Introduction to Abstract Algebra II

A collection of notes on major definitions and results, proofs, and commentary based on the corresponding course at Illinois, as instructed by Hardt

Lecture Notes By

Dheeran E. Wiggins

Department of Mathematics
University of Illinois Urbana-Champaign

Disclaimer
The lecture notes in this document were based on Introduction to Abstract Algebra II [418], as instructed by Andrew Hardt [Department of Mathematics] in the Spring semester of 2024 [SP24] at the University of Illinois Urbana-Champaign. All non-textbook approaches, exercises, and comments are adapted from Hardt's lectures. These, in turn, were adapted from Nathan Dunfield's lecture notes for the same course.

Textbook
Many of the exercises and presentations were selected from *Abstract Algebra, Third Edition*, by David S. Dummit and Richard M. Foote.

Author Information
Dheeran E. Wiggins is, at the time of writing [Spring, 2024], a first-year student at Illinois studying mathematics and physics. All typesetting and verbiage are his own.

dheeran2@illinois.edu

Galois theory is a subtle, yet beautiful subject which characterizes solutions to polynomial equations through connections between groups and fields.

– Andrew Hardt

Contents

On the Theory of Rings

Euclidean Domains 1

After this point, unless otherwise stated, all rings R are commutative and contain a unity element $1 \in R$.

Definition 1.0.1 (Integral Domain) *Recall that integral domain is a ring without zero divisors. That is, if $a \neq 0$ and $b \neq 0$, then $ab \neq 0$.*

1.1 Normed Structure

We would now like to define the concept of "size" on our integral domains so we have the ability to measure distance between any two elements. The size structure here comes in the form of a norm.

Definition 1.1.1 (Norm) *A norm is a mapping $N : R \to \mathbb{Z}_{\geq 0}$[1] such that $N(0) = 0$.*

1: By $\mathbb{Z}_{\geq 0}$ we mean $\mathbb{Z}_+ \cup \{0\}$.

Definition 1.1.2 (Euclidean Norm) *A norm N is called Euclidean if for all $a, b \in R$, $b \neq 0$, there exist $q, r \in R$ such that*

$$a = qb + r.$$

Additionally, $r = 0$ or $N(r) < N(b)$.

Definition 1.1.3 (Euclidean Domain) *A Euclidean domain, is then defined as an integral domain R endowed with a Euclidean norm N.*

Example 1.1.1 Some examples of Euclidean domains are as follows:

(a) the ring $R := \mathbb{Z}$ with the norm

$$N : \mathbb{Z} \to \mathbb{Z}_{\geq 0} : a \mapsto |a|$$

(b) a field $R := \mathbb{F}$ with the norm

$$N : \mathbb{F} \to \mathbb{Z}_{\geq 0} : a \mapsto 0$$

for all $a \in \mathbb{F}$.

(c) a polynomial ring over a field $R := \mathbb{F}[x]$ with the norm

$$N : \mathbb{F}[x] \to \mathbb{Z}_{\geq 0} : p(x) \mapsto \deg(p).$$

(d) the ring $R := \mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$[2] with the norm

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0} : a + bi \mapsto |a + bi|^2 = a^2 + b^2.$$

2: This ring is called the Gaussian integers.

1.2 Divisibility and Principal Ideals

Now, given a Euclidean domain, we can use the Euclidean algorithm[3] to identify greatest common divisors.

Definition 1.2.1 (Divisibility) *We write $a \mid b$ in R if there exists an $x \in R$ such that $ax = b$.*[4]

Definition 1.2.2 (Greatest Common Divisor) *An element $d \in R$ of a ring R is a greatest common denominator, denoted* gcd,[5] *of a and b*

(i) if $d \mid a$ and $d \mid b$.
(ii) if $d' \mid a$ and $d' \mid b$, then $d' \mid d$.

Theorem 1.2.1 (Existence of gcd) *Let R be a Euclidean domain with $a, b \in R$ and $b \neq 0$. Then, a and b have a* gcd.[6]

Proof. Apply the Euclidean algorithm:

$$\begin{aligned} a &= q_0 b + r_0 \\ b &= q_1 r_0 + r_1 \\ r_0 &= q_2 r_1 + r_2 \\ &\vdots \\ r_{n-1} &= q_{n+1} r_n + 0, \end{aligned}$$

where

$$N(b) > N(r_0) > N(r_1) > \cdots > N(r_n).$$

We define $r_{-1} := b$ and $r_{-2} := a$ as a matter of convenience. At each step, notice that d is a common divisor of r_i and r_{i+1} if and only if d is a common divisor of r_{i+1} and r_{i+2}. As such, d is a $\gcd(r_i, r_{i+1})$ if and only if d is a gcd of r_{i+1} and r_{i+2}.

Since gcds are unchanged at each step, we have that

$$\gcd(r_n, r_{n+1}) = \gcd(r_n, 0) = r_n = \gcd(a, b),$$

proving $\gcd(a, b)$ exists □

Definition 1.2.3 (Ideal) *Recall that an ideal $I \subseteq R$ is an additive subgroup such that if $a \in I$ and $r \in R$, then $ra \in I$.*[7]

Definition 1.2.4 (Principal Ideal) *An ideal I is called principal if I has the form*

$$\langle a \rangle := \{ra : r \in R\}.$$

Theorem 1.2.2 *If R is a Euclidean domain, then every ideal is principal.*

3: If you have not seen the Euclidean algorithm before, review any text on elementary number theory.

4: We pronounce this as "a divides b" or "b is a multiple of a."

5: It is worthwhile to note that $\gcd(a, b)$ is not actually a well-defined notational choice, since these objects are not unique, generally. However, for the sake of convenience, we will use the notation to simply mean *a* gcd of the pair of elements.

6: In the case where $b = 0$, then $\gcd(a, b) = a$. Thus, the statement is more accurately written as "at least one of a or b are nonzero."

7: Note that since we are now solely working with commutative rings, so there is no need to distinguish left and right ideals.

Proof. Choose some $d \neq 0$ in I with minimum norm. If $a \in I$, then by the Euclidean property, we have

$$a = qd + r,$$

such that either $r = 0$ or $r \neq 0$ and $N(r) < N(d)$. However, the latter is impossible by assumption, meaning $r = 0$. Thus, $d \mid a$, so $I = \langle d \rangle$.[8] □

8: That is, we have demonstrated that $I \subseteq (d)$, and the reverse inclusion is trivial by definition.

Remark 1.2.1 The Gaussian integers $\mathbb{Z}[i]$ is a Euclidean domain.

Proof. Let $a, b \in \mathbb{Z}[i]$ with nonzero b. Then, let $q \in \mathbb{Z}[i]$ be an element which is closest in the complex plane to a/b (Fig. 1.1). That is to say,

$$\left| q - \frac{a}{b} \right|$$

is minimal. Now, let

$$r = a - qb \in \mathbb{Z}[i],$$

so $a = qb + r$.[9] All that remains for us to check is that of the norm. We have $N : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$ prescribed by

$$N : r \mapsto |r|^2 = |a - qb|^2 = \left| \frac{a}{b} - q \right|^2 |b|^2 \leq \frac{1}{2}|b|^2 = \frac{1}{2}N(b) < N(b),$$

since $N(b) \neq 0$, completing the proof.

□

9: The closest Gaussian integer may not be unique; i.e. there are equidistant points in $\mathbb{C}$, in which case we simply choose one of them.

Note that if we have $\mathbb{Z}[\sqrt{-5}] = \mathbb{Z}[i\sqrt{5}]$, this does not work, since the lattice formed by these points forces a potential distance between $|q - a/b| > 1$, which ruins the inequalities.

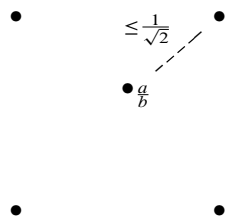


Figure 1.1: We visualized the complex plane with the $\mathbb{Z}[i]$ lattice embedded. The closest point to a/b is marked.

1.3 Consequences of Principality

Definition 1.3.1 (Principal Ideal Domain) *A principal ideal domain*[10] *is an integral domain in which every ideal is principal.*

10: Abbreviate as PID.

Remark 1.3.1 Since we know that in a Euclidean domain every ideal is principal, we can say that all Euclidean domains are PIDs.

Definition 1.3.2 *Recall that*

$$R[a] := \{r_0 + r_1 a + r_2 a^2 + \cdots + r_n a^n : r_i \in R \text{ and } n \in \mathbb{Z}_{\geq 0}\}.$$

Though we have not defined UFDs yet, we can now construct a series of structure-type inclusions with Euclidean domains, PIDs, UFDs,[11] and integral domains:

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

11: By this we abbreviate *unique factorization domains* which we will elaborate on in the next chapter.

Proposition 1.3.1 *Let R be a PID with $a, b \in R$. Take the ideal $\langle a, b\rangle = \langle d\rangle$. Then, we have*

(i) $d = sa + tb$ *for some* $s, t \in R$.
(ii) d *is a* gcd *of* a *and* b.

Proof. We have part (i) as a consequence of

$$d \in \langle d\rangle = \langle a, b\rangle = \{sa + tb : s, t \in R\}.$$

Since $a, b \in \langle d\rangle$, d is a common divisor of a and b. If $d' \mid a$ and $d' \mid b$, then $d' \mid (sa + tb) = d$. Thus, d is $\gcd(a, b)$, proving part (ii). □

Remark 1.3.2 Consider $\mathbb{F}[x, y]$. This structure is not a PID since $\langle x, y\rangle$ is not principal.[12]

12: Notice that we have $1 = \gcd(x, y)$ but we cannot have $1 = sx + ty$.

Definition 1.3.3 *Recall that if we have $r \in R$ in an integral domain. Then,*

(i) r *is a unit if there exists an* $s \in R$ *such that* $rs = sr = 1$.
(ii) *If r is not a unit and nonzero, then r is irreducible if $r = ab$ implies that a or b is a unit.*
(iii) r *is prime if* $r \mid ab$ *implies* $r \mid a$ *or* $r \mid b$.

Proposition 1.3.2 (Prime Irreducibility) *If $r \in R$ is prime in an integral domain, then r is irreducible.*

Proof. Let $r = ab$ and assume without loss of generality that $r \mid a$. That is, $a = rt$ for some $t \in R$. Then,

$$r = ab = rtb,$$

meaning $tb = 1$, demonstrating that b is a unit in R.[13] □

13: Note that the converse does not hold. For instance, $3 \in \mathbb{Z}[\sqrt{-5}]$ is irreducible, but

$$3^2 = (2 + \sqrt{-5})(2 - \sqrt{-5}),$$

and $3 \nmid 2 \pm \sqrt{-5}$, so 3 is not prime.

Definition 1.3.4 *Recall that if we have an ideal $I \subset R$,*

(i) I *is called maximal if either/both of these hold:*
- *there does not exist an ideal J such that $I \subset J \subset R$.*
- *R/I is a field.*

(ii) I *is called prime if either/both of these hold:*
- *$ab \in I$ implies $a \in I$ or $b \in I$.*
- *R/I is an integral domain.*

Notably, we have that every maximal ideal is prime.

Lemma 1.3.3 *We have that $\langle r\rangle$ is a prime ideal if and only if r is a prime element.*

Proof. We know $a \in \langle r \rangle$ if and only if a is a multiple of r, yielding

$$\underbrace{[ab \in \langle r \rangle \Rightarrow a \in \langle r \rangle \text{ or } b \in \langle r \rangle]}_{\text{prime ideal}} \iff \underbrace{[r \mid ab \Rightarrow r \mid a \text{ or } r \mid b]}_{\text{prime element}}.$$

□

Proposition 1.3.4 *Every nonzero prime ideal in a PID is maximal.*

Proof. Let

$$\{0\} \subset \langle p \rangle \subseteq \langle m \rangle \subseteq R,$$

where $\langle p \rangle$ is prime. By the previous results, $\langle p \rangle$ being prime implies p is prime, meaning p is irreducible. Since $\langle p \rangle \subseteq \langle m \rangle$, we know $p \in (m)$, so $p = am$ for some $a \in R$. Then, either

- a is a unit, in which case we have $\langle m \rangle = \langle p \rangle$.
- m is a unit, in which case we have $\langle m \rangle = R$.

Therefore, $\langle p \rangle$ is maximal. □

Corollary 1.3.5 *If $r \in R$ is a PID element, then r is prime if and only if r is irreducible.*

Proof. Note that the forward implication holds in any integral domain. For the converse, remember by the previous proof r is irreducible means (r) is maximal, by principality. Additionally, we observed that (r) must be prime as it is maximal, meaning r is prime. □

Remark 1.3.3 Note that $\mathbb{Z}[x]$ is not a PID since $(2, x)$ is not principal.

Proposition 1.3.6 *Motivated by the previous remark, $R[x]$ is a PID if and only if R is a field $\mathbb{F}$.*

Proof. For the converse direction, if $R =: \mathbb{F}$, then $\mathbb{F}[x]$ is a Euclidean domain, meaning it must be a PID. For the forward implication, assume $R[x]$ is a PID. Then, $R[x]$ being an integral domain implies R is an integral domain, so (x) must be prime.[14] As such, we have that $\langle x \rangle$ must be maximal,[15] implying that $R \cong {}^{R[x]}/_{(x)}$, forcing it to be a field. □

14: This is a result of the ismorphism

$$\varphi : {}^{R[x]}/_{\langle x \rangle} \xrightarrow{\sim} R.$$

15: We have this from it being a prime ideal in a PID.

1.4 Association and Uniqueness

Definition 1.4.1 (Associates) *In an integral domain R, r and s are called associates if $r \mid s$ and $s \mid r$.*[16]

16: That is, $r = us$ where $u \in R^\times$.

Definition 1.4.2 (UFD) *An integral domain R is a unique factorization domain (UFD) if for all nonzero, non-unit elements $r \in R$ if*

(i) $r = p_1 \cdot \cdots \cdot p_n$ *where each* $p_i \in R$ *is an irreducible.*
(ii) If we also have

$$r = q_1 \cdot \cdots \cdot q_m$$

such that $q_i \in R$ *are irreducible, then* $m = n$ *and there is some permutation* σ *on* $\mathbb{N}_n$ *such that* p_i *is an associate of* $q_{\sigma(i)}$.

Proposition 1.4.1 *Let* R *be a UFD with* $r, s \in R$.

(i) If r *is irreducible then* r *is prime.*
(ii) If

$$r = up_1^{e_1} \cdot \cdots \cdot p_n^{e_n}$$

and

$$s = vp_1^{f_1} \cdot \cdots \cdot p_n^{f_n},$$

where $u, v \in R^\times$ *and* $p_i \in R$ *are irreducible and pairwise non-associates, then*

$$d := p_1^{\min(e_1, f_1)} \cdot \cdots \cdot p_n^{\min(e_n, f_n)}$$

is a $\gcd(r, s)$.

Example 1.4.1 Let $R := \mathbb{Z}$ with

$$r := 36 = 2^2 \cdot 3^2$$

and

$$s := -192 = (-1) \cdot 2^6 \cdot 3,$$

so

$$d := 2^{\min(2,6)} \cdot 3^{\min(3,1)} = 4 \cdot 3 = 12.$$

Theorem 1.4.2 (PID to UFD Implication) *Let* R *be a PID. Then, it is also a UFD.*

17: We want to show that r has a unique prime factorization.

Proof. Let $r \in R$.[17] First, if r is irreducible, then we are done. Otherwise, we write $r = r_1 s_1$, where r_1 and s_1 are not units. Try to factor r_1 and s_1 similarly, and if this process eventually terminates, then r has a prime factorization. If the process does not terminate, then there exist elements

$$\underbrace{r_1, r_2, \cdots \in R}_{\text{infinitely many such elements}}$$

such that

$$\cdots r_3 \mid r_2 \mid r_1 \mid r.$$

18: Note that this uses choice.

That is, we have an ascending chain of ideals [18]

$$\langle r \rangle \subset \langle r_1 \rangle \subset \langle r_2 \rangle \subset \cdots \subset R.$$

Let

$$I := \bigcup_R \langle r_R \rangle .$$

It is not difficult to show that this is, in fact, an ideal. Since R is a PID,

$I = \langle a \rangle$ for some $a \in R$. Since $a \in I$, there exists a k such that $a \in \langle r_k \rangle$. Yet, then,

$$\langle r_{k+1} \rangle \subseteq I = \langle a \rangle \subseteq \langle r_{k+1} \rangle ,$$

which is a contradiction.[19] Thus, r has a prime factorization.

19: We have contradicted that the factoring process does not termiante.

Now, for uniqueness, suppose

$$r = \underbrace{p_1 \cdot \cdots \cdot p_n = q_1 \cdot \cdots \cdot q_m}_{\text{irreducible elements}} .$$

Since R is a PID, we know that irreducibility holds if and only if primality holds. Since $p_1 \mid r$, $p_1 \mid q_i$ for some i.[20] We know q_i is irreducible and u is a unit, so p_1 and q_1 are associates. Cancellation obtains

20: That is $p_1 u = q_1$ for a unit $u \in R^\times$.

$$\begin{aligned} p_2 \cdot \cdots \cdot p_n &= u^{-1} q_1 \cdot \cdots \cdot q_{i-1} q_{i+1} \cdot \cdots \cdot q_m \\ &= (u^{-1} q_1) \cdot \cdots \cdot q_{i-1} q_{i+1} \cdot \cdots \cdot q_m, \end{aligned}$$

and proceed by induction. □

Corollary 1.4.3 *Note that PIDs are Noetherian. That is, they do not have an infinite ascending chain of ideals*

$$I_1 \subset I_2 \subset \cdots \subset I_n \subset \cdots .$$

1.5 Consequences of Unique Factorization

Lemma 1.5.1 *$p = a^2 + b^2$ if and only if p is reducible in $\mathbb{Z}[i]$.*[21]

21: Recall the Euclidean norm

$$N : \mathbb{Z}[i] \to \mathbb{Z}_{\geq 0}$$

prescribed by

$$N : a + bi \mapsto |a + bi|^2 = a^2 + b^2.$$

Remember that

$$N(rs) = N(r)N(s),$$

since $|\cdot|$ is multiplicative. Additionally $N(z) = 1$ if and only if z is a unit, which is true if and only if $z = \pm 1$ or $\pm i$.

Proof. If $p = a^2 + b^2$, then in $\mathbb{Z}[i]$

$$p = (a + bi)(a - bi),$$

and neither factor is a unit since

$$N(a \pm bi) = a^2 + b^2 = p \neq 1.$$

For the converse, suppose $p = rs$ with $r, s \in \mathbb{Z}[i]$, where $r, s \notin \mathbb{Z}[i]^\times$. Then,

$$p^2 = N(p) = N(r)N(s),$$

and since r and s are not units, $N(r, s) \neq 1$. As such, we must have $N(r) = N(s) = p$. If $r = a + bi$, then

$$p = N(r) = a^2 + b^2.$$

□

Theorem 1.5.2 (Fermat) *Let $p \in \mathbb{Z}_{\geq 0}$ be an odd prime. Then, $p = a^2 + b^2$*

for integral a and b if and only if

$$p \equiv 1 \pmod 4.$$

This expression is unique up to order and sign.

Proof. If $p = a^2 + b^2$, then

$$p \equiv a^2 + b^2 \pmod 4.$$

Yet, this is impossible if $p \equiv 3 \pmod 4$, as all squares are congruent to 0 or 1 modulo 4. For the converse, let $p \in \mathbb{Z}_{\geq 0}$ be a prime with

$$p \equiv 1 \pmod 4,$$

and let $p = 4n + 1$ for $n \in \mathbb{Z}$. Let

$$a = (2n)! = \left(\frac{p-1}{2}\right)!.$$

Then,

$$a^2 = ((2n)!)^2(-1)^{2n},$$

which we can simply write as

$$\begin{aligned} &(1 \cdot 2 \cdot \cdots \cdot 2n)((-2n)(-2n+1) \cdot \cdots \cdot (-2) \cdot (-1)) \\ \equiv\ &(1 \cdot 2 \cdot \cdots \cdot 2n)((2n+1) \cdot \cdots \cdot (4n-1) \cdot (4n)) \pmod p \\ =\ &(p-1)! \equiv 1 \pmod p. \end{aligned}$$

The final step is achieved from Wilson's Theorem. Thus, $p \mid a^2 + 1$ in $\mathbb{Z}$. If p is irreducible in $\mathbb{Z}[i]$, then p is prime, as $\mathbb{Z}[i]$ is a PID. Since

$$a^2 + 1 = (a + i)(a - i),$$

we must have $p \mid a + i$ or $p \mid a - i$. However, this is impossible since

$$p(c + di) = pc + pdi.$$

Therefore, p is reducible in $\mathbb{Z}[i]$, so by the lemma, p has the desired form. □

Polynomial Rings 2

2.1 Factorization in Polynomial Rings

Definition 2.1.1 (Multivariate Polynomial Ring) *Recall that the multivariate polynomial ring*[1] $R[x_1, \ldots, x_n]$ *is defined inductively by*

$$R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n].$$

1: Note that $R[x, y] = R[y, x]$.

It is important to distinguish between the adjoining of a transcendental or variable x to a ring R is wildly different from adjoining an element which is related to the ring.[2]

2: For instance, $\mathbb{Z}[x]$ and $\mathbb{Z}[\sqrt{-5}]$, as the latter can have the adjoined element squared to enter the ring.

We would like to find a precise answer to the question: When is $R[x]$ a UFD? Though we cannot give a complete answer right now, we can give some partial answers:

(a) If $\mathbb{F}$ is a field, then $\mathbb{F}[x]$ is a Euclidean domain with the norm given by
$$N : p(x) \mapsto \deg p.$$
meaning $\mathbb{F}[x]$ is a UFD.

(b) If R is not a field, then $R[x]$ is not a PID.[3]

Proof I. (r, x) is not principal if we have the element $r \notin R^\times$. □

Proof II. (x) is prime, but not maximal, since $R[x]/\langle x \rangle \cong R$ is not a field. □

3: This does not actually give us information on whether or not the structure is a UFD, as there are UFDs that are not PIDs.

(c) If $R[x]$ is a UFD, then R is a UFD.

Proof. With $R \subseteq R[x]$ due to constant polynomials, and $p(x)q(x) \in R$, then $p(x), q(x) \in R$. □

Now, we give the complete answer.

Theorem 2.1.1 $R[x]$ *is a UFD, if and only if* R *is a UFD.*[4]

4: This will be restated and proven later in the chapter. The idea of the proof is to seek a way to factor the polynomials over a field $\mathbb{F}$ and show that the factors can be chosen in $R[x]$.

For instance, factoring $x^2 + x - 2 \in \mathbb{Z}[x]$ yields $(2x - 2)(x/2 + 1) \in \mathbb{Q}[x]$, which we can see yields $(x - 1)(x + 2) \in \mathbb{Z}[x]$.

Definition 2.1.2 (Field of Fractions) *Given an integral domain* R*, the field of fractions,*[5] *or quotient field, of* R *is defined to be*

$$\mathbb{F} := \left\{ \frac{a}{b} : a, b \in R \quad \textit{with} \quad b \neq 0 \right\},$$

where

$$\frac{a}{b} = \frac{c}{d}$$

if and only if $ad = bc$.

5: It is important here to consider $R \subseteq \mathbb{F}$ where
$$R = \left\{ \frac{a}{1} : a \in R \right\} \subseteq \mathbb{F}.$$

Theorem 2.1.2 (Gauß's Lemma) *Let R be a UFD with field of fractions $\mathbb{F}$. If $p(x) \in R[x]$ is reducible in $\mathbb{F}[x]$, it is reducible in $R[x]$.*

More precisely, if $p(x) \in R[x]$ as

$$p = AB$$

for non-constant $A, B \in \mathbb{F}[x]$, then there exists an $f \in \mathbb{F}$ such that $a := fA$ and $b := f^{-1}B$ are in $R[x]$.[6]

6: Note that $p = ab$.

Proof. Choose $r, s \in R$ such that

$$\tilde{a}(x) := rA(x) \quad \text{and} \quad \tilde{b}(x) := sB(x) \in R[x].$$

Then,

$$dp(x) = \tilde{a}(x)\tilde{b}(x)$$

where $d = rs$. If $d \in R^\times$, we are done, since we then have $r, s \in R^\times$, so

$$A = r^{-1}\tilde{a} \quad \text{and} \quad B = s^{-1}\tilde{b} \in R[x].$$

If $d \notin R^\times$, take a factorization

$$d = \underbrace{q_1 \cdot \cdots \cdot q_n}_{\text{irreducibles/primes}}.$$

Let $\overline{R} := R/\langle q_1 \rangle$. Then, $\overline{R}[x] := R[x]/\langle q_1 \rangle$ is an integral domain since we are quotienting by a prime ideal. In $\overline{R}[x] \cong R[x]/\langle q_1 \rangle$,

$$O = \overline{d}\,\overline{p}(x) = \overline{\tilde{a}}(x)\overline{\tilde{b}},$$

so $\overline{\tilde{a}}$ or $\overline{\tilde{b}} = 0$. Without loss of generality, let it be the former. Then,

$$\tilde{a}(x) = q_1 \hat{a}(x)$$

for some $\hat{a} \in R[x]$. Additionally,

$$q_2 \cdot \cdots \cdot q_n\, p(x) = \hat{a}(x)\tilde{b}(x)$$

Perform induction on n, proving the result.[7]

□

7: We construct f by

$$f := \frac{r}{\prod_i q_i},$$

where i is such that $q_i \mid \tilde{a}(x)$. The inverse is then

$$f^{-1} = \frac{s}{\prod_j q_j},$$

where j is such that $q_j \nmid \tilde{a}(x)$.

Remark 2.1.1 Note that the converse of Gauß's lemma is false for "silly" reasons. Consider $2x = 2 \cdot x$, which is reducible in $\mathbb{Z}[x]$. Yet, $2x$ is irreducible in $\mathbb{Q}[x]$, since 2 is a unit.

Corollary 2.1.3 *Let R be a UFD with a field of fractions $\mathbb{F}$. Let*

$$p(x) := a_0 + a_1 x + \cdots + a_n x^n \in R[x].$$

If

$$\gcd(a_0, a_1, \ldots, a_n) = 1,$$

then p is irreducible in $R[x]$, if and only if it is irreducible in $\mathbb{F}[x]$.

Proof. The forward direction is given by Gauß's lemma. For the converse, the only possible nontrivial factorization in $R[x]$ that is trivial in $\mathbb{F}[x]$ is

$$p(x) = cq(x),$$

where the ring element $c \notin R^\times$ and $q(x) \in R[x]$. If $q(x) \in R[x]$, we must have

$$c \mid a_0, a_1, \ldots, a_n.$$

Thus, c is a common factor. However, we said the gcd of the coefficients is 1, meaning c is a unit, yielding a contradiction.

□

An important case of this corollary is monic polynomials. If $p(x)$ is monic,[8] then p is irreducible in $R[x]$ if and only if p is irreducible in $\mathbb{F}[x]$.

8: This means the top coefficient is 1.

2.2 $R[x]$ Irreducibility Criteria

Now, we prove the reverse direction of our UFD theorem.

Theorem 2.2.1 *A polynomial ring $R[x]$ is a UFD if and only if R is a UFD.*

Proof. Let R be a UFD with a field of fractions $\mathbb{F}$. Let $p(x) \in R[x]$ be non-constant. Assume, for convenience, that the

$$\gcd(\text{coefficients of } p) = 1.$$

Otherwise, we can factor out this gcd, which has unique factorization since it is an element of R. First, we want to show existence. Since $\mathbb{F}[x]$ is a Euclidean domain,[9] it is a UFD, so $p(x)$ factors into irreducibles in $\mathbb{F}[x]$. By Gauß's Lemma, we can take these factors to be over $R[x]$:

$$p(x) = q_1(x) \cdots q_n(x),$$

where $q_i(x) \in R[x]$ are non-constant and irreducible in $\mathbb{F}[x]$. Since the

$$\gcd(\text{coefficients of } p) = 1,$$

we have that

$$\gcd(\text{coefficients of } q_i) = 1$$

for all i.[10] As such, by Gauß's Lemma, q_i is irreducible in $R[x]$ for all i, and the above factorization is the desired factorization into irreducibles in $R[x]$. Now, for uniqueness, let

$$p = q_1 \cdots q_n = q_1' \cdots q_m'$$

be two irreducible factorizations of $p(x) \in R[x]$. Then, these are also irreducible factorizations in $\mathbb{F}[x]$ by Gauß's Lemma. Since $\mathbb{F}[x]$ is a UFD,

9: We set the Euclidean norm to be

$$N(p(x)) = \deg p.$$

10: We have this from the fact that the gcds multiply.

we now have that $m = n$, and after reordering if necessary, q_i and q_i' are associates over $\mathbb{F}$. That is,

$$q_i = \frac{a_i}{b_i} q_i'$$

for some $a_i, b_i \in R$. We want to show that these must then be associates over R. Clearing denominators yields $b_i q_i = a_i q_i' \in R[x]$ Now, notice that

$$\gcd(\text{coefficients of } b_i q_i) = b_i \gcd(\text{coefficients of } q_i) = b_i.$$

Similarly, we have

$$\gcd(\text{coefficients of } a_i q_i') = a_i \gcd(\text{coefficients of } q_i') = a_i.$$

Therefore, a_i and b_i are associates in $R[x]$.[11] Thus, q_i and q_i' are associates in $R[x]$, meaning the factorization is unique. □

11: In other words, we have

$$\frac{a_i}{b_i} \in R^\times.$$

Corollary 2.2.2 *A multivariate polynomial ring $R[x_1, \dots, x_n]$ is a UFD if and only if R is a UFD.*[12]

12: We just proceed by iterating the previous theorem.

Now, as the upshot of all this, we can mostly consider factorization over a field $\mathbb{F}$. We would now like to test when a $p(x) \in \mathbb{F}[x]$ is irreducible. The following results provide a series of criteria for irreducibility.

Proposition 2.2.3 *If $\deg p \leq 3$, then p is reducible in $\mathbb{F}[x]$ if and only if p has a root in $\mathbb{F}$.*

Proof. Begin with the forward direction. If p is irreducible, then one factor is linear: $ax + b$, so $-b/a$ is a root. For the converse, let $c \in \mathbb{F}$ be a root. Since $\mathbb{F}[x]$ is Euclidean, we divide p by $x - c$ to get

$$p(x) = q(x)(x - c) + \underbrace{r}_{\in \mathbb{F}}.$$

We get the remainder as a constant from the fact that

$$N(r) < N(x - c) = 1.$$

Therefore,$0 = p(c) = \underbrace{q(c)(c - c)}_{=0} + r = r$, so $r = 0$, and p is reducible.[13]

13: Note that the converse works even in a higher degree.

□

Theorem 2.2.4 (Rational Root Theorem) *Let*

$$p(x) := a_n x^n + \cdots + a_1 x + a_0 \in R[x],$$

where R is a UFD. Let $r/s \in \mathbb{F}[x]$ be a root of p in lowest terms.[14] *Then, $r \mid a_0$ and $s \mid a_n$.*

14: By lowest terms we mean

$$\gcd(r, s) = 1$$

in R.

Proof. Note that

$$0 = p\left(\frac{r}{s}\right) = a_n \left(\frac{r}{s}\right)^n + \cdots + a_1 \left(\frac{r}{s}\right) + a_0,$$

so

$$a_n r^n = -s\left(a_{n-1} r^{n-1} + \cdots + a_n s^{n-1}\right).$$

Since we assumed $\gcd(r, s) = 1$, we need $s \mid a_n$ in R. Solving for $a_0 s^n$ shows that $r \mid a_0$. □

Corollary 2.2.5 *If $p(x) \in R[x]$ is monic, then p has a root in R if and only if p has a root in $\mathbb{F}$.*[15]

15: This follows directly from the criterion, realizing that $s = 1$ yields $r/1 \in R[x]$.

Example 2.2.1 Consider

$$p(x) := x^3 - 3x - 1 \in \mathbb{Q}[x].$$

We have that

$$p(1) = -3 \neq 0 \quad \text{and} \quad p(-1) = 1 \neq 0,$$

so by the Rational Root Theorem, p has no roots in $\mathbb{Q}$ at all. Since $\deg p = 3$, it is irreducible over $\mathbb{Q}$, and thus over $\mathbb{Z}$.[16]

16: The latter comes from directly Gauß's Lemma.

Proposition 2.2.6 *Let R be a ring with an ideal $I \subset R$. Let $p(x) \in R[x]$ be a non-constant, monic polynomial. If $\overline{p}(x)$ is irreducible*[17] *in ${}^{R}/_{I}[x]$, then $p(x)$ is irreducible over R.*

17: Remember, here we are looking at the coset $p(x) + I$.

Proof. If p is reducible over R, then we write $p = ab$ for $a, b \in R$. Then, $\overline{p} = \overline{a}\overline{b}$, and if p and thus $\overline{p}$ are monic, this is a nontrivial factorization. □

Example 2.2.2 Let

$$p(x) := x^3 - 3x - 1 \in \mathbb{Z}[x].$$

Then,

$$\overline{p}(x) = x^2 + x + 1 \in {}^{\mathbb{Z}}/_{2\mathbb{Z}}[x],$$

so

$$\overline{p}(0) = 1 \neq 0 \neq 1 = \overline{p}(1).$$

Thus, $\overline{p}$ has no roots, so $\overline{p}$ is irreducible in ${}^{\mathbb{Z}}/_{2\mathbb{Z}}[x]$, hence p is irreducible in $\mathbb{Z}[x]$.[18]

18: Note that the converse does not hold. In fact, even a weaker version of the converse is false:

$$x^4 - 72x^2 + 4$$

is reducible in ${}^{\mathbb{Z}}/_{n\mathbb{Z}}[x]$ for *every* n, but irreducible in $\mathbb{Z}[x]$.

Theorem 2.2.7 (Eisenstein's Criterion) *Let*

$$a(x) := x^n + a_{n-1} x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x].$$

If $p \in \mathbb{Z}$ is a prime such that $p \mid a_i$ and $p^2 \nmid a_0$, then $a(x)$ is irreducible in $\mathbb{Z}[x]$ and thus, in $\mathbb{Q}[x]$.

On the Theories of Fields and Galois

Fields 3

3.1 Fields and Characteristic

Definition 3.1.1 (Field) *Recall that a field is a commutative ring with* $1 \in \mathbb{F}$ *in which every nonzero element is in* $\mathbb{F}^\times$.

Example 3.1.1 Our standard examples of fields include

$$\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p \cong \mathbb{Z}/p\mathbb{Z}, \text{ and } \mathbb{F}_{p^n}.$$

Example 3.1.2 (Rational Polynomial Field) We also have the field $\mathbb{Q}(x)$ defined as

$$\mathbb{Q}(x) := \left\{ \frac{p(x)}{q(x)} : p, q \in \mathbb{Q}[x] \right\},$$

the field of fractions of $\mathbb{Q}[x]$.

Example 3.1.3 (Formal Laurent Power Series) We can also have

$$\mathbb{Q}((t)) := \left\{ a_n t^n + a_{n+1} t^{n+1} + \cdots : n \in \mathbb{Z} \right\}$$

Example 3.1.4 (Gaussian Rationals) We have $\mathbb{Q}(i)$ as a field.

Example 3.1.5 (Adjoin nth Root of Unity) We can have the field $\mathbb{Q}(\zeta_n)$.[1]

Example 3.1.6 (Adjoin $\sqrt{D}$) We can have the field $\mathbb{Q}(\sqrt{D})$.[2]

Definition 3.1.2 (Field Chracteristic) *The characteristic of a field, denoted* $\operatorname{char} \mathbb{F}$*, is the smallest* $n > 0$ *such that*

$$n \cdot 1 = \underbrace{1 + 1 + \cdots + 1}_{n \text{ summands}} = 0 \in \mathbb{F},$$

or $\operatorname{char} \mathbb{F} = 0$ *if no such n exists.*

Example 3.1.7 Note that

$$\operatorname{char} \mathbb{C} = \operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{Q}(\zeta_n) = 0$$

and

$$\operatorname{char} \mathbb{F}_p = \operatorname{char} \mathbb{F}_p(x) = \operatorname{char} \mathbb{F}_p((x)) = p.$$

1: We will study such "cyclotomic" extensions after building some theory.

2: Adjoining the square root of the discriminant of a polynomial is vital to our study of polynomial solvability.

Proposition 3.1.1 *Let $\mathbb{F}$ have characteristic n. Then,*

(a) n is either 0 or prime.
(b) If $\alpha \in \mathbb{F}$,

$$n\alpha = \underbrace{\alpha + \alpha + \cdots + \alpha}_{n \text{ summands}} = 0.$$

Proof.

(a) If $n = ab \neq 0$, where $a, b \neq \pm 1$, then

$$(a \cdot 1)(b \cdot 1) = \underbrace{(1 + \cdots + 1)}_{a}\ \underbrace{(1 + \cdots_1)}_{b} = \underbrace{(1 + 1 \cdots + 1)}_{ab},$$

so one of the factors is 0, contradicting minimality of n.

(b)

$$\underbrace{\alpha + \alpha + \cdots \alpha}_{n} = \alpha(1 + \cdots + 1) = \alpha(0) = 0.$$

□

Definition 3.1.3 *A prime subfield is the subfield of $\mathbb{F}$ generated by $1_{\mathbb{F}}$.*[3]

3: Note that this is preciesely the smallest subfield of $\mathbb{F}$ containing 1.

Remark 3.1.1 The prime subfield $\mathbb{K}$ of $\mathbb{F}$ is always isomorphic to

$$\mathbb{K} \cong \begin{cases} \mathbb{Q}, & \text{if } \operatorname{char} \mathbb{F} = 0 \\ \mathbb{F}_p, & \text{if } \operatorname{char} \mathbb{F} = p. \end{cases}$$

Definition 3.1.4 (Field Extension) *If $\mathbb{K}$ and $\mathbb{F}$ are fields with $\mathbb{F} \subseteq \mathbb{K}$, the pair $\mathbb{K}/\mathbb{F}$ is called a field extension.*[4]

4: Note that this is not a quotient, which is why we have used a distinct notation for quotients thus far.

We write $\mathbb{F}$ to be the *base field*, $\mathbb{K}$ to be the *extension field*. We also write the extension as the diagram

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

3.2 Vector Spaces and Extensions

Definition 3.2.1 (Vector Space) *A vector, or linear, space over an arbitrary field $\mathbb{F}$ is a non-empty set $\mathcal{V}$ equipped with two binary functions, addition $+ : \mathcal{V} \times \mathcal{V} \to \mathcal{V}$ and scalar multiplication $\cdot : \mathbb{F} \times \mathcal{V} \to \mathcal{V}$, satisfying the following eight axioms, alongside two closure axioms.*[5]

(C 1) $(\forall x, y \in \mathcal{V})[(x + y) \in \mathcal{V}]$
(VS 1) $(\forall x, y \in \mathcal{V})[x + y = y + x]$
(VS 2) $(\forall x, y, z \in \mathcal{V})[(x + y) + z = x + (y + z)]$
(VS 3) $(\forall x \in \mathcal{V})(\exists 0 \in \mathcal{V})[x + 0 = x]$
(VS 4) $(\forall x \in \mathcal{V})(\exists y \in \mathcal{V})[x + y = 0]$
and
(C 2) $(\forall a \in \mathbb{F})(\forall x \in \mathcal{V})[(ax) \in \mathcal{V}]$
(VS 5) $(\forall x \in \mathcal{V})[1x = x]$
(VS 6) $(\forall a, b \in \mathbb{F})(\forall x \in \mathcal{V})[(ab)x = a(bx)]$
(VS 7) $(\forall a \in \mathbb{F})(\forall x, y \in \mathcal{V})[a(x + y) = ax + ay]$
(VS 8) $(\forall a, b \in \mathbb{F})(\forall x \in \mathcal{V})[(a + b)x = ax + bx]$

5: That is, it is an abelian group with a compatible linear action from a field of scalars.

Definition 3.2.2 (Basis) *A basis of a linear space $\mathcal{V}$ over $\mathbb{F}$ is a set $S \subseteq \mathcal{V}$ which is both linearly independent and spanning.*[6]

6: That is,

(i) Every $v \in \mathcal{V}$ can be written

$$v = \sum_{i=1}^{n} a_i s_i .$$

with $a_i \in \mathbb{F}$ and $s_i \in S$.

(ii) If

$$\sum_{i=1}^{n} a_i s_i = 0,$$

then

$$a_1 = \cdots = a_n = 0$$

with $a_i \in \mathbb{F}$ and $s_i \in S$.

Definition 3.2.3 (Dimension) *The dimension of a vector space $\mathcal{V}$ over $\mathbb{F}$ is the cardinality of the basis*[7]

$$\dim_{\mathbb{F}} \mathcal{V} := |S|.$$

7: Note that we can say *the basis*, as all bases necessarily have the same size.

Proposition 3.2.1 (Extension Linearity) *An extension field $\mathbb{K}$ of $\mathbb{F}$ is a vector space over $\mathbb{F}$.*

Proof. Checking the axioms is left as an exercise. It is trivial. □

Definition 3.2.4 (Degree) *The degree, denoted $[\mathbb{K} : \mathbb{F}]$ is defined as*

$$[\mathbb{K} : \mathbb{F}] := \dim_{\mathbb{F}} \mathbb{K}.$$

Example 3.2.1 Some examples of extensions include

(a) $\mathbb{C}/\mathbb{R}$ yields a basis of $S = \{1, i\}$. Thus, $[\mathbb{C} : \mathbb{R}] = 2$.
(b) $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ yields a basis of $S = \{1, \sqrt{2}\}$. Thus, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$.
(c) $\mathbb{F}_p(x)/\mathbb{F}_p$ yields an extension of degree $[\mathbb{F}_p(x) : \mathbb{F}_p] = \infty$.

Our goal is to form field extensions by adding the root of certain polynomials. Let $\mathbb{F}$ be a field with a polynomial $p(x) \in \mathbb{F}[x]$ which is irreducible and non-constant. It turns out, the extension field which includes the root is

$$\mathbb{K} := {}^{\mathbb{F}[x]}/_{\langle p \rangle}.$$

Proposition 3.2.2 $\mathbb{K}$, *as above, is a field.*

Proof. We have that $p(x)$ being irreducible implies $p(x)$ is prime.[8] Thus, $\langle p(x)\rangle$ is a prime ideal, which means it is maximal.[9] Thus, $\mathbb{K}$ is a field. □

8: This is since $\mathbb{F}[x]$ is a PID.

9: Once again, we have this from $\mathbb{F}[x]$ being a PID.

Theorem 3.2.3 *Let* $\mathbb{K}$ *be an extension field of* $\mathbb{F}$ *containing a root* θ *of* p*. If* $\deg p = n$*, then*

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

is a basis for $\mathbb{K}/\mathbb{F}$*, so* $[\mathbb{K} : \mathbb{F}] = n$*.*

Proof. We need to show that an isomorphic copy of $\mathbb{F}$ is contained as a subfield $\mathbb{F} \subset \mathbb{K}$. We have[10]

$$\mathbb{F} \hookrightarrow \mathbb{F}[x] \twoheadrightarrow {}^{\mathbb{F}[x]}/_{\langle p\rangle}$$

10: The hooked arrow means an inclusion, and the two-headed arrow means a projection.

and the composition of these maps is an injection, so $\mathbb{F} \subseteq \mathbb{K}$. Let

$$\theta := x + \langle p(x)\rangle \in {}^{\mathbb{F}[x]}/_{\langle p\rangle} = \mathbb{K}.$$

Then,

$$p(\theta) = p(x + \langle p(x)\rangle = p(x) + \langle p(x)\rangle = 0 + \langle p(x)\rangle\,,)$$

which is $0_{\mathbb{K}}$. Now, for the basis, let $a(x) \in \mathbb{F}[x]$. Since $\mathbb{F}[x]$ is a Euclidean domain, we have

$$a(x) = q(x)p(x) + r(x)$$

with $\deg r < n$. Thus,

$$a(x) + \langle p(x)\rangle = r(x) + \langle p(x)\rangle \in \mathbb{K},$$

meaning $\mathbb{K}$ is spanned by

$$S := \{1, \theta, \ldots, \theta^{n-1}\}.$$

For linear independence, if S is linearly independent, then there exist $b_0, \ldots, b_{n-1} \in \mathbb{F}$ where not all are zero such that

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

Therefore,

$$b_0 + b_1 x + \cdots + b_{n-1}x^{n-1} + \langle p(x)\rangle = 0 + \langle p(x)\rangle$$

in $\mathbb{K}$, so

$$b_0 + b_1 + \cdots + b_{n-1}x^{n-1}$$

is a multiple of $p(x)$ in $\mathbb{F}[x]$. However, this is impossible, since

$$\deg p = n > n - 1.$$

□

Remark 3.2.1 Note that we *need* p to be irreducible, otherwise $\mathbb{K}$ is not a field.

Now, we have a trick to reduce polynomials modulo $p(x)$. Given

$$\begin{aligned} p(x) &= x^n + p_{n-1}x^{n-1} + \cdots + p_1 x + p_0 \\ p(\theta) &= 0, \end{aligned}$$

so

$$\begin{aligned} \theta^n &= -\left(p_{n-1}\theta^{n-1} + \cdots + p_1\theta + p_0\right) \\ \theta^{n+1} &= \theta\theta^n = -\left(p_{n-1}\theta^n + \cdots + p_1\theta^2 + p_0\theta\right) \\ &= -(p_{n-1}(-\left(p_{n-1}\theta^{n-1} + \cdots + p_1\theta + p_0\right) + p_{n-1}\theta^{n-1} \\ &\quad + \cdots + p_0\theta)) \text{ etcetera.} \end{aligned}$$

Example 3.2.2 Let $\mathbb{F} := \mathbb{R}$, with $p(x) := x^2 + 1$. Then,

$$\mathbb{K} := {}^{\mathbb{R}[x]}/_{\langle x^2+1\rangle} = \{a + b\theta : a, b \in \mathbb{R}\},$$

the $\mathbb{R}$-linear combinations of 1 and θ. Of course, $\theta^2 = -1$, as $\theta^2 + 1 = 0$. Then,

$$(a + b\theta)(c + d\theta) = (ac - bd) + (ad - bc)\theta,$$

so there exist two isomorphisms of $\mathbb{K} \cong \mathbb{C}$

$$\theta \mapsto \pm i.$$

Now, we will try to relate our new construction with a more "intuitive" way of thinking about field extensions.

Definition 3.2.5 (Alternative Field Extension) *Let* $\mathbb{F} \subseteq \mathbb{K}$ *with*

$$\alpha, \beta, \cdots \in \mathbb{K}.$$

Then, $\mathbb{F}(\alpha, \beta, \dots)$ *is the smallest subfield of* $\mathbb{K}$ *containing* $\mathbb{F}$ *and* $\alpha, \beta, \dots$.[11]

11: Equivalently, $\mathbb{F}(\alpha, \beta, \dots)$ is the inetersection of all subfields of $\mathbb{K}$ with this property.

Definition 3.2.6 (Simple Extension) *A simple extension* $\mathbb{E}$ *is of the form*

$$\mathbb{E} := \mathbb{F}(\alpha),$$

where α *is called a primitive element.*

Example 3.2.3 We have,[12] non-trivially, that

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\underbrace{\sqrt{2} + \sqrt{3}}_{\alpha})$$

is simple.

12: As a non-example, note that

$$\mathbb{Q}(\sqrt{2}, \sqrt[4]{2}, \sqrt[8]{2}, \dots)$$

is not simple.

Theorem 3.2.4 *Let $p(x) \in \mathbb{F}[x]$ with p irreducible. Then, let $\mathbb{K}$ be an extension field of $\mathbb{F}$ which contains a root α of p. Then,*

$$\mathbb{F}[x]/\langle p \rangle \cong \mathbb{F}(\alpha) \subseteq \mathbb{K}.$$

Proof. Consider the map given by

$$x + \langle p \rangle \xmapsto{\varphi} \alpha$$

That is,

$$g(x) + \langle p(x) \rangle \xmapsto{\varphi} g(\alpha)$$

For showing it is well-defined, note that if $g \in \langle p \rangle$, then $g(\alpha) = 0$, so $g \mapsto 0$.[13] For seeing that the homomorphism forms an injection, notice that $\ker \varphi$ is an ideal, which for a field is either $\langle 0 \rangle$ or $\mathbb{F}[x]/\langle p \rangle$. It cannot be the latter, since we have $x + \langle p \rangle \mapsto \alpha$. Finally, for surjectivity, note that $\mathcal{R}(\varphi)$ is a field containing both $\mathbb{F}$ and α, so it must be $\mathbb{F}(\alpha)$.

13: We leave out the proof of the map being a ring homomorphism, as it is just a matter of checking the axioms.

□

Corollary 3.2.5 *Let*

$$\mathbb{E} := \mathbb{F}(\alpha) \subseteq \mathbb{K},$$

such that $[\mathbb{E} : \mathbb{F}] = n < \infty$.[14] *Then,*

(i) there exists an irreducible polynomial $p(x) \in \mathbb{F}[x]$ such that $p(\alpha) = 0$.
(ii) $\deg p = n$.
(iii) $\mathbb{E} \cong \mathbb{F}[x]/\langle p \rangle$.
(iv) $\mathbb{E}$ is independent of the choice of the root of p.[15]

14: We call an object like this a *finite extension*.

15: That is, if $p(\beta) = 0$, then $\mathbb{F}(\alpha) \cong \mathbb{F}(\beta)$.

Proof.

(i) Since $[\mathbb{E} : \mathbb{F}] = n$, all

$$1, \alpha, \ldots, \alpha^n$$

are all linearly dependent. That is, there exists $\{a_i\}_{i=0}^n \subseteq \mathbb{F}$ where not every $a_i = 0$ such that

$$\sum_{i=0}^{n} a_i \alpha^i = 0.$$

Let $p(x)$ be an irreducible factor of

$$\sum_{i=0}^{n} a_i x^i \in \mathbb{F}[x],$$

such that $p(\alpha) = 0$.[16]

(ii) This part follows from earlier material.
(iii) This part follows from Theorem 3.2.4.
(iv) This part follows from part (c).

16: This is guaranteed since the α^i are linearly dependent.

□

On the other hand, if $[\mathbb{F}(\alpha) : \mathbb{F}] = \infty$, then

$$\mathbb{F}(\alpha) \cong \mathbb{F}(x),$$

with

$$\frac{p(\alpha)}{q(\alpha)} \mapsto \frac{p(x)}{q(x)}.$$

For instance, letting $\mathbb{F} := \mathbb{Q}$, then[17]

$$\underbrace{\alpha = \pi, e, \ln 2}_{\text{difficult to show}}.$$

17: For the most part, such *infinite extensions* are not in the scope of this course, as these objects can become a sprawling mess. The main idea, is that none of the possible α have any sort of polynomial relation.

3.3 Algebraic Extensions

Theorem 3.3.1 *To sum up, defining $\mathbb{K} := \mathbb{F}(\alpha)$[18] yields that*

(i) if $[\mathbb{K} : \mathbb{F}] < \infty$, then there exists a $p(x) \in \mathbb{F}[x]$ with p irreducible such that $p(\alpha) = 0$ and

$$\mathbb{K} \cong {}^{\mathbb{F}[x]}\!/_{\langle p \rangle}.$$

(ii) if $[\mathbb{K} : \mathbb{F}] = \infty$, then $\mathbb{K} \cong \mathbb{F}(x)$ and for all $p(x) \in \mathbb{F}[x]$, $p(\alpha) \neq 0$.

18: This is contained in some larger field.

Thus, we can define our scope of study based on these cases.

Definition 3.3.1 (Algebraic and Transcendental Elements)

(i) In case (i), we call α and $\mathbb{K}/\mathbb{F}$ algebraic.
(ii) In case (ii). we call α and $\mathbb{K}/\mathbb{F}$ transcendental.

Proposition 3.3.2 *If α is algebraic over $\mathbb{F}$, then there exists a unique monic polynomial*[19]

$$m_{\alpha,\mathbb{F}}(x) \in \mathbb{F}[x]$$

of minimal degree such that

$$m_{\alpha,\mathbb{F}}(\alpha) = 0.$$

Furthermore,

$$\deg m_{\alpha,\mathbb{F}} = [\mathbb{F}(\alpha) : \mathbb{F}],$$

and $\mathbb{F}[x] \ni p(\alpha) = 0$ if and only if

$$p \in \langle m_{\alpha,\mathbb{F}}(x) \rangle.$$

19: We call this polynomial the *minimal polynomial of α over $\mathbb{F}$*.

Proof. Define the ideal

$$I := \{p(x) \in \mathbb{F}[x] : p(\alpha) = 0\}.$$

Since $\mathbb{F}[x]$ is a PID, and $I \neq \langle 0 \rangle$, let $m_{\alpha,\mathbb{F}}(x)$ be a monic generator for the ideal I. Since I must be prime,[20] p must be irreducible. Now, we have, by Theorem 3.2.4, that

$$\mathbb{F}(\alpha) \cong {}^{\mathbb{F}[x]}\!/_{\langle m_{\alpha,\mathbb{F}} \rangle},$$

20: This comes from the fact that if it was not prime, there would exists a product of polynomials which form I without being in I themselves. However, this is impossible, as this is an integral domain, lacking zero divisors.

so

$$[\mathbb{F}(\alpha) : \mathbb{F}] = \deg m_{\alpha,\mathbb{F}}.$$

□

Example 3.3.1 For instance, let $\mathbb{F} := \mathbb{Q}$ with $\alpha = \sqrt{2}$. Then,

$$m_{\alpha,\mathbb{F}}(x) = x^2 - 2.$$

Now, since there exists

$$\mathbb{Q}[x] \ni p(\sqrt{2}) = 0,$$

we must have

$$x^2 - 2 \mid p(x) \in \mathbb{Q}[x].$$

Proposition 3.3.3 *If α is algebraic over $\mathbb{F}$ and $\mathbb{F} \subseteq \mathbb{L}$,*[21] *then α is algebraic over $\mathbb{L}$ and*

$$m_{\alpha,\mathbb{L}}(x) \mid m_{\alpha,\mathbb{F}}(x)$$

in $\mathbb{L}[x]$.

21: We let $\mathbb{L}$ be a field.

Example 3.3.2 For instance, if we have

$$\mathbb{F} := \mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) =: \mathbb{L}$$

with $\alpha = \sqrt{2}$, then taking

$$m_{\alpha,\mathbb{F}}(x) = x^2 - 2$$

and

$$m_{\alpha,\mathbb{L}}(x) = x - \sqrt{2}.$$

Thus,

$$x - \sqrt{2} \mid x^2 - 2 \in \mathbb{L}[x],$$

as

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2}).$$

Theorem 3.3.4 (Extension Theorem) *Let*

$$\varphi : \mathbb{F} \xrightarrow{\sim} \mathbb{F}'$$

be a field isomorphism. Additionally, let $p(x) \in \mathbb{F}[x]$ *be irreducible and* $p'(x) \in \mathbb{F}'[x]$ *be the irreducible polynomial obtained by applying* φ *to the coefficients of* p.

Now, let α *be a root of* p *in some extension of* $\mathbb{F}$, *and let* β *be a root of* p' *in some extension of* $\mathbb{F}'$. *Then, there exists an isomorphism (Figure 4.1)*

$$\sigma : \mathbb{F}(\alpha) \xrightarrow{\sim} \mathbb{F}'(\beta).$$

Proof. Let $\tilde{\varphi}$ be the isomorphism

$$\begin{array}{ccc} \mathbb{F}[x] & \xrightarrow[\tilde{\varphi}]{\sim} & \mathbb{F}'[x] \\ f & \longmapsto & \varphi(f) \\ x & \longmapsto & x \end{array}$$

Then, $\tilde{\varphi}$ maps $\langle p(x) \rangle$ to $\langle p'(x) \rangle$, so it induces an isomorphism

$$\begin{array}{ccc} \mathbb{F}[x]/\langle p \rangle & \xrightarrow{\sim} & \mathbb{F}'[x]/\langle p' \rangle \\ f & \longmapsto & \varphi(f) + \langle p' \rangle \\ x + \langle p \rangle & \longmapsto & x + \langle p' \rangle \end{array}$$

Combining this diagram with our previous isomorphisms gives σ to be the composite mapping

$$\begin{array}{ccccccc} \mathbb{F}(\alpha) & \xrightarrow{\sim} & \mathbb{F}[x]/\langle p \rangle & \xrightarrow{\sim} & \mathbb{F}'[x]/\langle p' \rangle & \xrightarrow{\sim} & \mathbb{F}'(\beta) \\ f & \xmapsto{\sim} & f + \langle p \rangle & \mapsto & \varphi(f) + \langle p' \rangle & \mapsto & \varphi(f) \\ \alpha & \longmapsto & x + \langle p \rangle & \longmapsto & x + \langle p' \rangle & \longmapsto & \beta \end{array}$$

$\square$

Note that we have the below square demonstrating the extension relationship within the isomorphisms.

$$\begin{array}{ccc} \mathbb{F}(\alpha) & \xrightarrow[\sigma]{\sim} & \mathbb{F}'(\beta) \\ f & \longmapsto & \varphi(f) \\ \alpha & \longmapsto & \beta \end{array}$$

Figure 3.1: Mapping diagram for the isomorphism σ in Theorem 3.3.4. Note that $\sigma|_{\mathbb{F}} = \varphi$.

$$\begin{array}{ccc} \mathbb{F}(\alpha) & \xrightarrow[\sigma]{\sim} & \mathbb{F}'(\beta) \\ \big| & & \big| \\ \mathbb{F} & \xrightarrow[\varphi]{\sim} & \mathbb{F}' \end{array}$$

Definition 3.3.2 (Algebraic Extension) *A field extension $\mathbb{K}/\mathbb{F}$ is algebraic if every $\alpha \in \mathbb{K}$ is algebraic over $\mathbb{F}$.*

Example 3.3.3 Let $\mathbb{K} := \mathbb{Q}(\sqrt{2})$ and $\mathbb{F} := \mathbb{Q}$. Then

$$\alpha = a + b\sqrt{2}.$$

To know that this is algebraic, we need to know that there exists a

$$p(x) \in \mathbb{Q}[x]$$

for all $a, b \in \mathbb{Q}$, such that

$$p(a + b\sqrt{2}) = 0.$$

Proposition 3.3.5 *If $[\mathbb{K} : \mathbb{F}] < \infty$, then $\mathbb{K}/\mathbb{F}$ is algebraic.*[22]

22: Note that the converse is false. For instance, consider

$$\mathbb{K} := \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}, \sqrt[4]{2}, \dots).$$

Then, $\mathbb{K}$ is algebraic over $\mathbb{Q}$, but $[\mathbb{K} : \mathbb{Q}] = \infty$, since $x^n - 2$ is the minimal polynomial of $\sqrt[n]{2}$.

Thus,

$$[\mathbb{K} : \mathbb{Q}] \geq [\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$$

for all n.

Proof. If α is not algebraic over $\mathbb{F}$, then

$$1, \alpha, \alpha^2, \alpha^3, \dots$$

are linearly independent. Then, $[\mathbb{K} : \mathbb{F}] = \infty$, a contradiction. □

Corollary 3.3.6 *If α is algebraic over $\mathbb{F}$, then $\mathbb{F}(\alpha)$ is algebraic over $\mathbb{F}$.*

Proof. If α is algebraic over $\mathbb{F}$, then there exists an n such that

$$1, \alpha, \alpha^2, \dots, \alpha^{n-1}$$

form a basis of $\mathbb{F}(\alpha)$ over $\mathbb{F}$. Then, for all $\beta \in \mathbb{F}(\alpha)$,

$$1, \beta, \beta^2, \dots, \beta^n$$

must be linearly dependent. Thus, β is algebraic over $\mathbb{F}$. □

Definition 3.3.3 (Algebraic Numbers) *The set of algebraic numbers is*

$$\overline{\mathbb{Q}} := \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}.$$

Proposition 3.3.7 *Let $\mathbb{F} \subseteq \mathbb{K}$ and let $\alpha, \beta \in \mathbb{K}$ be algebraic over $\mathbb{F}$. Then, $\mathbb{F}(\alpha, \beta)/\mathbb{F}$ is algebraic.*[23]

23: In particular,

$$\alpha + \beta, \alpha - \beta, \alpha\beta, \alpha/\beta$$

are algebraic over $\mathbb{F}$.

Proof. Since β is algebraic over $\mathbb{F}$, it is also algebraic over $\mathbb{F}(\alpha)$. Let

$$\{b_1 1, \ldots, b_m\}$$

be a basis for $\mathbb{F}(\alpha, \beta)$ over $\mathbb{F}(\alpha)$, and let

$$\{a_1, \ldots, a_n\}$$

be a basis for $\mathbb{F}(\alpha)$ over $\mathbb{F}$ (Figure 4.2). Then, every element of $\mathbb{F}(\alpha, \beta)$ is an $\mathbb{F}$-linear combination of

$$\{a_i b_j : 1 \leq i \leq n, 1 \leq j \leq m\},$$

so $[\mathbb{F}(\alpha, \beta) : \mathbb{F}]$ is finite, and thus, algebraic.

□

Theorem 3.3.8 *$\overline{\mathbb{Q}}$ is a field.*

Proof. This follows from the proposition above. □

Theorem 3.3.9 (Tower Law) *Let*

$$\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L},$$

then[24]

$$[\mathbb{L} : \mathbb{F}] = [\mathbb{L} : \mathbb{K}][\mathbb{K} : \mathbb{F}].$$

Proof. First, assume that the RHS is finite. Then, define

$$n := [\mathbb{K} : \mathbb{F}] \text{ and } m := [\mathbb{L} : \mathbb{K}].$$

That is, we have bases

$$\text{span}\{\alpha_1, \ldots, \alpha_n\} = \mathbb{K}$$

and

$$\text{span}\{\beta_1, \ldots, \beta_m\} = \mathbb{L}.$$

Then, we claim that

$$\{\gamma_{ij} := \alpha_i \beta_j \in \mathbb{L}\}$$

forms an $\mathbb{F}$-basis for $\mathbb{L}$. Let $\ell \in \mathbb{L}$. Since $\{\beta, \ldots, \beta_m\}$ is a basis for $\mathbb{L}/\mathbb{K}$, then we can uniquely write

$$\ell = k_1 \beta_1 + \cdots + k_m \beta_m$$

for a collection of field scalars $\{k_i\}_{i=1}^m \subseteq \mathbb{K}$. Similarly, since $\{\alpha_i\}_{i=1}^n$ is a basis for $\mathbb{K}/\mathbb{F}$, we can uniquely write

$$k_i = f_{i1}\alpha_1 + \cdots + f_{in}\alpha_n$$

for a collection of field scalars $\{f_{ij}\}_{j=1}^n \subseteq \mathbb{F}$. Thus, we get a unique decomposition

$$\ell = f_{11}\beta_1\alpha_1 + f_{12}\beta_1\alpha_2 + \cdots + f_{mn}\beta_m\alpha_n,$$

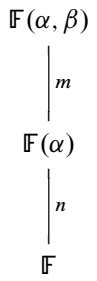


Figure 3.2: The extension diagram for Proposition 4.3.7 with dimensions.

24: For instace, take

$$\underbrace{\mathbb{Q}}_{\mathbb{F}} \subseteq \underbrace{\mathbb{Q}(\sqrt{2})}_{\mathbb{K}} \subseteq \underbrace{\mathbb{Q}(\sqrt[6]{2})}_{\mathbb{L}},$$

yielding $\beta \in \mathbb{Q}(\sqrt[6]{2})$ of the form

$$\beta = a + b\alpha + c\alpha^2 + d\alpha^3 + e\alpha^4 + f\alpha^5,$$

where $a, \ldots, f \in \mathbb{Q}$. Then, we can rewrite this with coefficients entirely in $\mathbb{K}$, meaning our basis for $\mathbb{L}/\mathbb{F}$ is our powers of α up to α^5. Our basis for $\mathbb{L}/\mathbb{K}$ is powers of α up to α^2, and our basis for $\mathbb{K}/\mathbb{F}$ is 1 and $\alpha^3 = \sqrt{2}$:

$$6 = 3 \cdot 2.$$

completing our proof of the finite case. Now, if the RHS is infinite, then either n or m is infinite, meaning the LHS is also infinite,[25] as

$$[\mathbb{L} : \mathbb{F}] \geq [\mathbb{L} : \mathbb{L}] \text{ and } [\mathbb{L} : \mathbb{F}] \geq [\mathbb{K} : \mathbb{F}].$$

□

25: If S spans $\mathbb{L}$ over $\mathbb{F}$, then S also spans $\mathbb{L}$ over $\mathbb{K}$. Additionally, if S spans $\mathbb{L}$ over $\mathbb{F}$, then every vector in $\mathbb{K} \subseteq \mathbb{L}$ is expressible as an $\mathbb{F}$-linear combination of S.

Corollary 3.3.10 *Take the tower $\mathbb{F} \subseteq \mathbb{K} \subseteq \mathbb{L}$. Then,*

(i) If $\mathbb{L}/\mathbb{K}$ and $\mathbb{K}/\mathbb{F}$ are both finite, so is $\mathbb{L}/\mathbb{F}$.
(ii) If $\mathbb{L}/\mathbb{K}$ and $\mathbb{K}/\mathbb{F}$ are both algebraic, so is $\mathbb{L}/\mathbb{F}$.[26]

26: Note that finite implies algebraic. Similarly, if

$$\mathbb{F}(\alpha_1, \ldots, \alpha_n)$$

with algebraic α_i, then this structure is finite.

Proof.

(i) This follows from the Tower Law.
(ii) Let $\beta \in \mathbb{L}$. Consider the minimal polynomial

$$m_{\beta,\mathbb{K}}(x) = x^n + \alpha_{n-1}x^{n-1} + \cdots + \alpha_1 x + \alpha_0 \in \mathbb{K}[x].$$

Since simple algebraic extensions are finite,[27] $\mathbb{F}(\beta)/\mathbb{F}$ is finite, as

27: The degree of the extension has degree equal to that of the minimal polynomial.

$$\begin{array}{c} \mathbb{F}(\alpha_0, \ldots, \alpha_n, \beta) \supseteq \mathbb{F}(\beta) \\ \Big| \deg m_{\beta,\mathbb{K}} \\ \mathbb{F}(\alpha_0, \ldots, \alpha_n) \subseteq \mathbb{K} \\ \vdots \\ \mathbb{F}(\alpha_0, \alpha_1) \\ \Big| \deg m_{\alpha_1,\mathbb{F}} \\ \mathbb{F}(\alpha_0) \\ \Big| \deg m_{\alpha_0,\mathbb{F}} \\ \mathbb{F} \end{array}$$

are all simple algebraic extensions. Thus, β is algebraic over $\mathbb{F}$ for all $\beta \in \mathbb{L}$, so $\mathbb{L}$ is algebraic over $\mathbb{F}$. □

Now, let's take a look at some surprising consequences of the Tower Law.

Remark 3.3.1 For instance, $\sqrt{2} \notin \mathbb{Q}(\sqrt[3]{2})$.

Proof. We know the degree

$$[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n,$$

as $x^n - 2$ is irreducible by Eisenstein's criterion. Then,

$$[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3 \text{ and } [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2.$$

If $\sqrt{2} \in \mathbb{Q}(\sqrt[3]{2})$, then

$$\mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt[3]{2}),$$

and

$$3 = [\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = \underbrace{[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}(\sqrt{2})]}_{\in \mathbb{Z}_+} \underbrace{[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}]}_{2},$$

which is a contradiction. □

Definition 3.3.4 (Composite) *If $\mathbb{K}_1, \mathbb{K}_2 \subseteq \mathbb{L}$, the composite $\mathbb{K}_1\mathbb{K}_2$ is the smallest subfield of $\mathbb{L}$ containing $\mathbb{K}_1$ and $\mathbb{K}_2$.*

Example 3.3.4

(a) $\mathbb{F}(\alpha)\mathbb{F}(\beta) = \mathbb{F}(\alpha, \beta)$.
(b) $\mathbb{Q}(\sqrt{2})\mathbb{Q}(\sqrt[3]{2}) = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) = \mathbb{Q}(\sqrt[6]{2})$.[28]

28: We give two quick proofs of the second equality below.

Proof I.

$$\sqrt{2} = (\sqrt[6]{2})^3 \text{ and } \sqrt[3]{2} = (\sqrt[6]{2})^2 \in \mathbb{Q}(\sqrt[6]{2}),$$

so we have

$$\sqrt[6]{2} = \frac{\sqrt{2}}{\sqrt[3]{2}} \in \mathbb{Q}(\sqrt{2}, \sqrt[3]{2}).$$

□

Proof II. We have $\sqrt{2}, \sqrt[3]{2} \in \mathbb{Q}(\sqrt[6]{2})$, so

$$\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) \subseteq \mathbb{Q}(\sqrt[6]{2}).$$

Then,

$$[\mathbb{Q}(\sqrt[6]{2}) : \mathbb{Q}] = 6,$$

so

$$[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2})] \mid 6,$$

by the Tower Law. Additionally, by the Tower Law,[29] we have

$$2 = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] \mid [\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}].$$

Similarly,

$$3 \mid [\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}],$$

so

$$6 \mid [\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}],$$

meaning

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

□

29: The Tower Law says

$$[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}]$$

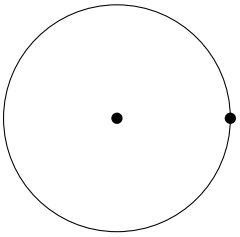
is precisely

$$[\mathbb{Q}(\sqrt{2}, \sqrt[3]{2}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}].$$

3.4 Straightedge and Compass Constructions

We would like to explore straightedge and compass constructions from a field-theoretic view. First, however, we need to review what rules these constructions follow: Given two points, we can draw a line intersecting them.

From here, we can draw a circle given the center and a point on the circumference.



We can also find intersection points of lines and circles. There are three main problems that the Greeks could not solve:[30]

(i) "Double the cube."
(ii) Trisect an arbitrary angle.
(iii) "Square the circle."

30: Our goal is to build up a framework in which we can answer these questions in terms of contemporary language and field theory.

The main idea is to have a set of *constructible numbers*.

We start with two points:

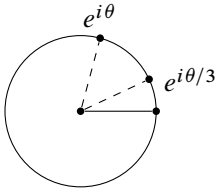


Figure 3.3: Trisecting an angle

Definition 3.4.1 (Constructible Numbers) *We define*

$$\mathcal{C} := \{z \in \mathbb{C} : \textit{the point } z \textit{ is constructible from 1 and 0}\}.$$

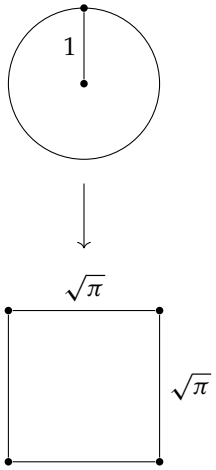


Figure 3.4: Squaring the circle

Definition 3.4.2 (Constructible Distance) *We also define a set of constructible distances.*

$$\mathcal{D} := \{d \in \mathbb{R} : \textit{there exist } a, b \in \mathcal{C} \textit{ with } |a - b| = d\}.$$

Then, we are interested in a subset

$$\mathcal{C}_{\mathbb{R}} := \mathcal{C} \cap \mathbb{R} \subseteq \pm\mathcal{D}.$$

Now, we can rephrase our original problems as

(i) Construct $\sqrt[3]{2}$.
(ii) Given $e^{i\theta}$, construct $e^{i\theta/3}$ (Fig. 3.3).
(iii) Construct $\sqrt{\pi}$ (Fig. 3.4).

Proposition 3.4.1 *$\mathscr{C}$ is closed under*

(i) $z \mapsto |z|$.
(ii) $z \mapsto \overline{z}$.
(iii) $z \mapsto \mathrm{Re}(z)$.
(iv) $z \mapsto \mathrm{Im}(z)$.
(v) addition.
(vi) subtraction.
(vii) multiplication by i.

Proof. We prove these with constructions. All (i)-(iv) are given by (Fig. 3.5).

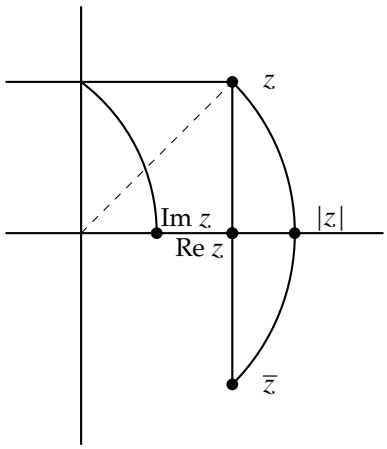


Figure 3.5: Closure of complex arithmetic

Both (v) and (vi) are given by (Fig. 3.6).

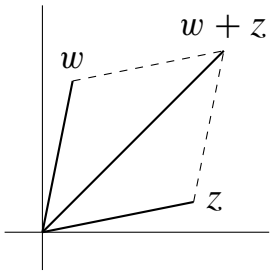


Figure 3.6: Closure of addition

Finally, (vii) is given by (Fig. 3.7).

□

Proposition 3.4.2 *We have $z = x + yi \in \mathscr{C}$ if and only if $x, y \in \mathscr{C}_{\mathbb{R}}$.*

Proof. The forward direction is given by (iii) and (iv) above, and the converse is given by (v) and (vii) above. □

Proposition 3.4.3 *We have that $\pm\mathscr{D} = \mathscr{C}_{\mathbb{R}}$.*

Proof. We get this from (vi) and (i) above. □

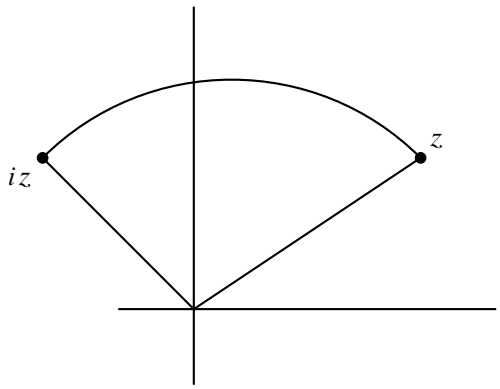


Figure 3.7: Closure of imaginary multiplication

Proposition 3.4.4 *Both $\mathscr{C}_{\mathbb{R}}$ and $\mathscr{C}$ are fields.*

Proof. It will suffice to show that $\mathscr{C}_{\mathbb{R}}$ is closed under multiplication and division. We omit the proof.[31] □

31:
$$\frac{a+bi}{c+di} = \frac{(ac+bd)(bc-ad)}{c^2+d^2}$$

Proposition 3.4.5 *The field $\mathscr{C}_{\mathbb{R}}$ is closed under $\sqrt{(\cdot)}$.*

Theorem 3.4.6 *If $z \in \mathscr{C}$, then $[\mathbb{Q}(z) : \mathbb{Q}]$ is a power of 2.*

Sketch of Proof. All intersections of lines and circles give quadratic equations. □

Corollary 3.4.7 *It is impossible to double the cube.*

Proof. We cannot construct $\sqrt[3]{2}$ which has minimal polynomial $x^3 - 2$. □

Corollary 3.4.8 *It is impossible to trisect and arbitrary angle.*

Proof. Take $\theta := 60°$ and $\theta/3 := 20°$. Then,

$$z = e^{i\pi/9},$$

which is a root of

$$x^6 - x^3 + 1,$$

which is irreducible over $\mathbb{Q}$. □

Corollary 3.4.9 *It is impossible to square the circle.*

Proof. We have a transcendental π, which means $\sqrt{\pi}$ is also transcendental. □

3.5 Splitting Fields

The main question we want to address, now, is whether or not we can adjoin *all* the roots of a polynomial p to a field $\mathbb{F}$.

Definition 3.5.1 (Splitting Field) *The extension field $\mathbb{K}$ of $\mathbb{F}$ is a splitting field for $f(x) \in \mathbb{F}[x]$ if*

(i) f factors into linear factors in $\mathbb{K}[x]$.[32]
(ii) $\mathbb{F} \subseteq \mathbb{L} \subset \mathbb{K}$ with f not splitting in $\mathbb{L}$.

32: We say f 'splits' or 'splits completely.' That is, $\mathbb{K}$ contains $n := \deg f$ roots of f, counting multiplciity.

Example 3.5.1 Consider $\mathbb{Q}(\sqrt{2})$. This is the splitting field for $x^2 - 2 \in \mathbb{Q}[x]$. This is clear, as if we factor, we get

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

Suppose $\mathbb{Q} \subseteq \mathbb{L} \subset \mathbb{Q}(\sqrt{2})$. Then, we know $\sqrt{2} \notin \mathbb{L}$, so $x^2 - 2$ does not split over $\mathbb{L}$.[33]

33: Note that if we take $x^2 - 2 \in \mathbb{Q}(\sqrt{3})[x]$, we get the same factorization as above, so the splitting field is $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Example 3.5.2 If we consider

$$(x^2 - 2)(x^2 - 3) \in \mathbb{Q}[x],$$

then we need the splitting field $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. If

$$\mathbb{Q} \subseteq \mathbb{L} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3}),$$

then $\mathbb{L}$ is missing a root, so the polynomial cannot split over $\mathbb{L}$.

Example 3.5.3 Consider $\mathbb{Q}(\sqrt[3]{2})$. This is *not* the splitting field for $x^3 - 2 \in \mathbb{Q}[x]$.[34] Since $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$, but f has two non-real roots, as we have the factorization

$$f(x) = x^3 - 2 = (x - \sqrt[3]{2}) \underbrace{(x^2 + \sqrt[3]{2} + (\sqrt[3]{2})^2)}_{\text{irreducible}} \in \mathbb{Q}(\sqrt[3]{2})[x].$$

34: This will usually be our default base field.

The way we fix our problem is by adjoining a primitive root of unity. Let

$$\zeta := \zeta_3 = e^{2\pi i/3}.$$

Then, $\zeta^3 = 1$,[35] so

$$f(\sqrt[3]{2}) = f(\zeta_3 \sqrt[3]{2}) = f(\zeta_3^2 \sqrt[3]{2}) = 0.$$

35: In general, we can take ζ_n to be any nth root of 1 that is not a dth root of 1 for $d < n$

Let $\mathbb{K} := \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$. Then,

$$f(x) = (x - \sqrt[3]{2})(x - \zeta_3 \sqrt[3]{2})(x - \zeta_3^2 \sqrt[3]{2}) \in \mathbb{K}[x],$$

so f splits over $\mathbb{K}$.[36]

36: Note that if f splits over $\mathbb{L} \subseteq \mathbb{K}$, then $\sqrt[3]{2}, \zeta_3 \sqrt[3]{2} \in \mathbb{L}$, so $\zeta_3 \in \mathbb{L}$, so $\mathbb{L} = \mathbb{K}$.

Theorem 3.5.1 *Let $f(x) \in \mathbb{F}[x]$. There always exists a field extension $\mathbb{K}/\mathbb{F}$ such that $\mathbb{K}$ is a splitting field for f.*

Proof. We perform induction on $n := \deg f$. Let f_1 be an irreducible factor of f, and let

$$\mathbb{L} := {}^{\mathbb{F}[x]}/_{\langle f_1 \rangle}.$$

Then, f_1 has a root $\theta_1 \in \mathbb{L}$, so

$$f(x) = (x - \theta_1) \underbrace{f_2(x)}_{\deg n-1} \in \mathbb{L}[x].$$

By induction, there is a splitting field $\mathbb{K}$ for f_2 over $\mathbb{L}$. Over $\mathbb{K}$,

$$\begin{aligned} f(x) &= (x - \theta_1) f_2(x) \\ &= (x - \theta_1)(x - \theta_2) \cdots (x - \theta_n) \in \mathbb{K}[x]. \end{aligned}$$

Thus, $\mathbb{F}(\theta_1, \ldots, \theta_n)$ is a splitting field of f over $\mathbb{F}$.[37] □

37: We get minimality be noting that if

$$\mathbb{F} \subseteq \mathbb{E} \subset \mathbb{F}(\theta_1, \ldots, \theta_n),$$

then there exists a j such that $\theta_j \notin \mathbb{E}$, so f does not split.

Remark 3.5.1 The spitting field $\mathbb{K}$, as above, is unique up to isomorphism, so we will talk about *the* splitting field $\operatorname{Sp} f := \operatorname{Sp}_{\mathbb{F}} f$ of f over $\mathbb{F}$.[38]

38: While we proved existence above, we do not include the proof of uniqueness here. See Hardt's lecture notes for the proof.

Corollary 3.5.2 *If $\mathbb{K}$ is the splitting field for $f(x) \in \mathbb{F}[x]$, then*

$$[\mathbb{K} : \mathbb{F}] \leq (\deg f)!.$$

Proof. By induction, we get

$$[\mathbb{K} : \mathbb{F}] = \underbrace{[\mathbb{K} : \mathbb{F}(\theta)]}_{\leq (n-1)!} \underbrace{[\mathbb{F}(\theta) : \mathbb{F}]}_{\leq n},$$

where θ is a root of f. □

Remark 3.5.2 Most polynomials have $[\mathbb{K} : \mathbb{F}] = n!$.

Remark 3.5.3 Note that $n! = |S_n|$.[39]

39: This may seem like a random fact, but...

Definition 3.5.2 (Cyclotomic Field) *Let ζ_n be a primitive nth root of unity.*[40] *We call the field $\mathbb{Q}(\zeta_n)$ the cyclotomic field of nth roots of 1.*

40: Recall that we usually let $\zeta_n := e^{2\pi i/n}$.

Clearly ζ_n is the root of the polynomial

$$\begin{aligned} x^n - 1 &= (x - 1)(x^{n-1} + x^{n-2} + \cdots + x + 1) \in \mathbb{Q}[x] \\ &= (x - 1)(x - \zeta_n)(x - \zeta_n^2) \cdots (x - \zeta_n^{n-1}) \in \mathbb{Q}(\zeta_n)[x]. \end{aligned}$$

We want to know if it is reducible over $\mathbb{Q}$, and we have proven that it is, if and only if n is prime. Now, if $n = p$ is a prime, then we know $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$. However, if n is composite, then $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] < p - 1$.[41]

41: We will discuss the actual structure of these polynomials in the cyclotomic field later.

Now, the reason we are interested in this is that

$$1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1} \in \mathbb{Q}(\zeta_n),$$

so $\mathbb{Q}(\zeta_n)$ is precisely $\mathrm{Sp}(x^n - 1)$. [42]

42: Conversely, $\mathbb{Q}(\sqrt[3]{2})$ is not a splitting field for *any* polynomial.

Example 3.5.4 Let $f(x) := x^p - 2 \in \mathbb{Q}[x]$ with prime p. Factoring gives

$$f(x) = (x - \sqrt[p]{2})(x - \zeta_p \sqrt[p]{2}) \cdots (x - \zeta_p^{p-1} \sqrt[p]{2}).$$

The splitting field

$$\mathrm{Sp}_{\mathbb{Q}}(x^p - 2) = \mathbb{Q}(\sqrt[p]{2}, \zeta_p).$$

Then, the composite extension

$$\mathbb{Q}(\sqrt[p]{2}, \zeta_p) = \mathbb{Q}(\sqrt[p]{2})\mathbb{Q}(\zeta_p),$$

so

$$[\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}] \leq [\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}][\mathbb{Q}(\zeta_p) : \mathbb{Q}].$$

By the Tower Law, we now get

$$\begin{aligned} p &= [\mathbb{Q}(\sqrt[p]{2}) : \mathbb{Q}] \mid [\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}] \\ p - 1 &= [\mathbb{Q}(\zeta_p) : \mathbb{Q}] \mid [\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}], \end{aligned}$$

but p and $p - 1$ are coprime, so

$$[\mathbb{Q}(\sqrt[p]{2}, \zeta_p) : \mathbb{Q}] = p(p - 1).$$

You may wonder, if $\mathbb{K} := \mathbb{Q}(\alpha)$ contains all roots of $x^p - 1$, can we have a strictly smaller field than $\mathbb{Q}(\zeta_p, \sqrt[p]{2})$? It turns out, the answer is *no*, as

$$\mathbb{K} \ni \sqrt[p]{2}, \zeta_p \sqrt[p]{2}, \ldots, \zeta_p^{p-1} \sqrt[p]{2},$$

so $\mathbb{K}$ contains $\mathbb{Q}(\zeta_p, \sqrt[p]{2})$. As such, describing the splitting field specifically is purely an aesthetic matter. Note that we have a basis for $\mathbb{Q}(\sqrt[p]{2}, \zeta_p)$ over $\mathbb{Q}$ of

$$\begin{array}{cccc} \sqrt[p]{2}, & \zeta_p \sqrt[p]{2}, & \cdots & \zeta_p^{p-1} \sqrt[p]{2} \\ (\sqrt[p]{2})^2, & \zeta_p (\sqrt[p]{2})^2, & \cdots & \zeta_p^{p-1} (\sqrt[p]{2})^2 \\ \vdots & \vdots & \cdots & \vdots \\ 1, & \zeta_p, & \cdots & \zeta_p^{p-1}. \end{array}$$

That is, every monomial

$$(\sqrt[p]{2})^m \zeta_p^n$$

with $0 \leq m < p$ and $0 \leq n < p - 1$.

Definition 3.5.3 (Algebraic Closure) *Now, $\overline{\mathbb{F}}$ is an algebraic closure of $\mathbb{F}$ if*

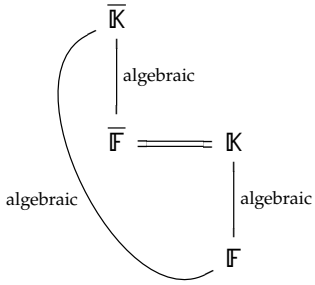
(i) $\overline{\mathbb{F}}/\mathbb{F}$ is algebraic.
(ii) every $f(x) \in \mathbb{F}[x]$ splits completely in $\overline{\mathbb{F}}[x]$.
(ii) Equivalently, every non-constant polynomial in $\mathbb{F}[x]$ has a root in $\overline{\mathbb{F}}$.

Definition 3.5.4 (Algebraically Closed) *We say that a field $\mathbb{K}$ is algebraically closed if $\overline{\mathbb{K}} = \mathbb{K}$.*

Proposition 3.5.3 *If $\mathbb{K} = \overline{\mathbb{F}}$, then $\mathbb{K} = \overline{\mathbb{K}}$.*

Proof. We have a two-part extension, so every element of $\overline{\mathbb{K}}$ is a root of some polynomial over $\mathbb{F}$.

□



Theorem 3.5.4 *Every field $\mathbb{F}$ has a unique algebraic closure $\overline{\mathbb{F}}$, up to isomorphism.*

Proof. See Propositions 30 and 31 from Dummit-Foote. □

Theorem 3.5.5 (Gauß's Fundamental Theorem of Algebra) *The field $\mathbb{C}$ is algebraically closed.*

Corollary 3.5.6 *If $\mathbb{F} \subseteq \mathbb{C}$, then $\overline{\mathbb{F}} \subseteq \mathbb{C}$, so*[43]

$$\overline{\mathbb{Q}} = \text{ the set of algebraic numbers } \subset \mathbb{C}.$$

43: Note that we previously defined the closure of $\mathbb{Q}$ as the set of *complex* algebraic numbers, but as it turns out, this is all of them!

Interestingly, the Fundamental Theorem of Algebra is *necessarily analytically proven*, as we absolutely need some analytic tools to achieve the theorem.

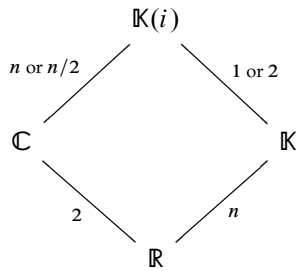
Sketch of Proof. First, we take two immediate consequences of the Intermediate Value Theorem:

(A) Every odd-degree polynomial in $\mathbb{R}[x]$ has a root in $\mathbb{R}$.[44]
(B) Every $\alpha \in \mathbb{R}_{\geq 0}$ has a square root $\sqrt{\alpha} \in \mathbb{R}_{\geq 0}$.

44: In particular, $\mathbb{R}$ has no proper, odd-degree extensions.

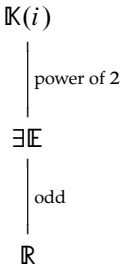
As a result, $\mathbb{C}$ has no degree-2 extensions. Let $f(x) \in \mathbb{R}[x]$ with f irreducible. We define $n := \deg f$.[45] Let $\mathbb{K} := \mathrm{Sp}_{\mathbb{R}} f$, after which we can draw the diagram

45: At this point, we simply need to show that f has a root in $\mathbb{C}$.

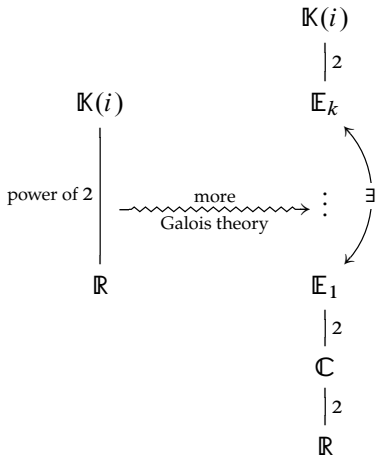


Galois theory, in fact, gives us detailed information about intermediate fields.

In this case,



where the odd extension is impossible by (A),[46] so we have



However, $\mathbb{E}_1/\mathbb{C}$ with degree 2 is impossible by (B).[47] □

This sketch suggests that we want more detailed information about extensions and their intermediate fields.

46: It is impossible unless we trivially take

$$\mathbb{E} := \mathbb{R}^1 = \mathbb{R}.$$

47: It is impossible unless we take

$$\mathbb{C} = \mathbb{K}(i).$$

3.6 Separable Extensions

Let $f(x) \in \mathbb{F}[x]$ be monic over $\mathbb{K} = \mathrm{Sp}_{\mathbb{F}}\ f$. We have

$$f(x) = (x-\alpha_1)^{n_1} \cdots (x-\alpha_k)^{n_k},$$

where these α_i are distinct.

The n_i is called the multiplicity of α_i and α_i is called *simple* if $n_i = 1$ and α_i is *multiple* if $n_i > 1$.

Definition 3.6.1 (Separable) *We call f, as above, separable if all its roots in $\mathbb{K}$ are simple. Otherwise, f is inseparable.*

Example 3.6.1 As some examples, we have

(a)
$$x^2 - 2 = (x+\sqrt{2})(x-\sqrt{2}).$$

(b)
$$x^n - p = (x - \sqrt[n]{p})(x - \zeta_n \sqrt[n]{p}) \cdots (x - \zeta_n^{n-1} \sqrt[n]{p})$$

(c)
$$x^2 + 1 = (x + i)(x - i)$$

(d)
$$x^2 - 1 = (x + 1)(x - 1)$$

Example 3.6.2 As some non-examples, we have

(a)
$$x^2 + 2x + 1 = (x + 1)^2,$$
where -1 is a multiple root.

(b)
$$f(x) := x^2 + t \in \mathbb{F}_2(t)[x].$$
f is irreducible by Eisenstein's Criterion applied to the prime $t \in \mathbb{F}_2[t]$, which is a UFD.[48]

48: Additionally, the rational root theorem yields a similar result.

Let $\mathbb{K} := \mathrm{Sp}_{\mathbb{F}_2(t)} f$, and let $a \in \mathbb{K}$ be a root of $x^2 + t$, meaning $a^2 = t$. Then,

$$\begin{aligned}(x - \alpha)^2 &= x^2 - 2\alpha x + \alpha^2 \\ &= x^2 + t \\ &= f(x).\end{aligned}$$

Thus, f is not separable.

Definition 3.6.2 (Derivative) *The derivative of*
$$f(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{F}[x]$$
is
$$Df(x) := n a_n x^{n-1} + \cdots + 2a_2 + a_1 \in \mathbb{F}[x].$$

Note that we are doing nothing analytic in defining this! However, the usual product, sum, and chain rules still hold.

Theorem 3.6.1 (Separability Criterion) *Let $f(x) \in \mathbb{F}[x]$. Then,*

(i) α is a multiple root of f if and only if α is a root of f and Df.
(ii) $f(x)$ is separable if and only if $\gcd(f, Df) = 1$.

(i) *Proof.* Over $\mathbb{K} := \mathrm{Sp}_{\mathbb{F}} f$,
$$\begin{aligned}f(x) &= (x - \alpha)^n g(x) \\ Df(x) &= \underbrace{n(x - \alpha)^{n-1} g(x) + (x - \alpha)^n Dg(x)}_{\text{multiple of } x - \alpha},\end{aligned}$$

so $Df(\alpha) = 0$. Conversely,

$$\begin{aligned} f(x) &= (x-\alpha)h(x) \\ Df &= h(x) + (x-\alpha)Dh(x) \\ 0 = Df(\alpha) &= h(\alpha) + (\alpha-\alpha)Dh(\alpha), \end{aligned}$$

so $h(\alpha) = 0$, meaning $(x-\alpha)^2 \mid f(x)$, so α a multiple root of f. □

(ii) *Proof.* We will show that for $p, q \in \mathbb{F}[x]$, that $\gcd(p,q) = 1$ if and only if p, q have no common roots in an extension field[49] $\mathbb{K}$ where they split completely. First, suppose that p, q have a common root α over some extension field $\mathbb{K}$. Then, p, q are both divisible by $m_{\alpha,\mathbb{F}}(x)$. Now, for the other case, suppose $\gcd(p,q) = r(x) \in \mathbb{F}[x]$, where r is non-constant. Then, any root of $r(x)$ in $\mathbb{K}$ is a common root of p and q, a contradiction.[50]

□

49: We can make this as large as we want.

50: Every deg ≥ 1 polynomial has a root over its splitting field.

Theorem 3.6.2 *If either*

(i) $\operatorname{char} \mathbb{F} = 0$, *or*
(ii) $\mathbb{F}$ *is finite,*

then every irreducible polynomial $f(x) \in \mathbb{F}[x]$ *is separable.*

Proof of (i). Let $\deg f =: n = 1$. This case is clear, so assume $n \geq 2$. Then,

$$\deg(Df) = n - 1,$$

as $0 = \operatorname{char} f \nmid n$. Now, let $g := \gcd(f, Df)$. Clearly, this has degree $\deg g < n$, so g is a proper divisor of f. Since we assumed f is irreducible over $\mathbb{F}$, g is a unit, so by the Separability Criterion, f is separable.[51] □

51: Again, we wonder why we need $\operatorname{char} \mathbb{F} = 0$? The answer is, we need to show that $\deg Df = n - 1$. In fact, the above proof holds *unless* $Df = 0$.

Definition 3.6.3 (Frobenius Map) *Let* $\operatorname{char} = p$. *The Frobenius map*

$$\operatorname{Frob} := \varphi : \mathbb{F} \to \mathbb{F} : a \mapsto a^p.$$

Proposition 3.6.3

(i) φ *is an injective homomorphism.*
(ii) If $\mathbb{F}$ *is finite,* φ *is an isomorphism.*

(i) *Proof.* The multiplication is given by

$$\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b),$$

and the addition is given by

$$\begin{aligned} \varphi(a+b) &= (a+b)^p \\ &= a^p + \binom{p}{1} a^{p-1}b^1 + \cdots + \binom{p}{p-1} a^1 b^{p-1} + b^p \\ &= a^p + b^p. \end{aligned}$$

Now, we can show this is an injection by noticing that $\ker\varphi$ is an ideal, so $\ker\varphi = \{0\}$ or $\mathbb{F}$. However,

$$\varphi(1) = 1^p = 1 \neq 0.$$

□

(ii) *Proof.* Suppose $\mathbb{F}$ is finite ad φ is injective. Thus, φ is a bijection.[52] □

52: Note that φ is not a surjection if $\mathbb{F} := \mathbb{F}_p(t)$, since $t \notin \operatorname{Im}\varphi$.

Proof of 3.6.2 (ii). In fact, we will choose to prove that if φ is a surjection, then every irreducible $f(x) \in \mathbb{F}[x]$ is separable. Let $f(x) \in \mathbb{F}[x]$ be irreducible and inseparable. Then, by the Separability Criterion, $\gcd(f, Df) \neq 1$. Thus, $Df = 0$. Therefore, $f(x)$ has the form[53]

$$\begin{aligned} f(x) &= a_n x^{pn} + a_{n-1}x^{p(n-1)} + \cdots + a_1 x^p + a_0 \\ &= b_n^p x^{pn} + b_{n-1}^p x^{p(n-1)} + \cdots + b_1^p x^p + b_0^p \\ &= \underbrace{\left(b_n x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0\right)^p}_{g(x)\in\mathbb{F}[x]} \\ &= (g(x))^p. \end{aligned}$$

53: Note, hereafter we let

$$b_i = \varphi^{-1}(a_i) \in \mathbb{F}.$$

Thus, f is reducible, a contradiction.[54] □

54: A big fact we use here is that φ, the Frobenius map, is a ring homomorphism.

Definition 3.6.4 (Perfect Field) *A field $\mathbb{F}$ is perfect if*

(i) $\operatorname{char}\mathbb{F} = 0$ *or*
(ii) $\operatorname{char}\mathbb{F} = p$ *and φ is surjective.*[55]

55: Remember, surjective implies isomorphism here.

Corollary 3.6.4 *If $\mathbb{F}$ is perfect, every irreducible $f \in \mathbb{F}[x]$ is separable.*

Note that some perfect fields include $\mathbb{Q}, \mathbb{R}, \mathbb{C}$, etc.,[56] finite fields, and algebraically closed fields.[57] Note that the last type comes from the fact that

$$\varphi^{-1}(a) \text{ is a root of } x^p - a.$$

56: Here, anything of char 0 works.

57: We could consider $\overline{\mathbb{F}_p}$ or $\overline{\mathbb{F}_p(t)}$.

We now take a brief moment to reconsider finite fields.

Proposition 3.6.5 *Let $n \in \mathbb{Z}_+$ and let p be a prime. Then, there exists a finite field with p^n elements, unique up to isomorphism.*

Proof. Let $f(x) := x^{p^n} - x \in \mathbb{F}_p[x]$, and define

$$\mathbb{F} := \operatorname{Sp}_{\mathbb{F}_p} f(x) =: \mathbb{F}_{p^n}.$$

Since f is separable,[58] f has p^n distinct roots in $\mathbb{F}$, and such a root satisfies $\alpha^{p^n} = \alpha$. These roots form a subfield of $\mathbb{F}$. We can see this by noticing that

$$(\alpha\beta)^{p^n} = \alpha^{p^n}\beta^{p^n} = \alpha\beta$$

and

$$(\alpha^{-1})^{p^n} = (\alpha^{p^n})^{-1} = \alpha^{-1}.$$

58: We can write

$$Df = p^n x^{p^n-1} - 1 = -1,$$

so $\gcd(f, Df) = 1$, so f is separable.

Finally,

$$(\alpha+\beta)^{p^n} = \text{Frob}\,(\cdots(\text{Frob}(\alpha+\beta)\cdots)),$$

which can be rewritten as

$$\text{Frob}(\cdots(\text{Frob}(\alpha)\cdots)) + \text{Frob}\,(\cdots(\text{Frob}(\beta)\cdots)) = \alpha^{p^n} + \beta^{p^n}.$$

Thus, by minimality,

$$\mathbb{F} = \{\text{roots of } x^{p^n} - x\},$$

where $|\mathbb{F}| = p^n$ and $[\mathbb{F} : \mathbb{F}_p] = n$. Now, we will proceed for uniqueness. Let $\mathbb{K}$ be any field of order p^n. Then, $\text{char}\,\mathbb{K} = p$, and we have $[\mathbb{K} : \mathbb{F}] = n$. We have the multiplicative group of the field with order

$$|\mathbb{K}^\times| = |\mathbb{K}| - 1 = p^n - 1,$$

so if $\alpha \in \mathbb{K}^\times$, $\alpha^{p^n-1} = 1$, so $\alpha^{p^n} = \alpha$ for all $\alpha \in \mathbb{K}$. Thus, α is a root of $x^{p^n} - x$. Since $\mathbb{K}$ has $|\mathbb{K}| = p^n$ roots of this polynomial, it is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$, which is unique up to isomorphism. □

3.7 Cyclotomic Fields

Recall that a cyclotomic field is precisely $\mathbb{Q}(\zeta_n)$, where $\zeta_n := e^{2\pi i/n}$. We define the group μ_n by

$$\begin{array}{c} \mathbb{Q}(\zeta_n) \\ | \\ \langle\zeta_n\rangle \\ \| \\ \{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\} \\ \| \\ \mu_n := \{\text{all } n\text{th roots of unity in } \mathbb{C}\} \end{array}$$

Now, the primitive nth root is precisely a generator ζ of μ_n.[59] Which ζ_n^k are primitive? Well, we can write the isomorphism

59: That is, $\zeta^d \neq 1$ for $d < n$.

$$\underbrace{\mu_n}_{\text{multiplicative}} \xrightarrow[\text{group ismorphism}]{\sim} \underbrace{\mathbb{Z}/n\mathbb{Z}}_{\text{under } +}$$

$$\zeta_n^k \longmapsto k$$

Thus, ζ_n^k is primitive if and only if $\gcd(k, n) = 1$. Now, we can use Euler's totient function φ to write

$$\varphi(n) = |\{0 < k < n : \gcd(k, n) = 1\}| = |\{\text{primitive } n\text{th roots of } 1\}|.$$

Now, $\varphi(p) = p - 1$, and since the totient is multiplicative,

$$\varphi\left(p_1^{k_1} \cdots p_n^{k_n}\right) = \prod_{i=1}^{n} p_i^{k_i - 1}(p_i - 1).$$

Definition 3.7.1 (Cyclotomic Polynomial) *The cyclotomic polynomial is*

$$\Phi_n(x) = \prod_{\zeta \in \mu_n \text{ primitive}} (x - \zeta) = \prod_{0 \le k < n \text{ with } \gcd(k,n)=1} (x - \zeta_n^k).$$

Example 3.7.1

$$\begin{aligned}
\Phi_1(x) &= x - 1 \\
\Phi_2(x) &= x + 1 \\
\Phi_3(x) &= x^2 + x + 1 \\
\Phi_4(x) &= x^2 + 1 \\
\Phi_5(x) &= x^4 + x^3 + x^2 + x + 1 \\
\Phi_6(x) &= x^2 - x + 1.
\end{aligned}$$

Additionally, we have that

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

Remark 3.7.1 Now, below are some facts characterizing Φ_n:

(i) Φ_n is monic.
(ii) $\Phi_d(x) \mid x^n - 1$ if $d \mid n$.
(iii) $\deg \Phi_b = \varphi(n)$.
(iv) Every root ζ of unity is a root of precisely one Φ_n.

Theorem 3.7.1 $\Phi_n(x) \in \mathbb{Z}[x]$, *and it is irreducible over* $\mathbb{Z}$ *or* $\mathbb{Q}$.

Proof. We perform induction on n. Assume that $\Phi_d(x) \in \mathbb{Z}[x]$ for $d < n$. Then,

$$x^n - 1 = f(x)\Phi_n(x),$$

where

$$f(x) := \prod_{d|n>d} \Phi_d(x).$$

Now, we divide with remainder in $\mathbb{Q}[x]$. Since $x^n - 1$, $f(x) \in \mathbb{Q}[x]$,

$$x^n - 1 = q(x)f(x) + r(x),$$

with $q, r \in \mathbb{Q}[x]$, and $\deg r < \deg f$, as $\mathbb{Q}[x]$ is a Euclidean domain. Then,

in $\mathbb{C}[x]$, we have that

$$\Phi_n(x)f(x) = q(x)f(x) + r(x)$$

implies

$$(\Phi_n(x) - q(x))f(x) = r(x),$$

so $r(x) = 0$, as $\deg r < \deg f$. Thus,

$$\Phi_n(x) = q(x) \in \mathbb{Q}[x],$$

and by Gauß's Lemma, since $x^n - 1$, $f(x) \in \mathbb{Z}[x]$, $\Phi_n(x) \in \mathbb{Z}[x]$. Now, for irreducibility, suppose not. In particular, we write

$$\Phi_n(x) = f(x)g(x) \quad (f, g \text{ monic in } \mathbb{Z}[x],\ f \text{ irreducible}).$$

We claim that if we let ζ be a root of f, then ζ^p is a root of f for any prime p coprime to n.[60] Iterating the claim, ζ^m is a root of f for any m coprime to n, so all primitive nth roots of 1 are roots of f. Thus, $f = \Phi_n$.[61] Fix ζ and p. Suppose instead that $g(\zeta^p) = 0$. Then, ζ is a root of $g(x^p)$, so $g(x^p) = f(x)h(x)$ for some $h(x) \in \mathbb{Z}[x]$. Now, we reduce

$$\begin{array}{ccc} \mathbb{Z}[x] & \xrightarrow{\quad \bmod (p) \quad} & \mathbb{F}_p[x] \\ x & \longmapsto & x \\ a & \overset{\equiv}{\longmapsto} & a \pmod{p} \end{array}$$

Now, $\overline{x^n} - 1$ is separable in $\mathbb{F}_p[x]$. as

$$D(x^n - 1) = nx^{n-1} \neq 0,$$

so $\overline{\Phi_n(x)}$ has distinct roots. Additionally, we have that

$$\text{Frob} : \mathbb{F}_p \to \mathbb{F}_p$$

is the identity map.[62] Hence,

$$\left(\overline{g(x)}\right)^p = \overline{g(x^p)} = \overline{h(x)f(x)} \in \mathbb{F}_p[x].$$

Finally, this means that $\overline{g}$ and $\overline{f}$ have a common root, but

$$\overline{\Phi_n} = \overline{f}\,\overline{g}$$

has a multiple root, a contradiction. □

Corollary 3.7.2 *We have that*

(i) $m_{\zeta_n, \mathbb{Q}} = \Phi_n(x)$.
(ii) $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$.

60: We first prove that the claim implies the result, and then will prove tha claim itself.

61: We now begin to prove the claim.

62: We have that $a \in \mathbb{F}_p^\times$, which implies that $|a| \mid p - 1$, so $a^{p-1} = 1$, meaning $a^p = a$ for all $a \in \mathbb{F}_p$. This is simply Fermat's Little Theorem from a more sophisticated perspective.

Galois Theory 4

4.1 Automorphisms

Definition 4.1.1 (Automorphism) *Recall, an automorphism is a field isomorphism*

$$\sigma : \mathbb{K} \xrightarrow{\sim} \mathbb{K}.$$

For instance, we have the automorphisms

(a) $\mathbb{K} := \mathbb{C}$,

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\quad\sim\quad} & \mathbb{C} \\ z & \longmapsto & \overline{z} \\ a+bi & \longmapsto & a-bi. \end{array}$$

(b) $\mathbb{K} := \mathbb{Q}(\sqrt{2})$,

$$\begin{array}{ccc} \mathbb{Q}(\sqrt{2}) & \xrightarrow{\quad\sim\quad} & \mathbb{Q}(\sqrt{2}) \\ a+b\sqrt{2} & \longmapsto & a-b\sqrt{2}. \end{array}$$

Note that this is induced by $\sqrt{2} \mapsto -\sqrt{2}$. Additionally, note that

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

with σ the composite map.

Definition 4.1.2 (Aut $\mathbb{K}$) *We define the group of* $\mathbb{K}$*-automorphisms* $\mathrm{Aut}(\mathbb{K})$.[1]

1: We have this under the operation of function composition, where

$$\sigma : a \mapsto b$$

and

$$\sigma^{-1} : b \mapsto a.$$

Example 4.1.1

(a) $\mathrm{Aut}(\mathbb{Q}) = \{\mathrm{id}\}$.
(b) $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})) = \{\mathrm{id}, \sqrt{2} \mapsto -\sqrt{2}\}$

$$\begin{aligned} \alpha &= \sigma(\sqrt{2}) \\ \alpha^2 &= \sigma(\sqrt{2})^2 = \sigma(\sqrt{2})\sigma(\sqrt{2}) = 2. \end{aligned}$$

(c) $|\mathrm{Aut}(\mathbb{C})| = 2^{\aleph_0}$.

Definition 4.1.3 (Fixing) *If $\mathbb{K}/\mathbb{F}$ is a field extension, let*

$$\mathrm{Aut}(\mathbb{K}/\mathbb{F}) := \{\sigma \in \mathrm{Aut}(\mathbb{K}) : \sigma(a) = a \text{ for all } a \in \mathbb{F}\}.$$

If $\sigma : a \mapsto a$, then we say "σ fixes a," and if $\sigma : a \mapsto a$ for all $a \in \mathbb{F}$, then we say "σ fixes $\mathbb{F}$."

Remark 4.1.1

(i) $\mathrm{Aut}(\mathbb{K}/\mathbb{F}) \leq \mathrm{Aut}(\mathbb{K})$.
(ii) $\mathrm{Aut}\,(\mathbb{K}/\text{ prime subfield }) = \mathrm{Aut}(\mathbb{K})$, since every automorphism fixes $\langle 1\rangle$.

Example 4.1.2

(a) With $\mathbb{K} := \mathbb{Q}(\sqrt{2}, i)$, we get

$$\mathrm{Aut}(\mathbb{K}) = \mathrm{Aut}(\mathbb{K}/\mathbb{Q}) = \{1, \sigma, \tau, \sigma \circ \tau\},$$

where

$$\sigma : \sqrt{2} \mapsto -\sqrt{2} : i \mapsto i$$

and

$$\tau : \sqrt{2} \mapsto \sqrt{2} : i \mapsto -i,$$

so

$$\sigma \circ \tau = \tau \circ \sigma : \sqrt{2} \mapsto -\sqrt{2} : i \mapsto -i.$$

We get a basis

$$\underbrace{\overbrace{a + b\sqrt{2} + ci + di\sqrt{2}}^{a,\ldots,d \in \mathbb{Q}} \mapsto a - b\sqrt{2} + ci - di\sqrt{2}}_{[\mathbb{K}:\mathbb{Q}]=4}$$

Then,

$$\mathrm{Aut}(\mathbb{K}/\mathbb{Q}(\sqrt{2})) = \langle\tau\rangle = \{\mathrm{id}, \tau\}$$

and

$$\mathrm{Aut}(\mathbb{K}/\mathbb{Q}(i)) = \langle\sigma\rangle\,.$$

(b) Let $\mathbb{K} := \mathbb{Q}(\sqrt[3]{2})$. We claim that $\mathrm{Aut}(\mathbb{K}/\mathbb{Q}) = \{\mathrm{id}\}$.

Proof. Let $\tau \in \mathrm{Aut}(\mathbb{K}/\mathbb{Q})$. Then,

$$\begin{aligned} 0 = \tau(0) &= \tau(\sqrt[3]{2}^3 - 2) \\ &= \tau(\sqrt[3]{2}^3) - \tau(2) \\ &= \tau(\sqrt[3]{2})^3 - \tau(2) \\ &= \tau(\sqrt[3]{2})^3 - 2. \end{aligned}$$

Thus, $\tau(\sqrt[3]{2})$ is a root of $x^3 - 2$.[2] □

2: That is,

$$\tau(\sqrt[3]{2}) = \sqrt[3]{2},$$

which is the only such root in $\mathbb{K}$.

Proposition 4.1.1 *Let $\mathbb{F} \subseteq \mathbb{K}$ with $f(x) \in \mathbb{F}[x]$. Let $\sigma \in \mathrm{Aut}(\mathbb{K}/\mathbb{F})$. If $\alpha \in \mathbb{K}$ is a root of f, then so is $\sigma(\alpha)$.*

Proof. Let

$$f(x) := a_n x^n + \cdots + a_1 x + a_0.$$

Since σ is a field automorphism fixing $\mathbb{F}$,

$$\begin{aligned} f(\sigma(\alpha)) &= a_n(\sigma(\alpha))^n + \cdots + a_1(\sigma(\alpha)) + a_0 \\ &= \sigma(a_n)(\sigma(\alpha))^n + \cdots + \sigma(a_1)\sigma(\alpha) + \sigma(a_0) \\ &= \sigma(a_n\alpha^n) + \cdots + \sigma(a_1\alpha) + \sigma(a_0) \\ &= \sigma(a_n\alpha^n + \cdots + a_1\alpha + a_0) \\ &= \sigma(f(\alpha)) = \sigma(0) = 0. \end{aligned}$$

□

Therefore, for any $f(x) \in \mathbb{F}[x]$, every element of $\mathrm{Aut}(\mathbb{K}/\mathbb{F})$ permutes the roots of f.

Definition 4.1.4 (Fix H) *Let $H \leq \mathrm{Aut}(\mathbb{K})$. We define*[3]

$$\mathrm{Fix}\, H := \{\alpha \in \mathbb{K} : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}.$$

3: For instance,

$$\mathrm{Fix}\{\mathrm{id}\} = \mathbb{K}.$$

Note that if $H \leq \mathrm{Aut}(\mathbb{K}/\mathbb{Q})$, then

$$\mathbb{Q} \subseteq \mathrm{Fix}\, H \subseteq \mathbb{K}.$$

Proposition 4.1.2

(i) Fix H *is a field.*
(ii) If $H_1 \leq H_2$, then Fix $H_2 \subseteq$ Fix H_1.
(iii) If $\mathbb{F}_1 \subseteq \mathbb{F}_2 \subseteq \mathbb{K}$, then

$$\mathrm{Aut}(\mathbb{K}/\mathbb{F}_2) \leq \mathrm{Aut}(\mathbb{K}/\mathbb{F}_1) \leq \mathrm{Aut}(\mathbb{K}).$$

(i) *Proof.* If $a, b \in \mathrm{Fix}\, H$, then for all $\sigma \in H$,

$$\begin{aligned} \sigma(a+b) &= \sigma(a) + \sigma(b) = a + b \\ \sigma(ab) &= \sigma(a)\sigma(b) = ab \\ \sigma(a^{-1}) &= \sigma(a)^{-1} = a^{-1}. \end{aligned}$$

□

(ii) *Proof.* If $H_1 \leq H_2$, the elements of Fix H_2 satisfy all the conditions of elements of Fix H_1. □

(iii) *Proof.* This is similar to (ii). □

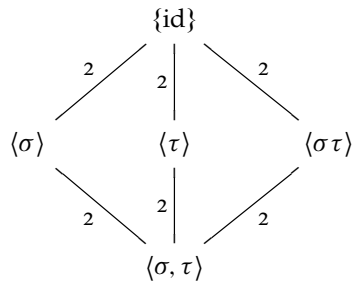
(a) We let $\mathbb{K} := \mathbb{Q}(\sqrt{2}, i)$, again. The subgroups of $\mathrm{Aut}(\mathbb{K}/\mathbb{Q}) \cong V_4$ are

$$\{\mathrm{id}\}, \langle\sigma\rangle, \langle\tau\rangle, \langle\sigma\tau\rangle, \langle\sigma, \tau\rangle = \mathrm{Aut}(\mathbb{K}/\mathbb{Q}).$$

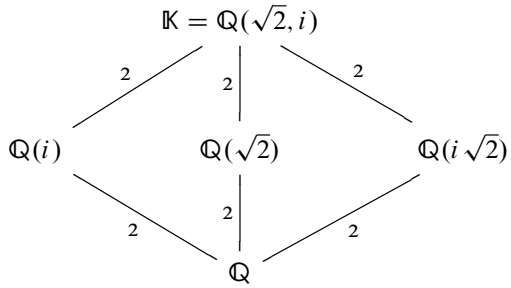
Now, we have

$$\begin{aligned}\operatorname{Fix}\{\mathrm{id}\} &= \mathbb{K}\\ \operatorname{Fix}\langle\sigma\rangle &= \mathbb{Q}(i)\\ \operatorname{Fix}\langle\tau\rangle &= \mathbb{Q}(\sqrt{2})\\ \operatorname{Fix}\langle\sigma\tau\rangle &= \mathbb{Q}(i\sqrt{2})\\ \operatorname{Fix}\langle\sigma,\tau\rangle &= \mathbb{Q}\end{aligned}$$

We draw the subgroups, though we draw it upside down.



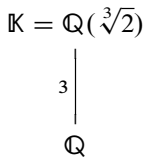
Now, we draw the lattice of intermediate fields.[4]



4: Notice how, effectively, these lattices are identical.

It turns out, this is *all* of the intermediate fields.

(b) Now, $\mathbb{K} := \mathbb{Q}(\sqrt[3]{2})$ has a trivial subgroup lattice $\{\mathrm{id}\}$, with a lattice of intermediate fields



This is rather annoying.

Theorem 4.1.3 *Let $f(x) \in \mathbb{F}[x]$, and $\mathbb{K} := \operatorname{Sp}_{\mathbb{F}} f$. Then,*

$$|\operatorname{Aut}(\mathbb{K}/\mathbb{F})| \leq [\mathbb{K} : \mathbb{F}],$$

where equality holds if and only if f is separable.[5]

5: For the complete proof, see Dummit & Foote.

Demonstrative Example. Let $f(x) := x^3 - 2 \in \mathbb{Q}[x]$. By Eisenstein's Criterion, this is irreducible, and it splits as[6]

6: We define $\alpha := \sqrt[3]{2}$, $\beta := \zeta_3 \sqrt[3]{2}$, and $\gamma := \zeta_3^2 \sqrt[3]{2}$.

$$(x - \sqrt[3]{2})(x - \zeta_3\sqrt[3]{2})(x - \zeta_3^2\sqrt[3]{2}) \text{ over } \mathbb{Q}(\alpha, \beta).$$

Now, we can write

$$\begin{array}{lll} \mathbb{K} = \mathbb{Q}(\alpha, \beta) & & (x-\alpha)(x-\beta)(x-\gamma) \\ \Big| 2 & & \\ \mathbb{L} = \mathbb{Q}(\alpha) & & (x-\alpha)(x^2+\alpha x+\alpha^2) \\ \Big| 3 & & \\ \mathbb{Q} & & x^3-2. \end{array}$$

Now, we attempt to build $\sigma \in \mathrm{Aut}(\mathbb{K}/\mathbb{Q})$ in two steps[7]

7: Note that we count $*_3$ as step one, and $*_{1,2}$ as step two, building our way up to the splitting field.

$$\begin{array}{ccc} & \mathbb{K} = \mathrm{Sp}_{\mathbb{F}}\, f & \\ \swarrow & & \searrow \\ \mathbb{Q}(\alpha,\beta) & \xrightarrow[\beta\mapsto\gamma]{\sim} & \mathbb{Q}(\beta,\gamma) \\ \Big| *_1 & & \Big| *_2 \\ \mathbb{Q}(\alpha) & \xrightarrow[\alpha\mapsto\beta]{\sim} & \mathbb{Q}(\beta) \\ \Big| *_3 & & \Big| *_3 \\ \mathbb{Q} & \xrightarrow[\mathrm{id}]{\sim} & \mathbb{Q}, \end{array}$$

where each $*_i$ mean the following:

($*_1$) Adjoin a root of $g(x) = x^2 + \alpha x + \alpha^2$.
($*_2$) Adjoin a root of $\sigma(g(x)) = x^2 + \beta x + \beta^2$.
($*_3$) Adjoin a root of $f(x)$.

The question we have now is, how many such σ can we construct? Well,

$$\begin{aligned} \#\text{ of } \sigma &= \underbrace{(\#\text{ of choices in } *_3)}_{3}\ \underbrace{(\#\text{ of choices in } *_{1,2})}_{2} \\ &= (\deg f)(\deg g) \\ &= [\mathbb{Q}(\alpha) : \mathbb{Q}][\underbrace{\mathbb{Q}(\alpha,\beta)}_{\mathbb{K}} : \mathbb{Q}\alpha] = [\mathbb{K} : \mathbb{Q}]. \end{aligned}$$

□

Remark 4.1.2 If $f(x) \in \mathbb{F}[x]$ has roots $\alpha_1, \ldots, \alpha_n$ and $\mathbb{K} := \mathrm{Sp}_{\mathbb{F}}$ with $\sigma \in \mathrm{Aut}(\mathbb{K}/\mathbb{F})$, then the restriction

$$\overline{\sigma} = \sigma\big|_{\{\alpha_1,\ldots,\alpha_n\}} \quad \text{yields a permutation} \quad \begin{Bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{Bmatrix} \mapsto \begin{Bmatrix} \alpha_{\overline{\sigma}(1)} \\ \vdots \\ \alpha_{\overline{\sigma}(n)} \end{Bmatrix}.$$

The homomorphism

$$\mathrm{Aut}(\mathbb{K}/\mathbb{F}) \rightarrowtail S_n : \sigma \mapsto \overline{\sigma}$$

is injective,[8] but not necessarily surjective.

8: Here, we use that every automorphism gives a different permutation.

4.2 Galois Groups

Definition 4.2.1 (Galois Extension) *A finite extension $\mathbb{K}/\mathbb{F}$ is Galois if*

$$|\mathrm{Aut}(\mathbb{K}/\mathbb{F})| = [\mathbb{K} : \mathbb{F}].$$

Definition 4.2.2 (Galois Group) *In the case above, we define the Galois group*

$$\mathrm{Gal}(\mathbb{K}/\mathbb{F}) := \mathrm{Aut}(\mathbb{K}/\mathbb{F})$$

of $\mathbb{K}/\mathbb{F}$.

Corollary 4.2.1 *If $f \in \mathbb{F}[x]$ is separable with $\mathbb{K} := \mathrm{Sp}_{\mathbb{F}} f$, then $\mathbb{K}/\mathbb{F}$ is Galois.*[9]

9: It turns out *every* Galois extension is of this form.

(a) The extension $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$ is Galois, since

$$|\mathrm{Aut}(\mathbb{K}/\mathbb{Q})| = 4 = [\mathbb{K} : \mathbb{Q}].$$

Now, $\mathbb{K} := \mathrm{Sp}_{\mathbb{Q}} f$ where[10]

$$f(x) := (x^2 - 2)(x^2 + 1).$$

10: Note that this polynomial has roots $\pm\sqrt{2}$ and $\pm i$.

Then, we get the group[11]

$$\mathrm{Aut}(\mathbb{K}/\mathbb{Q}) = \mathrm{Gal}(\mathbb{K}/\mathbb{F}) = \{\mathrm{id}, \sigma, \tau, \sigma\tau\} = V_4 < S_4.$$

11: Note that V_4 is a proper subgroup of S_4, so it is not all of the group of permutations on $\mathbb{N}_4$.

(b) If we have $f(x) := x^3 - 2 \in \mathbb{Q}[x]$, with $\mathbb{L} := \mathbb{Q}(\alpha)$ and $\mathbb{K} := \mathbb{Q}(\alpha, \beta)$, with the roots defined as previously. Then,

$$|\mathrm{Aut}(\mathbb{K}/\mathbb{Q})| = 6 = [\mathbb{K} : \mathbb{Q}],$$

so $\mathbb{K}/\mathbb{Q}$ is Galois. Then,

$$\mathrm{Aut}(\mathbb{K}/\mathbb{Q}) = \mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong S_3.$$

However,

$$|\mathrm{Aut}(\mathbb{L}/\mathbb{Q})| = 1 \neq [\mathbb{L} : \mathbb{Q}] = 3,$$

so $\mathbb{L}/\mathbb{Q}$ is *not* Galois. Additionally,

$$|\mathrm{Aut}(\mathbb{K}/\mathbb{L})| = 2 = [\mathbb{K} : \mathbb{L}],$$

so $\mathbb{K}/\mathbb{L}$ is Galois, meaning we have

$$\mathrm{Aut}(\mathbb{L}/\mathbb{L}) = \mathrm{Gal}(\mathbb{K}/\mathbb{L}) \cong S_2.$$

Note that for the next few topics, we will focus our proofs on fields with char 0 and/or finite fields. Our results will still be stated for the general case, but this makes a lot of our work easier for demonstration.

Definition 4.2.3 (Separable Extension) *An extension $\mathbb{K}/\mathbb{F}$ is separable if $\mathbb{K}/\mathbb{F}$ is algebraic and $m_{\alpha,\mathbb{F}}(x) \in \mathbb{F}[x]$ is separable for all $\alpha \in \mathbb{K}$.*[12]

12: Note that if $\operatorname{char} \mathbb{F} = 0$ or $\mathbb{F}$ is finite, then

$$\mathbb{K}/\mathbb{F} \text{ finite } \Rightarrow \mathbb{K}/\mathbb{F} \text{ separable.}$$

Theorem 4.2.2 (Primitive Element Theorem) *Every finite, separable extension is simple.*[13]

13: For instance,

$$\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3}).$$

Proof. Since $\mathbb{K}/\mathbb{F}$ is finite, $\mathbb{K} = \mathbb{F}(\alpha_1, \dots, \alpha_n)$ for some generators $\alpha_1, \dots, \alpha_n$. Inducting on n, it suffices to consider $\mathbb{K} = \mathbb{F}(\alpha, \beta)$.

Let $f := m_{\alpha,\mathbb{F}}(x)$ and $g := m_{\beta,\mathbb{F}}(x)$. Now, let $\mathbb{E}$ be a splitting field over $\mathbb{K}$ for fg, containing roots $\alpha = \alpha_1, \dots, \alpha_m$ of f and $\beta = \beta_1, \dots, \beta_n$ of g.

Choose $c \in \mathbb{F} \setminus \{0\}$, and set $\gamma := \alpha + c\beta$ with $\mathbb{L} := \mathbb{F}(\gamma)$. If $\mathbb{L} \subseteq \mathbb{K}$, if $\mathbb{K} \neq \mathbb{L}$, then $\alpha \notin \mathbb{L}$, so $m_{\alpha,\mathbb{L}}(x)$ has at least one other root $\delta \neq \alpha$. Now, $m_{\alpha,\mathbb{L}} \mid m_{\alpha,\mathbb{F}} = f$. Additionally,

$$m_{\alpha,\mathbb{L}} \mid g\left(\frac{\gamma - x}{c}\right) =: h(x),$$

since $g = m_{\beta,\mathbb{L}}$ and

$$\frac{\gamma - \alpha}{c} = \beta,$$

so

$$h(\alpha) = g(\gamma - c\alpha) = g(\beta) = 0.$$

The roots of h in $\mathbb{E}$ are

$$\delta_i := \gamma - c\beta_i = \alpha + c(\beta - \beta_i)$$

for $1 \leq i \leq n$, and we must have $\delta = \alpha_i = \delta_j$ for some i, j. Since $\delta \neq \alpha$,[14]

14: This was assumed above.

$$\alpha_i = \delta_j = \alpha_1 + c(\beta_1 - \beta_j)$$
$$c = \frac{\alpha_i - \alpha_1}{\beta_1 - \beta_j}.$$

That is, there are only finitely many such choices, and $\mathbb{F}$ is infinite, so $\mathbb{K}/\mathbb{F}$ is simple.

□

Corollary 4.2.3 *If $\mathbb{K}/\mathbb{F}$ is finite, then $|\operatorname{Aut}(\mathbb{K}/\mathbb{F})| \leq [\mathbb{K} : \mathbb{F}]$.*[15]

15: That is, we got rid of the necessity of $\mathbb{K} := \operatorname{Sp}_{\mathbb{F}} f$.

Proof. Let $\mathbb{K} := \mathbb{F}(\gamma)$ and $f := m_{\gamma,\mathbb{F}}(x)$. Then, f has at most

$$n := \deg f = [\mathbb{K} : \mathbb{F}]$$

roots $\gamma = \gamma_1, \dots, \gamma_k$ in $\mathbb{K}$, and $\sigma \operatorname{Aut}(\mathbb{K}/\mathbb{F})$ is determined by the image $\sigma(\gamma) = \gamma_i$. □

4.3 Fixed and Finite Fields

Theorem 4.3.1 *Let $G \leq \mathrm{Aut}(\mathbb{K})$, where $\mathbb{K}$ is any field, and define $\mathbb{F} := \mathrm{Fix}\, G$. Then, $\mathbb{K}/\mathbb{F}$ is Galois!*[16]

16: More precisely,

$$[\mathbb{K} : \mathrm{Fix}\, G] = |G|.$$

Furthermore,

$$\mathrm{Aut}(\mathbb{K}/\mathrm{Fix}\, G) = G.$$

We do not have the tools to prove this, yet, but we will come back to it after a short aside. Now, given $\alpha \in \mathbb{K}$, let us determine $m_{\alpha,\mathbb{F}}(x) \in \mathbb{F}[x]$. Let the finite group $G \leq \mathrm{Aut}(\mathbb{K}/\mathbb{F})$ have the action

$$G\alpha := \{\sigma(\alpha) : \sigma \in G\} =: \{\underbrace{\alpha = \alpha_1, \ldots, \alpha_n}_{\text{distinct}}\}.$$

We know that $\alpha_1, \ldots, \alpha_n$ are roots of $m_{\alpha,\mathbb{F}}$, so set[17]

17: Note that $f(x) \in \mathbb{K}[x]$, but not *a priori* $f(x) \in \mathbb{F}[x]$.

$$f(x) := \prod_{1 \leq i \leq n} (x - \alpha_i) \in \mathbb{K}[x].$$

Proposition 4.3.2

(i) $f(x) \in \mathbb{F}[x]$.
(ii) $f(x) = m_{\alpha,\mathbb{F}}(x)$.

Proof. We have that (i) implies (ii) easily, as $f(x) \mid m_{\alpha,\mathbb{F}}(x)$,[18] and conversely, $m_{\alpha,\mathbb{F}}$ is the lowest-degree polynomial in $\mathbb{F}[x]$ such that α is a root. Now, for part (i), we begin by writing

18: This comes from the fact that α_i are roots of $m_{\alpha,\mathbb{F}}$.

$$f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0.$$

Let $\sigma, \tau \in G$, where $\sigma\alpha = \alpha_i$ and $\tau\sigma\alpha = \alpha_j$. Note that

$$\tau(\alpha_i) = \tau(\sigma(\alpha)) = \tau\sigma\alpha = \alpha_j,$$

so $\tau \in G$ permutes the α_i. Then,

$$\begin{aligned} &x^n + \tau(a_{n-1})x^{n-1} + \tau(a_{n-2})x^{n-2} + \tau(a_1)x + \tau(\alpha_0) \\ &= \tau(f(x)) = \tau\left(\prod_i (x - \alpha_i)\right) \\ &= \prod_i (x - \tau\alpha_i) = \prod_i (x - \alpha_i) \\ &= f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0. \end{aligned}$$

Thus, $\alpha \in \mathrm{Fix}\, G = \mathbb{F}$ for all i, so $f(x) \in \mathbb{F}[x]$. □

Definition 4.3.1 (Galois Conjugates) *In the case where $G = \mathrm{Gal}(\mathbb{K}/\mathbb{F})$,*[19] *the elements of $G\alpha$ are called the Galois conjugates.*

19: By the theorem we are attempting to show, this will always hold when $\mathbb{F} = \mathrm{Fix}\, G$.

For instance, when $\alpha := i$,

$$\mathrm{Gal}(\mathbb{C}/\mathbb{R})\alpha =: G\alpha = \{\pm i\},$$

and when $\alpha := \sqrt{2}$, then

$$\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})\alpha =: G\alpha = \{\pm\sqrt{2}\}.$$

Let $\mathbb{K} := \mathbb{F}_{p^n}$, which is precisely $\mathrm{Sp}_{\mathbb{F}_p}(x^{p^n} - x)$.

Proposition 4.3.3 *Let $f(x) \in \mathbb{F}_p[x]$ be irreducible of degree n. Then,*

$$\mathbb{L} := {}^{\mathbb{F}_p[x]}/_{\langle f \rangle} \cong \mathbb{K}.$$

Proof. Since $\deg f = n$, we have that $[\mathbb{L} : \mathbb{F}_p] = n$, so $|\mathbb{L}| = p^n$. By uniqueness, $\mathbb{L} \cong \mathbb{K}$. □

Theorem 4.3.4 *Let $\mathbb{K} := \mathbb{F}_{p^n}$. Then, $\mathbb{K}^\times = \mathbb{K} \setminus \{0\}$ is a cyclic group.*[20]

Proof. By the Fundamental Theorem of Abelian Groups,[21]

$$\mathbb{K}^\times = \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_k\mathbb{Z} = \bigoplus_{i=1}^{k} C_i \cong \prod_{i=1}^{k} C_i,$$

where $d := \gcd(n_1, n_2) > 1$. Suppose $k > 1$, and consider the roots in $\mathbb{K}^\times$ of $x^{n_1} - 1$. Every element in C_{n_1} is such a root, and so is $n_2/d \in C_{n_2}$, but that is $n_1 + 1$ roots of a $\deg n_1$ polynomial, a contradiction. □

Corollary 4.3.5 (Primitive Element Theorem for Finite Fields) *Any extension $\mathbb{K}/\mathbb{F}$ with $\mathbb{K}$ finite is simple.*

Proof. We have $\mathbb{K} = \mathbb{F}(\gamma)$, where γ is any generator of $\mathbb{K}^\times$. □

Corollary 4.3.6

$$\mathrm{Aut}(\mathbb{F}_{p^n}) = \mathrm{Aut}({}^{\mathbb{F}_{p^n}}/_{\mathbb{F}_p}) \cong \mathbb{Z}/n\mathbb{Z} = C_n,$$

with generator $\mathrm{Frob}_p : \alpha \mapsto \alpha^p$.

Proof. We have[22]

$$\langle \mathrm{Frob} \rangle = C_n \leq \mathrm{Aut}({}^{\mathbb{F}_{p^n}}/_{\mathbb{F}_p}).$$

Conversely, since $\mathbb{F}_{p^n}$ is the splitting field of the separable polynomial $x^{p^n} - x$, $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois and

$$|\mathrm{Aut}({}^{\mathbb{F}_{p^n}}/_{\mathbb{F}_p})| = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n.$$

□

We now present a proof of the earlier theorem when $\mathrm{char}\,\mathbb{K} = 0$ or when $\mathbb{K}$ is finite.

20: For instance, for a trivial example, take $\mathbb{K} := {}^{\mathbb{F}_2}/_{\langle x^2+x+1 \rangle} = \{0, 1, 1x, x+1\}$. Then,

$$\mathbb{K}^\times = \{1, x, x+1\},$$

where $x^1 = x$, $x^2 = x+1$, and $x^3 = 1$, so $\mathbb{K} \cong C_3$.

21: We will occasionally use the notation that

$$\mathbb{Z}_n = {}^{\mathbb{Z}}/_{n\mathbb{Z}} = C_n,$$

with the last of the three used to emphasize that we are looking at a *cyclic* group.

22: We cite [13.6.10, Dummit-Foote].

Proof. If $\alpha \in \mathbb{K}$ is primitive for $\mathbb{K}/\mathbb{F}$, then

$$m_{\alpha,\mathbb{F}}(x) = \prod_{\beta \in G\alpha} (x - \beta),$$

so

$$[\mathbb{K} : \mathbb{F}] = [\mathbb{F}(\alpha) : \mathbb{F}] = \deg m_{\alpha,\mathbb{F}} = |G\alpha| \leq |G|.$$

Therefore,

$$|G| \underbrace{\leq}_{\text{(iii)}} |\mathrm{Aut}(\mathbb{K}/\mathbb{F})| \underbrace{\leq}_{\text{(i)}} [\mathbb{K} : \mathbb{F}] \underbrace{\leq}_{\text{(ii)}} |G|,$$

meaning all these are in fact equalities, so

(i) $\mathbb{K}/\mathbb{F}$ is Galois.
(ii) $[\mathbb{K} : \mathbb{F}] = |G|$.
(iii) $\mathrm{Gal}(\mathbb{K}/\mathbb{F}) = G$.

□

4.4 The Fundamental Theorem

Corollary 4.4.1 *If $G_1 \neq G_2$ are distinct finite subgroups of* $\mathrm{Aut}(\mathbb{K})$*, then* $\mathrm{Fix}\, G_1 \neq \mathrm{Fix}\, G_2$.

Proof. By the theorem,[23]

$$G_i = \mathrm{Aut}(\mathbb{K}/\mathrm{Fix}\, G_i).$$

□

23: The only way to have these distinct is for $G_i \neq G_j$.

Theorem 4.4.2 *Let $\mathbb{K}/\mathbb{F}$ be a finite extension. Then, the following are equivalent:*

(i) $\mathbb{K}/\mathbb{F}$ *is Galois.*
(ii) $\mathbb{K}$ *is the splitting field of a separable polynomial in* $\mathbb{F}[x]$.
(iii) $\mathrm{Fix}(\underbrace{\mathrm{Aut}(\mathbb{K}/\mathbb{F})}_{G}) = \mathbb{F}$.

Proof. We have already demonstrated that (ii) implies (i). For (i) implies (iii), note that

$$\mathbb{F} \subseteq \mathrm{Fix}\, G \subseteq \mathbb{K},$$

and by the previous theorem,[24]

$$[\mathbb{K} : \mathrm{Fix}\, G] = |G| = [\mathbb{K} : \mathbb{F}].$$

Finally, for (iii) implies (ii), we will prove in the case of simple extensions.[25] If $\mathbb{K} = \mathbb{F}(\alpha)$, then since $\mathbb{F} := \mathrm{Fix}\, G$,

$$m_{\alpha,\mathbb{F}}(x) = m_{\alpha,\mathrm{Fix}\, G}(x) = \prod_{\beta \in G\alpha} (x - \beta).$$

24: By the Tower Law, since we have the previous subset relation, we get

$$[\mathbb{K} : \mathbb{F}] = [\mathbb{K} : \mathrm{Fix}\, G][\mathrm{Fix}\, G : \mathbb{F},]$$

so

$$[\mathrm{Fix}\, G : \mathbb{F}] = 1,$$

meaning $\mathbb{F} = \mathrm{Fix}\, G$.

25: In particular, this includes char **0** and finite char p.

This is a separable polynomial, by construction, whose splitting field over $\mathbb{F}$ is precisely $\mathbb{K}$. □

Theorem 4.4.3 (Fundamental Theorem of Galois Theory) *Let $\mathbb{K}/\mathbb{F}$ be a Galois extension,*[26] *$G := \mathrm{Gal}(\mathbb{K}/\mathbb{F})$. Then, there exists a bijection*

$$\left\{ \begin{array}{c} \textit{Intermediate} \\ \textit{Fields} \\ \mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K} \end{array} \right\} \overset{\textit{bijection}}{\longleftrightarrow} \left\{ \begin{array}{c} \textit{subgroups} \\ H \leq G \end{array} \right\}$$

$$\varphi : \mathbb{E} \longmapsto \mathrm{Aut}(\mathbb{K}/\mathbb{E})$$

$$\psi : \mathrm{Fix}\, H \longmapsfrom H.$$

We have the properties[27]

(i) $\mathbb{E}_1 \subseteq \mathbb{E}_2$ *if and only if* $H_1 \geq H_2$.
(ii) $[\mathbb{K} : \mathbb{E}] = |H|$ *and* $[\mathbb{K} : \mathbb{F}] = \underbrace{|G : H|}_{\textit{index}}$.
(iii) $\mathbb{K}/\mathbb{E}$ *is Galois with* $\mathrm{Gal}(\mathbb{K}/\mathbb{E}) = H$.
(iv) $\mathbb{E}/\mathbb{F}$ *is Galois if and only if* $H \trianglelefteq G$. *In this case,* $\mathrm{Gal}(\mathbb{E}/\mathbb{F}) = {}^{G}/_{H}$.
(v) $\mathbb{E}_1 \cap \mathbb{E}_2 \leftrightarrow \langle H_1, H_2 \rangle \leq G$ *and* $\mathbb{E}_1\mathbb{E}_2 \leftrightarrow H_1 \cap H_2$.

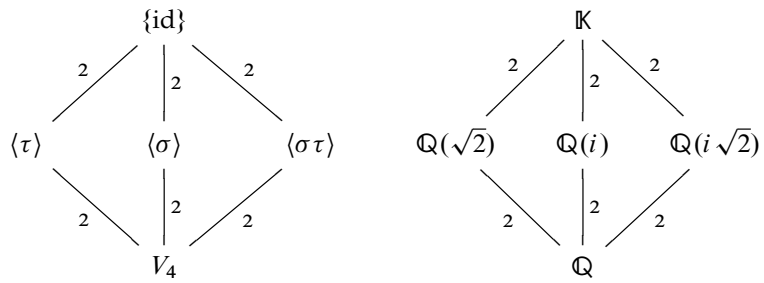
26: In general, assume $\mathbb{K}/\mathbb{F}$ is finite unless/until otherwise stated. Note that Lang addresses the infinite cases as well, but this is outside the scope of our goals.

27:

$$E \leftrightarrow H, E_1 \leftrightarrow H_1, E_2 \leftrightarrow H_2.$$

Let us now take a look at some examples.

(a) $\mathbb{K} := \mathbb{Q}(\sqrt{2}, i) = \mathrm{Sp}_{\mathbb{Q}}(x^2 - 2)(x^2 + 1)$. $\mathbb{K}/\mathbb{Q}$ is Galois with $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) = \langle \tau, \sigma \rangle \cong V_4$.[28]



Since $V_4 \cong \langle \tau \rangle \times \langle \sigma \rangle$ is abelian, every sub-extension is Galois.

28: The automorphisms look like

$$\tau : \begin{Bmatrix} \sqrt{2} \\ i \end{Bmatrix} \mapsto \begin{Bmatrix} \sqrt{2} \\ -i \end{Bmatrix}$$

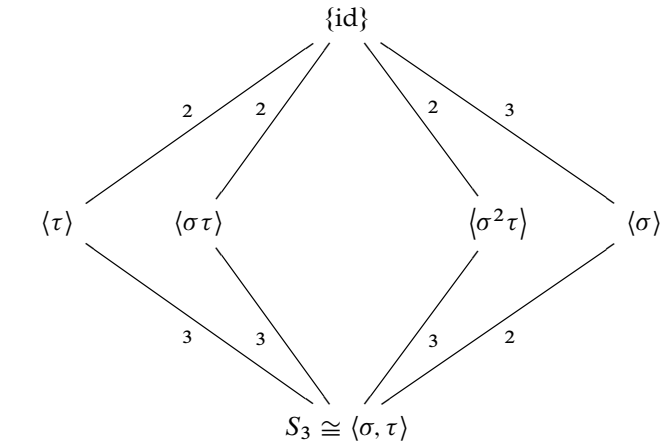
$$\sigma : \begin{Bmatrix} \sqrt{2} \\ i \end{Bmatrix} \mapsto \begin{Bmatrix} -\sqrt{2} \\ i \end{Bmatrix}$$

$$\sigma\tau : \begin{Bmatrix} \sqrt{2} \\ i \end{Bmatrix} \mapsto \begin{Bmatrix} -\sqrt{2} \\ -i \end{Bmatrix}$$

$$\mathrm{id} : \begin{Bmatrix} \sqrt{2} \\ i \end{Bmatrix} \mapsto \begin{Bmatrix} \sqrt{2} \\ i \end{Bmatrix}.$$

Figure 4.1: We list the lattices of subgroups (left) and intermediate fields (right) for Example (a). Note that the lattice of intermediate fields is horizontally mirrored in its correspondence with the subgroup lattice.

(b) $\mathbb{K} := \mathbb{Q}(\sqrt[3]{2}, \zeta_3) = \mathrm{Sp}_{\mathbb{Q}}(x^3 - 2)$ is Galois with $\mathrm{Gal}(\mathbb{K}/\mathbb{Q}) \cong S_3$.[29]



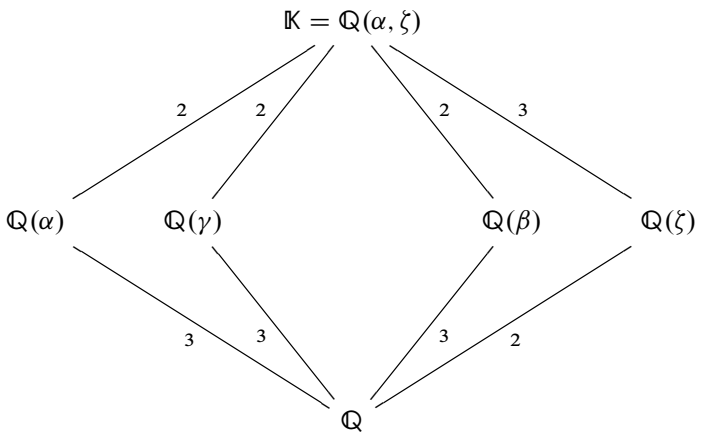


Figure 4.2: We list the lattices of subgroups (top) and intermediate fields (bottom) for Example (b). Once again, the subfields in the second diagram are the fixed fields of the subgroups in the first, where the inclusion-reversing correspondence is reflected in the mirror symmetry.

The third property of the theorem gives that

$$\mathbb{K}/\mathbb{Q}(\alpha), \mathbb{K}/\mathbb{Q}(\gamma), \dots \text{ are all Galois.}$$

Note that only $\langle\sigma\rangle \trianglelefteq S_3$, so $\mathbb{Q}(\zeta)$ is the only Galois subfield over $\mathbb{Q}$.[30]

Proof of the Fundamental Theorem. From basic set theory we have that if $f \circ g$ is injective, then g is injective. Furthermore, if $f \circ g = \mathrm{id}$ and $g \circ f = \mathrm{id}$, then f, g are both bijections, and are inverses. We know that if $H \leq G$, then $\mathrm{Aut}(\mathbb{K}/\operatorname{Fix} H) = H$. Thus, $\varphi \circ \psi = \mathrm{id}$. Now, if $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$, then $\mathbb{K}$ is the splitting field of a polynomial in $\mathbb{F}[x]$, hence in $\mathbb{E}[x]$, so $\mathbb{K}/\mathbb{E}$ is Galois. Additionally,

$$\mathrm{Fix}(\mathrm{Aut}(\mathbb{K}/\mathbb{E})) = \mathbb{E},$$

so $\psi \circ \varphi = \mathrm{id}$. Thus, $\psi = \varphi^{-1}$, and both are bijections. □

Proof of the Properties.

(i) We proved this previously.

29: Defining $\alpha := \sqrt[3]{2}, \zeta := \zeta_3, \beta := \zeta\alpha, \gamma := \zeta^2\alpha$, the automorphisms look like the permutations on $\mathbb{N}_3$:

$$\begin{aligned}
\mathrm{id} &: \begin{Bmatrix}\alpha\\ \zeta\end{Bmatrix} \mapsto \begin{Bmatrix}\alpha\\ \zeta\end{Bmatrix}\\
\sigma &: \begin{Bmatrix}\alpha\\ \zeta\end{Bmatrix} \mapsto \begin{Bmatrix}\beta\\ \zeta\end{Bmatrix}\\
\sigma^2 &: \begin{Bmatrix}\alpha\\ \zeta\end{Bmatrix} \mapsto \begin{Bmatrix}\gamma\\ \zeta\end{Bmatrix}\\
\tau &: \begin{Bmatrix}\alpha\\ \zeta\end{Bmatrix} \mapsto \begin{Bmatrix}\alpha\\ \zeta^2\end{Bmatrix}\\
\sigma\tau = \tau\sigma^2 &: \begin{Bmatrix}\alpha\\ \zeta\end{Bmatrix} \mapsto \begin{Bmatrix}\beta\\ \zeta^2\end{Bmatrix}\\
\sigma^2\tau = \tau\sigma &: \begin{Bmatrix}\alpha\\ \zeta\end{Bmatrix} \mapsto \begin{Bmatrix}\gamma\\ \zeta^2\end{Bmatrix}.
\end{aligned}$$

30: We have that every second-order subgroup is normal, since there are only two cosets.

(ii) By the Galois correspondence, $\mathrm{Gal}(\mathbb{K}/\mathbb{E}) = H$, and by the definition of a Galois extension,

$$[\mathbb{K} : \mathbb{E}] = |\mathrm{Gal}(\mathbb{K}/\mathbb{E})| = |H|.$$

By the Tower Law,

$$[\mathbb{E} : \mathbb{F}] = \frac{[\mathbb{K} : \mathbb{F}]}{[\mathbb{K} : \mathbb{F}]} = \frac{|G|}{|H|} = |G : H|.$$

(iii) This follows from the theorem of equivalent Galois statements.

(iv) Every $\sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{F})$ sends $\mathbb{E}$ to $\sigma(\mathbb{E}) \subseteq \mathbb{K}$, and in particular, because it is an isomorphism, $\sigma(\mathbb{E}) \cong \mathbb{E}$. The set of *embeddings* of $\mathbb{E}$ *into* $\mathbb{K}$ fixing $\mathbb{F}$ is given by[31]

$$\mathrm{Emb}_{\mathbb{K}}(\mathbb{E}/\mathbb{F}) = \left\{\sigma\big|_{\mathbb{E}} : \sigma \in \mathrm{Gal}(\mathbb{K}/\mathbb{F})\right\}.$$

Now,

$$\sigma\big|_{\mathbb{E}} = \sigma'\big|_{\mathbb{E}} \text{ if and only if } \sigma H = \sigma' H,$$

so

$$|\mathrm{Emb}_{\mathbb{K}}(\mathbb{E}/\mathbb{F})| = |G : H| \underbrace{=}_{\text{(ii)}} [\mathbb{E} : \mathbb{F}].$$

Now,

$$\mathrm{Aut}(\mathbb{E}/\mathbb{F}) = \{\overline{\sigma} \in \mathrm{Emb}_{\mathbb{K}}(\mathbb{E}/\mathbb{F}) : \overline{\sigma}(\mathbb{E}) = \mathbb{E}\} \subseteq \mathrm{Emb}_{\mathbb{K}}(\mathbb{E}/\mathbb{F}).$$

Thus, $\mathbb{E}/\mathbb{F}$ is Galois if and only if $\mathrm{Aut}(\mathbb{E}/\mathbb{F}) = \mathrm{Emb}_{\mathbb{K}}(\mathbb{E}/\mathbb{F})$, which is true if and only if $\sigma(\mathbb{E}) = \mathbb{E}$ for all $\sigma \in G$, which holds if and only if

$$H = \mathrm{Aut}(\mathbb{K}/\mathbb{E}) = \mathrm{Aut}(\mathbb{K}/\sigma(\mathbb{E})) = \sigma H \sigma^{-1}$$

for all $\sigma \in G$.[32] In this case, $\mathrm{Aut}(\mathbb{E}/\mathbb{F}) \cong {}^{G}/_{H}$.

(v) We have that if $e \in \mathbb{E}_1 \cap \mathbb{E}_2$ if and only if e is fixed by $H_1 \cup H_2$, which is true if and only if e is fixed by $\langle H_1, H_2 \rangle$. The other part of (v) is similar.

□

31: This requires proof, but we will continue with our sketch. See Dummit & Foote for the complete proof.

32: This is precisely $H \trianglelefteq G$.

4.5 Cyclotomic Galois Groups and n-gon Construction

Recall that

$$\mathscr{C} := \text{ the field of constructible numbers } \subseteq \mathbb{C}.$$

We have previously discussed that if $\alpha \in \mathscr{C}$, then $\sqrt{\alpha} \in \mathscr{C}$, so $\mathbb{F} \subseteq \mathscr{C}$ with any deg 2 extension $\mathbb{F}(\alpha) \subseteq \mathscr{C}$. Additionally, $\alpha \in \mathscr{C}$ implies that

$$[\mathbb{Q}(\alpha) : \mathbb{Q}] = 2^k \text{ for some } k \in \mathbb{Z}_+.$$

Theorem 4.5.1 *Now, the proper statement is that $\alpha \in \mathscr{C}$ if and only if there*

exists a chain

$$\mathbb{E}_0 := \mathbb{Q} \subseteq \mathbb{E}_1 \subseteq \cdots \subseteq \mathbb{E}_k$$

such that $\alpha \in \mathbb{E}_k$ *and*

$$\begin{aligned}[\mathbb{E}_1 : \mathbb{Q}] &= 2\\ [\mathbb{E}_2 : \mathbb{E}_1] &= 2\\ &\vdots\\ [\mathbb{E}_k : \mathbb{E}_{k-1}] &= 2.\end{aligned}$$

We will try to use Galois theory to understand this. Now, it is clear that the *regular* n-gon is constructible if and only if $\zeta_n = e^{2\pi i/n}$ is constructible. Recall that

$$\mathbb{Q}(\zeta_n) = \mathrm{Sp}_{\mathbb{Q}}(x^n - 1) = \mathrm{Sp}_{\mathbb{Q}}\, \Phi_n(x),$$

so $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois.

Proposition 4.5.2

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times.$$

33: That is, $a \in (\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. Take $\sigma \in G$ determined by $\sigma(\zeta_n) = \zeta_n^a$, where $\gcd(a, n) = 1$.[33] Let $\sigma_a \in G$ have $\sigma_a(\zeta_n) = \zeta_n^a$. Then,

$$\sigma_a\sigma_b(\zeta_n) = \sigma_a(\zeta_n^b) = \underbrace{\zeta_n^a \cdots \zeta_n^a}_{b} = \zeta^{ab} = \sigma_{ab}(\zeta_n).$$

□

Corollary 4.5.3 *G, as above, is abelian!*

Example 4.5.1 Take $n = 13$. Then,

$$G = \mathrm{Gal}(\mathbb{Q}(\zeta_{13})/\mathbb{Q}) \cong (\mathbb{Z}/13\mathbb{Z})^\times \cong C_{12}.$$

Now, this is *cyclic*, and one possible generator is $\sigma := \sigma_2 : \zeta_{13} \mapsto \zeta_{13}^2$. We need the elements of $\mathbb{Q}(\zeta)$ fixed by each subgroup of G. The idea is is to sum over the orbits. For instance,

$$\langle \sigma^6 \rangle = \{1, \sigma^6\}$$

has an orbit

$$\langle \sigma^6 \rangle \zeta = \{\zeta, \sigma^6\zeta\}.$$

Let $\alpha := \zeta + \sigma^6\zeta$. We claim that α is fixed by $\langle \sigma^6 \rangle$.

Proof. $\sigma^{12} = 1$, so

$$\sigma^6\zeta = \sigma^6(\zeta + \sigma^6\zeta) = \sigma^6\zeta + \sigma^{12}\zeta = \sigma^6\zeta + \zeta = \alpha.$$

□

Now, $\sigma^6\zeta = \zeta^{2^6} = \zeta^{64} = \zeta^{12} = \zeta^{-1}$.

$$\mathrm{Fix}\langle \sigma^6 \rangle = \mathbb{Q}(\zeta + \zeta^{-1}).$$

We get this this has the correct degree, since

$$\mathbb{Q}(\zeta + \zeta^{-1}) \ni \zeta^2 + (\zeta + \zeta^{-1})\zeta - 1 = 0.$$

If we instead take $\langle\sigma^4\rangle = \{1, \sigma^4, \sigma^8\}$, then the orbit is

$$\langle\sigma^4\rangle\zeta = \{\zeta, \sigma^4\zeta, \sigma^8\zeta\},$$

so

$$\mathrm{Fix}\langle\sigma^4\rangle = \mathbb{Q}(\zeta + \sigma^4\zeta + \sigma^8\zeta) = \mathbb{Q}(\zeta + \zeta^3 + \zeta^9).$$

We continue this process to find all our intermediate fields.[34]

34: This would be immensely difficult without summing over the orbits.

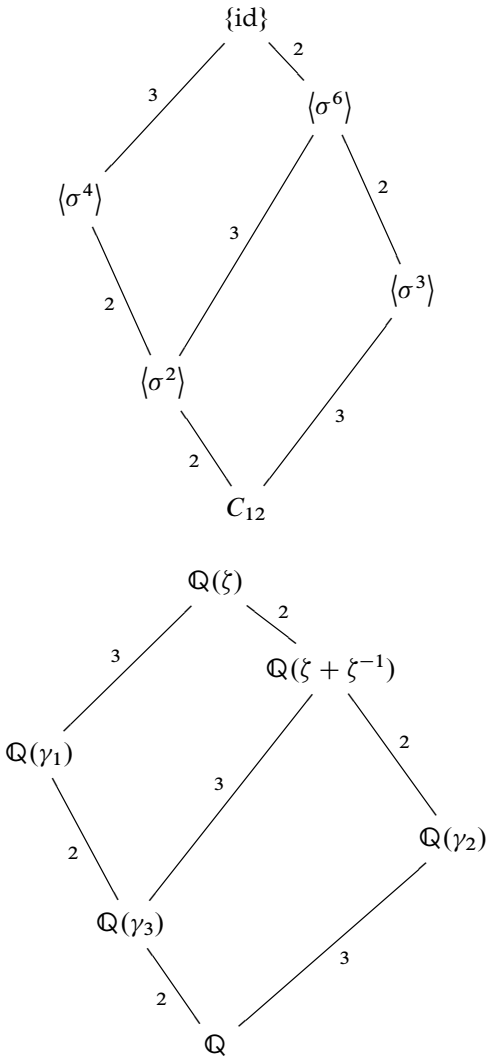


Figure 4.3: We list the lattices of subgroups (top) and intermediate fields (bottom) for Example 5.5.1. We set

$\gamma_1 := \zeta + \zeta^3 + \zeta^9$
$\gamma_2 := \zeta, \zeta^5, \zeta^8, \zeta^{12}$
$\gamma_3 := \zeta + \zeta^3 + \zeta^4 + \zeta^7 + \zeta^{10} + \zeta^{12}.$

Theorem 4.5.4 *The n-gon is constructible if and only if $\varphi(n)$ is a power of 2.*

Proof. We have $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$, and we have already shown that this must be a power of 2. For the converse, suppose $\varphi(n) = 2^k$. Then, since

$\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is Galois,

$$G := \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$$

is an abelian group of order 2^k. Now, abelian groups of order r have subgroups of order every divisor $d \mid r$.[35] Thus,

35: We use the Fundamental Theorem of Abelian Groups.

$$\{\mathrm{id}\} = G_0 \leq G_1 \leq \cdots \leq G_{k-1} \leq G_k = G,$$

with $|G_i| = 2^i$, and by the Galois correspondence,

$$\mathbb{Q}(\zeta_n) = \mathbb{E}_0 \supseteq \mathbb{E}_1 \supseteq \cdots \supseteq \mathbb{E}_{k-1} \supseteq \mathbb{E}_k = \mathbb{Q},$$

so $\zeta_n \in \mathscr{C}$. □

Corollary 4.5.5 *The n-gon is constructible if and only if*

$$n = 2^k p_1 \cdots p_r,$$

where the p_i are distinct primes of the form[36]

36: Primes of this form are known as *Fermat primes*.

$$p_i = 2^{2^{s_i}} + 1.$$

Proof. These are the numbers n such that $\varphi(n)$ is a power of 2. □

4.6 The Quintic

Let us take $f(x) \in \mathbb{F}[x]$, and per usual, take the extension $\mathbb{K} := \mathrm{Sp}_{\mathbb{F}} f(x)$.

Definition 4.6.1 *The Galois group of $f(x)$ is precisely*

$$\mathrm{Gal}_{\mathbb{F}}(f) := \mathrm{Gal}(\mathbb{K}/\mathbb{F}).$$

Our goal is to understand $\mathrm{Gal}(f)$ for different polynomials. We are building towards the following *very famous* theorem by Abel and Ruffini.

Theorem 4.6.1 (Abel-Ruffini) *The "generic"*[37] deg 5 *polynomial over $\mathbb{Q}$ is not solvable by radicals.*

37: Galois went even further and said there exist specific such polynomials.

We know that if $\deg f(x) = n$, then $\mathrm{Gal}(f) \leq S_n$. Now let us take a look at the generic version. Define

$$\mathbb{K} := \mathbb{F}(x_1, \ldots, x_n) = \text{field of fractions of } \mathbb{F}[x_1, \ldots, x_n].$$

We have $S_n \leq \mathrm{Aut}(\mathbb{K}/\mathbb{F})$, where we just permute the x_i's. Now, set $\mathbb{L} := \mathrm{Fix}\, S_n$, and we have $\mathrm{Gal}(\mathbb{K}/\mathbb{L}) = S_n$.

Definition 4.6.2 (Field of Symmetric Fuctions) *We call $\mathbb{L} := \mathrm{Fix}\, S_n$ the field of symmetric functions.*

For instance, we have the elements

(a) $f \in \mathbb{F}$.
(b) $e_1 := e_1(x_1, , x_2, \ldots, x_n) = x_1 + x_2 + \cdots + x_n$.
(c) $e_2 := \sum_{i<j} x_i x_j = x_1x_2 + x_1x_3 + x_2x_3 + \cdots$.
(d) $e_k := \sum_{i_1<\cdots<i_k} x_{i_1} \cdots x_{i_k}$.[38]

38: These examples are precisely what are called the *elementary symmetric functions*.

Theorem 4.6.2 (1/2 Fundamental Theorem of Symmetric Functions)

$$\mathbb{L} = \mathbb{F}(e_1, \ldots, e_n).$$

Proof. Let $\mathbb{L}' := \mathbb{F}(e_1, \ldots, e_n)$. Then, $\mathbb{L}' \subseteq \mathbb{L}$, and

$$[\mathbb{K} : \mathbb{L}] = |S_n| = n!,$$

so we just need to show that $[\mathbb{K} : \mathbb{L}'] = n!$. This follows since $\mathbb{K}$ is the splitting field of the following $\deg n$ polynomial in $\mathbb{L}'[x]$:

$$\begin{aligned} f_{\text{gen}}^{(n)} &:= \prod_{1\le i\le n} (x - x_i) \\ &= x^n - (x_1 + \cdots x_n)x^{n-1} + \cdots + (-1)^n x_1x_2\cdots x_n \\ &= x^n - e_1x^{n-1} + \cdots + (-1)^n e_n \in \mathbb{L}'[x]. \end{aligned}$$

□

Definition 4.6.3 (Discriminant) *The discriminant of $f(x) \in \mathbb{F}[x]$ is*

$$D := \prod_{i<j} (\alpha_i - \alpha_j)^2,$$

where α_i are the roots of f in $\mathbb{K} := \text{Sp}_{\mathbb{F}}(f)$.[39]

39: This is with multiplicity.

Proposition 4.6.3 *$D = 0$ if and only if f is inseparable.*[40]

40: Recall that this means f has multiple roots.

Proposition 4.6.4 *$D \in \mathbb{F}$.*

Proof. D is symmetric in the α_i, so[41]

$$\mathbb{F}(e_1(\alpha_1, \ldots, \alpha_n), \ldots, e_n(\alpha_1, \ldots, \alpha_n)) = \mathbb{F}.$$

41: Note that the $e_i(\alpha_1, \ldots, \alpha_n)$ is precisely the coefficients of f.

□

Example 4.6.1

(a) Take $f := f_{\text{gen}}^{(2)}(x) = (x - x_1)(x - x_2)$. Then, our discriminant is

$$D = (x_1 - x_2)^2 = x_1^2 - 2x_1x_2 + x_2^2,$$

which we can rewrite as

$$(x_1 + x_2)^2 - 4x_1x_2 = e_1^2 - 4e_2.$$

Thus, if $f(x) := x^2 + bx + c$, then[42]

$$D = e_1^2 - 4e_2^2 = b^2 - 4c.$$

(b) If

$$f(x) := x^3 + ax^2 + bx + c,$$

then

$$D = a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 19abc.$$

In general, we have no "nice" formula for D in terms of the e_i!

42: This is precisely the discriminant you learned in high school, lacking the a soleley because f is monic.

Proposition 4.6.5 $\sqrt{D} \notin \mathbb{F}$.

Proof. Consider a square root

$$\sqrt{D} = \prod_{i<j}(\alpha_i - \alpha_j).$$

This is not symmetric, as it depends on the order of the roots.[43]

43: For instance, for $n = 3$
$\sqrt{D} = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)(\alpha_2 - \alpha_3)$.

$$\begin{array}{c} \mathbb{K} := \mathrm{Sp}_{\mathbb{F}}\ f(x) \\ \| \\ \mathbb{F}(\alpha_1, \ldots, \alpha_n) \\ | \\ \mathbb{F}(\sqrt{D}) \\ | \ 1 \text{ or } 2 \\ \mathbb{F} := \mathbb{F}(D) \end{array}$$

Now, assume $\mathrm{char}\,\mathbb{F} \neq 2$. If $G := \mathrm{Gal}(\mathbb{K}/\mathbb{F}) = S_n$, then there exists some automorphism $\sigma \in G$ such that $\sigma(\sqrt{D}) = -\sqrt{D}$. Thus, $\sqrt{D} \notin \mathbb{F}$. □

Now, recall that

$$A_n := \left\{ \begin{array}{c} \text{even permutations} \\ \text{on } \mathbb{N}_n \end{array} \right\} \underbrace{\leq}_{\text{index } 2} S_n.$$

Proposition 4.6.6 *We have $G \leq A_n$ if and only if $\sqrt{D} \in \mathbb{F}$.*

Proof. If $\sigma \in G$, then $\sigma(\sqrt{D}) = \sqrt{D}$ if and only if σ is an even permutation. That is, $G \leq A_n$ if and only if $\sigma(\sqrt{D}) = \sqrt{D}$ for all $\sigma \in G$, which is true if and only if $\sqrt{D} \in \mathrm{Fix}\, G = \mathbb{F}$. □

Now, let us find some Galois groups. Take $f(x) \in \mathbb{F}[x]$ with $\mathrm{char}\,\mathbb{F} \neq 2$. Define $\mathbb{K} := \mathrm{Sp}_{\mathbb{F}}\ f(x)$ and $G := \mathrm{Gal}(\mathbb{K}/\mathbb{F})$.

(i) Take $\deg f = n = 2$. Then, $f(x) = x^2 + bx + c$. If f is reducible, then $\mathbb{K} = \mathbb{F}$, $G = \{\mathrm{id}\} = A_2$. If f is irreducible, then $[\mathbb{K} : \mathbb{F}] = 2$ and $G = C_2 = S_2$.[44]

(ii) Take $\deg f = n = 3$. Then,

$$f(x) = x^3 + ax^2 + bx + c.$$

If f is reducible, see the $n = 2$ case. If f is irreducible, S_3 has a lot of subgroups. What could G be?

44: Note that
$\mathbb{K} = \mathbb{F}(\sqrt{D}) = \mathbb{F}(\alpha_1 - \alpha_2) = \mathbb{F}(\sqrt{b^2 - 4c})$.
We get the roots to be
$$\frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

Definition 4.6.4 (Transitive Group Action) *A group G acts transitively on a set A if*[45]

$$Ga = A \quad \text{for all } a \in A.$$

45: That is, the action has exactly one orbit.

Proposition 4.6.7 *If $f(x) \in \mathbb{F}[x]$ is irreducible, with $\mathbb{K} := \mathrm{Sp}_{\mathbb{F}}(f)$, then* $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ *acts transitively on the set of of roots of $f(x)$.*

Proof. Let $G\alpha := \{\alpha_1, \ldots, \alpha_k\}$. If $\sigma \in F$, σ permutes $G\alpha$, so

$$\sigma(e_i(\alpha_1, \ldots, \alpha_k)) = e_i(\sigma(\alpha_1), \ldots, \sigma(\alpha_k)) = e_i(\underbrace{\alpha_1, \ldots, \alpha_k}_{\text{permuted but sym.}}).$$

This means that $e_i(\alpha_1, \ldots, \alpha_k) \in \mathrm{Fix}\, G = \mathbb{F}$. Thus,

$$\prod_{i=1}^{k}(x - \alpha_i) = x^k - e_1(\alpha_1, \ldots, \alpha_k)x^{k-1} + \cdots + (-1)^k e_k(\alpha_, \ldots, \alpha_k) \in \mathbb{F}[x].$$

Since this divides f,[46] it must equal f, so G acts transitively. □

46: Remember, f is the minimal polynomial.

Let us take a look at the case of $n = 3$, where

$$f(x) := x^3 + ax^2 + bx + c,$$

taking $G \leq S_3$. If f is reducible, see the $n = 2$ case. If f is irreducible, then G is a transitive subgroup of S_3.[47] Now, $G = A_3$, if and only if $[\mathbb{K} : \mathbb{F}] = 3$, which holds if and only if

$$\sqrt{D} = \sqrt{a^2b^2 - 4b^3 - 4a^3c - 27c^2 + 18abc} \in \mathbb{F}.$$

47: The only transitive subgroups are S_3 and $A_3 \cong C_3$.

Additionally, $G = S_3$ if and only if $[\mathbb{K} : \mathbb{F}] = 6$, and equivalently, $\sqrt{D} \notin \mathbb{F}$.[48]

48: For instance, with $f(x) = x^3 - 2$, we know $[\mathbb{K} : \mathbb{F}] = 6$, so $G = S_3$ and $\sqrt{D} \notin \mathbb{Q}$.

To get a better feel for this, take $\mathbb{F} := \mathbb{Q}$ and consider two very similar looking polynomials:

$$\underbrace{x^3 + 3x + 1 \quad \text{and} \quad x^3 - 3x + 1}_{\text{irreducible by rational root theorem}}.$$

Computing the discriminant of the former yields $D = 81$, and $\sqrt{D} = 9 \in \mathbb{Q}$, so $G = C_3$. For the latter, $D = -135$, $\sqrt{D} \notin \mathbb{Q}$, so $G = S_3$.[49]

49: See Dummit & Foote pp. 627-629 for the, rather involved process, of finding the Galois group of a quartic. Given a quartic, you can compute an object called a resolvent cubic. That is, in a very non trivial way, the quartic case reduces to the cubic case.

Theorem 4.6.8 (Cardano, 1545) *The cubic equation is solvable by radicals.*

Proof. Take $f(x) := x^3 + ax^2 + bx + c$, and define

$$g(y) := f\left(x + \frac{a}{3}\right) = y^3 + py + q,$$

where

$$p = \frac{1}{3}(3b - a^2) \quad \text{and} \quad q = \frac{1}{27}(2a^3 - 9ab + 27c).$$

Let $\zeta := \zeta_3$ and $\zeta^2 + \zeta_1 = 0$. Let $g(y)$ have roots α, β, γ, so

$$\alpha + \beta + \gamma = e_1(\alpha, \beta, \gamma) = -(x^2 - \text{ coeff. }) = 0.$$

We get $e_2 = p$ and $e_3 = -q$. We know $0 = \alpha + \beta + \gamma$. We can then define *Lagrange Resolvents*, taking

$$\text{Lagrange Resolvents: } \begin{cases} 0 = \alpha + \beta + \gamma \\ \theta_1 := \alpha + \zeta\beta + \zeta^2\gamma \\ \theta_2 := \alpha + \zeta^2\beta + \zeta\gamma. \end{cases}$$

50: We are just solving an easy system of equations here.

Then, $\theta_1 + \theta_2 = 3\alpha$, $\zeta^2\theta_1 + \zeta\theta_2 = 3\beta$, and $\zeta\theta_1 + \zeta^2\theta_2 = 3\gamma$.[50] Now, note that

$$\begin{aligned} \sqrt{D} &= (\alpha - \beta)(\alpha - \gamma)(\beta - \gamma) \\ &= \alpha^2\beta + \beta^2\gamma + \gamma^2\alpha - \alpha\beta^2 - \beta\gamma^2 - \gamma\alpha^2, \end{aligned}$$

so if

$$\mathcal{S} := \alpha^2\beta + \beta^2\gamma + \gamma^2\alpha + \alpha\beta^2 + \beta\gamma^2 + \gamma\alpha^2,$$

then

$$\theta_1^3 = \alpha^3 + \beta^3 + \gamma^3 + \frac{3}{2}\zeta(\mathcal{S} + \sqrt{D}) + \frac{3}{2}\zeta^2(\mathcal{S} - \sqrt{D}) + \underbrace{6\alpha\beta\gamma}_{-6q}.$$

We can show, given that $\alpha + \beta + \gamma = 0$, that

$$\alpha^3 + \beta^3 + \gamma^3 = -3q,$$

and we also have that $\mathcal{S} = 3q$. Hence,

$$\theta_1^3 = -3q + \frac{3}{2}\zeta(3q + \sqrt{D}) + \frac{3}{2}\zeta^2(3q - \sqrt{D}) - 6q.$$

Now, this can be rewritten as

$$\theta_1^3 - \frac{27}{2}q + \frac{3}{2}\sqrt{-3D}$$

as $\zeta + \zeta^2 = -1$ and $\zeta - \zeta^2 = \sqrt{-3}$. Similarly, we get

$$\theta_2^3 = -\frac{27}{2}q - \frac{3}{2}\sqrt{-D}.$$

We need $\theta_1\theta_2 = -3p$, so we can constrain these equations enough to get

our α, β, γ.[51] We will write out the cubic formula, choosing

$$A := \sqrt[3]{-\frac{27}{2}q + \frac{3}{2}\sqrt{-3D}}$$

and

$$B := \sqrt[3]{-\frac{27}{2}q - \frac{3}{2}\sqrt{-3D}},$$

such that $AB = -3p$. Then,

$$\alpha = \frac{A+B}{3}, \beta = \frac{\zeta^2 A + \zeta B}{3}, \gamma = \frac{\zeta A + \zeta^2 B}{3}.$$

□

51: That is, any choice works after modding out by this relation.

Definition 4.6.5 (Solvable by Radicals) *A polynomial $f(x) \in \mathbb{F}[x]$ is solvable by radicals if there exists an extension chain*

$$\mathbb{F} = \mathbb{K}_0 \subseteq \mathbb{K}_1 \subseteq \cdots \subseteq \mathbb{K}_s \supseteq \mathrm{Sp}_{\mathbb{F}}\, f(x),$$

where $\mathbb{K}_{i+1} = \mathbb{K}_i(\alpha_i)$ with α_i a root of $x^{n_i} - a_i \in \mathbb{K}_i[x]$.[52]

52: That is, an nth root of a_i.

This is especially nice, since it allows the nth roots of unity. Now, assume $\mathrm{char}\, \mathbb{F} = 0$.[53]

53: This is a stronger asusmption than we need. We just need $\mathrm{char}\, \mathbb{F}$ to not divide anything we do not want it to.

Theorem 4.6.9 (ancients, Cardano, Ferrari) *All* $\deg \leq 4$ *polynomials are solvable.*[54]

54: The ancients did $n = 2$, Cardano did $n = 3$, and Ferrari did $n = 4$.

Theorem 4.6.10 (Abel-Ruffini) *There is no general solution by radicals for $f^{(n)}_{gen}$, where $n \geq 5$.*

4.7 Solvability

We are now working towards proving this major theorem by Galois.

Theorem 4.7.1 (Galois)

(i) $f(x)$ is solvable by radicals if and only if $\mathrm{Gal}\, f(x)$ *is a "solvable group."*
(ii) There exists a degree 5 polynomials which is not solvable by radicals.

Definition 4.7.1 (Solvable Group) *A finite group G is solvable*[55] *if the tower*

$$\{\mathrm{id}\} = G_s \lhd G_{s-1} \lhd \cdots \lhd G_0 = G,$$

where G_i/G_{i+1} is cyclic.[56]

55: UK: "soluable."

56: Technically this can be weakened to *abelian*, but since abelian groups can be reduced down into cyclic groups, it does not matter.

Example 4.7.1

(a) Abelian groups are solvable, as we can decompose them into a

direct sum of cyclic groups.[57] For instance,

$$\{\mathrm{id}\} \underbrace{\lhd}_{C_2} C_2 \underbrace{\lhd}_{C_2} C_2 \oplus C_2 \underbrace{\lhd}_{C_4} \overbrace{C_2 \oplus C_2 \oplus C_4}^{G}.$$

(b) Dihedral groups are solvable, as we can always write

$$\{\mathrm{id}\} \underbrace{\lhd}_{C_n} C_n \underbrace{\lhd}_{C_2} D_{2n} = G.$$

(c) We have that p-groups are always solvable.[58]

(d) We know S_4 is solvable, as

$$\{\mathrm{id}\} \underbrace{\lhd}_{C_2} C_2 \underbrace{\lhd}_{C_2} V_4 \underbrace{\lhd}_{C_3} A_4 \underbrace{\lhd}_{C_2} S_4 = G.$$

Now, let us take a look at some *non-examples*.

Example 4.7.2

(a) S_n or A_n for $n \geq 5$ have no normal subgroups.[59]

(b) Other finite simple groups are also not solvable.[60]

Corollary 4.7.2 *If $n = 5$ and $\mathbb{K} := \mathrm{Sp}_{\mathbb{F}} f(x)$, then*

$$\mathrm{Gal}(\mathbb{K}/\mathbb{F}) = S_n \text{ or } A_n$$

implies f is not solvable by radicals. Thus, Galois' theorem implies Abel-Ruffini.

Proposition 4.7.3

(i) If $H \leq G$, then G being solvable implies H is solvable.
(ii) If $H \lhd G$, then H and ${}^{G}/_{H}$ being solvable implies G is solvable.

(i) *Proof.* Let

$$\{\mathrm{id}\} = G_s \lhd G_{s-1} \lhd \cdots \lhd G_0 = G,$$

where ${}^{G_i}/_{G_{i+1}}$ is cyclic. Let $H_i := H \cap G_i$. Then, $H_{i+1} \lhd H_i$ and ${}^{H_i}/_{H_{i+1}}$ is isomorphic to a subgroup of ${}^{G_i}/_{G_{i+1}}$, so it is cyclic:

$$\{\mathrm{id}\} = H_s \lhd \cdots \lhd H_0 = H.$$

□

(ii) *Proof.* Let us write the solvable towers

$$\{\mathrm{id}\} = H_s \lhd H_{s-1} \lhd \cdots \lhd H_0 = H$$
$$\{\mathrm{id}\} = J_r \lhd J_{r-1} \lhd \cdots \lhd J_0 = {}^{G}/_{H}.$$

If $\pi : G \to {}^{G}/_{H}$ canonically,[61] then

$$\{\mathrm{id}\} = H_s \lhd \cdots \lhd H_0 = \pi^{-1}(J_r) \lhd \pi^{-1}(J_{r-1}) \lhd \cdots \lhd \pi^{-1}(J_0),$$

57: This is simply the Fundamental Theorem of Abelian Groups.

58: That is, any group G of the form $|G| = p^k$.

59: That is, they are simple. See Dummit & Foote Theorem 4.24 for the proof that S_n is not solvable.

60: For instance, the *monster* group.

61: That is, we are just using the standard projection map.

where we use the pullbacks of π as needed.[62] □

62: Remember, here J_r is just our way of writing {id}.

Consider $\mathbb{K} := \mathrm{Sp}_{\mathbb{Q}}(x^2 - 2)$. We have part of the two corresponding diagrams looking like

$$\begin{array}{ccc} \mathbb{K} & & \{\mathrm{id}\} \\ \Big| 3 & & \Big| 3 \\ \mathbb{Q}(\zeta_3) & & C_3 = A_3 \\ \Big| 2 & & \Big| 2 \\ \mathbb{Q} & & S_3, \end{array}$$

where, per usual, the subgroup lattice is inverted. Now, we get the chain

$$\{\mathrm{id}\} \underbrace{\lhd}_{C_3} C_3 \underbrace{\lhd}_{C_2} S_3,$$

or equivalently,

$$\mathrm{Gal}(\mathbb{K}/\mathbb{K}) \lhd \mathrm{Gal}(\mathbb{K}/\mathbb{Q}(\zeta_3)) \lhd \mathrm{Gal}(\mathbb{K}/\mathbb{Q}).$$

Lemma 4.7.4 *Suppose $\mathbb{F} \subseteq \mathbb{E} \subseteq \mathbb{K}$ with $\mathbb{K}/\mathbb{F}$ and $\mathbb{E}/\mathbb{F}$ are both Galois. Then, if*

$$\mathrm{Gal}(\mathbb{K}/\mathbb{E}), \mathrm{Gal}(\mathbb{E}/\mathbb{F}) \quad \textit{is solvable},$$

then $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ *is solvable.*

Proof. Since $\mathbb{E}/\mathbb{F}$ is Galois, by the fourth proposition of the Fundamental Theorem of Galois Theory,

$$\mathrm{Gal}(\mathbb{K}/\mathbb{E}) \lhd \mathrm{Gal}(\mathbb{K}/\mathbb{F}),$$

and

$$\mathrm{Gal}(\mathbb{E}/\mathbb{F}) \cong {}^{\mathrm{Gal}(\mathbb{K}/\mathbb{F})}/_{\mathrm{Gal}(\mathbb{K}/\mathbb{E})}.$$

By part (ii) of the previous proposition, $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ is solvable. □

Note that part (i) of Galois' theorem is true over any characteristic of our field, but part (ii) does depend on the characteristic. We are generally keeping our proofs to char 0 for brevity.

Remark 4.7.1 Galois groups of extensions of finite fields are *always cyclic*,[63] so it is *always solvable* by radicals. We just need to take a finite field of the correct degree, then our roots sit where we need them to.

63: We can get this from a few of our previous results, including our work on the Frobenius map.

However, infinite char p is rather terrible to work with, which is why we are sticking to char 0.

Lemma 4.7.5 *Let* $\operatorname{char} \mathbb{F} = 0$. *If* $a \in \mathbb{F}$ *and* $\mathbb{K} := \operatorname{Sp}_{\mathbb{F}}(x^n - a)$, *then*

$$\operatorname{Gal}(\mathbb{K}/\mathbb{F}) = \operatorname{Gal}_{\mathbb{F}}(x^n - a)$$

is solvable.

Proof. $\mathbb{K}$ is the splitting field of a separable polynomial, so $\mathbb{K}/\mathbb{F}$ is Galois. In particular, if α is a root of $x^n - a$, then the roots are

$$\left\{\alpha\zeta_n^k : 0 \leq k < n\right\}.$$

Let $\mathbb{E} := \mathbb{F}(\zeta_n)$. Then, $\operatorname{Gal}(\mathbb{E}/\mathbb{F})$ is abelian, since it is isomorphic to $\operatorname{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \cong C_n^\times$. Furthermore, the map

$$\begin{array}{ccc} \operatorname{Gal}(\mathbb{K}/\mathbb{E}) & \longrightarrow & C_n \\ (\alpha \mapsto \alpha\zeta_n^k) & \longmapsto & k \end{array}$$

is an injective homomorphism, so $\operatorname{Gal}(\mathbb{K}/\mathbb{E})$ is cyclic. By the lemma, $\operatorname{Gal}(\mathbb{K}/\mathbb{F})$ is solvable. □

Lemma 4.7.6 *Suppose* $\mathbb{K}/\mathbb{F}$ *is Galois with* $\operatorname{Gal}(\mathbb{K}/\mathbb{F}) \cong C_n$. *If* $\zeta_n \in \mathbb{F}$, *then* $\mathbb{K} = \mathbb{F}(\alpha)$ *for some* $\alpha \in \mathbb{K}$ *with* $\alpha^n \in \mathbb{F}$.

Sketch of Proof. Consider the Lagrange resolvent of $\alpha \in \mathbb{K}$:

$$\beta := L(\alpha) := \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha),$$

where $\zeta := \zeta_n$ and σ is a generator of $\operatorname{Gal}(\mathbb{K}/\mathbb{F})$. Since $\sigma(\zeta) = \zeta$,

$$\sigma(\beta) = \sigma(\alpha) + \zeta\sigma^2(\alpha) + \cdots + \zeta^{n-1}\alpha = \zeta^{-1}\beta.$$

Hence,[64]

$$\sigma^{\beta^n} = (\zeta^{-1}\beta)^n = \beta^n.$$

Conversely, if $\beta \neq 0$, then $\mathbb{F}(\beta) = \mathbb{K}$, since $\sigma^i(\beta) = \zeta^{-i}\beta \neq \beta$, where $i \in [n-1]$. Therefore,

$$\operatorname{Aut}(\mathbb{K}/\mathbb{F}(\beta)) = \{\mathrm{id}\}.$$

By Dummit & Foote Theorem 14.7, the elements of $\operatorname{Gal}(\mathbb{K}/\mathbb{F})$ are linearly independent. Hence, there exists $\alpha \in \mathbb{K}$ such that $L(\alpha) \neq 0$. □

64: The key point to notice here is that since σ fixes β^n, and of course, σ generates all of the Galois group, we must have $\beta^n \in \mathbb{F}$.

Proof of Galois (i). If $f(x) \in \mathbb{F}[x]$ is solvable by radicals, then there exists a tower[65]

$$\mathbb{F} = \mathbb{K}_0 \subseteq \mathbb{K}_2 \subseteq \cdots \subseteq \mathbb{K}_s \supseteq \mathbb{K} := \operatorname{Sp}_{\mathbb{F}} f(x),$$

with $\mathbb{K}_{i+1} = \mathbb{K}_i(\alpha)$. Remember, α_i is a root of $x^{n_i} - a_i$ for $a_i \in \mathbb{K}_i$. Let

$$\mathbb{F} = \mathbb{L}_0 \subseteq \mathbb{L}_1 \subseteq \cdots \subseteq \mathbb{L}_s = \mathbb{L},$$

where $\mathbb{L}_{i+1} = \operatorname{Sp}_{\mathbb{L}_i}(x^{n_i} - a_i)$. Then, $\mathbb{K}_i \subseteq \mathbb{L}_i$ for all i, so

$$\operatorname{Sp}_{\mathbb{F}} f(x) = \mathbb{K} \subseteq \mathbb{K}_s \subseteq \mathbb{L}_s.$$

65: As a reminder, we are doing this in $\operatorname{char} \mathbb{F} = 0$. The result holds for $\operatorname{char} \mathbb{F} = p$, but it requires some careful linear algebraic approaches that we do not have time for.

Thus, $\mathrm{Gal}(\mathbb{L}_{i+1}/\mathbb{L}_i)$ is solvable, so $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$ is solvable. Since $\mathbb{K}/\mathbb{F}$ is Galois, by the Fundamental Theorem of Galois Theory's fourth property, $\mathrm{Gal}(\mathbb{K}/\mathbb{F})$ is a quotient of the bigger group $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$. Since we have a quotient of a solvable group, it is solvable. Conversely, if $G := \mathrm{Gal}(\mathbb{K}/\mathbb{F})$ is solvable, then there exists a chain

$$\{\mathrm{id}\} = G_s \lhd G_{s-1} \lhd \cdots \lhd G_0 = G,$$

with cyclic quotients. Let $\mathbb{K}_i := \mathrm{Fix}\, G_i$, so

$$\mathbb{K} = \mathbb{K}_s \supseteq \mathbb{K}_{s-1} \supseteq \cdots \supseteq \mathbb{K}_0 = \mathbb{F}.$$

The extension $\mathbb{K}_{i+1}/\mathbb{K}_i$ is Galois by the Fundamental Theorem of Galois Theory's fourth property, with

$$\mathrm{Gal}(\mathbb{K}_{i+1}/\mathbb{K}_i) \cong {}^{\mathrm{Gal}(\mathbb{K}/\mathbb{K}_i)}\!/_{\mathrm{Gal}(\mathbb{K}/\mathbb{K}_{i+1})} = {}^{G_i}\!/_{G_{i+1}} \cong C_{n_i},$$

for some $n_i \in \mathbb{Z}_+$. Let

$$\mathbb{F}' := \mathbb{F}(\zeta_{n_1}, \zeta_{n_2}, \ldots, \zeta_{n_s}),$$

and set $\mathbb{K}'_i := \mathbb{K}_i\mathbb{F}'$. We have that

$$\mathbb{F} \underbrace{\subseteq}_{x^{n_i}-1} \mathbb{F}' = \mathbb{K}_0 \subseteq \mathbb{K}'_1 \subseteq \cdots \subseteq \mathbb{K}'_s \supseteq \mathbb{K}.$$

By the previous lemma, $\mathbb{K}'_{i+1} = \mathbb{K}'_i(\alpha_i)$, where α_i is a root of $x^{n_i} - a_i$, and where $a_i \in \mathbb{K}'_i$, so f is solvable by radicals. □

Proof of Galois (ii). First, note that if $\sigma, \tau \in S_5$ with σ a 5-cycle and τ a 2-cycle, then $\langle \sigma, \tau \rangle = S_5$.[66] Let[67] $f(x) := x^5 - 6x + 3 \in \mathbb{Q}[x]$. Thus, $G \leq S_5$, meaning G is transitive on the roots, meaning it has an order which is a multiple of 5. The only fifth-order elements of S_5 are 5-cycles, so G contains a 5-cycle. Now, f must have ≥ 3 real roots by the intermediate value theorem, and it cannot have more, as $Df(x) = 5x^4 - 6$ has only two real roots. By the Fundamental Theorem of Algebra, $f(x)$ has 5 roots in $\mathbb{C}$.[68] Let $\tau \in \mathrm{Aut}(\mathbb{K}/\mathbb{Q})$ be complex conjugation. This τ fixes the real roots, so we must have the non-real roots as complex conjugates. Therefore, τ is a 2-cycle. Hence, $G = S_5$, which is not solvable, so by Galois part (i), it is impossible to express the roots of $f(x)$ by radicals. □

66: Check this by casework.

67: Per usual, $\mathbb{K} := \mathrm{Sp}_{\mathbb{Q}} f(x)$ and $G := \mathrm{Gal}(\mathbb{K}/\mathbb{Q})$. Note that f is irreducible by Eisenstein's Criterion ($p = 3$).

68: That is, there are two non-real roots.

On Algebraic Geometry

The Zero-Locus Theorem 5

We now begin our short section on algebraic geometry via the language of varieties. Roughly speaking, algebraic geometry studies the solutions to sets of multivariate polynomial equations.

5.1 Radicals

In general, we want to know whether a solution exists, and if a solution exists, we want to know the "shape" of the solution set.

Let us take a look at some motivating examples in $\mathbb{C}[x, y]$.

(a) Consider the system

$$\begin{cases} x + y = 3 \\ x - y = 5 \end{cases} \rightsquigarrow \begin{cases} x + y - 3 = 0 =: f(x, y) \\ x - y - 5 = 0 =: g(x, y). \end{cases}$$

We can plot these polynomials as seen in (Fig. 5.1).

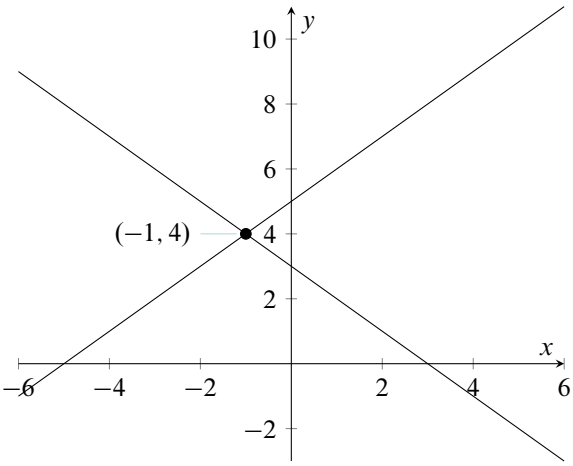


Figure 5.1: Plot of the system $\{f(x, y), g(x, y)\}$, as above

(b) Now, consider the system

$$\begin{cases} y = x^2 = 0 \\ x - y^2 = 0. \end{cases}$$

We can plot these as seen in (Fig. 5.2).[1]

Theorem 5.1.1 (Bézout's Theorem) *The "usual" situation is that two polynomials in $\mathbb{C}[x, y]$ of degrees m and n have mn intersection points in $\mathbb{C}$.*[2]

1: We also have the complex intersection points (ζ_3, ζ_3^2) and (ζ_3^2, ζ_3).

2: This is the standard starting point for "intersection (co)homology."

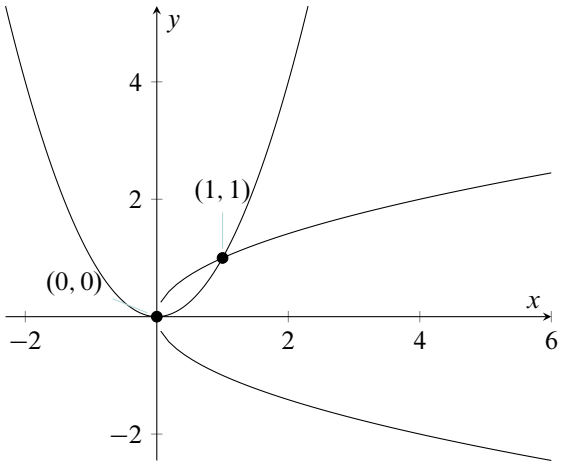


Figure 5.2: Plot of the second system

Now, what happens if we have the system

$$\begin{cases} y = x^3 = 0 \\ 2y - 2x^3 = 0. \end{cases}$$

Clearly we have two curves (Fig. 5.3) which are identical, so their solution set is every point on the curve.

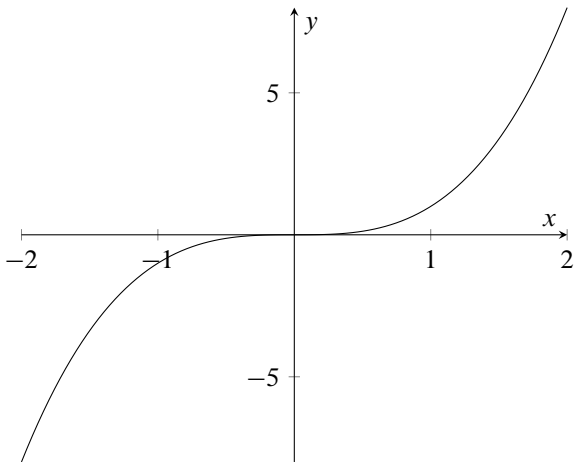


Figure 5.3: Plot of the third system

Finally, consider

$$\begin{cases} f(x, y) := 4y - 2x - 6 = 0 \\ g(x, y) := -6y + 3x + 20. \end{cases}$$

Clearly this has no solutions when plotted (Fig. 5.4). Why not? Well,

$$3f + 2g = 12y - 6x - 18 - 12y + 6x + 4 = -14.$$

We are going to take the next few lectures to prove the first version of the weak form of Hilbert's Nullstellensatz.[3] The statement is given below.

3: Literally, Hilbert's zero-locus-theorem.

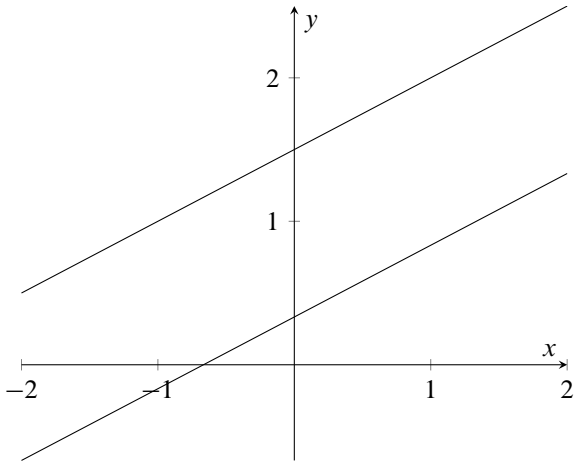


Figure 5.4: Plot of the fourth system

Theorem 5.1.2 (Nullstellensatz, weak form, first version) *Let*

$$f_1(x_1, \ldots, x_n), \ldots, f_m(x_1, \ldots, x_n) \in \mathbb{C}[x_1, \ldots, x_n].$$

Then, the system of equations

$$f_1(x_1, \ldots, x_n) = \cdots = f_m(x_1, \ldots, x_n) = 0$$

has no solution[4] *in* $\mathbb{C}^n$ *if and only if there exist*

$$g_1, \ldots, g_m \in \mathbb{C}[x_1, \ldots, x_n]$$

such that

$$f_1 g_1 + f_2 g_2 + \cdots + f_m g_m = 1 \in \mathbb{C}[x_1, \ldots, x_n].$$

4: An example of this was computed directly above. Note that the Nullstellensatz is the standard starting place in algebraic geometry, as it was the first major result proved in the field.

Definition 5.1.1 (Ideals) *Recall, an ideal of a commutative, unital ring* R *is a subset* $I \subseteq R$ *such that* $a, b \in I$ *with* $r \in R$ *implies* $a + b, ra \in I$.

Definition 5.1.2 (Radical) *The radical of an ideal* I *is the ideal*

$$\sqrt{I} := \{r \in R : r^n \in I \text{ for some } n \in \mathbb{Z}_+\}.$$

If $\sqrt{I} = I$, we call it a *radical ideal*.[5]

5: Is this a Ted Kaczynski reference?

Remark 5.1.1 $\sqrt{\sqrt{I}} = \sqrt{I}$.

Example 5.1.1

(a) Let $R := \mathbb{Z}$ and $I := \langle 8 \rangle$. Then, we get $\sqrt{I} = \langle 2 \rangle$.
(b) Let $R := \mathbb{C}[x]$ and $I := \left\langle x^2(x+1) \right\rangle$. Then, $\sqrt{I} = \langle x(x+1) \rangle$.

5.2 Algebraic Varieties

Hereafter, unless otherwise stated, let $\Bbbk$ be an algebraically closed field.

Definition 5.2.1 (Affine Algebraic Variety) *An (affine) algebraic variety*[6] *is a subset $V \subseteq \Bbbk^n$ of the form*

$$V = \mathbb{V}(I) := \{a \in \Bbbk^n : f_i(\underbrace{a_1, \ldots, a_n}_{a}) = 0 \text{ for all } f_i \in I\}$$

for some subset $I \subseteq \Bbbk[x_1, \ldots, x_n]$.[7]

6: You may also see the terminnology "algebraic set." We distinguish affine when also considering projective varieties, which we may or may not cover in these notes.

7: Note that Dummit & Foote require "irreducibility" for varieties, whereas algebraic sets need not be.

All of our original examples were, in fact, varieties.

Remark 5.2.1 We can (and will) take I to be an ideal, since

$$f(x_1, \ldots, x_n) = g(x_1, \ldots, x_n) = 0 \Rightarrow (f + g)(x_1, \ldots, x_n) = 0$$

and

$$f(x_1, \ldots, x_n) = 0 \Rightarrow (f \cdot h)(x_1, \ldots, x_n) = 0$$

for all $h \in \Bbbk[x_1, \ldots, x_n]$.[8]

8: This is nice, because we get the information about individual solution sets via our operations underlying the ideal. We're being a bit sloppy with our function notation here, but it should be alright.

Proposition 5.2.1 *Let $I, J \subseteq R$ be ideals. Then,*

(i) $I \subseteq J$ *implies* $\mathbb{V}(I) \supseteq \mathbb{V}(J)$.
(ii) $\mathbb{V}(I) \cap \mathbb{V}(J) = \mathbb{V}(I \cup J) = \mathbb{V}(I + J)$.[9]
(iii) $\mathbb{V}(I) \cup \mathbb{V}(J) = \mathbb{V}(I \cap J) = \mathbb{V}(IJ)$.[10]
(iv) $\mathbb{V}(\langle 0 \rangle) = \mathbb{V}(0) = \Bbbk^n$ *and* $\mathbb{V}(\langle I \rangle) = \mathbb{V}(R) = \varnothing$.

9: Note that $I \cup J$ is not an ideal, so we rewrite as $I + J$, as that is. The variety associated to them is identical.

10: $I \cap J$ is certainly not IJ, but again, these produce the same variety.

Definition 5.2.2 ($\mathbb{I}(V)$) *Let $V \subseteq \Bbbk^n$ be an algebraic variety. Then, set*

$$\mathbb{I}(V) := \{f \in \Bbbk[x_1, \ldots, x_n] : f(a) = 0 \text{ for all } a \in V\}.$$

Proposition 5.2.2 *If U, V are varieties, then*

(i) $U \subseteq V$ *implies* $\mathbb{I}(U) \supseteq \mathbb{I}(V)$.
(ii) $\mathbb{I}(U \cup V) = \mathbb{I}(U) \cap \mathbb{I}(V)$.
(iii) $\mathbb{I}(U \cap V) \supseteq \mathbb{I}(U) + \mathbb{I}(V)$.

Proposition 5.2.3 *Let V be a variety and $I \subseteq \Bbbk[x_1, \ldots, x_n]$ be an ideal. Then,*

(i) $V = \mathbb{V}(\mathbb{I}(V))$.
(ii) $I \subseteq \mathbb{I}(\mathbb{V}(I))$.

Proof of (i). If $a \in V$, then for all $f \in \mathbb{I}(V)$, $f(a) = 0$. In particular, $a \in \mathbb{V}(\mathbb{I}(V))$. Since V is a variety, $V = \mathbb{V}(J)$ for some ideal $J \subseteq \Bbbk[x_1, \ldots, x_n]$. We must have $J \subseteq \mathbb{I}(\mathbb{V}(J)) = \mathbb{I}(V)$,[11] but then $V = \mathbb{V}(J) \supseteq \mathbb{V}(\mathbb{I}(V))$, so we have equality. □

11: This is by (ii).

That is, (i) is an equality we already know that every variety is of the form

$V = \mathbb{V}(J)$. If we know in advance that $I = \mathbb{I}(V)$, for some variety V, then $\mathbb{I}(\mathbb{V}(I)) = I$, by the same argument.

We want to figure out when we can have ideals mapping as we "want them to." This leads us back to the Nullstellensatz.

5.3 Hilbert's Nullstellensatz

We now state the strong form of Hilbert's Nullstellensatz, prove the easy direction of the statement, and then state the "second version" of the weak form as a corollary.

Theorem 5.3.1 (Nullstellensatz, strong form)

$$\mathbb{I}(\mathbb{V}(I)) = \sqrt{I} = \{f \in \Bbbk[x_1, \ldots, x_n] : f^n \in I \text{ for some } n \in \mathbb{Z}_{\geq 1}\}$$

Moreover, we have inverse bijections

$$\left\{\begin{array}{c}\text{algebraic varieties} \\ V \subseteq \Bbbk^n\end{array}\right\} \underset{\mathbb{V}}{\overset{\mathbb{I}}{\rightleftarrows}} \left\{\begin{array}{c}\text{radical ideals} \\ I \subseteq \Bbbk[x_1, \ldots, x_n]\end{array}\right\}$$

Proof of Easy Direction. If $f \in \sqrt{I}$, then $f^n \in I$ for some N. If $a \in \mathbb{V}(I)$, then $0 = f^n(a) = f(a)^n$, so $f(a) = 0$, as $\Bbbk$ is an integral domain. Hence, $f(a) = 0$ for all $a \in \mathbb{V}(I)$, so $f \in \mathbb{I}(\mathbb{V}(I))$. □

Corollary 5.3.2 (Nullstellensatz, weak form, second version) *Let $I \subseteq \Bbbk[x_1, \ldots, x_n]$ be an ideal. Then, $\mathbb{V}(I) = \varnothing$ if and only if $1 \in I$.*[12]

12: Hence, $I = \Bbbk[x_1, \ldots, x_n]$.

Note that we will actually use the weak form to prove the strong form, but in this case we take the implication in this direction so as to show how the strong form reduces down.

Proof of Weak Form Given Strong Form. By the strong form, if $\mathbb{V}(I) = \varnothing$

$$\sqrt{I} = \mathbb{I}(\mathbb{V}(I)) = \mathbb{I}(\varnothing) = \Bbbk[x_1, \ldots, x_n] \ni 1.$$

This means that $1^n \in I$ for some n, so $1 \in I$. Conversely, $\mathbb{V}(\langle 1 \rangle) = \varnothing$, by a previous proposition.[13] □

13: That is, the case for the zero variety is a special case of the general statement.

Example 5.3.1

(a) Let $\Bbbk := \mathbb{C}$ with $n = 2$.[14] Given the ideals $I := \langle x - y \rangle$ and $J := \langle x + y \rangle$. Then, $I + J = \langle x, y \rangle$, and in this case $I \cap J = IJ = \langle (x - y)(x + y) \rangle$. We get

$$\mathbb{I}(\mathbb{V}(J)) = \{f \in \mathbb{C}[x, y] : f(x, -x) = 0 \text{ for all } x\}.$$

Recall that $\Bbbk[x_1, \ldots, x_n]$ is a UFD. If $(x + y) \mid f(x, y)$, then

14: Use $\mathbb{R}$ to vizualize.

$f(x,-x)=0$, so $J \subseteq \mathbb{I}(\mathbb{V}(J))$.[15] Now,

$$\begin{aligned}\mathbb{I}(\mathbb{V}(I+J)) &= \{f \in \Bbbk[x,y] : f(0,0)=0\}\\ &= \text{ all functions without a constant term}\\ &= \langle x,y\rangle + I + J.\end{aligned}$$

(b) Take $n=1$ with $I := \langle x^2\rangle \subseteq \Bbbk[x]$. Then, $\mathbb{V}(I)=\{0\}$, so $\mathbb{I}(\mathbb{V}(I)) = \langle x\rangle = \sqrt{I} \supset I$.

15: By the Nullstellensatz,

$$J = \sqrt{J} = \mathbb{I}(\mathbb{V}(J)).$$

5.4 Prime Ideals and Irreducible Varieties

Firstly, *prime ideals* are radical, since in a prime ideal $ab \in I$ implies $a \in I$ or $b \in I$, so $a^n \in I$ implies $a \in I$.

Definition 5.4.1 (Irreducible Variety) *A variety V is irreducible*[16] *if whenever $V = V_1 \cup V_2$ for varieties V_1 and V_2, $V = V_1$ or $V = V_2$.*

16: A *reducible* variety is one which is not irreducible.

Proposition 5.4.1 *V is irreducible if and only if $I := \mathbb{I}(V)$ is prime.*

Proof. Let $f_1 f_2 \in I$. Let

$$V_i = V \cap \mathbb{V}(\langle f_i\rangle) = \mathbb{V}(I + \langle f_i\rangle) = \{a \in V : f_i(a) = 0\},$$

where $i \in [2]$.[17] Let $a \in V$. Then,

$$0 = (f_1 f_2)(a) = f_1(a) f_2(a),$$

so $f_1(a)=0$ or $f_2(a)=0$, so $a \in V_1$ or $a \in V_2$. Thus, $V = V_1 \cup V_2$. Since V is irreducible $V = V_j$ for $j \in [2]$, so $f_j(a)=0$ for all $a \in V$, so $f_j \in I$, meaning we must have that I is prime. For the converse, let $V = V_1 \cup V_2$, and assume $V_1 \subsetneq V$. This means that $\mathbb{I}(V) \subsetneq \mathbb{I}(V_1)$, since otherwise

$$V = \mathbb{V}(\mathbb{I}(V)) = \mathbb{V}(\mathbb{I}(V_1)) = V_1.$$

Let $f_1 \in \mathbb{I}(V_1) \setminus \mathbb{I}(V)$, and take $f_2 \in \mathbb{I}(V_2)$. Then, $f_1 f_2 \in \mathbb{I}(V)$, since one of f_1, f_2 is zero on every point in the union. Since $\mathbb{I}(V)$ is prime, we must have $f_2 \in \mathbb{I}(V)$.[18] Thus, $\mathbb{I}(V_2) \subseteq \mathbb{I}(V)$, so $V \subseteq V_2$, meaning $V = V_2$. □

17: We know that

$$\mathbb{V}(I) \cap \mathbb{V}(J) = \mathbb{V}(I+J)$$

and

$$\mathbb{V}(\mathbb{I}(V)) = V.$$

Here, $V = \mathbb{V}(I) = \mathbb{V}(\mathbb{I}(V))$, $J = \langle f_i\rangle$, so

$$V \cap \mathbb{V}(\langle f_i\rangle) = \mathbb{V}(I + \langle f_i\rangle).$$

18: Remember, we assumed $f_1 \notin \mathbb{I}(V)$.

Definition 5.4.2 (Noetherian Ring) *A commutative, unital ring R is Noetherian if every strictly increasing chain of ideals is finite. That is, if*

$$I_1 \subseteq I_2 \subseteq I_3 \subseteq \cdots,$$

then there exists $m \in \mathbb{Z}_+$ such that $I_k = I_m$ for all $k \geq m$.[19]

19: That is, $\boldsymbol{R}$ satisfies the *ascending chain condition*. Remember, *Artinian* rings are Noetherian, but not vice-versa.

Theorem 5.4.2 (Hilbert's Basis Theorem) *$\Bbbk[x_1,\ldots,x_n]$ is Noetherian.*[20]

20: See Dummit & Foote Section 9.6 for a proof using "leading coefficients."

Proposition 5.4.3 *Any variety $V \subseteq \Bbbk^n$ is a finite union of irreducible varieties.*

Proof. Suppose otherwise. Since V is reducible, we can write

$$V = \underbrace{V_1 \cup W_1}_{V_1, W_1 \subsetneq V}.$$

One of V_1, W_1 must be reducible. Without loss of generality, let $V_1 = V_2 \cup W_2$ with $V_2, W_2 \subsetneq V_1$.[21] Continuing in this manner, we have

$$V = V_0 \supsetneq V_1 \supseteq V_2 \supseteq V_3 \supseteq \cdots,$$

and letting $I_i = \mathbb{I}(V_i)$, we get

$$I_0 \subsetneq I_1 \subsetneq I_1 \subsetneq I_2 \subsetneq \cdots,$$

by the standard reverse inclusion. How do we know that we do not have equality? Well, we know

$$\mathbb{V}(I_i) = V_i \supseteq V_{i+1} = \mathbb{V}(I_{i+1}).$$

Hence, since $\Bbbk[x_1, \ldots, x_n]$ is Noetherian,[22] this is impossible. □

21: As before, the strictness of this inclusion is vital.

22: This is where we cite Hilbert's Basis Theorem.

What about *maximal ideals*? It turns out, they have an even *nicer* characterization:

$$\text{maximal ideals} \subseteq \text{prime ideals} \subseteq \text{radical ideals}.$$

For $a \in \Bbbk^n$, let

$$\mathbb{I}(a) := \mathbb{I}(\{a\}) = \{f \in \Bbbk[x_1, \ldots, x_n] : f(a) = 0\}.$$

Lemma 5.4.4

(i) $\mathbb{I}(a) = \langle x_1 - a_1, \ldots, x_n - a_n \rangle =: J$ *if* $a = \langle a_1, \ldots, a_n \rangle$.
(ii) $\mathbb{I}(a)$ *is maximal.*

Proof. Firstly, $J \subseteq \mathbb{I}(a)$, so we will prove that J is a maximal ideal. Notice that Under the quotient map

$$\Bbbk[x_1, \ldots, x_n] \to {}^{\Bbbk[x_1, \ldots, x_n]}/_{J},$$

we have $p(x) \mapsto p(a) \in \Bbbk$, so

$${}^{\Bbbk[x_1, \ldots, x_n]}/_{J} \cong \Bbbk,$$

a field. Thus, $J = \mathbb{I}(a)$ is maximal.

□

Proposition 5.4.5 *Every maximal ideal is of the form $\mathbb{I}(a)$ for some $a \in \Bbbk^n$.*

Proof for $|\Bbbk| > \aleph_0$. Let $I \subseteq \Bbbk[x_1, \ldots, x_n]$ be a maximal ideal, and let

$$\mathbb{F} := {}^{\Bbbk[x_1,\ldots,x_n]}\!/_{I}.$$

We know $\Bbbk \subseteq \mathbb{F}$, since $\Bbbk \cap I = \{0\}$, so either $\mathbb{F} = \Bbbk$ or $\mathbb{F}$ is a transcendental extension of $\Bbbk$. In the former case,

$$I = \mathbb{I}(a) = \mathbb{I}(\langle a_1, \ldots, a_n \rangle),$$

where $x_i \mapsto a_i$. In the latter case,[23] $\dim_{\Bbbk} \mathbb{F}$ is *at most* countable since $\dim_{\Bbbk} \Bbbk[x_1, \ldots, x_n]$ is countable, and the quotient map is a vector space homomorphism. On the other hand, let $t \in \mathbb{F}$ be transcendental over $\Bbbk$. Now,

$$\left\{ \frac{1}{t-a} : a \in \Bbbk \right\}$$

is an uncountable, linearly independent set,[24] a contradiction.

23: This is where we need $|\Bbbk| > \aleph_0$.

24: We prove this claim directly below.

□

Proof of Claim. If

$$\frac{c_1}{t-a_1} + \cdots + \frac{c_n}{t-a_n} = 0,$$

where $c_1, \ldots, c_n \in \Bbbk$, then

$$c_1(t-a_2)\cdots(t-a_n) + \cdots + c_n(t-a_1)\cdots(t-a_{n-1}) = 0,$$

and setting $t = a_i$ shows that each $c_i = 0$. □

Proof of Weak Nullstellensatz. Note that every proper ideal I is contained in a maximal ideal $\mathbb{I}(a)$.[25] If $\mathbb{V}(I) = \varnothing$, then $\mathbb{V}(\mathbb{I}(a)) = \varnothing$, but this contradicts the fact that $\mathbb{V}(\mathbb{I}(a)) = \{a\}$. □

25: We do not need Zorn's lemma since the ring is Noetherian.

Proof of Strong Nullstellensatz. We have previously demonstrated that $\sqrt{I} \subseteq \mathbb{I}(\mathbb{V}(I))$. Since $\Bbbk[x_1, \ldots, x_n]$ is Noetherian,[26] I is finitely generated. That is, $I = \langle f_1, \ldots, f_m \rangle$. Let $g \in \mathbb{I}(\mathbb{V}(I))$. We introduce a new variable x_{n+1} and consider

$$I' := \langle f_1, \ldots, f_n, x_{n+1}g - 1 \rangle \subseteq \Bbbk[x_1, \ldots, x_{n+1}].$$

For any $a \in \Bbbk^{n+1}$, if

$$f_1(a) = \cdots = f_n(a) = 0,$$

then it certainly holds that $g(a) = 0$,[27] so $a_{n+1}g(a) - 1 \neq 0$, meaning $\mathbb{V}(I') = \varnothing$. By the weak form of the Nullstellensatz, $1 \in I'$, so

$$1 = h_1 f_1 + \cdots + h_m f_m + h_{m+1}(x_{n+1}g - 1)$$

for some $h_i \in \Bbbk[x_1, \ldots, x_{n+1}]$. Let $y = x_{n+1}^{-1}$ and multiply by y^N:[28]

$$y^n = p_1 f_1 + \cdots + p_m f_m + p_{m+1}(g - y),$$

for some $p_i \in \Bbbk[x_1, \ldots, x_n, y]$. Plug in $y = g$:

$$g^N = \tilde{p_1} f_1 + \cdots + \tilde{p_m} f_m \in I \subseteq \Bbbk[x_1, \ldots, x_n],$$

26: This is given by Hilbert.

27: $g \in \mathbb{I}(\mathbb{V}(I))$.

28: We take $N \gg 0$.

where

$$\tilde{p}_i(x_1, \ldots, x_n) := p_1(x_1 m \ldots, x_n, g) \in \Bbbk[x_1, \ldots, x_n],$$

so $g \in \sqrt{I}$, meaning $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$. □

5.5 Coordinate Rings

We now briefly discuss *coordinate rings*, of which some qualities can be deduced trivially based on the work we have done already.

Definition 5.5.1 (Coordinate Ring) *The coordinate ring of a variety V is*

$$\Bbbk[V] := \{f : V \to \Bbbk : f = g\big|_V \text{ for some } g \in \Bbbk[x_1, \ldots, x_n]\}.$$

That is,

$$\Bbbk[V] = {}^{\Bbbk[x_1, \ldots, x_n]}/_{\mathbb{I}(V)},$$

as $\mathbb{I}(V)$ is $\ker \Psi$ of the ring homomorphism

$$\Bbbk[x_1, \ldots, x_n] \xrightarrow{\quad\Psi\quad} \Bbbk[V].$$

Corollary 5.5.1

(i) V is irreducible if and only if $\Bbbk[V]$ is an integral domain.
(ii) V is a point if and only if $\Bbbk[V] \cong \Bbbk$.
(iii) For any variety V,

$$\{\text{points in } V\} \xleftrightarrow{\text{bijection}} \{\text{maximal ideals in } \Bbbk[V]\}.$$

(i) *Proof.* We know that V is irreducible if and only if $\mathbb{I}(V)$ is prime, which holds if and only if $\Bbbk[V] = {}^{\Bbbk[x_1, \ldots, x_n]}/_I$ is an integral domain. □

(ii) *Proof.* We have preciously shown that V is a point if and only if $\mathbb{I}(V)$ is maximal. Of course, $\mathbb{I}(V)$ is maximal if the quotient $\Bbbk[V] = {}^{\Bbbk[x_1, \ldots, x_n]}/_I$ is a field.[29] □

29: We must have that this field is isomorphic to $\Bbbk$, as we know $I = \mathbb{I}(a)$ for some $a \in \Bbbk$.

(iii) *Proof.* By the fourth ring isomorphism theorem, given a ring R and an ideal I, there is a bijection

$$\{\text{ideals in } R \text{ containing } I\} \xleftrightarrow{\text{bijection}} \{\text{ideals in } {}^R/_I\}.$$

Since maximality is preserved under this bijection, the weak Nullstellensatz gives us the proof. □

6 Projective Spaces and Varieties

6.1 Projective Space $\mathbb{C}\mathbf{P}^n$

Recall, per Bézout's Theorem, the "usual" situation is that two polynomials in $\mathbb{C}[x, y]$ of degrees m and n have mn intersection points in $\mathbb{C}$.[1]

1: This is including multiplicity.

Well, what about parallel lines? Then,

$$(\deg L)(\deg M) = 1 \cdot 1 = 1,$$

but L and M do not intersect. One fix is to add points "at ∞" where parallel lines meet. Consider equivalence classes of lines under parallelism.[2]

2: That is, each equivalence class consists of all lines of a given slope.

Definition 6.1.1 (Complex Projective Space v.1) *The (complex) projective plane is the set*

$$\widetilde{\mathbb{C}\mathbf{P}^2} := \mathbb{C}^2 \cup \underbrace{\left\{ \begin{matrix} \textit{one point "at" } \infty \textit{ for} \\ \textit{each equivalence class of lines} \end{matrix} \right\}}_{H_\infty}.$$

Well, this "works," but it is a weird definition.[3] Let us define *homogenous coordinates* in $\mathbb{C}^3$. We say that two points in $\mathbb{C}^3$ are equivalent

3: We are going to work and prove a different defintion is equivalent.

$$(a_0, a_1, a_2) \sim (b_0, b_1, b_2)$$

if and only if

$$(b_0, b_1, b_2) = (\lambda a_0, \lambda a_1, \lambda a_2)$$

for some $\lambda \in \mathbb{C}^\times$.[4] That is, if $a, b \in \mathbb{C}^3$ are nonzero, then $a \sim b$ if and only if a and b are on the same line through the origin in $\mathbb{C}^3$. We denote equivalence classes by

$$[a_0 : a_1 : a_2].$$

4: That is, the ratios are all the same. For instance,

$$\frac{a_0}{a_1} = \frac{b_0}{b_1},$$

and so forth.

Definition 6.1.2 (Complex Projective Space v.2) *The (complex) projective plane is the set of equivalence classes*[5]

$$\mathbb{C}\mathbf{P}^2 := \mathbb{C}^{3\times}/\sim.$$

5: That is, the set of one-dimensional linear subspaces of $\mathbb{C}^3$.

Proposition 6.1.1 *There exists a "nice" bijection*

$$\mathbb{C}\mathbf{P}^2 \to \widetilde{\mathbb{C}\mathbf{P}^2}.$$

Proof. We write that[6]

$$\mathbb{C}\mathbf{P}^2 = \underbrace{\{[1 : x : y]\}}_{S_1} \sqcup \underbrace{\{[0 : 1 : y]\}}_{S_2} \sqcup \underbrace{\{[0 : 0 : 1]\}}_{S_3}.$$

6: We have $x, y \in \mathbb{C}$ arbitrarily. Note that S_j is not *at all* the j-sphere. We are just denoting sets.

Then,

$$S_1 \to \mathbb{C}^2 : [1 : x : y] \mapsto (x, y)$$

is a bijection. Let $a_m \in H_\infty$, and let $m \in \mathbb{C} \cup \{\infty\}$ be the equivalence class of lines in $\mathbb{C}^2$ of slope m. Then,

$$S_2 \sqcup S_3 \to H_\infty : \begin{Bmatrix} [0 : 1 : m] \\ [0 : 0 : 1] \end{Bmatrix} \mapsto \begin{Bmatrix} a_m \\ a_\infty \end{Bmatrix}$$

is a bijection. □

We can now define arbitrary complex projective spaces.

Definition 6.1.3 (Complex Projective Space)

$$\begin{aligned} \mathbb{CP}^n &:= \{\textit{lines through origin in } \mathbb{C}^{n+1}\} \\ &= \{a \in \mathbb{C}^{n+1\times}\}/(a \sim \lambda a, \lambda \in \mathbb{C}^\times) \\ &= \{[a_0 : a_1 : \cdots : a_n]\}. \end{aligned}$$

Corollary 6.1.2 $\mathbb{CP}^n = \mathbb{C}^n \cup \mathbb{CP}^{n-1}$.

Proof. Use the maps from the previous proposition:[7]

$$[1 : a_1 : \cdots : a_n] \mapsto (a_1, \ldots, a_n) \in \mathbb{C}^n$$

and

$$[0 : a_1 : \cdots : a_n] \mapsto [a_1 : \cdots : a_n] \in \mathbb{CP}^{n-1},$$

so we are done. □

7: Note that

$$\underbrace{[a_1 : \cdots : a_n] \in \mathbb{CP}^{n-1}}_{\text{not all } 0}.$$

Example 6.1.1 Consider $\mathbb{CP}^1$.[8] We can write

$$\begin{aligned} \mathbb{CP}^1 &= \{\text{lines in } \mathbb{C}^2\} = \{[x : y]\} \\ &= \{[1 : m] : m \in \mathbb{C}\} \cup \{[0 : 1]\}. \end{aligned}$$

8: This is the "projective line." This is also called the "Riemann sphere."

6.2 Projective Varieties and Homogenous Polynomials

We want to define *projective varieties* in $\mathbb{CP}^n$. Let $f(x, y, z) := xy - z$. Then, $f(1, 1, 1) = 0$ and $f(2, 2, 2) = 2$, so $f([1 : 1 : 1])$ is undefined![9] It turns out, our problem was that when we scaled the variables, we doubled z but quadrupled xy.[10]

Definition 6.2.1 (Homgenous Polynomial) *We define* $f(x_0, \ldots, x_n) \in \mathbb{C}[x_0, \ldots, x_n]$ *to be homogenous of degree* d *if every term has total degree* d.

Notice that if f is homogenous of degree d, then

$$f(\lambda a_0, \ldots, \lambda a_n) = \lambda^d f(a_0, \ldots, a_n).$$

9: In case you did not notice, $0 \neq 2$.

10: We will look at a fix where we only look at a particular subset of

$$\mathbb{C}[x_1, \ldots, x_n].$$

If $\lambda \neq 0$, $f(\lambda a_0, \dots, \lambda a_n) = 0$ if and only if $f(a_0, \dots, a_n) = 0$.[11]

11: Thus, we can just choose any representative and use this criterion to determine if f is zeroed.

Definition 6.2.2 (Projective Variety of Polynomial) *If $f \in \mathbb{C}[x_0, \dots, x_n]$ is homogenous, then we define*

$$\mathbb{V}(f) := \{[a_0 : \cdots : a_n] \in \mathbb{CP}^n : f(a_0, \dots, a_n) = 0\}$$

to be the projective variety corresponding to f.[12]

12: This is well-defined by the prior notes.

Note that *no* nonzero ideal consists of *only* homogenous polynomials. Write[13]

13: This is a graded ring.

$$\mathbb{C}[x_0, \dots, x_n] = \bigoplus_{d=0}^{\infty} A_d,$$

as an additive group, where

$$A_d := \{f \in \mathbb{C}[x_0, \dots, x_n] : f \text{ hom. of degree } d\}.$$

Hence, any $f \in \mathbb{C}[x_0, \dots, x_n]$ can be written *uniquely* in the form[14]

14: The f_d are the "graded pieces."

$$f = f_0 + f_1 + f_2 + \cdots + f_k \quad \text{where } f_d \in A_d.$$

Definition 6.2.3 (Homogenous Ideal) *An ideal $I \subseteq \mathbb{C}[x_0, \dots, x_n]$ is homogenous if $f \in I$ implies $f_d \in I$ for all d.*[15]

15: This is equivalent to saying that I has a generating set consisting only of homogenous polynomials.

Example 6.2.1 Take $\mathbb{C}[x, y]$. The ideal $I := \langle x + y, x^2 + y^2 \rangle$ is homogenous, even when its written as

$$I = \langle x + y, x + y + x^2 + y^2 \rangle.$$

On the other hand, $J := \langle y - x^2 \rangle$ is not homogenous.

Definition 6.2.4 (Projective Variety of Ideal) *Let $I \subseteq \mathbb{C}[x_0, \dots, x_n]$ be a homogenous ideal. Then, the projective variety associated to I is*

$$\begin{aligned}\mathbb{V}(I) &:= \{a = [a_0 : \cdots : a_n] \in \mathbb{CP}^n : f(a) = 0\} \\ &= \mathbb{V}(f^{(1)}) \cap \cdots \cap \mathbb{V}(f^{(k)})\end{aligned}$$

for all $f \in I$.[16]

16: We take $f^{(i)}$ to be homogenous and

$$I = \langle f^{(1)}, \dots, f^{(k)} \rangle.$$

Proposition 6.2.1

$$\mathbb{I}(V) := \{f \in \mathbb{C}[x_0, \dots, x_n] : f(a) = 0\}$$

for all $a \in V$, is a homogenous ideal.

Proposition 6.2.2 *If I is homogenous, then $\sqrt{I}$ is homogenous.*

We have now built up the framework to state, and mostly prove, the *Projective Nullstellensatz.*[17]

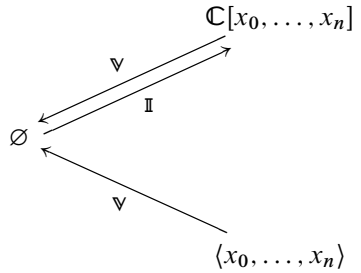
17: This is moslty stated in analogue of the affine case, with a few tweaks to make our projective charactersitics work.

Theorem 6.2.3 (Projective Nullstellensatz) *We have inverse bijections*

$$\left\{\begin{array}{c}\textit{nonempty}\\ \textit{projective varieties}\\ V \subseteq \mathbb{C}\mathbf{P}^n\end{array}\right\} \underset{\mathbb{V}}{\overset{\mathbb{I}}{\rightleftarrows}} \left\{\begin{array}{c}\textit{radical}\\ \textit{homogenous ideals}\\ I \subsetneq \langle x_0, \ldots, x_n\rangle\end{array}\right\}.$$

For these varieties and ideals, $\mathbb{V}(\mathbb{I}(V)) = V$ *and* $\mathbb{I}(\mathbb{V}(I)) = \sqrt{I}$.

What about $\varnothing$? Well, $\mathbb{I}(\varnothing) = \mathbb{C}[x_0, \ldots, x_n]$, $\mathbb{V}(\mathbb{C}[x_0, \ldots, x_n]) = \varnothing$. Yet, $\mathbb{V}(\langle x_0, \ldots, x_n\rangle) = \{\text{pts. in } \mathbb{C}\mathbf{P}^n : x_0 = \cdots = x_n = 0\} = \varnothing$.



Furthermore,

$$\left\{\begin{array}{c}\text{irreducible}\\ \text{nonempty}\\ \text{projective varieties}\end{array}\right\} \underset{\mathbb{V}}{\overset{\mathbb{I}}{\rightleftarrows}} \left\{\begin{array}{c}\text{prime}\\ \text{homogenous ideals}\\ I \subsetneq \langle x_0, \ldots, x_n\rangle\end{array}\right\}$$

and

$$\left\{\begin{array}{c}\text{points}\\ a = [a_0 : \cdots : a_n]\end{array}\right\} \underset{\mathbb{V}}{\overset{\mathbb{I}}{\rightleftarrows}} \left\{\begin{array}{c}\text{maximal homogenous ideals}\\ \mathbb{I}(a) = \left(\dfrac{x_i}{a_i} - \dfrac{x_j}{a_j} : 0 \le i, j \le n\right)\end{array}\right\}.$$

Sketch of Proof. Let I be a homogenous ideal $\subsetneq \langle x_0, \ldots, x_n\rangle$ and let $V := \mathbb{V}(I)$. Let[18]

$$V' := \{a \in \mathbb{C}^{n+1} : f(a) = 0 \text{ for all } f \in I\}.$$

By the affine Nullstellensatz, $\mathbb{I}(V') = \sqrt{I}$. We have

$$(a_0, \ldots, a_n) \in V'^{\times} \iff [a_0 : \cdots : a_n] \in V,$$

so $\sqrt{I} = \mathbb{I}(V') \subseteq \mathbb{I}(V)$. Conversely, if f is homogenous and *non-constant*,[19] we always have $f(0) = 0$, so $f \in \mathbb{I}(V)$ implies $f(a) = 0$ for all $a \in V$, which means $f(a) = 0$ for all $a \in V'$. Hence, $f \in \mathbb{I}(V') = \sqrt{I}$. The rest of the statement of the projective Nullstellensatz follows by similar arguments to the affine case. □

18: This is precisely the *affine* variety corresponding to the same ideal I. We are going to do some legwork, then the rest of the proof follows by the logic of the proof of the "standard" variety.

19: This has to be the case, otherwise the ideal is the whole ring.