Review of modern algebra

October 4, 2022

Contents

Preface

This note is written to help anyone who reviews undergraduate algebra. Thus, it is highly recommended to study undergraduate algebra at least once before reading this note, for most of details will not be introduced in this note. Also, some sections are not written yet, because I haven't studied them.

Part I

Ring theory

Chapter 1

Basic ring theory

1.1 Basic ideal theory

Proposition 1.1.1. Let R be a ring and assume A and B are ideals of R. Define two subsets $A+B$ and AB of R as follows:

(1) $A+B := \{x+y : x \in A,\, y \in B\}$.

(2) AB is defined as the collection of finite sums of elements of the form ab with $a \in A$ and $b \in B$.

Then both $A+B$ and AB are ideals of R. In fact, one can prove the following statements: For $I,\ J \trianglelefteq R$,

(a) $I+J$ is the smallest ideal of R containing I and J.

(b) $I \cap J$ is the largest ideal of R contained in $I \cap J$.

(c) IJ is an ideal of R contained in $I \cap J$.

(d) Assume that R is a commutative ring with the nonzero identity. If I and J are comaximal, i.e., $I+J=R$, then $IJ = I \cap J$. In general, if $I_1, I_2, \cdots, I_n$ are pairwise comaximal ideals of R, then $I_1 I_2 \cdots I_n = \bigcap_{i=1}^{n} I_i$.

Proof. Checking from (a) to (c) is left as an exercise. To prove (d), assume that R is a commutative ring with the nonzero identity. Because I and J are assumed to be comaximal, there are elements $a \in I$ and $b \in J$ such that $a+b=1$. Thus, if $x \in I \cap J$, then $x = 1x = (a+b)x = ax + xb \in IJ$, as desired. The generalized case will be explained when proving the Chinese remainder theorem. □

Proposition 1.1.2. Let R be a ring and A be a nonempty subset of R.

(a) RAR is an ideal of R.

(b) Assume that R contains the nonzero identity. Then RAR is the smallest ideal of R containing A, i.e., $(A) = RAR$.

Proof. (a) can be easily justified if one notes that $ras \times r'a's' = tasr' \times a' \times s' \in RAR$ for all $r, r', s, s' \in R$ and $a, a' \in A$. To prove (b), assume R is a ring with the nonzero identity. Clearly, RAR is an ideal of R containing A. If I is an ideal of R containing A, then RAR is contained in I by definition, so $(A) = RAR$. □

Observation 1.1.3. Let R be a commutative ring and let A and B be finitely generated ideals of R given by $A = (a_1, \cdots, a_m)$ and $B = (b_1, \cdots, b_n)$. One can easily check that $AB = (a_i b_j : 1 \leq i \leq m, 1 \leq j \leq n)$.

Proposition 1.1.4. Let R be a ring with the nonzero identity, and let I be an ideal of R.

(a) $I = R$ if and only if I contains a unit of R.

(b) Assume that R is commutative. Then R is a field if and only if its only ideals are 0 and R. Hence, a ring homomorphism from a field is either injective or trivial.

Definition 1.1.5. Let R be a ring.

(a) A proper ideal M of R is called a maximal ideal if I is an ideal of R containing M then $I = M$ or $I = R$.

(b) A proper ideal P of R is called a prime ideal if $ab \in P$ implies $a \in P$ or $b \in P$.

Proposition 1.1.6. Let R be a ring with the nonzero identity. Then R has a maximal ideal.

Proof. We try to apply Zorn's lemma to prove this statement.

Step 1. Setting a nonempty partially ordered subset.

Let X be a collection of all proper ideals of R. Then X is nonempty and partially ordered by set inclusion.

Step 2. Checking the upper bound axiom.

Let $\mathcal{C}$ be any ascending chain in X, and let U be the union of the members of $\mathcal{C}$. Our goal in this step is to prove that U is an upper bound of the the chain $\mathcal{C}$ in X, and for this it suffices to show that $U \in X$, i.e., U is a proper ideal of R.

Since U is a union of ideals in the chain $\mathcal{C}$, U is an ideal of R. If $U = R$, then U contains the identity, which implies that there is a member of $\mathcal{C}$ which contains the identity, a contradiction. Hence, $U \in X$ and U is an upper bound of $\mathcal{C}$.

Step 3. Deriving desired results.

Therefore, by Zorn's lemma, X has a maximal element M. And it is clear that a maximal element of X is a maximal ideal of R. □

Remark. Slightly modifying the proof, one can prove that every proper ideal of R is contained in a maximal ideal of R or that there is a maximal ideal of R containing $a \in R$ whenever a is a nonunit element of R.

Properties of maximal ideals and prime ideals are given as follows:

Proposition 1.1.7. Let R be a ring with the nonzero identity, and suppose I is an ideal of R.

(a) I is a maximal ideal of R if and only if R/I is a field.

(b) I is a prime ideal of R if and only if R/I is an integral domain.

1.2 Field of fractions

Throughout this section, D is an integral domain.

Define a relation $\sim$ on $Y_D := D \times (D \setminus \{0\})$ by $(a, b) \sim (c, d)$ if and only if $ad - bc = 0$. (Explain why the relation is an equivalence relation on Y_D.) And let $[a/b]$ denote the equivalence class of (a, b) in $Q_D := Y_D/\sim$. Also, define the addition and the multiplication on $Y_D/\sim$ as follows:

$$[a/b] + [c/d] := [(ad + bc)/bd], \quad [a/b] \times [c/d] := [ac/bd].$$

Theorem 1.2.1. Q_D is a field, and the map $\jmath : D \to Q_D$ defined by $\jmath(a) = [a/1]$ for $a \in D$ is a ring monomorphism. In fact, if D is a field, then $\jmath$ is a field isomorphism.

According to the preceeding theorem, we may identify D as a subset or a subring of Q_D. Hence, we may also write $[a/b] = [a/1][1/b] = \jmath(a)\jmath(b)^{-1} = ab^{-1}$ for all $a, b \in D$ with $b \neq 0$.

Together with the ring monomorphism $\jmath : D \hookrightarrow Q_D$, Q_D satisfies the following universal property:

Theorem 1.2.2 (A universal property of the field of fractions $(Q_D, \jmath : D \hookrightarrow Q_D)$). For any monomorphism $\imath : D \hookrightarrow F$ of the integral domain D into a ring F, there is a unique field monomorphism $\imath_* : Q_D \hookrightarrow F$ such that $\imath_* \circ \jmath = \imath$.

$$\begin{tikzcd}
D \arrow[r, hook, "\jmath"] \arrow[dr, "\imath\text{(ring mono.)}"'] & Q_D \arrow[d, hook, dashed, "\imath_*"] \\
& F
\end{tikzcd}$$

Proof. Given an embedding $\imath$ of the integral domain D into a field F, define

$$\imath_*[a/b] := \imath(a)\imath(b)^{-1} \quad (a \in D, b \in D \setminus \{0\}).$$

Once it is proved that $\imath_*$ is a well-defined map, it can easily be seen that $\imath_*$ is a field homomorphism which is injective and that $\imath_* \circ \jmath = \imath$. □

1.3 Chinese remainder theorem for rings

Throughout this section, unless stated otherwise, all rings are assumed to be commutative and have the nonzero identity.

Remark. In this section, applying comaximality appropriately is essential, and the key propositions are as follows: For a commutative ring R with the nonzero identity and comaximal ideals A and B,

(a) $A \cap B = AB$.

(b) The map $\phi : R \to R/A \times R/B$ defined by $\phi(r) = (r + A, r + B)$ for $r \in R$ is a ring epimorphism. Thus, by the first isomorphism theorem, $R/AB = R/(A \cap B) \approx R/A \times R/B$.

The above two propositions will be a lot helpful not only when proving the Chinese remainder theorem but also when solving some relevant problems.

Theorem 1.3.1 (Chinese remainder theorem)**.** Let R be a commutative ring with the nonzero identity, and suppose that $A_1, \cdots, A_n$ be pairwise comaximal ideals of R. Then $A_1 \cdot \cdots \cdot A_n = \bigcap_{i=1}^n A_i$, so we have the following isomorphism of rings:

$$\frac{R}{A_1 \cdot \cdots \cdot A_n} \approx \frac{R}{A_1} \times \cdots \times \frac{R}{A_n}.$$

Proof. We prove the theorem by induction on n.

Step 1. Proof for $n = 2$.

When $n = 2$, since A_1 and A_2 are comaximal, $A_1A_2 = A_1 \cap A_2$ and there are elements $a \in A_1$ and $b \in A_2$ such that $a + b = 1$. Hence, the ring homomorphism $\phi : R \to R/A_1 \times R/A_2$ defined by $\phi(x) = (x + A_1, x + A_2)$ for $x \in R$ is surjective, since $\phi(xb + ya) = (x + A_1, y + A_2)$. The desired result follows from the first isomorphism theorem.

Step 2. Generalization.

What we want to show is the following two statements:

(a) $A_1 \cdot \cdots \cdot A_n = \bigcap_{i=1}^n A_i$.

(b) The ring homomorphism $\phi : R \to R/A_1 \times \cdots \times R/A_n$ defined by $\phi(x) = (x + A_1, \cdots, x + A_n)$ for $x \in R$ is surjective.

We prove (a) by induction; we assume the equation holds for $(n-1)$-pairwise comaximal ideals. For each $i = 1, \cdots, n-1$, let $a_i \in A_i$ and $b_i \in A_n$ be elements such that $a_i + b_i = 1$. Because

$$1 = (a_1 + b_1) \cdots (a_{n-1} + b_{n-1}) = a_1 \cdot \cdots \cdot a_{n-1} + \star$$

with $\star := 1 - (a_1 + b_1) \cdots (a_{n-1} + b_{n-1}) \in A_n$ and $a_1 \cdot \cdots \cdot a_{n-1} \in A_1 \cdot \cdots \cdot A_{n-1}$, we find that $A_1 \cdots A_{n-1}$ and A_n are comaximal. Therefore, $\bigcap_{i=1}^n A_i = A_1 \cdot \cdots \cdot A_n$, as desired.

To prove (b), it suffices to find $x_i \in R$ for each $i = 1, \cdots, n$ such that

$$x_i \equiv 1 \text{ mod } A_i \text{ and } x_i \equiv 0 \text{ mod } A_j \text{ whenever } j \neq i.$$

And for this, it suffices to find $x_i \in R$ for each i such that

$$x_i \equiv 1 \text{ mod } A_i \text{ and } x_i \equiv 0 \text{ mod } B_i,$$

where $B_i = \bigcap_{j \neq i} A_j$; such x_i indeed exists for each i, since A_i and B_i are comaximal as found in the preceeding paragraph. □

Example 1.3.2 (Ideals of product rings)**.** Suppose R and S are commutative rings with respective nonzero identities. We will justify that every ideal of $R \times S$ is of the form $I \times J$, where $I \trianglelefteq R$ and $J \trianglelefteq S$.

Suppose $A \trianglelefteq R \times S$, and let $\pi_1 : R \times S \to R$ and $\pi_2 : R \times S \to S$ be the natural projections.

$$\text{Goal: To prove that } A = \pi_1(A) \times \pi_2(A).$$

To prove the goal, it suffice to prove that $\pi_1(A) \times \pi_2(A) \subset A$. Choose a point $(p, q) \in \pi_1(A) \times \pi_2(A)$ and let $x \in R$ and $y \in S$ be elements such that $(p, y), (x, q) \in A$. Then it easily follows that $(p, q) = (1, 0)(p, y) + (0, 1)(x, q) \in A$, as desired.

1.4 Noetherian ring

Definition 1.4.1 (Noetherian ring)**.** Let R be a ring (not necessarily an integral domain). Then the followings are equivalent, and a ring satisfying any of the following property is called a Noetherian ring.

(a) (Finite condition) Every ideal of R is finitely generated.

(b) (Ascending chain condition) Every ascending chain of ideals of R is finite. To be precise, if $I_1, I_2, \cdots$ are ideals of R such that $I_1 \subset I_2 \subset \cdots$, then there is an integer $n \in \mathbb{N}$ such that $I_j = I - k$ for all $j, k \geq n$.

(c) (Maximal condition) Let S be any nonempty collection of ideals of R partially ordered by set inclusion. Then S contains a maximal member.

Remark. Every principal ideal domain is a Noetherian ring, since it satisfies the finite conditon.

Proof. We first prove that the finite condition implies the ascending chain condition. Let $I_1 \subset I_2 \subset \cdots$ be an ascending chain of ideals of R, and define

$$I = \bigcup_{n=1}^{\infty} I_n.$$

One can easily check that I is an ideal of R. By hypothesis, $I = (a_1, \cdots, a_k)$ for some $a_1, \cdots, a_k \in R$; because, for each i, $a_i \in I_j$ for some $j \in \mathbb{N}$, the ascending chain is finite.

We now prove that the ascending chain condition implies the maximal condition. Let S be a nonempty collection of ideals of R and partially order S by set inclusion. Choose a member I_1 of S; if I_1 is maximal, the proof is done. If I_1 is not maximal, there is another member I_2 of S strictly containing I_1. By induction, given a non-maximal member I_n of S, there is another member I_{n+1} of S strictly containing I_n. Because the ascending chain $I_1 \subset I_2 \subset \cdots$ is finite by hypothesis, there is an integer n such that I_n is maximal, which proves that S contains a maximal member. (Hence, in this case, we did not have to apply Zorn's lemma.)

Finally, we prove that the maximal condition implies the finite condition. Define the collection S of ideals of R by

$$S := \{J \trianglelefteq R : J \subset I \text{ and } J \text{ is finitely generated}\}.$$

By hypothesis, S contains a maximal member M. We will show that $I = M$ by contradiction. Assume $M \subsetneq I$. Then there is an element $x \in I \setminus M$, thus $M \subsetneq (M, x) \subset I$. Because (M, x) is also finitely generated, $(M, x) \in S$, so M is not a maximal member of S, a contradiction. □

Chapter 2

Types of integral domains

Throughout this chapter, all rings are assumed to be integral domains, unless stated otherwise. Also, unless stated otherwise, D denotes an integral domain.

2.1 Multiples and divisors

The idea of multiples and divisors are assumed to be considered in integral domains. Throughout this section, D denotes an integral domain.

Definition 2.1.1 (Multiple and divisor). Let a and b be elements of D. If there is $c \in D$ such that $a = bc$, then a is called a multiple of b (and b is called a divisor of a). If $d \in D$ is a divisor of both a and b, then d is called a common divisor of a and b; if $m \in D$ is a multiple of both a and b, then m is called a common multiple of a and b.

Assume $a_1, \cdots, a_n \in D$. Then an element $d \in D$ is called a greatest common divisor of $a_1, \cdots, a_n$ if

(1) d is a common divisor of $a_1, \cdots, a_n$ and

(2) d is a multiple of every common divisor of $a_1, \cdots, a_n$.

Also, an element $l \in D$ is called a least common multiple of $a_1, \cdots, a_n$ if

(3) l is a common multiple of $a_1, \cdots, a_n$ and

(4) l is a divisor of every common multiple of $a_1, \cdots, a_n$.

We say a and b are relatively prime if (a) and (b) are comaximal, i.e., $(a, b) = (a) + (b) = D$.

To illustrate properties of multiple and divisor in terms of ideals, we define an equivalence relation $\sim$ on D as follows:

For $a, b \in D$, $a \sim_\times b$ if and only if $a = ub$ for some $u \in D^\times$.

Observation 2.1.2. Suppose $a, b \in D$.

(a) a is a divisor of b if and only if $(b) \trianglelefteq (a) \trianglelefteq R$. Thus, $a \sim_\times b$ if and only if $(a) = (b)$, and $(u) = D$ whenever u is a unit of D. Note that $(a) = (b)$ if and only if a divides b and b divides a.

(b) $a \sim_\times 0$ if and only if $a = 0$; assuming $a \in D^\times$, $a \sim_\times b$ if and only if $b \in D^\times$.

(c) Suppose $x_1, \cdots, x_n \in D$ and $a \sim_\times b$. If a is a common divisor (or a common multiple, respectively) of $x_1, \cdots, x_n$, then so is b.

Proposition 2.1.3. Suppose $a, b \in D$.

(a) $(a) + (b) = (a, b)$

(b) $(a)(b) = (ab)$.

Proposition 2.1.4. Suppose $x_1, \cdots, x_n \in D$. Then $d \in D$ is a greatest common divisor of $x_1, \cdots, x_n$ if and only if $(x_1, \cdots, x_n) \trianglelefteq (d) \trianglelefteq (d')$ whenever $d' \in D$ is a common divisor of $x_1, \cdots, c_n$; $m \in D$ is a least common multiple of $x_1, \cdots, x_n$ if and only if $(m') \trianglelefteq (m) \trianglelefteq (x_1) \cap \cdots \cap (x_n)$ whenever $m' \in D$ is a common multiple of $x_1, \cdots, x_n$. Also, a greatest common divisor and a least common multiple of $x_1, \cdots, x_n$ are unique up to multiplication by a unit in D, respectively.

We end this section with an observation on principal ideal domains.

Observation 2.1.5. Let D be a principal ideal domain and $a, b \in D$. If we let $(a) + (b) = (x)$, then x is a greatest common divisor of a and b, and vice versa. Similarly, if we let $(a) \cap (b) = (y)$, then y is a least common multiple of a and b, and vice versa.

2.2 Irreducible elements and prime elements

Definition 2.2.1. Let D be an integral domain.

(a) (Irreducible element) A nonzero and nonunit element $r \in D$ is called an irreducible element if r satisfies the following property:

If $r = ab$ for some $a, b \in D$, either a or b is a unit in D.

(b) (Prime element) A nonzero and nonunit element $p \in D$ is called a prime element if p satisfies the following property:

If $p|ab$ for some $a, b \in D$, then $p|a$ or $p|b$.

The above statement is equivalent to the following statement:

If $ab \in (p)$ for some $a, b \in D$, then $a \in (p)$ or $b \in (p)$.

Hence, a nonzero and nonunit element p of D is a prime element if and only if (p) is a prime ideal of D.

Observation 2.2.2. Suppose x, y are nonzero and nonunit elements of D and assume $x \sim_\times y$. Then y is an irreducible (a prime, respectively) element of D if x is an irreducible (a prime) element of D.

Proof. Write $y = ux$ for some unit u in D, and assume first that x is irreducible. Whenever $y = ab$ for some $a, b \in D$, because $x = u^{-1}ab$ and x is irreducible, $u^{-1}a$ or b is a unit in D, implying that a or b is a unit in D. Now assume that x is a prime element. Then y is clearly a prime element, since $(x) = (y)$. □

Proposition 2.2.3. A prime element is an irreducible element.

Proof. Let p be a prime element of the integral domain D, and write $p = ab$ with $a, b \in D$. Without loss of generality, we may assume that $a \in (p)$, i.e., $a = px$ for some $x \in D$; from $p = pxb$, we have $b \in D^\times$ as desired. □

Remark. Later in this chapter, it will be proved that a Euclidean domain is a principal ideal domain. Since any integral domain contains a maximal ideal, every Euclidean domain (or a principal ideal domain) contains a prime element and an irreducible element.

We end this section with a simple property satisfied in any integral domain.

Observation 2.2.4 (Factorization of elements of integral domains). Let D be an integral domain and r be a nonzero and nonunit element of D. Then there clearly exist elements $a_1, a_2 \in D$ such that $r = a_1a_2$. If r is irreducible, then either a_1 or a_2 is a unit in D; if r is reducible, then a_1, a_2 can be chosen to be (nonzero and) nonunit. (What if not?)

2.3 Euclidean domain

Definition 2.3.1 (Size function and Euclidean domain)**.** Let D be an integral domain. Any function $N : D \to \mathbb{Z}^{>0}$ such that $N(0) = 0$ is called a size function on D. The integral domain D is called a Euclidean domain if it has a size funciton N on D satisfying the following property:

For any $a, b \in D$ with $b \neq 0$, there are $q, r \in D$ such that $a = qb + r$ with either $r = 0$ or $N(r) < N(b)$.

Example 2.3.2. Fields, the Gaussian integer ring $\mathbb{Z}[i]$ are Euclidean domains.

Theorem 2.3.3. Euclidean domains are principal ideal domains.

Proof. Let D be a Euclidean domain and I be an ideal of D. By the well-ordering principle of $\mathbb{N}$, there is a nonzero element α of I with the smallest value of a size function on D. If $x \in I$, there are elements $q, r \in D$ such that $x = q\alpha + r$ with either $r = 0$ or $N(r) < N(\alpha)$. Because $r = x - q\alpha$, r is an element of I, which forces $r = 0$ and $x = q\alpha$. Therefore, $I = (\alpha)$, proving that D is a principal ideal domain. □

2.4 Principal ideal domain

Definition 2.4.1 (Principal ideal domain)**.** An integral domain in which every ideal is principal is called a principal ideal domain.

Remark. Let D be a principal ideal domain and $a, b \in D$. Write $(a, b) = (x)$ and $(a) \cap (b) = (y)$. Then, x is a greatest common divisor of a and b, and y is a least common multiple of a and b, which exist uniquely up to multiplication by units in D, respectively.

Theorem 2.4.2. In principal ideal domains, nonzero prime ideals and nonzero maximal ideals coincide.

Proof. It suffices to prove that any nonzero prime ideal of a prinicpal ideal D is a maximal ideal of D. Let $P = (p)$ be a nonzero prime ideal of D, and suppose $P \leq I \trianglelefteq D$ with $I = (a)$ for some $a \in D$. Since $p \in (a)$, $p = ab$ for some $b \in D$. Because p is a prime element of D, we have $p|a$ or $p|b$, which, respectively, implies $I = P$ or $a \in D^\times$ so that $I = D$. Therefore, every nonzero prime ideal of D is a maximal ideal of D. □

We have observed that in any integral domain a prime element is an irreducible element and that nonzero prime ideals and nonzero maximal ideals coincide in principal ideal domains. The following theorem states some equivalences in principal ideal domains.

Theorem 2.4.3 (Equivalences in principal ideal domains)**.** Let D be a principal ideal domain and p be a nonzero element of D. Then the followings are equivalent:

(a) p is a prime element of D.

(b) p is an irreducible element of D.

(c) (p) is a prime ideal of D.

(d) (p) is a maximal ideal of D.

Proof. (a) and (c) are verified to be equivalent when we defined prime elements; we have proved that (c) and (d) are equivalent; we have proved that (a) implies (b). Thus, it remains to prove that (b) implies any other statement; here, we will show that (b) implies (d).

Suppose $(p) \leq I \trianglelefteq D$ and write $I = (a)$. We can write $p = ab$ for some $b \in D$, thus a or b is a unit in D, which, respectively, implies that $I = D$ or $I = P$, implying that (p) is a maximal ideal of D. □

2.5 Unique factorization domain

Definition 2.5.1 (Unique factorization domain)**.** An integral domain D is called a unique factorization domain if every nonzero and nonunit element r of D satisfies the following properties:

(a) r can be written as a finite product of irreducible elements of D.

(b) The decomposition in (a) is unique ip to multiplication by units; if $r = p_1 p_2 \cdots p_m = q_1 q_2 \cdots q_n$, where $m, n \in \mathbb{N}$ and p_i and q_j for $1 \leq i \leq m, 1 \leq j \leq n$ are irreducible elements of D, then $m = n$ and $p_i \sim_\times q_i$ for each i.

We have studied the following equivalences valid in principal ideal domains:

(a) p is a prime element of D.

(b) p is an irreducible element of D.

(c) (p) is a prime ideal of D.

(d) (p) is a maximal ideal of D.

Among them, (a) and (c) are equivalent by definition, (a) implies (b) and (d) implies (c) in any integral domain. In UFDs, a nonzero prime ideal is no longer necessarily a maximal ideal; howerver, an irreducible element is still a prime element.

Proposition 2.5.2. In a UFD, an irreducible element is a prime element.

Proof. Let r be an irreducible element of a UFD D and assume $r|ab$ for some nonzero elements a, b of D. Then r is an irreducible factor of ab and an irreducible factor of a or b. Therefore, $r|a$ or $r|b$ and r is a prime element. □

In the following observation, some obvious but helpful properties of unique factor domains are listed.

Observation 2.5.3. Let D be a UFD. Suppose that $a = u{p_1}^{r_1}{p_2}^{r_2} \cdots {p_n}^{r_n} \in D$, where $u \in D^\times$, p_i is an irreducible element of D and $r_i \in \mathbb{N}$ for each i.

(a) If p is an irreducible element of D dividing a, then $a \sim_\times p_i$ for some i. Hence, if d is an element of D dividing a, then $d \sim_\times {p_1}^{f_1}{p_2}^{f_2} \cdots {p_n}^{f_n}$, where $0 \leq f_i \leq r_i$ for each i.

Suppose further that $b = v{p_1}^{s_1}{p_2}^{s_2} \cdots {p_n}^{s_n} \in D$, where $v \in D^\times$, p_i is an irreducible element of D and $s_i \in \mathbb{N}$ for each i.

(b) Letting $e_i = \min\{r_i, s_i\}$ and $f_i = \max\{r_i, s_i\}$ for each i, ${p_1}^{e_1}{p_2}^{e_2} \cdots {p_n}^{e_n}$ is a greatest common divisor of a and b, and ${p_1}^{f_1}{p_2}^{f_2} \cdots {p_n}^{f_n}$ is a least common multiple of a and b.

(c) Hence, if g is a greatest common divisor and l is a least common multiple of a and b, respectively, then $gl \sim_\times ab$. Also, if a and b are nonzero, then $(l/a, l/b) = (a/g, b/g) = D$.

In the remaining of this seciton, we will prove that a principal ideal domain is a UFD. In the proof, given a nonzero and nonunit element a from a principal ideal domain D, we should factorize r into irreducible elements. For this, we should investigate the existence of an irreducible element of D dividing a; for this, it suffices to prove the existence of a prime (or a maximal) ideal of D containing a, which is already proved in the preceeding chapter.

Theorem 2.5.4. Every principal ideal domain is a UFD.

Proof. Let D be a principal ideal domain and let a be a nonzero and nonunit element of D.

Step 1. Proving the existence part

Note that whenever $c \in D$ is nonzero and nonunit, there is a maximal ideal of D containing c. If a is reducible, find a maximal ideal (r_1) of D containing a and write $a = r_1 a_1$; if a_1 is reducible, find an irreducible element r_2 of D dividing a_1 and write $a_1 = r_2 a_2$. By induction, when a_n is reducible, let r_{n+1}

be an irreducible element of D dividing a_n and write $a_n = r_{n+1}a_{n+1}$. We will justify that such process terminates in finite steps so that a_n is irreducible for some $n \in \mathbb{N}$. Assume that a_n is not irreducible for all n. Because each r_n is nonunit, we have a properly ascending chain $(a) \subsetneq (a_1) \subsetneq (a_2) \subsetneq \cdots$ of ideals of D. Since a principal ideal domain is a Noetherian ring, the ascending chain is finite, i.e., $(a_n) = (a_{n+1}) = \cdots$ for some integer $n \in \mathbb{N}$, a contradiction. Therefore, whenever a is a nonzero and nonunit element of D, then one can find a factorization of a into irreducible elements of D.

Step 2. Proving the uniqueness part
The uniqueness part can be proved by induction. Assume that a has the following two factorizations into irreducible elements of D:

$$a = up_1 \cdots p_m \text{ and } a = vq_1 \cdots q_n,$$

where $u, v \in D^\times$ and p_i's and q_j's are irreducible elements of D for all i and j. (Without loss of generality, assume that $m \leq n$.) Since $p_1|(q_1 \cdots q_n)$ and p_1 is a prime element of D, (after renumbering we can write) $p_1|q_1$ so that $p_1 \sim_\times q_1$. (How?) By the same argument, we have (again, after renumbering) $p_i \sim_\times q_i$ for each i. Hence, if $m < n$, by the law of cancellation, $q_{m+1} \cdots q_n \sim_\times 1$, a contradiction. Therefore, $m = n$ and $p_i \sim_\times q_i$ for each i.

By Step 1 and Step 2, every principal ideal domain is a UFD. □

2.6 The Gaussian integer ring

2.6.1 Quotients of the Gaussian integer ring

Observation 2.6.1. If I is a nonzero ideal of $\mathbb{Z}[i]$, the quotient ring $\mathbb{Z}[i]/I$ is a finite ring. To be precise, letting $I = (\alpha)$, the order of $\mathbb{Z}[i]/I$ is at most $|\alpha|^2$.

Proof. Write $I = (\alpha)$ for some $\alpha \in \mathbb{Z}[i]$. Every element of $\mathbb{Z}[i]/I$ can be uniquely written in the form of $\overline{a+bi}\,(a, b \in \mathbb{Z})$ with $a \in \mathbb{Z}[i]$ and $a^2 + b^2 < |\alpha|^2$ by the division algorithm. Because there are finitely many Gaussian integers of modulus smaller than $|\alpha|$, the quotient ring $\mathbb{Z}[i]/I$ is finite. □

Proposition 2.6.2. Let p be a prime number.

(a) If $p \equiv 3$ mod 4, then $\mathbb{Z}[i]/(p)$ is isomorphic to the field of order p^2.

(b) If $p \equiv 1$ mod 4, then $p = \pi\overline{\pi}$ for some irreducible element $\pi \in \mathbb{Z}[i]$. Because (π) and $(\overline{\pi})$ are comaximal, by the Chinese remainder theorem,

$$\frac{\mathbb{Z}[i]}{(p)} \approx \frac{\mathbb{Z}[i]}{(\pi)} \times \frac{\mathbb{Z}[i]}{(\overline{\pi})}.$$

Proof. We first prove (a). Since p is a prime element of $\mathbb{Z}[i]$, the quotient ring is a field of characteristic p. Suppose that $a, b, x, y \in \mathbb{Z}$. Then $a + bi \equiv x + yi$ mod p if and only if $a \equiv x$ and $b \equiv y$ mod p, thus the order of the quotient ring is p^2.

We now prove (b). To show that (π) and $(\overline{\pi})$ are comaximal,it suffices to prove that $\overline{\pi} \neq (\pi)$; the maximality of (π) will prove the comaximality. Assuming $\overline{\pi} \in (\pi)$, we have $\alpha\overline{\pi} = \pi$ for some $\alpha \in \mathbb{Z}[i]$ with $|\alpha| = 1$. Writing $\pi = a + bi$ for some $a, b \in \mathbb{Z}$,

(1) When $\alpha = 1$, we have $a + bi = a - bi$ so that $b = 0$ and $p = a^2$.

(2) When $\alpha = -1$, we have $-a - bi = a - bi$ so that $a = 0$ and $p = b^2$.

(3) When $\alpha = i$, we have $-b + ai = a - bi$ so that $a = -b$ and $p = 2a^2$.

(4) When $\alpha = -i$, we hace $b - ai = a - bi$ so that $a = b$ and $p = 2a^2$.

In either of the above cases, p is not a prime number, a contradiction. Hence, (π) and $(\overline{\pi})$ are comaximal and the Chinese remainder theorem holds. □

Theorem 2.6.3. $|\mathbb{Z}[i]/(\alpha)| = |\alpha|^2$, where α is a nonzero element of $\mathbb{Z}[i]$.

Chapter 3

Polynomial rings

Throughout this chapter, we assume that R is a commutative ring with the nonzero identity and that D is an integral domain.

3.1 Basic properties

Definition 3.1.1 (Polynomial rings)**.** Let R be a commutative ring with the nonzero identity. The set $R[x]$ is defined as the collection of functions $f : \mathbb{Z}^{\geq 0} \to R$ with an integer $n \in \mathbb{Z}$ such that $f(k) = 0$ whenever $k \geq n$. Polynomial rings with multiple indeterminates are defined inductively: $R[x_1, \cdots, x_n] := R[x_1, \cdots, x_{n-1}][x_n]$. Imposing the usual operations on $R[x]$, $R[x]$ becomes a commutative ring with the nonzero identity.

Proposition 3.1.2 (A universal property of polynomial rings)**.** Let R be a commutative ring with the nonzero identity. Let $\phi : R \to S$ be a ring homomorphism and let θ be an element of S. Then there is a unique ring homomorphism $\phi_* : R[x] \to S$ which extends ϕ and maps x to θ.

$$\begin{tikzcd}
R \arrow[r, hook, "\imath"] \arrow[dr, "\phi"'] & R[x] \arrow[d, dashed, "\phi_*: x\mapsto\theta"] \\
& S
\end{tikzcd}$$

Proof. If such ϕ_* exists, then it should be satisfied that

$$\phi_*\left(\sum_{r=0}^{n} a_r x^r\right) = \sum_{r=0}^{n} a_r \theta^r.$$

Checking details are left to readers. □

A simple proposition follows.

Proposition 3.1.3. Let I be an ideal of R and let (I) be the ideal of $R[x]$ generated by I, i.e., $(I) = R[x]I = I[x]$. Then $R[x]/(I) \approx (R/I)[x]$. In particular, if I is a prime ideal of R, then (I) is a prime ideal of $R[x]$.

Proof. Consider the projection map $f : R[x] \to (R/I)[x]$ defined by

$$f\left(\sum_{r=0}^{n} a_r x^r\right) = \sum_{r=0}^{n} \overline{a_r} x^r.$$

Checking details are left to readers. □

Another simple, but important, proposition follows.

Theorem 3.1.4 (Division algorithm on polynomial rings over fields)**.** Let F be a field and impose the following division algorithm on $F[x]$:

$$\text{Given } a(x), b(x) \in F[x] \text{ with } b(x) \neq 0, \text{ find } q(x), r(x) \in F[x] \text{ such that}$$

$$a(x) = q(x)b(x) + r(x),$$

$$\text{where either } r(x) = 0 \text{ or } \mathit{deg}\, r(x) < \mathit{deg}\, b(x).$$

(a) For each pair of $a(x)$ and $b(x)$, such $q(x)$ and $r(x)$ exist uniquely, respectively.

(b) Hence, $F[x]$ is a Euclidean domain.

Remark. By the uniqueness part, when E is a field extension of F and $a(x) = Q(x)b(x) + R(x)$ for some $Q(x), R(x) \in E[x]$ with $R(x) = 0$ or $\mathit{deg}\, R(x) < \mathit{deg}\, b(x)$, we have $Q(x) = q(x)$ and $R(x) = r(x)$.

Proof. We prove the assertion by induction on $\mathit{deg}\, a(x)$. (By removing the leading term of $a(x)$, the case is reduced to the case which is assumed by the induction hypothesis, proving the existence part.) To prove the uniqueness part, assume $a(x) = q_1(x)b(x) + r_1(x) = q_2(x)b(x) + r_2(x)$ for some $q_i(x), r_i(x) \in F[x]$ with $r_i(x) = 0$ or $\mathit{deg}\, r_i(x) < \mathit{deg}\, b(x)$ for $i = 1, 2$. Because $r_1(x) - r_2(x) = (q_2(x) - q_1(x))b(x)$, considering the degrees of the polynomials, the uniqueness part can easily be explained. □

Corollary 3.1.5. Let F be a field and $f(x)$ be a nonzero and nonunit element of $F[x]$. Because $F[x]$ is a Euclidean domain, $(f(x))$ is a maximal ideal of $F[x]$ if and only if $f(x)$ is an irreducible element of $F[x]$, i.e., $f(x)$ is an irreducible polynomial. Therefore, $F[x]/(f(x))$ is a field if and only if $f(x)$ is irreducible.

Corollary 3.1.6. Let F be a field and $p(x)$ be a polynomial over F. By the lattice isomorphism theorem, the ideals of $F[x]/(p(x))$ and the ideals of $F[x]$ containing $(p(x))$ are in bijection. Also, an ideal of $F[x]$ containing $(p(x))$ is of the form $(a(x))$ for some $a(x) \in F[x]$ with $a(x)|p(x)$ and vice versa. Therefore, the ideals of $F[x]/(p(x))$ are of the form $ol(a(x))$ with $a(x)|p(x)$ and vice versa.

Problem 3.1.1. Let F be a field and $R = F[x, x^2y, x^3y^2, \cdots, x^{n+1}y^n, \cdots] \trianglelefteq F[x, y]$.

(a) Show that the field of fractions of R and $F[x, y]$ are the same.

(b) Explain why R contains an ideal which is not finitely generated.

Solution. (a) Clearly, the field Q_R of fractions of R is contained in the field Q of fractions of $F[x, y]$. Conversely, if $f(x, y) \in F[x, y]$, for some large integer N, we have $x^N f(x, y) \in R$, thus Q is contained in Q_R.

(b) Consider the following ascending chain $(x) \subsetneq (x, x^2y) \subsetneq (x, x^2y, x^3y^2) \subsetneq \cdots$ of ideals of R. If R does not contain an infinitely generated ideal, then R does not contain an infinite ascending chain of ideals, being a Noetherian ring.

Problem 3.1.2. Prove that $(x^i - y^j)$ is a prime ideal of $R[x, y]$, whenever i and j are relatively prime positive integers.

Solution. Note from $R[x, y] = R[x][y]$ that every polynomial in $R[x, y]$ differs by a polynomial in $(x^i - y^j)$ by a polynomial in $R[x, y]$ with degree in y less than j. In other words, given $a(x, y) \in R[x, y]$, there are $q(x, y), r(x, y) \in R[x, y]$ such that $a(x, y) = (x^i - y^j)q(x, y) + r(x, y)$ with $\mathit{deg}_y r(x, y) < j$.

Define a ring homomorphism $f : R[x, y] \to R[s]$ extending the identity map on R by

$$f(x) = s^j, \quad f(y) = s^i.$$

Then $f(a(x, y)) = f(r(x, y))$, so

$$f(a(x, y)) = k_0(s^j) + s^i k_1(s^j) + \cdots + s^{(j-1)i} k_{j-1}(s^j),$$

where

$$r(x,y) = k_0(x) + k_1(x)y + \cdots + k_{j-1}(x)y^{j-1} \quad (k_0(x),\, k_1(x),\, \cdots,\, k_{j-1}(x) \in R[x]).$$

Because i and j are relatively prime, the above summation is a partition of $f(r(x,y))$ regarding degree of each monomial in s modulo j. In other words, all monomials in each summand $s^{mi}k_m(s^j)\,(m = 0,1,\cdots,j-1)$ has the same degree modulo j, and any two monomials in two other summands have distinct degree modulo j. Therefore, $f(a(x,y)) = 0$ if and only if $k_0(x) = k_1(x) = \cdots = k_{j-1}(x) = 0$, i.e., $a(x,y) \in \mathit{ker} f$ if and only if $a(x,y) \in (x^i - y^j)$. By the first isomorphism theorem, we have $R[x,y]/(x^i - y^j) \approx R[s]$, so $(x^i - y^j)$ is a prime ideal of $R[x,y]$.

3.2 Gauss's lemmas

Our goal in this section is to prove that $D[x]$ is a UFD if D is a UFD. Throughout this section, D is an integral domain and Q is the field of fractions of D.

Definition 3.2.1 (Content of a polynomial)**.** Let D be an integral domain and $f(x) = a_nx^n + \cdots + a_1x + a_0$ be a polynomial over D. A greatest common divisor of $a_0, a_1, \cdots, a_n$ is called a content of f, and is denoted by *cont*(f). If *cont*(f) is a unit in D, then the polynomial f is called a primitive polynomial.

Some obvious observations:

Observation 3.2.2. (a) If $p(x) \in D[x]$ is a nonzero polynomial, then there is a primitive polynomial $p_1(x)$ over D such that $p(x) = \mathit{cont}(p) \cdot p_1(x)$.

Suppose $a, b \in D$ and $f(x), g(x) \in D[x]$ are nonzero and primitive polynomials.

(b) *cont*$(af) = a$.

(c) If $af(x) = bg(x)$, then $a \sim_\times b$.

Example 3.2.3. If $p(x) \in D[x]$ is a nonconstant irreducible polynomial, then $p(x)$ is primitive.

Theorem 3.2.4 (Gauss's lemma of primitivity)**.** Let D be a UFD and $f(x), g(x)$ be polynomials over D.

(a) *cont*$(fg) =$ *cont*$(f) \cdot$ *cont*(g)

(b) Hence, if $f(x)$ and $g(x)$ are primitive, then so is $f(x)g(x)$.

Proof. Since (b) follows from (a), it suffices to prove (a). Because $f(x) = \mathit{cont}(f) \cdot f_1(x)$ and $g(x) = \mathit{cont}(g) \cdot g_1(x)$ for some primitive polynomials $f_1(x), g_1(x) \in D[x]$, it suffices to prove that $f_1(x)g_1(x)$ is a primitive polynomial over D. For this, assume that $f_1(x)g_1(x)$ is not primitive and let p be a prime element of D dividing *cont*(f_1g_1). Consider the map $\phi : D[x] \to D[x]/(p)$ defined by

$$\phi\left(\sum_{r=0}^{n} a_rx^r\right) = \sum_{r=0}^{n} \overline{a_r}x^r \quad (a_r \in D \text{ for each } r).$$

Note that $D[x]/(p) \approx (D/pD)[x]$ is an integral domain and $\phi(f_1(x)g_1(x)) = 0$, and that ϕ is a ring homomorphism. Thus, without loss of generality, we may assume that $\phi(f_1(x)) = 0$, implying that p divides $f_1(x)$, which contradicts the primitivity of f_1. Therefore, $f_1(x)g_1(x)$ is primitive. □

Corollary 3.2.5. Let D be a UFD, and suppose that $p(x)$ is a nonzero polynomial over D. Then $p(x)$ is reducible in $D[x]$ if $p(x)$ is reducible in $Q[x]$. (To be precise, if $p(x) = A(x)B(x)$ for some $A(x), B(x) \in Q[x]$, then there are elements $s, t \in Q$ such that $a(x) := sA(x)$ and $b(x) := tB(x)$ belong to $D[x]$ and $p(x) = a(x)b(x)$. Hence, there exist $a(x), b(x) \in D[x]$ such that $p(x) = a(x)b(x)$ and $\mathit{deg}\, a = \mathit{deg}\, A$ and $\mathit{deg}\, b = \mathit{deg}\, B$.)

Proof. Because $p(x)$ is reducible over Q, we can write $p(x) = A(x)B(x)$ for some (nonconstant polynomials) $A(x), B(x) \in Q[x]$. By reducing fractions, we can write $A(x) = \dfrac{c}{m}a(x)$ and $B(x) = \dfrac{d}{n}b(x)$ for some primitive polynomials $a(x), b(x)$ over D and $c, d, m, n \in D$ with $m, n \neq 0$. Writing $p(x) = \textit{cont}(p) \cdot p_1(x)$ with $p_1(x) \in D[x]$ being primitive, we have $mn \cdot \textit{cont}(p) \cdot p_1(x) = cd \cdot a(x)b(x)$, hence $mn \cdot \textit{cont}(p) \sim_\times cd$, i.e., $p(x) \sim_\times \textit{cont}(p) \cdot a(x)b(x)$. This proves the desired statements. □

Theorem 3.2.6 (Gauss's lemma of irreducibility)**.** Let D be a UFD and Q be the field of fractions of D. Assume that $p(x)$ is a primitive polynomial over D. Then $p(x)$ is irreducible over D if and only if $p(x)$ is irreducible over Q.

Proof. We first assume that $p(x)$ is irreducible over D and let $a(x), b(x)$ be polynomials over Q such that $p(x) = a(x)b(x)$. By reducing fractions, we may write $a(x) = \dfrac{c}{m}a_0(x)$ and $b(x) = \dfrac{d}{n}b_0(x)$, where $c, d, m, n \in D \setminus \{0\}$ and $a_0(x), b_0(x)$ are primitive polynomials over D. Because $mn \cdot p(x) = cd \cdot a_0(x)b_0(x)$ and $p(x)$ is primitive, we have $mn \sim_\times cd$, so $p(x) \sim_\times a_0(x)b_0(x)$. Because $p(x)$ is irreducible over D, either $a_0(x)$ or $b_0(x)$ is a unit in $D[x]$, so either $a_0(x)$ or $b_0(x)$ is a constant polynomial. This proves that $p(x)$ is irreducible over Q.

We now assume that $p(x)$ is irreducible over Q and let $a(x), b(x)$ be polynomials over D such that $p(x) = a(x)b(x)$. Then, without loss of generality, $a(x) \in Q[x]^\times = Q$, thus $a(x)$ is a constant polynomial over D. Becasue $p(x)$ is primitive, we find that $a(x) \in D^\times$, priving that $p(x)$ is irreducible over D. □

Corollary 3.2.7. Let D be a UFD and $f(x), g(x)$ be primitive polynomials over D. Then $f(x) \sim_\times g(x)$ in $D[x]$ if and only if $f(x) \sim_\times g(x)$ in $Q[x]$.

Proof. It is clear that $f(x) \sim_\times g(x)$ in $Q[x]$ if $f(x) \sim_\times g(x)$ in $D[x]$. Assume conversely that $f(x) \sim_\times g(x)$ in $Q[x]$ so that we can write $f(x) = (b/a)g(x)$ for some $b/a \in Q[x]^\times = Q^\times$. Since both $f(x)$ and $g(x)$ are primitive and $af(x) = bg(x)$, we have $a \sim_\times b$, so $b/a \in D^\times$. Therefore, $f(x) \sim_\times g(x)$ in $D[x]$. □

Remark (Review of Gauss's lemmas)*.* Let D be a UFD and Q be the field of fractions of D. Gauss's lemma of primitivity implies that any finite product of primitive polynomials over D is primitive. Gauss's lemma of irreduciblity implies the followings:

(a) A polynomial $p(x)$ over D is reducible over D if it is reducible over Q.

(b) Let $p(x)$ be a primitive polynomial over D. Then $p(x)$ is irreducible over D if and only if $p(x)$ is irreducible over Q.

Theorem 3.2.8. If D is a UFD, then so is $D[x]$.

Proof. Let $f(x)$ be a nonzero and nonunit polynomial over D.

Step 1. Proving the existence part

Let $f_1(x)$ be the polynomial over D such that $f(x) = \textit{cont}(f) \cdot f_1(x)$. The factorization of $\textit{cont}(f)$ cen be accomplished in D. To factorize $f_1(x)$ in $D[x]$, we first factorize $f_1(x)$ in a UFD $Q[x]$; write $f_1(x) = p_1(x) \cdot \cdots \cdot p_n(x)$ be the factorization of $f_1(x)$ in $Q[x]$. By reducing fractions, for each $i = 1, \cdots, n$, there is a primitive polynomial $q_i(x)$ over D and $a_i, b_i \in D \setminus \{0\}$ such that $p_i(x) = (b_i/a_i)q_i(x)$.

(1) Since each $p_i(x)$ is irreducible over Q, each $q_i(x)$ is also irreducible over Q, and so over D.

(2) Because $(a_1 \cdot \cdots \cdot a_n)f_1(x) = (b_1 \cdot \cdots \cdot b_n) \cdot q_1(x) \cdot \cdots \cdot q_n(x)$, we have $a_1 \cdot \cdots \cdot a_n \sim_\times b_1 \cdot \cdots \cdot b_n$.

Therefore, $f(x) = \textit{cont}(f) \cdot f_1(x) \sim_\times \textit{cont}(f) \cdot q_1(x) \cdot \cdots \cdot q_n(x)$ has a factorization into irreducible elements in $D[x]$.

Step 2. Proving the uniqueness part

Suppose that two factorization of $f(x)$ into irreducible elements in $D[x]$ are given as follows:

$$f(x) = (r_1 \cdot \cdots \cdot r_m) \cdot a_1(x) \cdot \cdots \cdot a_j(x) = (s_1 \cdot \cdots \cdot s_n) \cdot b_1(x) \cdot \cdots \cdot b_k(x),$$

where $r_1, \cdots, d_m, s_1, \cdots, s_n$ are irreducible elements of D and $a_1(x), \cdots, a_j(x), b_1(x), b_k(x)$ are irreducible polynomials in $D[x]$. (Being primitive, all nonconstant polynomial factors can be assumed to be primitive.)

In this case, $r_1 \cdot \cdots \cdot r_m$ and $s_1 \cdot \cdots \cdot s_n$ are the content of the polynomial $f(x)$, so they differ by multiplication by a unit; hence, $m = n$ and $r_i \sim_\times s$ for each i. Because $a_1(x), \cdots, a_j(x), b_1(x), \cdots, b_k(x)$ are primitive and irreducible over D, they are irreducible over Q; because $Q[x]$ is a UFD, $j = k$ and (up to renumbering) $a_i(x) \sim_\times b_i(x)$ for each i. This proves the uniqueness part. □

An additional problem, which is not essential when studying further theory.

Problem 3.2.1. Suppose that $f(x), g(x) \in D[x]$ are primitive. Explain that if $f(x) = g(x)h(x)$ for some $h(x) \in Q[x]$ then $h(x)$ is a polynomial over D.

Solution. By reducing fractions, we can write $h(x) = \dfrac{b}{a}h_0(x)$ for some $a, b \in D \setminus \{0\}$ and a primitive polynomial $h_0(x)$ over D. From $af(x) = bg(x)h_0(x)$, we obtain $a \sim_\times b$ so $u = b/a \in D^\times$. Therefore, $h(x) = uh_0(x) \in D[x]$, as desired.

Chapter 4

Further ring theory

4.1 The field of real numbers

In this section, we construct the field of real numbers. Keep in mind that we do not admit the existence of the field of real numbers yet.

Let $\mathcal{C}_{\mathbb{Q}}$ denote the collection of all Cauchy sequences of rational numbers and define operations as follows:

$$(a_n)_n + (b_n) := (a_n + b_n)_n, \quad c \cdot (a_n)_n := (ca_n)_n, \quad (a_n) \times (b_n) := (a_n b_n).$$

Checking well-definedness is left as an exercise. Then $\mathcal{C}_{\mathbb{Q}}$ is a $\mathbb{Q}$-algebra with the above operations and has the multiplicative identity $(1)_n$.

For a sequence $(a_n)_n$ of rational numbers and a rational number α, $(a_n)_n$ is said to converge to α if there is a rational number α with the following property:

Whenever $\epsilon > 0$, there is a positive integer N such that $n \geq N$ implies $|a_n - \alpha| < \epsilon$.

And let $\mathcal{M}$ denote the collection of all rational sequences which converges to 0.

Proposition 4.1.1. $\mathcal{M}$ is a maximal ideal of $\mathcal{C}_{\mathbb{Q}}$. Therefore, the quotient ring $\mathcal{C}_{\mathbb{Q}}/\mathcal{M}$ is a field containing an isomorphic copy of $\mathbb{Q}$.

Proof. It is easy to justify that $\mathcal{M}$ is an ideal of $\mathcal{C}_{\mathbb{Q}}$.

To show that $\mathcal{M}$ is a maximal ideal of $\mathcal{C}_{\mathbb{Q}}$, suppose that $(a_n)_n \in \mathcal{C}_{\mathbb{Q}} \setminus \mathcal{M}$. Set

$$x_n = \begin{cases} 10^{-n} & (a_n \neq 10^{-n}) \\ 0 & (a_n = 10^{-n}) \end{cases},$$

then $(x_n)_n \in \mathcal{M}$ and $(a_n - x_n)_n \in \mathcal{C}_{\mathbb{Q}}$ and $a_n - x_n \neq 0$ for all n. Because $((a_n - x_n)^{-1})_n \in \mathcal{C}_{\mathbb{Q}}$, $(1)_n = ((a_n - x_n)^{-1})_n \times (a_n - x_n)_n \in \mathcal{C}_{\mathbb{Q}}$.

Finally, it can be easily justified that $\mathcal{C}_{\mathbb{Q}}/M$ is a field containing an isomorphic copy of $\mathbb{Q}$ by considering the field embedding $\mu : \mathbb{Q} \hookrightarrow \mathcal{C}_{\mathbb{Q}}$ defined by $\mu(1) = \overline{(1)_n}$. □

Definition 4.1.2. (a) In the remaining of this section, we define $\mathbb{R} = \mathcal{C}_{\mathbb{Q}}/\mathcal{M}$.

(b) An element $\alpha \in \mathbb{R}$ is defined to be not less than 0 if there is a rational sequence $(a_n)_n$ such that $\alpha = \overline{(a_n)_n}$ and $a_n \geq 0$ for all n.

Proposition 4.1.3. Suppose that $\alpha, \beta \in \mathbb{R}$. Show the followings.

(a) Either $\alpha > \beta$ or $\alpha = \beta$ or $\alpha < \beta$, and not simultaneously.

(b) If $\alpha, \beta > 0$, then $\alpha + \beta, \alpha\beta > 0$.

Proof. Almost clear. □

Given $\alpha = \overline{(a_n)_n} \in \mathbb{R}$, let $|\alpha| := \overline{(|a_n|)_n}$. This induces the natural metric d on $\mathbb{R}$.

Theorem 4.1.4. $(\mathbb{R}, d)$ is a complete metric space.

Proof. Somebody proved the theorem. □

4.2 Limits and inverse limits

Part II

Field theory

Chapter 5

Basic field theory

5.1 Field extensions

What you basically need to know: field extensions, algebraic elements, algebraic extensions.

Observation 5.1.1 (Basic observations on field compositions). For a field F and a set S, $F(S)$ is defined to be the smallest field containing $F \cup S$, i.e., $F(S)$ is the intersection of all fields containing $F \cup S$. (For composition of infinitely many fields, see Observation 6.2.8.)

Suppose that E and F are subfields of a field K. Then $E(F) = F(E)$, because both of them are the smallest subfield of K containing $E \cup F$. (Hence, it does not matter to write EF in place of $E(F)$.) Moreover,

$$EF = \left\{ \frac{\alpha_1'\beta_1' + \cdots + \alpha_n'\beta_n'}{\alpha_1\beta_1 + \cdots + \alpha_m\beta_m} : m, n \in \mathbb{Z}^{>0}, \text{ and } \alpha_i, \alpha_j' \in E \text{ and } \beta_i, \beta_j' \in F \text{ for all } i, j \right\}. \tag{5.1}$$

(i) Since EF is the smallest subfield of K containing $E \cup F$, EF necessarily contains all fractional elements as illustrated in eq. (5.1).

(ii) Conversely, the collection suggested in eq. (5.1) is a field containing $E \cup F$.

By (i) and (ii), eq. (5.1) holds.

Now, assume that E/F is a field extension and $\alpha, \beta \in E$. Then there is an obvious equivalence:

$$(F(\alpha))(\beta) = F(\alpha, \beta) = (F(\beta))(\alpha) = F(\alpha)F(\beta).$$

The first three naturally coincides (the third also coincides by symmetry), because

(1) $(F(\alpha))(\beta)$ is the smallest field containing $F(\alpha) \cup \{\beta\}$, so it clearly contains $F(\alpha, \beta)$, the smallest field containing $F \cup (\alpha, \beta)$.

(2) $F(\alpha, \beta)$ is the smallest field containing $F \cup \{\alpha, \beta\}$, so it contains $(F(\alpha))(\beta)$, the smallest field containing $F(\alpha) \cup \{\beta\}$.

In short, the first two coincides since both are the smallest fields containing $F \cup \{\alpha, \beta\}$. To show that the fourth also coincides the first three, note that $F(\alpha)F(\beta)$ contains $F(\alpha) \cup F(\beta)$ and that $F(\alpha, \beta)$ contains $F \cup \{\alpha, \beta\}$ so that it contains $F(\alpha) \cup F(\beta)$.

Observation 5.1.2. Suppose that E/F is a field extension and $\alpha \in E$.

(a) $F(\alpha)$ is the smallest field containing $F \cup \{\alpha\}$, so it necessarily contains $Q_{F[\alpha]} = \{f(\alpha)/g(\alpha) : f(t), g(t) \in F[t], f(\alpha) \neq 0\}$. Conversely, $Q_{F[\alpha]}$ is a field containing F. Therefore, $F(\alpha) = Q_{F[\alpha]}$.

(b) Any element of the form $1/f(\alpha)$ with $f(t) \in F[t]$ and $f(\alpha) \neq 0$ if and only if $F(\alpha) = F[\alpha]$. (One implication is clear; because $F(\alpha) \geq F[\alpha]$, if the former condition is satisfied then $F(\alpha) = F[\alpha]$.)

Question 5.1.1. Given a field extension E/F with an elements $\alpha \in E$, what can be an equivalent condition for $F(\alpha) = F[\alpha]$?

Observation 5.1.3 (The minimal polynomial of an algebraic element). Suppose that E/F is a field extension and $\alpha \in E$ is algebraic over F. Let $\mathit{ker}\mathcal{E}_\alpha = \{f(t) \in F[t] : \mathcal{E}_\alpha(f(t)) = 0\}$.

(1) Since $F[t]$ is a PID. and α is algebraic over F, there is a monic polynomial $m(t) \in F[t]$ which generates $\mathit{ker}\mathcal{E}_\alpha$. Moreover, a monic generator of $\mathit{ker}\mathcal{E}_\alpha$ is unique; if $m(t)$ and $n(t)$ are monic polynomials over F and each of them generates $\mathit{ker}\mathcal{E}_\alpha$, then $(m(t)) = (n(t))$, so $m(t) \sim_\times n(t)$ and $m(t) = n(t)$.

   Definition 5.1.4. The unique monic polynomial over F which generates $\mathit{ker}\mathcal{E}_\alpha$ is called the minimal polynomial of α over F.

(2) Assume that $a(t)b(t) \in \mathit{ker}\mathcal{E}_\alpha$ for some $a(t), b(t) \in F[t]$. Then $a(\alpha)b(\alpha) = 0$, so $a(t) \in \mathit{ker}\mathcal{E}_\alpha$ or $b(t) \in \mathit{ker}\mathcal{E}_\alpha$. This proves that $\mathit{ker}\mathcal{E}_\alpha$ is a nonzero prime ideal of $F[t]$. Hence, the minimal polynomial of α over F is irreducible over F. Moreover, $\mathit{ker}\mathcal{E}_\alpha$ is a maximal ideal of $F[t]$ and $F[t]/\mathit{ker}\mathcal{E}_\alpha$ is a field, for $F[t]$ is a PID.

Suppose that E/F is a field extension with $\alpha \in E$, and assume that $f(\alpha) = 0$ for some nonzero monic polynomial $f(t)$ over F. Then the followings are equivalent:

(a) $f(t)$ is irreducible over F.

(b) $f(t)$ is the minimal polynomial of α over F.

(c) $f(t)$ is a polynomial of the least degree having a root α.

This equivalence follows from the observation that the minimal polynomial $m(t)$ of α over F is irreducible over F and that $f(t) = g(t)m(t)$ for some nonzero polynomial $g(t) \in F[t]$.

Observation 5.1.5 (An answer to Question 5.1.1). We will prove that $F(\alpha) = F[\alpha]$ if and only if α is algebraic over F.

If $F(\alpha) = F[\alpha]$, then $1/\alpha = u(\alpha)$ for some polynomial $u(t) \in F[t]$, thus α is a root of $tu(t) - 1 \in F[t]$ and α is algebraic over F. Assuming conversely, it suffices to show that $1/f(\alpha) \in F[\alpha]$ whenever $f(t) \in F[t]$ is a polynomial such that $f(\alpha) \neq 0$. Let $r(t) \in F[t]$ be a unique polynomial such that $\mathit{deg}\, r(t) < \mathit{deg}\, m(t)$, where $m(t)$ is the minimal polynomial of α over F. Since $r(t)$ and $m(t)$ are relatively prime, there are polynomials $a(t), b(t) \in F[t]$ such that $a(t)r(t) + b(t)m(t) = 1$, so $1/f(\alpha) = 1/r(\alpha) = a(\alpha)$.

The following theorem, called Kronecker's theorem, has been expected in Observation 5.1.3.

Theorem 5.1.6 (Kronecker's theorem)**.** Let F be a field and $f(t) \in F[t]$ be an irreducible polynomial. Then there is a field extension E/F such that E contains a root of $f(t)$.

Proof. Since $F[t]$ is a Euclidean domain and $f(t) \in F[t]$ is irreducible, the quotient ring $K := F[t]/(f(t))$ is a field. Our goal is to show that K contains an isomorphic copy of F and that K contains a root of $f(t)$.

First, consider the map $\imath : F \to K$ defined by $\imath(a) = \overline{a} = a + (f(t))$ for $a \in F$. One can easily check that $\imath$ is a field embedding, implying that K contains an isomorphic copy of F. Next, in the field $K = F[t]/(f(t))$, the element $\overline{t} = t + (f(t)) \in K$ satisfies

$$f^\imath(\overline{t}) = \overline{f(t)} = \overline{0},$$

so $\overline{t} \in K$ is a root of $f(t)$. □

Remark. In fact, $f(t)$ need not be irreducible, since we may replace $f(t)$ with its irreducible factor.

Question 5.1.2. Suppose that E/F is a field extension and $\alpha \in E$ is algebraic over F. Is $m_\alpha(t) \in F[t]$ of the form $m_\alpha(t) = ((t - \alpha_1) \cdots (t - \alpha_k))^m$? If so, can it be implied that $k = j$ and $m = n$, if we also have $m_\alpha(t) = ((t - \beta_1) \cdots (t - \beta_j))^n$? This question will be answered in Corollary 5.4.2.

We now study some preliminary properties regarding field extensions and algebraic extensions, in particular. Note that whenever E/F is a field extension, we can treat E as an F-vector space. As an application of this idea, we shortly prove that the order of any finite field is a prime power. If $E/\mathbb{F}_p$ is a finite field extension, where p is a positive prime number, then $E \approx \mathbb{F}_p^n$ as $\mathbb{F}_p$-vector space, implying $|E| = p^n$.

Proposition 5.1.7. Suppose that E/F is a field extension and $\alpha \in E$ is algebraic over F. Then $[F(\alpha) : F]$ is the degree of the minimal polynomial of α over F.

Proof. Since α is algebraic over F, we have $F(\alpha) = F[\alpha]$. Thus, if the degree of the minimal polynomial of α over F is n, we may conjecture that $\{1, \alpha, \cdots, \alpha^{n-1}\}$ is an F-basis of $F(\alpha)$, which is, in fact, true. □

Proposition 5.1.8. Finite field extensions are algebraic extensions.

Proof. Suppose that E/F is a finite field extension and let x be an element of E. Writinig $n = [E : F]$, then $\{1, x, \cdots, x^{n-1}, x^n\}$ is F-linearly dependent. □

Remark. Later, it will be proved that a finite field extension is a finite succesive simple algebraic extension.

Corollary 5.1.9. Let E/F be a field extension and let K be the set of all elements of E which are algebraic over F. Then K is a field. In particular, if $\alpha, \beta \in E$ are algebraic over F, then $\alpha \pm \beta$ and $\alpha\beta^{\pm 1}$ (assume $\beta \neq 0$ when taking -1) are also algebraic over F.

Proof. Given such α and β, $F(\alpha, \beta)/F$ is, clearly, a finite extension, so it is an algebraic extension. □

Applying the structure of the composition of two fields suggested in Observation 5.1.1 and Corollary 5.1.9, one can show that algebraic extensions shift to the composition of two fields. The statement and proof are given in Proposition 5.1.16.

Proposition 5.1.10. If K/E and E/F are field extensions, then $[K : F] = [K : E][E : F]$, even if either of the extensions is infinite.[1]

Proof. Let $\{\alpha_i : i \in I\}$ be an E-basis of K and $\{\beta_j : j \in J\}$ be an F-basis of E.

Goal: To show that $\mathcal{B} := \{\alpha_i\beta_j : i \in I, j \in J\}$ is an F-basis of K.

It is clear by hypothesis that $\mathcal{B}$ generates the F-vector space K. Suppose that a finite sum $\sum c_{i,j}\alpha_i\beta_j$ is zero, where $c_{i,j} \in F$ for all i and j. Gathering terms i by i, we have $\sum(\sum c_{i,j}\beta_j)\alpha_i = 0$, so $\sum c_{i,j}\beta_j = 0$ for each i, hence $c_{i,j} = 0$ for all i, j. □

The multiplicativity of extension degree is valid when an extension is given as a linear tower, but it may not be valid when the extension is not linear. In general, the 'sub'multiplicativity (not the multiplicativity) holds for finite extensions. And the following submultiplicativity implies that two field extensions are finite extensions if and only if the composition is a finite extension over the base field.

Proposition 5.1.11. If E/F is a field extension and both K/F and L/F are finite field extensions with $K, L \leq E$, then $[KL : F] \leq [K : F][L : F]$. The equality holds if and only if an F-basis of one of K and L is linearly independent over the other field. (See also Corollary 5.1.14.)

Proof. Let $\{x_1, \cdots, x_m\}$ be an F-basis of K and let $\{y_1, \cdots, y_n\}$ be an F-basis of L. Since $KL = L(x_1, \cdots, x_m)$, we obtain the inequality from

$$[KL : F] = [KL : L][L : F] \leq mn = [K : F][L : F].$$

As illustrated in the above inequality, the equaility holds if and only if $[KL : L] = [K : F]$ (or $[KL : K] = [L : F]$), which is equivalent to the case where $\{x_1, \cdots, x_m\}$ is L-linearly independent (or $\{y_1, \cdots, y_n\}$ is K-linearly independent). □

Corollary 5.1.12. If E/F is a field extension and both K and L are intermediate subfields such that $[K : F]$ and $[L : F]$ are relatively prime, then $[KL : F] = [K : F][L : F]$, hence an F-basis of one of K and L is linearly independent over the other field.

Proof. Remark that $[K : F]$ and $[L : F]$ divides $[KL : F]$. □

[1] We understand $[K : F] = [K : E][E : F]$ as an equality of cardinal numbers.

Theorem 5.1.13. A field extension E/F is a finite extension if and only if $E = F(\alpha_1, \cdots, \alpha_n)$ for some finitely many elements $\alpha_1, \cdots, \alpha_n \in E$ which are algebraic over F.

Proof. Assume first that E/F is a finite extension and let $\{\alpha_1, \cdots, \alpha_n\}$ be an F-basis of E. Then each α_i is algebraic over F and $E = F(\alpha_1, \cdots, \alpha_n)$.

Assume conversely that E is generated over F by finitely many elements in E which are algebraic over F. Then $[E : F]$ is not greater than the product of the degree of α_i over F for all i. □

Corollary 5.1.14. Suppose that $F \leq E \leq L$ and $F \leq K \leq L$ are field extensions. Then EK/K is a finite extension if E/F is a finite extension, even if K/F may be an infinite extension. (In Proposition 5.1.11, we proved that the EK/F is a finite extension if and only if both E/F and K/F are finite extensions.)

$$\begin{tikzcd}
& L \arrow[d, dash] & \\
& EK \arrow[dl, dash] \arrow[dr, dash, dashed, "\text{finite}"] & \\
E \arrow[dr, dash] \arrow[ddr, dash, bend right, "\text{finite}"'] & & K \arrow[dl, dash] \\
& E \cap K \arrow[d, dash] & \\
& F &
\end{tikzcd}$$

Proof. Let $\alpha_1, \cdots, \alpha_n$ be elements of E which are algebraic over F such that $E = F(\alpha_1, \cdots, \alpha_n)$. Then $EK = K(\alpha_1, \cdots, \alpha_n)$, so EK/K is a finite extension. □

Question 5.1.3 (The existence of a primitive element)**.** Given a finite field extension E/F, can we find an element $\alpha \in E$ such that $E = F(\alpha)$? (Such an element α is called a primitive elements of E over F.)

Theorem 5.1.15. Suppose that $F \leq L \leq K$ is a field extension. Then K/F is an algebraic extension if and only if both K/L and L/F are algebraic extensions.

Proof. It is clear that K/L and L/F are algebraic extensions if K/F is an algebraic extension. Assume conversely that voth K/L and L/F are algebraic extensions. Given an element $\alpha \in K$, write $m_{\alpha,K}(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$.

$$\begin{tikzcd}
K \arrow[dd, dash] \arrow[dr, dash] & \\
& F(\alpha, a_0, a_1, \cdots, a_{n-1}) \arrow[dd, dash] \\
L \arrow[dd, dash] & \\
& F(a_0, a_1, \cdots, a_{n-1}) \\
F \arrow[ur, dash] &
\end{tikzcd}$$

Then α is algebraic over $F(a_0, a_1, \cdots, a_{n-1})$ and $F(a_0, a_1, \cdots, a_{n-1})/F$ is a finite extension. Hence, $[F(\alpha, a_0, a_1, \cdots, a_{n-1}) : F] < \infty$, so α is algebraic over F. Therefore, K/F is an algebraic extension. □

Regarding algebraic extensions, there are some shifts of algebraic extensions to the composition of fields, as given in Corollary 5.1.14.

Proposition 5.1.16. Suppose that both E and K are intermediate subfield of L/F.

(a) Show that EK/K is an algebraic extension, if E/F is an algebraic extension.

(b) Show that EK/F is an algebraic extension if E/F and K/F are algebraic extensions.

Proof. Note that an element of EK is of the form

$$\frac{\alpha_1'\beta_1' + \cdots + \alpha_n'\beta_n'}{\alpha_1\beta_1 + \cdots + \alpha_m\beta_m},$$

where $m, n \in \mathbb{Z}^{>0}$ and $\alpha_i, \alpha_j' \in E$ and $\beta_i, \beta_j' \in K$ for all integers $1 \leq i \leq m$ and $1 \leq j \leq n$. When proving (a), it suffices to show that $\alpha\beta$ is algebraic over K whenever $\alpha \in E$ and $\beta \in K$, which is clear. When proving (b), it suffices to show that $\alpha\beta$ is algebraic over F, which is justified in Corollary 5.1.9. □

5.2 Splitting fields

Definition 5.2.1 (Splitting field, normal extension)**.** Let F be a field and $\mathcal{R}$ be a collection of nonconstant polynomials over F. If all polynomials in $\mathcal{R}$ split completely over a field K containing F but not over any proper subfield of F, then K is called a splitting field for the polynomials in $\mathcal{R}$ over F and K/F is said to be a normal extension. In particular, if $\mathcal{R}$ is finite and $p(t) \in F[t]$ is the product of all polynomials in $\mathcal{R}$, then K is called a splitting field for $p(t)$ over F.

Proposition 5.2.2. If F is a field and $p(t)$ is a nonconstant polynomial over F, then there is a splitting field for $p(t)$ over F.

Proof. Using Kronecker's theorem inductively, we can find a field $K := F(\alpha_1, \cdots, \alpha_n)$, where $\alpha_1, \cdots, \alpha_n$ are pairwise distint roots of $p(t)$. It is clear that $p(t)$ splits completely over K; if $p(t)$ splits completely over an extended field, then the extension necessarily contains all rooots of $p(t)$, thus it contains (an isomorphic copy of) K. Therefore, K is a splitting field for $p(t)$ over F. □

Remark. The uniqueness part will be proved later in this chapter. See Theorem 5.4.5.

Example 5.2.3. Suppose that K/F is a finite extension. We will justify that the followings are equivalent:

(a) K/F is a normal extension.

(b) Every nonconstant polynomial over F with a root in K splits completely over K.

To prove that (a) implies (b), assume that K/F is the splitting field for $k(t) \in F[t]$ over F (we can think so, since K/F is a finite extension) and let $p(t) \in F[t]$ be a nonconstant polynomial with a root α in K. If β is another root of $p(t)$, by Theorem 5.4.1, there is an F-isomorphism $\sigma : F(\alpha) \to F(\beta)$ such that $\sigma(\alpha) = \beta$. Since the splitting field for $p(t)$ over $F(\alpha)$ is $K(\alpha) = K$ and the splitting field for $p(t)$ over $F(\beta)$ is $K(\beta)$ (why?), there is a field isomorphism $\widetilde{\sigma} : K \to K(\beta)$ extending σ. Since $\widetilde{\sigma}$ is an F-isomorphism, $\widetilde{\sigma}$ is an F-linear isomorphism, so $\mathit{dim}_F K = \mathit{dim}_F K(\beta)$, implying that $\beta \in K$.

We now show that (b) implies (a). Since K/F is a finite extension, we may write $K = F(\alpha_1, \cdots, \alpha_n)$, where α_i is algebraic over F for each $i = 1, \cdots, n$. Let $p(t)$ be the product of the minimal polynomials of α_i over F.

(i) By hypothesis, $p(t)$ splits completely over K. Hence, K is not smaller than the splitting field for $p(t)$ over F.

(ii) Conversely, the splitting field for $p(t)$ over F necessarily contains all roots of $p(t)$, so it contains K.

Therefore, K is the splitting field for $p(t)$ over F, so K/F is a normal extension.

Example 5.2.4. Let K_1/F and K_2/F be finite normal extensions. We will justify that K_1K_2 is a (finite) normal extension over F, and $K_1 \cap K_2$ is a (finite) normal extension over F.

Let $a(t), b(t) \in F[t]$ be nonconstant polynomials such that K_1 is the splitting field for $a(t)$ over F and K_2 is the splitting field for $b(t)$ over F (such setting is plausible, since K_1/F and K_2/F are finite extensions). We will show that K_1K_2 is the splitting field for $a(t)b(t)$ over F.

(i) Since K_1 contains all roots of $a(t)$ and K_2 contains all roots of $b(t)$, the composition K_1K_2 contains all roots of $a(t)b(t)$. Hence, K_1K_2 contains the splitting field for $a(t)b(t)$ over F.

(ii) Conversely, K_1K_2 is the smallest field containing F and the roots of $a(t)b(t)$, which are necessarily contained in the splitting field for $a(t)b(t)$ over F.

Therefore, K_1K_2 is the splitting field for $a(t)b(t)$ over F.

To show that $K_1 \cap K_2$ is a normal extension over F, we apply the result of the previous example. Let $p(t)$ be a polynomial over F with a root in $K_1 \cap K_2$. Because K_1/F and K_2/F are finite normal extensions, $p(t) \in F[t]$ splits completely over K_1 and K_2. This implies that all roots of $p(t)$ are in $K_1 \cap K_2$, so $K_1 \cap K_2$ is a finite normal extension over F.

Example 5.2.5. Let t be an indeterminate and $F = \mathbb{F}_p(t)$, where p is a positive prime number. And let $f(x) = x^p - t \in F[x]$ and α be a root of $f(x)$. Then $\alpha^p = t$ and $f(x) = x^p - \alpha^p = (x - \alpha)^p$, so the splitting field for $f(x)$ over F is $F(\alpha)$, which is a simple algebraic extension over F of degree p.

5.3 Algebraic closures

Definition 5.3.1 (Algebraic closedness)**.** A field F is said to be algebraically closed if every nonconstant polynomial over F has a root in F.[2]

Observation 5.3.2. For a field F, the followings are equivalent:

(a) F is algebraically closed.

(b) If E/F is a field extension and $\alpha \in E$ is algebraic over F, then $\alpha \in F$.

(c) If E/F is an algebraic extension, then $E = F$.

(d) If E/F is a finite extension, then $E = F$.

Proof. (a)⇒(b): Since F is algebraically closed, the minimal polynomial $m_\alpha(t) \in F[t]$ of α over F splits completely over F, so $\alpha \in F$.
(b)⇒(c)⇒(d): Clear.
(d)⇒(a): Let $f(t) \in F[t]$ be a nonconstant polynomial and let α be a root of $f(t)$. Because $F(\alpha)/F$ is a finite extension, $\alpha \in F$. □

Definition 5.3.3 (Algebraic closure)**.** An algebraic extension $\overline{F}$ over F is called an algebraic closure of F if every nonconstant polynomial over F has a root in $\overline{F}$ (or equivalently, every nonconstant polynomial over F splits completely over $\overline{F}$).

Remark. By definition, a field F is algebraically closed if and only if F is an algebraic closure of F.

The following proposition solves a technical problem when defining algebraic closures.

Proposition 5.3.4. If $\overline{F}$ is an algebraic closure of the field F, then $\overline{F}$ is algebraically closed. Hence, by Observation 5.3.2, an algebraic closure of $\overline{F}$ is $\overline{F}$, i.e., there is no strictly larger algebraic extension over $\overline{F}$.

Proof. Let $f(t)$ be a nonconstant polynomial over $\overline{F}$ and let α be a root of $f(t)$. It suffices to show that $\alpha \in \overline{F}$. Since $\overline{F}(\alpha)/\overline{F}$ and $\overline{F}/F$ are algebraic extensions, $\overline{F}(\alpha)/F$ is an algebraic extension. Because the minimal polynomial of α over F splits completely over $\overline{F}$, $\alpha \in \overline{F}$, as desired. □

Theorem 5.3.5. An algebraic closure of a field exists.

Proof 1. We first introduce the proof due to Emil Artin.

Step 1: A remarkable setting.

Let F be a field. For every nonconstant polynomial $f = f(x) \in F[x]$, let x_f be an indeterminate and consider the polynomial ring $R := F[x_f : f \in F[u]]$. In this polynomial ring, consider the ideal I generated by the polynomials $f(x_f)$ for $f \in F[u]$.

We now prove that I is a proper ideal of R by contradiction; assume $I = R$. Then we have a relation

$$g_1 f_1(x_{f_1}) + \cdots + g_n f_n(x_{f_n}) = 1,$$

where $g_i \in R$ for $i = 1, \cdots, n$. For simplicity, let $x_i = x_{f_i}$ and let $x_{n+1}, \cdots, x_m$ be the remaining variables occurring in the polynomials g_j for $j = 1, \cdots, n$. Then the above relation reads

$$g_1(x_1, \cdots, x_m) f_1(x_1) + \cdots + g_n(x_1, \cdots, x_m) f_n(x_n) = 1.$$

By Kronecker's thoerem, for each $i = 1, \cdots, n$, there is a root α_i of f_i; letting $x_i = \alpha_i$ for each i, we have $0 = 1$, a contradiction.

Step 2: Deriving the result.

There is a maximal ideal M of R containing I. Then R/M is a field which contains an isomorphic copy of F. Moreover, the image of x_f in R/M is a root of a nonconstant polynomial $f(x) \in F[x]$, since

[2] Or equivalently, a field F is said to be algebraically closed if every nonconstant polynomial over F splits completely over F, i.e., the only irreducible polynomials over F are the polynomials of degree 1.

$f(x_f) \in I \subset M$. Therefore, every nonconstant polynomial over F has a root in $F_1 := R/M$. Continuing the above process on F_1 and so on, we obtain an ascending chain $F = F_0 \leq F_1 \leq F_2 \leq \cdots$.

Define $K := \bigcup_{n=0}^{\infty} F_n$. Since $(F_n)_{n=0}^{\infty}$ is monotonically increasing, K is a field. If $a(x) \in K[x]$, then $a(x) \in F_N[x]$ for some positive integer N, so $a(x)$ has a root in F_{N+1} and in K, proving that K is an algebraic closure of F. □

Proof 2. Invoking Zorn's lemma, we may prove the theorem.

Given a field F, let $\mathcal{X}$ be the collection of all algebraic extensions over F. Since F/F is algebraic, $\mathcal{X}$ is nonempty. Furthermore, $\mathcal{X}$ is partially ordered by set inlcusion (or by field extension).

Given a chain $\mathcal{C}$ in $\mathcal{X}$, define

$$K = \bigcup_{E \in \mathcal{C}} E.$$

It is clear that K is a field and K/F is algebraic, implying that $K \in \mathcal{X}$ and K is an upper bound of $\mathcal{C}$.

By Zorn's lemma, $\mathcal{X}$ has a maximal member L. Assume that L is not an algebraic closure of F. Then, there is a nonconstant polynomial with a root α such that $\alpha \notin L$. Because $L(\alpha)$ is a proper extension of L and $L(\alpha)$ is an algebraic extension over F, the maximality of L is disobeyed. □

In fact, an algebraic closure of a field is unique up to isomorphism. See Theorem 5.4.7.

5.4 Isomorphism extension theorems

Due to their importance, the below three isomorphism extension theorems are moved to this section, even though they could be proved in eralier sections.

Theorem 5.4.1 (For simple algebraic extensions)**.** Let K/E and L/F be field extensions and $\sigma : E \to F$ be a field isomorphism. If $p(t) \in E[t]$ is irreducible, then $p^\sigma(t) \in F[t]$ is also irreducible. Also, if $\alpha \in K$ is a root of $p(t)$ and $\beta \in L$ is a root of $p^\sigma(t)$, then there is a unique field isomorphism $\widetilde{\sigma} : E(\alpha) \to F(\beta)$ extending σ such that $\widetilde{\sigma}(\alpha) = \beta$.

$$\begin{tikzcd}
K \arrow[d, dash] & L \arrow[d, dash] \\
E(\alpha) \arrow[r, dashed, "\widetilde{\sigma}", "{\approx,\ \text{unique}}"'] \arrow[d, dash, "p(t)"'] & F(\beta) \arrow[d, dash, "p^\sigma(t)"] \\
E \arrow[r, "\approx", "\sigma"'] & F
\end{tikzcd}$$

Proof. It should be satisfied that $\widetilde{\sigma}(u(\alpha)) = u^\sigma(\beta)$ for all $u(t) \in E[t]$. □

Corollary 5.4.2 (An answer to Question 5.1.2)**.** Let K/F be a field extension and $\alpha \in K$ is algebraic over F. Then the minimal polynomial $p(t)$ of α is of the form

$$p(t) = ((t - \alpha_1) \cdots (t - \alpha_k))^m,$$

where $\alpha_1, \cdots, \alpha_k$ are in a splitting field for $p(t)$ over F. Moreover, if

$$p(t) = ((t - \beta_1) \cdots (t - \beta_j))^n,$$

where $\beta_1, \cdots, \beta_j$ are in a splitting field for $p(t)$ over F, then $k = j$ and $m = n$.

Proof. Suppose that α and β are roots of $p(t)$. Then there is a unique F-isomorphism $\mu : F(\alpha) \to F(\beta)$ such that $\mu(\alpha) = \beta$. Because $p(t) \in F[t]$, we have $p^\mu(t) = p(t)$, so the multiplicity of α is not greater than the multiplicity of β and vice versa, due to symmetry. □

Speaking of the isomorphism extension theorem for simple algebraic extensions, we introduce an equivalence regarding algebraic conjugates.

Definition 5.4.3 (Algebraic conjugates)**.** Let E/F and K/F be field extensions. Elements $\alpha \in E$ and $\beta \in K$ are called algebraic conjugates over F if their minimal polynomial over F are the same.

From Theorem 5.4.1, we can deduce the following equivalence:

Observation 5.4.4. Let α, β be elements in a field extension of F which are algebraic over F.

(a) α and β are algebraic conjugates over F if and only if there is an F-isomorphism $\sigma : F(\alpha) \to F(\beta)$ such that $\sigma(\alpha) = \beta$.

(b) Let $m(t)$ be the minimal polynomial of α over F. A root of $m(t)$ is an algebraic conjugate of α over F, and an algebraic conjugate of α over F is a root of $m(t)$.

Proof. (a) When α and β are algebraic conjugates over F, Theorem 5.4.1 proves the existence of a desired F-isomorphism. Assuming conversely, since $m_\alpha(t) \in F[t]$ is fixed by σ, we have $m_\alpha(\beta) = 0$, so $m_\beta(t)|m_\alpha(t)$. It naturally follows from symmetry that $m_\alpha(t)|m_\beta(t)$. Therefore, α and β are algebraic conjugates over F.

(b) By definition, an algebraic conjugate β of α over F is a root of $m(t)$. Let β be a root of $m(t)$ and assume that the minimal polynomial $f(t)$ of β over F is not $m(t)$. Then there is a nonconstant monic polynomial $g(t) \in F[t]$ such that $m(t) = f(t)g(t)$, and either $f(t)$ or $g(t)$ has α a root, a contradiction. Therefore, a root of the minimal polynomial of α over F is an algebraic conjugate of α over F. □

Remark. The above observation induces an equivalence relation regarding algebraic conjugates over a given field. Let F be a field and write $\alpha \sim \beta$ for elements α, β which are algebraic over F, whenever

$$\beta \text{ is an algebraic conjugate of } \alpha \text{ over } F.$$

Then $\sim$ denotes an equivalence relation on the field of elements algebraic over F. Hence, α and β are algebraically conjugate over F if and only if the minimal polynomials of α and β over F are the same.

Theorem 5.4.5 (For splitting fields)**.** Let $\sigma : E \to F$ be a field isomorphism and $f(t)$ be a nonconstant polynomial over E. Suppose that K is a splliting field for $f(t)$ over E and L is a splitting field for $f^\sigma(t)$ over F. Then there is a field isomorphism $\widetilde{\sigma} : K \to L$ extending σ.

$$\begin{tikzcd}
K \arrow[r, dashed, "\widetilde{\sigma}", "\approx"'] \arrow[d, dash, "f(t)"'] & L \arrow[d, dash, "f^{\sigma}(t)"] \\
E \arrow[r, "\approx", "\sigma"'] & F
\end{tikzcd}$$

Proof 1. We prove the theorem by applying Kronecker's theorem inductively. Let $a(t) \in E[t]$ be an irreducible factor of $f(t)$ and $\alpha_1 \in K$ be a root of $a(t)$. Then $a^\sigma(t) \in F[t]$ is an irreducible factor of $f^\sigma(t)$ and has a root $\beta_1 \in L$. By Theorem 5.4.1, there is a field isomorphism $\sigma_1 : E(\alpha_1) \to F(\beta_1)$ extending σ. Hence, there are polynomials $p_1(t) \in E(\alpha_1)[t]$ and $q_1(t) \in F(\beta_1)[t]$ such that

$$(t - \alpha_1)p_1(t) = f(t) = (t - \beta_1)q_1(t).$$

As we have done earlier, let $a_2(t) \in E(\alpha_1)[t]$ be an irreducible factor of $p_1(t)$ and $\alpha_2 \in K$ be a root of $a_2(t)$. Then $a_2^\sigma(t) \in F(\beta_1)[t]$ is also irreducible and has a root β_2, and there is a field isomorphism $\sigma_2 : E(\alpha_1)(\alpha_2) \to F(\beta_1)(\beta_2)$ extending σ_1. Since *deg* $f(t)$ is finite, this process will terminate and produces a field isomorphism $\widetilde{\sigma} : K \to L$. □

Proof 2. We prove the theorem by induction on *deg* $f(t)$. Note that the theorem is clear when *deg* $f(t) = 1$. Assuming that the theorem is valid for all nonconstant polynomials over E of degree less than n, suppose that *deg* $f(t) = n$. Let $\alpha \in K$ be a root of $f(t)$ and $\beta \in L$ be a root of $f^\sigma(t)$. By Theorem 5.4.1, there is a unique field isomorphism $\sigma_1 : E(\alpha) \to F(\beta)$ extending σ mapping α to β. Writing

$$(t - \alpha)p(t) = f(t) = (t - \beta)q(t)$$

for some $p(t) \in E(\alpha)[t]$ and $q(t) \in F(\beta)[t]$, we have $q(t) = p^{\sigma_1}(t)$. Thus, it remains to justify that K is a splitting field for $p(t)$ over $E(\alpha)$ and L is a splitting field for $q(t)$ over $F(\beta)$; it then follows from the induction hypothesis that there is a field isomorphism $\widetilde{\sigma} : K \to L$ extending σ_1 (thus, extending σ).

(i) It is clear that $p(t)$ splits completely over K.

(ii) If there is a proper subfield I of K containing $E(\alpha)$ over which $p(t)$ splits completely, then $f(t) = (t-\alpha)p(t)$ would split complitely over I, which contradicts the hypothesis that K is a splitting field for $f(t)$ over E. Therefore, there is no proper subfield of K over which $p(t)$ splits completely.

The same argument holds for L, as desired. □

Corollary 5.4.6. A splitting field for a nonconstant polynomial over a field is unique up to isomorphism.

Theorem 5.4.7 (For algebraic closures)**.** Let $\sigma : E \to F$ be a field isomorphism. If K/E is an algebraic extension, there is a field embedding $\widetilde{\sigma} : K \to \overline{F}$ extending σ.

$$\begin{tikzcd}
 & \overline{F} \arrow[d, dash] \\
K \arrow[r, dashed, "\widetilde{\sigma}", "\approx"'] \arrow[d, dash] & \widetilde{\sigma}(K) \arrow[d, dash] \\
E \arrow[r, "\approx", "\sigma"'] & F
\end{tikzcd}$$

Proof. We find a field embedding of K into $\overline{F}$ by applying Zorn's lemma.

Step 1. Setting a nonempty partially ordered set.

Set

$$\mathcal{X} := \left\{ (L, \tau) : \begin{array}{c} E \leq L \leq K \text{ and} \\ \tau : L \to K \text{ is a field embedding extending } \sigma \end{array} \right\}.$$

Then $(E, \sigma) \in \mathcal{X}$, so X is nonempty. And for $(L_1, \tau_1), (L_2, \tau_2) \in \mathcal{X}$, let $(L_1, \tau_1) \leq (L_2, \tau_2)$ if and only if

$$L_1 \leq L_2 \text{ and } \tau_2|_{L_1} = \tau_1.$$

Then this relation is a partial order on $\mathcal{X}$.

Step 2. Showing that every subchain has an upper bound.

Let $\mathcal{C}$ be an ascending chain of X. To find its upper bound in X, let

$$C := \bigcup_{(L,\tau) \in \mathcal{C}} L$$

and define a map $\tau_C : L \to \overline{F}$ by $\tau_C(x) := \tau_x(x)$, where $(L_x, \tau_x) \in \mathcal{C}$ is a member such that $x \in L_x$. Then $E \leq C \leq K$ and τ_C is a well-defined field embedding, so (C, τ_C) is an upper bound of $\mathcal{C}$ in X.

Step 3. Deriving the result.

By Zorn's lemma, there is a maximal element $(M, \mu) \in X$. We will justify that $M = K$ by contradiction. Assume $M \lneqq K$. Then there is an element $\alpha \in K \setminus M$; let $p(t) \in M[t]$ be the minimal polynomial of α over M, and let $\beta \in \overline{F}$ be a root of $p^{\mu}(t) \in F[t]$. By Theorem 5.4.1, there is a field embedding $\widetilde{\mu} : M(\alpha) \to \overline{F}$ extenidng μ, so $(M, \mu) \lneqq (M(\alpha), \widetilde{\mu})$, which contradicts the maximality of (M, μ). □

Corollary 5.4.8. An algebraic closure of a field is unique up to isomorphism.

Proof. Given a field F, let K and L be algebraic closures of F. For id_F, by Theorem 5.4.7, there is a field embedding $\mu : K \to L$. Since K is algebraically closed, so is $\mu(K)$. Because $L/\mu(K)$ is an algebraic extension, we have $\mu(K) = L$, as desired. □

5.5 Constructible numbers

Theorem 5.5.1 (Constructibility criterion I)**.** $\alpha \in \mathbb{R}$ is constructible if and only if there is a tower of quadratic extensions from $\mathbb{Q}$ whose head field contains α.

Proof. Assuming the existence of such a tower, it is almost clear that α is constructible. Conversely, if $\alpha \in \mathbb{R}$ is constructible, a construction of α by straight lines and circles naturally induces a tower of quadratic extensions with α being contained in the head field. □

Another constructibility criterion is introduced in Theorem 9.4.3.

Corollary 5.5.2. A real algebraic conjugate of a constructible real number is also constructible.

Proof. Let α be a constructible real number and β be a real algebraic conjugate of α. Then there is a unique $\mathbb{Q}$-isomorphism $\sigma : \mathbb{Q}(\alpha) \to \mathbb{Q}(\beta)$ mapping α to β. By the previous theorem, there is a tower of quadratic extensions

$$\mathbb{Q} < \mathbb{Q}(\sqrt{d_1}) < \cdots < \mathbb{Q}(\sqrt{d_1}, \cdots, \sqrt{d_n}) = K$$

where $d_1, \cdots, d_n \in \mathbb{Q}$ and K contains α. By isomorphism extension theorem, there is a field embedding $\widetilde{\sigma} : K \to \overline{\mathbb{Q}(\beta)} = \overline{\mathbb{Q}}$ extending σ. Then

$$\mathbb{Q} < \mathbb{Q}(\widetilde{\sigma}(\sqrt{d_1})) < \cdots < \mathbb{Q}(\widetilde{\sigma}(\sqrt{d_1}), \cdots, \widetilde{\sigma}(\sqrt{d_n})) = \widetilde{\sigma}(K)$$

is a tower of quadratic extensions and β belongs to $\widetilde{\sigma}(K)$. □

Corollary 5.5.3. If $\alpha \in \mathbb{R}$ is constructible, then the degree of α over $\mathbb{Q}$ is a power of 2.

Proof. Clear. □

Chapter 6

Separable extensions and normal extensions

6.1 Separable extensions

Definition 6.1.1 (Separability)**.** Given an algebraic field extension E/F, an element $\alpha \in E$ is said to be separable over F if its minimal polynomial over F is a separable polynomial. In particular, the extension E/F is said to be a separable extension if every element in E is separable over F. If every algebraic extension over a F is separable, then F is said to be perfect.

Example 6.1.2. (a) It is easy to check that an irreducible polynomial over a field of characteristic 0 is a separable polynomial. It will be proved in the next chapter that an irreducible polynomial over a finite field is also a separable polynomial. Hence, fields of characteristic 0 and finite fields are perfect fields.

(b) Algebraically closed fields are perfect fields, and algebraic extensions of perfect fields are perfect fields.

Some expereice from algebraic extensions helps studying separable extensions.

Question 6.1.1. (a) Are the sum and multiplication of two separable elements separable?

(b) Is a separable extension of a separable extension is a separable extension?

Our study begins with the degree which can measure the separability.

Observation 6.1.3. Suppose that E/F is a field extension and $\alpha \in E$ is algebraic over F. Then the minimal polynomial $m(t)$ of α over F is irreducible and

$$m(t) = ((t - \alpha_1) \cdots (t - \alpha_k))^n$$

for some pairwise distinct elements $\alpha_1, \cdots, \alpha_k \in \overline{F}$ and $n \in \mathbb{Z}^{>0}$. It is clear from the above expression that k is the number of distinct roots of the minimal polynomial of α over F and that k divides the extension degree of $F(\alpha)/F$. But we will find what k also means, by noticing that $m(t)$ is the irreducible polynomial of α_i for all i.

(Without loss of generality, assume $\alpha_1 = \alpha$.) After choosing an index i, by Theorem 5.4.1, there is a unique F-embedding $\sigma : F(\alpha) \hookrightarrow \overline{F}$ such that $\sigma(\alpha) = \alpha_i$, so $k \leq |\mathrm{Emb}(F(\alpha)/F)|$.[1] Conversely, given $\sigma \in \mathrm{Emb}(F(\alpha)/F)$, since $m(t)$ is fixed by the action of σ, $\sigma(\alpha)$ is a root of $m(t)$; because every F-embedding of $F(\alpha)$ into $\overline{F}$ is determined by its action on α, we have $k \geq |\mathrm{Emb}(F(\alpha)/F)$. Therefore, k also denotes the number of all distinct F-embeddings of $F(\alpha)$ into $\overline{F}$.

Generalizing the above observation, we define the separable degree of an algebraic extension as follows:

[1] When considering $\mathrm{Emb}(E/F)$ as a set, it is assumed that an algebraic closure $\overline{F}$ of F is given and we consider F-embeddings of E into $\overline{F}$. Still, its cardinality does not depend on the choice of an algebraic closure of $\overline{F}$.

Definition 6.1.4. Let E/F be an algebraic field extension, where $F \leq E \leq \overline{F}$ with $\overline{F}$ being the algebraic closure of F. The separable degree of E/F, denoted by $[E : F]_{\text{sep}}$, is defined by the cardinality of the set of F-embeddings of E into $\overline{F}$. In other words,

$$[E : F]_{\text{sep}} := |\{\tau : E \hookrightarrow \overline{F} : \tau \text{ is an } F\text{-embedding}\}|.$$

$$\begin{tikzcd}
\overline{F} & \overline{F} \\
E \arrow[u, dash] \arrow[r, dashed, "\tau", "\approx"'] & \tau(E) \arrow[u, dash] \\
F \arrow[u, dash] \arrow[r, "=", "id_F"'] & F \arrow[u, dash]
\end{tikzcd}$$

The above definition seems to be poorly defined, since the cardinality of the set of such F-embeddings seems to depend on the choice of an algebraic closure of F. (This is intuitively (and, in fact, logically) true, for an algebraic closure is unique up to isomorphism.) Moreover, one may wish to generalize the definition so that τ extends a field isomorphism, not just the idenity map on F.

Observation 6.1.5. Let E/F be an algebraic extension and let $\overline{F}$ and $\widetilde{F}$ be algebraic extensions of F, which contains E. We will show that there is a bijection

$$\{\tau : E \hookrightarrow \overline{F} : \tau \text{ is an } F\text{-embedding}\} \longleftrightarrow \{\mu : E \hookrightarrow \widetilde{F} : \mu \text{ is an } F\text{-embedding}\},$$

which explains that the above definition of separable degree does not depend on the choice of an algebraic closure of F.

Consider the following diagram, where an F-embedding $\tau : E \hookrightarrow \overline{F}$ is given.

$$\begin{tikzcd}
\widetilde{F} & & \overline{F} \arrow[ll, "\widetilde{id_F}", "\approx"'] \\
\star \arrow[u, dash] & E \arrow[l, dashed, "f(\tau)", "\approx"'] \arrow[r, "\tau", "\approx"'] & \tau(E) \arrow[u, dash] \\
F \arrow[u, dash] & F \arrow[u, dash] \arrow[l, "id_F", "="'] \arrow[r, "id_F", "="'] & F \arrow[u, dash]
\end{tikzcd}$$

For the diagram to be commutative, it should be satisfied that $f(\tau) = \widetilde{id_F} \circ \tau$. By defining f so, we have established a map

$$f : \{\tau : E \hookrightarrow \overline{F} : \tau \text{ is an } F\text{-embedding}\} \to \{\mu : E \hookrightarrow \widetilde{F} : \mu \text{ is an } F\text{-embedding}\},$$

which is a bijection; thus, we may write without any confusion that $[E : F]_{\text{sep}} = |\mathrm{Emb}(E/F)|$.

Observation 6.1.6. As in the preceeding observation, assume that $F \leq E \leq \overline{F}$ is a tower of algebraic extensions, where olF is an algebraic closure of F. And let $\sigma : F \hookrightarrow \overline{F}$ be a field embedding, i.e., $\sigma : F \to \sigma(F)$ is a field isomorphism. We will justify that

$$[E : F]_{\text{sep}} = |\{\mu : E \hookrightarrow \overline{F} : \tau \text{ is a field embedding and } \tau|_F = \sigma\}|$$

(the separable degree of a given algebraic extension does not depend on the base field isomorphism (embedding)) by showing that there is a bijection

$$\{\tau : E \hookrightarrow \overline{F} : \tau \text{ is an } F\text{-embedding}\} \longleftrightarrow \{\mu : E \hookrightarrow \overline{F} : \tau \text{ is a field embedding and } \tau|_F = \sigma\}.$$

Consider the following diagram when an F-embedding $\tau : E \hookrightarrow \overline{F}$ is given.

$$\begin{tikzcd}
\overline{F} & & \overline{F} \arrow[ll, "\widetilde{\sigma}", "\approx"'] \\
\star \arrow[u, dash] & E \arrow[l, dashed, "g(\tau)", "\approx"'] \arrow[r, "\tau", "\approx"'] & \tau(E) \arrow[u, dash] \\
\sigma(F) \arrow[u, dash] & F \arrow[u, dash] \arrow[l, "\approx", "\sigma"'] \arrow[r, "=", "id_F"'] & F \arrow[u, dash]
\end{tikzcd}$$

For the diagram to be commutative, it should be satisfied that $g(\tau) = \widetilde{\sigma} \circ \tau$. By defining g so, we have establised a map

$$g : \{\tau : E \hookrightarrow \overline{F} : \tau \text{ is an } F\text{-embedding}\} \to \{\mu : E \hookrightarrow \overline{F} : \tau \text{ is a field embedding and } \tau|_F = \sigma\}.$$

which is a bijection.

By the preceeding two observations, we may re-define the separable degree of an algebraic extension.

Definition 6.1.7 (Separable degree)**.** Let E/F be an algebraic field extension and let $\overline{F}$ be the algebraic closure of F. And let $\sigma : F \hookrightarrow \overline{F}$ be a field embedding. Then the separable degree of E/F, denoted by $[E : F]_{\mathsf{sep}}$, is defined by the cardinality of field embeddings from E into $\overline{F}$ whose restriction to F is σ. In other words,

$$[E : F]_{\mathsf{sep}} := |\{\tau : E \hookrightarrow \overline{F} : \tau \text{ is a field embedding and } \tau|_F = \sigma\}|.$$

(As observed in the preceeding two observations, this definition is independent of the choice of an algebraic closure of F and a field embedding $\sigma : F \hookrightarrow \overline{F}$.)

Remark. Suppose that α is an element which is algebraic over F. Then α is separable over F if and only if its separable degree and extension degree are the same.

In the remaining of this section, we study some properties regarding separable degrees and separability of algebraic field extensions, and the primitive element theorem for separable extensions in the end of this section.

Lemma 6.1.8. Suppose that K/E and E/F are algebraic field extensions.

(a) $[K : F]_{\mathsf{sep}} = [K : E]_{\mathsf{sep}}[E : F]_{\mathsf{sep}}$.

(b) In particular, if E/F is a finite extension, then the separable degree of E/F divides the extension degree of E/F.

Proof. Fix an algebraic closure $\overline{F}$ of F containing K.

(a) Given $\sigma \in \mathrm{Emb}(K/F)$, σ is an extension of $\sigma|_E \in \mathrm{Emb}(E/F)$, so $[K : F]_{\mathsf{sep}} \le [K : E]_{\mathsf{sep}}[E : F]_{\mathsf{sep}}$. Conversely, there are $[E : F]_{\mathsf{sep}}$-distinct F-embeddings of E into $\overline{F}$, thus there are at least $[K : E]_{\mathsf{sep}}[E : F]_{\mathsf{sep}}$-distinct F-embeddings of K into $\overline{F}$, so $[K : F]_{\mathsf{sep}} \ge [K : E]_{\mathsf{sep}}[E : F]_{\mathsf{sep}}$.

(b) Assume that E/F is a finite extension and write $E = F(\alpha_1, \cdots, \alpha_n)$ for some elements $\alpha_1, \cdots, \alpha_n \in E$ which are algebraic over F. Considering the following tower of simple algebraic extensions:

$$F \le F(\alpha_1) \le F(\alpha_1, \alpha_2) \le \cdots \le F(\alpha_1, \cdots, \alpha_n) = E.$$

In each simple algebraic extension, the separable degree divides the extension degree. Since each degree is multiplicative, we find that $[E : F]_{\mathsf{sep}}$ divides $[E : F]$.

This completes the proof. □

Proposition 6.1.9. Let E/F be a finite extension. Then E/F is a separable extension if and only if its separable degree and extension degree are the same.

Proof. Write $E = F(\alpha_1, \cdots, \alpha_r)$ for some $\alpha_1, \cdots, \alpha_r \in E$ which are algebraic over F, and consider a tower of simple algebraic extensions. If E/F is a separable extension, then each simple extension is separable. Hence, the separable degree and the extension degree of each simple extension are the same, and $[E : F] = [E : F]_{\mathsf{sep}}$. Conversely, if $[E : F] = [E : F]_{\mathsf{sep}}$ and $\alpha \in E$, then $[F(\alpha) : F] = [F(\alpha) : F]_{\mathsf{sep}}$, implying that E/F is a sepatable extension. □

Remark. In particular, if $\alpha_1, \cdots, \alpha_r \in \overline{F}$, then $F(\alpha_1, \cdots, \alpha_r)/F$ is a separable extension if and only if $\alpha_1, \cdots, \alpha_r$ are separable over F.

Corollary 6.1.10. Suppose that K/E and E/F are finite field extensions. Then K/F is a separable extension if and only if both K/E and E/F are separable extensions.

Proof. It is clear that both K/E and E/F are separable extensions if K/F is a separable extension. Assume conversely that K/E and E/F are separable extensions. Since $[K:E] = [K:E]_{\mathsf{sep}}$ and $[E:F] = [E:F]_{\mathsf{sep}}$, we have $[K:F] = [K:F]_{\mathsf{sep}}$, implying that K/F is a separable extension. □

In fact, Corollary 6.1.10 extends to the following proposition:

Proposition 6.1.11. Suppose that K/E and E/F are algebraic field extensions. Then K/F is a separable extension if and only if both K/E and E/F are separable extensions.

Proof. It is clear that both K/E and E/F are separable extensions if K/F is a separable extension. Assume conversely that K/E and E/F are separable extensions. Given $\alpha \in K$, there is the separable minimal polynomial $m(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0 \in E[t]$ of α over E, hence α is a separable element over $F(a_0, a_1, \cdots, a_{n-1})$. Since a_i is a separable element over F, we can easily find that $F(\alpha, a_0, a_1, \cdots, a_{n-1})/F$ is a separable extension by showing that its extension degree and separable degree are the same. Thus, α is a separable element over F, and K/F is a separable extension. □

Corollary 6.1.12. Given an algebraic extension E/F, let $S_{E/F}$ be the collection of all elements of E which are separable over F. Then $S_{E/F}$ is an intermediate subfield of E/F.

Proof. Given two elements $\alpha, \beta \in E$ which are separable over F, $F(\alpha, \beta)/F$ is a separable extension, so $\alpha \pm \beta, \alpha\beta^{\pm 1}$ are separable over F. □

Remark. Hence, if $\alpha, \beta \in E$ are algebraic over F, then so are $\alpha \pm \beta$ and $\alpha\beta^{\pm 1}$.

Proposition 6.1.13. Suppose that E_1/F and E_2/F are separable extensions, where E_1, E_2 are contained in $\overline{F}$. Then $(E_1E_2)/F$ is a separable extension.

Proof. Considering the form of the typical element of E_1E_2, it suffices to check that $\alpha\beta \in E_1E_2$ is separable over F, where $\alpha \in E_1$ and $\beta \in E_2$; now this is clear by Corollary 6.1.12. □

Theorem 6.1.14 (Primitive element theorem)**.** Suppose that E/F is a finite separable extension. Then there is an element $\alpha \in E$ such that $E = F(\alpha)$.

Proof. This proof is not well-motivated, yet.

Suppose that F is a finite field. Because E/F is a finite extension, E is a finite field, hence there is a primitive element for E/F. Thus, we may assume that F is an infinite field. It suffices to show that for any two elements $\beta, \gamma \in \overline{F}$ there is an element $\alpha \in \overline{F}$ such that $F(\gamma) = F(\alpha, \beta)$, for E/F is a finite extension. Let $\{\beta_1, \cdots, \beta_r\}$ be the set of roots of the minimal polynomial $f(t)$ of β over F, and let $\{\gamma_1, \cdots, \gamma_s\}$ be the set of roots of the minimal polynomial $g(t)$ of γ over F, where $\beta_1 = \beta$ and $\gamma_1 = \gamma$. Because F is infinite, there is an element $c \in F$ such that

$$c \neq \frac{\beta - \beta_i}{\gamma_j - \gamma} \quad (2 \leq i \leq r, 2 \leq j \leq s).$$

Then let $\alpha = \beta + c\gamma$; we will show that $F(\beta, \gamma) = F(\alpha)$. Consider the polynomial $h(t) = f(\alpha - ct) \in F(\alpha)[t]$.

(i) $h(\gamma) = f(\beta) = 0$, so the minimal polynomial $m(t)$ of γ over $F(\alpha)$ divides $h(t)$.

(ii) Since $c\gamma - c\gamma_j \neq \beta_i - \beta$ for all $2 \leq i \leq r$ and $2 \leq j \leq s$, we have $h(\gamma_j) = f(\beta + c\gamma - c\gamma_j) \neq 0$.

Because $m(t)$ also divides $g(t)$ and E/F is a separable extension, $m(t) = t - \gamma$. So, $\gamma \in F(\alpha)$ and $\beta = \alpha - c\gamma \in F(\alpha)$, hence $F(\beta, \gamma) = F(\alpha)$. □

6.2 Normal extensions

Before studying normal extensions, we first observe the following proposition, whose proof, in particular, provides us essential intuition regarding normal extensions.

Proposition 6.2.1. Suppose that E/F is an algebraic field extension and $\sigma : E \hookrightarrow E$ is an F-embedding. Then $\sigma(E) = E$, i.e., $\sigma \in \mathrm{Aut}(E/F)$.

Proof. If E/F is a finite extension, the proposition follows from the observation that σ is a vector space isomorphism between finite dimensional vector spaces over F. To prove the proposition in general settings, it suffices to show that $\alpha \in \sigma(E)$, where $\alpha \in E$. Given $\alpha \in E$, let $f(t)$ be the minimal polynomial of α over F and write

$$f(t) = \left((t-\alpha_1)\cdots(t-\alpha_k) \times (t-\beta_1)\cdots(t-\beta_s)\right)^r ,$$

where $\alpha_1, \cdots, \alpha_k \in E$ and $\beta_1, \cdots, \beta_s \in \overline{F} \setminus E$ are pairwise distinct. Since $\sigma(E) \leq E$ and $f(t)$ is fixed by the action of σ, σ permutes $\{\alpha_1, \cdots, \alpha_k\}$, justifying that $\alpha \in \sigma(E)$. □

We defined a normal extension in Definition 5.2.1. Since we now know that the splitting field for a nonconstant polynomial $f(t)$ over a field F is the smallest field containing F and all roots $f(t)$ and that the splitting field for $f(t)$ over F is unique up to isomorphism, we emphasize the following general definition for splitting fields.

Definition 6.2.2 (Splitting field)**.** Let F be a field and R be a collection of nonconstant polynomials over F. If S is the collection of the roots of the polynomials in R, the splitting field for R over F is defined as the field $F(S)$. (Note that this definition coincides the old definition, where R is a finite collection.)

Example 6.2.3. If R is the collection of all nonconstant (monic) polynomials over a field F, then the splitting field for R over F is the algebraic closure of F.

Theorem 6.2.4 (Normal extension)**.** Suppose that E/F is an algebraic extension and assume $E \leq \overline{F}$. Then the followings are equivalent:

(a) There is a collection $\mathcal{R}$ of nonconstant polynomials over F for which E is the splitting field over F.

(b) If $\tau \in \mathrm{Emb}(E/F)$, then $\tau \in \mathrm{Aut}(E/F)$. In other words, $\mathrm{Emb}(E/F) = \mathrm{Aut}(E/F)$.[2]

(c) If $\alpha \in E$, then all roots of $m_{\alpha,F}(t)$ are in E. In other words, $m_{\alpha,F}(t)$ splits completely over E.

In either of the above cases, we call E/F a normal extension.

Proof. Assume (a) and let $\tau : E \hookrightarrow \overline{F}$ be an F-embedding. By the first proposition in this section, it suffices to verify that $\tau(E) \leq E$. If α is a root of a polynomial in $\mathcal{R}$, it can easily be checked that $\tau(\alpha)$ is a root of the same polynomial. Hence $\tau(E) \leq E$.

Assume (b), and let $m(t)$ be the minimal polynomial of $\alpha \in E$ over F. Given a root β of $m(t)$, let $\sigma : F(\alpha) \to F(\beta)$ be the unique F-isomorphism such that $\sigma(\alpha) = \beta$. We then can extend σ to $\widetilde{\sigma} : E \hookrightarrow \overline{F}$; by the assumption (b), *im* $\widetilde{\sigma} = E$, so $\beta \in E$, as desired.

Finally, assume (c). Then $E = F(\mathcal{R})$, where $\mathcal{R}$ is the collection of the minimal polynomial of $\alpha \in E$ over F for $\alpha \in E$. This proves that (a), (b), and (c) are equivalent. □

Example 6.2.5. (a) Suppose that E/F is an algebraic extension of degree 2. Then $E = F(\alpha)$ for some $\alpha \in E$, where the minimal polynomial $m(t)$ of α over F is of the form $t^2 + bt + c$ for some $b, c \in F$. The other root of $m(t)$ is given by $-b - \alpha \in E$, so E is the splitting field for $m(t)$ over F.

(b) Unlike algebraic and separable extensions, a normal extension of a normal extension may not be a normal extension. (An example: $\mathbb{Q} < \mathbb{Q}(\sqrt{2}) < \mathbb{Q}(\sqrt[4]{2})$.)

[2] Hence, in particular, a finite field extension E/F is a normal extension if and only if $[E : F]_{\text{sep}} = |\mathrm{Aut}(E/F)|$.

In fact, normal extensions seems to have some properties satisfied in group theory when extension towers are seen reversely. A counterpart of the following proposition in group theory is that if $H \leq K \leq G$ and H is a normal subgroup of G, then H is a normal subgroup of K.

Proposition 6.2.6. Suppose that $F \leq E \leq K$ and K/F is a normal extension. Then K/E is a normal extension.

Proof. Suppose that $\tau : K \hookrightarrow \overline{E}$ is an E-embedding. Since $F \leq E$ and we may assume that $\overline{E} = \overline{F}$, τ is an F-embedding of K into $\overline{F}$, so $\tau(K) = K$ and K/E is a normal extension. □

Proposition 6.2.7. Let E_1/F and E_2/F are algebraic extensions such that $E_1, E_2 \leq \overline{F}$.

(a) If $\tau : \overline{F} \hookrightarrow \overline{F}$ is a field embedding, then $\tau(E_1E_2) = \tau(E_1)\tau(E_2)$.

Assume further that E_1/F and E_2/F be normal extensions such that $E_1, E_2 \leq \overline{F}$.

(b) $(E_1E_2)/F$ is a normal extension.

(c) $(E_1 \cap E_2)/F$ is a normal extension.

Proof. (a) easily follows from the identity

$$\tau\left(\frac{\alpha_1'\beta_1' + \cdots + \alpha_n'\beta_n'}{\alpha_1\beta_1 + \cdots + \alpha_m\beta_m}\right) = \frac{\tau(\alpha_1')\tau(\beta_1') + \cdots + \tau(\alpha_n')\tau(\beta_n')}{\tau(\alpha_1)\tau(\beta_1) + \cdots + \tau(\alpha_m)\tau(\beta_m)},$$

where $\alpha_i, \alpha_j' \in E_1$ and $\beta_i, \beta_j' \in E_2$ for all integers $1 \leq i \leq m$ and $1 \leq j \leq n$.

To prove (b), let $\tau : E_1E_2 \hookrightarrow \overline{F}$ be an F-embedding. Then $\tau(E_1E_2) = \tau(E_1)\tau(E_2) = E_1E_2$, for E_1/F and E_2/F are normal extensions. This proves that $(E_1E_2)/F$ is a normal extension.

To prove (c), assume $\alpha \in E_1 \cap E_2$. Then all roots of the minimal polynomial $m(t)$ of α over F are in both E_1 and E_2, so $(E_1 \cap E_2)/F$ is a normal extension. □

We end this section with the notion of normal closures and introducing an algebraic extension which we call a Galois extension. But before this, we solve a technical problem.

Observation 6.2.8. Let $\{F_\alpha : \alpha \in \mathcal{A}\}$ be a collection of fields which are contained in a larger field E. The composition F of F_α for $\alpha \in A$ (the smallest subfield of E containing $\bigcup_{\alpha \in \mathcal{A}} F_\alpha$) is

$$K := \{x \in E : x \text{ belongs to a composition of } F_\alpha \text{ for finitely many } \alpha\text{'s}\}.$$

(In fact, F_0 necessarily (by definition) contains K, and K is a field containing $\bigcup_{\alpha \in \mathcal{A}} F_\alpha$.)

Theorem 6.2.9 (Normal closure)**.** Let E/F be a field extension and assume $E \leq \overline{F}$.

(a) The set $\{K : E \leq K \leq \overline{F}$ and K/F is a normal extension$\}$ has the least element K_0. In fact, K_0 is the composition of $\sigma(E)$ for $\sigma \in \mathrm{Emb}(E/F)$. We call K_0 the normal closure of E/F.

(b) In particular, if E/F is a separable extension, then so is K_0/F.

Proof. We first show that K_0 is the smallest normal extension over F containing E.

(i) Since $\mathrm{Emb}(E/F)$ contains the inclusion of E into $\overline{F}$, $E \leq K_0$.

(ii) Given an F-embedding $\tau : K_0 \hookrightarrow \overline{F}$, note that $\tau \circ \sigma \in \mathrm{Emb}(E/F)$ whenever $\sigma \in \mathrm{Emb}(E/F)$. In fact, τ permutes $\mathrm{Emb}(E/F)$ by left multiplication, so $\tau(K_0) = K_0$.

(iii) Finally, if K is an intermediate subfield of $\overline{F}/E$ which is normal over F, then K necessarily contains $\sigma(E)$ for $\sigma \in \mathrm{Emb}(E/F)$; if $\sigma \in \mathrm{Emb}(E/F)$, by extending σ to $\widetilde{\sigma} \in \mathrm{Emb}(K/F)$, we have $\sigma(E) \leq \widetilde{\sigma}(K) = K$.

We now assume that E/F is a separable extension. Then $(\sigma E)/F$ is a separable extension whenever $\sigma \in \mathrm{Emb}(E/F)$. If $x \in K_0$, then x belongs to the composition of some finitely many fields (σE)'s, and such finite composition is a separable extension over F. Therefore, when E/F is a separable extension, then the normal closure of E over F is also separable over F. □

Example 6.2.10. In this example, we find the normal closure of $E = \mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$. For this, we first need to find all $\mathbb{Q}$-embeddings of E into $\overline{\mathbb{Q}}$; because $\sigma \in \mathrm{Emb}(E/\mathbb{Q})$ is completely determined by its action on $\sqrt[3]{2}$, it suffices to determine all possible values of $\sigma(\sqrt[3]{2})$. Let σ be a $\mathbb{Q}$-embedding of E into $\overline{\mathbb{Q}}$ and write $\alpha = \sqrt[3]{2}$. Then $(\sigma\alpha)^3 = \sigma(\alpha^3) = 2$, so $\sigma\alpha$ is a root of $t^3 - 2$. Hence, all possible values of $\sigma\alpha$ is α, $\alpha\zeta$, and $\alpha\zeta^2$, where $\zeta = \exp(2\pi i/3)$.

As indicated in the preceeding theorem, all we have to do to obtain the normal closure of E over $\mathbb{Q}$ is to adjoin all σE for all $\mathbb{Q}$-embeddings σ of E into $\overline{\mathbb{Q}}$, which are $E = \mathbb{Q}(\alpha)$, $\mathbb{Q}(\alpha\zeta)$, and $\mathbb{Q}(\alpha\zeta^2)$. Hence, the normal closure of E over $\mathbb{Q}$ is $\mathbb{Q}(\alpha, \alpha\zeta, \alpha\zeta^2) = \mathbb{Q}(\alpha, \zeta)$, which is the splitting field for $t^3 - 2$ over $\mathbb{Q}$. As indicated in part (b) of the preceeding theorem, because $E/\mathbb{Q}$ is separable (for char($\mathbb{Q}$) $= 0$), the extension $\mathbb{Q}(\alpha, \zeta)/\mathbb{Q}$ is also separable. (Hence, $\mathbb{Q}(\alpha, \zeta)/\mathbb{Q}$ is a (finite) Galois extension.)

In particular, (b) of Theorem 6.2.9 implies that we can construct a separable and normal extension whenever a separable field extension is given, by extending the extension field, if necessary.

Definition 6.2.11 (Galois extension)**.** A field extension which is separable and normal is called a Galois extension.

Chapter 7

Further field theory

7.1 Basic properties of finite fields

For a positive prime number p, it is conventional to denote a power of p by q. We already have studied in the previous chapter that if F is a finite field of characteristic p, then $|F| = q$ for some $n \in \mathbb{N}$. Even though we do not know the existence of a finite field of order q, we first investigate some properties that a finite field of order q should satisfy.

Proposition 7.1.1. Suppose that F is a finite field of order $q = p^n$.

(a) $\text{char}(F) = p$, so the prime subfield of F is isomorphic to $\mathbb{F}_p$. Hence, we may write $\mathbb{F}_p \leq F$.

(b) Every element of F is a root of $t^q - t \in \mathbb{F}_p[t]$.

Proof. Considering an additive group F and letting $\text{char}(F) = a$ for some positive prime number a, we must have $a = p$. (b) easily follows if we consider $F^\times$ □

Observation 7.1.2. The statement in (b) implies that every element of a finite field of order q (if such a field exists) is a root of the polynomial $t^q - t$ over $\mathbb{F}_p$. Since $(t^q - t)' = qt^{q-1} - 1 = -1 \neq 0$, the polynomial $t^q - t \in \mathbb{F}_p[t]$ is separable, so it has q-distinct roots. Thus, to find a finite field of order q, there is no other choice but to consider the collection of all roots of $t^q - t \in \mathbb{F}_p[t]$, and such collection is contained in the splitting field for $t^q - t$ over $\mathbb{F}_p$.

Theorem 7.1.3 (Existence and uniqueness of finite fields)**.** Let K be the splitting field for $t^q - t \in \mathbb{F}_p[t]$ over $\mathbb{F}_p$. If we let

$$F = \{\alpha \in K : \alpha^q = \alpha\},$$

then F is a finite field of oreder q. Hence, $F = K$. By Observation 7.1.2, a finite field of order q is unique up to isomorphism.

Proof. We already proved that $|F| = q$. Thus, it remains to show that F is a subfield of K; if it is done, then F is a field which consists of all roots of $t^q - t \in \mathbb{F}_p[t]$, so F is the smallest field containing all roots of $t^q - t$, i.e., $F = K$. (For example, if $\alpha, \beta \in F$, then $(\alpha + \beta)^q = \alpha^q + \beta^q = \alpha + \beta$ and $(\alpha\beta)^q = \alpha^q \beta^q = \alpha\beta$. Proving details are left as an exercise.) □

Remark. Note that a finite field of a prime order is a set-theoretically defined field, while a finit field whose order is a power of a prime number is uniquely defined up to isomorphism, for a field of order q is the splitting field for $t^q - t \in \mathbb{F}_p[t]$ over $\mathbb{F}_p$.

Remark that we have deduced by applying the cyclic decomposition theorem that a finite multiplicative subgroup of a field is a cyclic group.

Notation. In this chapter, for an element α which is algebraic over $\mathbb{F}_q$, the minimal polynomial of α over $\mathbb{F}_q$ will be denoted by $m_{\alpha,q}(t)$.

Proposition 7.1.4. (a) $\mathbb{F}_q = \mathbb{F}_p(\alpha)$ for some $\alpha \in \mathbb{F}_q$.

(b) Given a positive integer m, there is an irreducible polynomial over $\mathbb{F}_q$ whose degree is m.
In short, if E/F is a field extension and $|E| < \infty$, then there is a primitive element $\alpha \in E$ over F.

Proof. Writing $\mathbb{F}_q^\times = \langle \alpha \rangle$ for some $\alpha \in \mathbb{F}_q^\times$, we easily obtain (a). If $\beta \in \mathbb{F}_{q^m}$ is a generator of $\mathbb{F}_{q^m}$, then $m_{\alpha,q}(t) \in \mathbb{F}_q[t]$ is a desired polynomial, for $\mathbb{F}_{q^m} = \mathbb{F}_q(\beta)$. □

Regarding the separability of polynomials, we have studied that an irreducible polynomial over a field of characteristic 0 is separable. The same property holds for finite fields.

Proposition 7.1.5. An irreducible polynomial over a finite field is separable.

Proof. Let F be a finite field of order q and let $f(t) \in F[t]$ be an irreducible polynomial. Then $f(t) = m_{\alpha,q}(t)$ for some $\alpha \in \mathbb{F}_{q^k}$. Since $\alpha^{q^k} - \alpha = 0$, $f(t)$ divides $t^{q^k} - t \in \mathbb{F}_q[t]$, which is separable. Therefore, $f(t)$ is separable. □

Proposition 7.1.6. Suppose that r, n are positive integers. Then $\mathbb{F}_{p^r} \leq \mathbb{F}_{p^n}$ if and only if $r|n$.

Proof. If $\mathbb{F}_{p^r} \leq \mathbb{F}_{p^n}$, then $\mathbb{F}_{p^n}$ is a $\mathbb{F}_{p^r}$-vector space, so $r|n$. Conversely, if $r|n$, whenever $\alpha \in \mathbb{F}_{p^r}$, we have $\alpha^{p^n} = \alpha^{p^r p^r \cdots p^r} = (\cdots((\alpha^{p^r})^{p^r})\cdots)^{p^r} = \alpha$, so $\mathbb{F}_{p^r} \leq \mathbb{F}_{p^n}$. □

We end this section by introducing the algebraic closure of $\mathbb{F}_q$. Let $F/\mathbb{F}_q$ be an algebraic extension and suppose $\alpha \in F$. Then $F(\alpha) \approx \mathbb{F}_{p^n}$ for some $n \in \mathbb{N}$, so we may write $\alpha \in \mathbb{F}_{p^n}$.

Theorem 7.1.7. The algebraic closure of $\mathbb{F}_q$ is, up to isomorphism, $\bigcup_{n=1}^{\infty} \mathbb{F}_{q^n}$.

Proof. It is clear that $F := \bigcup_{n=1}^{\infty} \mathbb{F}_{q^n}$ is an algebraic extension over $\mathbb{F}_q$. It remains to show that an irreducible polynomial $f(t)$ over $\mathbb{F}_q[t]$ splits completely over F. If $n = \mathit{deg}\, f(t)$ and α is a root of $f(t)$ then $\alpha \in \mathbb{F}_{p^n} \subset F$, as desired. □

7.2 Some problems in field theory

Problem 7.2.1. Find all $\mathbb{Q}$-automorphisms of $\mathbb{R}$.

Solution. Suppose that $\sigma \in \mathrm{Aut}(\mathbb{R}/\mathbb{Q})$. Since σ is the identity on $\mathbb{Q}$, if σ is continuous, then $\sigma = \mathit{id}_{\mathbb{R}}$.

Suppose that $a \in \mathbb{R}$ is positive. Then $\sigma(a) = (\sigma(\sqrt{a}))^2 \geq 0$. Hence, if $a, b \in \mathbb{R}$ and $a < b$, then $\sigma a \leq \sigma b$, i.e., σ is monotonically increasing. Thus, in particular, if $a, b \in \mathbb{R}$ and $|a - b| < 1/n$ for some integer n, then $|\sigma a - \sigma b| \leq 1/n$, so σ is continuous whenever $\sigma \in \mathrm{Aut}(\mathbb{R}/\mathbb{Q})$. By continuity, $\sigma = \mathit{id}_{\mathbb{R}}$ and $\mathrm{Aut}(\mathbb{R}/\mathbb{Q}) = \{\mathit{id}_{\mathbb{R}}\}$.

Problem 7.2.2. Let k be a field and let $t = P(x)/Q(x)$, where $P(x)$ and $Q(x)$ are relatively prime polynomials over k and $Q(x) \neq 0$. Then $k(x)$ is a simple extension over $k(t)$ obtained by adjoining t. Show that the extension degree of $k(x)/k(t)$ is $\max\{\mathit{deg}\, P(x), \mathit{deg}\, Q(x)\}$.

Solution. Because $k(x) = k(t)(x)$, it suffices to find the degree of the minimal polynomial of x over $k(t)$. Observe that the indeterminate x is satisfied by the polynomial $f(s) := P(s) - tQ(s) \in k(t)[s]$, and we will show that $f(s)$ is irreducible over $k(t)$.

In fact, since $f(s) \in k[t][s]$ and $\mathit{cont}(f) \sim_\times 1$, it suffices to show that $f(s)$ is irreducible over $k[t]$ (by Gauss's lemma), for the field of fractions of $k[t]$ is $k(t)$. Since $k[t][s] = k[t, s] = k[s][t]$, it also suffices to show that the polynomial $f(s)$ over $k[s]$ in t is irreducible over $k[s]$. The latter is clear, because $\mathit{deg}_t f(s) = 1$ and $P(s)$ and $Q(s)$ are relatively prime. Therefore, $[k(x) : k(s)] = \mathit{deg}_s f(s) = \max\{\mathit{deg}\, P(x), \mathit{deg}\, Q(x)\}$.

Problem 7.2.3 (Lüroth's theorem)**.** Show that $\mathrm{Aut}(k(x)/k) \approx PGL_2(k)$, where k is a field and x is an indeterminate.

Solution. Any k-automorphism of $k(x)$ is completely determined by its action on x. Write $\sigma(x) = f(x)/g(x)$ for some relatively prime polynomials $f(x)$, $g(x)$ over k such that $g(x) \neq 0$. Because σ fixes k, $k(\sigma(x)) = \sigma(k(x))$; because an automorphism is surjective, $\sigma(k(x)) = \sigma(x)$. Hence, $k(\sigma(x)) = k(x)$ and $[k(x) : k(\sigma(x))] = 1$. This implies that *deg* $f(x)$ and *deg* $g(x)$ are not greater than 1, with at least one of them being 1. Therefore, $\sigma(x) = (ax+b)/(cx+d)$ for some $a, b, c, d \in k$ and $ad - bc \neq 0$.

Conversely, assume that a k-embedding $\tau : k(x) \to k(x)$ defined by $\tau(x) = (ax+b)/(cx+d)$ with $a, b, c, d \in k$ and $ad - bc \neq 0$ is given. Because $\tau(k(x)) = k(\tau(x))$ and $[k(x) : k(\tau(x))] = \max\{\textit{deg}\,(ax+b), \textit{deg}\,(cx+d)\} = 1$, we have $\tau(k(x)) = k(x)$, so τ is a k-automorphism of $k(x)$.

So far, we have found a surjection $\rho : GL_2(k) \to \mathrm{Aut}(k(x)/k)$, defined by

$$\rho \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \sigma.$$

Because ρ is a group homomorphism, by the first isomorphism theorem, we have

$$GL_2(k)/\textit{ker}\,\rho \approx \mathrm{Aut}(k(x)/k),$$

where $\textit{ker}\,\rho = \{sI : s \in k^\times\} = Z(GL_2(k))$. Therefore, $\mathrm{Aut}(k(x)/k) \approx PGL_2(k)$.

Part III

Galois theory

Chapter 8

Basic Galois theory

8.1 Basic observation regarding Galois extensions

Remark that an algebraic field extension which is both separable and normal is called a Galois extension. When E/F is a Galois extension, we write $\mathrm{Aut}(E/F) = \mathrm{Gal}(E/F)$; because E/F is a normal extension, we have $\mathrm{Aut}(E/F) = \mathrm{Gal}(E/F) = \mathrm{Emb}(E/F)$ and we call $\mathrm{Gal}(E/F)$ the Galois group of E/F (note that $\mathrm{Aut}(E/F)$ is a group with the multiplication being function composition.)

Remark. (a) (A review of Theorem 6.2.4) An algebraic field extension E/F is a normal extension if and only if $\mathrm{Emb}(E/F) = \mathrm{Aut}(E/F)$. Hence, in particular, if E/F is a finite extension, then E/F is a normal extension if and only if $[E : F]_{\mathsf{sep}} = |\mathrm{Aut}(E/F)|$.

(b) (Finite Galois extension) A finite field extension E/F is a Galois extension if and only if $[E : F] = |\mathrm{Aut}(E/F)|$. (It is left as an exercise to check the equivalence.)

(c) Except for Section 11.4, all Galois extensions are assumed to be a finite extension.

Note that if K/F is a Galois extension and E is an intermediate subfield of K/F, then K/E is a Galois extension and $\mathrm{Gal}(K/E) \leq \mathrm{Gal}(K/F)$. Conversely, given a subgroup H of $\mathrm{Gal}(K/F)$, we define the fixed field K^H of H in K by

$$K^H := \{x \in K : \sigma x = x \text{ for all } \sigma \in H\}.$$

It is easy to check that $F \leq K^H \leq K$.

In the following section, the fundamental theorem of finite Galois's extensions, also known as Galois's main theorem, is introduced, in which we are interested in a one-to-one bijection between the collection of the intermediate subfields of a finite Galois extension and the collection of the subgroups of the Galois group of the extension. The following propositions, which could be introduced before proving Galois's main theorem, are moved to this section, due to its generality.

Proposition 8.1.1. Suppose that E/F is a separable extension. If there is a positive integer n such that $[F(\alpha) : F] \leq n$ for all $\alpha \in E$, then (E/F is a finite extension and) $[E : F] \leq n$.

Proof. By assumption, there is an element $\beta \in E$ for which $[F(\beta) : F]$ is the greatest.

Goal: To show that $E = F(\beta)$.

In fact, our goal can easily be deduced from the primitive element theorem for finite separable extensions. If $F(\beta) < E$, then there is an element $\gamma \in E \setminus F(\beta)$ and $F(\beta) < F(\beta, \gamma)$; because $F(\beta, \gamma)/F$ is a finite separable extension, there is an element $\alpha \in F(\beta, \gamma)$ such that $F(\beta, \gamma) = F(\alpha)$, which contradicts the maximality of β. □

Lemma 8.1.2 (Artin's theorem)**.** Let K be a field and H be a finite subgroup of $\mathrm{Aut}(K)$. Then K/K^H is a Galois extension and $\mathrm{Gal}(K/K^H) = H$.[1]

[1] If H is an infinite subgroup of $\mathrm{Aut}(K)$, Artin's theorem is not valid, in general. Hence, the map $E \mapsto \mathrm{Gal}(K/E)$ is not a surjection, in general.

Proof. We first show that K/K^H is a Galois extension. For this, we show that for any $\alpha \in K$ the minimal polynomial $m(t)$ of α over K^H is separable and has all roots in K.

Let $\{\sigma_1, \cdots, \sigma_r\}$ be a maximal subset of H such that $\sigma_1\alpha, \cdots, \sigma_r\alpha$ are pairwise distinct. Letting $\tau_i = \sigma_1^{-1} \circ \sigma_i$ for each integer $i = 1, \cdots, r$, then $\tau_1\alpha, \cdots, \tau_r\alpha$ are pairwise distinct. If they are not maximally pairwise distinct, then there is another field automorphism τ_{r+1} of K such that $\tau_1\alpha, \cdots, \tau_r\alpha, \tau_{r+1}\alpha$ are pairwise distinct; then $\sigma_1\alpha, \cdots, \sigma_r\alpha, \sigma_{r+1}\alpha$ are also pairwise distinct, which contradicts the maximality of $\{\sigma_1, \cdots, \sigma_r\}$. Hence, $\{\tau_1 = id_K, \cdots, \tau_r\}$ is also a maximal subset of H such that $\tau_1\alpha, \cdots, \tau_r\alpha$ are pairwise distinct; thus, we may assume that $\sigma_1 = id_K$.

Define a polynomial

$$f(t) := (t - \sigma_1\alpha) \cdots (t - \sigma_r\alpha),$$

which is satisfied by α. Given $\tau \in H$, by the maximality of $\{\sigma_1, \cdots, \sigma_r\}$, we have $\tau \circ \sigma_i \in \{\sigma_1, \cdots, \sigma_r\}$ for all i; $\tau \in H$ *permutes* $\{\sigma_1, \cdots, \sigma_r\}$. Therefore, $f^\tau(t) = f(t)$ and $f(t) \in K^H[t]$, for evey coefficient of $f(t)$ is fixed by every field automorphism in H. Because $f(t)$ is a multiple of $m(t)$ and $f(t)$ is separable, $m(t)$ is separable and K/K^H is a separable extension. Moreover, a root of $m(t)$ is of the form $\sigma_i\alpha$ for some i, which is contained in K, so K/K^H is a normal extension. Because $[F(\alpha) : F] \leq r \leq |H| < \infty$ for all $\alpha \in K$, we conclude that K/K^H is a finite Galois extension with $[K : K^H] \leq |H|$.

We finally show that $\mathrm{Gal}(K/K^H) = H$. It is clear that $H \leq \mathrm{Gal}(K/K^H)$, thus it follows from

$$|H| \leq |\mathrm{Gal}(K/K^H)| = [K : K^H] \leq |H|$$

that $\mathrm{Gal}(K/K^H) = H$. □

8.2 Fundamental theorems of finite Galois extensions

Theorem 8.2.1 (Galois's theorem (Part I)). Let K/F be a finite Galois extension.

(a) There is an order-reversing bijection between the intermediate subfields of K/F and the subgroups of $\mathrm{Gal}(K/F)$, which maps an intermediate subfield E of K/F to the corresponding Galois group $\mathrm{Gal}(K/E)$ and a subgroup H of $\mathrm{Gal}(K/F)$ to the fixed field K^H.

(b) If E is an intermediate subfield of K/F, then $\mathrm{Emb}(E/F)$ is in bijection with $\mathrm{Gal}(K/F)/\mathrm{Gal}(K/E)$. Furthermore, E/F is a Galois extension if and only if $\mathrm{Gal}(K/E) \trianglelefteq \mathrm{Gal}(K/F)$. In particular, if E/F is a Galois extension, then

$$\mathrm{Gal}(E/F) \approx \frac{\mathrm{Gal}(K/F)}{\mathrm{Gal}(K/E)}.$$

Remark. Let K/F be a finite Galois extension. Suppose that $F \leq E_1 \leq E_2 \leq K$ and $H_1 \leq H_2 \leq \mathrm{Gal}(K/F)$. By order-reversing we mean that $\mathrm{Gal}(K/E_1) \geq \mathrm{Gal}(G/E_2)$ and $K^{H_1} \geq K^{H_2}$, which is easy to verify. Hence, the subfield lattice of a finite Galois extension and the *flipped* subgroup lattice of the Galois group are the same. Moreover, corresponding extension degrees and group indices coincide; for example, $[E_2 : E_1] = [K : E_1]/[K : E_2] = [\mathrm{Gal}(K/E_1) : \mathrm{Gal}(K/E_2)]$ and $[K^{H_1} : K^{H_2}] = [\mathrm{Gal}(K/K^{H_2}) : \mathrm{Gal}(K/K^{H_1})] = [H_2 : H_1]$. Finally, since an intermediate subfield E of K/F is a Galois extension over F if and only if E/F is a normal extension, E/F is a normal extension if and only if $\mathrm{Gal}(K/E)$ is a normal subgroup of $\mathrm{Gal}(K/F)$.

To prove Galois's theorem, we need the following proposition:

Proposition 8.2.2. Suppose that K/F is a finite Galois extension and $F \leq E \leq K$. Then $K^{\mathrm{Gal}(K/E)} = E$.

Proof. Write $L = K^{\mathrm{Gal}(K/E)}$. It is clear that $E \leq K^{\mathrm{Gal}(K/E)} = L$, and it follows that $\mathrm{Gal}(K/L) \leq \mathrm{Gal}(K/E)$. If $\sigma \in \mathrm{Gal}(K/E)$, then $\sigma x = x$ for all $x \in L$, thus $\sigma \in \mathrm{Gal}(K/L)$, i.e., $\mathrm{Gal}(K/E) \leq \mathrm{Gal}(K/L)$. Thus, $\mathrm{Gal}(K/E) = \mathrm{Gal}(K/L)$ and

$$[K : E] = |\mathrm{Gal}(K/E)| = |\mathrm{Gal}(K/L)| = [K : L]$$

implies that $L = E$. □

Remark. This also explains that the map $E \mapsto \mathrm{Gal}(K/E)$ is injective; if $\mathrm{Gal}(K/E_1) = \mathrm{Gal}(K/E_2)$, then $E_1 = K^{\mathrm{Gal}(K/E_1)} = K^{\mathrm{Gal}(K/E_2)} = E_2$.

Proof of (a) of Theorem 8.2.1. Clearly, the given bijection is order-reversing. If $F \leq E \leq K$, then $E \mapsto \mathrm{Gal}(K/E) \mapsto K^{\mathrm{Gal}(K/E)} = E$ by the preceeding proposition; if $H \leq \mathrm{Gal}(K/F)$, then $H \mapsto K^H \mapsto \mathrm{Gal}(K/K^H) = H$ by Artin's theorem. □

Proposition 8.2.3. Let K/F be a Galois extension (not necessarily finite) and suppose $\sigma \in \mathrm{Gal}(K/F)$. If $F \leq E \leq K$, then both K/E and $K/\sigma E$ are Galois extensions, and

$$\mathrm{Gal}(K/\sigma E) = \sigma \cdot \mathrm{Gal}(K/E) \cdot \sigma^{-1}.$$

Proof. It is clear that K/E and $K/\sigma E$ are Galois extensions. Define a map $\rho : \mathrm{Gal}(K/E) \to \mathrm{Gal}(K/\sigma E)$ by $\rho(\tau) = \sigma \circ \tau \circ \sigma^{-1}$. Then ρ is a well-defines group homomorphism with $\mathit{ker}\rho = \{\mathit{id}_K\}$. Also, given $\eta \in \mathrm{Gal}(K/\sigma E)$, clearly $\tau = \sigma^{-1} \circ \eta\sigma \in \mathrm{Gal}(K/E)$ and $\rho(\tau) = \eta$, so ρ is surjective. Therefore, $\mathrm{Gal}(K/\sigma E) = \mathit{im}\,\rho = \sigma \cdot \mathrm{Gal}(K/E) \cdot \sigma^{-1}$. □

Proof of (b) of Theorem 8.2.1. Because E/F is a separable extension, we have

$$|\mathrm{Emb}(E/F)| = [E : F] = \frac{[K : F]}{[K : E]} = [\mathrm{Gal}(K : F) : \mathrm{Gal}(K/E)],$$

so $\mathrm{Emb}(E/F)$ and $\mathrm{Gal}(K/F)/\mathrm{Gal}(K/E)$ are in bijection.

We now prove the normality part.

(i) Suppose that E/F is a normal extension (or equivalently, a Galois extension). Define a group homomorphism $\rho : \mathrm{Gal}(K/F) \to \mathrm{Gal}(E/F)$ by

$$\rho(\sigma) = \sigma|_E \quad (\sigma \in \mathrm{Gal}(K/F)).$$

It is clear that $\mathit{ker}\,\rho = \mathrm{Gal}(K/E)$. Given $\tau \in \mathrm{Gal}(E/F)$, there is an extension $\widetilde{\tau} : K \to \overline{F}$, where $\overline{F}$ is an algebraic closure of F containing K. The desired isomoprhism follows from the first isomoprhism theorem.

(ii) Assume that E/F is not a normal extension (or equivalently, not a Galois extension). Then there is an F-embedding $\sigma : E \hookrightarrow \overline{F}$ such that $\sigma E \neq E$. Then, $\mathrm{Gal}(K/E) \neq \mathrm{Gal}(K/\sigma E)$ by (a) of Theorem 8.2.1, while

$$\mathrm{Gal}(K/\sigma E) = \sigma \cdot \mathrm{Gal}(K/E) \cdot \sigma^{-1} = \mathrm{Gal}(K/E).$$

Therefore, if $\mathrm{Gal}(K/E)$ is a normal subgroup of $\mathrm{Gal}(K/F)$, then E/F is a normal (Galois) extension.

The desired isomoprhism under the condition that E/F is a normal extension follows from $\mathrm{Gal}(K/E) = \mathit{ker}\,\rho \trianglelefteq \mathrm{Gal}(K/F)$. □

The following further properties of Galois correspondence can be easily verified.

Theorem 8.2.4 (Galois's theorem (Part II)). Let K/F be a finite Galois extension and suppose E_1, E_2 are intermediate subfields of K/F. Write $H_1 = \mathrm{Gal}(K/E_1)$ and $H_2 = \mathrm{Gal}(K/E_2)$.

(a) $\mathrm{Gal}(K/E_1E_2) = H_1 \cap H_2$, i.e., $K^{H_1 \cap H_2} = E_1E_2$.

(b) $\mathrm{Gal}(K/(E_1 \cap E_2)) = \langle H_1, H_2 \rangle$, i.e., $K^{\langle H_1, H_2 \rangle} = E_1 \cap E_2$.

Proof. We first show that $K^{H_1 \cap H_2} = E_1E_2$. Since E_1E_2 contains E_1 and E_2, $\mathrm{Gal}(K/E_1E_2)$ is contained in H_1 and H_2, so $K^{H_1 \cap H_2} \leq K^{\mathrm{Gal}(K/E_1E_2)} = E_1E_2$. Conversely, since $H_1 \cap H_2$ is contained in H_1 and H_2, its fixed field $K^{H_1 \cap H_2}$ contains E_1 and E_2, hence $E_1E_2 \leq K^{H_1 \cap H_2}$.

We now prove the second correspondence. Since $E_1 \cap E_2$ is contained in E_1 and E_2, $\mathrm{Gal}(K/(E_1 \cap E_2))$ contains $H_1 \cup H_2$, hence $E_1 \cap E_2 \leq K^{\langle H_1, H_2 \rangle}$. Conversely, since $K^{\langle H_1, H_2 \rangle}$ is contained in K^{H_1} and K^{H_2}, $K^{\langle H_1, H_2 \rangle} \leq E_1 \cap E_2$. □

Theorems 8.2.1 and 8.2.4, together, are called Galois's main theorem. Sometimes, the following correspondence is also included in Galois's main theorem.

Proposition 8.2.5. Suppose that K/F and L/F are finite Galois extensions, where $K, L \le \overline{F}$. Then KL/F is a finite Galois extension and $\mathrm{Gal}(KL/L) \approx \mathrm{Gal}(K/(K \cap L))$.

Proof. By assumption, it is clear that the extension KF/L is finite, separable, and normal, i.e., KF/L is a finite Galois extension. To show the isomorphism, consider the map $\rho : \mathrm{Gal}(KL/L) \to \mathrm{Gal}(K/(K \cap L))$ defined by $\rho(\sigma) = \sigma|_K$ for $\sigma \in \mathrm{Gal}(KL/L)$. Since K/F is a normal extension, $\sigma(K) = K$ for all $\sigma \in \mathrm{Gal}(KL/L)$, i.e., ρ is a well-defined group homomorphism. Also, $\mathit{ker}\,\rho = \{\mathit{id}_{KL}\}$, so ρ is injective. Thus, it remains to show that ρ is surjective. The problem in this step is we could not apply the isomoprhism extension theorem to prove the surjectivity, for an extension may not be the identity map on L. Instead, we show that ρ is surjective by showing $\mathit{im}\,\rho = \mathrm{Gal}(K/(K \cap L))$. For this, it suffices to show $\mathit{im}\,\rho \ge \mathrm{Gal}(K/(K \cap L))$, or equivalently, $K^{\mathit{im}\,\rho} \le K \cap L$. If $x \in K^{\mathit{im}\,\rho}$ and $\sigma \in \mathrm{Gal}(KL/L)$, then $\sigma(x) = \sigma|_K(x) = x$. Thus, $x \in (KL)^{\mathrm{Gal}(KL/L)} = L$, implying that $K^{\mathit{im}\,\rho} \le K \cap L$, as desired. □

Remark. The following results can be considered corollaries of the above proposition: Suppose K/F and L/F are finite Galois extensions with $K, L \le \overline{F}$.

(a) $[KL : F] = [KL : L][L : F] = \dfrac{[K : F][L : F]}{[K \cap L : F]}$.

(b) $[KL : L]$ divides $[K : F]$. In particular, $[KL : L] = [K : F]$ if and only if $K \cap L = F$.

Remark. In the above proof, one might think of the following proof with a gap when proving the surjectivity of ρ by constructing an extension $\widetilde{\tau} \in \mathrm{Gal}(KL/L)$ of $\tau \in \mathrm{Gal}(K/(K \cap L))$.

(1) Since L/F is a finite separable extension, by the primitive element theorem, there is an element $\gamma \in L$ such that $L = (K \cap L)(\gamma)$.

(2) Hence, $KL = K(\gamma)$. If $\gamma \in K$, there is nothing to prove, for $K = KL$ and $L \le K$.

(3) Assume $\gamma \notin K$. Since γ is an algebraic conjugate of γ, by the isomoprhism extension theorem, there is an extension $\widetilde{\tau} : KL \to KL$ extending τ. It is easy to check that $\widetilde{\tau} \in \mathrm{Gal}(KL/L)$.

In the above proof, when one seeks to apply the isomophism extension theorem, one should consider the minimal polynomial $m(t)$ of γ over K and $m^{\tau}(t)$. Although $m(\gamma) = 0$ is clear, $m^{\tau}(t)$ may not be satisfied by γ, unless $m(t) \in (K \cap L)[t]$, where the field $K \cap L$ is fixed by τ. (We say this error is a 'gap,' because it is in fact true, as justified in Problem 8.3.1.)

The following correspondence will show some significance when computing the Galois group of a reducible polynomial over a field.

Proposition 8.2.6. Suppose that K/F and L/F are Galois extensions, where $K, L \le \overline{F}$, and define the map $\rho : \mathrm{Gal}(KL/F) \to \mathrm{Gal}(K/F) \times \mathrm{Gal}(L/F)$ by $\rho(\sigma) = (\sigma|_K, \sigma|_L)$ for $\sigma \in \mathrm{Gal}(KL/F)$.

(a) ρ is a well-defined group monomorphism. Hence, $\mathrm{Gal}(KL/F)$ embeds into $\mathrm{Gal}(K/F) \times \mathrm{Gal}(L/F)$.

(b) Assume further that the field extensions K/F and L/F are finite. Then $|\mathit{im}\,\rho| = [KL : F] = [K : F][L : F] = |\mathrm{Gal}(K/F) \times \mathrm{Gal}(L/F)|$ if and only if $K \cap L = F$. In other words, ρ is a group isomophism if and only if $K \cap L = F$.

Observation 8.2.7. We review some properties regarding field compositions. Suppose that K, L are intermediate subfields of $\overline{F}/F$ so that the composition KL of K and L is well-defined.

(i) If K/F is a finite (algebraic, separable, normal) extension, then so is KL/L.

(ii) Hence, if K/F is a finite Galois extension, then so is KL/L. (In fact, if K/F is a Galois extension, then so is KL/L.) Furthermore, we have $\mathrm{Gal}(KL/L) \approx \mathrm{Gal}(K/(K \cap L))$. Hence, $[KL : L] = [K : K \cap L]$, and $[KL : L] = [K : F]$ if and only if $K \cap L = F$.

Note from Theorem 6.2.9 that given an algebraic field extension E/F there is the smallest field K containing E such that K/F is a normal extension, and that K/F is the smallest Galois extension if E/F is assumed to be a separable extension. Thus, the normal closure of a separable extension is often called a Galois closure.

One last remark:

Remark. Suppose that K/F is a Galois extension and $F \leq E \leq K$. Let $\sigma \in \mathrm{Gal}(K/F)$ and $\tau \in \mathrm{Emb}(E/F)$, where an algebraic closure $\overline{F}$ of F is given. By the isomophism extension theorem, there is an F-embedding $\widetilde{\tau} : K \hookrightarrow \overline{F}$ extending τ. Since K/F is a normal extension, $\widetilde{\tau}K = K$, so $\tau E \leq K$ and $\sigma \circ \tau : E \hookrightarrow K$ is a well-defined F-embedding of E into $\overline{F}$. Hence, an element of $\mathrm{Gal}(K/F)$ permutes the elements of $\mathrm{Emb}(E/F)$ by left multiplication.

8.3 Some problems regarding Galois's theorem

Problem 8.3.1. Suppose that K/F and L/F are finite Galois extensions with $K, L \leq \overline{F}$. As in the preceeding remark, write $L = (K \cap L)(\gamma)$. Show that the minimal polynomial of γ over K and over $K \cap L$ are the same.

Solution. Using the suggested notations, we have $KL = K(\gamma)$. Letting $m_1(t)$ and $m_2(t)$ be the minimal polynomial of γ over $K \cap L$ and over K, respectively, because $m_2(t)|m_1(t)$, it suffices to show that $[K : K \cap L] = [KL : K]$ (already justified); this implies *deg*$m_1(t) =$ *deg*$m_2(t)$ and $m_1(t) = m_2(t)$, as desired.

Problem 8.3.2. Find the minimal polynomial of $1 + \sqrt[3]{2} + \sqrt[3]{4}$ over $\mathbb{Q}$.

Solution. Considering a Galois extension over $\mathbb{Q}$ containing $\alpha := 1 + \sqrt[3]{2} + \sqrt[3]{4}$, it is natural to suggest $E := \mathbb{Q}(\rho, \zeta)$, the splitting field for $t^3 - 2$ over $\mathbb{Q}$. (Here, $\rho = \sqrt[3]{2}$ and $\zeta = \exp(2\pi i/3)$.) Computing its Galois group, we find that $\mathrm{Gal}(E/\mathbb{Q}) = \langle \sigma, \tau \rangle$, where

$$\sigma : \begin{cases} \rho \mapsto \rho\zeta \\ \zeta \mapsto \zeta \end{cases}, \quad \tau : \begin{cases} \rho \mapsto \rho \\ \zeta \mapsto \zeta^{-1} \end{cases}.$$

If $f(t)$ is a nonconstant polynomial over $\mathbb{Q}$, then $f(t)$ is fixed by the action of automorphisms in $\mathrm{Gal}(E/\mathbb{Q})$ by Galois's theorem. Hence, if $f(\alpha) = 0$, then $\eta\alpha$ is also a root of $f(t)$, where $\eta \in \mathrm{Gal}(E/\mathbb{Q})$; this implies that the minimal polynomial $m(t)$ of α over $\mathbb{Q}$ is necessarily satisfied the following elements:

$$1 + \rho + \rho^2, \quad 1 + \rho\zeta + \rho^2\zeta^{-1}, \quad 1 + \rho\zeta^{-1} + \rho^2\zeta.$$

Because $\mathbb{Q}$ is of characteristic 0, $m(t)$ is separable. Hence, $m(t)$ is divisible by

$$(t - (1 + \rho + \rho^2))(t - (1 + \rho\zeta + \rho^2\zeta^{-1}))(t - (1 + \rho\zeta^{-1} + \rho^2\zeta)) = t^3 - 3t^2 - 3t - 1.$$

Since $t^3 - 3t^2 - 3t - 1$ is irreducible over $\mathbb{Q}$, we conclude that $m(t) = t^3 - 3t^2 - 3t - 1$.

Remark. In fact, when K/F is a finite Galois extension and $\alpha \in K$, then the minimal polynomial of α over F is the square-free part $p(t)$ of

$$\prod_{\sigma \in \mathrm{Gal}(K/F)} (t - \sigma\alpha).$$

Here's a justification. By Galois's theorem, the minimal polynomial $m(t)$ of α over F is satisfied by $\sigma\alpha$ for all $\sigma \in \mathrm{Gal}(K/F)$, so $m(t)$ is necessarily divisible by $p(t)$. On the other hand, because the roots of $p(t)$ are the whole pairwise distinct $\sigma\alpha$'s (even when counting multiplicity), we have $p(t) \in F[t]$ by Galois's theorem. This proves that $p(t)$ is the minimal polynomial of α over F.

Remark. Because a finite Galois extension is a finite separable extension, the primitive element theorem is applicable in this case. Hence, if K/F is a finite Galois extension, then there is an element $\alpha \in K$ such that $K = F(\alpha)$.

Problem 8.3.3. Let K/F be a Galois group of extension degree p^n, where p is a positive prime number and n is a positive integer. Show that, for each integer $1 \leq r \leq n$, that there is a subfield E_r of K/F such that E_r/F is a Galois extension of extension degree p^r.

Solution. Since $\mathrm{Gal}(K/F)$ is a group of order p^n, for each integer $1 \leq r \leq n$, there is a normal subgroup H_r of G such that $[G : H_r] = p^r$.[2] Therefore, the fixed field $E_r = K^{H_r}$ is a Galois extension over F of degree p^r.

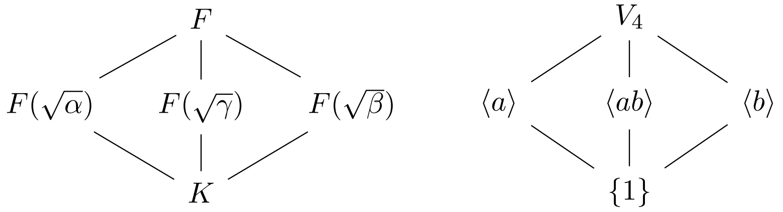
Problem 8.3.4 (Biquadratic extension)**.** Let F be a field such that $\mathrm{char}(F) \neq 2$.

(a) Suppose that $K = F(\sqrt{D_1}, \sqrt{D_2})$, where $D_1, D_2 \in F$ have the property that none of D_1, D_2 or D_1D_2 is a square in F. Prove that K/F is a Galois extension with the Galois group isomorphic to the Klein 4-group.

(b) Conversely, suppose that K/F is a Galois extenion with the Galois group isomorphic to the Klein 4-group. Show that $K = F(\sqrt{D_1}, \sqrt{D_2})$, where $D_1, D_2 \in F$ have the property that none of D_1, D_2 or D_1D_2 is a square in F.

Solution. Assume first that $K = F(\sqrt{D_1}, \sqrt{D_2})$, where $D_1, D_2 \in F$ have the property that none of D_1, D_2 or D_1D_2 is a square in F. Then K/F is clearly a Galois extension with the extension degree at most 4. In fact, K is the splitting field for $(t^2 - D_1)(t^2 - D_2)$ over F, so (after identification) $\mathrm{Gal}(K/F) \leq \mathrm{Gal}(F(\sqrt{D_1})/F) \times \mathrm{Gal}(F(\sqrt{D_2})/F) \approx V_4$. Moreover, because none of D_1, D_2 or D_1D_2 is a square in F, $F(\sqrt{D_1}) \cap F(\sqrt{D_2}) = F$, thus the Galois group of K/F is the Klein 4-group.

Conversely, assume that K/F is a Galois extension with the Galois group isomorphic to the Klein 4-group $\langle a, b : a^2, b^2, aba^{-1}b^{-1} \rangle$.



where $\alpha, \beta, \gamma \in F$ are not squares in F. Because a fixes α and b fixes β, $ab = a \circ b$ fixes $\alpha\beta$. Moreover, since $F(\sqrt{\alpha}) \neq F(\sqrt{\beta})$, $\alpha\beta$ is not a square in F. (Hence, we may let $\gamma = \alpha\beta$.) Therefore, $K = F(\sqrt{\alpha}, \sqrt{\beta})$.

8.4 Abelian extensions and solvable extensions

Definition 8.4.1. Let K/F be a Galois extension.

(a) (Abelian extension) K/F is called an abelian extension if $\mathrm{Gal}(K/F)$ is an abelian group.

(b) (Solvable extension) K/F is called a solvable extension if $\mathrm{Gal}(K/F)$ is a solvable group.

Throughout this section, in order for Galois's theorem to be valid, we assume that all extensions are finite extensions. We introduce some applications of Galois's theorem in some kinds of finite extensions.

Observation 8.4.2. If K/F is a finite cyclic(abelian) extension and $F \leq E \leq K$, then K/E and E/F are also cyclic(abelian) extensions. The converse is not true, in general.

Proposition 8.4.3. Suppose that $F \leq E \leq K$ and K/F is a finite Galois extension. If E/F and K/E are solvable extensions, then K/F is also a solvable extension.

Proof. $\mathrm{Gal}(E/F) \approx \mathrm{Gal}(K/F)/\mathrm{Gal}(K/E)$ and $\mathrm{Gal}(K/E)$ are solvable, so $\mathrm{Gal}(K/F)$ is solvable. □

Proposition 8.4.4. Suppose that $F \leq E \leq K$ and K/F is a solvable extension.

[2] This can be proved by deducing that the center of the Galois group is nontrivial and then applying the lattice isomorphism theorem for groups.

(a) K/E is a solvable extension.

(b) If E/F is a Galois extension, then E/F is a solvable extension.

Proof. (a) is clear, because a subgroup of a solvable group is solvable. (b) is clear, because $\mathrm{Gal}(E/F) \approx \mathrm{Gal}(K/F)/\mathrm{Gal}(K/E)$ is a quotient of a solvable group by its normal subgroup. □

Proposition 8.4.5. Suppose that K/F is a finite Galois extension. Then the followings are equivalent:

(a) K/F is a (finite) solvable extension.

(b) K/F has an abelian tower; there are fields $F_1, \cdots F_k$ such that

$$F = F_0 \leq F_1 \leq \cdots \leq F_{k-1} \leq F_k = K$$

and F_i/F_{i-1} is an abelian extension for $i = 1, \cdots, k$.

Proof. (This equivalence is almost clear by Galois's theorem.) Assume first that K/F is a finite solvable extension, and let $\{id_K\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_k = \mathrm{Gal}(K/F)$ be a 'solvability chain' of $\mathrm{Gal}(K/F)$. It is easy to check that $K = K^{H_0} \geq K^{H_1} \geq \cdots \geq K^{H_k} = F$ and $K^{H_{i-1}}/K^H$ is an abelian extension. Assuming that K/F has an abelian tower, Galois's theorem establishes a corresponding tower for $\mathrm{Gal}(K/F)$, and it is clear that $\mathrm{Gal}(F_i/F_{i-1}) \approx \mathrm{Gal}(K/F_{i-1})/\mathrm{Gal}(K/F_i)$ is abelian. □

Some topics regarding abelian extensions will be introduced later when studying cyclotomic extensions. In studying solvability of polynomial equations, we will justify that the equation is solvable by radicals if and only if its Galois group is a solvable group.

8.5 Galois groups of polynomials

Remark. Let F be a field and $f(t)$ be a nonconstant separable polynomial over F, and let $\alpha_1, \cdots, \alpha_n$ be the roots of $f(t)$, where $n = deg\, f(t)$. Let K be the splitting field for $f(t)$ over F.

(a) Every automorphism $\sigma \in \mathrm{Gal}(K/L)$ permutes the root of $f(t)$. Hence, the group action of $\mathrm{Gal}(K/L)$ on $\{\alpha_1, \cdots, \alpha_n\}$ (by left multiplication) affords a group embedding

$$\mathrm{Gal}(K/L) \hookrightarrow S_n.$$

In general, if $f(t) = f_1(t) \cdots f_k(t)$ is the factorization of $f(t)$ into irreducible polynomials in $F[t]$, then an automorphism $\sigma \in \mathrm{Gal}(K/L)$ permutes the roots of $f_i(t)$ for each $1 \leq i \leq k$, i.e., $\mathrm{Gal}(K/L)$ permutes the roots of the irreducible factors among themselves. Thus, the group action affords a group embedding

$$\mathrm{Gal}(K/L) \hookrightarrow S_{n_1} \times \cdots \times S_{n_d},$$

where $n_i = deg\, f_i(t)$ for each i.

(b) In particular, suppose that $f(t)$ is irreducible. Given any two roots α_i and α_j $(1 \leq i, j \leq n)$, by isomorphism extension theorem, id_F extends to an F-automorphism $\sigma : K \to K$ such that $\sigma\alpha_i = \alpha_j$ (how?). In other words, $\mathrm{Gal}(K/F)$ is transitive on the roots of each irreducible factor of $f(t)$.

(c) In (a), suppose, in particular, that $f(t) = g(t)h(t)$ for some nonconstant polynomial $g(t), h(t)$ over F. Then the splitting field K_f for $f(t)$ over F is the composition of the splitting field K_g and K_h for $g(t)$ and $h(t)$ over F, respectively. Thus, $G_f \hookrightarrow G_g \times G_h$ as explained in (a); here, $G_f \approx G_g \times G_h$ if and only if $K_g \cap K_h = F$.

Notation. Given a nonconstant polynomial $f(t)$ over F and its splitting field over F, $\mathrm{Gal}(K/F)$ is called the Galois group of $f(t)$ over F, and is denoted by $G_{f,F}$, or simply by G_f, if the base field F is understood. Also, unless stated otherwise, the splitting field for $f(t)$ over F is denoted by $K_{f,F}$, or shortly by K_f, if the base field F is understood.

Some basic propositions required to investigate Galois groups are given as the following two propositions.

Proposition 8.5.1. Let $f(t)$ be a nonconstant separable polynomial over F, and write $n = \textit{deg}\, f(t)$.

(a) G_f embeds into S_n. Furthermore, if $f(t) = f_1(t) \cdots f_k(t)$ is the factorization of $f(t)$ into irreducible polynomials over F, then G_f embeds into $S_{n_1} \times \cdots \times S_{n_k}$, where $n_i = \textit{deg}\, f_i(t)$ for each $i = 1, \cdots, k$.

(b) If $f(t)$ is irreducible over F, then n divides the order of G_f.

Proof. (a) is already proved in the beginning of this section. If $f(t)$ is irreducible and α is any root of $f(t)$, then the splitting field for $f(t)$ over F contains α, so n divides $|G_f|$. □

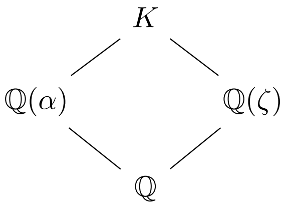
Proposition 8.5.2. Let $f(t)$ be a nonconstant separable polynomial over F. Then $f(t)$ is irreducible over F if and only if G_f acts transitively on the roots of $f(t)$.

Proof. Suppose that $f(t)$ is irreducible over F and let α and β be any roots of $f(t)$. By isomorphism extension theorem, there is an F-automorphism of K mapping α to β (why?), as desired.

Assume conversely that G_f acts on the roots of $f(t)$ transitively. If $f(t)$ is reducible, there are nonconstant polynomials $g(t), h(t) \in F[t]$ such that $f(t) = g(t)h(t)$. If α and β are roots of $g(t)$ and $h(t)$, respectively, there is an automorphism $\sigma \in G_f$ such that $\sigma\alpha = \beta$. So β is a root of $g(t)$, for $0 = \sigma(g(\alpha)) = g(\sigma\alpha) = g(\beta)$, which contradicts the separability of $f(t)$. □

From now on, throughout this section, F is assumed to be a perfect field, over which every irreducible polynomial is separable.

Example 8.5.3. Consider $f(t) = t^3 - 2 \in \mathbb{Q}[t]$. Its roots are $\alpha, \alpha\zeta, \alpha\zeta^2$, where $\alpha = \sqrt[3]{2}, \zeta = \exp(2\pi i/3)$. We then have the following (possibly incomplete) subfield lattice:



In fact, since $f(t)$ is irreducible over $\mathbb{Q}$, 3 divides $|G_f|$; because $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$, 2 also divides $|G_f|$; because $G_f \hookrightarrow S_3$, we conclude that $G_f \approx S_3$.

Example 8.5.4. Let $f(t) = t^4 - 2 \in \mathbb{Q}[t]$, and write $\alpha = \sqrt[4]{2}$. Then the splitting field K for $f(t)$ over $\mathbb{Q}$ is $\mathbb{Q}(\alpha, i)$. Since $[K : \mathbb{Q}] = [K : \mathbb{Q}(\alpha)][\mathbb{Q}(\alpha) : \mathbb{Q}] = 8$ and $f(t)$ is irreducible over $\mathbb{Q}$, G_f is isomorphic to a transitive subgroup of S_4. Therefore, $G_f \approx D_8$, where D_8 is the dihedral group of order 8.

To investigate explicitly, note that $\mathbb{Q}(i)/\mathbb{Q}$ and $K/\mathbb{Q}(i)$ are separable extensions. Thus, there are two distinct $\mathbb{Q}$-embbedings of $\mathbb{Q}(i)$ into $\overline{\mathbb{Q}}$:

$$\textit{id}_{\mathbb{Q}(i)}, \quad \gamma : i \mapsto -i.$$

Also, there are four distinct embeddings extending $\textit{id}_{\mathbb{Q}(i)}$ and γ, respectively; they map α to either α or $-\alpha$ or αi or $-\alpha i$. Letting σ and τ be the $\mathbb{Q}$-automorphisms such that

$$\sigma(\alpha) = \alpha, \quad \sigma(i) = -i,$$
$$\tau(\alpha) = \alpha i, \quad \tau(i) = i,$$

we find that $G_f = \langle \sigma, \tau \,|\, \sigma^2 = \tau^4 = \textit{id}_K, \sigma\tau\sigma = \tau^{-1} \rangle \approx D_8$.

Example 8.5.5. Let $f(t) = (t^2 - 2)(t^3 - 2) \in \mathbb{Q}[t]$ and write $a(t) = t^2 - 2$ and $b(t) = t^3 - 2$. Since $\sqrt{2} \notin K_b$, we have $K_a \cap K_b = \mathbb{Q}$, so $G_f \approx G_a \times G_b \approx Z_2 \times S_3$.

Example 8.5.6. Let $f(t) = (t^2 - 2)(t^2 - 3)(t^3 - 2) \in \mathbb{Q}[t]$. Then $K_f = \mathbb{Q}(\alpha, \beta, i)$, where $\alpha = \sqrt[6]{2}$ and $\beta = \sqrt{3}$. Letting $a(t) = t^2 - 2$ and $b(t) = (t^2 - 3)(t^3 - 2)$, we have $K_a = \mathbb{Q}(\sqrt{2})$ and $K_b = \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}, i)$, so $K_a \cap K_b = \mathbb{Q}$ and $G_f \approx G_a \times G_b$. It is easy to check that $G_b \approx Z_2 \times S_3$, so $G_f \approx Z_2 \times Z_2 \times S_3 \approx V_4 \times S_3$.

Example 8.5.7. Let $f(t) = (t^2 - 5)(t^5 - 1) \in \mathbb{Q}[t]$. Since $\sqrt{5} \in \mathbb{Q}(\zeta_5)$, $K_f = \mathbb{Q}(\zeta_5)$, thus $G_f \approx (\mathbb{Z}/5\mathbb{Z})^\times \approx Z_4$.

Example 8.5.8. We will find a necessary and sufficient condition of an integer d for $\sqrt{d}$ being contained in $\mathbb{Q}(\zeta_5)$. In fact, $\sqrt{d} \in \mathbb{Q}(\zeta_5)$ if and only if $\mathbb{Q}(\sqrt{d})$ is a subfield of $\mathbb{Q}(\zeta_5)$ containing $\mathbb{Q}$. By Galois theorem, the only proper subfield of $\mathbb{Q}(\zeta_5)/\mathbb{Q}$ is $\mathbb{Q}(\zeta_5 + \zeta_5^{-1}) = \mathbb{Q}(\sqrt{5})$, so $\sqrt{d} \in \mathbb{Q}(\zeta_5)$ if and only if $d = 5k^2$ for an integer k. In particular, $\zeta_3 \notin \mathbb{Q}(\zeta_5)$, for otherwise, $\sqrt{-3} \in \mathbb{Q}(\zeta_5)$, which contradicts our result.

Example 8.5.9. Let $f(t) = (t^3 - 2)(t^3 - 3) \in \mathbb{Q}[t]$ and write $\alpha = \sqrt[3]{2}$ and $\beta = \sqrt[3]{3}$. Letting $a(t) = t^3 - 2$ and $b(t) = t^3 - 3$, we have

$$[K_f : \mathbb{Q}] = \frac{[K_a : \mathbb{Q}][K_b : \mathbb{Q}]}{[K_a \cap K_b : \mathbb{Q}]} = 18.$$

To determine the isomorphic type of G_f, note that G_f is not abelian. Also, since $G_f \hookrightarrow S_3 \times S_3$, there is no element in G_f or order 9. Thus, G_f is one among all possible nonabelian groups of order 18 with no element of order 9.

Chapter 9

Some Galois extensions

9.1 Galois extensions over finite fields

Throughout this section, p is a positive prime number and $q = p^n$ for some positive integer n.

Theorem 9.1.1. $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \sigma_p \rangle \approx \mu_n$, where $\sigma_p : \mathbb{F}_{p^n} \to \mathbb{F}_{p^n}$ is the $\mathbb{F}_p$-automorphism defined by $\sigma_p(x) = x^p$ for $x \in \mathbb{F}_{p^n}$.

Proof. Of course, one could directly show that $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ and the cyclic group generated by σ_p are the same. Its rigorous justification, however, seems to have technical difficulty. Thus, we prove the thoerem by justifying that the subgroup $\langle \sigma_p \rangle$ of the Galois group has the same order of the Galois group.

Note that $|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$ and $\sigma_p \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$. Since $\sigma_p^r(x) = x^{p^r}$ for all integer r and $x \in \mathbb{F}_{p^n}$, the order of σ_p is n, as desired. □

Observation 9.1.2. (a) Considering the subgroup lattice of μ_n, there is a unique subgroup of index d, where d is a positive divisor of n. By Galois's thoerem, it is equivalent to the statement that there is a unique intermediate subfield of $\mathbb{F}_{p^n}/\mathbb{F}_p$ whose extension degree over $\mathbb{F}_p$ is d. In fact, $\mathbb{F}_{p^d}$ is such a field, so $\mathbb{F}_{p^d}$ is a unique interediate subfield of $\mathbb{F}_{p^n}/\mathbb{F}_p$ whose extension degree over $\mathbb{F}_p$ is d. Because μ_n is abelian, $\mathbb{F}_{p^d}/\mathbb{F}_p$ is clearly a (finite) Galois extension, and we have

$$\mathrm{Gal}(\mathbb{F}_{p^d}/\mathbb{F}_p) \approx \frac{\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)}{\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^d})}.$$

(b) Let x be an element of $\mathbb{F}_{p^n}$ and d be a positive divisor of n. By Galois's theorem, $x \in \mathbb{F}_{p^d}$ if and only if $\sigma_p^{n/d} x = x$. Writing $\mathbb{F}_{p^n} = \mathbb{F}_p(\alpha)$ for some $\alpha \in \mathbb{F}_{p^n}$, we can write $x = \alpha^k$ for some positive integer k.

Proposition 9.1.3. The polynomial $t^{p^n} - t$ is precisely the product of all the distinct irreducible polynomials over $\mathbb{F}_p$ of degree d, where d runs through all positive divisors of n.

Proof. □

We have observed that $t^p - t \in \mathbb{F}_p[t]$ is a *reducible* separable polynomial, whose roots are exactly the elements of $\mathbb{F}_p$. If one adds a nonzero constant to the polynomial, one can get a irreducible separable polynomial, as illustrated in the following proposition.

Proposition 9.1.4 (Artin-Schreier extension)**.** Let p be a positive prime number and a be a nonzero element of $\mathbb{F}_p$.

(a) The polynomial $f(t) = t^p - t + a \in \mathbb{F}_p[t]$ is irreducible and separable over $\mathbb{F}_p$.

(b) The splitting field K for $f(t)$ over $\mathbb{F}_p$ is $\mathbb{F}_{p^p}$. Writing $K = \mathbb{F}_p(\alpha)$, $\mathrm{Gal}(K/\mathbb{F}_p) = \langle \sigma_p \rangle$, where $\sigma_p : K \to K$ is the $\mathbb{F}_p$-automorphism defined by $\sigma_p \alpha = \alpha + 1$.

Proof. Because $f'(t) = -1 \neq 0$, $f(t)$ is separable. To show the irreducibility of $f(t)$, observe that $\beta + 1$ is a root of $f(t)$ if $\beta \in K$ is a root of $f(t)$. So, (after writing $\beta_i = \beta + (i-1)$ for each integer $1 \leq i \leq p$) we may write

$$f(t) = (t - \beta_1)(t - \beta_2) \cdots (t - \beta_p).$$

Letting $m_i(t)$ be the minimal polynomial of β_i over $\mathbb{F}_p$, we have $m_{i+k}(t) = m_i(t-k)$ for all allowed indices i, k. Hence, if $f(t)$ is not irreducible, then *deg* $m_1(t) = \cdots =$ *deg* $m_p(t) < p$, so $\beta_i \in \mathbb{F}_p$ for all $1 \leq i \leq p$; then, $f(t) = t^p - t$ and $a = 0$, a contradiction. Therefore, when $a \in \mathbb{F}_p$ is nonzero, $f(t)$ is an irreducible and separable polynomial over $\mathbb{F}_p$.

Since *deg* $f(t) = p$, the splitting field K for $f(t)$ over $\mathbb{F}_p$ is isomorphic to the finite field $\mathbb{F}_{p^p}$ and $\mathrm{Gal}(K/\mathbb{F}_p) \approx \mu_p$. Thus, we may write $K = \mathbb{F}_p(\alpha)$ for some $\alpha \in K$. To complete the proof, we need to justify that the *map* $\sigma_p : K \to K$ defined by $\sigma_p \alpha = \alpha + 1$ is an $\mathbb{F}_p$-automorphism of K of order p, which is easy to check. □

9.2 More on finite fields

9.3 Cyclotomic extensions

In this section, we study the polynomial $t^n - 1 \in F[t]$, where n is a positive integer and F is a fiven base field.

Definition 9.3.1 (n-th root of unity)**.** For a positive integer n, every member of the collection

$$\mu_n(\overline{F}) := \{\alpha \in \overline{F} : \alpha^n = 1\}$$

is called an n-th root of unity. Since $\mu_n(\overline{F})$ is a finite subgroup of the multiplicative group $F^\times$, $\mu_n(\overline{F})$ is a cyclic group. A generator of the finite cyclic group $\mu_n(\overline{F})$ is called a primitive n-th root of unity.

Example 9.3.2. $\mu_n(\overline{\mathbb{Q}}) = \{\exp(2\pi i k/n) : k \text{ is an integer such that } 0 \leq k \leq n-1\}$.

9.3.1 The splitting field for $t^n - 1$ over a finite field

Observation 9.3.3. Suppose that F is a field of characteristic $p > 0$ and let $n = qm$, where m is a positive integer relatviely prime to p.

(a) $\mu_p(\overline{F}) \approx \mathbb{F}_p$ and $\mu_q(\overline{F}) \approx \mathbb{F}_q$.

(b) We now show that $\mu_n(\overline{F}) = \mu_m(\overline{F})$ It is clear that $\mu_m(\overline{F}) \subset \mu_n(\overline{F})$. Suppose that $\alpha \in \mu_n(\overline{F})$. Then $(\alpha^m)^q = 1$ and $(\alpha^m - 1)^q = 0$, hence $\alpha \in \mu_m(\overline{F})$. Therefore, if $\mathrm{char}(F) = p > 0$ and when we consider $\mu_n(\overline{F})$, we may assume that $(n, p) = 1$.

Observation 9.3.4. Let F be a field of characteristic $p > 0$ and n be a positive integer which is relatively prime to p. Let ζ be a primitive n-th root of unity.

(a) $F(\zeta)$ is the splitting field for $t^n - 1 \in F[t]$ over F. Since $t^n - 1$ is a separable polynomial over F, $F(\zeta)/F$ is a finite Galois extension and $\mu_n(\overline{F}) = \{1, \zeta, \cdots, \zeta^{n-1}\}$.

(b) Since $\sigma \in \mathrm{Aut}(F(\zeta))$ fixes 1, σ permutes $\mu_n(\overline{F})$, i.e., $\sigma(\mu_n(\overline{F})) = \mu_n(\overline{F})$. Therefore, $\sigma\mu$ is also a primitive n-th root of unity, hence $\sigma\mu = \mu^k$ for some integer which is relatively prime to n.

Our first goal is to compute $\mathrm{Gal}(F(\zeta)/F)$ when $\mathrm{char}(F) = p > 0$.

Theorem 9.3.5. Suppose that F is a field of characteristic $p > 0$ and let n be a positive integer relatively prime to p, and let ζ be a primitive n-th root of unity. Then $\mathrm{Gal}(F(\zeta)/F)$ embeds into $(\mathbb{Z}/n\mathbb{Z})^\times$, so $F(\zeta)/F$ is an abelian extension.

Proof. Let $\phi : \mathrm{Gal}(F(\zeta)/F) \to (\mathbb{Z}/n\mathbb{Z})^\times$ be the map defiend by

$$\phi(\sigma) = \overline{k} \quad (\sigma \in \mathrm{Gal}(F(\zeta)/F))$$

where k is an integer such that $\sigma(\zeta) = \zeta^k$. Since $\sigma \in \mathrm{Gal}(F(\zeta)/F)$ is a field automorphism of $F(\zeta)$, $\sigma(\zeta)$ is a primitive n-th root of unity. Hence, $(n, k) = 1$ and $\overline{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$. It is easy to check that ϕ is an injective group homomorphism, as desired. □

Remark. Unlike the splitting field for $t^n - 1$ over $\mathbb{Q}$ which will be studied in the following subsection, $\mathrm{Gal}(F(\zeta)/F)$ need not be isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$. As an example, consider $\mathbb{F}_7$ and the splitting field K for $t^3 - 1$ over $\mathbb{F}_7$. Since $2 \in \mathbb{F}_7$ is a primitive third root of unity (in fact, $\mu_3(\overline{\mathbb{F}_7}) = \{1, 2, 4\} \subset \mathbb{F}_7$), we have $K = \mathbb{F}_7$ and $\mathrm{Gal}(K/\mathbb{F}_7) = \{id_{\mathbb{F}_7}\}$.

9.3.2 The splitting field for $t^n - 1$ over $\mathbb{Q}$

Definition 9.3.6. Let $\zeta_n \in \overline{\mathbb{Q}}$ be a primitive n-th root of unity.

(a) (Cyclotomic polynomial) The minimal polynomial $\Phi_n(t) \in \mathbb{Q}[t]$ of ζ_n is called the n-th cyclotomic polynomial.

(b) (Cyclotomic extension) The splitting field $\mathbb{Q}(\zeta_n)$ for $t^n - 1$ over $\mathbb{Q}$ is often called the n-th cyclotomic field. If $\mathbb{Q} \leq E \leq \mathbb{Q}(\zeta_n)$ for some positive integer n, we call E an cyclotomic extension over $\mathbb{Q}$.

Remark. In the above definition, the n-th cyclotomic polynomial is defined as the minimal polynomial of a primitive n-th root of unity over $\mathbb{Q}$. This definition of $\Phi_n(t)$ seems to depend on the choice of a primitive n-th root of unity.

Goal: To show that $\Phi_n(t)$ is the product of $t - \zeta$, where ζ runs through all primitive n-th roots of unity.

Fix a primitive n-th root ζ of unity and suppose $\Phi_n(t)$ is the minimal polynomial of ζ over $\mathbb{Q}$. If β is a root of $\Phi_n(t)$, then there is a $\mathbb{Q}$-isomorphism from $\mathbb{Q}(\beta)$ into $\mathbb{Q}(\zeta)$ mapping β to ζ. Since $\mathbb{Q}(\zeta)$ is the splitting field for $\Phi_n(t)$ over $\mathbb{Q}$, $\mathbb{Q}(\beta) = \mathbb{Q}(\zeta)$ and β is a primitive n-th root of unity. In other words, every root of $\Phi_n(t)$ is a primitive n-th root of unity. Conversely, if γ is a primitive n-th root of unity, there is a $\mathbb{Q}$-isomorphism from $\mathbb{Q}(\zeta)$ to $\mathbb{Q}(\gamma)$ mapping ζ to γ, so γ is an algebraic conjugate of ζ and is a root of $\Phi_n(t)$. Since char$(\mathbb{Q}) = 0$, $\Phi_n(t)$ is separable, which completes the proof. To be precise, whenever n is a positive integer,

$$\Phi_n(t) = \prod_{\substack{1 \leq k \leq n \\ (n,k)=1}} \left(t - \exp\left(i\frac{2\pi k}{n} \right) \right).$$

Because *deg* $\Phi_n(t)$ is the number of primitive n-th roots of unity, *deg* $\Phi_n(t)$ is the number of positive integers not greather than n which are relatively prime to n. Therefore, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$, where ϕ is the Euler's ϕ-function.

Example 9.3.7. Let p be a positive prime number. Since $t^p - 1 = (t - 1)(t^{p-1} + t^{p-2} + \cdots + t + 1)$ is a separable polynomial with roots $1, \zeta_p, \zeta_p^2, \cdots, \zeta_p^{p-1}$, ζ_p satisfies the polynomial $t^{p-1} + t^{p-2} + \cdots + t + 1$. Moreover, letting $t - 1 = s$ and applying Eisenstein's criterion, we can deduce that $t^{p-1} + t^{p-2} + \cdots + t + 1$ is an irreducible polynomial over $\mathbb{Q}$. Therefore, $\Phi_p(t) = t^{p-1} + t^{p-2} + \cdots + t + 1$ whenever p is a positive prime number.

Observation 9.3.8. By considering the orders of n-th roots of unity, we have

$$t^n - 1 = \prod_{\zeta \in \mu_n(\overline{\mathbb{Q}})} (t - \zeta) = \prod_{0<d|n} \prod_{\zeta \in \mu_d(\overline{\mathbb{Q}})} (t - \zeta) = \prod_{0<d|n} \Phi_d(t).$$

Also, $\phi(n) = \sum \phi(d)$ with d running through all positive divisors of n.

Combining all preceeding observations and applying Gauss's lemma, we obtain the following theorems.

Theorem 9.3.9. For each positive integer n, $\Phi_n(t)$ is an irreducible polynomial over $\mathbb{Z}$ of degree $\phi(n)$.

Proof. It suffices to prove that $\Phi_n(t) \in \mathbb{Z}[t]$ for all $n \in \mathbb{N}$. Assume that $\Phi_n(t)$ is a polynomial over $\mathbb{Z}$ for all positive integers $n < N$. Note that $t^N - 1 = \Phi_N(t) \times \prod_{0<d|N, d\neq N} \Phi_d(t)$ and $\Phi_N(t) \in \mathbb{Q}[t]$. By Gauss's lemma (see Problem 3.2.1) we have $\Phi_N(t) \in \mathbb{Z}[t]$, for $t^N - 1$ and $\prod_{0<d|N, d\neq N} \Phi_d(t)$ are primitive polynomials over $\mathbb{Z}$. □

Theorem 9.3.10. The n-th cylcotomic field $\mathbb{Q}(\zeta_n)$ is, in fact, the splitting field for $\Phi_n(t)$ over $\mathbb{Q}$. The extension $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is a finite Galois extension of extension degree $\phi(n)$, and its Galois group is isomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. It suffices to prove that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \approx (\mathbb{Z}/n\mathbb{Z})^\times$. In fact, any automorphism $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is determined by its action on ζ_n, and the only possible return for ζ_n is ζ_n^k with $1 \leq k \leq n$ with $(n, k) = 1$. Thus, defining the map $\rho : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \to (\mathbb{Z}/n\mathbb{Z})^\times$ by $\rho(\sigma) = \overline{k}$, it easily turns out that ρ is a group isomorphism. □

When studying Galois's theorem, we have observed how we could treat the Galois group of a composition field. Using such method, we can establish an isomorphism type of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ where ζ_n is a primitive n-th root of unity.

Observation 9.3.11. In this example, assume $F = \mathbb{Q}$ and let ζ_k denote a primitive k-th root of unity. Assume further that m, n are relatively prime positive integers.

(a) $\zeta_m\zeta_n$ is a primitive mn-th root of unity. Hence, $\mathbb{Q}(\zeta_m) \cdot \mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_{mn})$.

(b) $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$.

(c) If d is a positive divisor of n, then ζ_n^d is a primitive (n/d)-th root of unity.

Proof. To prove (a), note from $(m, n) = 1$ that $(\zeta_m\zeta_n)^m = \zeta_n^m$ is a primitive n-th root of unity and that there are integers a, b such that $na + mb = 1$. The former observation implies $\mathbb{Q}(\zeta_m\zeta_n)$ contains ζ_n (and ζ_m for a similar reason), and the latter observation implies $\zeta_m^a\zeta_n^b = \zeta_{mn}$. Therefore, $\mathbb{Q}(\zeta_m\zeta_n)$ contains $\zeta_{mn} = \zeta_m^a\zeta_n^b$, so $\zeta_m\zeta_n$ is a primitive mn-root of unity.

To prove (b), note from (a) that

$$[\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}] = \frac{[\mathbb{Q}(\zeta_m) : \mathbb{Q}][\mathbb{Q}(\zeta_n) : \mathbb{Q}]}{[\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) : \mathbb{Q}]}.$$

Since $[\mathbb{Q}(\zeta_{mn}) : \mathbb{Q}] = \phi(mn) = \phi(m)\phi(n) = [\mathbb{Q}(\zeta_m) : \mathbb{Q}][\mathbb{Q}(\zeta_n) : \mathbb{Q}]$, we have $\mathbb{Q}(\zeta_m) \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$.

Checking (c) is easy. □

Proposition 9.3.12 (Chinese remainder theorem for cyclotomic fields)**.** Let $n = {p_1}^{a_1} \cdots {p_k}^{a_k}$ be the factorization of a positive integer to prime numbers. (Assume that $p_1, \cdots, p_k$ are pairwise distinct positive prime numbers and $a_1, \cdots, a_k$ are positive integers.)

(a) If s, t are relatively prime positive divisors of n, then $\mathbb{Q}(\zeta_s) \cdot \mathbb{Q}(\zeta_t) = \mathbb{Q}(\zeta_{st})$ and $\mathbb{Q}(\zeta_s) \cap \mathbb{Q}(\zeta_t) = \mathbb{Q}$.

(b) $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \approx \mathrm{Gal}(\mathbb{Q}(\zeta_{{p_1}^{a_1}})/\mathbb{Q}) \times \cdots \times \mathrm{Gal}(\mathbb{Q}(\zeta_{{p_k}^{a_k}})/\mathbb{Q})$.

Proof. (a) follows directly from the preceeding example; it remains to prove (b). Let $s = {p_1}^{a_1}$ and $t = n/s$. Because $\mathbb{Q}(\zeta_n)$ is the composition of $\mathbb{Q}(\zeta_s)$ and $\mathbb{Q}(\zeta_t)$, there is a group monomorphism $\rho : \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \hookrightarrow \mathrm{Gal}(\mathbb{Q}(\zeta_{{p_1}^{a_1}})/\mathbb{Q}) \times \mathrm{Gal}(\mathbb{Q}(\zeta_t)/\mathbb{Q})$; because $\mathbb{Q}(\zeta_s) \cap \mathbb{Q}(\zeta_t) = \mathbb{Q}$, ρ is a group isomorphism. Proceeding the proof inductively, we can obtain a desired isomorphism. □

Observation 9.3.13 (Subfield lattice of $\mathbb{Q}(\zeta_p)$). Let p be a prime number. We will show that every intermediate subfield of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ has a primitive element over $\mathbb{Q}$ and deliver a formula to find a primitive elemtent.

By Galois's theorem, an intermediate subfield E of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ and a subgroup H of $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ correspond bijectively. Because p is a prime number, $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \phi(p) = p-1$, so $\{\zeta_p, \zeta_p^2, \cdots, \zeta_p^{p-1}\}$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\zeta_p)$. Hence, the element

$$\alpha := \sum_{\sigma \in H} \sigma\alpha$$

is a (finite) sum of basis members. Thus, if $\tau \in \mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ and $\tau\alpha = \alpha$, then $\tau\zeta_p = \sigma\zeta_p$ for some $\sigma \in H$, hence $\tau = \sigma \in H$. This implies that $\mathbb{Q}(\alpha) \geq \mathbb{Q}(\zeta_p)^H$. Conversely, since $\mathbb{Q}(\alpha)$ is fixed by every automorphism in H, we have $\mathbb{Q}(\alpha) \leq \mathbb{Q}(\zeta_p)^H$. Therefore, $\mathbb{Q}(\zeta_p)^H = \mathbb{Q}(\alpha)$.

In particular, suppose that $E/\mathbb{Q}$ is an intermediate subfield of $\mathbb{Q}(\zeta_p)\mathbb{Q}$ of degree 2 over $\mathbb{Q}$, where p is an odd prime. (Such field E exists uniquely, because there is a unique subgroup $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q}) \approx Z_{p-1}$ of index 2.) Then

$$E = \begin{cases} \mathbb{Q}(\sqrt{p}) & (\text{if } p \equiv 1 \text{ mod } 4) \\ \mathbb{Q}(\sqrt{-p}) & (\text{if } p \equiv 3 \text{ mod } 4) \end{cases} \tag{9.1}$$

The proof of the above equation is given in Appendix A.2.

Example 9.3.14. We will justify that $\sqrt[3]{2}$ is not contained in any cyclotomic field of $\mathbb{Q}$. If $\sqrt[3]{2} \in \mathbb{Q}(\zeta_n)$ for some $n \in \mathbb{N}$, then the normal closure of $\mathbb{Q}(\sqrt[3]{2})$ over $\mathbb{Q}$ is contained in $\mathbb{Q}(\zeta_n)$. Though, the Galois closure of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is nonabelian, a contradiction.

9.4 Applications of cyclotomic extensions

9.4.1 Cyclotomic extensions and abelian extensions

In this section, we study a matching between finite abelian groups and finite abelian extensions. To be precise,

(I) Given a finite abelian group G, there is a cyclotomic extension E of $\mathbb{Q}$ such that $\mathrm{Gal}(E/\mathbb{Q}) \approx G$.

(II) (Kronecker-Weber's theorem) Every finite abelian extension E over $\mathbb{Q}$ is a cyclotomic extension of $\mathbb{Q}$.

In this note, the proof of Kronecker-Weber's theorem will not be introduced, but only the proof of (I) will be introduced.

Sketch. Write $G \approx Z_{m_1} \times \cdots Z_{m_k}$, where $m_1 | \cdots | m_k$. We wish to find a positive integer n such that $\mathbb{Q} \leq E \leq \mathbb{Q}(\zeta_n)$ such $\mathrm{Gal}(E/\mathbb{Q}) \approx G$. (Note that $E/\mathbb{Q}$ is a Galois extension when such n exists, for $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ is an abelian extension.) If $n = {p_1}^{a_1} \cdots {p_k}^{a_k}$ is the factorization of n into pairwise distinct positive prime numbers, then

$$\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \approx (\mathbb{Z}/{p_1}^{a_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/{p_k}^{a_k}\mathbb{Z})^\times.$$

If one assumes $a_i = 1$ for all $1 \leq i \leq k$ for easy computation, we have $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}) \approx Z_{p_1-1} \times \cdots \times Z_{p_k-1}$. Since $\mathrm{Gal}(E/\mathbb{Q}) \approx \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})/\mathrm{Gal}(\mathbb{Q}(\zeta_n)/E)$, if, for each $1 \leq i \leq k$, one can find a prime number p_i such that $m_i | (p_i - 1)$, then the proof proceeds as follows. For each $1 \leq i \leq k$, let $h_i = (q_i - 1)/m_i$ and find a subgroup H_i of Z_{p_i-1} of order h_i. Then there is a subgroup A of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ such that $A \approx H_1 \times \cdots \times H_k$. If E is the fixed field of A in $\mathbb{Q}(\zeta_n)$, then

$$\mathrm{Gal}(E/\mathbb{Q}) \approx \frac{\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})}{\mathrm{Gal}(\mathbb{Q}(\zeta_n)/E)} \approx \frac{Z_{p_1-1} \times \cdots \times Z_{p_k-1}}{H_1 \times \cdots \times H_k} \approx \prod_{i=1}^{k} \frac{Z_{p_i-1}}{H_i} \approx \prod_{i=1}^{k} Z_{m_i} \approx G.$$

To complete the proof of (I), the following lemma should be proved, whose proof is given in Appendix A.1:

Lemma 9.4.1. Given a positive integer m, there are infinitely many prime numbers modulo m.

9.4.2 Constructibility

We first find the condition of n for which a regular n-gon can be constructed.

Theorem 9.4.2 (Constructibility of a regular n-gon)**.** Suppose that n is an integer greater than or equal to 3. Then a regular n-gon (with the length of a side 1) is constructible if and only if $n = 2^k p_1 \cdots p_l$, where $k, l \geq 0$ and $p_1, \cdots, p_l$ are pairwise distinct Fermat primes.[1]

Proof. Remark that the constructibility of a regular n-gon coincides the constructibility of

$$\gamma := \cos\left(\frac{2\pi}{n}\right) = \frac{\zeta_n + \zeta_n^{-1}}{2},$$

where $\zeta_n = \exp(2\pi i/n)$. Since $t^2 - 2\gamma t + 1$ is satisfied by $\zeta_n \in \mathbb{C} \setminus \mathbb{R}$, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\gamma)] = 2$.

Assume first that a regular n-gon is constructible, i.e., γ is constructible. Then $[\mathbb{Q}(\gamma) : \mathbb{Q}]$ is a power of 2, so $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$ is also a power of 2. This forces n is the product of a power of 2 and pairwise distinct Fermat primes.

Assuming conversely, we find that $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is a 2-group. Therefore, (writing $|\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})| = 2^m$) there is a subgroup H_r of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ of order 2^r for each integer $0 \leq r \leq m$ such that

$$\{\mathit{id}_{\mathbb{Q}(\zeta_n)}\} = H_0 < H_1 < \cdots < H_{m-1} < H_m = \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q}).$$

By Galois's theorem, we have

$$\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_n)^{H_0} > \mathbb{Q}(\zeta_n)^{H_1} > \cdots > \mathbb{Q}(\zeta_n)^{H_{m-1}} > \mathbb{Q}(\zeta_n)^{H_m} = \mathbb{Q},$$

hence $\gamma \in \mathbb{Q}(\zeta_n)$ is constructible, as desired. □

We end this section with another constructibility criterion. In Theorem 5.5.1, we proved that a real number α is constructible if and only if there is a tower of quadratic extensions from $\mathbb{Q}$ whose head field contains α. In the following theorem in which we consider the normal(Galois) closure of $\mathbb{Q}(\alpha)$, we do not have to consider its subfields but only have to know the extension degree of the Galois closure.

Theorem 9.4.3 (Constructibility criterion II)**.** Let α be a real algebraic number and K be the normal(Galois) closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. Then α is constructible if and only if $[K : \mathbb{Q}]$ is a power of 2.

Proof. Assume first that α is constructible and let $\alpha_1, \cdots, \alpha_n$ be all algebraic conjugates of α (and let $\alpha_1 = \alpha$). Because

$$\mathbb{Q} \leq \mathbb{Q}(\alpha_1) \leq \cdots \leq \mathbb{Q}(\alpha_1, \cdots, \alpha_n) = K$$

and α_i is constructible for $1 \leq i \leq n$, each subextension degree is a power of 2, as desired.

Assume conversely that $[K : \mathbb{Q}] = 2^r$ for some nonnegative integer r. For each integer $0 \leq i \leq r$, there is a subgroup H_r of $\mathrm{Gal}(K/\mathbb{Q})$ of index 2^i. Then

$$\mathbb{Q} = K^{H_0} < K^{H_1} < \cdots < K^{H_r} = K$$

is a desired tower of quadratic extensions from $\mathbb{Q}$. □

[1] A prime number of the form $2^a + 1$ for some positive integer a is called a Fermat prime.

Chapter 10

Solving polynomial equations

10.1 Symmetric polynomials and discriminants

Remark. When F is a field such that char$(F) \neq 2$, the roots of the quadratic equation $x^2 + ax + b = 0\,(a, b \in F)$ are given by

$$x = \frac{-a \pm \sqrt{a^2 - 4b}}{2}.$$

We will consider above formula as a function in the coefficients of the polynomial $t^2 + at + b$, i.e., a function of the coefficients of the polynomial.

Observation 10.1.1. Let F be a field and $s_1, \cdots, s_n$ be pairwise distinct indeterminates with $n \in \mathbb{Z}^{>0}$. Then the polynomial

$$G(t) := t^n - s_1 t^{n-1} + \cdots + (-1)^n s_n \in F(s_1, \cdots, s_n)[t]$$

is called the general polynomial of degree n. (Here, the field $F(s_1, \cdots, s_n)$ is transcendental over F.) Writing $E = F(s_1, \cdots, s_n)$ (and fixing an algebraic closure $\overline{E}$ of E) and

$$G(t) = (t - x_1) \cdots (t - x_n) \quad (x_1, \cdots, x_n \in \overline{E}),$$

we can find the formula for s_i in $x_1, \cdots, x_n$ for each integer $i = 1, \cdots, n$. The indeterminates $s_1, \cdots, s_n$ are called the elementary symmetric polynomials in $x_1, \cdots, x_n$. (The extension $E(x_1, \cdots, x_n)/E$ is a finite Galois extension.)

For a clear argument, we start from $x_1, \cdots, x_n$, rather than from the elementary symmetric polynomials in $x_1, \cdots, x_n$.

Definition 10.1.2 (General polynomial). Let F be a field and $x_1, \cdots, x_n$ be pairwise distinct indeterminates ($n \in \mathbb{Z}^{>0}$). Define

$$s_1 = \sum_{1 \leq i \leq n} x_i, \quad s_2 = \sum_{1 \leq i < j \leq n} x_i x_j, \quad \cdots, \quad s_n = x_1 \cdots x_n.$$

Then s_i is called the i-th elementary symmetric polynomial in $x_1, \cdots, x_n$ for each integer $1 \leq i \leq n$. Under the above definition, letting $E = F(s_1, \cdots, s_n)$ (which is transcendental over F), the polynomial

$$G(t) := (t - x_1) \cdots (t - x_n) = t^n - s_1 t^{n-1} + \cdots + (-1)^n s_n \in E[t]$$

is a separable polynomial over E and is called the general polynomial over F of degree n. Hence, the splitting field for $G(t)$ over E is clearly $E(x_1, \cdots, x_n)$, which is a finite Galois extension over F.

Our first goal is to find the Galois group of $G(t)$ over E, which clearly embeds into S_n. Note that S_n acts on $\{x_1, \cdots, x_n\}$ by permutation, i.e., given $\sigma \in S_n$, $\sigma(x_i) = x_{\sigma(i)}$ for all i. This action naturally extends to the group action of S_n by left multiplication on $F[x_1, \cdots, x_n]$ and $F(x_1, \cdots, x_n)$. Hence, the latter group action affords a group embedding $S_n \hookrightarrow \mathrm{Aut}(K)$, where $K = E(x_1, \cdots, x_n)$. (How can S_K be reduced to $\mathrm{Aut}(K)$?) Because the action fixes the elements of E, the above group embedding reduces to $S_n \hookrightarrow \mathrm{Aut}(K/E) = \mathrm{Gal}(K/E)$. Therefore, the Galois group of $G(t)$ over E is, up to isomorphism, S_n.

We summarize the above observation as the following theorem:

Theorem 10.1.3. Let F be a field and $x_1, \cdots, x_n$ be pairwise distinct indeterminates for $n \geq 1$, and let $E = F(s_1, \cdots, s_n)$ and $K = E(x_1, \cdots, x_n)$. Then K is the splitting field for $G(t)$ over E and K/E is a finite Galois extension with the Galois group S_n, up to isomorphism. (Hence, we may identify $\mathrm{Gal}(K/E) = S_n$.)

Remark. (a) Because $G(t)$ is separable and $\mathrm{Gal}(K/E)$ acts on the roots of $G(t)$ transitively, $G(t)$ is an irreducible polynomial over E.

(b) By Galois's theorem, $F(x_1, \cdots, x_n)^{S_n} = F(s_1, \cdots, s_n)$. In fact, $F[x_1, \cdots, x_n]^{S_n} = F[s_1, \cdots, s_n]$. To justify the latter identity (which cannot be direcly deduced from Galois's theorem), it suffices to prove $F[x_1, \cdots, x_n]^{S_n} \subset F[s_1, \cdots, s_n]$: If $u \in F[x_1, \cdots, x_n]^{S_n}$, then $u \in F(s_1, \cdots, s_n) \cap F[x_1, \cdots, x_n]$, so $u \in F[s_1, \cdots, s_n]$.

(c) For any positive integer $n > 1$, A_n is defined set-theoretically to be the collection of all even permutations in S_n. Thus, there is a unique subgroup of $\mathrm{Gal}(K/E)$ of index 2, so there is no confusion to identify such a subgroup with A_n.

Our next goal is to find $F(x_1, \cdots, x_n)^{A_n}$. Define E and K as we have defined in this section. By Artin's theorem (or by Galois's theorem), we have $\mathrm{Gal}(K/K^{A_n}) = A_n$, thus $[K^{A_n} : E] = 2$, i.e., K^{A_n} is a quadratic extension over E.

Definition 10.1.4 (Discriminant). Let $\alpha_1, \cdots, \alpha_n$ be the roots of $f(t) \in F[t]$ (where $n = \mathit{deg}\, f(t) \geq 2$). Define

$$\delta = \delta_f = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j), \quad \Delta = \Delta_f = \delta^2.$$

Both δ and Δ are called the discriminant of $f(t)$.[1]

Observation 10.1.5 (Computation of discriminants). Remark a formula for the determinant of a Vandermonde matrix:

$$\mathit{det} \begin{pmatrix} 1 & x_1 & \cdots & x_1^{n-1} \\ 1 & x_2 & \cdots & x_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & x_n & \cdots & x_n^{n-1} \end{pmatrix} = \prod_{1 \leq i < j \leq n} (x_j - x_i).$$

Hence, letting $V = (x_i^{j-1})_{\substack{1 \leq i \leq n, \\ q \leq j \leq n}}$, $\Delta_G = \mathit{det}(V^T V)$. Here, $V^T V = (z_{i+j-2})_{i,j}$, where $z_k = z_1^k + \cdots + z_n^k$ for $k \geq 0$.

By computing the determinant for $n = 3$, we have

$$\Delta_G = -4s_2^3 - 27s_3^2 - 4s_1^3 s_3 + s_1^2 s_2^2 + 18 s_1 s_2 s_3.$$

In fact, the above result reduces to a simpler formula when one reduces the t^{n-1}-term of $G(t)$ by shifting $G(t)$; if one obtains $b(t) = t^3 + pt + q$ by shifting $G(t)$, then

$$\Delta_G = \Delta_b = -4p^3 - 27q^3.$$

We postpone to compute the discriminant of the general polynomial of degree 4 later in this note.

Remarking that δ is a square root of δ which is defined up to sign, we investigate when δ is fixed by a permutaion of the roots.

Proposition 10.1.6. Throughout this proposition, $G(t)$ stands for the general polynomial in $F(s_1, \cdots, s_n)$ for $n \geq 2$. Let $f(t)$ be a separable polynomial over F of degree d and identify $G_f \leq S_d$.

(a) $\Delta_f \in F$. In particular, $\Delta_G \in F(s_1, \cdots, s_n)$.

[1] Note that δ is defined up to sign. In this note, we mean Δ when speaking of a discriminant.

(b) $\sigma\delta_f = \delta_f$ whenever $\sigma \in G_f$ is even and $\sigma\delta_f = -\delta_f$ whenever $\sigma \in G_f$ is odd. Hence, if K is the splitting field for $f(t)$ over F and $\text{char}(F) \neq 2$, then $K^{G_f \cap A_d} = F(\delta_f)$. In particular, if $\text{char}(F) \neq 2$, then $F(x_1, \cdots, x_n)^{A_n} = F(s_1, \cdots, s_n)(\delta_G)$.

Proof. In proving (a), the splitting field K for $f(t)$ over F is a finite Galois extension over F. Because Δ_f is fixed by every automorphism in $\text{Gal}(K/E)$, by Galois's theorem, $\Delta_f \in K^{\text{Gal}(K/F)} = F$.

The first part of (b) easily follows from the definition of δ_f, so $\delta_f \in K^{G_f \cap A_d}$. Since $f(t)$ is assumed to be separable, when $\text{char}(F) \neq 2$, we have $\delta_f \neq -\delta_f$. Thus, if $\sigma \in G_f \cap A_d$ fixes δ_f, then σ is necessarily even, so $\text{Gal}(K/F(\delta_f)) \leq G_f \cap A_d$, i.e., $F(\delta_f) \geq K^{G_f \cap A_d}$. □

Corollary 10.1.7. Suppose that F is a field such that $\text{char}(F) \neq 2$ and $f(t)$ is a separable polynomial over F (where $n = \mathit{deg}\, f(t) \geq 2$). Let K be the splitting field for $f(t)$ over F and identify $G_f \leq S_n$. Then $G_f \leq A_n$ if and only if $\delta_f \in F$.

Proof. $G_f \cap A_n = G_f$ if and only if $F(\delta_f) = K^{G_f \cap A_n} = K^{G_f} = F$. □

This concludes our study on general polynomials and their discriminants (for fields with characteristic not being 2). We end this section with categorizing the Galois group of a cubic polynomial over a field with the characteristic not being 2.

Observation 10.1.8. Let F be a field such that $\text{char}(F) \neq 2$ and $f(t) = t^3 + pt^2 + qt + r$ be a separable polynomial over F. (Separability is always ensured when the base field is perfect, and we generally consider perfect fields.) After shifting $f(t)$, redefine $f(t) = t^3 + at + b$. (The roots of the former and the latter $f(t)$ differ by $p/3$, respectively.)

(a) Suppose that $f(t)$ is reducible.

  (i) If $f(t)$ splits completely over F, then all root of $f(t)$ are in F, so $G_f = \{id_F\}$.

  (ii) If $f(t)$ does not split completely over F, then $f(t)$ is a product of a linear factor over F and an irreducible quadratic factor over F. Hence, $G_f \approx Z_2$.

(b) Suppose that $f(t)$ is irreducible. Then $\mathit{deg}\, f(t)$ divides the order of the Galois group of $f(t)$. (And since $f(t)$ is assumed to be separable, G_f is transitive on the roots of $f(t)$.) Remark that the discriminant Δ of $f(t)$ is given by $\Delta = -4a^3 - 27b^2$.

  (iii) $\delta \in F$ if and only if $G_f \leq A_3$. In this case, $G_f \approx A_3$.

  (iv) $\delta \notin F$ if and only if $G_f \not\leq A_3$. In this case, $G_f \approx S_3$.

Example 10.1.9. In this example, we compute the Galois group of the polynomial

$$f(t) = t^3 + t + 1 \in F[t]$$

with the base field F varies among $\mathbb{Q}$, $\mathbb{Q}(\sqrt{-31})$, $\mathbb{F}_3$, and $\mathbb{F}_7$. Note that $\Delta = \Delta_f = -31$.

(a) Because $f(t)$ is irreducible over $\mathbb{Q}$ and $\delta = \delta_f = \sqrt{-31} \notin \mathbb{Q}$, $G_{f,\mathbb{Q}} \approx S_3$.

(b) One can verify that $f(t)$ is irreducible over $\mathbb{Q}(\sqrt{-31})$ by checking if $f(t)$ is irreducible over $\mathbb{Z}[\sqrt{-31}]$, whose field of fractions is $\mathbb{Q}(\sqrt{-31})$. Since $\delta = \sqrt{-31} \in \mathbb{Q}(\sqrt{-31})$, we have $G_{f,\mathbb{Q}(\sqrt{-31})} \approx A_3$.

(c) Since $f(t) = (t-1)(t^2 + t + 2)$ and $t^2 + t + 2 \in \mathbb{F}_3[t]$ is irreducible, $G_{f,\mathbb{F}_3} \approx Z_2$.

(d) Since $f(t)$ is irreducible over $\mathbb{F}_7$ and $\Delta = -31 = 4$ is a square in $\mathbb{F}_7$, $G_{f,\mathbb{F}_7} \approx A_3$.

10.2 Cyclic extensions

Starting from this section, we study the splitting field for $t^n - a \in F[t]$ over F under some conditions, due to some technical problems.

Observation 10.2.1. Let F be a field. Then $t^n - a \in F[t]$ is separable whenever $a \neq 0$ and char(F) does not divide n.

Note that we are mainly interested in (finite) Galois extensions and the condition that char(F) does not divide n (together with $a \in F \setminus \{0\}$) is the separability condition. Hence, we are interested in the splitting field for $t^n - a \in F[t]$ over F under the following assumption:

Assumption: F is a field and char(F) does not divide n.

In particular, when char$(F) = 0$, then $t^n - a$ is separable whenever $n \in \mathbb{N}$ and $a \neq 0$.

Proposition 10.2.2. Let F be a field and n be a positive integer which is not divisible by char(F), and assume that F contains an n-th root of unity. If $a \in F$ and α is a root of $t^n - a \in F[t]$, then

(a) $F(\alpha)$ is the splitting field for $t^n - a$ over F.

(b) $F(\alpha)/F$ is a cyclic extension and $\mathrm{Gal}(F(\alpha)/F)$ embeds into Z_n.

Proof. The proof of (b) would be sufficient. Without loss of generality, we may assume $a \neq 0$, for $a = 0$ forces $F(\alpha) = F$. Since $t^n - a$ is a separable polynomial over F, $F(\alpha)/F$ is a finite Galois extension, and an automorphism $\sigma \in \mathrm{Gal}(F(\alpha)/F)$ maps α to $\alpha\zeta^k$, where ζ is a primitive n-th root of unity and k is an integer. This induces the map $\rho : \mathrm{Gal}(F(\alpha)/F) \to \mathbb{Z}/n\mathbb{Z}$ defined by $\rho\sigma = \overline{k}$, which is a group monomorphism. □

Corollary 10.2.3. Let F be a field and n be a positive integer which is not divisible by char(F). If $a \in F$ and $f(t) = t^n - a \in F[t]$, then G_f is a solvable group.

Proof. The roots of $f(t)$ are $\alpha, \alpha\zeta, \cdots, \alpha\zeta^{n-1}$, where α is a root of $f(t)$ and ζ is a primitive n-th root of unity. (Remark that the separability of $f(t)$ is ensured by the assumption on char(F) and n.) Consider the tower $F \leq F(\zeta) \leq F(\alpha, \zeta)$, and observe that bith $F(\zeta)/F$ and $F(\alpha,\zeta)/F(\zeta)$ are (finite) abelian extensions. It now follows that G_f is a solvable group. □

We now prove the following converse of (b) in Proposition 10.2.2.

Proposition 10.2.4. Suppose that n is a positive integer and F is a field whose characteristic does not divide n. Assume that F contains a primitive n-th root of unity. If K/F is a finite cyclic extension of degree n, then there is an element $\alpha \in K$ such that $\alpha^n \in F$ and $K = F(\alpha)$ (in short, $K = F(\sqrt[n]{a})$ for some $a \in F$).

Proof. See Observation 11.2.2. □

Remark. We summarize the preceeding equivalence as follows:

> Suppose that n is a positive integer and F is a field whose characteristic doen not divide n, and assume further that F contains a primitive n-th root of unity.
>
> (a) Let α be a root of $t^n - a \in F[t]$. Then $F(\alpha)$ is the splitting field for $t^n - a$ over F, and $F(\alpha)/F$ is a cyclic extension of degree dividing n.
>
> (b) Conversely, if K/F is a cyclic extension of degree n, then there is an element $\alpha \in K$ such that $K = F(\alpha)$ and $\alpha^n \in F$. (Hence, K/F is a radical extension.)

10.3 Radical extensions

We introduce another type of finite field extension, called the radical extension, and we define the solvability of a nonconstant polynomial over a field in terms of a radical extension.

Definition 10.3.1. Let F be a field

(a) (Radical extension) Let E/F be a finite field extension with a 'radical tower' given as follows:

$$F \leq (\alpha_1) \leq F(\alpha_1, \alpha_2) \leq \cdots \leq F(\alpha_1, \cdots, \alpha_k) = E,$$

where ${\alpha_1}^{n_1} \in F$ and ${\alpha_i}^{n_i} \in F(\alpha_1, \cdots, \alpha_{i-1})\,(2 \leq i \leq k)$ for some positive integers $n_1, \cdots, n_k$. Then E/F is called an $\{n_i\}$-radical extension, or just a radical extension, in short.

(b) (Solvability of a nonconstant polynomial) Let $f(t)$ be a nonconstant polynomial over F and let K be the splitting field for $f(t)$ over F. If there is a radical extension E/F such that $F \leq K \leq E$, then $f(t)$ is said to be solvable by radicals.

Remark. Indeed, given a nonconstant polynomial $f(t)$ over a field F, all roots of $f(t)$ can be written in terms of elementary operations and radicals if and only if the splitting field for $f(t)$ over F is contained in a radical extension over F (i.e., $f(t)$ is solvable by radicals).

Observation 10.3.2. Let E/F be an $\{n_i\}$-radical extension, and let K be the normal closure of E over F. (Here, K/F need not be a Galois extension.) Then K/F is also an $\{n_i\}$-radical extension.

Proof. Write a radical tower of E/F as

$$F \leq F(\alpha_1) \leq \cdots \leq F(\alpha_1, \cdots, \alpha_n) = E.$$

Remark that K is the composition of σE, where σ runs through $\mathrm{Emb}(E/F)$. For simplicity, write $\mathcal{A} = \{\alpha_1, \cdots, \alpha_n\}$ and $\mathrm{Emb}(E/F) = \{id_E = \sigma_1, \cdots, \sigma_s\}$. Then $K = F(\sigma_1\mathcal{A}, \cdots, \sigma_s\mathcal{A})$, so by adjoining $\sigma_i\alpha_j$ for each i and j one by one, one can establish a radical tower for K/F. □

Assumption: By the end of this chapter, for simplicity, we assume that all fields are of characteristic 0.

Our goal in this section is to prove the following equivalence:

Theorem 10.3.3 (Solvability of a polynomial)**.** Let F be a field (of characteristic 0) and $f(t)$ be a nonconstant polynomial over F. Then $f(t)$ is solvable by radicals if and only if G_f is a solvable group.

Proof of 'if' part. Assume that G_f is a solvable group and let K be the splitting field for $f(t)$ over F. To construct a tower for a field extension with each adjacent extension being cyclic, we make use of a property of finite solvable groups. Let $H_1, \cdots, H_k$ be subgroups of G_f such that

$$G_f = H_0 \rhd H_1 \rhd \cdots \rhd H_{k-1} \rhd H_k = \{id_K\},$$

where H_{i-1}/H_i is a cyclic group of a prime order p_i for $i = 1, \cdots, k$. By Galois's theorem, we have a tower

$$F = K_0 < K_1 < \cdots < K_{k-1} < K_k = K,$$

where K_i/K_{i-1} is a cyclic extension of degree p_i for $i = 1, \cdots, k$. To let each adjacent extension be radical, we adjoin an appropriate primitive root of unity. Write $n = |G_f|$ and let ζ be a primitive n-th root of unity and consider the following tower:

$$F \leq F(\zeta) = K_0(\zeta) < \cdots < K_{k-1}(\zeta) < K_k(\zeta) = K(\zeta).$$

Because $\mathrm{Gal}(K_i(\zeta)/K_{i-1}(\zeta)) \approx \mathrm{Gal}(K_i/(K_i \cap K_{i-1}(\zeta))) \hookrightarrow \mathrm{Gal}(K_i/K_{i-1})$ and each base field contains an appropriate primitive root of unity, $K_i(\zeta)/K_{i-1}(\zeta)$ is a radical extension ($i = 1, \cdots, k$). Because $F(\zeta)/F$ is also radical, $K(\zeta)/F$ is a radical extension. Therefore, $f(t)$ is solvable by radicals. □

Proof of 'only if' part. Assume that $f(t)$ is sovable by radicals. Let E be the splitting field for $f(t)$ over F, L be an $\{n_i\}$-radical extension over F containing E, and K be the normal closure of L over F. Then K/F is a finite Galois extension which is $\{n_i\}$-radical. Hence, there are elements $\alpha_1, \cdots, \alpha_k \in K$ such that

$$F \leq F(\alpha_1) \leq \cdots \leq F(\alpha_1, \cdots, \alpha_k) = K$$

where ${\alpha_1}^{n_1} \in F$ and ${\alpha_i}^{n_i} \in F(\alpha_1, \cdots, \alpha_{i-1})\,(2 \leq i \leq k)$.

To let each adjacent extension be cyclic, we adjoin an appropriate primitive root of unity. Let $n = \text{lcm}\{n_1, \cdots, n_k\}$ and ζ be a primitive n-th root of unity. Adjoining ζ, we have

$$F \leq F(\zeta) \leq F(\zeta)(\alpha_1) \leq \cdots \leq F(\zeta)(\alpha_1, \cdots, \alpha_k) = K(\zeta).$$

(i) Note that K/F is a finite Galois extension, so K is the splitting field for some nonconstant polynomial $h(t)$ over F. Then, $K(\zeta)$ is the splitting field for $(t^n - 1)h(t)$ over F, so $K(\zeta)/F$ is also a finite Galois extension.

(ii) Observe that $F(\zeta)/F$ is an abelian extension with the Galois group isomorphic to a subgroup of Z_n and the other adjacent extensions are cyclic extensions.

Hence, the Galois extension $K(\zeta)/F$ is a solvable extension. Because K/F is a Galois extension, K/F is also a solvable extension. □

Corollary 10.3.4. General polynomials of degree at least 5 are insolvable.

Proof. S_n is insolvable if and only if $n \geq 5$. □

Proposition 10.3.5. Let p be a prime number and $f(t) \in \mathbb{Q}[t]$ be an irreducible polynomial of degree p. If $f(t)$ has only two nonreal complex roots, then $G_f \approx S_p$.

Proof. Since $f(t)$ is irreducible, p divides the order of G_f and G_f contains an element of order p. Identifying $G_f \leq S_p$, such an element is a p-cycle. On the other hand, because there are only two nonreal complex roots, G_f contains a transposition. Therefore, $G_f = S_p$, for G_f contains a p-cycle and a transposition. □

Example 10.3.6. The Galois group of $t^5 - 9t + 3 \in \mathbb{Q}[t]$ is S_5.

10.4 Cubic and quartic polynomials

Chapter 11

Further Galois theory

11.1 Character theory

Definition 11.1.1. Let G be a group and L be a field. A linear character χ of G with values in L is a group homomorphism from G into the multiplicative group $L^\times$. We say a collection of characters $\{\chi_1, \cdots, \chi_r\}$ of G with values in L is L-linearly indepenedent whenever there is no nontrivial relation

$$a_1\chi_1 + \cdots + a_r\chi_r = 0 \quad (a_1, \cdots, a_r \in L).$$

Proposition 11.1.2. Let $\{\chi_1, \cdots, \chi_d\}$ be a collection of pairwise distinct characters of a group G with values in a field L. Then $\{\chi_1, \cdots, \chi_d\}$ is L-linearly indepenedent.

Proof. Assume that $\{\chi_1, \cdots, \chi_d\}$ is L-linearly depenedent, and among all linear dependence relataions, we choose one with the minimal number m of nonzero coefficients a_i. (By renumbering, we may write $a_1\chi_1 + \cdots + a_m\chi_m = 0$ with $a_1, \cdots, a_m \in L^\times$.) Let g_0 be an element of G such that $\chi_1(g_0) \neq \chi_d(g_0)$. From

$$\begin{cases} a_1\chi_1(g) + \cdots + a_{d-1}\chi_{d-1}(g) + a_d\chi_d(g) = 0 \\ a_1\chi_1(g_0g) + \cdots + a_{d-1}\chi_{d-1}(g_0g) + a_d\chi_d(g_0g) = 0 \end{cases}$$

we have

$$\sum_{i=1}^{d-1} a_i(\chi_d(g_0) - \chi_i(g_0))\chi_i(g) = 0.$$

Since the first term is nonzero, we obtained another linear dependence with fewer nonzero coefficients. This contradicts the minimality of m, hence $\{\chi_1, \cdots, \chi_d\}$ is L-linearly indepenedent. □

11.2 Lagrange resolvent

In this section, we assume the followings:

(i) F is a field containing a primitive n-th root of unity, where n is not divisible by char(F).

(ii) K/F is a cyclic extension of degree n.

And let σ be a generator of $\mathrm{Gal}(K/F)$.

Definition 11.2.1 (Lagrange resolvent)**.** For $\alpha \in K$ and any n-th root of unity ζ, define the Lagrange resolvent $\mathcal{L}_\sigma(\alpha, \zeta) \in K$ by

$$\mathcal{L}_\sigma(\alpha, \zeta) = \alpha + \zeta\sigma(\alpha) + \zeta^2\sigma^2(\alpha) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha).$$

Observation 11.2.2. Let ζ be any n-th root of unity.

(a) By Proposition 11.1.2, $\{id_K, \sigma, \cdots, \sigma^{n-1}\}$ is K-linearly independent. Hence, in particular, there is an element $\alpha \in K$ such that $\mathcal{L}_\sigma(\alpha, \zeta) \neq 0$.

(b) One can easily find that $\sigma^k \mathcal{L} = \zeta^{-k}\mathcal{L}$ for all integer k. Thus, when ζ is a primitive n-th root of unity and α is given as in (a), $id_K \in \mathrm{Gal}(K/F)$ is the unique automorphism fixing $\mathcal{L}$. Hence, $\mathcal{L}$ is contained in K but not in proper subfield of K containing F. This implies that $K = F(\mathcal{L})$.

(c) Furthermore, since $\sigma\mathcal{L} = \zeta^{-1}\mathcal{L}$, we have $\sigma(\mathcal{L}^n) = (\zeta^{-1}\mathcal{L})^n = \mathcal{L}^n$. By Galois's theorem, we have $\mathcal{L}^n \in F$.

To sum up, if ζ is a primitive n-th root of unity and α is an element of K such that $\mathcal{L}_\sigma(\alpha, \zeta) \neq 0$, then $K = F(\mathcal{L})$ and $\mathcal{L}^n$ belongs to F.

11.3 Norm and trace

Definition 11.3.1. Let E/F be a finite separable extension and write $\mathrm{Emb}(E/F) = \{\sigma_1, \cdots, \sigma_n\}$. The norm map $N_{E/F} : E \to F$ and the trace map $tr_{E/F} : E \to F$ is defined by

$$N_{E/F}(\alpha) = \prod_{i=1}^{n} \sigma_i(\alpha) \quad \text{and} \quad tr_{E/F}(\alpha) = \sum_{i=1}^{n} \sigma_i(\alpha) \quad (\alpha \in E).$$

Remark. Let K be the normal closure of E over F and suppose $\tau \in \mathrm{Gal}(K/E)$. Given $\sigma \in \mathrm{Emb}(E/F)$, its extension to K is an F-embedding of K into $\overline{F}$, so $\sigma(E) \leq K$ and $\tau \circ \sigma$ is an F-embedding of E into $\overline{F}$. Therefore, an automorphism in $\mathrm{Gal}(K/F)$ permutes $\mathrm{Emb}(E/F)$ by left multiplication. This proves that $\tau(N_{E/F}(\alpha)) = N_{E/F}(\alpha)$ and $\tau(tr_{E/F}(\alpha)) = tr_{E/F}(\alpha)$, i.e., $N_{E/F}(\alpha), tr_{E/F}(\alpha) \in F$.

Observation 11.3.2. One can easily find the norm and the trace of an element α which is separable over a field F by computing its minimal polynomial over F. To be precise, if α is separable over F, then its minimal polynomial $m(t) = t^n + a_{n-1}t^{n-1} + \cdots + a_1 t + a_0$ over F satisfies

$$m(t) = (t - \sigma_1\alpha)\cdots(t - \sigma_n\alpha),$$

where $n = [F(\alpha) : F]_{\mathsf{sep}} = [F(\alpha) : F]$, thus $N_{F(\alpha)/F}(\alpha) = (-1)^n a_0$ and $tr_{F(\alpha)/F}(\alpha) = -a_{n-1}$.

Proposition 11.3.3. Suppose that K/F is a finite separable extension and $F \leq E \leq K$. Then

$$N_{K/F} = N_{E/F} \circ N_{K/E} \quad \text{and} \quad tr_{K/F} = tr_{E/F} \circ tr_{K/E}.$$

Proof. Let L be the normal(Galois) closure of K over F, and write

$$G = \mathrm{Gal}(L/F), \quad H = \mathrm{Gal}(L/E), \quad I = \mathrm{Gal}(L/K).$$

Then, for $\alpha \in K$,

$$N_{K/E}(\alpha) = \prod_{\sigma \in \mathrm{Emb}(K/E)} \sigma\alpha = \prod_{\sigma I \in H/I} \sigma\alpha, \quad tr_{K/E}(\alpha) = \sum_{\sigma \in \mathrm{Emb}(K/E)} \sigma\alpha = \sum_{\sigma I \in H/I} \sigma\alpha.$$

(It suffices to check that the computation of the last (finite) product(sum) is well-defined. If $\sigma I = \tau I$ for some $\sigma, \tau \in H$, then $\tau^{-1}\sigma \in I$ so $\sigma\alpha = \tau\alpha$ whenever $\alpha \in K$.) Letting $n = N_{K/E}(\alpha)$ and $t = tr_{K/E}(\alpha)$, we have

$$N_{E/F}(n) = \prod_{\tau H \in G/H} \tau n = \prod_{\sigma\tau I \in G/I} (\sigma\tau\alpha), \quad tr_{E/F}(t) = \sum_{\tau H \in G/G} \tau t = \sum_{\sigma\tau I \in G/I} (\sigma\tau\alpha).$$

Such $\sigma\tau$'s form G/I and they are F-embeddings of K into $\overline{F}$, so $N_{K/F} = N_{E/F} \circ N_{K/E}$ and $tr_{K/F} = tr_{E/F} \circ tr_{K/E}$, as desired. □

11.4 Infinite Galois extensions

Krull topology

Appendix A

Proof of some propositions

A.1 Prime numbers congruent to 1 modulo an integer

See Lemma 9.4.1 for the statement.

Proof. □

A.2 Quadratic cyclotomic extension

See eq. (9.1) in page 56 for the statement.

Proof. □