + \cdots + b_{n-1}x^{n-1}$. Every time we encounter an x^n we just replace it with $-a_{n-1}a^{n-1} - \ldots - a_0$. We also need to know that we can divide by such elements. It's easy to see that we can divide by x, because if $a_0 \neq 0$, then we can divide $(*)$ by x to get $\frac{a_0}{x} = -a_1 - a_2 x - \cdots - x^{n-1}$ and then divide by a_0 to isolate $\frac{1}{a}$. This isn't enough because we also have to be able to divide by $a - 1$ or $a^4 + 8a^3 - 6a - 5$. Sometimes this isn't possible.

§1.1.4 Linear Algebra

Definition 1.5. Let F be a field. A **vector space** over F is an abelian group V, together with a binary operation $\cdot : F \times V to V$ called **scalar multiplication**, s.t. for all $a, b \in F$ and $v, w \in V$:

- $0_F v = 0_V$ where 0_F is "zero" for F and 0_V is V's identity
- $1v = v$
- $a(v + w) = av + aw$
- $(ab)v = a(bv)$
- $(a + b)v = av + bv$

Definition 1.6.

- Let F be a field a V a vector space over F. We say that $v_1, \dots, v_n \in V$ are **linearly independent** if whenever $a_1, a_2, \dots, a_n \in F$ are such that
$$a_1 v_1 + a_2 v_2 + \ldots + a_n v_n = 0,$$
then a_i is $0 \forall i$.
- We say that $v_1, v_2, \dots, v_n \in V$ **span** V if for every $v \in V$, there exist $a_1, a_2, \dots, a_n \in F$ s.t. $v = a_1 v_1 + a - 2v_2 + \ldots + a_n v_n$.
- We say that $v_1, v_2, \dots, v_n \in V$ is a **basis** for V if they are linearly independent and spanning.

- Any element of the form $a_1v_1 + \cdots + a_nv_n \in V$ is said to be a **linear combination** of $v_1, v_2, \ldots, v)n$.

Theorem 1.7

Any two bases of a vector space V have the same size.

The result is that the size of a basis is an important invariant of a vector space.

Definition 1.8. Let V be a vector space over F. We say that V has **dimension** n if some (hence any) basis of V consists of n element. We write $\dim_F V$, or sometimes just $\dim V$ if F is clear from context.

§1.1.5 Field Extensions as Vector Spaces

If K/F is a field extension, then we can think of K as being a vector space over F.

Definition 1.9. Let K/F be a field extension. We write $[K : F]$ for the dimension $\dim_f K$, and we call this number the **degree** of K/F.

For example, find $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]$. We claim that it's **2**.

We claim that $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{2})$ as a $\mathbb{Q}$-vector space. To check linear independence, suppose $a + b\sqrt{2} = 0$ for rational a, b. if $b = 0$, then $a = 0$ as well. Suppose $b \neq 0$. Then $\sqrt{2} = \dfrac{a}{b}$ where $a, b \in \mathbb{Q}$. But we know that $\sqrt{2} \notin \mathbb{Q}$. Thus $\{1, \sqrt{2}\}$ is linearly independent. We know it's spanning because $\mathbb{Q}(2) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$.

$[\mathbb{Q}(\sqrt{a}) : \mathbb{Q}] = 2$ if $a \in \mathbb{Q}$ is not a perfect square, and $[\mathbb{Q}(\sqrt{a} : \mathbb{Q}] = 1$ if a is a perfect square.

$[\mathbb{Q}(\sqrt[3]{2} : \mathbb{Q}] = 3$. A basis is $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$.

$[\mathbb{C} : \mathbb{R}] = 2$, with basis $\{1, i\}$.

$[\mathbb{R} : \mathbb{Q}] = \infty$, as it contains arbitrarily large linearly independent sets, such as $\{1, 2^{1/n}, 4^{1/n}, (2^{n-1})^{1/n}\}$. *This may require a proof.*

Definition 1.10. A field F is called a **number field** if F contains $\mathbb{Q}$ and $[F : \mathbb{Q}] < \infty$.

Theorem 1.11 (The Tower Law)

If L/K and K/F are finite extensions, then so is L/F, and $[L : F] = [L : K][K : F]$.

Proof. Supposed that $a_1, \ldots, a_m$ is a basis for K/F and $b_1, \ldots, b_n$ is a basis of L/K. We claim that $\{a_ib_j\}_{1 \leq i \leq m, 1 \leq j \leq n}$ is a basis for L/F. Suppose we have a linear dependence relation

$$\sum_{1 \leq i \leq m, 1 \leq j \leq n} c_{ij}a_ib_j = 0.$$

Then for each j, we can group all the $c_{ij}a$is together to get

$$\sum_{j=1}^{n} \left(\sum_{i=1}^{m} c_{ij}a_i \right) b_j = 0,$$

where the parenthesized term is in K. Since the b_j are linearly independend over K, each parenthesized term must be 0, i.e.

$$\sum_{i=1}^{m} c_{ij}a_i = 0$$

for each j. Now, because a_i's are linearly independent over F, this means that $c_{ij} = 0$. Thus, $\{a_ib_j\}$ is linearly independent.

Next, we must show that $\{a_ib_j\}$ is spanning. Let $x \in L$. Since the b_js are a basis for L/K, there exist elements $d_1, \cdots, d_n \in K$ s.t. $x = d_1b_1 + \cdots + d_nb_n$. Now, since the a_i are a basis for K/F, we can write each d_j are $d_j = \sum_{i=1}^{m} c_{ij}a_i$ for some $c_{ij} \in F$. Thus, we have $x = \sum_{j=1}^{n} d_jb_j$, which is a linear combination and we are done. □

Corollary 1.12

If $L/K/F$ is a tower of fields, then $[K : F]$ divides $[L : F]$.

§1.1.6 Algebraic Extensions

Suppose $[K : F] = n$. This means that any $n + 1$ elements of K must be linearly dependent. Thus if we take any $a \in K$, then $1, a, a^2, \ldots, a^n$ must be linearly dependent. This means that there exist $c_0, \ldots, c_n \in F$, not all zero, s.t. $c_0 + c_1a + \cdots + c_na^n = 0$. Let $f(x) = c_0 + c_1x + \cdots + c_nx^n$. Then a is a root of $f(x)$.

Example: Let $F = \mathbb{Q}$ and $K = \mathbb{Q}(\sqrt{2})$. Then $a^2 = 3 + 2\sqrt{2}$. The numbers $1, a, a^2$ satisfy the relation $a^2 - 2a - 1 = 0$ so a is a root of the polynomial $f(x) = x^2 - 2x - 1$.

If a is a root of f, then for any $c \in F$, a is a root of cf, so we can force a to be a root of a *monic* polynomial of degree n. In fact, if n is the lowest degree of a polynomial with a as a root then there's only one such monic polynomial.

Definition 1.13. Let K/F be a field extension and $a \in K$. The **minimal polynomial** of a, if it exists, is the monic polynomial $m_a(x)$ of lowest degree s.t. $m_a(a) = 0$.

Definition 1.14. A polynomial $f(x)$ with coefficients in F is said to be **irreducible** over F if, whenever $f(x) = g(x)h(x)$ where g, h are polynomials with coefficients in F, then either g or h (or both) is constant.

Proposition 1.15

Minimal polynomials are irreducible.

Proof. Suppose $m_a(x)$ factors as $m_a(x) = g(x)h(x)$. Then $m_a(a) = 0 = g(a)h(a)$, so $g(a) = 0$ or $h(a) = 0$. WLOG let $g(a) = 0$. then a must be a root of $g(x)$, so $\deg g \geq \deg m_a$, hence they're equal. Thus h is constant. □

Note 1.16. We know that $\deg g \geq \deg m_a$ because m_a must be the polynomial of minimal degree s.t. $m_a(a) = 0$.

Definition 1.17. Let K/F be a field extension. We say that $a \in K$ is **algebraic** over F is a a has a minimal polynomial, or equivalently, if $[F(a) : F] < \infty$. Else we say that a is **transcendental** over F. We say that K/F is an algebraic extension if K/F is an algebraic extension if *every* $a \in K$ is algebraic over F, and a transcendental extension otherwise.

If a is algebraic over F, we can express $F(a)$ as follows: suppose the degree of the minimal polynomial of a is n. Then, every element of $F(a)$ can be written in the form $c_0 + c_1 a + \cdots + c_{n-1}a^{n-1}$ for some $c_0, \ldots, c_{n-1} \in F$. How do we divide by, say, $a+1$?

Consider the elements $1, a+1, (a+1)^2, \ldots, (a+1)^n$: they're linearly dependent, and this provides us with a polynomial having $a+1$. Then we can use the same method as before to computer $\dfrac{1}{a+1}$.

Theorem 1.18

Let F be a field and a algebraic over F. Suppose $f(a) = 0$. Then $m_a(x)$ divides $f(x)$.

Proof. Look at what happens when $f(x)$ is divided by $m_a(x)$. We have $f(x) = q(x)m_a(x) + r(x)$, where $\deg r < \deg m_a$. Thus $0 = f(a) = q(a)m_a(a) + r(a) = r(a) = 0$. But we know that $\deg r < \deg m_a$, so r must be 0. □

Theorem 1.19 (Eisenstein's Criterion)

Let $f(x) = a_n x^n + \cdots + a_0$ be a polynomial with integer coefficients. Suppose that for some prime p, a_n is not divisible by p, $a_0, a_1, \ldots, a_{n-1}$ are divisible by p, and a_0 is not divisible by p^2. Then f is irreducible over $\mathbb{Q}$.

For example, $x^n - 2$ is irreducible via Eisenstein with $p = 2$.

Example 1.20

Let $f(x) = x^3 - 3x - 1$, $f(x+1) = x^3 + 3x^2 - 3$. This is an Eisenstein polynomial with $p = 3$, so it's irreducible.

§1.1.7 Adjoining one vs. all roots

Let's look at $x^3 - 2$ over $\mathbb{Q}$. The roots of this polynomial are $\sqrt[3]{2}$, $\sqrt[3]{2}e^{2\pi i/3}$, $\sqrt[3]{2}e^{4\pi i/3}$. The first of these roots is real, while the second and third aren't.

Since $\mathbb{Q}$ and $\sqrt[3]{2}$ are both contained in $\mathbb{R}$, so is $K = \mathbb{Q}(\sqrt[3]{2})$. As a result, the other two roots of $x^3 - 2$ aren't contained in K.

For $x^3 - 2$, we can adjoin *all* roots to get the field $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{2\pi i/3}, \sqrt[3]{2}e^{4i\pi/3})$.

What is $[L : \mathbb{Q}]$? It isn't 26. Consider L as the top of a tower of fields: $\mathbb{Q}, then \mathbb{Q}(\sqrt[3]{2})$, then $\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{2\pi i/3})$, then L. Tower Law:

$$[L : \mathbb{Q}] = [L : \mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{2\pi i/3})] \cdot [\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}e^{2\pi i/3}) : \mathbb{Q}(\sqrt[3]{2})] \cdot [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}].$$

$x^3 - 2$ is reducible over $\mathbb{Q}(\sqrt[3]{2})$, because we just adjoined a root of it; indeed, it factors as $(x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + \sqrt[3]{4})$. The quadratic factor is irreducible, so the degree in the second term is 2. Similarly, the degree of the first term is 1. Therefore, $[L : Q] = 6$.

Another way of seeing this is that $L = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$, and $e^{2\pi i/3}$ is a root of $x^2 - x + 1$.

More generally, if f is a polynomial over F of degree n, then if L is the field obtained by adjoining all roots of F, then $[L : F] \leq n!$. Actually, $[L : F] | n!$.

§1.2 Homework

Problem 1.21 (4)**.** Show that $f : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$, given by $f(a + b\sqrt{2}) = a - b\sqrt{2}$ is an automorphism.

Solution 1.22. This is obviously a bijection, so we focus on the homomorphism aspect of the problem. We just go through all of the axioms for homomorphisms.

1. $f(x_1 + x_2) = f(x_1) + f(x_2)$. We set $x_1 = a_1 + b_2\sqrt{2}$, $x_2 = a_2 + b_2\sqrt{2}$. Then, we have

$$\begin{aligned} f(a_1 + b_1\sqrt{2} + a_2 + b_2\sqrt{2}) &= (a_1 + a_2) - (b_1 + b_2)\sqrt{2} \\ &= a_1 - b_1\sqrt{2} + a_2 - b_2\sqrt{2} \\ &= f(a_1 + b_1\sqrt{2}) + f(a_2 + b_2\sqrt{2}). \end{aligned}$$

□

2. $f(x_1x_2) = f(x_1)f(x_2)$. We use the same notation as (1).

$$\begin{aligned} f((a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2})) &= f((a_1a_2 + 2b_1b_2) + (a_1b_2 + a_2b_1)\sqrt{2} \\ &= (a_1a_2 + 2b_1b_2) - (a_1b_2 + a_2b_1)\sqrt{2} \\ &= (a_1 - b_1\sqrt{2})(a_2 - b_2\sqrt{2}) \\ &= f(a_1 + b_1\sqrt{2})f(a_2 + b_2\sqrt{2}). \end{aligned}$$

□

3. $f(1) = 1$. The domain and codomain are the same, so it doesn't really matter between the domain field and codomain field's 1. We have $f(1) = f(1 + 0\sqrt{2} = 1 - 0\sqrt{2} = 1$. □

Therefore, it is a homomorphism, and it follows that it is an isomorphism and because the domain is the codomain an automorphism. ■

Problem 1.23 (7)**.** Show that if $v_1, \ldots, v_n$ is a basis for a vector space V over a field F, then for every $b \in V$, there is a unique set of elements $a_1, \ldots, a_n$ of F s.t. $b = a_1v_1 + \cdots + a_nv_n$.

Solution 1.24. We know that because $v_1, \ldots, v_n$ is a basis, $\forall b \in V$:

- $b = a_1v_2 + a_2v_2 \cdots + a_nv_n$ for some $a_1, \ldots, a_n \in F$.
- $0 = a_1v_2 + a_2v_2 + \cdots + a_nv_n \implies a_1 = a_2 = \cdots = a_n = 0$.

Now let's assume for the sake of contradiction that this set of elements $a+n, \ldots, a_n \in F$ is non-unique. In other words, there are two sets (say a_i and b_i) that sastisfy $b = a_1v - 1 + a_2v_2 + \cdots + a_nv_n$. Thus, we have that $b = a_1v_2 + a_2v - 2 + \cdots + a_nv_n = b_1v - 1 + \cdots + b_nv_n$. We can subtract the two equations to get something like

$$0 = (a_1 - b_1)v_1 + (a_2 - b_2)v_2 + \cdots + (a_n - b_n)v_n.$$

To preserve linear independence, we have that all of the $a_i - b_i$ must be 0. In other words, $a_i = b_i \forall i \in [1, n]$, so the set a is unique. ■

Problem 1.25 (12)**.** Find a factorization for $x^4 + 4$ or prove irreducible.

Solution 1.26. This follows immediately from Sophie Germain's identity, which states the factorization is $x^4 + 4 * 1^4 = (x^2 + 2 - 2x)(x^2 + 2 + 2x)$.

Problem 1.27 (13)**.** What is a 0-dimensional vector space?

Solution 1.28. We claim that $V = \{0\}$ is a 0-dimensional vector space. Note that there are only two subsets of V: the empty and whole set. The whole set is clearly not linearly dependent, as it contains 0. The empty set must be linearly independent as there are no values in the set at all, and thus none such that a linear combination evaluates to 0. Additionally, the empty set categorically spans because there are no elements of the set that can possibly be used to state otherwise. Therefore, the empty set must be a basis, and $\dim(V) = 0$. ■