Lecture 8: Field Theory I

Apr. 14, 2023

Lecturer: Bin Guan

This lecture refers to §13.1, §13.2, §13.3, §13.6 in [1]. All the equation numbers without reference labels are from this book.

1 Basic theory of field extensions

1.1 Characteristics

Exercise ([1] §7.3 Exercise 26)**.** *The **characteristic** of a ring R with identity $1_R = 1 \neq 0$, denoted $\mathrm{char}(R)$, is the smallest positive integer n such that $1 + 1 + \cdots + 1 = 0$ (n times) in R; if no such integer exists the characteristic of R is said to be 0. For example, $\mathbb{Z}/n\mathbb{Z}$ is a ring of characteristic n for each positive integer n and $\mathbb{Z}$ is a ring of characteristic 0.*

(a) Prove that the map $\mathbb{Z} \to R$ defined by

$$k \mapsto k \cdot 1_R \coloneqq \begin{cases} 1 + 1 + \cdots + 1 \text{ (k times)} & \text{if } k > 0 \\ 0 & \text{if } k = 0 \\ -1 - 1 - \cdots - 1 \text{ ($|k|$ times)} & \text{if } k < 0. \end{cases}$$

is a ring homomorphism whose kernel is $n\mathbb{Z}$, where n is the characteristic of R (this explains the use of the terminology "characteristic 0" instead of the archaic phrase "characteristic ∞" for rings in which no sum of 1's is zero).

(b) Show that $mn \cdot 1_R = (n \cdot 1_R)(m \cdot 1_R)$ for positive integers m and n, and that the characteristic of an integral domain is either 0 or a prime p.

(c) Prove that if p is a prime and if R is a commutative ring of characteristic p, then

$$(a + b)^p = a^p + b^p \quad \text{for all } a, b \in R.$$

(d) Show that the characteristic of an integral domain is the same as that of its field of fractions.

Exercise (b) shows that, the characteristic of an integral domain is either 0 or a prime p. Let 1_F denotes the identity of F. Exercise (a) along with the First Isomorphism Theorem shows that, F contains a subfield isomorphic either to $\mathbb{Q}$ (the field of fractions of $\mathbb{Z}$) or to $\mathbb{F}_p \coloneqq \mathbb{Z}/p\mathbb{Z}$ (the field of fractions of $\mathbb{Z}/p\mathbb{Z}$) depending on the characteristic of F, and in either case is the smallest subfield of F containing 1_F (the field generated by 1_F in F). This subfield is called the **prime subfield** of F.

One can verify that, if $\mathrm{char}(F) = p$ then for any $\alpha \in F$,

$$p \cdot \alpha \coloneqq \underbrace{\alpha + \alpha + \cdots + \alpha}_{p \text{ times}} = 0.$$

We shall usually denote the identity 1_F of a field F simply by 1. Then in a field of characteristic p, one has $p \cdot 1 = 0$, frequently written simply $p = 0$ (for example, $2 = 0$ in a field of characteristic 2). It should be kept in mind, however, that this is a shorthand statement — the element "p" is really $p \cdot 1_F$ and is not a distinct element in F.

1.2 Field extensions

Any homomorphism $\varphi : F \to F'$ of fields is either identically 0 or is injective, so that the image of φ is either 0 or isomorphic to F. This follows from the fact that the only ideals of a field F are 0 and F.

If K is a field containing the subfield F, then K is said to be an **extension field** (or simply an **extension**) of F, denoted K/F or by the diagram

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

In particular, every field F is an extension of its prime subfield. The field F is sometimes called the **base field** of the extension. (The notation K/F for a field extension is a shorthand for "K over F" and is not the quotient of K by F.)

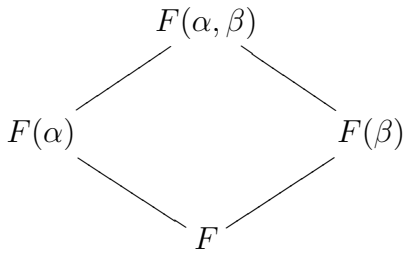
If K/F is any extension of fields, then the multiplication defined in K makes K into a vector space over F. In particular every field F can be considered as a vector space over its prime field. The **degree** (or **relative degree** or **index**) of a field extension K/F, denoted $[K : F]$, is the dimension of K as a vector space over F (i.e. $[K : F] \coloneqq \dim_F K$). The extension is said to be **finite** if $[K : F]$ is finite and is said to be **infinite** otherwise.

Exercise ([1] §13.2 Exercise 1)**.** *Let $\mathbb{F}$ be a finite field of characteristic p. Prove that $|\mathbb{F}| = p^n$ for some positive integer n.*

Suppose F is a subfield of a field K and $\alpha \in K$ is an element of K. Then the collection of subfields of K containing both F and α is nonempty (K is such a field, for example). Since the intersection of subfields is again a subfield, it follows that there is a unique minimal subfield of K containing both F and α (the intersection of all subfields with this property). Let $\alpha, \beta, \cdots \in K$ be a collection of elements of K. Then the smallest subfield of K containing both F and the elements $\alpha, \beta, \ldots$, denoted $F(\alpha, \beta, \ldots)$, is called the field **generated by** $\alpha, \beta, \ldots$ **over** F.

If the field K is generated by a single element a over F, $K = F(\alpha)$, then K is said to be a **simple extension** of F and the element α is called a **primitive element** for the extension.

Lemma ([1] §13.2 Lemma 16)**.** *$F(\alpha,\beta) = (F(\alpha))(\beta)$, i.e., the field generated over F by α and β, is the field generated by β over the field $F(\alpha)$ generated by α. Pictorially,*



1.3 Simple extensions

An important class of field extensions are those obtained by trying to solve equations over a given field F. For example, if $F = \mathbb{R}$ is the field of real numbers, then the simple equation $x^2 + 1 = 0$ does not have a solution in F. The question arises whether there is some larger field containing $\mathbb{R}$ in which this equation does have a solution, and it was this question that led Gauss to introduce the complex numbers $\mathbb{C} = \mathbb{R} + \mathbb{R}i$, where i is defined so that $i^2 + 1 = 0$. One then defines addition and multiplication in $\mathbb{C}$ by the usual rules familiar from elementary algebra and checks that in fact $\mathbb{C}$ so defined is a field, i.e., it is possible to find an inverse for every nonzero element of $\mathbb{C}$.

Given any field F and any polynomial $p(x) \in F[x]$ one can ask a similar question: does there exist an extension K of F containing a solution of the equation $p(x) = 0$ (i.e., containing a root of $p(x)$)? Note that we may assume here that the polynomial $p(x)$ is irreducible in $F[x]$, since a root of any factor of $p(x)$ is certainly a root of $p(x)$ itself.

Recall that $F[x]$ is an Euclidean Domain and hence a Principal Ideal Domain; $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible (cf. [1] §9.2 Exercise 3).

Theorem ([1] §13.1 Theorem 3)**.** *Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial. Then there exists a field K containing an isomorphic copy of F in which $p(x)$ has a root. (Identifying F with this isomorphic copy shows that there exists an extension of F in which $p(x)$ has a root.)*

Proof. Consider the quotient

$$K \coloneqq F[x]/(p(x))$$

of the polynomial ring $F[x]$ by the ideal generated by $p(x)$. Since by assumption $p(x)$ is an irreducible polynomial in the P.I.D. (Principal Ideal Domain) $F[x]$, K is actually a field.

The canonical projection $\pi : F[x] \to F[x]/(p(x))$ restricted to $F \subset F[x]$ gives a homomorphism $\varphi = \pi|_F : F \to K$, which is not identically 0 since it maps the identity 1 of F to the identity 1 of K. Hence $\varphi(F) \cong F$ is an isomorphic copy of F contained in K. We identify F with its isomorphic image in K and view F as a subfield of K.

If $\bar{x} \coloneqq \pi(x) = x \pmod{p(x)}$ denotes the image of x in the quotient K, then

$$\begin{aligned} p(\bar{x}) &= \overline{p(x)} && \text{(since } \pi \text{ is a homomorphism)} \\ &= p(x) \pmod{p(x)} && \text{in } F[x]/(p(x)) \\ &= 0 && \text{in } F[x]/(p(x)) \end{aligned}$$

so that K does indeed contain a root of the polynomial $p(x)$. Then K is an extension of F in which the polynomial $p(x)$ has a root. □

Example. *Let $F = \mathbb{Q}$ and $p(x) = x^3 - 2$, irreducible over $\mathbb{Q}$ by Eisenstein's Criterion. Clearly $\mathbb{C}$ is an extension of $\mathbb{Q}$ containing "all" solutions of the equation $x^3 - 2 = 0$:*

$$x = \sqrt[3]{2}, \sqrt[3]{2}\omega, \sqrt[3]{2}\omega^2, \quad \text{where } \omega = \zeta_3 \coloneqq \frac{-1 + \sqrt{3}i}{2}.$$

In particular, $\mathbb{Q}(\sqrt[3]{2})$ (the smallest subfield of $\mathbb{C}$ containing $\sqrt[3]{2}$) is an extension of $\mathbb{Q}$ in which $p(x) = x^3 - 2$ has a root. But by the proof of the above theorem, we know $K \coloneqq \mathbb{Q}[x]/(x^3 - 2)$ is also an extension of $\mathbb{Q}$ containing (at least one) solution of the equation $x^3 - 2 = 0$; the solution in K is denoted by $\bar{x} \coloneqq x \pmod{x^3 - 2}$. Later in this section we will show that K is isomorphic to $\mathbb{Q}(\sqrt[3]{2})$ (cf. [1] §13.1 Theorem 6).

Theorem ([1] §13.1 Theorem 4)**.** *Let $p(x) \in F[x]$ be an irreducible polynomial of degree n over the field F and let K be the field $F[x]/(p(x))$. Let $\theta \coloneqq x \bmod (p(x)) \in K$. Then the elements*

$$1, \theta, \theta^2, \ldots, \theta^{n-1}$$

are a basis for K as a vector space over F, so the degree of the extension is n, i.e., $[K : F] = n$. Hence

$$K = F(\theta) = \{a_0 + a_1\theta + a_2\theta^2 + \cdots + a_{n-1}\theta^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in F\}$$

consists of all polynomials of degree $< n$ in θ.

Proof. Exercise. □

Example. *Let $F = \mathbb{F}_p(t)$ be the field of rational functions in the variable t over the finite field $\mathbb{F}_p$. Let $p(x) = x^p - t \in F[x]$. Then $p(x)$ is irreducible (it is Eisenstein at the prime (t) in $\mathbb{F}_p[t]$). If we denote a root by θ, the corresponding degree p field extension $F(\theta)$ consists of the elements*

$$\{a_0(t) + a_1(t)\theta + \cdots + a_{p-1}(t)\theta^{p-1} \mid a_0(t), a_1(t), \ldots, a_{p-1}(t) \in F = \mathbb{F}_p(t)\}$$

where the coefficients $a_i(t)$'s are rational functions in t with coefficients in $\mathbb{F}_p$ and where $\theta^p = t$. This is an example of an extension over an infinite field with prime characteristic.

Example. *Take $F = \mathbb{F}_2$, the finite field with two elements, and $p(x) = x^2 + x + 1$, which is irreducible over $\mathbb{F}_2$ (if not, then $p(x)$ has a factor of degree one, and hence has a root in $\mathbb{F}_2$, but neither 0 nor $1 \in \mathbb{F}_2$ is a root of $p(x)$). Here we obtain a degree 2 extension of $\mathbb{F}_2$:*

$$\mathbb{F}_2[x]/(x^2 + x + 1) = \{a + b\theta \mid a, b \in \mathbb{F}_2\}$$

where $\theta^2 = -\theta - 1 = \theta + 1$. Multiplication in this field $\mathbb{F}_2(\theta)$ (which contains four elements because $[\mathbb{F}_2(\theta) : \mathbb{F}_2] = \deg p(x) = 2$) is defined by

$$\begin{aligned}(a + b\theta)(c + d\theta) &= ac + (ad + bc)\theta + bd\theta^2 \\ &= ac + (ad + bc)\theta + bd(\theta + 1) \\ &= (ac + bd) + (ad + be + bd)\theta.\end{aligned}$$

Exercise ([1] §13.2 Exercise 2)**.** *Construct a finite field containing 27 elements.*

The above theorem provides an easy description of the elements of the field $K = F[x]/(p(x))$ as polynomials of degree $< n$ in θ where θ is an element (in K) with $p(\theta) = 0$. We may suppose $p(x)$ is monic (since its roots and the ideal it generates do not change by multiplying by a constant), say $p(x) = x^n + p_{n-1}x^{n-1} + \cdots + p_1x + p_0$. Then in K, since $p(\theta) = 0$, we have

$$\theta^n = -(p_{n-1}\theta^{n-1} + \cdots + p_1\theta + p_0),$$

i.e., θ^n is a linear combination of lower powers of θ. Multiplying both sides by θ and replacing the θ^n on the right hand side by these lower powers again, we see that also θ^{n+1} is a polynomial of degree $< n$ in θ. Similarly, any positive power of θ can be written as a polynomial of degree $< n$ in θ, hence any polynomial in θ can be written as a polynomial of degree $< n$ in θ.

Example. *Let $F = \mathbb{Q}$ and $p(x) = x^3 - 2$. Denoting a root (in $K = \mathbb{Q}[x]/(x^3 - 2)$) of $p(x)$ by $\theta \coloneqq x \bmod (p(x))$, we obtain the field*

$$\mathbb{Q}[x]/(x^3 - 2) = \{a + b\theta + c\theta^2 \mid a, b, c \in \mathbb{Q}\} = \mathbb{Q}(\theta)$$

with $\theta^3 = 2$, an extension of degree 3.

To find the inverse of, say, $1 + \theta$ in this field, we can proceed as follows: By the Euclidean Algorithm in $\mathbb{Q}[x]$ there are polynomials $a(x)$ and $b(x)$ with

$$a(x)(1 + x) + b(x)(x^3 - 2) = 1$$

(since $p(x) = x^3 - 2$ is irreducible, it is relatively prime to every polynomial of smaller degree). In the quotient field this equation implies that $a(\theta)$ is the inverse of $1 + \theta$. In this case, a simple computation shows that we can take $a(x) = \frac{1}{3}(x^2 - x + 1)$ (and $b(x) = -\frac{1}{3}$), so that

$$(1 + \theta)^{-1} = \frac{1}{3}(\theta^2 - \theta + 1).$$

In particular,

$$(1 + \sqrt[3]{2})^{-1} = \frac{1}{3}((\sqrt[3]{2})^2 - \sqrt[3]{2} + 1), \quad (1 + \sqrt[3]{2}\omega)^{-1} = \frac{1}{3}((\sqrt[3]{2}\omega)^2 - \sqrt[3]{2}\omega + 1).$$

The connection between the simple extension $F(\alpha)$ generated by α over F where α is a root of some irreducible polynomial $p(x)$ and the field $F[x]/(p(x))$ is provided by the following:

Theorem ([1] §13.1 Theorem 6)**.** *Let F be a field and let $p(x) \in F[x]$ be an irreducible polynomial of degree n. Suppose K is an extension field of F containing a root α of $p(x)$. Let $F(\alpha)$ denote the subfield of K generated over F by α. Then*

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

In particular,

$$F(\alpha) = \{a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{n-1}\alpha^{n-1} \mid a_0, a_1, \ldots, a_{n-1} \in F\} \subseteq K.$$

Proof. There is a natural homomorphism

$$\begin{aligned} \varphi : F[x] &\longrightarrow F(\alpha) \subseteq K \\ a(x) &\longmapsto a(\alpha) \end{aligned}$$

obtained by mapping F to F by the identity map and sending x to α and then extending so that the map is a ring homomorphism (i.e., the polynomial $a(x)$ in x maps to the polynomial $a(\alpha)$ in α).

Since $p(\alpha) = 0$ by assumption, the element $p(x)$ is in the kernel of φ, so we obtain an induced homomorphism (also denoted φ)

$$\varphi : F[x]/(p(x)) \longrightarrow F(\alpha).$$

But since $p(x)$ is irreducible, the quotient on the left is a field, and φ is not the 0 map (it is the identity on F, for example), hence φ is an isomorphism of the field on the left with its image.

Since this image is then a subfield of $F(\alpha)$ containing F and containing α, by the definition of $F(\alpha)$ the map must be surjective, proving the theorem. □

As the above theorem indicates, the roots of an irreducible polynomial $p(x)$ are **algebraically indistinguishable** in the sense that the fields obtained by adjoining any root of an irreducible polynomial are isomorphic. For example, the fields obtained by adjoining one of the three possible (complex) roots of $x^3 - 2 = 0$ to $\mathbb{Q}$ were all algebraically isomorphic: $\mathbb{Q}(\sqrt[3]{2}) \cong \mathbb{Q}(\sqrt[3]{2}\omega) \cong \mathbb{Q}[x]/(x^3-2)$. The fields were distinguished not by their algebraic properties, but by whether their elements were *real*, which involves *continuous* operations.

Exercise. *Show that* $\mathbb{Q}(\sqrt{2}) \ncong \mathbb{Q}(\sqrt{3})$.

1.4 Cyclotomic polynomials and extensions

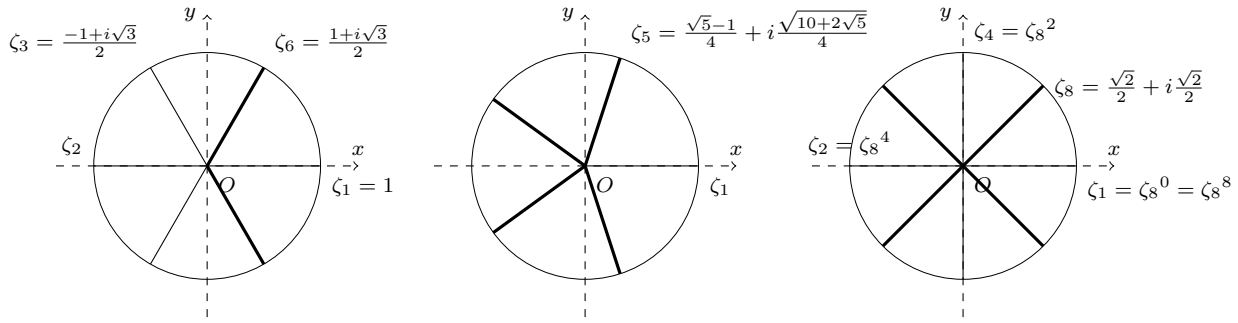
Consider the polynomial $x^n - 1$ over $\mathbb{Q}$. The roots of this polynomial are called the n^{th} **roots of unity**. Over $\mathbb{C}$ there are n distinct solutions of the equation $x^n = 1$, namely the elements

$$e^{2\pi i \frac{k}{n}} = \cos\frac{2\pi k}{n} + i \sin\frac{2\pi k}{n}$$

for $k = 0, 1, \ldots, n-1$. These points are given geometrically by n equally spaced points starting with the point $(1, 0)$ (corresponding to $k = 0$) on a circle of radius 1 in the complex plane.

The collection of n^{th} roots of unity form a group of order n under multiplication. Obviously this is a cyclic group, denoted μ_n, and it can be generated by $e^{2\pi i/n}$. A generator of μ_n is called a **primitive** n^{th} root of unity.

Let ζ_n denote a primitive n^{th} root of unity. (For example, over $\mathbb{C}$ we usually use ζ_n to denote $e^{2\pi i/n}$.) The other primitive n^{th} roots of unity are then the elements ${\zeta_n}^a$ where $1 \le a < n$ is an integer relatively prime to n, since these are the other generators for a cyclic group of order n. In particular there are precisely $\varphi(n)$ primitive n^{th} roots of unity, where $\varphi(n)$ denotes the Euler totient function. The primitive roots of unity in $\mathbb{C}$ for some small values of n are:



The splitting field of $x^n - 1$ over $\mathbb{Q}$ (the smallest extension over $\mathbb{Q}$ which contains all n^{th} roots of unity) is the field $\mathbb{Q}(\zeta_n)$ and is called the **cyclotomic field of** n^{th} **roots of unity**.

Determining the degree of this extension requires some analysis of the minimal polynomial of ζ_n over $\mathbb{Q}$. For example, when $n = p$ is a prime, ζ_p is a root of the polynomial

$$\Phi_p(x) \coloneqq \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

which is irreducible (since $\Phi_p(y+1)$ is Eisenstein). It follows that $\Phi_p(x)$ is the minimal polynomial of ζ_p over $\mathbb{Q}$, so that $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$.

In general, ζ_n satisfies the n^{th} **cyclotomic polynomial** $\Phi_n(x)$, which is the polynomial whose roots are the primitive n^{th} roots of unity:

$$\Phi_n(x) \coloneqq \prod_{\substack{\zeta \in \mu_n \\ \text{primitive}}} (x - \zeta) = \prod_{\substack{1 \le a < n \\ GCD(a,n)=1}} (x - {\zeta_n}^a)$$

which is of degree $\varphi(n)$.

Example. *Let $n = 6$. The roots of the polynomial $x^6 - 1$ are precisely the 6^{th} roots of unity so we have the factorization*

$$x^6 - 1 = \prod_{i=0}^{5}(x - {\zeta_6}^i) = \underbrace{(x - {\zeta_6}^0)}_{\Phi_1(x)} \cdot \underbrace{(x - {\zeta_6}^3)}_{\Phi_2(x)} \cdot \underbrace{(x - {\zeta_6}^2)(x - {\zeta_6}^4)}_{\Phi_3(x)} \cdot \underbrace{(x - {\zeta_6}^1)(x - {\zeta_6}^5)}_{\Phi_6(x)}.$$

Precisely we have

$$\Phi_1(x) = x - 1, \quad \Phi_2(x) = x + 1, \quad \Phi_3(x) = x^2 + x + 1, \quad \Phi_6(x) = x^2 - x + 1.$$

Moreover

$$x^2 - 1 = \Phi_1(x)\Phi_2(x), \quad x^3 - 1 = \Phi_1(x)\Phi_3(x), \quad x^6 - 1 = \Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_6(x).$$

As shown in the example, grouping together the factors $(x - {\zeta_n}^i)$ where ${\zeta_n}^i$ is an element of order d in μ_n (i.e., ${\zeta_n}^i$ is a primitive d^{th} root of unity), we have the factorization

$$x^n - 1 = \prod_{d|n} \prod_{\substack{\zeta \in \mu_d \\ \text{primitive}}} (x - \zeta) = \prod_{d|n} \Phi_d(x).$$

(Note incidentally that comparing degrees gives the identity $n = \sum_{d|n} \varphi(d)$.) One can show by induction and by Gauss' Lemma (cf. [1] §13.6 Lemma 40) that the cyclotomic polynomial $\Phi_n(x)$ is a monic polynomial in $\mathbb{Z}[x]$.

Theorem ([1] §13.6 Theorem 41 & Corollary 42)**.** *The cyclotomic polynomial $\Phi_n(x)$ is an irreducible monic polynomial in $\mathbb{Z}[x]$ of degree $\varphi(n)$. Therefore $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.*

Exercise. *We know the coefficients of $\Phi_p(x)$ are all 1 when p is a prime. Is it true that all the coefficients of any cyclotomic polynomial are 0 and ± 1?*

2 Algebraic extensions

2.1 Algebraic and transcendental elements

Let F be a field and let K be an extension of F. The element $\alpha \in K$ is said to be **algebraic** over F if α is a root of some nonzero polynomial $f(x) \in F[x]$. If α is not algebraic over F (i.e., is not the root of any nonzero polynomial with coefficients in F) then α is said to be **transcendental** over F. The extension K/F is said to be **algebraic** if every element of K is algebraic over F.

Let α be algebraic over F. Then (cf. [1] §13.2 Proposition 9) there is a unique monic irreducible polynomial $m_{\alpha,F}(x) \in F[x]$ which has α as a root; a polynomial $f(x) \in F[x]$ has α as a root if and only if $m_{\alpha,F}(x)$ divides $f(x)$ in $F[x]$. The polynomial $m_{\alpha,F}(x)$ (or just $m_\alpha(x)$ if the field F is understood) is called the **minimal polynomial** for α over F. The degree of $m_\alpha(x)$ is called the degree of α. By [1] §13.1 Theorem 6 we have

$$F(\alpha) \cong F[x]/(m_\alpha(x))$$

so that in particular

$$[F(\alpha) : F] = \deg m_\alpha(x) = \deg \alpha,$$

i.e., the degree of α over F is the degree of the extension it generates over F. Moreover, a monic polynomial over F with α as a root is the minimal polynomial for α over F if and only if it is irreducible over F.

Note that if α is algebraic over a field F then it is algebraic over any extension field L of F (if $f(x)$ having α as a root has coefficients in F then it also has coefficients in L). Moreover, $m_{\alpha,L}(x)$ divides $m_{\alpha,F}(x)$ in $L[x]$. In particular, $[L(\alpha):L] \leq [F(\alpha):F]$.

Example. *$\sqrt[6]{2}$ is algebraic over $\mathbb{Q}$ and it has minimal polynomial $m_{\sqrt[6]{2},\mathbb{Q}}(x) = x^6 - 2$. But the minimal polynomial of $\sqrt[6]{2}$ over $\mathbb{Q}(\sqrt{2})$ is $m_{\sqrt[6]{2},\mathbb{Q}(\sqrt{2})}(x) = x^3 - \sqrt{2}$.*

$\sqrt{3}$ is algebraic over $\mathbb{Q}$ and it has minimal polynomial $m_{\sqrt{3},\mathbb{Q}}(x) = x^2 - 3$. But the minimal polynomial of $\sqrt{3}$ over $\mathbb{Q}(\sqrt{2})$ is still $m_{\sqrt{3},\mathbb{Q}(\sqrt{2})}(x) = x^2 - \sqrt{3}$: we know that $m_{\sqrt{3},\mathbb{Q}(\sqrt{2})}(x)$ divides $m_{\sqrt{3},\mathbb{Q}}(x) = x^2 - \sqrt{3}$ so $m_{\sqrt{3},\mathbb{Q}(\sqrt{2})}(x)$ has degree 1 or 2; if $\deg m_{\sqrt{3},\mathbb{Q}(\sqrt{2})}(x) = 1$ then $\sqrt{3} \in \mathbb{Q}(\sqrt{2})$, i.e. $\sqrt{3} = a + b\sqrt{2}$ for some $a, b \in \mathbb{Q}$, which is impossible (why).

In particular $[\mathbb{Q}(\sqrt[6]{2}, \sqrt{2}) : \mathbb{Q}(\sqrt{2})] = [\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}(\sqrt{2})] = 3$ and $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{2})] = 2$.

The next exercise gives an effective procedure for determining an equation of degree n (the "characteristic polynomial") satisfied by an element α in an extension of F of degree n, with which one can compute its minimal polynomial.

Exercise ([1] §13.2 Exercises 19 & 20)**.** *Let K be an extension of F of degree n.*

(a) For any $\alpha \in K$ prove that α acting by left multiplication on K is an F-linear transformation of K.

(b) Prove that K is isomorphic to a subfield of the ring of $n \times n$ matrices over F, so the ring $M_n(F)$ contains an isomorphic copy of every extension of F of degree $\leq n$.

(c) Show that if the matrix of the linear transformation "multiplication by α" is A, then α is a root of the characteristic polynomial for A.

(d) Find the monic polynomial of degree 3 satisfied by $\sqrt[3]{2}$ and by $1 + \sqrt[3]{2} + \sqrt[3]{4}$.

2.2 Quadratic extensions

Let F be a field of characteristic $\neq 2$, and let K be an extension of F of degree 2, $[K:F] = 2$. Let α be any element of K not contained in F. Then $1, \alpha, \alpha^2$ are linearly dependent over F, i.e., α satisfies an equation of degree at most 2 over F. This equation cannot be of degree 1, since α is not an element of F by assumption. It follows that the minimal polynomial of α is a monic quadratic

$$m_\alpha(x) = x^2 + bx + c, \quad b, c \in F.$$

Since $F \subsetneq F(\alpha) \subseteq K$ and $F(\alpha)$ is already a vector space over F of dimension 2, we have $K = F(\alpha)$.

The roots of this quadratic equation can be determined by the quadratic formula, which is valid over any field of characteristic $\neq 2$:

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

(the reason for requiring the characteristic of F not be 2 is that we must divide by 2). Here $b^2 - 4c$ is not a square in F since a is not an element of F and the symbol $\sqrt{b^2 - 4c}$ denotes a root of the equation $x^2 - (b^2 - 4c) = 0$ in K. Note that here there is no natural choice of one of the roots — the roots are algebraically indistinguishable.

Then $F(\alpha) = F(\sqrt{b^2 - 4c})$. It follows that any extension K of F of degree 2 is of the form $F(\sqrt{D})$ where D is an element of F which is not a square in F, and conversely, every such extension is an extension of degree 2 of F. For this reason, extensions of degree 2 of a field F are called **quadratic extensions** of F.

2.3 Finite extensions

Theorem ([1] §13.2 Proposition 12 & Corollary 13)**.** *If the extension K/F is finite, then it is algebraic. In particular, the element α is algebraic over F if and only if the simple extension $F(\alpha)/F$ is finite, if and only if $F(\alpha)/F$ is algebraic.*

Proof. Let $[K : F] = n$. Then, for any $\alpha \in K$, the $n + 1$ elements $1, \alpha, \alpha^2, \ldots, \alpha^n$ of K are linearly dependent over F, say

$$b_0 + b_1\alpha + b_2\alpha^2 + \cdots + b_n\alpha^n = 0$$

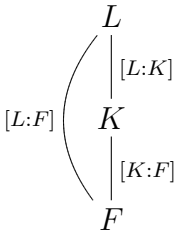
with $b_0, b_1, b_2, \ldots, b_n \in F$ not all 0. Hence α is the root of a nonzero polynomial with coefficients in F (of degree $\leq n$), which proves any $\alpha \in K$ is algebraic over F. □

Suppose that F is a subfield of a field K which in turn is a subfield of a field L. Then there are three associated extension degrees — the dimension of K and L as vector spaces over F, and the dimension of L as a vector space over K.

Theorem ([1] §13.2 Theorem 14)**.** *Let $F \subseteq K \subseteq L$ be fields. Then*

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

i.e. extension degrees are multiplicative, where if one side of the equation is infinite, the other side is also infinite. Pictorially,

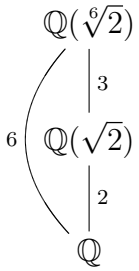


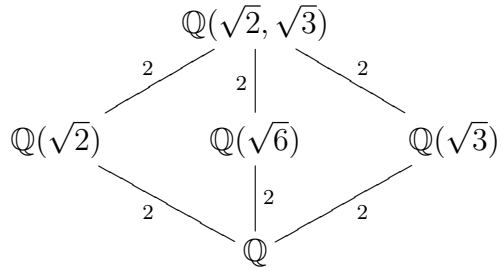
In particular, if L/F is a finite extension, then $[K : F]$ divides $[L : F]$.

Note the similarity of this result with the result on group orders. We shall frequently indicate the relative degrees of extensions in field diagrams.

Proof. Exercise. □

Example.





In particular, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$ *and* $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}(\sqrt{6})] = 2$

Exercise ([1] §13.2 Exercise 7)**.** *Prove that* $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$*. Conclude that* $[\mathbb{Q}(\sqrt{2} + \sqrt{3}) : \mathbb{Q}] = 4$*. Find an irreducible polynomial satisfied by* $\sqrt{2} + \sqrt{3}$*.*

Corollary ([1] §13.2 Corollaries 18 & 19)**.** *Suppose α and β are algebraic over F. Then $\alpha \pm \beta$, $\alpha\beta$, α/β (for $\beta \neq 0$), (in particular α^{-1} for $\alpha \neq 0$) are all algebraic. Moreover, if L/F is an arbitrary extension, then the collection of elements of L that are algebraic over F form a subfield $\bar{L}$ of L, called the* ***algebraic closure*** *of F in L.*

Proof. All of these elements lie in the extension $F(\alpha, \beta)$. By [1] §13.2 Theorem 14

$$[F(\alpha, \beta) : F] = [F(\alpha, \beta) : F(\alpha)][F(\alpha) : F] \leq [F(\beta) : F][F(\alpha) : F] < \infty,$$

and by [1] §13.2 Corollary 13 $F(\alpha, \beta)/F$ is algebraic. □

Example. *Consider the extension $\mathbb{C}/\mathbb{Q}$ and let $\overline{\mathbb{Q}}$ denote the subfield of all elements in $\mathbb{C}$ that are algebraic over $\mathbb{Q}$. In particular, the elements $\sqrt[n]{2}$ (the positive n^{th} roots of 2 in $\mathbb{R}$) are all elements of $\overline{\mathbb{Q}}$, so that $[\overline{\mathbb{Q}} : \mathbb{Q}] \geq n$ for all integers $n > 1$. Hence $\overline{\mathbb{Q}}$ is an infinite algebraic extension of $\mathbb{Q}$, called the field of* ***algebraic numbers****.*

It is extremely difficult in general to prove that a given real number is not algebraic. For example, it is known that $\pi = 3.14159\ldots$ and $e = 2.71828\ldots$ are transcendental elements of $\mathbb{R}$. Even the proofs that these elements are not rational are not too easy.

2.4 The composite fields

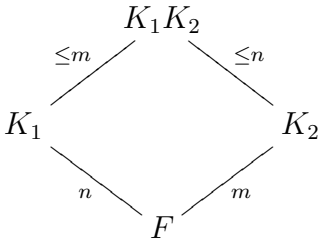
Let K_1 and K_2 be two subfields of a field K. Then the **composite field** of K_1 and K_2, denoted K_1K_2, is the smallest subfield of K containing both K_1 and K_2. Similarly, the composite of any collection of subfields of K is the smallest subfield containing all the subfields.

Note that the composite K_1K_2 can also be described as the intersection of all the subfields of K containing both K_1 and K_2 and similarly for the composite of more than two fields, analogous to the subgroup generated by a subset of a group (cf. [1] §2.4).

Proposition ([1] §13.2 Proposition 21)**.** *Let K_1 and K_2 be two finite extensions of a field F contained in K. Then*

$$[K_1K_2 : F] \leq [K_1 : F][K_2 : F]$$

with equality if and only if an F-basis for one of the fields remains linearly independent over the other field. If $\alpha_1, \alpha_2, \ldots, \alpha_n$ and $\beta_1, \beta_2, \ldots, \beta_m$ are bases for K_1 and K_2 over F, respectively, then the elements $\alpha_i\beta_j$ for $i = 1, 2, \ldots, n$ and $j = 1, 2, \ldots, m$ span K_1K_2 over F. We have the following diagram:



Proof. It is clear that the bases give generators for the composite K_1K_2 over F:

$$K_1K_2 = F(\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_m).$$

Since $\alpha_1, \alpha_2, \ldots, \alpha_n$ is an F-basis for K_1 any power ${\alpha_i}^k$ of one of the α's is a linear combination with coefficients in F of the α's and a similar statement holds for the β's. It follows that the collection of linear combinations

$$\sum_{1 \leq i \leq n,\ 1 \leq j \leq m} c_{ij}\alpha_i\beta_j$$

with coefficients in F is closed under multiplication and addition since in a product of two such elements any higher powers of the α's and β's can be replaced by linear expressions. Hence, the elements $\alpha_i\beta_j$ span the composite extension K_1K_2 over F. In particular, $[K_1K_2 : F] \leq mn$.

From $K_1K_2 = F(\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_m) = K_1(\beta_1, \beta_2, \ldots, \beta_m)$, we see as above that $\beta_1, \beta_2, \ldots, \beta_m$ span K_1K_2 over K_1. Hence $[K_1K_2 : K_1] \leq m = [K_2 : F]$ with equality if and only if these elements are linearly independent over K_1. Since $[K_1K_2 : F] = [K_1K_2 : K_1][K_1 : F]$ this proves the proposition. □

3 Classical straightedge and compass constructions

As a simple application of the results we have obtained on algebraic extensions, and in particular on the multiplicativity of extension degrees, we can answer (in the negative) the following geometric problems posed by the Greeks:

I. (*Doubling the Cube*) Is it possible using only straightedge and compass to construct a cube with precisely twice the volume of a given cube?

II. (*Trisecting an Angle*) Is it possible using only straightedge and compass to trisect any given angle θ?

III. (*Squaring the Circle*) Is it possible using only straightedge and compass to construct a square whose area is precisely the area of a given circle?

To answer these questions we must translate the construction of lengths by compass and straightedge into algebraic terms. Let 1 denote a fixed given unit distance. Then any distance is determined by its length $a \in \mathbb{R}$, which allows us to view geometric distances as elements of the real numbers $\mathbb{R}$. Using the given unit distance 1 to define the scale on the axes, we can then construct the usual Cartesian plane $\mathbb{R}^2$ and view all of our constructions as occurring in $\mathbb{R}^2$.

The problems above then amount to determining whether particular lengths in $\mathbb{R}$ can be obtained by compass and straightedge constructions from a fixed unit distance. The collection of such real numbers together with their negatives will be called the **constructible** elements of $\mathbb{R}$. A point $(x, y) \in \mathbb{R}^2$ is then constructible if and only if its coordinates x and y are constructible elements of $\mathbb{R}$. We shall not distinguish between the lengths that are constructible and the real numbers that are constructible.

Each straightedge and compass construction consists of a series of operations of the following four types:

(1) connecting two given points by a straight line,

(2) finding a point of intersection of two straight lines,

(3) drawing a circle with given radius and center, and

(4) finding the point(s) of intersection of a straight line and a circle or the intersection of two circles.

Lemma ([1] §13.3 p.532 Fig.1)**.** *If two lengths a and b are given, then the lengths $a \pm b$, ab and a/b are all constructible. In particular, every rational number is constructible, and the collection of constructible elements form a subfield of $\mathbb{R}$ strictly larger than $\mathbb{Q}$ (since $\sqrt{2}$ is constructible).*

Theorem ([1] §13.3 Proposition 23)**.** *If the element $\alpha \in \mathbb{R}$ is obtained from a field $F \subseteq \mathbb{R}$ by a series of compass and straightedge constructions, then $[F(\alpha) : F] = 2^k$ for some integer $k \geq 0$.*

Proof. A straightedge construction (type (2)) defines points obtained by the intersection of two straight lines. The "two-point form" formula $\frac{x-x_0}{x_1-x_0} = \frac{y-y_0}{y_1-y_0}$ for the straight line connecting two points with coordinates in some field F gives an equation for the line of the form $ax + by - c = 0$ with $a, b, c \in F$. Solving two such equations simultaneously to determine the point of intersection of two such lines gives solutions also in F (following from Cramer's Rule). It follows that if the coordinates of two points lie in the field F then straightedge constructions alone will not produce additional points whose coordinates are not also in F.

A compass construction (type (3) or (4) above) defines points obtained by the intersection of a circle with either a straight line or another circle. A circle with center (h, k) and radius r has equation $(x - h)^2 + (y - k)^2 = r^2$ so when we consider the effect of compass constructions on elements of a field F we are considering simultaneous solutions of such an equation with a linear equation $ax + by - c = 0$ where $a, b, c, h, k, r \in F$, or the simultaneous solutions of two quadratic equations.

In the case of a linear equation and the equation for the circle, solving for y in the linear equation and substituting gives a *quadratic* equation for x (and y is given linearly in terms of x). Hence the coordinates of the point of intersection are at worst in a **quadratic extension** of F.

In the case of the intersection of two circles, say

$$(x - h_1)^2 + (y - k_1)^2 = {r_1}^2 \quad \text{and}$$
$$(x - h_2)^2 + (y - k_2)^2 = {r_2}^2,$$

subtraction of the second equation from the first shows that we have the same intersection by considering the two equations

$$(x - h_1)^2 + (y - k_1)^2 = {r_1}^2 \quad \text{and}$$
$$2(h_2 - h_1)x + 2(k_2 - k_1)y = \text{[a number in } F\text{]},$$

which is the intersection of a circle and a straight line (the straight line connecting the two points of intersection, in fact) of the type just considered.

It follows that if a collection of constructible elements is given, then one can construct all the elements in the subfield F of $\mathbb{R}$ generated by these elements and that any straightedge and compass operation on elements of F produces elements in at worst a *quadratic* extension of F. Since quadratic extensions have degree 2 and extension degrees are multiplicative, it follows that if $\alpha \in \mathbb{R}$ is obtained from elements in a field F by a (finite) series of straightedge and compass operations then α is an element of an extension K of F such that $[K : F] = 2^m$ for some m. Since $[F(\alpha) : F]$ divides this extension degree, it must also be a power of 2. □

Corollary ([1] §13.3 Theorem 24)**.** *None of the classical Greek problems: (I) Doubling the Cube, (II) Trisecting an Angle, and (III) Squaring the Circle, is possible.*

Proof. We will prove for example that it is impossible using only straightedge and compass to trisect $\theta = 60°$. By the triple angle formula for cosines:

$$\cos(3\alpha) = 4\cos^3\alpha - 3\cos\alpha,$$

we see that $\cos 20°$ satisfies the equation $8x^3 - 6x - 1 = 0$, which is irreducible in $\mathbb{Q}[x]$ (because it has no rational solution, cf. [1] §9.4 Proposition 11), so $[\mathbb{Q}(\cos 20°) : \mathbb{Q}] = 3$ and hence $\cos 20°$ is not constructible.

One can also study $\cos 20°$ by $2\cos\frac{\pi}{9} = \zeta_{18} + {\zeta_{18}}^{-1}$. In [1] §14.5 we shall see that

$$[\mathbb{Q}(\zeta_{18} + {\zeta_{18}}^{-1}) : \mathbb{Q}] = [\mathbb{Q}(\zeta_{18}) \cap \mathbb{R} : \mathbb{Q}] = [\mathbb{Q}(\zeta_{18}) : \mathbb{Q}]/2 = \varphi(18)/2 = 3.$$

In fact, one can verify, using the proposition of 18^{th} roots of unity, that the minimal polynomial of $\zeta_{18} + {\zeta_{18}}^{-1}$ in $\mathbb{Q}[x]$ is $x^3 - 3x - 1$. □

After discussing the cyclotomic fields in [1] §14.5 we shall consider another classical geometric question: "which regular n-gons can be constructed by straightedge and compass?" The construction of the regular n-gon in $\mathbb{R}^2$ is evidently equivalent to the construction of the n^{th} roots of unity, since the n^{th} roots of unity form the vertices of a regular n-gon on the unit circle in $\mathbb{C}$ with one vertex at the point 1. The construction of ζ_n is equivalent to the constructibility of the first coordinate x in $\mathbb{R}^2$ of ζ_n, namely $\operatorname{Re} \zeta_n = \cos \frac{2\pi}{n}$.

Theorem ([1] §14.5 Proposition 29)**.** *The regular n-gon can be constructed by straightedge and compass if and only if $n = 2^k p_1 \cdots p_r$ is the product of a power of 2 and distinct Fermat primes (primes of the form $2^{2^m} + 1$).*

Exercise ([1] §13.3 Exercise 1)**.** *Prove that it is impossible to construct the regular 9-gon.*

Exercise ([1] §13.3 Exercise 5)**.** *Construct the regular 5-gon by straightedge and compass.*

Other related exercises in [1]

§13.1 1 3 5 7
§13.2 5 11 12 13 14 16 18 21 22
§13.3 4
§13.6 3 4 7 8 9 10 11 12

References

[1] D. S. Dummit and R. M. Foote. *Abstract algebra*. John Wiley & Sons, Inc., Hoboken, NJ, third edition, 2004.