Galois Theory

Ronnie Sebastian

May 5, 2023

Thus conscience does make cowards of us all;
And thus the native hue of resolution
Is sicklied o'er with the pale cast of thought,
And enterprises of great pith and moment
With this regard their currents turn awry,
And lose the name of action.

-Hamlet

Contents

Chapter 1

Introduction

We will assume (very minimal) familiarity with Rings and Fields. By a field we shall always mean a commutative field (as opposed to a division algebra). By a ring we shall always mean a commutative ring with a multiplicative identity. The typical example of a ring that we have in mind is $K[X]$, where K is a field. In this chapter we address some very basic and simple questions that can be asked about fields and field extensions.

1.1 Extensions and Subfields

Let F be a field. A field extension of F is a field K and an inclusion $i : F \hookrightarrow K$ such that i respects addition and multiplication. It is easily checked that these conditions force $i(0_F) = 0_K$ and $i(1_F) = 1_K$. Similarly, a subfield of F is a field E and an inclusion $j : E \hookrightarrow F$ such that j respects addition and multiplication.

Question 1.1.1. Given a field F, does it always have a proper extension?

Answer. Yes. Consider the ring $F[X]$ whose elements are polynomials in the variable X. Let $K = F(X)$ denote its field of fractions. The precise definition of K is

$$K := \left\{ \frac{f(X)}{g(X)} \;\middle|\; f(X), g(X) \in F[X],\ g(X) \neq 0 \right\}.$$

Then $F \subset K$. The field K is called the field of rational functions in one variable over F. □

Question 1.1.2. Given a field F, does it always have a proper subfield?

Answer. No. Let $F = \mathbb{Q}$. If $E \subset F$ were a subfield, then $1 \in E$ (by definition of subfield). This will force that $n \in E$ for every $n \in \mathbb{Z}$. Finally this shows that $n/m \in E$ for all $n \in \mathbb{Z}$ and $m \in \mathbb{Z}, m \neq 0$. This proves that $E = F$. The same proof works with $F = \mathbb{Z}/(p)$. □

The characteristic of a field is defined as follows. Consider the unique ring homomorphism $\mathbb{Z} \to F$ defined by sending 1 to 1_F. The kernel of this homomorphism is a prime ideal of $\mathbb{Z}$. This prime ideal is either (0) or (p), for some positive prime p. The characteristic of F is defined to be 0 or p accordingly. Equivalently, the characteristic may be defined to be the smallest positive integer p such that $p \cdot 1_F = 0$, if there is such a positive integer, or else define it to be 0. If F is a field of positive characteristic, then we get that $\mathbb{Z}/(p) \subset F$. Thus, given any field, there is a smallest subfield it contains. This subfield is the one which is generated by 1_F. This subfield is isomorphic to $\mathbb{Z}/(p)$ or $\mathbb{Q}$.

1.2 Subfields generated by elements

Remark 1.2.1. Recall the following property of polynomial rings. Let R and S be rings and let $\phi : R \to S$ be a ring homomorphism. Let I be a set and consider the **polynomial ring** $R[X_i]_{(i \in I)}$. Here the X_i are indeterminates indexed by the set I. Clearly, there is an inclusion $R \subset R[X_i]_{(i \in I)}$. Let T denote the set of all ring homomorphisms $\tilde{\phi} : R[X_i]_{(i \in I)} \to S$ whose restriction to R is ϕ. There is an obvious map

$$T \to \prod_{i \in I} S$$

given by $\tilde{\phi} \mapsto (\tilde{\phi}(X_i))_{i \in I}$. An important fact about polynomial rings is that this map is a bijection. □

Suppose we are given fields $F \subset K$. Then we can form fields E which satisfy $F \subset E \subset K$. This is done as follows. Let α_i, for $i \in I$, be a collection of elements in K. First consider the smallest subring of K which contains F and all the α_i. This ring, call it R, is the image of the unique

ring homomorphism from the polynomial ring $F[X_i]_{i\in I}$ (see Remark 1.2.1)

$$F[X_i]_{i\in I} \to K \tag{1.2.2}$$

which sends each $X_i \mapsto \alpha_i$. Thus, we have $F \subset R \subset K$. Now define

$$F(\alpha_i)_{i\in I} := \left\{ \frac{a}{b} \;\middle|\; a, b \in R, b \neq 0 \right\}.$$

Clearly $F(\alpha_i)_{i\in I}$ is a field which contains F and all the α_i. We claim that it is the smallest subfield of K which contains F and all the α_i. In other words, if E' is a subfield of K which contains F and all the α_i, then $F(\alpha_i)_{i\in I} \subset E'$. This is left as an exercise to the reader.

1.3 Algebraic and Transcendental elements

We know that $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are fields and satisfy the inclusions $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$. Inside $\mathbb{C}$ we have the complex number i which has the property that it satisfies the equation $X^2 + 1 = 0$. Similarly, inside $\mathbb{R}$ we have $\sqrt{2}$, which has the property that it satisfies the equation $X^2 - 2 = 0$.

Definition 1.3.1 (Algebraic elements)**.** *Let $F \subset K$ be fields. An element $\alpha \in K$ is said to be algebraic over F if there exists a polynomial $f(X) \in F[X]$ such that $f(\alpha) = 0$.*

Thus, $i \in \mathbb{C}$ is algebraic over $\mathbb{Q}$. Similarly, $\sqrt{2} \in \mathbb{R}$ is algebraic over $\mathbb{Q}$. It is natural to ask if every element of $\mathbb{C}$ is algebraic over $\mathbb{Q}$. The next proposition shows that this is not the case.

We will use the following simple observation in the proof. Let R be a ring and let $f(X) \in R[X]$ be a polynomial with coefficients in R. Let $\alpha \in R$. Then

$$f(X) = (X - \alpha)g(X) + f(\alpha) \tag{1.3.2}$$

for some polynomial $g(X) \in R[X]$. To see this, simply write $X = X - \alpha + \alpha$ in place of X in the expression for $f(X)$, and then expand each monomial $X^n = (X - \alpha + \alpha)^n$ using the binomial expansion. For example,

$$X^2 = (X - \alpha)^2 + 2\alpha(X - \alpha) + \alpha^2.$$

From this (1.3.2) follows. In particular, if $f(\alpha) = 0$ then we get that $f(X) = (X - \alpha)g(X)$. We can ask if $g(X)$ has a root in R. Repeating this process, we see that we can write

$$f(X) = (X - \alpha_1)(X - \alpha_2) \dots (X - \alpha_r)h(X)\,.$$

Here $h(X)$ is a polynomial of degree $\deg(f(X)) - r \geqslant 0$ and has no roots in R. Consider the situation when R is a domain. This shows that the set of roots of $f(X)$ in R is a finite set. In fact, it is a subset of $\{\alpha_1, \dots, \alpha_r\}$.

Proposition 1.3.3. *Let A denote the elements in $\mathbb{C}$ which are algebraic over $\mathbb{Q}$. Then A is a countable set.*

Proof. The cardinality of $\mathbb{Q}[X]$ is countable. We sketch for the benefit of the reader. If T_1 and T_2 are countable sets then $T_1 \times T_2$ is also countable. Applying this repeatedly we see that $T^{\times n}$ is a countable set. In particular, the vector space $\mathbb{Q}^n$ is countable. The polynomials of degree $\leqslant n$ are identified with the vector space $\mathbb{Q}^{n+1}$. This shows that the set of polynomials of degree $\leqslant n$, denote is by $\mathcal{P}_{\leqslant n}$ is countable. Finally, a countable union of countable sets is countable, and so $\mathbb{Q}[X] = \bigcup_{n \geqslant 0} \mathcal{P}_{\leqslant n}$ is countable.

Then

$$A = \bigcup_{f \in \mathbb{Q}[X]} \{\alpha \in \mathbb{C} \mid f(\alpha) = 0\}$$

For each f, the set of roots of f is a finite set. Thus, the above is a countable union of sets, each of which is finite. Since a countable union of countable sets is countable, it follows that A is countable. On the other hand we know that $\mathbb{C}$ is not countable. Thus, there are plenty of elements in $\mathbb{C}$ which are not algebraic over $\mathbb{Q}$. □

Remark 1.3.4. The same proof shows that there are elements in $\mathbb{R}$ which are not algebraic over $\mathbb{Q}$.

Definition 1.3.5. *Let $F \subset K$ be fields. An element $\alpha \in K$ is called transcendental over F if α is not algebraic over F.*

Remark 1.3.6. Suppose $F \subset K$ and $\alpha \in K$. Let $E := F(\alpha)$ denote the smallest subfield of K containing F and α. Then clearly α is algebraic over E since it satisfies the polynomial $X - \alpha \in E[X]$. In particular, α may be transcendental over F, but it is obviously algebraic over $F(\alpha)$.

Remark 1.3.7. The above proof that $\mathbb{R}$ (or $\mathbb{C}$) has transcendental elements over $\mathbb{Q}$ is not constructive. It motivates the following question, can we explicitly write down a number which is transcendental over $\mathbb{Q}$? Although almost every real number is transcendental, it is very difficult to prove that a given number is transcendental. Joseph Liouville discovered the first transcendental number in 1844:

$$\sum_{n=1}^{\infty} 10^{-n!} = 0.11000100000000000000000010\ldots$$

In 1873 Charles Hermite proved that e is transcendental and in 1882 Ferdinand von Lindemann proved that π is transcendental. This course is all about algebraic elements. However, in this chapter let us make a small digression and see Liouville's construction of transcendental real numbers. □

Theorem 1.3.8. *[Liouville's Theorem] Let $\alpha \in \mathbb{R}\setminus\mathbb{Q}$ be algebraic, satisfying a polynomial of degree n. Then there exists a constant $c > 0$ dependent on α ($c = c(\alpha)$) such that $\left|\alpha - \frac{p}{q}\right| > \frac{1}{cq^n} \quad \forall p, q \in \mathbb{Z}, q > 0$.*

Proof. We know that for algebraic α, there is a monic polynomial $P(X) \in \mathbb{Q}[X]$ which is irreducible, of degree n and $P(\alpha) = 0$, and this is the polynomial of least degree. Clearing denominators we get $P(X) \in \mathbb{Z}[X]$ of degree n such that $P(\alpha) = 0$. By the Mean Value Theorem we have,

$$\left|P(\alpha) - P\left(\frac{p}{q}\right)\right| = \left|\alpha - \frac{p}{q}\right| \cdot |P'(\xi)|$$

for some ξ lying between α and $\frac{p}{q}$. Let us observe that $P'(\xi) \neq 0$, or else, by looking at the LHS in the above equation, we will have (since $P(\alpha) = 0$)

$$P\Big(\frac{p}{q}\Big) = 0\,.$$

This will mean that p/q is a root of $P(X)$, contradicting the fact that $P(X)$ is irreducible over $\mathbb{Q}$. Then

$$\begin{aligned} P\left(\frac{p}{q}\right) &= a_n\frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}q}{q^n} + a_{n-2}\frac{p^{n-2}q^2}{q^n} + \cdots + a_0 \\ &= \frac{a_np^n + a_{n-1}p^{n-1}q + \cdots + a_0q^n}{q^n}\,. \end{aligned}$$

Since $a_n p^n + a_{n-1}p^{n-1} + \cdots + a_0 \in \mathbb{Z}$ and is nonzero, its absolute value is $\geqslant 1$. Thus, we get

$$\left| P\left(\frac{p}{q}\right) \right| \geqslant \frac{1}{q^n}\,.$$

This shows that

$$\left| \alpha - \frac{p}{q} \right| \geqslant \frac{1}{q^n |P'(\xi)|}\,.$$

Assume $\left|\alpha - \frac{p}{q}\right| < 1$. Since ξ lies between α and $\frac{p}{q}$ we get $|\xi| < |\alpha| + 1$. Using this we get

$$|P'(\xi)| \leqslant \sum_{i=0}^{n} \left| i a_i \xi^{i-1} \right| \leqslant \sum_{i=0}^{n} i|a_i|(|\alpha|+1)^{i-1}\,.$$

Define

$$M := \sum_{i=0}^{n} i|a_i|(|\alpha|+1)^{i-1}\,.$$

Note that it only depends on α. Then we have just seen that

$$|P'(\xi)| \leqslant M\,.$$

Thus, if $\left|\alpha - \frac{p}{q}\right| < 1$ then

$$\left| \alpha - \frac{p}{q} \right| > \frac{1}{(M+1)q^n}\,.$$

If $\left|\alpha - \frac{p}{q}\right| \geqslant 1$, then obviously $\left|\alpha - \frac{p}{q}\right| > \frac{1}{2q^n}$. If $c = \max(M+1, 2)$ then it satisfies the condition $\left|\alpha - \frac{p}{q}\right| > \frac{1}{cq^n}$ for all rationals. This proves the Theorem. □

Corollary 1.3.9. *Let $\alpha \in \mathbb{R} \setminus \mathbb{Q}$. Assume there is $\beta > 0$ and an infinite sequence of distinct rationals p_n/q_n satisfying $\left|\alpha - \frac{p_n}{q_n}\right| < \frac{\beta}{q_n^{\omega_n}}$ and $\omega_n \to \infty$. Then α is transcendental.*

Proof. For any $\beta > 0$, there are only finitely many numbers with $q = 1$ and $\left|\alpha - \frac{p}{q}\right| < \beta$. Thus, we can discard those $\frac{p_n}{q_n}$ for which $q_n = 1$, there are only

finitely many such. From now on we assume $q_n \geqslant 2$. If α were algebraic with degree m, by the previous theorem we can find a bound $c(\alpha)$ such that

$$\frac{1}{c(\alpha)q_n^m} < \left|\alpha - \frac{p_n}{q_n}\right| \quad \forall n$$

By the assumption on α we have

$$\frac{1}{c(\alpha)q_n^m} < \left|\alpha - \frac{p_n}{q_n}\right| < \frac{\beta}{q_n^{\omega_n}} \quad \forall n$$

Thus, $q_n^{\omega_n - m} < \beta.c(\alpha)$. But as $\omega_n \to \infty, q_n^{\omega_n - m} \to \infty$. We reach a contradiction, and hence α is not algebraic. □

Corollary 1.3.10. *Consider the real number*

$$\alpha = \sum_{i \geqslant 0} \frac{1}{10^{i!}}\,.$$

This is transcendental over $\mathbb{Q}$.

Proof. Define

$$\frac{p_n}{q_n} := \sum_{i=0}^{n} \frac{1}{10^{i!}} = \frac{p_n}{10^{n!}}$$

Then

$$\begin{aligned}\left|\alpha - \frac{p_n}{q_n}\right| &= \sum_{i \geqslant n+1} \frac{1}{10^{i!}} \\ &\leqslant \frac{1}{10^{(n+1)!}} \sum_{i \geqslant n+1} \frac{1}{10^{i! - (n+1)!}} \\ &< \frac{2}{10^{(n+1)!}}\end{aligned}$$

To apply the previous corollary, it suffices to show that $\alpha \notin \mathbb{Q}$. To the contrary, let us assume that $\alpha = p/q$. Clearly, $\alpha \neq p_n/q_n$ (since $\alpha > p_n/q_n$) and so $pq_n - qp_n \neq 0$. Then we have

$$\frac{1}{qq_n} \leqslant \left|\frac{pq_n - p_n q}{qq_n}\right| = \left|\alpha - \frac{p_n}{q_n}\right| < \frac{2}{10^{(n+1)!}}$$

This shows that for all n we have

$$\frac{1}{q10^{n!}} < \frac{2}{10^{(n+1)!}},$$

that is, $10^{(n+1)!} < 2q10^{n!}$. This is of course not possible when n is sufficiently large. This proves that $\alpha \notin \mathbb{Q}$ and now we apply the previous corollary. □

Remark 1.3.11. Using the same idea as above, we may show that e is irrational. Let

$$e = \sum_{i \geqslant 0} \frac{1}{i!}\,.$$

Assume that $e = p/q$ and define

$$\frac{p_n}{q_n} = \sum_{i=0}^{n} \frac{1}{i!} = \frac{p_n}{n!}\,.$$

Then

$$\begin{aligned}\left| e - \frac{p_n}{q_n} \right| &= \sum_{i \geqslant n+1} \frac{1}{i!} \\ &< \frac{2}{(n+1)!}\end{aligned}$$

Clearly $e - p_n/q_n \neq 0$. Thus, we have

$$\frac{1}{qq_n} < \left| \frac{p}{q} - \frac{p_n}{q_n} \right| < \frac{2}{(n+1)!}\,.$$

This shows that

$$(n+1)! < 2qn!$$

which is clearly not possible when n is sufficiently large. □

1.4 Eisenstein's criterion

In this section we will see a criterion to check when a polynomial is irreducible. Let

$$f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$$

be a nonzero polynomial.

Definition 1.4.1. *The content of $f(X)$ is defined to be the integer*

$$\operatorname{cont}(f) := \gcd(a_0, \ldots, a_n) \in \mathbb{Z}$$

If $\operatorname{cont}(f) = 1$*, we say that $f(X)$ is a primitive polynomial.*

Proposition 1.4.2. *Product of two nonzero primitive polynomials in $\mathbb{Z}[X]$ is a primitive polynomial in $\mathbb{Z}[X]$.*

Proof. Let

$$f(X) = \sum_{i=0}^{r} a_i X^i \qquad \text{and} \qquad g(X) = \sum_{j=0}^{s} b_j X^j$$

be two nonzero primitive polynomials in $\mathbb{Z}[X]$. If $f(X)g(X)$ is not primitive in $\mathbb{Z}[X]$, there is a prime number p which divides $\operatorname{cont}(f(X)g(X))$. In particular, it divides all the coefficients of $f(X)g(X)$. Going mod p we see that

$$f(X)g(X) \equiv 0 \qquad \bmod p\,.$$

But this gives a contradiction since $f(X) \bmod p \not\equiv 0$ and $f(X) \bmod p \not\equiv 0$ and $\mathbb{F}_p[X]$ is an integral domain. □

Corollary 1.4.3. *Let $f(X), g(X) \in \mathbb{Z}[X] \setminus \{0\}$. Then*

$$\operatorname{cont}(f(X)g(X)) = \operatorname{cont}(f(X)) \cdot \operatorname{cont}(g(X))\,.$$

Proof. Note that $f(X) = c_f \cdot f_0(x)$ and $g(X) = c_g \cdot g_0(x)$, where

$$c_f = \operatorname{cont}(f(X)), \qquad c_g = \operatorname{cont}(g(X))$$

and both $f_0(x)$ and $g_0(x)$ are primitive polynomials in $\mathbb{Z}[X]$. Then

$$\begin{aligned} \operatorname{cont}(f(X)g(X)) &= \operatorname{cont}(c_f c_g \cdot f_0(X)g_0(X)) \\ &= c_f c_g \cdot \operatorname{cont}(f_0(X)g_0(X)) \\ &= c_f c_g \end{aligned}$$

since $f_0(x)g_0(x)$ is primitive by Proposition 1.4.2. □

Lemma 1.4.4 (Gauss)**.** *Let $f(X) \in \mathbb{Z}[X]$. Then $f(X)$ is irreducible in $\mathbb{Z}[X]$ if and only if $f(X)$ is irreducible in $\mathbb{Q}[X]$.*

Proof. Let $f(X) \in \mathbb{Z}[X]$ be irreducible in $\mathbb{Z}[X]$. If $f(X)$ is reducible in $\mathbb{Q}[X]$, then there are two non-constant polynomials $g(X), h[X] \in \mathbb{Q}[X]$ such that

$$f(X) = g(X)h[X]\,.$$

Then there are integers a, b, c, d with $b \neq 0$ and $d \neq 0$, and primitive polynomials $g_0(x), h_0(x) \in \mathbb{Z}[X]$ such that

$$g(X) = ab^{-1}g_0(x) \qquad \text{and} \qquad h(X) = cd^{-1}h_0(x)\,.$$

Then $f(X) = ab^{-1}cd^{-1}g_0(x)h_0(x)$ and so

$$bd \cdot f(X) = ac \cdot g_0(x)h_0(x)\,.$$

Taking content we have

$$\begin{aligned} bd\,\mathrm{cont}(f) &= \mathrm{cont}(ac \cdot g_0(x)h_0(x)) \\ &= ac \cdot \mathrm{cont}(g_0(x)h_0(x)) \\ &= ac\,. \end{aligned}$$

by Corollary 1.4.3. Therefore,

$$bd\,f(X) = bd\,\mathrm{cont}(f)g_0(x)h_0(x)\,,$$

that is, $f(X) = \mathrm{cont}(f)g_0(x)h_0(x)$ which contradicts irreducibility of $f(X)$ in $\mathbb{Z}[X]$.

If $f(X)$ is irreducible in $\mathbb{Q}[X]$ then it is obvious that it is irreducible in $\mathbb{Z}[X]$. This is left as an exercise to the reader. □

Theorem 1.4.5 (Eisenstein's irreducibility criterion)**.** *Let $f(X) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$. If there is a prime integer $p > 0$ such that*

(i) $p \big| a_i$, *for all* $i = 0, 1, \ldots, n-1$,

(ii) $p \nmid a_n$, *and*

(iii) $p^2 \nmid a_0$,

then $f(X)$ is irreducible in $\mathbb{Z}[X]$ and so also in $\mathbb{Q}[X]$.

Proof. It follows from Lemma 1.4.4 that if $f(X)$ is irreducible in $\mathbb{Z}[X]$, it is irreducible in $\mathbb{Q}[X]$. Thus, it suffices to show that $f(X)$ is irreducible in $\mathbb{Z}[X]$.

Suppose on the contrary that $f(X)$ is reducible in $\mathbb{Z}[X]$. Then there are two nonzero non-constant polynomials

$$g(X) = \sum_{i=0}^{s} b_i X^i, \qquad h[X] = \sum_{i=0}^{t} c_i X^i \in \mathbb{Z}[X]\,.$$

such that $f(X) = g(X)h[X]$. Note that $n = r + s$ and $a_n = b_s c_t$. Now we go mod p. Note that p divides all the a_i except for a_n. This shows that the leading coefficient of $g(X)$ and $h(X)$ are not divisible by p. We get that

$$a_n X^n = g(X)h(X) \qquad \bmod p\,.$$

This forces that $g(X) \equiv b_s X^s \bmod p$ and $h(X) \equiv c_t X^t \bmod p$. This proves that the constant coefficients b_0 and c_0 are divisible by p. But since $a_0 = b_0 c_0$ this shows that p^2 divides a_0, which is a contradiction. Therefore, $f(X)$ must be irreducible in $\mathbb{Z}[X]$. □

Corollary 1.4.6. *For any prime number $p > 0$, the cyclotomic polynomial $\Phi_p(X) := 1 + X + X^2 + \cdots + X^{p-1}$ is irreducible in $\mathbb{Q}[X]$.*

Proof. Note that $(X-1)\Phi_p(X) = X^p - 1$. Putting $X + 1$ in place of X, we get

$$X\Phi_p(X+1) = (X+1)^p - 1 = \sum_{i=1}^{p} \binom{p}{i} X^i\,.$$

This shows that

$$\Phi_p(X+1) = \sum_{i=1}^{p} \binom{p}{i} X^{i-1}\,.$$

Since p divides $\binom{p}{i}$, for all $i = 1, \ldots, p-1$; $p \nmid \binom{p}{p}$ and $p^2 \nmid \binom{p}{1}$, by Theorem 1.4.5 we conclude that $\Phi_p(X+1)$ is irreducible in $\mathbb{Q}[X]$. Hence $\Phi_p(X)$ is irreducible in $\mathbb{Q}[X]$. □

Example 1.4.7. Let $f(X) = X^3 - 3X^2 - 3X - 1 \in \mathbb{Z}[X]$. Then $f(X+1) = (X+1)^3 - 3(X+1)^2 - 3(X+1) - 1 = X^3 - 6X^2 + 6X - 2$. Then by Eisenstein's irreducibility criterion, $f(X+1)$ is irreducible in $\mathbb{Q}[X]$, and hence $f(X)$ is irreducible in $\mathbb{Q}[X]$. □

Remark 1.4.8. With the same line of arguments, Theorem 1.4.5 can be proved in the following more general setup. Let A be a unique factorization domain and $f(X) = \sum_{i=0}^{n} a_i X^i \in A[X]$ a nonzero non-unit polynomial. If there is a prime element $p \in A$ such that

(i) $p \mid a_i$, for all $i = 0, 1, \ldots, n-1$,

(ii) $p \nmid a_n$ and

(iii) $p^2 \nmid a_0$,

then $f(X)$ is irreducible in $Q(A)[X]$, where $Q(A)$ is the field of fractions of A. Take $A = K[X]$ where K is a field, and formulate and prove the theorem in this case. □

Chapter 2

Algebraic Extensions

In this chapter we introduce and study the notion of finite extensions and algebraic extensions. Algebraic extensions are almost like finite extensions. Almost all statements about algebraic extensions are proved by first proving those results for finite extensions.

2.1 Finite extensions

Let $E \subset F$ be fields. Then clearly F is a vector space over E. The vector space dimension of F as an E vector space is denoted by $[F : E]$ and is called the degree of the extension. Although the techniques in this chapter may seem very modest, to understand their utility, the reader may try the following exercise before and after reading this section.

Exercise: Compute the degree $[\mathbb{Q}(\sqrt[3]{2}, \sqrt{5}) : \mathbb{Q}]$.

Definition 2.1.1. *We say that F is a finite extension of E if $[F : E]$ is finite.*

We next explain a construction which gives several examples of finite extensions. First we need the following Lemma.

Lemma 2.1.2. *Let F be a field. Then the ring $F[X]$ is a principal ideal domain.*

Proof. Let $I \neq 0$ be a nonzero ideal. We need to show that there is a polynomial $f(X)$ such that $I = (f(X))$. Let $f(X)$ be a nonzero polynomial

in I of least degree. We claim that $I = (f(X))$. If not, then there is $h(X) \in I \setminus (f(X))$. Dividing $h(X)$ by $f(X)$ we get

$$h(X) = b(X)f(X) + t(X)$$

where $\deg(t(X)) < \deg(f(X))$. As $h(X), b(X)f(X) \in I$, it follows that $t(X) \in I$. But this contradicts the minimality of degree of $f(X)$. Thus, it follows that $I = (f(X))$. This completes the proof of the Lemma. □

Proposition 2.1.3. *Let F be a field and let $p(X) \in F[X]$ be an irreducible polynomial. Let $(p(X))$ denote the ideal generated by the polynomial $p(X)$. Then the ring $E := F[X]/(p(X))$ is a field. The vector space dimension of E over F is* $\deg(p(X))$.

Proof. To show E is a field, it suffices to show that if $\alpha \in E$ and $\alpha \neq 0$, then there is a β such that $\alpha\beta = 1$. Let $\alpha = f(X) \bmod p(X)$. Let $I := (f(X), p(X))$ denote the ideal in $F[X]$ generated by $f(X)$ and $p(X)$. By Lemma 2.1.2 it follows that $I = (t(X))$. Since $t(X)$ divides $p(X)$ it follows that $t(X)$ is either a constant, which we may assume to be 1, or it is $p(X)$. If it were $p(X)$ then we get that $p(X)$ divides $f(X)$, which is not true. Thus, $t(X) = 1$, that is, $I = (1)$. Thus, we get that

$$1 = g(X)f(X) + k(X)p(X)\,.$$

Going modulo $p(X)$ we see that $\beta = g(X) \bmod p(X)$ is such that $\beta\alpha = 1$. This proves that E is a field.

Let $d = \deg(p(X))$. We will show that the images of $1, X, \ldots, X^{d-1}$ in E form a basis for E as a vector space over F.

Linear independence. First we claim that these are linearly independent. If not, suppose there is a relation

$$a_0 + a_1\overline{X} + \ldots + a_{d-1}\overline{X^{d-1}} = 0\,.$$

This implies that $p(X)$ divides the polynomial $a_0 + a_1X + \ldots + a_{d-1}X^{d-1}$, that is,

$$p(X)h(X) = a_0 + a_1X + \ldots + a_{d-1}X^{d-1}\,.$$

But this is impossible, as is seen by looking at the degree. This proves that the images of $1, X, \ldots, X^{d-1}$ in E are linearly independent over F.

Spanning set. Next we show that the images of $1, X, \ldots, X^{d-1}$ span E as a vector space over F. Given any $f(X) \in F[X]$, we have

$$f(X) \equiv r(X) \bmod p(X) \qquad \deg(r(X)) < d\,.$$

This shows that the element $\overline{f(X)}$ is represented by $\overline{r(X)}$ which is in the span of $1, \overline{X}, \ldots, \overline{X}^{d-1}$. This completes the proof of the Proposition. □

As a corollary of the above proposition, corresponding to an irreducible polynomial,we may construct a finite extension.

Next let us consider the situation when we are given an extension of fields $E \subset K$ and we want to construct subfields of K which are finite over E. This is closely related to elements in K which are algebraic over E. The reader may recall the definition of $E(\alpha)$ from section 1.2. Similar to the notation in section 1.2, we will use the following notation. Suppose $E \subset K$ and α_i, $i \in I$ is a collection of elements, then $E[\alpha_i]_{i\in I} \subset K$ is by definition the smallest subring of K that contains E and all the α_i. In section 1.2 this is the image of the ring homomorphism (1.2.2).

Proposition 2.1.4. *Let $E \subset K$ be an extension of fields. Let $\alpha \in K$ be algebraic over E and let $f(X) \in E[X]$ be a polynomial of least degree such that $f(\alpha) = 0$. Then*

(i) $f(X)$ is irreducible,

(ii) the subring $E[\alpha]$ is isomorphic to $E[X]/(f(X))$,

(iii) there is an equality $E[\alpha] = E(\alpha)$.

Proof. (i) Let us assume that $f(X)$ is not irreducible. Then there are polynomials $f_1(X)$ and $f_2(X)$ such that $f(X) = f_1(X)f_2(X)$ and $\deg(f_i(X)) < \deg(f(X))$. Evaluating at α we see that one of the $f_i(\alpha)$ has to be zero. This contradicts the assumption that f was of least degree such that $f(\alpha) = 0$.

(ii) and (iii) There is a unique homomorphism from $\Phi : E[X] \to K$ which is the identity on E and sends X to α. We claim that the kernel of this homomorphism is $(f(X))$, the ideal generated by $f(X)$. Assume that $h(X) \mapsto 0$. Then we can write

$$h(X) = g(X)f(X) + r(X) \qquad \deg(r(X)) < \deg(f(X))\,.$$

Evaluating at α we see that $r(\alpha) = 0$, which forces that $r(X) = 0$. This shows that $h(X) \in (f(X))$. From this we conclude that Φ induces an inclusion $\Phi : E[X]/(f(X)) \to K$. Thus, Φ is an isomorphism onto its image, which is clearly $E[\alpha]$. This proves (ii).

(iii) Since $E[\alpha]$ is isomorphic to $E[X]/(f(X))$, it follows that it is a field. Recall that $E(\alpha)$ is obtained by taking all elements in K of the type a/b, where $a, b \in E[\alpha]$ and $b \neq 0$. Thus, clearly, $E[\alpha] \subset E(\alpha)$. On the other hand since $E(\alpha)$ is the smallest subfield of K containing E and α, and $E[\alpha]$ is also a field that has this property, it follows that $E(\alpha) \subset E[\alpha]$. This proves that $E[\alpha] = E(\alpha)$. □

Remark 2.1.5. In the above we have proved that $E[\alpha] = E(\alpha)$. In particular, this means that given a polynomial $g(X)$ such that $g(\alpha) \neq 0$ there is an inverse $1/g(\alpha)$ in $E[\alpha]$. This inverse can be found as follows. Since $g(\alpha) \neq 0$ it follows that $f(X)$ does not divide $g(X)$ and so they are coprime, since $f(X)$ is irreducible. Thus, there are polynomials $h(X)$ and $q(X)$ such that

$$h(X)g(X) + q(X)f(X) = 1\,.$$

Evaluating both sides at α we see that

$$h(\alpha) = \frac{1}{g(\alpha)}\,.$$

We emphasize that this means that every element of $E(\alpha)$ can be obtained by evaluating a polynomial in $E[X]$, of degree $< \deg(f(X))$, at α. □

Corollary 2.1.6. *Let $E \subset K$ be extension. Let $\alpha \in K$ be algebraic over E with irreducible polynomial $f(X)$. Then the extension $E(\alpha)$ is finite over E of degree equal to* $\deg(f(X))$.

Proof. Since $E(\alpha) \cong E[X]/(f(X))$ and $E[X]/(f(X))$ is finite dimensional over E, it follows that $E(\alpha)$ is finite dimensional. Now use Proposition 2.1.3 and Proposition 2.1.4. □

Corollary 2.1.7. *Let $E \subset K$ be fields and let $\alpha_1, \alpha_2, \ldots, \alpha_r \in K$ be elements which are algebraic over E. Then*

$$E[\alpha_1, \alpha_2, \ldots, \alpha_r] = E(\alpha_1, \alpha_2, \ldots, \alpha_r)\,.$$

Proof. Recall that from the definition of $E(\alpha_1, \alpha_2, \ldots, \alpha_r)$ we have that

$$E[\alpha_1, \alpha_2, \ldots, \alpha_r] \subset E(\alpha_1, \alpha_2, \ldots, \alpha_r)\,.$$

Thus, to prove the assertion, we will first show that $E[\alpha_1, \alpha_2, \ldots, \alpha_r]$ is a field. Then using the fact that $E(\alpha_1, \alpha_2, \ldots, \alpha_r)$ is the smallest subfield of K which contains E and α_i, it will follow that both are equal. Define $E_i = E[\alpha_1, \ldots, \alpha_i]$ and $E_0 = E$. Applying Proposition 2.1.4 to E_0 and α_1 we see that $E_1 = E[\alpha_1] = E(\alpha_1)$ is a field. The element α_2 is algebraic over E_1 and so similarly we get that $E_2 = E_1[\alpha_2] = E_1(\alpha)$ is a field. Proceeding in this way we see that $E[\alpha_1][\alpha_2]\ldots[\alpha_r]$ is a field. But

$$E[\alpha_1][\alpha_2]\ldots[\alpha_r] = E[\alpha_1, \alpha_2, \ldots, \alpha_r]$$

and so the assertion is proved. □

Lemma 2.1.8. *Let $E \subset L \subset K$ be fields. Consider the three numbers $[K : E], [L : E], [K : L]$. There is an equality*

$$[K : E] = [K : L][L : E]\,.$$

Proof. Assume that both $[K : L] =: n$ and $[L : E] =: m$ are finite. This means that we can find $k_1, k_2, \ldots, k_n \in K$ such that these form a basis for K as a vector space over L. Similarly, we can find $l_1, l_2, \ldots, l_m \in L$ such that these form a basis for L as a vector space over E. Consider the set $\{k_i l_j\}$. We claim that these form a basis for K over E. First let us check that these span K as a vector space over E. Every element of K can be written as

$$k = \sum_{i=1}^{n} \alpha_i k_i, \qquad \alpha_i \in L\,.$$

Each α_i can be written as

$$\alpha_i = \sum_{j=1}^{m} \beta_{ij} l_j, \qquad \beta_{ij} \in E\,.$$

Thus, we get

$$k = \sum_{i=1}^{n}\sum_{j=1}^{m} \beta_{ij} l_j k_i, \qquad \beta_{ij} \in E\,.$$

This shows that the set $\{k_i l_j\}$ spans K as a vector space over E.

Next let us prove that these are linearly independent over E. If not, then there is a relation

$$0 = \sum_{i=1}^{n} \sum_{j=1}^{m} \alpha_{ij} l_j k_i, \qquad \alpha_{ij} \in E\,.$$

Since the k_i are linearly independent over L, this shows that for each i we have

$$0 = \sum_{j} \alpha_{ij} l_j\,.$$

Since the l_j are linearly independent over E, this shows that the α_{ij} are 0. This proves that $\{k_i l_j\}$ is a basis for K over E. Thus, we get that if both $[K : L]$ and $[L : E]$ are finite then

$$[K : E] = [K : L][L : E]\,.$$

Now consider the situation when one of $[K : L]$ or $[L : E]$ is infinite. If $[L : E]$ is infinite then it is clear that $[K : E]$ is also infinite since $E \subset L \subset K$ (the vector space K has an infinite dimensional subspace). Now consider the case $[K : L]$ infinite. Choose an infinite basis for K over L. It is clear that these basis elements are linearly independent over E. Thus, the E span of these elements is an E-subspace of K which is infinite dimensional. This shows that $[K : E]$ is infinite.

Thus, the equality $[K : E] = [K : L][L : E]$ holds in all cases. □

Corollary 2.1.9. *Let $E \subset K$ be fields and let $\alpha_1, \ldots, \alpha_n \in K$ be algebraic over E. Then $E(\alpha_1, \ldots, \alpha_n)$ is a finite extension of E.*

Proof. We saw before that $E[\alpha_1, \ldots, \alpha_n] = E(\alpha_1, \ldots, \alpha_n)$. Define $E_0 = E$ and let $E_i = E[\alpha_1, \ldots, \alpha_i]$. Then we have

$$[E_n : E] = \prod_{i=1}^{n} [E_i : E_{i-1}] = \prod_{i=1}^{n} [E_{i-1}[\alpha_i] : E_{i-1}]\,.$$

As E_i is a field containing E and α_{i+1} is algebraic over E, it follows that α_{i+1} is algebraic over E_i. The degree of extension $[E_i[\alpha_{i+1}] : E_i]$ is the degree of the irreducible polynomial of α_{i+1} over E_i. Similarly, for the extension

$[E[\alpha_{i+1}] : E]$. Thus, we clearly have $[E_i[\alpha_{i+1}] : E_i] \leqslant [E[\alpha_{i+1}] : E]$. This shows that

$$[E_n : E] \leqslant \prod_{i=1}^{n} [E[\alpha_i] : E] < \infty \,.$$

This completes the proof of the Corollary. □

Let us now try to answer the question that was raised at the beginning of this section. First we note that $\mathbb{Q}(\sqrt[3]{2}, \sqrt{5}) = \mathbb{Q}[\sqrt[3]{2}, \sqrt{5}]$. Next note that

$$[\mathbb{Q}(\sqrt[3]{2}, \sqrt{5}) : \mathbb{Q}] = [\mathbb{Q}[\sqrt[3]{2}, \sqrt{5}] : \mathbb{Q}[\sqrt[3]{2}]] \cdot [\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] \,.$$

To compute $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}]$ we note that $\sqrt[3]{2}$ satisfies the equation $X^3 - 2 = 0$. This polynomial is irreducible, since if it factors, it will have a factor of degree 1, which implies that there is a rational number whose cube is 2, which is not possible. Thus, $\mathbb{Q}[\sqrt[3]{2}] \cong \mathbb{Q}[X]/(X^3 - 2)$ and so $[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = 3$.

To compute $[\mathbb{Q}[\sqrt[3]{2}, \sqrt{5}] : \mathbb{Q}[\sqrt[3]{2}]]$ we need to find the irreducible polynomial of $\sqrt{5}$ over $\mathbb{Q}[\sqrt[3]{2}]$. The element $\sqrt{5}$ satisfies the equation $X^2 - 5 = 0$. If this polynomial is reducible over $\mathbb{Q}[\sqrt[3]{2}]$, then it has linear factors, that is, a root in $\mathbb{Q}[\sqrt[3]{2}]$. But we can check by hand (a clumsy way to solve this problem) that the equation

$$(a_0 + a_1 \sqrt[3]{2} + a_2 \sqrt[3]{4})^2 = 5$$

has no solutions for $a_i \in \mathbb{Q}$.

Alternatively, (more cleverly) we can first check that $[\mathbb{Q}[\sqrt{5}] : \mathbb{Q}] = 2$. Now if $X^2 - 5 = 0$ has a root in $\mathbb{Q}[\sqrt[3]{2}]$ then this would mean that there is a nonzero homomorphism $\mathbb{Q}[\sqrt{5}] \cong \mathbb{Q}[X]/(X^2 - 5) \to \mathbb{Q}[\sqrt[3]{2}]$. That is, we will get an inclusion $\mathbb{Q}[\sqrt{5}] \subset \mathbb{Q}[\sqrt[3]{2}]$. Now this would imply that

$$[\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}] = [\mathbb{Q}[\sqrt[3]{2}] : \mathbb{Q}[\sqrt{5}]] \cdot [\mathbb{Q}[\sqrt{5}] : \mathbb{Q}] \,.$$

The LHS is 3 and the RHS is even, a contradiction. This means that $X^2 - 5$ is irreducible over $\mathbb{Q}[\sqrt[3]{2}]$ and so $\mathbb{Q}[\sqrt[3]{2}, \sqrt{5}] \cong \mathbb{Q}[\sqrt[3]{2}][X]/(X^2 - 5)$. This proves that $[\mathbb{Q}[\sqrt[3]{2}, \sqrt{5}] : \mathbb{Q}[\sqrt[3]{2}]] = 2$. Thus,

$$[\mathbb{Q}(\sqrt[3]{2}, \sqrt{5}) : \mathbb{Q}] = 6 \,.$$

Before we end this section, let us consider an abstract example we took earlier, $F \subset F(X)$, and try to see if $F(X)$ has any elements which are algebraic over F. The following lemma proves that the only elements in $F(X)$ which are algebraic over F are the ones in F.

Lemma 2.1.10. *If $\alpha \in F(X)$ is algebraic over F, then $\alpha \in F$.*

Proof. Suppose $\alpha = \frac{f(X)}{g(X)}$ is algebraic over F. Let $P(T)$ be the irreducible polynomial of α over F. We may assume that $f(X)$ and $g(X)$ have no common factors. Then we get $P(\alpha) = 0$, that is,

$$a_n \frac{f(X)^n}{g(X)^n} + a_{n-1} \frac{f(X)^{n-1}}{g(X)^{n-1}} + \cdots + a_0 = 0\,.$$

Multiplying with $g(X)^n$ this becomes

$$a_n f(X)^n + a_{n-1} f(X)^{n-1} g(X) + \cdots + a_0 g(X)^n = 0\,.$$

If $f(X)$ were a non-constant polynomial, then it will have an irreducible factor, call it $p(X)$. It follows that $p(X)$ will divide $g(X)$, which is a contradiction since we assumed that they have no common factor. If follows that $f(X)$ is constant. Similarly, we see that $g(X)$ is also a constant. □

Remark 2.1.11. This lemma shows that the extension $F(X)$ is far from being algebraic over F, in fact, it contains no algebraic elements other than those already in F. On the other hand, the extension $\mathbb{C}$ of $\mathbb{Q}$ contains elements which are algebraic over $\mathbb{Q}$ (for example, $\sqrt{2}$) and also elements which are transcendental over $\mathbb{Q}$ (as was seen in Proposition 1.3.3 and Corollary 1.3.10) □

2.2 Algebraic extensions

Definition 2.2.1. *Let $F \subset K$ be an extension of fields. We say that K is algebraic over F if every element of K is algebraic over F.*

Proposition 2.2.2. *Let E be a field extension of F. Suppose E is finite over F, then E is an algebraic extension.*

Proof. We need to show that every element of E is algebraic over F. Let $\alpha \in E$. Consider the F-vector subspace spanned by

$$1, \alpha, \alpha^2, \ldots$$

Since E is finite dimensional, it follows that this subspace is finite dimensional. Thus, there is l such that every element of this subspace is a span of $1, \alpha, \alpha^2, \ldots, \alpha^l$. We can write α^{l+1} as an F-linear combination of these, say

$$\alpha^{l+1} = a_0 + a_1\alpha + \ldots a_l\alpha^l \,.$$

This shows that α is a root of the polynomial

$$X^{l+1} - a_l X^l - \ldots - a_0 \in F[X] \,.$$

Thus, α is algebraic over F. This proves that E is algebraic over F. □

Proposition 2.2.3. *Let $E \subset K$ be an extension of fields. Let α and $\beta \neq 0$ be elements of K which are algebraic over E. Then $\alpha+\beta, \alpha\beta, \alpha/\beta$ are algebraic over E.*

Proof. By Corollary 2.1.9 the extension $E(\alpha, \beta)$ is a finite extension of E. The proposition now follows using Proposition 2.2.2. □

Corollary 2.2.4. *Let $E \subset K$ be field extensions. Let*

$$F := \{\alpha \in K \mid \alpha \text{ is algebraic over } E \} \,.$$

Then F is a field.

Proposition 2.2.5. *If $E \subset L \subset K$, L is algebraic over E and K is algebraic over L, then K is algebraic over E.*

Proof. Let $\beta \in K$. Since K is algebraic over L, it follows that β satisfies an equation $p(X) \in L[X]$. Let

$$p(X) = \alpha_n X^n + \alpha_{n-1}X^{n-1} + \ldots + \alpha_0, \qquad \alpha_i \in L \,.$$

Since L is algebraic over E, it follows that each of the α_i is algebraic over E. Define $E_0 = E$ and define $E_{i+1} = E_i[\alpha_{i-1}]$. Since α_i is algebraic over E, it is clearly algebraic over E_i. It follows, using Proposition 2.1.4 that each $[E_{i+1} : E_i] < \infty$. Using Lemma 2.1.8 we see

$$[E_{n+1} : E_0] = \prod_{i=0}^{n} [E_{i+1} : E_i] < \infty \,.$$

The polynomial $p(X) \in E_{n+1}[X]$ and this means that $[E_{n+1}[\beta] : E_{n+1}] < \infty$. Thus, we get that

$$[E_{n+1}[\beta] : E_0] = [E_{n+1}[\beta] : E_{n+1}][E_{n+1} : E_0] < \infty \,.$$

This shows that $E_{n+1}[\beta]$ is algebraic over E_0, in particular, β is algebraic over E_0. □

2.3 Algebraically closed fields

Definition 2.3.1. *A field K is called algebraically closed if every nonconstant polynomial $f(X) \in K[X]$ has a root in K.*

We will not prove the following important theorem which we will use later.

Theorem 2.3.2. *Let F be a field. There exists an algebraically closed field K such that $F \subset K$.*

Definition 2.3.3. *An extension $E \subset \bar{E}$ such that $\bar{E}$ is algebraically closed and algebraic over E is called an algebraic closure of E.*

Theorem 2.3.4. *Let E be a field. Then there is a field $\bar{E}$ which is algebraically closed and such that each element of $\bar{E}$ is algebraic over E.*

Proof. We apply Theorem 2.3.2. Let K be a field such that $E \subset K$ and K is algebraically closed. Let

$$\bar{E} := \{\alpha \in K \mid \alpha \text{ is algebraic over } E \}\,.$$

Using Corollary 2.2.4 we see that $\bar{E}$ is a field and it is algebraic over E. It remains to show that it is algebraically closed.

Let $p(X) \in \bar{E}[X]$ be a polynomial. Write

$$p(X) = \alpha_n X^n + \alpha_{n-1} X^{n-1} + \ldots + \alpha_0, \qquad \alpha_i \in \bar{E}\,.$$

For $i \geqslant 0$ let F_i be the extension $E[\alpha_0, \ldots, \alpha_i]$. Let $F_{-1} = E$. Then

$$[F_n : E] = [F_n : F_{n-1}][F_{n-1} : F_{n-2}] \ldots [F_1 : F_0][F_0 : F_{-1}]\,.$$

Since each α_i is algebraic over E, it follows that α_i is algebraic over F_{i-1}. This shows that the RHS is a finite number. Thus, it follows that F_n is a finite extension of E. Since K is algebraically closed, let β be a root of $p(X)$ in K. The polynomial $p(X) \in F_n[X]$. Let $f(X)$ be the unique monic polynomial of least degree in $F_n[X]$ such that $f(\beta) = 0$. Then $F_n[\beta] \cong F_n[X]/(f(X))$ and so $F_n[\beta]$ is a finite extension of F_n. This shows that $F_n[\beta]$ is a finite extension of E. Thus, β is algebraic over E, that is, $\beta \in \bar{E}$. This proves that $\bar{E}$ is algebraically closed. □

Chapter 3

Embeddings into algebraically closed fields

3.1 Existence of embeddings

Fix an algebraically closed field K. Assume that we are given a homomorphism of fields $\phi : E \to K$. Let $E \subset L$ be an algebraic extension. Consider the following diagram.

(3.1.1)
$$\begin{array}{ccc} L & \overset{\psi}{-\!\!-} & K \\ | & & \| \\ E & \xrightarrow{\quad\phi\quad} & K \end{array}$$

Definition 3.1.2. *The set of field homomorphisms $\psi : L \to K$ which make the above diagram commute is denoted by* $\mathrm{Hom}_\phi(L, K)$.

Proposition 3.1.3. *Fix an algebraically closed field K. Suppose that we are given a homomorphism of fields $\phi : E \to K$. Let $E \subset L$ be an algebraic extension. Assume that there is $\alpha \in L$ such that $L = E[\alpha]$. Then* $\mathrm{Hom}_\phi(L, K)$ *is non-empty.*

Proof. Let $p(X) \in E[X]$ be the monic irreducible polynomial of α. Say

$$p(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \,.$$

Then the kernel of the natural map $E[X] \to L$, which is identity on E and sends $X \mapsto \alpha$, is precisely $(p(X))$. Consider the polynomial

$$X^n + \phi(a_{n-1})X^{n-1} + \ldots + \phi(a_0) \in K[X]\,.$$

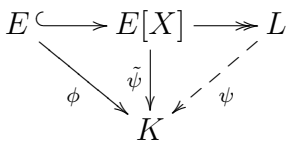
Let $\beta \in K$ be a root of this polynomial. Such a root exists since K is algebraically closed. Consider the unique ring homomorphism

$$\tilde{\psi} : E[X] \to K$$

given by

$$\tilde{\psi}(\sum b_i X^i) := \sum \phi(b_i)\beta^i\,.$$

Clearly, $\tilde{\psi}(p(X)) = 0$. Thus, there is a map ψ which makes the following diagram commute

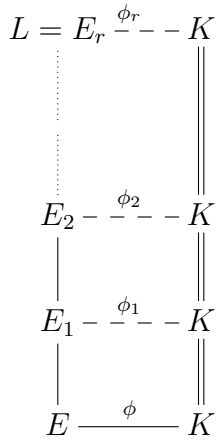


Clearly the restriction of ψ to E is ϕ. □

Proposition 3.1.4. *Fix an algebraically closed field K. Assume that we are given a homomorphism of fields $\phi : E \to K$. Let $E \subset L$ be an algebraic extension. Assume that L is a finite extension of E. Then* $\mathrm{Hom}_\phi(L, K)$ *is non-empty.*

Proof. The idea is to use the preceding proposition repeatedly. We can find elements $\alpha_1, \alpha_2, \ldots, \alpha_r$ such that $L = E[\alpha_1, \ldots, \alpha_r]$. Define $E_i = E[\alpha_1, \ldots, \alpha_i]$. Then $E_{i+1} = E_i[\alpha_{i+1}]$. Applying the preceding proposition to $E_1 = E[\alpha_1]$, we get that $\mathrm{Hom}_\phi(E_1, K) \neq \emptyset$. Let $\phi_1 \in \mathrm{Hom}_\phi(E_1, K)$. Again, applying the preceding proposition to ϕ_1 we get $\mathrm{Hom}_{\phi_1}(E_2, K) \neq \emptyset$. Proceeding in this fashion we get $\phi_r \in \mathrm{Hom}_{\phi_{r-1}}(E_r, K)$. Clearly, the restric-

tion of ϕ_r to E is ϕ. In terms of a diagram we have



We have found ϕ_i which make each of the above squares commute. □

Proposition 3.1.5. *Fix an algebraically closed field K. Assume that we are given a homomorphism of fields $\phi : E \to K$. Let $E \subset L$ be an algebraic extension. Then* $\mathrm{Hom}_\phi(L, K)$ *is non-empty.*

Proof. The main point in this case is that we can keep extending as in the preceding proposition and *finally we will have defined a map on all of L.* The following formal proof is a standard application of Zorn's Lemma.

1. Consider pairs (A, ϕ_A) where $E \subset A \subset L$ and $\phi_A : A \to K$ extends ϕ.

2. Put a partial order on such pairs as follows. $(A, \phi_A) \leqslant (T, \phi_T)$ if $A \subset T$ and $\phi_T|_A = \phi_A$. Let $\mathcal{P}$ denote this collection of pairs along with this partial order.

3. Let I be a totally ordered set and assume we are given a chain in $\mathcal{P}$ indexed by i. That is, we are given a collection (A_i, ϕ_{A_i}) for $i \in I$ such that if $i < j$ then $(A_i, \phi_{A_i}) \leqslant (A_j, \phi_{A_j})$. This chain has an upper bound, namely, $(\cup_i A_i, \phi)$. Here ϕ is defined as follows. If $a \in A_i$ then define $\phi(a) = \phi_{A_i}(a)$. If a was also in A_j, then we need to check that $\phi_{A_i}(a) = \phi_{A_j}(a)$. We have either $i < j$ or $j < i$. Assume that $i < j$. Then by the definition of the partial order, $A_i \subset A_j$ and $\phi_{A_j}|_{A_i} = \phi_{A_i}$. Thus, in this case both agree. The case $j < i$ is similar. Thus, we have proved that every chain in $\mathcal{P}$ has an upper bound in $\mathcal{P}$.

4. By Zorn's Lemma it follows that the collection $\mathcal{P}$ has a maximal element, that is, an element (A, ψ) such that if $(A, \psi) \leqslant (A', \psi')$ then $A = A'$ and $\psi = \psi'$. We claim that $A = L$. If not, then let $\alpha \in L \setminus A$. Then applying the preceding proposition we can extend ψ to an embedding of $A[\alpha]$, which contradicts the maximality of the pair (A, ψ).

□

Recall that we saw that given a field E, it has an algebraic closure. The way we saw this was to fix an inclusion $E \subset K$ into any algebraically closed field, and then taking $\bar{E}$ to be the set of elements of K which are algebraic over E. Now from this construction it may seem that given a field E, it may have two algebraic closures which are not isomorphic. We now prove that this is not the case.

Corollary 3.1.6. *Let $\bar{E}_1$ and $\bar{E}_2$ be two algebraic closures of E. Then they are isomorphic.*

Proof. Using Proposition 3.1.5 we can find a map $\psi : \bar{E}_1 \to \bar{E}_2$ such that

$$\begin{array}{ccc} \bar{E}_1 & \overset{\psi}{-\!\!-} & \bar{E}_2 \\ | & & \| \\ E & \text{——} & \bar{E}_2 \end{array}$$

The map ψ being a homomorphism of fields is an inclusion. It suffices to show that it is a surjection.

We first claim that $\psi(\bar{E}_1)$ is algebraically closed. Choose a polynomial $p(X) = \sum_{i=0}^{n} \psi(a_i) X^i \in \psi(\bar{E}_1)[X]$. Let $\alpha \in \bar{E}_1$ be a root of $\sum_{i=0}^{n} a_i X^i$. This means that $\psi(\alpha)$ is a root of $p(X)$. This shows that $\psi(\bar{E}_1)$ is algebraically closed.

Now we claim that ψ is a surjection. Since $\bar{E}_2$ is algebraic over E, it is algebraic over $\psi(\bar{E}_1)$. But as $\psi(\bar{E}_1)$ is algebraically closed, this forces that the irreducible polynomial of each $\beta \in \bar{E}_2$ over $\psi(\bar{E}_1)$ is of degree 1. That is, the irreducible polynomial is $X - \beta$. This shows $\beta \in \psi(\bar{E}_1)$. □

Let E, K be fields and suppose we are given a field homomorphism $\phi : E \to K$. Assume K is algebraically closed. Let $p(X) \in E[X]$ be a monic polynomial. Then we get a polynomial in $K[X]$ by applying ϕ to the

coefficients of $p(X)$. In other words, we can construct a ring homomorphism $\tilde{\phi} : E[X] \to K[X]$ which is ϕ on the coefficients E and maps X to X. It is easily checked that $\tilde{\phi}$ is a ring homomorphism. Since K is algebraically closed, the polynomial $\tilde{\phi}(p(X))$ factors into linear polynomials. Suppose we have another homomorphism into an algebraically closed field $\theta : E \to K'$, then similarly we get $\tilde{\theta}(p(X))$ and $\tilde{\theta}(p(X))$ factors into linear polynomials. Apriori, it is not clear if these factorizations have anything to do with each other. For instance, if $p(X)$ is of degree 6, can it happen that $\tilde{\phi}(p(X)) = (X - \alpha_1)^6$ and $\tilde{\theta}(p(X)) = (X - \beta_1)^2(X - \beta_2)^4$? As a consequence of the above Corollary let us see the following application.

Lemma 3.1.7. *If $\tilde{\phi}(p(X))$ has distinct roots $\alpha_1, \ldots, \alpha_n$ with multiplicity $a_1, \ldots, a_n$ then $\tilde{\theta}(p(X))$ has distinct roots $\beta_1, \ldots, \beta_n$ with multiplicity $a_1, \ldots, a_n$.*

Proof. Let $\bar{E}_1 \subset K$ denote the algebraic closure of E inside K and let $\bar{E}_2 \subset K'$ denote the algebraic closure of E inside K'. Note that the $\alpha_i \in \bar{E}_1$. Since $\tilde{\phi}(p(X)) = \prod_{i=1}^{n}(X - \alpha_i)^{a_i}$, note that $\tilde{\phi}(p(X)) \in \bar{E}_1[X]$ since it is a product of elements of $\bar{E}_1[X]$. Let $\psi : \bar{E}_1 \to \bar{E}_2$ be an isomorphism such that $\psi \circ \phi = \theta$. Such an isomorphism exists by Corollary 3.1.6. We get a ring isomorphism $\tilde{\psi} : \bar{E}_1[X] \to \bar{E}_2[X]$ such that $\tilde{\psi} \circ \tilde{\phi} = \tilde{\theta}$. Thus, it follows that

$$\begin{aligned}\tilde{\theta}(p(X)) &= \tilde{\psi} \circ \tilde{\phi}(p(X)) \\ &= \tilde{\psi}(\prod_{i=1}^{n}(X - \alpha_i)^{a_i}) \\ &= \prod_{i=1}^{n}(X - \psi(\alpha_i))^{a_i}\end{aligned}$$

Letting $\beta_i := \psi(\alpha_i)$ the Lemma is proved. □

3.2 Finiteness of embeddings

The next theorem is the main result of this chapter. We work with the same setup as above. Let $E \subset F \subset L$ be algebraic extensions of E. Fix an embedding $\phi : E \to K$. Then we have a restriction map

$$\text{Rest} : \text{Hom}_\phi(L, K) \to \text{Hom}_\phi(F, K) \tag{3.2.1}$$

given by

$$\psi \mapsto \psi|_F \,.$$

Fix an element $\psi_0 \in \mathrm{Hom}_\phi(F, K)$. It follows from Proposition 3.1.5 that the map Rest is surjective.

Proposition 3.2.2. *Fix an algebraically closed field K. Assume that we are given a homomorphism of fields $\phi : E \to K$. Let $E \subset L$ be a finite extension of E. Then $\#\mathrm{Hom}_\phi(L, K)$ is finite.*

Proof. Let us first assume that $L = E[\alpha]$ for some $\alpha \in L$. Let $p(X) \in E[X]$ denote the monic irreducible polynomial of α. Let

$$p(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0 \,.$$

An element of $\mathrm{Hom}_\phi(L, K)$ corresponds to a ring homomorphism $E[X] \to K$, which is ϕ on E and whose kernel is precisely $(p(X))$. If such a homomorphism sends $X \mapsto \beta$ then it is forced that β is a root of the polynomial

$$X^n + \psi_0(a_{n-1})X^{n-1} + \ldots + \psi_0(a_0) \,.$$

Thus, it follows that $\#\mathrm{Hom}_\phi(L, K)$ is finite as the number of roots of this polynomial is finite.

The general case can be proved by induction on the degree $[L : E]$. The base case for induction is $n = 1$. In this case $L = E$ and so

$$\#\mathrm{Hom}_\phi(L, K) = 1 \,.$$

Assume we have proved that whenever $[L : E] < n$ then $\#\mathrm{Hom}_\phi(L, K)$ is finite. Let $[L : E] = n$. Let $\alpha \in L \setminus E$ and assume we have

$$E \subsetneqq F = E[\alpha] \subsetneqq L$$

We have the restriction map

$$\mathrm{Hom}_\phi(L, K) \to \mathrm{Hom}_\phi(F, K) \,.$$

Since $[F : E] < n$ the set $\mathrm{Hom}_\phi(F, K)$ is finite. Let $\psi_0 \in \mathrm{Hom}_\phi(F, K)$. Then the fiber $\mathrm{Rest}^{-1}(\psi_0)$ is precisely $\mathrm{Hom}_{\psi_0}(L, K)$. Since $[L : F] < n$ the set $\mathrm{Hom}_{\psi_0}(L, K)$ is finite. Now if we have a map of sets $X \to Y$ such that Y is finite and the cardinality of each fiber is finite, then clearly the cardinality of X is finite. Thus, it follows that the set $\mathrm{Hom}_\phi(L, K)$ is finite. □

Theorem 3.2.3. *Fix an algebraically closed field K. Assume that we are given a homomorphism of fields $\phi : E \to K$. Let $E \subset F \subset L$ be finite extensions of E. Let $\psi_0 \in \mathrm{Hom}_\phi(F, K)$. Then the fibers of the map* Rest*, see equation* (3.2.1)*, are finite and have the same cardinality, each equal to* $\#\mathrm{Hom}_{\psi_0}(L, K)$.

Proof. Let $\psi_0, \psi_1 \in \mathrm{Hom}_\phi(F, K)$. We will construct a map

$$\mathrm{Rest}^{-1}(\psi_0) \to \mathrm{Rest}^{-1}(\psi_1)\,.$$

Let us denote by F_1 the algebraic closure of $\phi(E)$ inside K, that is,

$$F_1 := \{a \in K \,|\, a \text{ is algebraic over } \phi(E)\}$$

Since K is algebraically closed, it follows from Theorem 2.3.4 that F_1 is algebraically closed. Let $\beta \in L$ and let $p(X) \in E[X]$ be the irreducible polynomial of β. If $p(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_n$, then

$$0 = \phi(p(\beta)) = \phi(\beta)^n + \phi(a_{n-1})\phi(\beta)^{n-1} + \ldots + \phi(a_n)\,.$$

This proves that $\phi(\beta)$ is algebraic over $\phi(E)$, that is, $\phi(\beta) \in F_1$. Thus, the image of L under any extension of ϕ will actually land inside F_1. That is, the natural map (given a homomorphism to F_1, we obviously have a homomorphism to K)

$$\mathrm{Hom}_\phi(L, F_1) \xrightarrow{\sim} \mathrm{Hom}_\phi(L, K)\,,$$

is actually a bijection.

Consider the diagram

$$\begin{array}{ccc} F_1 & \overset{\theta}{\dashrightarrow} & F_1 \\ \big| & & \big\| \\ \psi_0(F) & \xrightarrow{\psi_1 \circ \psi_0^{-1}} & F_1 \end{array}$$

Since F_1 is an algebraic extension of $\psi_0(F)$, it follows from Proposition 3.1.5 that there is a θ which makes the above diagram commute. Since $\eta \in \mathrm{Rest}^{-1}(\psi_0)$, this means that $\eta \in \mathrm{Hom}_\phi(L, K)$ and the restriction of η to F is ψ_0. Consider the diagram

$$\begin{array}{ccccc} L & \xrightarrow{\eta} & F_1 & \overset{\theta}{\dashrightarrow} & F_1 \hookrightarrow K \\ \big| & & \big| & & \big\| \\ F & \xrightarrow{\psi_0} & \psi_0(F) & \xrightarrow{\psi_1 \circ \psi_0^{-1}} & K \end{array}$$

From the above diagram it is clear that $\theta \circ \eta$ restricted to F is ψ_1. Thus, the required map $\mathrm{Rest}^{-1}(\psi_0) \to \mathrm{Rest}^{-1}(\psi_1)$ is given by

$$\eta \mapsto \theta \circ \eta \,.$$

We claim that this map is an inclusion. This is because θ being a homomorphism of fields is an inclusion and so $\theta(\eta_1(x)) = \theta(\eta_2(x))$ implies that $\eta_1(x) = \eta_2(x)$. Interchanging the roles of ψ_0 and ψ_1 we get an inclusion the other way as well. This proves that

$$\#\mathrm{Rest}^{-1}(\psi_0) \leqslant \#\mathrm{Rest}^{-1}(\psi_1) \leqslant \#\mathrm{Rest}^{-1}(\psi_0)\,.$$

Thus, if we know that $\#\mathrm{Rest}^{-1}(\psi_0)$ is finite, then it will follow that both have the same cardinality. But the set $\mathrm{Rest}^{-1}(\psi_0) = \mathrm{Hom}_{\psi_0}(L, K)$ and this is finite because of the previous proposition. □

Corollary 3.2.4. *Let notation be as in Theorem 3.2.3. Then*

$$\#\mathrm{Hom}_{\phi}(L, K) = \#\mathrm{Hom}_{\psi_0}(L, K) \cdot \#\mathrm{Hom}_{\phi}(F, K)\,.$$

Let us show that this cardinality is independent of the algebraically closed field K and the map ϕ which is being chosen.

Lemma 3.2.5. *With notation as in Theorem 3.2.3, the cardinality of the set* $\mathrm{Hom}_{\phi}(L, K)$ *is independent of the algebraically closed field* K *and the map* ϕ*.*

Proof. Let $\phi : E \to K$ and F_1 be as in the proof of Theorem 3.2.3. Now let K' be another algebraically closed field and let $\psi : E \to K'$ be a homomorphism of fields. Let

$$F_2 := \{a \in K' \,|\, a \text{ is algebraic over } \psi(E)\}$$

As above, it follows that F_2 is algebraically closed and that

$$\mathrm{Hom}_{\phi}(L, F_2) \xrightarrow{\sim} \mathrm{Hom}_{\phi}(L, K')\,.$$

Thus, it suffices to show that the cardinality of the two sets $\mathrm{Hom}_{\phi}(L, F_1)$ and $\mathrm{Hom}_{\psi}(L, F_2)$ are the same. Consider the diagram

$$\begin{array}{ccc} F_2 & \xrightarrow{\theta} & F_1 \\ \big| & & \big| \\ \psi(E) & \xrightarrow{\phi\circ\psi^{-1}} & \phi(E) \end{array}$$

By Theorem 3.1.5 there is a map θ which makes the diagram commute. Now using the same proof as in Corollary 3.1.6 it follows that θ is an isomorphism. Consider the diagram

$$\begin{array}{ccccc} L & \xrightarrow{\eta} & F_2 & \overset{\theta}{\dashrightarrow} & F_1 \\ \downarrow & & \downarrow & & \downarrow \\ E & \xrightarrow{\psi} & \psi(E) & \xrightarrow{\phi\circ\psi^{-1}} & \phi(E) \end{array}$$

This diagram shows that the map which sends $\eta \mapsto \theta \circ \eta$ defines a map of sets

$$\mathrm{Hom}_{\psi}(L, F_2) \to \mathrm{Hom}_{\phi}(L, F_1)\,.$$

Applying the same argument we get the map induced by θ^{-1} from

$$\mathrm{Hom}_{\phi}(L, F_1) \to \mathrm{Hom}_{\psi}(L, F_2)\,.$$

Clearly these two maps are inverses of each other, as their composition is the identity. This proves that these sets have the same cardinality. □

Definition 3.2.6. *Let L be a finite extension of E. Let K be an algebraically closed field and let there be a map $\phi : E \to K$. Denote the cardinality of the set $\mathrm{Hom}_{\phi}(L, K)$ by $[L : E]_s$. We also call this the separable degree of L over E.*

With this definition we may restate Corollary 3.2.4 as

Proposition 3.2.7. *Let $E \subset F \subset L$ be finite extensions. Then*

$$[L : E]_s = [L : F]_s[F : E]_s\,.$$

3.3 Action of $\mathrm{Aut}(\bar{E}/E)$ on embeddings

Let us fix an embedding $i : E \subset \bar{E}$. Let $\mathrm{Aut}(\bar{E}/E)$ denote the set of field isomorphisms $\sigma : \bar{E} \to \bar{E}$ make the following diagram commute

$$\begin{array}{ccc} E & = & E \\ \downarrow{\scriptstyle i} & & \downarrow{\scriptstyle i} \\ \bar{E} & \xrightarrow{\sigma} & \bar{E} \end{array}$$

In other words, σ is the identity on E. Let $E \subset K \subset \bar{E}$ be a subfield. In this section we want to show that the group $\mathrm{Aut}(\bar{E}/E)$ acts on the set $\mathrm{Hom}_i(K, \bar{E})$ in a natural way and that this action is transitive. The action is defined as follows

$$\mathrm{Aut}(\bar{E}/E) \times \mathrm{Hom}_i(K, \bar{E}) \to \mathrm{Hom}_i(K, \bar{E}) \qquad (\sigma, \tau) \mapsto \sigma \circ \tau \,.$$

In terms of a diagram, we may express this as

$$\begin{array}{ccccc} K & \xrightarrow{\tau} & \bar{E} & \xrightarrow{\sigma} & \bar{E} \\ \uparrow & & \uparrow{\scriptstyle i} & & \uparrow{\scriptstyle i} \\ E & = & E & = & E \end{array}$$

Let $\tau_1, \tau_2 \in \mathrm{Hom}_i(K, \bar{E})$. To show this action is transitive, we need to find $\sigma \in \mathrm{Aut}(\bar{E}/E)$ such that $\sigma \circ \tau_1 = \tau_2$. Consider the following diagram (without the arrow σ)

$$\begin{array}{ccccc} & & \bar{E} & \overset{\sigma}{\dashrightarrow} & \bar{E} \\ & & \uparrow & & \uparrow \\ K & \xrightarrow{\tau_1} & \tau_1(K) & \xrightarrow{\tau_2 \circ \tau_1^{-1}} & \tau_2(K) \\ \uparrow & & \uparrow & & \uparrow \\ E & = & E & = & E \end{array}$$

Applying Proposition 3.1.5 we can find an arrow σ which makes the above diagram commute. Then it is clear that $\sigma \circ \tau_1 = \tau_2$.

Chapter 4

Separable Extensions

4.1 Criterion for separability using derivations

Define an E-linear map

$$D_E : E[X] \to E[X]$$

as follows. Define $D_E(1) = 0$, define $D_E(X^n) = nX^{n-1}$ for $n > 0$, and extend this map E-linearly. One easily checks that

1. $D_E(X^n X^m) = X^n D_E(X^m) + X^m D_E(X^n)$. Using this and linearity it follows that

   $$D_E(f(X)g(X)) = f(X)D_E(g(X)) + g(X)D_E(f(X)) \qquad \forall\, f, g \in E[X]\,.$$

2. If $E \subset F$, then $D_F|_{E[X]} = D_E$.

Lemma 4.1.1. *Let $p(X) \in E[X]$ be a non constant polynomial. If characteristic of E is zero then $D_E(p(X)) \neq 0$. If characteristic of E is $p > 0$ then there is a polynomial $p_1(X) \in E[X]$ such that $p(X) = p_1(X^p)$ iff $D_E(p(X)) = 0$.*

Proof. It is clear that if characteristic of E is zero then $D_E(p(X)) \neq 0$.

So let us assume that characteristic is $p > 0$. It is trivial to check that if $p(X) = p_1(X^p)$ then $D_E(p(X)) = 0$. So let us check the converse. Write

$$p(X) = X^n + \sum_{i=1}^{j} a_{t_i} X^{t_i}\,.$$

In the above, each $0 \leqslant t_i < n$ and each $a_{t_i} \neq 0$. Then

$$D_E(p(X)) = nX^{n-1} + \sum_{i=1}^{j} t_i a_{t_i} X^{t_i - 1} .$$

Since $D_E(p(X)) = 0$ it follows that the characteristic p divides n and each of the t_i. Thus, it follows that Then $p(X) = p_1(X^p)$, where

$$p_1(X) = X^{n/p} + \sum_{i=1}^{j} a_{t_i} X^{t_i/p} .$$

□

Proposition 4.1.2. *Let $p(X) \in E[X]$ denote a monic irreducible polynomial (obviously of degree $\geqslant 1$). Let K be an algebraically closed field and assume that $E \subset K$. Let α be a root of $p(X)$ in K. Then α is a repeated root iff $D_E(p(X)) = 0$.*

Proof. First let us assume that α is a repeated root of $p(X)$. It suffices to show that $D_E(p(X))$ has α as a root. Since $p(X)$ is the nonzero polynomial of least degree which has α as a root, and since $\deg(D_E(p(X))) < \deg(p(X))$, it will follow that $D_E(p(X)) = 0$. Since $D_E(p(X)) = D_K(p(X))$, it suffices to show that $D_K(p(X))$ has α as a root. Over K the polynomial $p(X)$ factors as

$$p(X) = \prod_{i=1}^{r} (X - \alpha_i)^{r_i} =: (X - \alpha_1)^{r_1} g(X) ,$$

where $g(X) \in K[X]$ is defined by the above equation. Assume that $\alpha = \alpha_1$, then by assumption $r_1 > 1$. Applying D_K we get

$$\begin{aligned} D_E(p(X)) = D_K(p(X)) &= D_K\Big((X - \alpha_1)^{r_1} g(X)\Big) \\ &= r_1 (X - \alpha_1)^{r_1 - 1} g(X) + (X - \alpha_1)^{r_1} D_K\Big(g(X)\Big) . \end{aligned}$$

Since $r_1 > 1$, it is clear that $(X - \alpha_1)$ divides the RHS. This shows that $\alpha = \alpha_1$ is a root of $D_E(p(X))$. This proves that $D_E(p(X)) = 0$.

Conversely, let us assume that $D_E(p(X)) = 0$. By Lemma 4.1.1 it follows that there is a polynomial $p_1(X) \in E[X]$ such that $p(X) = p_1(X^p)$. Let

$$p_1(X) = X^n + a_{n-1} X^{n-1} + \cdots + a_0 .$$

Let b_i be elements in K such that $b_i^p = a_i$. We can find such elements as we have assumed K to be algebraically closed. Then

$$p(X) = p_1(X^p) = (X^n + b_{n-1}X^{n-1} + \cdots + b_0)^p \in K[X]\,.$$

Then $p(X) = p_1(X)^p$. Thus, by looking at the roots of the RHS in K we see that every root of $p(X)$ is a repeated root. In particular, α is a repeated root. This proves the proposition. □

Definition 4.1.3. *Let $E \subset L$ be an algebraic extension. Let $\alpha \in L$ and let $p(X)$ denote the irreducible polynomial of α over E. Fix an algebraically closed field K such that $E \subset L \subset K$. We say that α is separable over E is α is not a repeated root of $p(X)$.*

Remark 4.1.4. In view of Proposition 4.1.2, the separability of α does not depend on the choice of the field K, since α is separable iff $D_E(p(X)) = 0$.

Definition 4.1.5. *An algebraic extension L is said to be separable over E if every element of L is separable over E.*

Corollary 4.1.6. *When characteristic is 0, all algebraic extensions are separable.*

Proof. The polynomial $D_E(p(X))$ can not be 0. □

Corollary 4.1.7. *Let $p(x) \in E[X]$ be an irreducible polynomial which has a repeated root in K. Then every root of $p(X)$ in K is a repeated root.*

Proof. Let α be a repeated root of $p(X)$. Then $D_E(p(X)) = 0$. From the Proposition 4.1.2 it follows that every root of $p(X)$ is a repeated root. □

4.2 Degree of separability

Lemma 4.2.1. *Let $L = E[\alpha]$ be a finite extension. Let $p(X)$ denote the monic irreducible polynomial of α over E. Then $[L : E]_s$ is equal to the number of distinct roots of $p(X)$.*

Proof. Let us fix an algebraically closed field K and an inclusion $E \subset K$ Giving a homomorphism from $L \to K$ is the same as giving a homomorphism from $E[X] \to K$ which is identity on E and 0 on $p(X)$. But such

homomorphisms are equivalent to sending X to a root of $p(X)$. Thus, the number of such homomorphisms is precisely the number of distinct roots of $p(X)$. □

Proposition 4.2.2. *Let char $k = 0$. Let L be a finite extension of E. Then $[L : E]_s = [L : E]$.*

Proof. Let us fix an algebraically closed field K and an inclusion $E \subset K$.

First consider the case where $L = E[\alpha]$. Let $p(X) \in E[X]$ be the monic irreducible polynomial of α. Since we are in char 0, it follows that all the roots of $p(X)$ are distinct.

The degree of the extension $[L : E] = \deg(p(X))$. By Lemma 4.2.1, the separable degree $[L : E]_s$ is equal to the number of distinct roots, that is, $\deg(p(X))$. This proves the assertion in the case where $L = E[\alpha]$.

The general case is proved by induction on $[L : E]$. The base case for the induction is when $[L : E] = 1$, in which case $L = E$ and there is nothing to prove. Let us assume that the assertion has been proved whenever $[L : E] < n$. Now let $[L : E] = n$ and choose $\alpha \in L \setminus E$. Assume that

$$E \subsetneqq F = E[\alpha] \subsetneqq L\,.$$

Then we have

$$[L : E] = [L : F][F : E]$$

and

$$[L : E]_s = [L : F]_s[F : E]_s\,.$$

By induction hypothesis, $[L : F]_s = [L : F]$ and $[F : E]_s = [F : E]$. Thus, $[L : E]_s = [L : E]$. This completes the proof. □

Proposition 4.2.3. *Let char $k = p > 0$. Let L be a finite extension of E. Then $[L : E]_s$ divides $[L : E]$.*

Proof. Let us fix an algebraically closed field K and an inclusion $E \subset K$.

First consider the case where $L = E[\alpha]$. Let $p(X) \in E[X]$ be the monic irreducible polynomial of α. Choose the largest possible $r \geqslant 0$ such that we can write $p(X) = f(X^{p^r})$.

The polynomial $f(Y)$ is clearly irreducible, or else, this will contradict the irreducibility of $p(X)$. The polynomial $f(Y)$ has no repeated roots. If this is not the case, then we get, using Proposition 4.1.2 that $D_E(f(Y)) = 0$, from which we can conclude, using Lemma 4.1.1, that $f(Y) = g(Y^p)$. But this would mean that $p(X) = g(X^{p^{r+1}})$, contradicting the maximality of r. This shows that $f(Y)$ has distinct roots. Denote these by $\beta_1, \ldots, \beta_l$. Let $\gamma_i \in K$ be such that $\gamma_i^{p^r} = \beta_i$. Then

$$f(Y) = (Y - \beta_1) \cdots (Y - \beta_l)\,.$$

This shows that

$$\begin{aligned} f(X^{p^r}) &= (X^{p^r} - \beta_1) \cdots (X^{p^r} - \beta_l) \\ &= (X - \gamma_1)^{p^r} \cdots (X - \gamma_l)^{p^r}\,. \end{aligned}$$

Thus, this shows that $\deg(p(X)) = p^r l$ and the number of distinct roots of $p(X)$ is equal to l. The degree of the extension $[L : E] = \deg(p(X)) = p^r l$. By Lemma 4.2.1, the separable degree $[L : E]_s$ is equal to the number of distinct roots, that is, l. This proves the assertion in the case where $L = E[\alpha]$.

The general case is proved by induction on $[L : E]$. The base case for the induction is when $[L : E] = 1$, in which case $L = E$ and there is nothing to prove. Let us assume that the assertion has been proved whenever $[L : E] < n$. Now let $[L : E] = n$ and choose $\alpha \in L \setminus E$. Assume that

$$E \subsetneqq F = E[\alpha] \subsetneqq L\,.$$

Then we have

$$[L : E] = [L : F][F : E]$$

and

$$[L : E]_s = [L : F]_s[F : E]_s\,.$$

By induction hypothesis, $[L : F]_s$ divides $[L : F]$ and $[F : E]_s$ divides $[F : E]$. Thus, $[L : E]_s$ divides $[L : E]$. This completes the proof. □

Definition 4.2.4. *Let char $k > 0$. Let L be a finite extension of E. Then the ratio $[L : E]_i = [L : E]/[L : E]_s$ is called the purely inseparable degree of L over E.*

Clearly, in view of the above results, we have

Proposition 4.2.5. *Let $E \subset F \subset L$ be finite extensions. Then*

$$[L : E]_i = [L : F]_i[F : E]_i\,.$$

4.3 Separable extensions and separable degree

Lemma 4.3.1. *Let $E \subset F \subset L$ be finite extensions. Let $\alpha \in L$ be an element which is separable over E. Then α is separable over F.*

Proof. Let $p_E(X)$ denote the monic irreducible polynomial of α over E and let $p_F(X)$ denote the monic irreducible polynomial over α over F. Clearly, the polynomial $p_E(X) \in F[X]$ since it has coefficients in E, which is a subset of F. Since $p_E(\alpha) = 0$, this shows that $p_F(X)$ divides $p_E(X)$. Since α is separable over E, $p_E(X)$ has no repeated roots. Thus, $p_F(X)$ also has no repeated roots. This shows that α is separable over F. □

Theorem 4.3.2. *Let L be a finite extension of E. Then L is separable over E iff $[L : E]_s = [L : E]$ (equivalently, iff $[L : E]_i = 1$).*

Proof. First assume that L is separable over E. Let $\alpha \in L$ and let $p(X)$ denote the monic irreducible polynomial of α. Then $[E[\alpha] : E] = \deg(p(X))$, and by Lemma 4.2.1, $[E[\alpha] : E]_s$ is equal to the number of distinct roots of $p(X)$. Since α is separable over E, it follows that both these are the same, that is, $[E[\alpha] : E]_s = [E[\alpha] : E]$. For a separable extension $E \subset L$. We will prove by induction on $[L : E]$ that $[L : E]_s = [L : E]$. The assertion is trivially true for $[L : E] = 1$. Assume that the assertion is true when $[L : E] < n$ and let $[L : E] < n$. Choose an $\alpha \in L$. If $L = E[\alpha]$ then we are done. Otherwise we have

$$E \subsetneqq E[\alpha] \subsetneqq L\,.$$

By the previous Lemma, L is separable over $E[\alpha]$. By induction hypothesis we have

$$[L : E[\alpha]]_s = [L : E[\alpha]]\,.$$

Thus,

$$[L : E]_s = [L : E[\alpha]]_s \cdot [E[\alpha] : E]_s = [L : E[\alpha]] \cdot [E[\alpha] : E] = [L : E]\,.$$

Now let us prove the converse. Assume that $[L : E]_s = [L : E]$. This is same as saying that $[L : E]_i = 1$. Let $\alpha \in L$. Then since $[L : E[\alpha]]_i \cdot [E[\alpha] : E]_i = [L : E]_i = 1$, it follows that $[E[\alpha] : E]_i = 1$, that is, $[E[\alpha] : E]_s = [E[\alpha] : E]$. Thus, if $p(X)$ is the monic irreducible polynomial of α over E, then this shows that the number of distinct roots is equal to the degree, that is, there

are no repeated roots. Thus, α is separable. This proves that L is separable over E. □

Proposition 4.3.3 (Primitive elements)**.** *Let E be an infinite field and let $E \subset L$ be a finite and separable extension. Then there is $\alpha \in L$ such that $L = E[\alpha]$.*

Proof. It suffices to prove this when $L = E[\alpha, \beta]$. Let $n = [L : E]$. Fix an embedding $E \subset \bar{E}$ into an algebraic closure. Since L is separable over E, we have $[L : E] = [L : E]_s = n$. Thus, there are n distinct extensions of the embedding to L. Denote these by $\phi_1, \phi_2, \ldots, \phi_n$. These are maps $\phi_i : L \to \bar{E}$.

Let $\alpha, \beta \in L \setminus E$. Now consider elements of the type $\alpha + \lambda\beta$, where $\lambda \in E$. Suppose $\phi_i(\alpha + \lambda\beta) = \phi_j(\alpha + \lambda\beta)$, then this means that

$$\lambda\big(\phi_i(\beta) - \phi_j(\beta)\big) = \phi_j(\alpha) - \phi_i(\alpha)\,. \tag{4.3.4}$$

For those pairs of i, j for which $\phi_i(\beta) - \phi_j(\beta) \neq 0$ consider the elements

$$S = \left\{ \frac{\phi_j(\alpha) - \phi_i(\alpha)}{\phi_i(\beta) - \phi_j(\beta)} \in \bar{E} \right\}.$$

Choose $\lambda_0 \in E$ such that λ_0 is different from the above. This is possible since the above collection is finite and E is infinite. We claim that the $\phi_i(\alpha + \lambda_0\beta)$ are distinct. If not then we get equation (4.3.4). If $\phi_i(\beta) - \phi_j(\beta) \neq 0$ then we get a contradiction since we chose $\lambda_0 \notin S$. Consider the case when $\phi_i(\beta) - \phi_j(\beta) = 0$. Equation (4.3.4) forces that $\phi_j(\alpha) - \phi_i(\alpha) = 0$. But this means that ϕ_i and ϕ_j agree on α and β. This in turn would mean that ϕ_i and ϕ_j agree on L, since $L = E[\alpha, \beta]$, but we chose the ϕ_i to be distinct. This gives a contradiction.

The above proves that $[E[\alpha + \lambda_0\beta] : E]_s = n$. Since every subfield of L is separable over E, this shows that

$$[E[\alpha + \lambda_0\beta] : E] = [E[\alpha + \lambda_0\beta] : E]_s = n\,.$$

Finally,

$$n = [L : E] = [L : E[\alpha + \lambda_0\beta]] \cdot [E[\alpha + \lambda_0\beta] : E] = [L : E[\alpha + \lambda_0\beta]] \cdot n,$$

shows that $[L : E[\alpha + \lambda_0\beta]] = 1$, that is, $L = E[\alpha + \lambda_0\beta]$. □

Proposition 4.3.5. *Let $E \subset K$ be an algebraic extension. Let $\alpha, \beta \in K$ be elements which are separable over E. Then $\alpha+\beta$ and α/β are separable over E.*

Proof. Since α is separable over E, it follows that $[E[\alpha] : E]_s = [E[\alpha] : E]$. Since β is separable over E, by Lemma 4.3.1 it follows that it is separable over $E[\alpha]$. Thus, $[E[\alpha, \beta] : E[\alpha]]_s = [E[\alpha, \beta] : E[\alpha]]$. Multiplying these we get that $[E[\alpha, \beta] : E]_s = [E[\alpha, \beta] : E]$. Using the above theorem we see that $E[\alpha, \beta]$ is separable over E. In particular, $\alpha + \beta$ and α/β are separable. □

In view of the above we have the following.

Theorem 4.3.6. *Let E be a field and let $\bar{E}$ be an algebraic closure. Let*

$$E^s := \{a \in \bar{E} \,|\, a \text{ is separable over } E\}.$$

Then E^s is a field.

4.4 Purely inseparable extensions

Throughout this section we will work with fields of characteristic $p > 0$.

Definition 4.4.1. *Let characteristic of E be $p > 0$. Let L be an algebraic extension such that for every element $\alpha \in L$ there is $r > 0$ such that $\alpha^{p^r} \in E$. Then we say that L is purely inseparable over E.*

Theorem 4.4.2. *Let L be a purely inseparable extension of E. Let $\alpha \in L \setminus E$ and let $s > 0$ be the smallest such that $\beta := \alpha^{p^s} \in E$. Then the irreducible polynomial of α over E is $X^{p^s} - \beta$.*

Proof. We know that there is $r > 0$ such that $\alpha^{p^r} \in E$. This means that α satisfies the polynomial $X^{p^r} - \alpha^{p^r} \in E[X]$. Let $p(X)$ be the irreducible polynomial of α over E. Then $p(X)$ divides $X^{p^r} - \alpha^{p^r}$. Fix an algebraic closure $E \subset L \subset \bar{E}$. Over $\bar{E}$, the polynomial $X^{p^r} - \alpha^{p^r}$ splits as $(X - \alpha)^{p^r}$, since we are in characteristic p. Since $p(X)$ divides this polynomial, it forces that $p(X) = (X - \alpha)^m$ for some $m > 0$.

Let $s > 0$ be the smallest integer such that $\alpha^{p^s} \in E$. Clearly, the polynomial $X^{p^s} - \alpha^{p^s} \in E[X]$. Thus, since $p(X)$ will divide this polynomial,

$m \leqslant p^s$. Let us assume that $m < p^s$ and write $m = lp^t$, where p does not divide l. Then

$$\begin{aligned} p(X) &= (X - \alpha)^{lp^t} \\ &= (X^{p^t} - \alpha^{p^t})^l \\ &= X^{lp^t} - l\alpha^{p^t} X^{p^t(l-1)} + \cdots \end{aligned}$$

This shows that $\alpha^{p^t} \in E$. But this is a contradiction since $t < s$. Thus, $m = p^s$. □

Corollary 4.4.3. *If L is purely inseparable over E then $[L : E]_s = 1$. That is, $[L : E] = [L : E]_i$.*

Proof. Let us fix an inclusion $E \subset L \subset \bar{E}$. We want to count the number of field homomorphisms $\phi : L \to \bar{E}$ which are identity when restricted to E. For any $\alpha \in L$, there is an r such that $\alpha^{p^r} \in E$. Thus, if ϕ is any such homomorphism, then $\phi(\alpha^{p^r}) = \alpha^{p^r}$. This forces that $\phi(\alpha)^{p^r} = \alpha^{p^r}$, which in turn forces that $\phi(\alpha) = \alpha$. This proves the corollary. □

Theorem 4.4.4. *Let L be a finite and purely inseparable extension of E. The degree $[L : E] = p^r$ for some $r \geqslant 0$.*

Proof. Let us first prove the following, from which the theorem will follow easily. Let $E \subset L_1 \subset L_2 \subset L$. Let $\alpha \in L_2$. The irreducible polynomial of α over L_1 is of the form $X^{p^t} - \beta$. First notice that L_2 is purely inseparable over L_1. Let s be the smallest such that $\alpha^{p^s} \in L_1$. Define $\beta := \alpha^{p^s}$. It now follows, using Theorem 4.4.2, that the irreducible polynomial of α over L_1 is $X^{p^s} - \beta$. Now the theorem follows easily. Simply take a tower

$$E \subset E[\alpha_1] \subset E[\alpha_1, \alpha_2] \subset \ldots \subset E[\alpha_1, \ldots, \alpha_n] = L$$

and apply Lemma 2.1.8. □

Let $E \subset L$ be an algebraic extension. In the preceding section we proved that the set

$$E_1 := \{a \in L \,|\, a \text{ is separable over } E\}$$

is a field. In this section we want to say something about the extension L over E_1.

Proposition 4.4.5. *The extension L is purely inseparable over E_1.*

Proof. Let $\alpha \in L \setminus E_1$. Let $f_0(X)$ denote the monic irreducible polynomial of α over E. Since α is not separable over E, it follows that $D_E(f_0(X)) = 0$. As we saw before, this shows that there is $f_1(X) \in E[X]$ such that

$$f_0(X) = f_1(X^p)\,.$$

Let $r > 0$ be largest so that

$$f_0(X) = f_1(X^p) = f_2(X^{p^2}) = \ldots = f_r(X^{p^r})\,.$$

We claim that $D_E(f_r(X)) \neq 0$, or else, $f_r(Y) = f_{r+1}(Y^p)$, which will show that $f_0(X) = f_{r+1}(X^{p^{r+1}})$, contradicting the maximality of r. Since

$$0 = f_0(\alpha) = f_r(\alpha^{p^r})\,,$$

it follows that α^{p^r} is a root of $f_r(X)$. Obviously, $f_r(X)$ is irreducible since $f_0(X)$ is irreducible. Since $D_E(f_r(X)) \neq 0$ it follows from proposition 4.1.2 that α^{p^r} is separable over E. This means that $\alpha^{p^r} \in E_1$. This proves the proposition. □

We conclude this section with summarizing the above results.

Theorem 4.4.6. *Let L be an algebraic extension of E. Then*

$$E_1 := \{a \in L \,|\, a \text{ is separable over } E\,\}$$

is a field and is a separable extension of E. The field L is purely inseparable over E_1. Further, if L is finite over E, then we have

(1) $[L : E_1]_s = 1$

(2) $[L : E_1] = [L : E_1]_i$

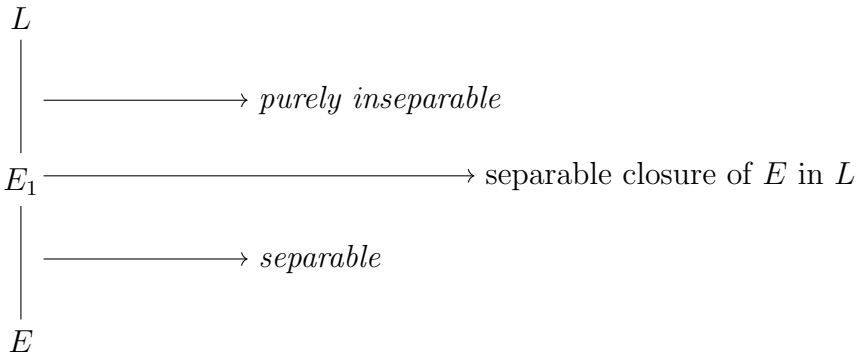
(3) $[E_1 : E] = [E_1 : E]_s$

(4) $[E_1 : E]_i = 1$

(5) $[L : E]_s = [E_1 : E]_s = [E_1 : E]$

(6) $[L : E]_i = [L : E_1]_i = [L : E_1]$

In terms of a diagram, the above says the following.



Chapter 5

Finite Fields

By $\mathbb{F}_p$ we shall denote the field $\mathbb{Z}/p\mathbb{Z}$. We fix, in this entire discussion, an algebraic closure of $\mathbb{F}_p$. Denote this field by $\bar{\mathbb{F}}_p$.

5.1 Existence and uniqueness

Given any integer $n > 1$, there are infinitely many extensions $\mathbb{Q} \subset K \subset \bar{\mathbb{Q}}$ such that $[K : \mathbb{Q}] = n$. For example, if we take $n = 2$, then for different primes p, the extensions $\mathbb{Q}[\sqrt{p}]$ are distinct. In contrast to this, we have the following theorem over finite fields.

We will need the following lemma.

Lemma 5.1.1. *Let $p(X) \in E[X]$ be a polynomial with root $\alpha \in \bar{E}$. Then α is a repeated root of $p(X)$ iff α is a root of $D_E(p(X))$.*

Proof. First let us assume that α is a repeated root of $p(X)$. Since $D_E(p(X)) = D_{\bar{E}}(p(X))$, it suffices to show that $D_{\bar{E}}(p(X))$ has α as a root. Over $\bar{E}$, the polynomial $p(X)$ factors as

$$p(X) = \prod_{i=1}^{r} (X - \alpha_i)^{r_i} .$$

Assume that $\alpha = \alpha_1$, then by assumption $r_1 > 1$. Applying $D_{\bar{E}}$ we get

$$D_E(p(X)) = D_{\bar{E}}(p(X)) = D_{\bar{E}}\Big(\prod_{i=1}^{r} (X - \alpha_i)^{r_i} \Big) .$$

Since $r_1 > 1$, it is clear that $(X - \alpha_1)$ divides the RHS. This shows that $\alpha = \alpha_1$ is a root of $D_E(p(X))$.

Conversely, let us assume that α is a root of $p(X)$ and $D_E(p(X))$. Since $D_E(p(X)) = D_{\bar{E}}(p(X))$, consider the factorization as above. If $r_1 = 1$, then when we evaluate $D_{\bar{E}}(p(X))$ at α, we will get

$$\prod_{i=2}^{r}(\alpha_1 - \alpha_i)^{r_i}\,.$$

This is nonzero and this is a contradiction to the assumption that α is a root of $D_E(p(X))$. □

Theorem 5.1.2. *Let $n \geqslant 1$ be an integer. Then there is a unique field K such that $\mathbb{F}_p \subset K \subset \bar{\mathbb{F}}_p$ and the degree $[K : \mathbb{F}_p] = n$.*

Proof. Let us first prove the existence of such a field. The idea is to show that the roots of the equation $X^{p^n} - X = 0$ in $\bar{\mathbb{F}}_p$ form a field. Let us first check that this equation has no repeated roots. First note that

$$D_{\mathbb{F}_p}(f(X)) = p^n X^{p^n - 1} - 1 = -1,$$

since $p^n \equiv 0$ in $\mathbb{F}_p$. By Lemma 5.1.1 it follows that all roots of this equation are distinct, since $D_{\mathbb{F}_p}(f(X))$ does not vanish for any root of $f(X)$. We could not have used Proposition 4.1.2 since we do not know if the polynomial $f(X)$ is irreducible (in fact, it is not, as we will see later).

Let K denote the set of roots of $f(X)$ in $\bar{\mathbb{F}}_p$. It follows that the cardinality of K is exactly p^n.

Claim: If $\alpha, \beta \in K$ then $\alpha + \beta$ is in K.
This simply follows from the binomial expansion since

$$\begin{aligned}(\alpha + \beta)^{p^n} &= ((\alpha + \beta)^p)^{p^{n-1}} \\ &= \Big(\sum_{i=0}^{p}\binom{p}{i}\alpha^i\beta^{p^n - i}\Big)^{p^{n-1}}\end{aligned}$$

(using that the binomial coefficients are divisible by p when $i \neq 0, p$)

$$\begin{aligned} &= (\alpha^p + \beta^p)^{p^{n-1}} \\ &= (\alpha^{p^2} + \beta^{p^2})^{p^{n-2}} \\ &= \dots \\ &= \alpha^{p^n} + \beta^{p^n} \end{aligned}$$

(using $\alpha, \beta \in K$)

$$= \alpha + \beta \,.$$

Thus, we have proved that $(\alpha + \beta)^{p^n} = \alpha + \beta$, which shows that $\alpha + \beta \in K$.

Claim: If $\alpha, \beta \in K$ then $\alpha\beta$ is in K.
This is clear since

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

Claim: If $\alpha \in K$ then $\alpha^{-1} \in K$
This is clear since

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

In view of the above three and the fact that 0,1 are in K, it follows that K is a field. It is clear that $\mathbb{F}_p \subset K$ since every element of $\mathbb{F}_p$ satisfies $\alpha^p = \alpha$. Thus,

$$\alpha = \alpha^p = \alpha^{p^2} = \cdots = \alpha^{p^n} \,.$$

Thus, $\mathbb{F}_p \subset K \subset \bar{\mathbb{F}}_p$ and this proves that there is at least one extension of degree n.

Let us next show that this is the unique extension of degree n. Let $\mathbb{F}_p \subset K' \subset \bar{\mathbb{F}}_p$ be another extension of degree n. Then K' has p^n elements. The set $K' \setminus \{0\}$ is a multiplicative group of order $p^n - 1$. Thus, if α is an element of $K' \setminus \{0\}$ then it satisfies $\alpha^{p^n - 1} = 1$. This shows that the elements of K' satisfy the equation $X^{p^n} - X = 0$. Thus, $K' \subset K$. Since both have the same cardinality, it follows that $K' = K$. This proves the uniqueness of the field extension of degree n. □

Corollary 5.1.3. *Every finite extension of $\mathbb{F}_p$ is separable.*

Proof. We saw above that every $\alpha \in K$ is a root of the polynomial $X^{p^n} - X$ and that this polynomial has distinct roots. Thus, the irreducible polynomial of α over $\mathbb{F}_p$, which divides this, also has distinct roots. Thus, α is separable over $\mathbb{F}_p$. □

5.2 Multiplicative group of a finite field

Theorem 5.2.1. *The group $K^\times \cong \mathbb{Z}/(p^n - 1)$.*

Proof. The structure theorem for finite abelian groups says that for every finite abelian group G of cardinality > 1, there is a positive integer r, and positive integers $1 < n_1 \leqslant n_2 \leqslant \ldots \leqslant n_r$ such that $n_i | n_{i+1}$ and G is isomorphic to $\mathbb{Z}/(n_1) \times \mathbb{Z}/(n_2) \times \cdots \times \mathbb{Z}/(n_r)$. Clearly every element satisfies $n_r g = 0$. Since $K^\times$ is a finite abelian group under multiplication, let us write

$$K^\times \cong \mathbb{Z}/(n_1) \times \mathbb{Z}/(n_2) \times \cdots \times \mathbb{Z}/(n_r)$$

Notice that the LHS is a multiplicative group and the RHS is an additive group. The RHS is an additive group in which every element g satisfies the equation $n_r g = 0$. This means that every element of $K^\times$ satisfies the equation $\alpha^{n_r} = 1$. The cardinality of $K^\times$ is $p^n - 1$. The cardinality of the RHS is $n_1 n_2 \ldots n_r$. If $r > 1$, then it follows that $n_r < n_1 n_2 \ldots n_r = p^n - 1$. This will mean that the equation $X^{n_r} - 1 = 0$ has more than n_r roots in the field $\overline{\mathbb{F}}_p$, which is a contradiction. Thus, the only possibility is $r = 1$ and $K^\times \cong \mathbb{Z}/(p^n - 1)$. □

As a corollary we see that there is an $\alpha \in K$ such that $K = \mathbb{F}_p[\alpha]$. In fact, we may take α to be the generator of the cyclic group $K^\times$. Then it is clear that every element of K can be written as a polynomial in α with coefficients in $\mathbb{F}_p$.

Theorem 5.2.2. *Let $E \subset K$ be a finite separable extension. Then there is an $\alpha \in K$ such that $K = E[\alpha]$.*

Proof. The case when E is an infinite field was proved in Proposition 4.3.3. Consider the case when E is a finite field. Then there is a p such that $\mathbb{F}_p \subset E \subset K$. Since K is a finite extension of E, it follows that K is also a finite field. It follows that $K^\times$ is a cyclic group. If α is a generator of this cyclic group then $K = E[\alpha]$. □

5.3 Frobenius

One of the questions that one considers when we talk about field extensions $E \subset L$ is what is the group of automorphims of L over E. The definition of $\mathrm{Aut}(L/E)$ is given by

$$\mathrm{Aut}(L/E) := \{\sigma : L \to L \mid \sigma \text{ is a field isomorphism, } \sigma|_E = Id_E\}$$

Theorem 5.3.1. *Let K denote the unique extension of $\mathbb{F}_p$ of degree n. Then there is an element $Fr \in \mathrm{Aut}(K/\mathbb{F}_p)$ which has order n.*

Proof. Denote by $Fr : K \to K$ the map $Fr(a) = a^p$. It is clear that

$$\begin{aligned} Fr(a+b) &= Fr(a) + Fr(b), \\ Fr(ab) &= Fr(a)Fr(b)\,. \end{aligned}$$

This shows that Fr is a field homomorphism. Since the kernel of a field homomorphism is 0, it follows that Fr is 1-1. If we view K as a vector space over $\mathbb{F}_p$, then we see that Fr is a map of $\mathbb{F}_p$ vector spaces, since for $a \in \mathbb{F}_p$ and $b \in K$ we have

$$Fr(ab) = a^p b^p = ab^p = aFr(b)\,.$$

Since Fr is an inclusion, this proves that the image of Fr is a vector space of dimension n. Thus, $\mathbb{F}_p \subset Fr(K) \subset K$ and both $Fr(K)$ and K are vector spaces over $\mathbb{F}_p$ of the same dimension. This shows that $Fr(K) = K$. Thus, Fr is a field automorphism.

Next we find the order of Fr. Since $Fr^n(a) = a^{p^n}$ and $a \in K$ we see that $Fr^n = Id_K$. Suppose that there is an integer $0 < m < n$ and $Fr^m = Id_K$. Then this would mean that all elements of K satisfy the equation $X^{p^m} = X$. However, this is not possible as that would mean that an equation of degree p^m has p^n roots. This shows that the order of the element Fr in $\mathrm{Aut}(K/\mathbb{F}_p)$ is exactly n. □

Theorem 5.3.2. *The group $\mathrm{Aut}(K/\mathbb{F}_p)$ is cyclic of order n and is generated by the Frobenius element.*

Proof. It suffices to show that the order of the group $\mathrm{Aut}(K/\mathbb{F}_p)$ is n. This will prove that

$$\mathrm{Aut}(K/\mathbb{F}_p) = \langle Fr \rangle\,,$$

since the order of the Frobenius is precisely n. Let $E \subset F$ be an algebraic extension. Fix an inclusion $i_E : E \to \bar{E}$ and a lift of this $i_F : F \to \bar{E}$. Now note the set $\mathrm{Aut}(F/E)$ can be made a subset of $\mathrm{Hom}_{i_E}(F, \bar{E})$ by sending $\phi \in \mathrm{Aut}(E/F)$ to $i_F \circ \phi$. This map is clearly an inclusion. Thus, if F is a finite extension of E, then we have that

$$\#\mathrm{Aut}(F/E) \leqslant [F : E]_s \leqslant [F : E] \,.$$

Applying this to the case $\mathbb{F}_p \subset K$ we see that

$$n \leqslant \#\mathrm{Aut}(K/\mathbb{F}_p) \leqslant [K : \mathbb{F}_p] = n \,.$$

This proves that the Frobenius generates the group of automorphisms. □

5.4 Galois correspondence for finite fields

Let us now see a glimpse of the main result of this course in the special case of finite fields. Above we proved that the group $\mathrm{Aut}(K/\mathbb{F}_p) = \mathbb{Z}/n\mathbb{Z}$ and is generated by the Frobenius automorphism. Let $H \subset \mathrm{Aut}(K/\mathbb{F}_p)$ be a subgroup. Define

$$K^H := \{a \in K \mid h(a) = a \,\text{for all}\, h \in H\} \,.$$

It is easily checked that K^H is a subfield of K. Consider the map

$$\Phi : \{\text{Subgroups of } \mathrm{Aut}(K/\mathbb{F}_p)\} \to \{\text{Subfields of } K \text{ containing } \mathbb{F}_p\}$$

given by

$$H \mapsto K^H \,.$$

We claim that the above map is a bijection between the two sets. To see this, note that for every integer $d|n$ we have

1. A unique subgroup of $\mathbb{Z}/n\mathbb{Z}$ which has cardinality d. In fact, this subgroup is generated by the element n/d.

2. A unique subfield $\mathbb{F}_p \subset K_d \subset K$ such that $[K : K_d] = d$. Let K_d be the unique extension of $\mathbb{F}_p$ of degree n/d. Then K_d contains the roots of

the equation $X^{p^{n/d}} - X = 0$. If $\alpha \in K_d$ then $\alpha^{p^{n/d}} = \alpha$. Raising both sides to the power $p^{n/d}$ we see that

$$(\alpha^{p^{n/d}})^{p^{n/d}} = \alpha^{p^{2n/d}} = \alpha^{p^{n/d}} = \alpha\,.$$

Repeating this d times we get $\alpha^{p^n} = \alpha$, that is, $\alpha \in K$. This proves that $K_d \subset K$.

The map Φ sends the subgroup $\langle Fr^{n/d} \rangle$ to the subfield $K^{\langle Fr^{n/d} \rangle}$. If γ is an element of $\mathrm{Aut}(K/\mathbb{F}_p)$, then it is trivial to check that $K^{\langle \gamma \rangle} = K^{\gamma}$. In particular, we have

$$K^{\langle Fr^{n/d} \rangle} = K^{Fr^{n/d}} = \{a \in K \mid Fr^{n/d}(a) = a\} = \{a \in K \mid a^{p^{n/d}} - a = 0\}\,.$$

This proves that $K^{Fr^{n/d}} = K_d$. In view of the above two points, we see that the map Φ is a bijection.

Chapter 6

Normal extensions

6.1 Normal extensions

Consider the extensions $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \bar{\mathbb{Q}} \subset \mathbb{C}$. Let us find the set of homomorphisms from $\mathbb{Q}[\sqrt{2}] \to \bar{\mathbb{Q}}$. Since $\mathbb{Q}[\sqrt{2}] \cong \mathbb{Q}[X]/(X^2-2)$, it follows that there are precisely two distinct homomorphisms from $\mathbb{Q}[X]/(X^2-2) \to \bar{\mathbb{Q}}$, namely, one which sends $X \mapsto \sqrt{2}$ and the other which sends $X \mapsto -\sqrt{2}$. Thus, there are precisely two homomorphisms $\mathbb{Q}[\sqrt{2}] \to \bar{\mathbb{Q}}$. One which sends $\sqrt{2} \mapsto \sqrt{2}$ and the other sends $\sqrt{2} \mapsto -\sqrt{2}$. However, note that the image of both the homomorphisms is the field $\mathbb{Q}[\sqrt{2}]$.

Let $\omega = e^{2\pi i/3} \in \mathbb{C}$. Consider the extensions $\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}] \subset \bar{\mathbb{Q}} \subset \mathbb{C}$. In the same way as above, we see that there are 3 possible homomorphisms from $\mathbb{Q}[\sqrt[3]{2}] \to \bar{\mathbb{Q}}$, these are given by $\sqrt[3]{2} \mapsto \sqrt[3]{2}$, $\sqrt[3]{2} \mapsto \omega\sqrt[3]{2}$ and $\sqrt[3]{2} \mapsto \omega^2\sqrt[3]{2}$. The image of $\mathbb{Q}[\sqrt[3]{2}]$ under the first of these, the one which $\sqrt[3]{2} \mapsto \sqrt[3]{2}$ is contained in $\mathbb{R}$. This is clearly not the case with the other two. For example, for the second one, the image of the homomorphism is $\mathbb{Q}[\omega\sqrt[3]{2}]$, which is clearly not a subset of $\mathbb{R}$, and so cannot be equal to $\mathbb{Q}[\sqrt[3]{2}]$.

Definition 6.1.1 (Normal extension)**.** *Let $E \subset L \subset \bar{E}$ be an algebraic extension. We say that L is normal if for every homomorphism $\phi : L \to \bar{E}$ such that $\phi|_E = Id$, the image $\phi(L) \subset L$.*

Thus, in the above examples, $\mathbb{Q}[\sqrt{2}]$ is a normal extension, whereas, $\mathbb{Q}[\sqrt[3]{2}]$ is not normal.

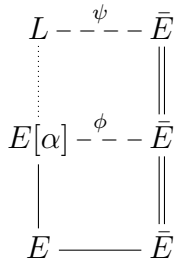
Theorem 6.1.2. *Let $E \subset L$ be an extension. Then the following are equiv-*

alent.

(1) L is a normal extension,

*(2) Let $f(X) \in E[X]$ be an **irreducible** polynomial. If $f(X)$ has one root in L, then all its roots are in L.*

Proof. First assume that L is a normal extension of E. Let $f(X) \in E[X]$ be an irreducible polynomial and let $\alpha \in L$ be a root of $f(X)$. Let $\beta \in \bar{E}$ be another root of $f(X)$. There is a unique field homomorphism $E[X]/(f(X)) \to \bar{E}$ which is the identity on E and which sends $X \mapsto \beta$. Since $E[\alpha] \cong E[X]/(f(X))$, we get a homomorphism $\phi : E[\alpha] \to \bar{E}$ which sends $\alpha \mapsto \beta$. Now we apply Proposition 3.1.5 and extend ϕ to all of L.



Since L is normal, it follows that $\psi(L) \subset L$. Thus, it follows that $\beta \in L$.

Now let us consider the converse of the above. Assume that L has the property that for every irreducible polynomial $f(X) \in E[X]$, if L contains one root of $f(X)$ then it contains all roots of $f(X)$. Let $\phi : L \to \bar{E}$ be a homomorphism. We need to show that if $\alpha \in L$ then $\phi(\alpha) \in L$. Let $f(X)$ be the irreducible polynomial of α over E. If $f(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0$, then we have that

$$a_n \alpha^n + a_{n-1} \alpha^{n-1} + \ldots + a_0 = 0 \,.$$

Applying ϕ to the above we get that

$$a_n \phi(\alpha)^n + a_{n-1} \phi(\alpha)^{n-1} + \ldots + a_0 = 0 \,.$$

This shows that $\phi(\alpha)$ is also a root of $f(X)$. Since L contains all roots of $f(X)$, it follows that $\phi(\alpha) \in L$. This proves that L is normal. □

Proposition 6.1.3. *Let $f(X) \in E[X]$ be a polynomial. Let $\alpha_1, \alpha_2, \ldots, \alpha_r$ denote its distinct roots in $\bar{E}$. Then the field $E[\alpha_1, \alpha_2, \ldots, \alpha_r]$ is a normal extension of E.*

Proof. Let $\phi : E[\alpha_1, \ldots, \alpha_r] \to \bar{E}$ be a field homomorphism. Let $\alpha = \alpha_i$. If $f(X) = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_0$, then we have that

$$a_n \alpha^n + a_{n-1} \alpha^{n-1} + \ldots + a_0 = 0 \,.$$

Applying ϕ to the above we get that

$$a_n \phi(\alpha)^n + a_{n-1} \phi(\alpha)^{n-1} + \ldots + a_0 = 0 \,.$$

This shows that $\phi(\alpha) = \alpha_j$, for some j. This shows that ϕ leaves the set $\{\alpha_1, \ldots, \alpha_r\}$ invariant. Since every element of $E[\alpha_1, \ldots, \alpha_r]$ can be written as a polynomial in the α_i with coefficients in E, this shows that the image of ϕ lands in $E[\alpha_1, \ldots, \alpha_r]$. This completes the proof of the Proposition. $\square$

Chapter 7

Galois correspondence

7.1 Galois extensions

Definition 7.1.1 (Galois extension)**.** *An extension $E \subset L \subset \bar{E}$ is called Galois if L is separable and normal over E.*

Proposition 7.1.2. *Let $E \subset L$ be a finite Galois extension. Then*

$$\#\mathrm{Aut}(L/E) = [L : E]\,.$$

Proof. Since L is normal, for every homomorphism $\phi : L \to \bar{E}$, the image $\phi(L) \subset L$. Since the vector space dimension of $\phi(L)$ and L over E are equal, it follows that they are equal. Thus, every such ϕ is in $\mathrm{Aut}(L/E)$. Since L is separable over E, we have $\#\mathrm{Hom}_E(L, \bar{E}) = [L : E]_s = [L : E]$. From this the proposition follows. □

Proposition 7.1.3. *Let $E \subset F \subset L$. If L is a finite Galois extension of E, then it is also a finite Galois extension of F. If L is Galois over E then* $\mathrm{Aut}(L/F) \subset \mathrm{Aut}(L/E)$.

Proof. Obvious and left as an exercise. □

Definition 7.1.4. *The group* $\mathrm{Aut}(L/E)$ *is often denoted* $\mathrm{Gal}(L/E)$*, in honour of Evariste Galois.*

https://en.wikipedia.org/wiki/%C3%89variste_Galois

The following lemma will be used in the proof of the next theorem.

Lemma 7.1.5. *Let $E \subset L$ be a separable extension, not necessarily finite. Assume that there is an $n \geqslant 1$ such that for every $\alpha \in L$, the degree $[E[\alpha] : E] \leqslant n$. Then the degree $[L : E] \leqslant n$.*

Proof. Let $\beta \in L$ be such that $[E[\beta] : E]$ is largest. There is such a β since we know that $[E[\alpha] : E] \leqslant n$ for all $\alpha \in L$. We claim that $L = E[\beta]$. If not, then there is β' such that $E[\beta] \subsetneqq E[\beta][\beta']$. By Theorem 5.2.2, there is a $\gamma \in E[\beta, \beta']$ such that $E[\beta, \beta'] = E[\gamma]$. This shows that $[E[\gamma] : E] > [E[\beta] : E]$. Since $\gamma \in L$, this contradicts the maximality of $[E[\beta] : E]$. Thus, $L = E[\beta]$ and $[L : E] \leqslant n$. □

Theorem 7.1.6. *Let K be a field and let $G \subset \mathrm{Aut}(K)$ be a finite subgroup of the group of field automorphisms of K. Then K^G is a field and K is a Galois extension of K^G of degree $\#G$. Moreover, the natural map $G \to \mathrm{Aut}(K/K^G)$ is an isomorphism.*

Proof. The check that K^G is a field is a trivial exercise which is left to the reader. Let us first show that K is a separable algebraic extension of K^G. Let $a \in K$ and let $H_a := \{g \in G \,|\, g(a) = a\}$. One easily checks that $H_a \subset G$ is a subgroup. Let $g_1, g_2, \ldots, g_l$ be coset representatives for G/H_a. Then $G = \bigsqcup_i g_i H_a$. Consider the polynomial

$$p(X) := \prod_i (X - g_i(a)) \in K[X]\,.$$

For $g \in G$, define an automorphism of $K[X]$ as follows. On the coefficients K, define the map to be g, and send X to X. Precisely,

$$a_n X^n + \ldots + a_0 \mapsto g(a_n)X^n + \ldots + g(a_0)\,.$$

Now it is clear that under this automorphism

$$g(p(X)) = \prod_i (X - gg_i(a)) = \prod_i (X - g_j h_i(a)) = \prod_i (X - g_j(a)) = p(X)\,.$$

This shows that the coefficients of $p(X)$ are in K^G. Let us now check that $p(X)$ has distinct roots. If not, then we will have $g_i^{-1}(g_j(a)) = a$, for some $i \neq j$, that is, $g_i^{-1} g_j \in H_a$. But this is a contradiction since the g_i were

representatives of distinct cosets. Taking the coset representative of the identity $e_G \in G$ to be e_G, we see that a is a root of $p(X)$. This shows that a is separable over K. This proves that K is an algebraic and separable extension of K^G.

Next let us show that K is a normal extension of K^G. Suppose

$$\phi : K \to \overline{K^G}$$

is a homomorphism into an algebraic closure, such that it is the identity on K^G. Let $a \in K$. Then, as we saw above, a is a root of the polynomial

$$p(X) = \prod_i (X - g_i(a)) \in K^G[X] \,.$$

Thus, $\phi(a)$ is also a root of this polynomial. But the roots of this polynomial are precisely $g_i(a)$ and all these are in K. This shows that $\phi(a) \in K$, that is, K is normal over K^G.

Applying the preceding lemma we see that $[K : K^G] \leqslant \#G$. Thus, K is a finite Galois extension of K^G. There are natural maps

$$G \to \mathrm{Aut}(K/K^G) \subset \mathrm{Aut}(K) \,.$$

Since the composite of the above is an inclusion by assumption, it follows that $G \to \mathrm{Aut}(K/K^G)$ is an inclusion. But from Proposition 7.1.2 we know that

$$\#G \leqslant \#\mathrm{Aut}(K/K^G) = [K : K^G] \leqslant \#G \,.$$

This proves that the natural map $G \to \mathrm{Aut}(K/K^G)$ is an isomorphism and that $[K : K^G] = \#G$. The proof of the theorem is now complete. □

7.2 Galois correspondence

Suppose we are given a finite Galois extension L/E. For a subgroup $H \subset \mathrm{Gal}(L/E)$ we shall denote by L^H the elements which are left fixed by all members of H, that is,

$$L^H := \{a \in L \,|\, h(a) = a \,\text{for all}\, h \in H\} \,.$$

Consider the following map

$$\Phi : \{\text{Subgroups of } \mathrm{Gal}(L/E)\} \to \{\text{Subfields of } L \text{ containing } E\}$$

given by

$$H \mapsto L^H .$$

Consider also the map in the other direction

$$\Psi : \{\text{Subfields of } L \text{ containing } E\} \to \{\text{Subgroups of } \mathrm{Gal}(L/E)\}$$

given by

$$F \mapsto \mathrm{Gal}(L/F) .$$

Definition 7.2.1 (Conjugates)**.** *Let E be a field and let $\alpha \in \bar{E}$. The roots of the irreducible polynomial of α over E are called the conjugates of α over E.*

The following is the main result of this course.

Theorem 7.2.2. *Let $E \subset L$ be a finite Galois extension.*

(1) Then $\Phi \circ \Psi = Id$ and $\Psi \circ \Phi = Id$. In particular, they are both bijections.

(2) Under this bijection normal subgroups correspond to normal extensions of E.

(3) Let $H \subset \mathrm{Gal}(L/E)$ be a normal subgroup and let $F = L^H$. By the previous part, F is a normal extension of E. The kernel of the natural (surjective) restriction map $\mathrm{Gal}(L/E) \to \mathrm{Gal}(F/E)$ is precisely H.

Proof. Let us first show that $\Psi \circ \Phi = Id$. This is equivalent to showing that for a subgroup $H \subset \mathrm{Gal}(L/E)$, we have $\mathrm{Gal}(L/L^H) = H$. But this is precisely the content of Theorem 7.1.6.

Next let us show that $\Phi \circ \Psi = Id$. Let $E \subset F \subset L$ be a subfield. We need to show that $L^{\mathrm{Gal}(L/F)} = F$. Suppose $g \in \mathrm{Gal}(L/F)$ then g fixes all elements of F. Thus, every element of F is left invariant by $\mathrm{Gal}(L/F)$. This shows that $F \subset L^{\mathrm{Gal}(L/F)}$. Let us assume that $F \subsetneqq L^{\mathrm{Gal}(L/F)}$. Let $\theta \in L^{\mathrm{Gal}(L/F)} \setminus F$. Since L is separable over E, it follows that L is separable over F, in particular, θ is separable over F. Thus,

$$1 < [F[\theta] : F] = [F[\theta] : F]_s .$$

Let $\theta = \theta_1, \theta_2, \ldots$ be conjugates of θ. Consider the field homomorphism from $\phi : F[\theta] \to \bar{E}$ which is identity on F and sends $\theta \mapsto \theta_2$. Extend ϕ to a field

homomorphism $\psi : L \to \bar{E}$. By normality of L, it follows that $\psi \in \mathrm{Gal}(L/F)$. However, $\psi(\theta) = \theta_2 \neq \theta_1$. This shows that $\theta \notin L^{\mathrm{Gal}(L/F)}$, which is a contradiction. This forces that $F = L^{\mathrm{Gal}(L/F)}$. Thus, (1) of the theorem is proved.

(2) Let us assume that $H \subset \mathrm{Gal}(L/E)$ is a normal subgroup. We need to show that L^H is a normal extension of E. Let $\phi : L^H \to \bar{E}$ and let $h \in H$. Extend ϕ to a map $\psi : L \to \bar{E}$. Then $\psi \in \mathrm{Gal}(L/E)$ since L is normal. Then $h(\psi(a)) = \psi(\psi^{-1}(h(\psi(a))))$. Since $\psi^{-1} \circ h \circ \psi \in H$ as H is normal, and since $a \in L^H$, it follows that $h(\psi(a)) = \psi(a)$. This shows that $\psi(a) = \phi(a) \in L^H$. This proves that L^H is a normal extension of E.

(3) Let $F := L^H$. Then we have the natural restriction map $\mathrm{Gal}(L/E) \to \mathrm{Gal}(F/E)$. This map is surjective because given any automorphism $\phi \in \mathrm{Gal}(F/E)$ we can first extend it to $\psi : L \to \bar{E}$. But then ψ is actually an element of $\mathrm{Gal}(L/E)$ since L is normal. The kernel of this map is precisely, those automorphisms of L which are identity on F, that is, $\mathrm{Gal}(L/F)$. By the Galois correspondence, this is H. Thus, we have an exact sequence of groups

$$1 \to H \to \mathrm{Gal}(L/E) \to \mathrm{Gal}(F/E) \to 1\,.$$

This completes the proof of the theorem. □

Proposition 7.2.3. *(1) If $H_1 \subset H_2 \subset \mathrm{Gal}(L/E)$ then $L^{H_2} \subset L^{H_1}$.*

(2) If $E \subset L_1 \subset L_2 \subset L$ then $\mathrm{Gal}(L/L_2) \subset \mathrm{Gal}(L/L_1)$.

(3) $L^{\mathrm{Gal}(L/E)} = E$.

Proof. All the above assertions are easy to prove and are left to the reader. □

7.3 Some examples

In this section we will work out a some examples of the Galois correspondence. Let $\omega = e^{2\pi i/3}$. Let $E = \mathbb{Q}[\sqrt[3]{5}, \omega]$. We will first show that $E/\mathbb{Q}$ is a Galois extension and then work out the Galois correspondence explicitly in this example.

7.3.1. Isomorphism class of the Galois group. Let $\sigma : E \to \bar{\mathbb{Q}}$ be a homomorphism. We need to show that $\sigma(E) \subset E$. It suffices to show that

$\sigma(\sqrt[3]{5}) \in E$ and $\sigma(\omega) \in E$. Note that $\sigma(\sqrt[3]{5})$ is forced to be $\sqrt[3]{5}$ or $\omega\sqrt[3]{5}$ or $\omega^2\sqrt[3]{5}$ and each of these is in E. Similarly, $\sigma(\omega)$ is forced to be ω or ω^2, again these are in E. This shows that $\sigma(E) \subset E$. Thus, E is a Galois extension of $\mathbb{Q}$.

Let us compute the degree of the extension $[E : \mathbb{Q}]$. We claim that the polynomial $X^2 + X + 1$ is irreducible over $\mathbb{Q}[\sqrt[3]{5}]$. This being a degree 2 polynomial, if it factors, then its roots lie in $\mathbb{Q}[\sqrt[3]{5}]$. The roots are ω and ω^2 and these are not in $\mathbb{R}$. Thus, they cannot be in $\mathbb{Q}[\sqrt[3]{5}] \subset \mathbb{R}$. This shows that $[\mathbb{Q}[\sqrt[3]{5}, \omega] : \mathbb{Q}[\sqrt[3]{5}]] = 2$. Since $[\mathbb{Q}[\sqrt[3]{5}] : \mathbb{Q}] = 3$, we get that $[\mathbb{Q}[\sqrt[3]{5}, \omega] : \mathbb{Q}] = 6$.

Thus, the Galois group $\mathrm{Gal}(E/\mathbb{Q})$ is of cardinality 6. Now up to isomorphism there are only two groups of order 6. These are $\mathbb{Z}/6\mathbb{Z}$ and S_3. Thus, if we can show that the Galois group is not abelian, then we will get that the Galois group is isomorphic to S_3. Consider the tower of extensions

$$\begin{array}{c} \mathbb{Q}[\sqrt[3]{5}, \omega] = \mathbb{Q}[\sqrt[3]{5}][X]/(X^2 + X + 1) \\ \Big| \\ \mathbb{Q}[\sqrt[3]{5}] = \mathbb{Q}[X]/(X^3 - 5) \\ \Big| \\ \mathbb{Q} \end{array}$$

There are three embeddings of $\mathbb{Q}[\sqrt[3]{5}]$ into $\bar{\mathbb{Q}}$. These are given by

$$\sigma_i(\sqrt[3]{5}) = \omega^i\sqrt[3]{5} \qquad i = 0, 1, 2\,.$$

For each σ_i we have

$$\sigma_i(X^2 + X + 1) = X^2 + X + 1$$

since the coefficients are in $\mathbb{Q}$. Thus, each σ_i can be extended to an embedding of $\mathbb{Q}[\sqrt[3]{5}, \omega] \to \bar{\mathbb{Q}}$ be defining

$$\sigma_{ij}(\omega) = \omega^j \qquad j = 1, 2\,.$$

Thus, we have constructed all the six embeddings of $E \to \bar{\mathbb{Q}}$. Precisely these are given by

$$\sigma_{ij}(\sqrt[3]{5}) = \omega^i\sqrt[3]{5} \qquad \sigma_{ij}(\omega) = \omega^j\,.$$

Let us check that $\sigma_{02} \circ \sigma_{11} \neq \sigma_{11} \circ \sigma_{02}$ which will prove that the group is not abelian.

$$\begin{aligned}
\sigma_{02} \circ \sigma_{11}(\sqrt[3]{5}) &= \sigma_{02}(\omega \sqrt[3]{5}) \\
&= \sigma_{02}(\omega)\sigma_{02}(\sqrt[3]{5}) \\
&= \omega^2 \sqrt[3]{5} \\
\sigma_{11} \circ \sigma_{02}(\sqrt[3]{5}) &= \sigma_{11}(\sqrt[3]{5}) \\
&= \omega \sqrt[3]{5}\,.
\end{aligned}$$

This shows that $\sigma_{02} \circ \sigma_{11} \neq \sigma_{11} \circ \sigma_{02}$. This proves that the Galois group is forced to be S_3.

7.3.2. An explicit isomorphism. Let us number the elements

$$\theta_i = \omega^{i-1} \sqrt[3]{5} \qquad\qquad i = 1, 2, 3\,.$$

The Galois group permutes the elements of the set $\{\theta_1, \theta_2, \theta_3\}$, since they are roots of the equation $X^3 - 5 = 0$. This means that there is a group homomorphism

$$\Phi : \mathrm{Gal}(E/\mathbb{Q}) \to S_3\,.$$

We need to compute explicitly what this group homomorphism is. To do that we simply apply the elements of the Galois group on this set and describe them as permutations. One checks easily that $\sigma_{11}(\theta_i) = \theta_{i+1}$. This shows that

$$\Phi(\sigma_{11}) = (123)\,.$$

Next let us check what the element σ_{12} does.

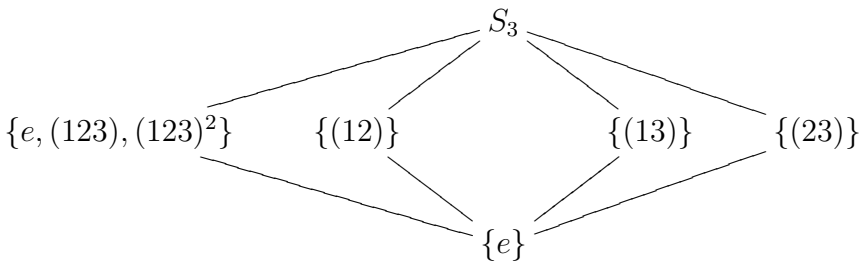
$$\begin{aligned}
\sigma_{12}(\sqrt[3]{5}) &= \omega \sqrt[3]{5} \\
\sigma_{12}^2(\sqrt[3]{5}) &= \sigma_{12}(\omega \sqrt[3]{5}) \\
&= \omega^2 \omega \sqrt[3]{5} \\
&= \sqrt[3]{5}\,.
\end{aligned}$$

Thus, $\sigma_{12}(\theta_1) = \theta_2$ and $\sigma_{12}(\theta_2) = \theta_1$. This computation shows that

$$\Phi(\sigma_{12}) = (12)\,.$$

Thus, the image of Φ contains both (123) and (12). Since these generate the group S_3, it follows that Φ is a surjection. Since both groups have the same size, which is 6, it follows that Φ is an isomorphism.

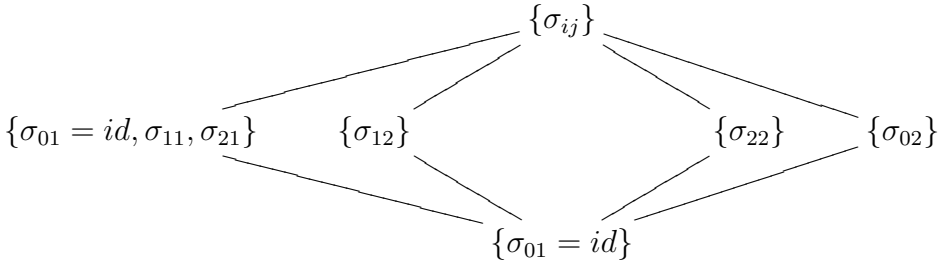
7.3.3. Galois correspondence The table of subgroups of S_3 is as follows.



Let us first apply the isomorphism Φ^{-1} to the above table and rewrite this table in terms of the σ_{ij}.

1. One checks that $\Phi(\sigma_{21}) = (132) = (123)^2$.
2. Similarly, $\Phi(\sigma_{02}) = (23)$.
3. The only element remaining is σ_{22} and this forces that $\Phi(\sigma_{22}) = (13)$.

Thus, applying Φ^{-1} to the above table we get the table.



Instead of computing the invariants explicitly, we will be more clever in writing down the table of subfields.

1. Notice that there is only one subgroup $H \subset \mathrm{Gal}(E/\mathbb{Q})$ of order 3. This means that there is only one subfield $\mathbb{Q} \subset F = E^H \subset E$ such that $[E : F] = \#H = 3$, that is, $[F : \mathbb{Q}] = 2$. But we know such a subfield, namely, $\mathbb{Q}[\omega]$.
2. Similarly, there are 3 subfield such that $[F : \mathbb{Q}] = 3$. We can write down 3 such subfields, namely, $\mathbb{Q}[\sqrt[3]{5}], \mathbb{Q}[\omega\sqrt[3]{5}], \mathbb{Q}[\omega^2\sqrt[3]{5}]$. But are these

distinct? Clearly, the first cannot be equal to the other two since the latter two contain elements which are not in $\mathbb{R}$. It is not possible that $\mathbb{Q}[\omega\sqrt[3]{5}] = \mathbb{Q}[\omega^2\sqrt[3]{5}]$ or else we will have that $\omega \in \mathbb{Q}[\omega\sqrt[3]{5}]$ which will mean that $\mathbb{Q}[\omega\sqrt[3]{5}] = \mathbb{Q}[\omega, \sqrt[3]{5}]$ which is not possible. It only remains to correctly associate the three subfields to the three subgroups of order 2.

3. Since $\Phi(\sigma_{02}) = (23)$, it follows that σ_{02} leaves θ_1 fixed, that is,

$$\sigma_{02}(\sqrt[3]{5}) = \sqrt[3]{5}\,.$$

This shows that $\mathbb{Q}[\sqrt[3]{5}] \subset E^{\langle\sigma_{02}\rangle}$ which implies that $\mathbb{Q}[\sqrt[3]{5}] = E^{\langle\sigma_{02}\rangle}$.

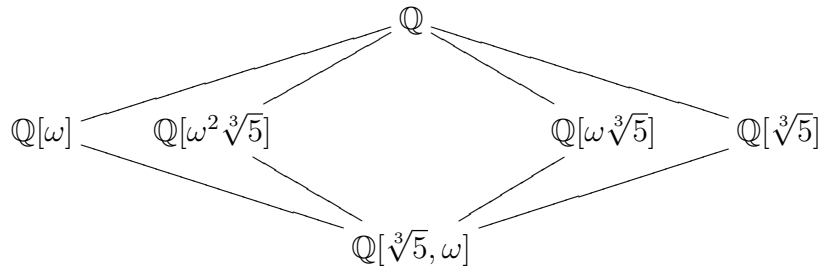
4. Since $\Phi(\sigma_{22}) = (13)$, it follows that σ_{22} leaves θ_2 fixed, that is,

$$\sigma_{22}(\omega\sqrt[3]{5}) = \omega\sqrt[3]{5}\,.$$

This shows that $\mathbb{Q}[\omega\sqrt[3]{5}] \subset E^{\langle\sigma_{22}\rangle}$ which implies that $\mathbb{Q}[\omega\sqrt[3]{5}] = E^{\langle\sigma_{22}\rangle}$.

5. Now it is forced that $\mathbb{Q}[\omega^2\sqrt[3]{5}] = E^{\langle\sigma_{12}\rangle}$.

Thus, it follows that the corresponding table of subfields is given by



7.3.4. Another example. Let us now compute $\mathrm{Gal}(\mathbb{Q}[\sqrt[4]{2}, i]/\mathbb{Q})$. That this is a Galois extension can be shown by arguing in the same manner as in the previous example. This is left to the reader. As before we will first compute the isomorphism class of the group.

We claim that the polynomial $X^2 + 1$ is irreducible over $\mathbb{Q}[\sqrt[4]{2}]$. This being a degree 2 polynomial, if it factors, then its roots lie in $\mathbb{Q}[\sqrt[4]{2}]$. The roots are $\pm i$ and these are not in $\mathbb{R}$. Thus, they cannot be in $\mathbb{Q}[\sqrt[4]{2}] \subset \mathbb{R}$.

Let $E := \mathbb{Q}[\sqrt[4]{2}, i]$. This shows that $[E : \mathbb{Q}] = 8$. We claim that $\mathrm{Gal}(E/\mathbb{Q})$ is not abelian. Consider the tower of extensions

$$\begin{array}{c} \mathbb{Q}[\sqrt[4]{2}, i] = \mathbb{Q}[\sqrt[4]{2}][X]/(X^2+1) \\ \Big| \\ \mathbb{Q}[\sqrt[4]{2}] = \mathbb{Q}[X]/(X^4-2) \\ \Big| \\ \mathbb{Q} \end{array}$$

There are four embeddings of $\mathbb{Q}[\sqrt[4]{2}]$ into $\bar{\mathbb{Q}}$. These are given by

$$\sigma_r(\sqrt[4]{2}) = \omega^r \sqrt[4]{2} \qquad r = 0, 1, 2, 3\,.$$

For each σ_r we have

$$\sigma_r(X^2 + X + 1) = X^2 + 1$$

since the coefficients are in $\mathbb{Q}$. Thus, each σ_r can be extended to an embedding of $\mathbb{Q}[\sqrt[4]{2}, i] \to \bar{\mathbb{Q}}$ be defining

$$\sigma_{rs}(i) = i^s \qquad s = 1, 3\,.$$

Thus, we have constructed all the eight embeddings of $E \to \bar{\mathbb{Q}}$. Precisely these are given by

$$\sigma_{rs}(\sqrt[4]{2}) = i^r \sqrt[4]{2} \qquad \sigma_{rs}(i) = i^s\,.$$

Let us check that $\sigma_{03} \circ \sigma_{11} \neq \sigma_{11} \circ \sigma_{03}$ which will prove that the group is not abelian.

$$\begin{aligned} \sigma_{03} \circ \sigma_{11}(\sqrt[4]{2}) &= \sigma_{03}(i\sqrt[4]{2}) \\ &= \sigma_{03}(i)\sigma_{03}(\sqrt[4]{2}) \\ &= i^3 \sqrt[4]{2} \\ \sigma_{11} \circ \sigma_{03}(\sqrt[4]{2}) &= \sigma_{11}(\sqrt[4]{2}) \\ &= i\sqrt[4]{2}\,. \end{aligned}$$

This shows that $\sigma_{03} \circ \sigma_{11} \neq \sigma_{11} \circ \sigma_{03}$. Thus, the Galois group is not abelian. Consider the restriction map

$$\phi : \mathrm{Gal}(E/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}[i]/\mathbb{Q})\,.$$

This map is surjective (why?) and the kernel contains σ_{r1} (why?). Notice that the kernel is forced to be of cardinality 4. Also notice that the cyclic subgroup generated by σ_{11} is of cardinality 4. This proves that the kernel is precisely $\{\sigma_{01}, \sigma_{11}, \sigma_{21}, \sigma_{31}\}$. Now consider the element σ_{03}. It is checked easily that $\sigma_{03}^2 = Id$. It is also clear that $\phi(\sigma_{03})$ is the generator of $\mathrm{Gal}(\mathbb{Q}[i]/\mathbb{Q})$.

Consider the following general statement from group theory. Let $\phi : G \to H$ be a ***surjective*** homomorphism of groups and let N be the ***kernel***. (This is often written as: Let

$$1 \to N \to G \xrightarrow{\phi} H \to 1$$

be a short exact sequence of groups.) Assume that there is a subgroup $M \subset G$ such that the restriction of ϕ to M is an isomorphism $M \xrightarrow{\sim} H$. Then every element of G can be written uniquely as nm where $n \in N$ and $m \in M$. In this case we say that G is the semi-direct product of N and M. The "semi" is because although G is a product of N and M as sets, but it may not be a product as groups. If further, elements of M and N commute with each other, then G is a direct product of M and N as groups.

Now we return to our example. Show that $\mathrm{Gal}(E/\mathbb{Q})$ is a semi direct product of $\langle\sigma_{03}\rangle$ (group of order 2) and $\langle\sigma_{11}\rangle$ (cyclic group of order 4). Suppose σ_{03} were to commute with σ_{11}, then it will also commute with all powers of σ_{11}, which would mean that $\mathrm{Gal}(E/\mathbb{Q})$ is the direct product of 2 cyclic groups, and so is abelian. But we know that $\mathrm{Gal}(E/\mathbb{Q})$ is not abelian. Thus, $\sigma_{03}\sigma_{11}\sigma_{03}^{-1} \neq \sigma_{11}$. This forces that (why?)

$$\sigma_{03}\sigma_{11}\sigma_{03}^{-1} = \sigma_{31}\,.$$

Thus, the group $\mathrm{Gal}(E/\mathbb{Q})$ is isomorphic to D_8. Here we have used the convention that D_{2n} is the unique group (up to isomorphism) of size $2n$ which has the following properties

1. A cyclic subgroup H_n of size n

2. A cyclic subgroup H_2 of size 2

3. If r is a generator of H_n and f is a generator of H_2 then $rf = fr^{-1}$.

7.4 $\mathbb{C}$ is algebraically closed

As an application of the above correspondence, let us show that $\mathbb{C}$ is algebraically closed. We need the following two easy observations, the proofs of which are left to the reader.

Lemma 7.4.1. *(1) Every odd degree polynomial in $\mathbb{R}[X]$ has a root.*

(2) Every $\alpha \in \mathbb{C}$ has a square root. In particular, this means that $\mathbb{C}$ has no extensions of degree 2.

Theorem 7.4.2. *$\mathbb{C}$ is algebraically closed.*

Proof. Let us first show that any finite extension of $\mathbb{R}$ has degree a power of 2. Let $\mathbb{R} \subset K \subset \bar{\mathbb{R}}$ be a finite extension. Since the characteristic is 0, we know that K is a separable finite extension, and so by Proposition 4.3.3 there is an element $\alpha \in K$ such that $K = \mathbb{R}[\alpha]$. Let $\alpha = \alpha_1, \alpha_2, \ldots, \alpha_d$ denote the conjugates of α. Then $E := \mathbb{R}[\alpha_1, \ldots, \alpha_d]$ is a normal extension of $\mathbb{R}$ by Proposition 6.1.3. Clearly, E is a finite Galois extension of $\mathbb{R}$. Let $G := \mathrm{Gal}(E/\mathbb{R})$ and write $\#G = 2^r m$ where m is odd. Let H be a 2-Sylow subgroup of G and consider the extensions

$$\mathbb{R} \subset E^H \subset E\,.$$

The degree of the extension $[E : E^H] = 2^r$ and so the degree $[E^H : \mathbb{R}] = m$. Now if we write $E^H = \mathbb{R}[\beta]$, then this shows that the irreducible polynomial of β over $\mathbb{R}$ has odd degree. Because of the first observation in the preceding Lemma, the only irreducible polynomials of odd degree are of degree 1. This forces that $\beta \in \mathbb{R}$ and $E^H = \mathbb{R}$. This proves the claim that every finite extension of $\mathbb{R}$ has degree a power of 2.

The following is an exercise in group theory. Let G be a group whose order is p^r. Then there is a filtration by normal subgroups

$$G_1 \subset G_2 \subset \ldots \subset G_r$$

such that each G_i has cardinality p^i. One may show this by first showing that a p-group has non-trivial center, then proceed by induction on the cardinality of G. In particular, this applies in our case. Consider the extension

$$\mathbb{R} \subset E^{G_{r-1}} \subset E^{G_{r-2}} \subset E\,.$$

The degree $[E : E^{G_{r-1}}] = \#G_{r-1} = 2^{r-1}$. This shows that $[E^{G_{r-1}} : \mathbb{R}] = 2$. If we write $E^{G_{r-1}} = \mathbb{R}[\beta]$ then we get that β satisfies an irreducible quadratic polynomial $X^2 + aX + b \in \mathbb{R}[X]$. Thus,

$$\mathbb{C} \cong \mathbb{R}[X]/(X^2 + aX + b) \cong E^{G_{r-1}}\,.$$

But now note that the degree of the extension $[E^{G_{r-2}} : E^{G_{r-1}}] = 2$. But this contradicts assertion (2) in the above Lemma, which says that $\mathbb{C}$ has no extensions of degree 2. From this we conclude that $\#G \leqslant 2$, that is, $[E : \mathbb{R}] \leqslant 2$. In particular, this also shows that $[K : \mathbb{R}] \leqslant 2$.

Assume that $\mathbb{C}$ is not algebraically closed. Then it has a finite extension K such that $[K : \mathbb{C}] \geqslant 2$. But then $[K : \mathbb{R}] \geqslant 4$, which contradicts the above. □

7.5 Infinite extensions

In this section we will show that the Galois correspondence, as stated above, is not true for infinite Galois extensions. Let $E \subset K$ be an algebraic extension. By $\mathrm{Gal}(K/E)$ we shall mean the group of automorphisms of K which are identity on E.

Consider the group homomorphism $\mathbb{Z} \to \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ which sends $1 \mapsto Fr$. We claim that this map is an inclusion. If not, then there is an $n > 0$ such that $Fr^n = Id$ on $\bar{\mathbb{F}}_p$. But this will mean that the elements of $\bar{\mathbb{F}}_p$ satisfy the equation $a^{p^n} = a$. This is not possible since we know that this equation has only finitely many roots and no finite field is algebraically closed. It is also clear that

$$\bar{\mathbb{F}}_p^{\langle Fr\rangle} = \mathbb{F}_p\,.$$

This is because if an element of $\bar{\mathbb{F}}_p$ is fixed by the Frobenius iff it satisfies the equation $a^p = a$, that is, $a \in \mathbb{F}_p$. Thus, if we can prove that there is a proper inclusion

$$\langle Fr\rangle \subsetneqq \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)\,,$$

then this will clearly violate the Galois correspondence as we will have

$$\mathbb{F}_p \subset \bar{\mathbb{F}}_p^{\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)} \subset \bar{\mathbb{F}}_p^{\langle Fr\rangle} = \mathbb{F}_p\,.$$

This will mean that the invariants under two distinct subgroups are the same.

Let $r_n := 2^n$. Consider the tower of extensions

$$\mathbb{F}_p \subset \mathbb{F}_{p^{r_1}} \subset \mathbb{F}_{p^{r_2}} \ldots \subset \mathbb{F}_{p^{r_n}} \subset \ldots$$

Let

$$E := \Big(\bigcup_{i=1}^{\infty} \mathbb{F}_{p^{r_n}} \Big) \subset \bar{\mathbb{F}}_p \,.$$

If $\sigma : E \to \bar{\mathbb{F}}_p$ is an embedding, then the image of σ is

$$\sigma(E) = \sigma\Big(\bigcup_{i=1}^{\infty} \mathbb{F}_{p^{r_n}} \Big) = \Big(\bigcup_{i=1}^{\infty} \sigma(\mathbb{F}_{p^{r_n}}) \Big) = \sigma\Big(\bigcup_{i=1}^{\infty} \mathbb{F}_{p^{r_n}} \Big) = E \,.$$

Thus, E is normal. (In fact, writing any extension of $\mathbb{F}_p$ as a union of finite extensions, the same proof shows that every extension of $\mathbb{F}_p$ is a normal extension.)

The group $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ is generated by the Frobenius iff the homomorphism $\mathbb{Z} \to \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ is surjective. Let us assume that this map is surjective. The map $\mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p) \to \mathrm{Gal}(E/\mathbb{F}_p)$ is surjective. Thus, the map $\mathbb{Z} \to \mathrm{Gal}(E/\mathbb{F}_p)$ will be surjective. We will now obtain a contradiction to this.

We have the following commutative diagram when $m|n$ are integers

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \xrightarrow{\sim} & \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \\ \downarrow & & \downarrow \\ \mathbb{Z}/m\mathbb{Z} & \xrightarrow{\sim} & \mathrm{Gal}(\mathbb{F}_{p^m}/\mathbb{F}_p) \end{array}$$

We know that $\mathrm{Gal}(\mathbb{F}_{p^{r_n}}/\mathbb{F}_p)$ is cyclic of order r_n and generated by the Frobenius. In particular, we have commutative diagrams:

$$\begin{array}{ccc} \mathbb{Z}/2^n\mathbb{Z} & \xrightarrow{\sim} & \mathrm{Gal}(\mathbb{F}_{p^{r_n}}/\mathbb{F}_p) \\ \downarrow & & \downarrow \\ \mathbb{Z}/2^{n-1}\mathbb{Z} & \xrightarrow{\sim} & \mathrm{Gal}(\mathbb{F}_{p^{r_{n-1}}}/\mathbb{F}_p) \end{array}$$

If we have an automorphism $\sigma : E \to E$ then we get automorphisms $\sigma_n : \mathbb{F}_{p^{r_n}} \to \mathbb{F}_{p^{r_n}}$ such that $\sigma_{n+1}|_{\mathbb{F}_{p^{r_n}}} = \sigma_n$. Conversely, suppose we have a family of such automorphisms σ_n, then it is easily checked that these will define

an automorphism of E, since we can define σ on $\mathbb{F}_{p^{r_n}}$ by σ_n. The condition $\sigma_{n+1}|_{\mathbb{F}_{p^{r_n}}} = \sigma_n$ ensures that this is well defined. Thus, using the isomorphism of Galois groups above, we see that elements of $\mathrm{Gal}(E/\mathbb{F}_p)$ are in bijection with elements

$$S := \{(a_1, a_2, \ldots) \in \prod_{n \geqslant 1} \mathbb{Z}/2^n\mathbb{Z} \,|\, a_{n+1} = a_n \bmod 2^n\}\,.$$

The Frobenius automorphism corresponds to the element $(1, 1, 1, \ldots)$. The subgroup generated by this consists of elements $(n, n, n, \ldots)$, for some $n \in \mathbb{Z}$. Consider the following element

$$\begin{aligned} a_{2k} &= 1 + 2^2 + 2^4 + \ldots + 2^{2k-2} \\ a_{2k+1} &= 1 + 2^2 + 2^4 + \ldots + 2^{2k} \end{aligned}$$

It is easily checked that this sequence defines an element in S. We claim that there is no $n \in \mathbb{Z}$ such that this is equal to $(n, n, n, \ldots)$. Suppose there is $n > 0$ such that $(a_1, a_2, a_3, \ldots) = (n, n, n, \ldots)$. Choose k very large so that $n < 2^{2k-2}$. Then we get

$$a_{2k} = 1 + 2^2 + 2^4 + \ldots + 2^{2k-2} = n \qquad \bmod 2^{2k}\,.$$

Viewing a_{2k} as an integer, it is easily seen that $n < a_{2k} < 2^{2k}$. Thus, such an equality is not possible. Next assume that there is a positive $n > 0$ such that $(a_1, a_2, a_3, \ldots) = (-n, -n, -n, \ldots)$. Choose k very large so that $n < 2^{2k-2}$. Then we get that

$$a_{2k} = 1 + 2^2 + 2^4 + \ldots + 2^{2k-2} = 2^{2k} - n \qquad \bmod 2^{2k}\,.$$

This gives that

$$n = 2^{2k} - (1 + 2^2 + 2^4 + \ldots + 2^{2k-2}) \qquad \bmod 2^{2k}\,.$$

That is,

$$n = \frac{2^{2k+1} + 1}{3} = b_{2k} \qquad \bmod 2^{2k}\,.$$

Again, if we view b_{2k} as an integer, then it is easily checked that $b_{2k} < 2^{2k}$. So for k very large we will have $n < b_{2k} < 2^{2k}$. But then an equality as above is not possible. This proves that $\mathbb{Z} \to \mathrm{Gal}(E/\mathbb{F}_p)$ is not surjective. Thus, $\mathbb{Z} \to \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)$ is not surjective. Thus,

$$\langle Fr \rangle \subsetneqq \mathrm{Gal}(\bar{\mathbb{F}}_p/\mathbb{F}_p)\,.$$

This shows that the Galois correspondence between subgroups and subfields breaks down for infinite extensions. However, one can define a topology on the group $\mathrm{Gal}(K/E)$. Then there is a correspondence between the closed subgroups of $\mathrm{Gal}(K/E)$ and the subfields of K. We will not prove this in this course.

Chapter 8

Groups occurring as Galois groups

In this chapter we will see examples of groups which can occur as Galois groups. In fact, the inverse Galois problem asks if every finite group can occur as the Galois group of an extension of $\mathbb{Q}$. This is an unsolved problem.

8.1 Finite groups as Galois groups

Let G be a finite group of cardinality n. Then there is an inclusion $G \to S_n$ which is defined as follows. First choose an ordering on the elements of G. For any $g \in G$, left multiplication by g, denoted m_g defines a permutation of G. This homomorphism is an inclusion since if m_g acts as the identity on G, then $g = m_g(e) = e$.

Proposition 8.1.1. *Let G be any finite group. Then there is a field extension $E \subset K$ such that* $\mathrm{Gal}(K/E) = G$.

Proof. First we embed $G \subset S_n$ as described above. Now let

$$K = \mathbb{Q}(X_1, X_2, \ldots, X_n)$$

and let S_n act on K be permuting the variables. This defines a homomorphism $S_n \to \mathrm{Aut}(K)$. Obviously the kernel of this homomorphism is trivial since only the identity element gives rise to the trivial automorphism. Thus, this makes $G \subset S_n \subset \mathrm{Aut}(K)$ a subgroup of $\mathrm{Aut}(K)$. Now we apply Theorem 7.1.6. □

8.2 S_4 as Galois group over $\mathbb{Q}$

In the previous section we saw that given any group G, we can find a field E (which depends on G) and a Galois extension K such that $\mathrm{Gal}(K/E) = G$. In the next few sections we shall see examples of groups which can be obtained as Galois groups over $\mathbb{Q}$.

In the previous chapter we saw that $\mathrm{Gal}(\mathbb{Q}[\sqrt[3]{5}, e^{2\pi i/3}]/\mathbb{Q}) \cong S_3$. In the proof we used the following Lemma.

Lemma 8.2.1. *Let K/E be a Galois extension. Let $p(X) \in E[X]$ be a polynomial of degree n whose roots are in K. There is an action of the Galois group on the roots of $p(X)$, which defines a homomorphism*

$$\rho : \mathrm{Gal}(K/E) \to S_n \,.$$

If K is generated over E by the roots of $p(X)$ then this homomorphism is also injective.

Proof. An element of the Galois group permutes the roots of $p(X)$. This permutation defines a group homomorphism. If K is generated over E by these roots, it follows that if $\sigma \in \mathrm{Gal}(K/E)$ fixes the roots, then it fixes every element of K. Thus, the homomorphism is injective. □

Inside the symmetric group we have the subgroup $A_n \subset S_n$ consisting of the even permutations. Equivalently, this is the kernel of the sign homomorphism

$$\mathrm{sgn} : S_n \to \{\pm 1\} \,.$$

It is a natural question to ask when the image of the homomorphism in Lemma 8.2.1 lands in A_n. This can be seen using the discriminant of the polynomial.

Definition 8.2.2. *Let $\alpha_1, \ldots, \alpha_n$ in K denote the roots of $p(X)$. The discriminant of $p(X)$ is defined as*

$$\Delta(p(X)) := \prod_{i<j} (\alpha_i - \alpha_j)^2 \,.$$

Lemma 8.2.3. $\Delta(p(X)) \in E$.

Proof. It suffices to show that $\Delta(p(X))$ is fixed by all elements in $\mathrm{Gal}(K/E)$. Let $\sigma \in \mathrm{Gal}(K/E)$. Then

$$\begin{aligned}
\sigma(\Delta(p(X))) &= \prod_{i<j}(\alpha_{\rho(\sigma)(i)} - \alpha_{\rho(\sigma)(j)})^2 \\
&= \Big(\prod_{i<j}(\alpha_{\rho(\sigma)(i)} - \alpha_{\rho(\sigma)(j)})\Big)^2 \\
&= \Big(\mathrm{sgn}(\rho(\sigma))\prod_{i<j}(\alpha_i - \alpha_j)\Big)^2 \\
&= \prod_{i<j}(\alpha_i - \alpha_j)^2 \\
&= \Delta(p(X))\,.
\end{aligned}$$

This proves the Lemma. □

Proposition 8.2.4. *The image of ρ is contained in A_n iff $\Delta(p(X))$ is a square in E.*

Proof. Let $\alpha := \prod_{i<j}(\alpha_i - \alpha_j)$. Then $\Delta(p(X)) = \alpha^2$.

Assume that the image of ρ is contained in A_n. It follows that

$$\sigma(\alpha) = \mathrm{sgn}(\rho(\sigma))\alpha = \alpha\,.$$

Thus, $\alpha \in E$. Thus, the discriminant, which is α^2, is a square in E.

Conversely, assume $\Delta(p(X))$ is a square in E. Then there is a $\beta \in E$ such that $\Delta(p(X)) = \beta^2$. On the other hand, since $\Delta(p(X)) = \alpha^2$, it follows that $\alpha = \pm\beta$, that is, $\alpha \in E$. It follows that for all $\sigma \in \mathrm{Gal}(K/E)$ we have $\sigma(\alpha) = \alpha$, that is, $\mathrm{sgn}(\rho(\sigma)) = 1$. Thus, the image of ρ is in A_n. □

Remark 8.2.5. Recall the Fundamental Theorem of Symmetric Polynomials. Let A be a commutative ring and let $R := A[X_1, \ldots, X_n]$ denote the polynomial ring in n variables. The group S_n acts on R by permuting the indeterminates $\{X_i\}$. Consider the ring $R[T]$. Define a polynomial $\theta_i \in R$ by setting $(-1)^i\theta_i$ to be the coefficient of T^{n-i} in $(T - X_1)\ldots(T - X_n)$. Each θ_i is invariant under the action of S_n. The Fundamental Theorem of Symmetric Polynomials says that the set of polynomials which are invariant under S_n are precisely those which are in the image of the ring homomorphism

$$A[Y_1, \ldots, Y_n] \to A[X_1, \ldots, X_n] \qquad\qquad Y_i \mapsto \theta_i\,.$$

Since the discriminant is invariant under S_n, it follows easily that it is a polynomial in the coefficients of $p(X)$. Let us mention two special cases which we shall use:

- If $p(X) = X^3 + aX + b$ then $\Delta(p(X)) = -4a^3 - 27b^2$,
- If $p(X) = X^4 + aX + b$ then $\Delta(p(X)) = -27a^4 + 256b^3$. □

Remark 8.2.6. Let $p(X) \in \mathbb{Q}[X]$ be a degree 4 polynomial with distinct roots $\alpha_1, \alpha_2, \alpha_3, \alpha_4$. Consider the following set

$$S := \{\alpha_1\alpha_2 + \alpha_3\alpha_4, \alpha_1\alpha_3 + \alpha_2\alpha_4, \alpha_1\alpha_4 + \alpha_2\alpha_3\}.$$

It is clear that any permutation of the α_i permutes the set S. Thus, the polynomial

$$r(X) := (X - (\alpha_1\alpha_2 + \alpha_3\alpha_4))(X - (\alpha_1\alpha_3 + \alpha_2\alpha_4))(X - (\alpha_1\alpha_4 + \alpha_2\alpha_3))$$

has coefficients which are invariant under $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ and so are in $\mathbb{Q}$. Moreover, one checks that

- $(\alpha_1\alpha_2 + \alpha_3\alpha_4) - (\alpha_1\alpha_3 + \alpha_2\alpha_4) = (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3)$
- $(\alpha_1\alpha_2 + \alpha_3\alpha_4) - (\alpha_1\alpha_4 + \alpha_2\alpha_3) = (\alpha_1 - \alpha_3)(\alpha_2 - \alpha_4)$
- $(\alpha_1\alpha_3 + \alpha_2\alpha_4) - (\alpha_1\alpha_4 + \alpha_2\alpha_3) = (\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4)$

The above equalities show that $\Delta(p(X)) = \Delta(r(X))$. The polynomial $r(X)$ is called the resolvent cubic of $p(X)$. The coefficients of $r(X)$ are symmetric polynomials in the α_i and so polynomials in the coefficients of $p(X)$. If $p(X) = X^4 + aX + b$ then $r(X) = X^3 - 4bX - a^2$.

Proposition 8.2.7. *Let K be the extension of $\mathbb{Q}$ obtained by adjoining all the roots of the polynomial $p(X) := X^4 - X - 1$. Then $\mathrm{Gal}(K/\mathbb{Q}) \cong S_4$.*

Proof. By the previous lemma, there is an injective group homomorphism $G := \mathrm{Gal}(K/\mathbb{Q}) \to S_4$. We will show that the cardinality of G is divisible by 12, the image of this homomorphism is not contained in A_4, and the only subgroup of S_4 of index 2 is A_4. From these it follows that the cardinality of G has to be 24, and so the embedding has to be an isomorphism.

To show that $p(X)$ is irreducible it suffices to show that it is irreducible after reducing mod 2. Let $\bar{p}(X)$ denote the reduction mod 2. We claim $\bar{p}$ does not have a root in $\mathbb{F}_2$. Note that $\mathbb{F}_2 \subset \mathbb{F}_4$ and every element of $\mathbb{F}_4$ is a root of the equation $X^4 - X = 0$. Thus, $\bar{p}$ evaluates to -1 for every element of $\mathbb{F}_4$ and so also every element of $\mathbb{F}_2$. This shows that $\bar{p}$ has no roots in $\mathbb{F}_2$. Thus, it cannot factor into a linear polynomial times a degree 3 polynomial. Suppose it factors as $\bar{p}(X) = h(X)g(X)$ where $h(X)$ and $g(X)$ have degree 2 and are irreducible. Since $h(X)$ has degree 2, it follows that if α is a root of $h(X)$ then $\alpha \in \mathbb{F}_4$. But this shows that $\bar{p}(X)$ has a root in $\mathbb{F}_4$, which we saw is not possible. This proves that $\bar{p}(X)$ is irreducible and so $p(X)$ is also irreducible.

Since $p(X)$ is irreducible, it follows that $4 \mid \#G$. Consider the resolvent cubic $r(X)$. The roots of $r(X)$ are contained in K. Let K_1 be the normal extension of $\mathbb{Q}$ obatined by adjoining the roots of $r(X)$ to $\mathbb{Q}$. Then $\mathbb{Q} \subset K_1 \subset K$ and so we have a surjective group homomorphism $G \to \mathrm{Gal}(K_1/\mathbb{Q})$. By Remark 8.2.6 the polynomial $r(X) = X^3 + 4X - 1$. It can be checked that when we go modulo 7, this polynomial has no roots, and so $r(X)$ is irreducible modulo 7, and so also in $\mathbb{Z}[X]$. Thus, 3 divides $[K_1 : \mathbb{Q}]$. This shows that $[K_1 : \mathbb{Q}] = 3$ or 6. Consider the homomorphism $\mathrm{Gal}(K_1/\mathbb{Q}) \to S_3$. In S_3 there is a unique subgroup of order 3, which is A_3. If $\mathrm{Gal}(K_1/\mathbb{Q})$ has cardinality 3, then the image is forced to be this unique subgroup. The discriminant of $r(X)$ is $-4.4^3 - 27$ which is not a square in $\mathbb{Q}$. Thus, the image is not contained in A_3, which shows that $\mathrm{Gal}(K_1/\mathbb{Q}) \cong S_3$ and so has cardinality 6. Since there is a surjective homomorphism $G \to \mathrm{Gal}(K_1/\mathbb{Q})$ it follows that $6 \mid \#G$. As $4 \mid \#G$, it follows that $12 \mid \#G$. Thus, $\#G = 12$ or 24.

Next we claim that S_4 has only one subgroup of order 12, which is A_4. Let H be a subgroup of S_4 of order 12. Then H is a normal subgroup and S_4/H is abelian, which shows that the commutator subgroup $[S_4, S_4] \subset H$. We claim that $A_4 \subset [S_4, S_4]$. For $\sigma \in S_4$ we have

$$\sigma(a,b)\sigma^{-1}(a,b) = (\sigma(a), \sigma(b))(a,b)\,.$$

Choose σ such that $\sigma(a) = a$ and $\sigma(b) = c$. Then

$$\sigma(a,b)\sigma^{-1}(a,b) = (a,c)(a,b) = (a,b,c)\,.$$

This shows that $A_4 \subset [S_4, S_4] \subset H$. Due to cardinality reasons we get that $A_4 = H$. This proves the uniqueness.

If $\#G = 12$ then the image of G would be contained in A_4. This would imply that the discriminant of $p(X)$ is a perfect square in $\mathbb{Q}$. But we already saw that $\Delta(p(X)) = \Delta(r(X)) = -4.4^3 - 27$, which is not a square. Thus, $\#G = 24$, which shows that $G \cong S_4$. This completes the proof of the Proposition. □

8.3 S_p as Galois group over $\mathbb{Q}$

Throughout this section $p > 0$ will be a prime. We will need the following Lemma about S_p.

Lemma 8.3.1. *(1) An element of S_p of order p is a p-cycle.*

(2) Let $\{3, \ldots, n\} = \{a_3, \ldots, a_n\}$. The elements $(1, 2)$ and $(1, 2, a_3, \ldots, a_n)$ generate the group S_n.

Proof. Left as exercises. For the second part use the fact that $(1, 2)$ and $(1, 2, \ldots, n)$ generate S_n. □

Theorem 8.3.2. *Let $f(X) \in \mathbb{Q}[X]$ be an irreducible polynomial of degree p. Assume that $f(X)$ has exactly $p - 2$ real roots and two roots in $\mathbb{C} \setminus \mathbb{R}$. Let K denote the field obtained by adjoining roots of $f(X)$ to $\mathbb{Q}$. Then $\mathrm{Gal}(K/\mathbb{Q}) \cong S_p$.*

Proof. Let G denote the Galois group $\mathrm{Gal}(K/\mathbb{Q})$. Then G embeds into S_p as the group permuting the roots of $f(X)$. Let H denote the image of G. Let α be a root of $f(X)$. Since $[\mathbb{Q}(\alpha) : \mathbb{Q}] = p$ divides $[K : \mathbb{Q}]$, it follows that p divides $\#G$. It follows that p divides $\#H$ and so H contains an element of order p. By Lemma 8.3.1 it follows that H contains a p-cycle, let us call it β.

Let $\alpha_1, \alpha_2, \ldots, \alpha_p$ denote the distinct roots of $f(X)$. Choose α_1 and α_2 to be the roots which are in $\mathbb{C} \setminus \mathbb{R}$. Then complex conjugation defines an automorphism of K over $\mathbb{Q}$ which fixes the roots $\alpha_3, \ldots, \alpha_p$. Thus, complex conjugation is represented by the permutation $(1, 2)$. We may write $\beta = (1, i_2, i_3, \ldots, i_p)$. There is an i with $0 < i < p$ such that $\beta^i = (1, 2, j_3, \ldots, j_p)$. Lemma 8.3.1 shows that $(1, 2)$ and β^i generate S_p. □

Thus, in order to show that S_p occurs as a Galois group over $\mathbb{Q}$, it suffices to construct a polynomial as in the preceding Theorem. We do this next. For later use we shall need the following Lemma.

Lemma 8.3.3. *Let p be a prime. Consider the polynomial $p(X) = X^p - X + \lambda$ for some $\lambda \neq 0$ in $\mathbb{F}_p[X]$. This polynomial is irreducible.*

Proof. Observe that if α is a root of this in $\bar{\mathbb{F}}_p$ then $\alpha + 1$ is also a solution. Using this repeatedly we see that the set of all roots is given by

$$\{\alpha, \alpha + 1, \ldots, \alpha + (p-1)\}.$$

Let $Fr(\alpha) = \alpha + i$ since $Fr(\alpha)$ is a root of $p(X)$. Assume this polynomial factors as $h(X)g(X)$ and let α be a root of $h(X)$. Then $Fr^j(\alpha)$ is a root of $h(X)$ for all j. Since p is prime, the set

$$\{Fr^j(\alpha)\} = \{\alpha, \alpha + 1, \ldots, \alpha + (p-1)\}.$$

This is a contradiction since $\deg(h(X)) < \deg(p(X))$. □

Lemma 8.3.4. *There exists a polynomial $f(X) \in \mathbb{Q}[X]$ of degree p which is irreducible and which has exactly $p-2$ roots in $\mathbb{R}$ and two roots in $\mathbb{C} \setminus \mathbb{R}$.*

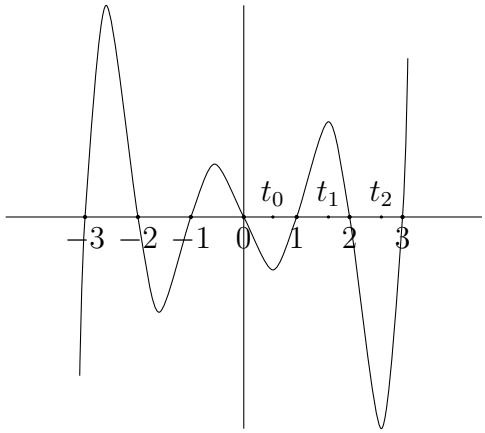
Proof. Let

$$f(X) := \lambda + \prod_{i=-\frac{p-1}{2}}^{\frac{p-1}{2}} (X - i) \qquad \lambda \in \mathbb{Q}.$$

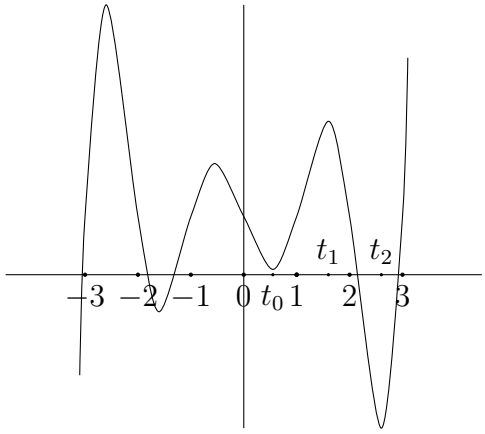
Let $\lambda = \frac{a}{b}$ where $a, b \in \mathbb{Z}$ and $p \nmid ab$. Irreducibility of $f(X)$ can be proved after going modulo p (after clearing denominators), whence it suffices to show,

$$X^p - X + \bar{\lambda}, \qquad \bar{\lambda} \neq 0$$

is irreducible. This is the content of the preceding Lemma. Thus, to apply Theorem 8.3.2, we only need to choose λ so that $f(T)$ has exactly $p-2$ real roots. The idea behind the proof is explained by taking a look at the graph of $f(X)$. When $p = 7$ the graph of $f(X)$ looks like:



The graph of $f(X) + \lambda$ looks like



Thus, $f(X)$ has two less real roots than $f(X)$. We now proceed with the detailed proof.

Consider the polynomial

$$g(X) := (X-n)(X-n+1)\dots(X-1)X(X+1)\dots(X+n)\,.$$
$$g(X+1) = \qquad (X-n+1)\dots(X-1)X(X+1)\dots(X+n)(X+1+n)$$

Thus,

$$(8.3.5)\quad g(X+1)+g(X) = (X-n+1)\dots(X-1)X(X+1)\dots(X+n)(2X+1)\,.$$

For every interval $(i, i+1)$, where $i \in \{0, 1, \dots, n-1\}$, the polynomial $g(X)$ attains local maxima or a local minima at a unique point $t_i \in (i, i+1)$. We

claim that

$$0 < |g(t_0)| < |g(t_1)| < \ldots < |g(t_{n-1})|\,. \tag{8.3.6}$$

Note that the signs of $g(t_i)$ and $g(t_{i+1})$ are different. Thus, in order to show that $|g(t_i)| < |g(t_{i+1})|$ it suffices to show that $g(t_i) + g(t_i + 1)$ is nonzero and has the same sign as $g(t_i + 1)$, which has the same sign as $g(t_{i+1})$. This will show that $|g(t_i)| < |g(t_i+1)|$, which shows that $|g(t_i)| < |g(t_i+1)| \leqslant |g(t_{i+1})|$.

The sign of $g(t_0)$ is $(-1)^n$. Thus, $g(t_i)$ has sign $(-1)^{i+n}$. Putting $X = t_i$ in (8.3.5) we get

$$g(t_i + 1) + g(t_i) = (t_i - n + 1)\ldots(t_i - 1)t_i(t_i + 1)\ldots(t_i + n)(2t_i + 1)\,.$$

The above is clearly nonzero since $t_i \in (i, i+1)$. The only terms in the above which are negative are $(t_i - i - 1), (t_i - i - 2), \ldots, (t_i - n + 1)$. Thus, the sign is $(-1)^{n-i-1} = (-1)^{i+n+1}$, which is the sign of $g(t_{i+1})$. This proves the claim (8.3.6).

Let λ be a rational number such that $|g(t_0)| < \lambda < |g(t_1)|$ such that p does not divide the numerator or denominator of λ. This can be easily achieved as follows. First choose $\lambda = a/b$ such that $|g(t_0)| < \lambda < |g(t_1)|$. Then consider $\lambda' = (p^j a + 1)/(p^j b + 1)$. Clearly, p does not divide the numerator or denominator of λ' and the difference $\lambda - \lambda'$ can be made very small by choosing j large. Note $g(X)$ has degree $2n + 1$ and exactly $2n + 1$ real roots. It is easily seen that $g(X) + \lambda$ has exactly $2n - 1$ real roots.

Applying the above discussion by taking $n = (p - 1)/2$, we see that we may choose λ so that $f(X) + \lambda$ is irreducible and has exactly $p - 2$ roots in $\mathbb{R}$. □

Corollary 8.3.7. *There exists a Galois extension $K/\mathbb{Q}$ with Galois group S_p.*

8.4 Composite of fields

In this section we will develop some results which we will use in the next section.

Definition 8.4.1. *Let $E, F \subset K$ be fields. The smallest subfield which contains E and F shall be denoted by EF. It is often referred to as the compositum of E and F.*

Remark 8.4.2. Let us make a remark about the field EF. First consider the collection $R \subset K$ which contains elements of the following kind:

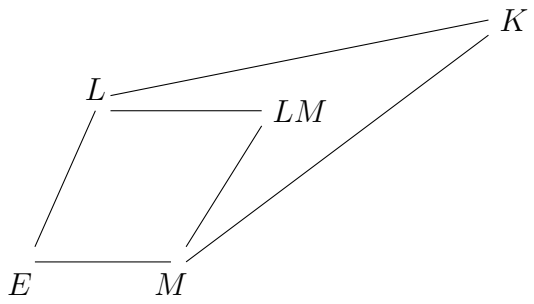
$$R := \{\alpha \in K \mid \alpha = \sum_{i=1}^{n} a_i b_i \ a_i \in E, b_i \in F\}.$$

It is obvious that R is a subring of K which contains both E and F. This follows trivially since sums and products of elements of R are in R. In fact, it is obvious that it is the smallest subring of K which contains both E and F. Now let

$$T := \{\frac{a}{b} \mid a, b \in R, b \neq 0\}$$

be the quotient field of R. Then it is clear that T is a field and that it is the smallest subfield of K which contains both E and F. □

Consider the following diagram of field extensions.



Proposition 8.4.3. *(1) If L is algebraic over E then LM is algebraic over M.*

(2) If L is algebraic and separable over E then LM is algebraic and separable over M.

(3) If L is algebraic and normal over E then LM is algebraic and normal over M.

Proof. (1) By the description of the field LM given in Remark 8.4.2, and using the Proposition 2.2.3, it suffices to show that every element of the type $\sum_{i=1}^{n} a_i b_i$ with $a_i \in L, b_i \in M$ is separable over M. Since a_i is algebraic over E, it follows that it is algebraic over M. Since $b_i \in M$, it is obviously algebraic over M. Thus, $a_i b_i$ is algebraic over M. Again applying Proposition

2.2.3 we see that $\sum_{i=1}^{n} a_i b_i$ is algebraic over M. This completes the proof of (1).

(2) The proof of (2) is identical to the proof of (1), except that one uses Proposition 4.3.5.

(3) Fix an algebraically closed field K_1 which contains all the fields. Let $\phi : LM \to K_1$ be a homomorphism which is the identity when restricted to M. Since L is normal, for every $a \in L$ it follows that $\phi(a) \in L$. Thus, from Remark 8.4.2 it follows that the image of ϕ lands in LM. This shows that LM is normal. This proves (3). □

Theorem 8.4.4. *Assume that L/E is a finite Galois extension. Then LM/M is a finite Galois extension and the natural restriction map*

$$\mathrm{Gal}(LM/M) \to \mathrm{Gal}(L/E)$$

is an inclusion with image isomorphic to $\mathrm{Gal}(L/(L \cap M))$.

Proof. Suppose we are given $\phi \in \mathrm{Gal}(LM/M)$ then we may restrict this to L. Since ϕ is the identity on M and $E \subset M$, it follows that ϕ is the identity on E. Since L is normal over E, it follows that $\phi|_L \in \mathrm{Gal}(L/E)$. Thus we get a map $\mathrm{Gal}(LM/M) \to \mathrm{Gal}(L/E)$. Suppose ϕ is in the kernel of this map, then this means that ϕ is the identity on L. But since ϕ is the identity on M, using Remark 8.4.2 it follows that ϕ is identity on LM. This shows that $\mathrm{Gal}(LM/M) \to \mathrm{Gal}(L/E)$ is an inclusion. Since ϕ is the identity on M, it follows that $\phi|_L$ is the identity on $L \cap M$. Thus, the image of the restriction map is contained in $\mathrm{Gal}(L/(L \cap M))$.

Finally we want to show that the image of the above homomorphism is precisely $\mathrm{Gal}(L/L \cap M)$. Using the Galois correspondence between subgroups and subfields, it suffices to show that $L^{\mathrm{Gal}(LM/M)} = L \cap M$. It is clear that $L \cap M \subset L^{\mathrm{Gal}(LM/M)}$. Conversely, $\alpha \in L$ is left fixed by all elements of $\mathrm{Gal}(LM/M)$, then it is in M (by the Galois correspondence for LM/M). Thus, $\alpha \in L \cap M$. This completes the proof of the Theorem. □

Theorem 8.4.5. *Assume that both L and M are finite Galois extensions of E. Then LM is a finite Galois extension of E and we have a commutative*

diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(L/(L\cap M)) & \longrightarrow & \mathrm{Gal}(LM/E) & \longrightarrow & \mathrm{Gal}(M/E) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \| & & \\ 1 & \longrightarrow & \mathrm{Gal}(L/E) & \longrightarrow & \mathrm{Gal}(L/E)\times\mathrm{Gal}(M/E) & \longrightarrow & \mathrm{Gal}(M/E) & \longrightarrow & 1 \end{array}$$

in which the middle vertical arrow is an inclusion. In particular, if $L\cap M = E$ then we see that the middle arrow is an isomorphism.

Proof. The exactness of the top row follows easily using the previous theorem and the fact that every element in $\mathrm{Gal}(M/E)$ can be extended to an element of $\mathrm{Gal}(LM/E)$. The exactness of the bottom row is obvious. The middle vertical arrow is an inclusion can be seen by using the description of LM in Remark 8.4.2. If $L \cap M = E$, then by looking at the cardinality we see that the middle vertical arrow is an isomorphism. □

8.5 Cyclotomic extensions

Let $\zeta_n := e^{2\pi i/n} \in \mathbb{C}$. This is clearly algebraic over $\mathbb{Q}$ since it satisfies the equation $X^n - 1 = 0$. We first claim that the extension $\mathbb{Q}[\zeta_n]$ is a normal extension of $\mathbb{Q}$. If $\phi : \mathbb{Q}[\zeta_n] \to \bar{\mathbb{Q}}$ then $\phi(\zeta_n)$ is forced to be a solution of $X^n - 1 = 0$. But all solutions of this equation are powers of ζ_n. Thus, $\phi(\zeta_n) \in \mathbb{Q}[\zeta_n]$. This shows that $\phi(\mathbb{Q}[\zeta_n]) \subset \mathbb{Q}[\zeta_n]$, which proves that $\mathbb{Q}[\zeta_n]$ is a normal, and hence Galois, extension of $\mathbb{Q}$.

We will need the following Lemma.

Lemma 8.5.1 (Gauss)**.** *Let $f(X) \in \mathbb{Z}[X]$ be a monic polynomial. Suppose that $f(X) = g(X)h(X)$, where $g(X), h(X) \in \mathbb{Q}[X]$ and both are monic. Then $g(X), h(X) \in \mathbb{Z}[X]$.*

Proof. Let $l \in \mathbb{Z}$ be the smallest positive integer such that $lg(X) \in \mathbb{Z}[X]$. Let us assume that $l > 1$. We claim that the gcd of the coefficients of $lg(X)$ is 1, or else, if this gcd is d, then the positive integer l/d would have worked. Similarly, define $t \in \mathbb{Z}$ to be the smallest positive integer such that $th(X) \in \mathbb{Z}[X]$. Then we have

$$ltf(X) = (lg(X)) \cdot (th(X)) .$$

If $lt > 1$, let p be a prime which divides lt. Then going modulo p the LHS is 0. However, since the gcd of the coefficients of $lg(X)$ is 1, it follows that p does not divide all the coefficients, and so $lg(X) \neq 0$ in $\mathbb{Z}/p\mathbb{Z}[X]$. Similarly, $th(X) \neq 0$ in $\mathbb{Z}/p\mathbb{Z}[X]$. But as $\mathbb{Z}/p\mathbb{Z}[X]$ is an integral domain, the product of two nonzero elements cannot become 0. Thus, we get a contradiction. Thus, $l = t = 1$ and this proves the lemma. □

Our aim in this section is to find $\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})$. We begin by finding the irreducible polynomial of ζ_n over $\mathbb{Q}$. Consider the polynomial

$$\Phi_n(X) = \prod_{\mathrm{gcd(i,n)=1}} (X - \zeta_n^i).$$

Theorem 8.5.2. *$\Phi_n(X) \in \mathbb{Q}[X]$ and is the irreducible polynomial of ζ_n over $\mathbb{Q}$.*

Proof. Apriori, the coefficients of this polynomial are in $\mathbb{Q}[\zeta_n]$. To show that the coefficients are in $\mathbb{Q}$, it suffices to show that for every $\phi \in \mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})$ the coefficients are left invariant by ϕ. Then by the Galois correspondence it will follow that the coefficients are in $\mathbb{Q}$. We claim that for any such automorphism ϕ we have $\phi(\zeta_n) = \zeta_n^l$ where $\gcd(l, n) = 1$. If not then $\phi(\zeta_n)$ would satisfy an equation $X^m - 1 = 0$ where $m < n$ and m divides n. Applying ϕ^{-1} we see that this would mean that ζ_n also satisfies this equation, which is impossible. If i is such that $\gcd(i, n) = 1$ then $\gcd(il, n) = 1$. Since $\phi(\zeta_n^i) = \zeta_n^{il}$, it follows that ϕ permutes the set of roots of $\Phi_n(X)$. From this it is clear that when we apply ϕ to the coefficients of $\Phi_n(X)$ then these are left invariant.

Now $X^n - 1 = \prod_{i=0}^{n-1}(X - \zeta_n^i)$. Since $\Phi_n(X)$ divides $X^n - 1$, it follows using Gauss' Lemma 8.5.1 that $\Phi_n(X) \in \mathbb{Z}[X]$. Obviously, from the definition, $\Phi_n(X)$ is monic. Let us assume that $\Phi_n(X) = f(X)g(X)$ where $f(X), g(X) \in \mathbb{Q}[X]$ are monic and $f(X)$ is the irreducible polynomial of ζ_n over $\mathbb{Q}$. Then again using Gauss' Lemma 8.5.1 we see that $f(X), g(X)$ are monic polynomials in $\mathbb{Z}[X]$. If ζ_n^i is a root of $\Phi_n(X)$, and p is a prime not dividing n, then clearly ζ_n^{ip} is a root of $\phi_n(X)$. Every i which is coprime to n is a product of such primes. Thus, to show that $\Phi_n(X)$ is irreducible, it suffices to show that if θ is a root of $f(X)$, then θ^p is a root of $f(X)$, for every p not dividing n.

So let us assume that θ is a root of $f(X)$ and θ^p is a root of $g(X)$. This means that θ is a root of $g(X^p)$, and since $f(X)$ is the irreducible polynomial

of θ, this implies that $f(X)$ divides $g(X^p)$. Now we go mod p. We have

$$\overline{g(X^p)} = \overline{g(X)}^p .$$

This is because the coefficients mod p lie in $\mathbb{F}_p$ and every element in $\mathbb{F}_p$ satisfies $a^p = a$. Thus, $\overline{f(X)}$ divides $\overline{g(X)}^p$. Let δ be a root of $\overline{f(X)}$ in $\bar{\mathbb{F}}_p$. Then this shows that $X - \delta$ divides $f(X)$ and $g(X)$.

Now since $f(X)g(X)$ divides $X^n - 1$, this also happens mod p, and this shows that $(X - \delta)^2$ divides $X^n - 1$ in $\bar{\mathbb{F}}_p[X]$. But this means that δ is a root of $X^n - 1$ and also a root of $D_{\bar{\mathbb{F}}_p}(X^n - 1) = nX^{n-1}$, using Lemma 5.1.1. Since δ is a root of $X^n - 1$, clearly, $\delta \neq 0$. The only root of $D_{\bar{\mathbb{F}}_p}(X^n - 1)$ is 0. This is a contradiction. □

Corollary 8.5.3. $[\mathbb{Q}[\zeta_n] : \mathbb{Q}] = \varphi(n)$.

Theorem 8.5.4. *There is a natural map* $(\mathbb{Z}/n\mathbb{Z})^\times \xrightarrow{\sim} \mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})$ *which is an isomorphism.*

Proof. Given an $i \in (\mathbb{Z}/n\mathbb{Z})^\times$ we define an element $\phi_i \in \mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q})$ by defining $\phi_i(\zeta_n) = \zeta_n^i$. Clearly, this defines a homomorphism from $\mathbb{Q}[\zeta_n] \to \mathbb{Q}[\zeta_n]$ since ζ_n^i is a root of $\Phi_n(X)$. It is also clear that distinct elements of $(\mathbb{Z}/n\mathbb{Z})^\times$ give rise to distinct automorphisms. Further, it is clear that this map is a homomorphism of groups. By comparing cardinalities of both groups we see that this is an isomorphism. □

8.6 Abelian groups as Galois groups over $\mathbb{Q}$

In this section we will show that every abelian group can be obtained as a Galois group of a finite extension of $\mathbb{Q}$. By the structure theorem for finite abelian groups, we know that

$$G \cong \bigoplus_{i=1}^{r} G_i ,$$

where each G_i is a finite cyclic group. Recall Dirichlet's Theorem on primes in an arithmetic progression.

Theorem 8.6.1 (Dirichlet)**.** *Let $a, b \in \mathbb{Z}$ be coprime. Then the arithmetic progression*

$$\{a + kb \mid k \in \mathbb{Z}\}$$

contains infinitely many primes.

In particular, given any integer n, we see that there are infinitely many primes in the arithmetic progression $1 + kn$. For each i, let n_i denote the cardinality of the group G_i above. Choose distinct primes p_i such that

$$n_i | (p_i - 1)\,.$$

Since $(\mathbb{Z}/p_i\mathbb{Z})^\times$ is a cyclic group of order $(p_i - 1)$, it follows that there is a surjective quotient

$$(\mathbb{Z}/p_i\mathbb{Z})^\times \twoheadrightarrow G_i\,.$$

Thus, there is a surjection

$$\bigoplus_{i=1}^{r} (\mathbb{Z}/p_i\mathbb{Z})^\times \twoheadrightarrow \bigoplus_{i=1}^{r} G_i\,.$$

By the Chinese Remainder Theorem, $\bigoplus_{i=1}^{r}(\mathbb{Z}/p_i\mathbb{Z})^\times \cong (\mathbb{Z}/n\mathbb{Z})^\times$, where $n = \prod_{i=1}^{r} p_i$, with p_i as above. This shows that there is a surjection

$$\mathrm{Gal}(\mathbb{Q}[\zeta_n]/\mathbb{Q}) \twoheadrightarrow G\,.$$

If H denotes the kernel, then by the Galois correspondence we have

$$\mathrm{Gal}(\mathbb{Q}[\zeta_n]^H/\mathbb{Q}) \cong G\,.$$

Thus we have proved that

Theorem 8.6.2. *Every finite abelian group is the Galois group of an extension of $\mathbb{Q}$.*

8.7 Kronecker-Weber Theorem

In the previous section we saw that every finite abelian group G is the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ for some K, where K is a subfield of a cyclotomic extension of $\mathbb{Q}$. The following theorem is a converse to this.

Theorem 8.7.1 (Kronecker-Weber)**.** *Let $K/\mathbb{Q}$ be a Galois extension such that* $\mathrm{Gal}(K/\mathbb{Q})$ *is abelian. Then K can be embedded into a cyclotomic extension of $\mathbb{Q}$.*

The proof of this very interesting theorem is beyond the scope of this course.

Chapter 9

Norm and Trace

9.1 Norm

Let $E \subset F$ be a finite extension. Then F is a finite dimensional vector space over E and for any element $a \in F$ we have the F-linear map $m_a : F \to F$, which is simply $x \mapsto ax$. Since it is F-linear, it is also E-linear.

Definition 9.1.1. *Define $N_{F/E} : F^\times \to E^\times$ as follows. For $a \in F$ define $N_{F/E}(a) = \det(m_a)$.*

Clearly $N_{F/E}(a) = 0$ iff $a = 0$. This is because if $a \neq 0$, then the inverse of m_a is $m_{a^{-1}}$. It is also clear that $N_{F/E}(ab) = N_{F/E}(a)N_{F/E}(b)$.

Let us see an example before we proceed. Consider the extension $\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}]$. Let us compute $N(\sqrt[3]{2})$. Since the determinant of a linear map can be computed using any basis, we may choose the basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ for $\mathbb{Q}[\sqrt[3]{2}]$ over $\mathbb{Q}$. In this basis, the matrix of $m_{\sqrt[3]{2}}$ is (we write elements of $\mathbb{Q}[\sqrt[3]{2}]$ as column vectors using the above basis)

$$\begin{bmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

Computing the determinant of this matrix we get $N(\sqrt[3]{2}) = 2$. As an exercise the reader may compute $N(\sqrt[3]{2} - 1)$.

Lemma 9.1.2. *If $a \in E$ then $N_{F/E} = a^{[F:E]}$.*

Proof. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be a basis for F/E. Clearly $n = [F : E]$. Then in this basis it is clear that the matrix for m_a is $\mathrm{diag}(a, a, \ldots, a)$. The lemma now follows easily. □

Lemma 9.1.3. *Let $E \subset \bar{E}$ and $\alpha \in \bar{E}$. Let $p(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ denote the monic irreducible polynomial of α over E. Let $F = E[\alpha]$. Then $N_{F/E}(\alpha) = (-1)^n a_0$.*

Proof. The proof is a straightforward generalization of the above example. Clearly $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis for F over E. Writing elements of F as column vectors in this basis we see that the matrix m_α is given by

$$\begin{bmatrix} 0 & 0 & \ldots & -a_0 \\ 1 & 0 & \ldots & -a_1 \\ 0 & 1 & \ldots & -a_2 \\ \vdots & & & \\ 0 & \ldots & 1 & -a_{n-1} \end{bmatrix}$$

The determinant of this matrix is clearly $(-1)^n a_0$. This proves the lemma. □

Lemma 9.1.4. *Let characteristic of E be 0. Let $E \subset \bar{E}$ and $\alpha \in \bar{E}$. Let $F = E[\alpha]$. Then $N_{F/E}(\alpha) = \prod_{\sigma \in \mathrm{Hom}_E(F, \bar{E})} \sigma(\alpha)$.*

Proof. Let $p(X) \in E[X]$ denote the monic irreducible polynomial of $\alpha = \alpha_1$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ denote the roots of $p(X)$. Since we are in characteristic 0, $p(X)$ has no repeated roots. Thus, over $\bar{E}$ we have

$$p(X) = \prod_{i=1}^{n} (X - \alpha_i) .$$

Since $F = E[\alpha] \cong E[X]/(p(X))$, the embeddings σ are in bijective correspondence with the roots of $p(X)$. Indeed, σ is completely determined by where it sends $\alpha = \alpha_1$. Thus, we may define σ_i to be that embedding which sends $\alpha_1 \mapsto \alpha_i$. Now it is clear that

$$\prod_{\sigma \in \mathrm{Hom}_E(F, \bar{E})} \sigma(\alpha) = \prod_{i=1}^{n} \alpha_i = (-1)^n a_0 = N_{F/E}(\alpha) .$$

This completes the proof of the lemma. □

Lemma 9.1.5. *Let characteristic of E be $p > 0$. Let $E \subset \bar{E}$ and $\alpha \in \bar{E}$. Let $F = E[\alpha]$. Then $N_{F/E}(\alpha) = \Big(\prod_{\sigma \in \mathrm{Hom}_E(F,\bar{E})} \sigma(\alpha) \Big)^{[F:E]_i}$.*

Proof. Let $p(X) \in E[X]$ denote the monic irreducible polynomial of $\alpha = \alpha_1$. Find the largest $r \geq 0$ such that $p(X) = f(X^{p^r})$. Then $f(X)$ is a separable polynomial. Let $\beta_1, \beta_2, \ldots, \beta_n$ denote the roots of $f(X)$. Thus, over $\bar{E}$ we have

$$f(X) = \prod_{i=1}^{n} (X - \beta_i) \,,$$

and so

$$p(X) = \prod_{i=1}^{n} (X - \alpha_i)^{p^r} ,$$

where α_i is the unique p^rth root of β_i. Since $F = E[\alpha] \cong E[X]/(p(X))$, the embeddings σ are in bijective correspondence with the distinct roots of $p(X)$. Indeed, σ is completely determined by where it sends $\alpha = \alpha_1$. Thus, we may define σ_i to be that embedding which sends $\alpha_1 \mapsto \alpha_i$. Now it is clear that

$$\Big(\prod_{\sigma \in \mathrm{Hom}_E(F,\bar{E})} \sigma(\alpha) \Big)^{p^r} = \Big(\prod_{i=1}^{n} \alpha_i \Big)^{p^r} = (-1)^n a_0 = N_{F/E}(\alpha) \,.$$

To complete the proof the lemma it suffices to show that $[F : E]_i = p^r$. Since $f(X)$ is irreducible and separable, and $f(\alpha^{p^r}) = 0$, it follows that α^{p^r} is separable over E. Thus, it follows that $E[\alpha^{p^r}]$ is separable over E. Now it is clear that $E[\alpha]$ is a purely inseparable extension of $E[\alpha^{p^r}]$. It now follows from Theorem 4.4.2 that the $[F : E[\alpha^{p^r}]] = p^r$. Now it follows from Theorem 4.4.6 that $[F : E]_i = p^r$. □

Lemma 9.1.6. *Let $E \subset K$ be a finite extension. Let $\alpha \in K$ and define $F := E[\alpha]$. Then $N_{K/E}(\alpha) = N_{F/E}(\alpha)^{[K:F]}$.*

Proof. Let $\{k_1, k_2, \ldots, k_r\}$ be a basis for K over F. Note $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis for F over E. Then $\{\alpha^i k_j\}$ is a basis for K over E. Let us compute the matrix for m_α in this basis. Since m_α takes F to itself, it follows that it takes the subspace $Fk_j \subset K$ to itself. Thus, writing

$$K = \bigoplus_{j=1}^{r} Fk_j \,.$$

it follows that the matrix of m_α is block diagonal, with each block being the matrix of m_α restricted to F. It follows that the determinant is $N_{F/E}(\alpha)^r$. This completes the proof of the lemma. □

Lemma 9.1.7. *Let $E \subset K$ be a finite extension. Let $\alpha \in K$. Then $N_{K/E}(\alpha) = \Big(\prod_{\sigma \in \mathrm{Hom}_E(K,\bar{E})} \sigma(\alpha)\Big)^{[K:E]_i}$.*

Proof. Let F denote $E[\alpha]$. Let $\sigma_1, \sigma_2, \ldots, \sigma_r$ be the elements of the set $\mathrm{Hom}_E(F, \bar{E})$. Each of these may be lifted to $\sigma_{ij} \in \mathrm{Hom}_E(K, \bar{E})$, where $1 \leqslant j \leqslant [K : F]_s$. Note that since $\sigma_{ij}|_F = \sigma_i$, it follows that $\sigma_{ij}(\alpha) = \sigma_i(\alpha)$. Then the RHS becomes

$$\begin{aligned}
\Big(\prod_{\sigma \in \mathrm{Hom}_E(K,\bar{E})} \sigma(\alpha)\Big)^{[K:E]_i} &= \Big(\prod_{\sigma \in \mathrm{Hom}_E(F,\bar{E})} \sigma(\alpha)\Big)^{[K:F]_s[K:E]_i} \\
&= \Big(\prod_{\sigma \in \mathrm{Hom}_E(F,\bar{E})} \sigma(\alpha)\Big)^{[F:E]_i[K:F]_s[K:F]_i} \\
&= N_{F/E}(\alpha)^{[K:F]} \\
&= N_{K/E}(\alpha)
\end{aligned}$$

For the third equality we have used Lemma 9.1.5 and for the fourth we have used Lemma 9.1.6. □

Theorem 9.1.8. *Let $E \subset F \subset K$ be finite extensions. Then*

$$N_{F/E} \circ N_{K/F} = N_{K/E}\,.$$

Proof. We will use the previous Lemma. Let $\sigma = \sigma_1, \sigma_2, \ldots, \sigma_r$ be the elements of the set $\mathrm{Hom}_E(F, \bar{E})$. Here $\sigma : F \subset \bar{E}$ is a fixed embedding, using which we view F as sitting inside $\bar{E}$.

Recall the main result of section 3.3. It says that the action of $\mathrm{Gal}(\bar{E}/E)$ on the set $\mathrm{Hom}_E(F, \bar{E})$ is transitive. There exist elements $\tilde{\sigma}_i \in \mathrm{Gal}(\bar{E}/E)$ such that $\tilde{\sigma}_i \circ \sigma = \sigma_i$.

Let us first extend σ to $\tau_1, \tau_2, \ldots, \tau_l \in \mathrm{Hom}_\sigma(K, \bar{E})$. Recall that this means that the $\tau_j : K \to \bar{E}$ and their restriction to F is equal to σ.

$$\begin{array}{ccc}
K & \xrightarrow{\tau_j} & \bar{E} \\
\uparrow & & \| \\
F & \xrightarrow{\sigma} & \bar{E}
\end{array}$$

Here $l = [K : F]_s$.

We emphasize that in all the above Lemmas, for example, in Lemma 9.1.7, we had fixed an embedding $i : E \subset \bar{E}$, and when we write

$$N_{K/E}(\alpha) = \Big(\prod_{\sigma \in \mathrm{Hom}_E(K,\bar{E})} \sigma(\alpha) \Big)^{[K:E]_i},$$

we mean

$$i(N_{K/E}(\alpha)) = \Big(\prod_{\sigma \in \mathrm{Hom}_E(K,\bar{E})} \sigma(\alpha) \Big)^{[K:E]_i}.$$

Keeping this in mind, it is clear that for $\alpha \in K$,

$$\Big(\prod_j \tau_j(\alpha) \Big)^{[K:F]_i} = \sigma(N_{K/F}(\alpha)) \,.$$

We will use this later.

Consider the elements $\tilde{\sigma}_i \circ \tau_j : K \to \bar{E}$.

$$\begin{array}{ccccc} K & \xrightarrow{\tau_j} & \bar{E} & \xrightarrow{\tilde{\sigma}_i} & \bar{E} \\ \uparrow & & \| & & \| \\ F & \xrightarrow{\sigma} & \bar{E} & \xrightarrow{\tilde{\sigma}_i} & \bar{E} \end{array}$$

These are elements of $\mathrm{Hom}_E(K, \bar{E})$. We claim that these are all distinct. On the contrary assume $\tilde{\sigma}_i \circ \tau_j = \tilde{\sigma}_a \circ \tau_b$. The τ_i's when restricted to F are equal to σ. This shows that $\tilde{\sigma}_i = \tilde{\sigma}_a$, that is, $i = a$. Since $\tilde{\sigma}_i$ is an isomorphism, as proved in Corollary 3.1.6, it follows that $\tau_j = \tau_b$. We also know that $[K : E]_s = [K : F]_s[F : E]_s = lr$. This proves that the set $\mathrm{Hom}_E(K, \bar{E})$ contains precisely the collection $\tilde{\sigma}_i \circ \tau_j$. Then

$$\begin{aligned} N_{K/E}(\alpha) &= \Big(\prod_{i,j} \tilde{\sigma}_i \tau_j(\alpha) \Big)^{[K:E]_i} \\ &= \Big(\prod_i \tilde{\sigma}_i \Big(\prod_j \tau_j(\alpha) \Big)^{[K:F]_i} \Big)^{[F:E]_i} \\ &= \Big(\prod_i \tilde{\sigma}_i(\sigma(N_{K/F}(\alpha))) \Big)^{[F:E]_i} \\ &= \Big(\prod_i \sigma_i(N_{K/F}(\alpha)) \Big)^{[F:E]_i} \\ &= N_{F/E}(N_{K/F}(\alpha)) \end{aligned}$$

This proves the theorem. □

9.2 Trace

Definition 9.2.1. *Define $Tr_{F/E} : F \to E$ as follows. For $a \in F$ define $Tr_{F/E}(a) = \text{Trace}(m_a)$.*

It is clear that $Tr_{F/E}(a+b) = Tr_{F/E}(a) + Tr_{F/E}(b)$.

Let us compute trace in the same example that we took earlier. Consider the extension $\mathbb{Q} \subset \mathbb{Q}[\sqrt[3]{2}]$. Let us compute $N(\sqrt[3]{2})$. We choose the basis $\{1, \sqrt[3]{2}, \sqrt[3]{4}\}$ for $\mathbb{Q}[\sqrt[3]{2}]$ over $\mathbb{Q}$. In this basis, the matrix of $m_{\sqrt[3]{2}}$ is (we write elements of $\mathbb{Q}[\sqrt[3]{2}]$ as column vectors using the above basis)

$$\begin{bmatrix} 0 & 0 & 2 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}$$

Computing the trace of this matrix we get $Tr(\sqrt[3]{2}) = 0$. As an exercise the reader may compute $Tr(\sqrt[3]{2} - 1)$.

Lemma 9.2.2. *If $a \in E$ then $Tr_{F/E} = [F : E]a$.*

Proof. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be a basis for F/E. Clearly $n = [F : E]$. Then in this basis it is clear that the matrix for m_a is $\text{diag}(a, a, \ldots, a)$. The lemma now follows easily. □

Lemma 9.2.3. *Let $E \subset \bar{E}$ and $\alpha \in \bar{E}$. Let $p(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_0$ denote the monic irreducible polynomial of α over E. Let $F = E[\alpha]$. Then $Tr_{F/E}(\alpha) = -a_{n-1}$.*

Proof. The proof is a straightforward generalization of the above example. Clearly $\{1, \alpha, \ldots, \alpha^{n-1}\}$ is a basis for F over E. Writing elements of F as column vectors in this basis we see that the matrix m_α is given by

$$\begin{bmatrix} 0 & 0 & \ldots & -a_0 \\ 1 & 0 & \ldots & -a_1 \\ 0 & 1 & \ldots & -a_2 \\ \vdots & & & \\ 0 & \ldots & 1 & -a_{n-1} \end{bmatrix}$$

The trace of this matrix is clearly $-a_{n-1}$. This proves the lemma. □

Lemma 9.2.4. *Let characteristic of E be 0. Let $E \subset \bar{E}$ and $\alpha \in \bar{E}$. Let $F = E[\alpha]$. Then $Tr_{F/E}(\alpha) = \sum_{\sigma \in \mathrm{Hom}_E(F,\bar{E})} \sigma(\alpha)$.*

Proof. Let $p(X) \in E[X]$ denote the monic irreducible polynomial of $\alpha = \alpha_1$. Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ denote the roots of $p(X)$. Since we are in characteristic 0, $p(X)$ has no repeated roots. Thus, over $\bar{E}$ we have

$$p(X) = \prod_{i=1}^{n} (X - \alpha_i)\,.$$

Since $F = E[\alpha] \cong E[X]/(p(X))$, the embeddings σ are in bijective correspondence with the roots of $p(X)$. Indeed, σ is completely determined by where it sends $\alpha = \alpha_1$. Thus, we may define σ_i to be that embedding which sends $\alpha_1 \mapsto \alpha_i$. Now it is clear that

$$\sum_{\sigma \in \mathrm{Hom}_E(F,\bar{E})} \sigma(\alpha) = \sum_{i=1}^{n} \alpha_i = -a_{n-1} = Tr_{F/E}(\alpha)\,.$$

This completes the proof of the lemma. □

Lemma 9.2.5. *Let characteristic of E be $p > 0$. Let $E \subset \bar{E}$ and $\alpha \in \bar{E}$. Let $F = E[\alpha]$. Then $Tr_{F/E}(\alpha) = [F : E]_i \Big(\sum_{\sigma \in \mathrm{Hom}_E(F,\bar{E})} \sigma(\alpha) \Big)$. In particular, if $[F : E]_i > 1$ then the trace is 0.*

Proof. Let $p(X) \in E[X]$ denote the monic irreducible polynomial of $\alpha = \alpha_1$. Find the largest $r \geq 0$ such that $p(X) = f(X^{p^r})$. Then $f(X)$ is a separable polynomial. Let $\beta_1, \beta_2, \ldots, \beta_n$ denote the roots of $f(X)$. Thus, over $\bar{E}$ we have

$$f(X) = \prod_{i=1}^{n} (X - \beta_i)\,,$$

and so

$$p(X) = \prod_{i=1}^{n} (X - \alpha_i)^{p^r}\,,$$

where α_i is the unique p^rth root of β_i. Since $F = E[\alpha] \cong E[X]/(p(X))$, the embeddings σ are in bijective correspondence with the distinct roots of

$p(X)$. Indeed, σ is completely determined by where it sends $\alpha = \alpha_1$. Thus, we may define σ_i to be that embedding which sends $\alpha_1 \mapsto \alpha_i$. In the proof of Lemma 9.1.5 we proved that $[F : E]_i = p^r$. If $r > 0$ then by Lemma 9.2.3 we see that $Tr_{F/E}(\alpha) = 0$. On the other hand since $[F : E]_i = p^r$ we see that

$$[F : E]_i \Big(\sum_{\sigma \in \mathrm{Hom}_E(F, \bar{E})} \sigma(\alpha) \Big) = 0 \, .$$

Thus, if $r > 0$ then the lemma is proved. Now consider the case when $r = 0$. Then

$$\Big(\sum_{\sigma \in \mathrm{Hom}_E(F, \bar{E})} \sigma(\alpha) \Big) = \Big(\sum_{i=1}^{n} \alpha_i \Big) = -a_{n-1} = Tr_{F/E}(\alpha) \, .$$

This completes the proof of the lemma. □

Lemma 9.2.6. *Let $E \subset K$ be a finite extension. Let $\alpha \in K$ and define $F := E[\alpha]$. Then $Tr_{K/E}(\alpha) = [K : F] Tr_{F/E}(\alpha)$.*

Proof. Let $\{k_1, k_2, \ldots, k_r\}$ be a basis for K over F. Note $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ is a basis for F over E. Then $\{\alpha^i k_j\}$ is a basis for K over E. Let us compute the matrix for m_α in this basis. Since m_α takes F to itself, it follows that it takes the subspace $Fk_j \subset K$ to itself. Thus, writing

$$K = \bigoplus_{j=1}^{r} Fk_j \, .$$

it follows that the matrix of m_α is block diagonal, with each block being the matrix of m_α restricted to F. It follows that the trace is $[K : F] Tr_{F/E}(\alpha)$. This completes the proof of the lemma. □

Lemma 9.2.7. *Let $E \subset K$ be a finite extension. Let $\alpha \in K$. Then $Tr_{K/E}(\alpha) = [K : E]_i \Big(\sum_{\sigma \in \mathrm{Hom}_E(K, \bar{E})} \sigma(\alpha) \Big)$.*

Proof. Let F denote $E[\alpha]$. Let $\sigma_1, \sigma_2, \ldots, \sigma_r$ be the elements of the set $\mathrm{Hom}_E(F, \bar{E})$. Each of these may be lifted to $\sigma_{ij} \in \mathrm{Hom}_E(K, \bar{E})$, where $1 \leqslant j \leqslant [K : F]_s$. Note that since $\sigma_{ij}|_F = \sigma_i$, it follows that $\sigma_{ij}(\alpha) = \sigma_i(\alpha)$.

Then the RHS becomes

$$\begin{aligned}[K:E]_i\Big(\sum_{\sigma\in \mathrm{Hom}_E(K,\bar{E})}\sigma(\alpha)\Big) &= [K:F]_s[K:E]_i\Big(\sum_{\sigma\in \mathrm{Hom}_E(F,\bar{E})}\sigma(\alpha)\Big)\\ &= [F:E]_i[K:F]_s[K:F]_i\Big(\sum_{\sigma\in \mathrm{Hom}_E(F,\bar{E})}\sigma(\alpha)\Big)\\ &= [K:F]Tr_{F/E}(\alpha)\\ &= Tr_{K/E}(\alpha)\end{aligned}$$

For the third equality we have used Lemma 9.2.5 and for the fourth we have used Lemma 9.2.6. □

Theorem 9.2.8. *Let $E \subset F \subset K$ be finite extensions. Then*

$$Tr_{F/E} \circ Tr_{K/F} = Tr_{K/E}\,.$$

Proof. We will use the previous Lemma. Let $\sigma_1, \sigma_2, \ldots, \sigma_r$ be the elements of the set $\mathrm{Hom}_E(F, \bar{E})$. Let us first extend these to $\tilde{\sigma}_i : \bar{E} \to \bar{E}$. Let $\tau_1, \tau_2, \ldots, \tau_l$ be the elements of the set $\mathrm{Hom}_F(K, \bar{E})$. Consider the maps $\tilde{\sigma}_i \circ \tau_j : K \to \bar{E}$. These are elements of $\mathrm{Hom}_E(K, \bar{E})$. We saw in the proof of Theorem 9.1.8 that the set $\mathrm{Hom}_E(K, \bar{E})$ is precisely the collection $\tilde{\sigma}_i \circ \tau_j$.

Then

$$\begin{aligned}Tr_{K/E}(\alpha) &= [K:E]_i\Big(\sum_{i,j}\tilde{\sigma}_i\tau_j(\alpha)\Big)\\ &= [F:E]_i\Big(\sum_i \tilde{\sigma}_i\Big([K:F]_i\sum_j \tau_j(\alpha)\Big)\Big)\\ &= [F:E]_i\Big(\sum_i \tilde{\sigma}_i(Tr_{K/F}(\alpha))\Big)\\ &= [F:E]_i\Big(\sum_i \sigma_i(Tr_{K/F}(\alpha))\Big)\\ &= Tr_{F/E}(Tr_{K/F}(\alpha))\end{aligned}$$

This proves the theorem. □

9.3 Linear independence of characters

Let G be a group and let L be a field. A character of G (in L) is a group homomorphism $\chi : G \to L^\times$. Given a character of G we may consider it as

a map from $\chi : G \to L$, that is, as an element of $\mathrm{Maps}(G, L)$. For any set S, the set $\mathrm{Maps}(S, L)$ has an obvious L-vector space structure, the one coming from L. This is given as follows. Let $f : S \to K$ and let $a \in L$. Then

$$(a \cdot f)(g) := af(g)\,.$$

In particular, this means that $\mathrm{Maps}(G, L)$ is a L-vector space.

Proposition 9.3.1. *Let $\chi_1, \chi_2, \ldots, \chi_n$ be characters of G in L. Then these are linearly independent as elements of* $\mathrm{Maps}(G, L)$.

Proof. Let us assume that this is not the case. Thus, there is a linear dependence

$$a_1\chi_1 + a_2\chi_2 + \ldots + a_n\chi_n = 0$$

in $\mathrm{Maps}(G, L)$. Let us choose the linear dependence which contains the least number of characters and renumber the characters and write

$$a_1\chi_1 + a_2\chi_2 + \ldots + a_r\chi_r = 0$$

for an r which is the smallest possible. By choice $a_i \neq 0$ for all i. Since $\chi_1 \neq \chi_2$, there is $h \in G$ such that $\chi_1(h) \neq \chi_2(h)$. Evaluating the above at g and hg we get

$$\begin{aligned} a_1\chi_1(g) + a_2\chi_2(g) + \ldots + a_r\chi_r(g) &= 0 \\ a_1\chi_1(h)\chi_1(g) + a_2\chi_2(h)\chi_2(g) + \ldots + a_r\chi_r(h)\chi_r(g) &= 0 \end{aligned}$$

Multiplying the first equation with $\chi_1(h)$ and subtracting we get that

$$\sum_{i=2}^{r} a_i(\chi_i(h) - \chi_1(h))\chi_i(g) = 0$$

for all $g \in G$. The coefficient when $i = 2$ is clearly nonzero and so this is a non-trivial relation among a smaller number of characters,

$$\sum_{i=2}^{r} a_i(\chi_i(h) - \chi_1(h))\chi_i = 0\,.$$

This proves the proposition. □

We will use the above Proposition and Lemma 9.2.7 to deduce the following.

Theorem 9.3.2. *Let $E \subset K$ be a finite separable extension. Then the pairing $K \times K \to E$ given by*

$$(x, y) \mapsto Tr_{K/E}(xy)$$

is non-degenerate.

Proof. Let us assume that this is not the case. Then there is $y \in K$ such that $y \neq 0$ and $Tr_{K/E}(xy) = 0$ for all $x \in K$. Since $[K : E]_i = 1$, by Lemma 9.2.7 it follows that $Tr_{K/E}(xy) = \sum_{i=1}^{n} \sigma_i(xy)$. Here σ_i are the elements of $\mathrm{Hom}_E(K, \bar{E})$. Thus, for all $x \in K$ we have

$$\sum_{i=1}^{n} \sigma_i(y)\sigma_i(x) = 0\,.$$

But $\sigma_i : K^\times \to \bar{E}^\times$ is a group homomorphism. The above equation shows that the characters $\sigma_1, \ldots, \sigma_n$ are linearly dependent. This contradicts the previous proposition by taking $G = K^\times$ and $L = \bar{E}$. □

9.4 Algebraic Integers

There is a very rich and interesting theory of algebraic integers, which we will not go into. For our purposes it will suffice to show that the set of algebraic integers is a subring of $\bar{\mathbb{Q}}$. The aim of this section is to give an application of Theorem 9.3.2.

Definition 9.4.1. *An element $\alpha \in \bar{\mathbb{Q}}$ is called an algebraic integer if there is a monic polynomial $g(X) \in \mathbb{Z}[X]$ such that $g(\alpha) = 0$.*

Lemma 9.4.2. *If α is an algebraic integer then the monic irreducible polynomial of α over $\mathbb{Q}$ has coefficients in $\mathbb{Z}$.*

Proof. Let $p(X)$ denote the monic irreducible polynomial of α over $\mathbb{Q}$. Then we may write $g(X) = p(X)h(X)$, where $h(X) \in \mathbb{Q}[X]$ is monic. Let $a > 0$ be an integer such that $ap(X) \in \mathbb{Z}[X]$ and $ah(X) \in \mathbb{Z}[X]$. Then

$$a^2 g(X) = (ap(X))(ah(X))\,.$$

Comparing content, recall Definition 1.4.1, we get

$$a^2 = \text{cont}(ap)\text{cont}(ah)\,.$$

Since $p(X)$ is monic, it follows that ap has leading coefficient a. Thus, $\text{cont}(ap) = \gcd(a, \ldots) \leqslant a$. Similarly, $\text{cont}(ah) \leqslant a$. It follows easily that $\text{cont}(ap) = \text{cont}(ah) = a$. Since $ap(X)/(\text{cont}(ap)) \in \mathbb{Z}[X]$, it follows that $p(X) \in \mathbb{Z}[X]$. □

Corollary 9.4.3. *Let α be an algebraic integer. Let $p(X)$ denote its monic irreducible polynomial. The subring $\mathbb{Z}[\alpha] \subset \bar{\mathbb{Q}}$ is isomorphic to $\mathbb{Z}[X]/(p(X))$.*

Proof. Consider the ring homomorphism $\mathbb{Z}[X] \to \bar{\mathbb{Q}}$ which sends $X \mapsto \alpha$. The image is clearly $\mathbb{Z}[\alpha]$. The kernel contains $(p(X))$. If $h(X) \in \mathbb{Z}[X]$ and $h(\alpha) = 0$ then $h(X) = p(X)q(X)$ for some $q(X) \in \mathbb{Q}[X]$. It is easily checked that $q(X) \in \mathbb{Z}[X]$. Thus, it follows that $h(X) \in (p(X)) \subset \mathbb{Z}[X]$. Thus, the kernel is precisely $(p(X))$. This proves the Corollary. □

Corollary 9.4.4. *If α is an algebraic integer then $\mathbb{Z}[\alpha] \subset \bar{\mathbb{Q}}$ is a free $\mathbb{Z}$ module of finite rank equal to degree of the irreducible polynomial of α over $\mathbb{Z}$.*

Proof. If $p(X) \in \mathbb{Z}[X]$ denotes the monic irreducible polynomial of α then $\mathbb{Z}[\alpha] \cong \mathbb{Z}[X]/(p(X))$. Clearly the ring $\mathbb{Z}[X]/(p(X))$ is a free $\mathbb{Z}$ module with basis $1, X, \ldots, X^{d-1}$, where $d = \deg(p(X))$. □

Proposition 9.4.5. *Let $\alpha \in \bar{\mathbb{Q}}$ be such that $\mathbb{Z}[\alpha] \subset \bar{\mathbb{Q}}$ is a finitely generated $\mathbb{Z}$ module. Then α is an algebraic integer.*

Proof. Consider the set $\{1, \alpha, \alpha^2, \ldots, \}$. These generate $\mathbb{Z}[\alpha]$ as a $\mathbb{Z}$ module. Thus, finitely many of these, say $\{1, \alpha, \ldots, \alpha^n\}$ will generate $\mathbb{Z}[\alpha]$ as a $\mathbb{Z}$ module. Writing α^{n+1} in terms of these gives a monic polynomial $g(X) \in \mathbb{Z}[X]$ of degree $n+1$ such that $g(\alpha) = 0$. □

Proposition 9.4.6. *If α, β are algebraic integers then $\mathbb{Z}[\alpha, \beta] \subset \mathbb{Q}$ is a finitely generated $\mathbb{Z}$ module.*

Proof. The subring $\mathbb{Z}[\alpha, \beta]$ is a quotient of $\mathbb{Z}[X, Y]/(p(X), q(Y))$, where $p(X)$ denotes the monic irreducible polynomial of α and $q(Y)$ denotes the monic irreducible polynomial of β. The ring $\mathbb{Z}[X, Y]/(p(X), q(Y))$ is finitely generated as a $\mathbb{Z}$ module (by elements of the type $X^i Y^j$, $0 \leqslant i \leqslant \deg(p(X))$

$0 \leqslant j \leqslant \deg(q(Y)))$. Since quotient of a finitely generated module is a finitely generated module, the Proposition follows. □

Corollary 9.4.7. *If α, β are algebraic then so are $\alpha \pm \beta$, $\alpha\beta$.*

Proof. If $\gamma \in \mathbb{Z}[\alpha, \beta]$ then $\mathbb{Z}[\gamma] \subset \mathbb{Z}[\alpha, \beta]$. Since submodule of a finitely generated $\mathbb{Z}$ module is finitely generated, it follows that $\mathbb{Z}[\gamma]$ is finitely generated and so γ is an algebraic integer. Apply this to $\gamma = \alpha \pm \beta, \alpha\beta$. □

Lemma 9.4.8. *If $\alpha \in \mathbb{Q}$ is an algebraic integer, then $\alpha \in \mathbb{Z}$.*

Proof. Left as an exercise. □

Let K be a finite extension of $\mathbb{Q}$ and let $\mathcal{O}_K \subset K$ denote the set of algebraic integers in K. By Corollary 9.4.7 it follows that this is a subring. Moreover, this subring contains the integers. This is often represented in the diagram

$$\begin{array}{ccc} \mathcal{O}_K & \longrightarrow & K \\ \uparrow & & \uparrow \\ \mathbb{Z} & \longrightarrow & \mathbb{Q} \end{array}$$

Theorem 9.4.9. *$\mathcal{O}_K$ is a free $\mathbb{Z}$-module of rank $n = [K : \mathbb{Q}]$.*

Proof. Let $\{\alpha_1, \ldots, \alpha_n\} \subset K$ be a $\mathbb{Q}$-basis for K. For any $\alpha \in K$, it is easily checked that there is a $b \in \mathbb{Z}$ such that $b\alpha \in \mathcal{O}_K$. Thus, multiplying by a suitable $b \in \mathbb{Z}$, we may assume that $\{\alpha_1, \ldots, \alpha_n\} \subset \mathcal{O}_K$ forms a $\mathbb{Q}$-basis for K. Let $B := \langle Tr_{K/\mathbb{Q}}(\alpha_i\alpha_j)\rangle$. Then B is an $n \times n$ matrix.

Consider the isomorphisms $\mathbb{Q}^n \xrightarrow{\sim} K \xrightarrow{\sim} \mathbb{Q}^n$ given by

$$v \mapsto x = \sum_i v_i\alpha_i \mapsto (Tr_{K/\mathbb{Q}}(x\alpha_1), \ldots, Tr_{K/\mathbb{Q}}(x\alpha_n)) = vB\,.$$

If $x \in \mathcal{O}_K$, the combining Lemma 9.2.3 and Lemma 9.2.6 we see that

$$(Tr_{K/\mathbb{Q}}(x\alpha_1), \ldots, Tr_{K/\mathbb{Q}}(x\alpha_n)) = vB \in \mathbb{Z}^n\,.$$

Thus, we get that $v = \frac{Cw}{det(B)}$ for some $w \in \mathbb{Z}^n$ and a matrix C which has integer coefficients. In other words, every element of $\mathcal{O}_K$ can be represented as

$$x = \frac{\sum_i v_i\alpha_i}{det(B)}\,.$$

Thus, under the isomorphism $\mathbb{Q}^n \xrightarrow{\sim} K$ given by $v \mapsto \sum_i v_i \alpha_i$, $\mathcal{O}_K$ is contained in the image of the finitely generated $\mathbb{Z}$-submodule $\frac{1}{det(B)}\mathbb{Z}^n$. Thus, $\mathcal{O}_K$ is contained in a finitely generated $\mathbb{Z}$-module and so is a finitely generated submodule. It is clear that $\mathcal{O}_K$ is torsion free. It follows from the structure theorem of finitely generated abelian groups that $\mathcal{O}_K$ is a finitely generated and free submodule.

If the rank of this module is strictly less than n, then it would follow that there is a $\mathbb{Z}$-linear relation among the α_i, which would imply that there is a $\mathbb{Q}$-linear relation among the α_i, which is a contradiction. Thus, it follows that the rank of $\mathcal{O}_K$ is n. $\square$

Chapter 10

Lindemann-Weierstrass Theorem

The main result of this chapter is the Lindemann-Weierstrass Theorem. First we shall prove that π is transcendental over $\mathbb{Q}$, as this will be used in the proof of the Lindemann-Weierstrass Theorem.

10.1 Transcendence of π

The transcendence of π was proved by Carl Louis Ferdinand von Lindemann in 1882.

We begin with a preliminary result we will need. Let $f(X) \in \mathbb{C}[X]$ be a polynomial. If $f(X) = \sum_{i=0}^{n} a_i X^i$ then denote by $\bar{f}(X)$ the polynomial $\sum_{i=0}^{n} |a_i| X^i$. For $\lambda \in \mathbb{C}$ define an integral

$$I(\lambda) := I(\lambda, f) = \lambda e^{\lambda} \int_0^1 e^{-u\lambda} f(u\lambda)\, du\,. \tag{10.1.1}$$

We shall need two properties of $I(\lambda)$. Note that

$$d(e^{-u\lambda} f(u\lambda)) = -\lambda e^{-u\lambda} f(u\lambda) du + \lambda e^{-u\lambda} f^{(1)}(u\lambda) du\,.$$

Integrating both sides from 0 to 1 we get

$$e^{-\lambda} f(\lambda) - f(0) + \lambda \int_0^1 e^{-u\lambda} f(u\lambda) du = \lambda \int_0^1 e^{-u\lambda} f^{(1)}(u\lambda) du\,.$$

This yields

$$f(\lambda) - e^{\lambda} f(0) + I(\lambda, f) = I(\lambda, f^{(1)}) .$$

Inductively, we get $f^{(k)}(\lambda) - e^{\lambda} f^{(k)}(0) + I(\lambda, f^{(k)}) = I(\lambda, f^{(k+1)})$. Adding these we see that

$$I(\lambda) = e^{\lambda} \sum_{i=0}^{n} f^{(i)}(0) - \sum_{i=0}^{n} f^{(i)}(\lambda) \tag{10.1.2}$$

We also have the estimate

$$\begin{aligned} |I(t)| &\leqslant \left| \lambda e^{\lambda} \int_0^1 e^{-u\lambda} f(u\lambda)\, du \right| \\ &\leqslant |\lambda| \int_0^1 e^{|(1-u)\lambda|} |f(u\lambda)| du \\ &\leqslant |\lambda| e^{|\lambda|} \int_0^1 |f(u\lambda)| du \\ &\leqslant |\lambda| e^{|\lambda|} \int_0^1 \bar{f}(|u\lambda|) du \\ &\leqslant |\lambda| e^{|\lambda|} \bar{f}(|\lambda|) . \end{aligned} \tag{10.1.3}$$

Theorem 10.1.4. *π is transcendental over $\mathbb{Q}$.*

Proof. Let us assume that π is algebraic over $\mathbb{Q}$. Then so is $i\pi$. Let $\theta = \theta_1 := i\pi$. Let $g(X) \in \mathbb{Q}[X]$ be the monic irreducible polynomial of θ over $\mathbb{Q}$. Let r be the degree of $g(X)$. If $b > 0$ is an integer such that $bg(X) \in \mathbb{Z}[X]$, then it is easy to check that the monic irreducible polynomial of $b\theta$ has coefficients in $\mathbb{Z}$. In fact, this polynomial is precisely $b^r g(X/b)$. This shows that $b\theta$ is an algebraic integer. Let $\theta_1, \theta_2, \ldots, \theta_r$ be the distinct roots of $g(X)$.

Since $e^{i\pi} = -1$, it follows that $e^{\theta_1} + 1 = 0$. Thus, we get

$$(e^{\theta_1} + 1)(e^{\theta_2} + 1) \ldots (e^{\theta_r} + 1) = 0 . \tag{10.1.5}$$

Multiplying out the LHS, we see that the LHS is a sum of terms of the type e^{ϕ}, where each

$$\phi = \epsilon_1 \theta_1 + \ldots + \epsilon_r \theta_r, \qquad \epsilon_i \in \{0, 1\} .$$

Thus, we have 2^r possible expressions as above. Some of these may be 0. Let us assume that $\phi_1, \ldots, \phi_n$ are nonzero and the remaining $2^r - n$ are 0. Let $q := 2^n - r$. Then (10.1.5) becomes

$$q + e^{\phi_1} + \ldots + e^{\phi_n} = 0\,. \tag{10.1.6}$$

It is possible that $\phi_i = \phi_j$, or $e^{\phi_i} = e^{\phi_j}$, for some $i \neq j$.

Let p be a prime (we will choose p precisely later). Consider the polynomial

$$g(Y) = Y^{p-1}(Y - b\phi_1)^p \ldots (Y - b\phi_n)^p\,.$$

Notice that if $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ then σ permutes the θ_i and so also the ϕ_i. This shows that the polynomial $g(X)$ has coefficients in $\mathbb{Q}$. The $b\theta_i$ are algebraic integers since they satisfy a monic polynomial in $\mathbb{Z}[X]$. By Corollary 9.4.7 it follows that $b\phi_i$ are algebraic integers. Again, since the coefficients of $g(X)$ are polynomials in $b\phi_i$, it follows that the coefficients are algebraic integers. By Lemma 9.4.8 it follows that the coefficients are in $\mathbb{Z}$ and so $g(X) \in \mathbb{Z}[X]$. Let

$$f(X) = g(bX)\,.$$

Let $m := (n+1)p - 1$. Then $f(X)$ has degree m.

Define, using definition (10.1.1) with $f(X)$, the integrals I and

$$J := I(\phi_1) + \ldots + I(\phi_n)\,.$$

Using (10.1.2) we get

$$J = -q\sum_{i=0}^{m} f^{(i)}(0) - \sum_{j=1}^{n}\sum_{i=0}^{m} f^{(i)}(\phi_j) = -q\sum_{i=0}^{m} f^{(i)}(0) - \sum_{i=0}^{m}\sum_{j=1}^{n} f^{(i)}(\phi_j)\,. \tag{10.1.7}$$

Note that $f^{(i)}(X) = b^i g^{(i)}(bX)$. Note that $f^{(i)}(\phi_j) = 0$ if $i < p$. If $i \geqslant p$ then $g^{(i)}(X)$ is a polynomial with integer coefficients such that every coefficient is divisible by $p!$. Let us write $g^{(i)}(X) = p!g_i(X)$ with $g_i(X) \in \mathbb{Z}[X]$. Thus, $f^{(i)}(X) = b^i p! g_i(bX)$ Then

$$\sum_{j=1}^{n} f^{(i)}(\phi_j) = b^i p! \sum_{j=1}^{n} g_i(b\phi_j)\,.$$

Again note that in the RHS $\sum_{j=1}^{n} g_i(b\phi_j)$ is invariant under the action of $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Thus, it is in $\mathbb{Q}$ and is also an algebraic integer. Thus, it is in $\mathbb{Z}$.

It follows that if $i \geqslant p$ then $\sum_{j=1}^{n} f^{(i)}(\phi_j)$ is an integer which is divisible by $p!$. Thus, it follows that

$$\sum_{i=0}^{m}\sum_{j=1}^{n} f^{(i)}(\phi_j)$$

is an integer which is divisible by $p!$.

Next let us look at the term $\sum_{i=0}^{m} f^{(i)}(0)$. Again, it is clear that if $i < p-1$ then $f^{(i)}(0) = 0$. If $i \geqslant p$ then $f^{(i)}(0)$ is an integer divisible by $p!$. For $i = p-1$ we have

$$f^{(p-1)}(0) = b^{p-1}g^{(p-1)}(0) = b^{p-1}(-1)^n(p-1)!(b\phi_1 \dots b\phi_n)^p \,.$$

As before, it follows that $(b\phi_1 \dots b\phi_n) \in \mathbb{Z}$. It follows that $f^{(p-1)}(0)$ is an integer which is divisible by $(p-1)!$, but not by p if p is chosen larger than $(b\phi_1 \dots b\phi_n)$. Thus, it follows that if p is chosen very large then $(p-1)!$ divides $q\sum_{i=0}^{m} f^{(i)}(0)$, but not p. We conclude that if $p \gg 0$ then J is not divisible by p but it is divisible by $(p-1)!$. This shows that $|J| \geqslant (p-1)!$.

Next let use use (10.1.3) to estimate the absolute value of J.

$$\begin{aligned} |J| &\leqslant \sum_{i=1}^{n} |I(\phi_i)| \\ &\leqslant \sum_{i=1}^{n} |\phi_i| e^{|\phi_i|} \bar{f}(|\phi_i|) \end{aligned}$$

Note that

$$\bar{f}(|\lambda|) \leqslant b^{np}|\lambda|^{p-1}(|\lambda| + |\phi_1|)^p \dots (|\lambda| + |\phi_n|)^p \,.$$

If $\mu = \max\{|\phi_i|\}$ then

$$\bar{f}(|\phi_i|) \leqslant (2b)^{np}\mu^{p-1}\mu^{np} \,.$$

Thus, we get that

$$(p-1)! \leqslant |J| \leqslant n\mu e^{\mu}(2b)^{np}\mu^{p-1}\mu^{p^2} = ne^{\mu}(2b)^{np}\mu^{np+p} \,.$$

This gives a contradiction when $p \gg 0$ (by Sterling's formula, after taking log, the LHS is of order $(p-1)\,log\,(p-1)$, while the RHS is of order $p\,log\,c$ for some constant c). This shows that π is transcendental over $\mathbb{Q}$. $\square$

10.2 Lindemann-Weierstrass Theorem

Recall the Fundamental Theorem of Symmetric Polynomials, see Remark 8.2.5. Let F be a field and let $A := F[X_1, \ldots, X_n]$ denote the polynomial ring in n variables. Let R be the ring $A[Y_1, \ldots, Y_n]$. For $\sigma \in S_n$, we have an automorphism of R, defined as identity on A and which sends Y_i to $Y_{\sigma(i)}$. We denote this automorphism by $\tilde{\sigma}$.

Lemma 10.2.1. *Consider the product $g := \prod_{\sigma \in S_n}(X_1 Y_{\sigma(1)} + \ldots + X_n Y_{\sigma(n)})$. For a monomial M in the Y_i, say $Y_1^{j_1} Y_2^{j_2} \ldots Y_n^{j_n}$, let $a_M \in A$ denote the coefficient of M in the above product. Then $a_M = a_{\tilde{\sigma}(M)}$.*

Proof. Let $S_i(Y)$ denote the i^{th} elementary symmetric polynomial in the Y_i. By the Fundamental Theorem on symmetric polynomials, it follows that the product g is a sum of elements of the type

$$\alpha := a S_1(Y)^{j_1} S_2(Y)^{j_2} \ldots S_n(Y)^{j_n},$$

where $a \in A$ and $j_i \geqslant 0$ are integers. If M is a monomial in the Y_i which appears in the above expression, then so does $\tilde{\sigma}(M)$ and clearly both these have the same coefficient, which will be some integer times a. Since g is a sum of elements of the above type, we may write it as a finite sum $g = \sum_j \alpha_j$. The given monomial M, if it appears in α_j, with coefficient $a_{M,j}$ then $\tilde{\sigma}(M)$ also appears in α_j with coefficient $a_{M,j}$. As the coefficient of M in g is $\sum_j a_{M,j}$, the Lemma follows. □

10.2.2. Lexicographic order on $\mathbb{C}$. Define a total order on $\mathbb{C}$ as follows. Let $\alpha \neq \beta \in C$. We say $\alpha > \beta$ if one of the following two holds

- $\mathrm{Re}(\alpha) > \mathrm{Re}(\beta)$, or
- $\mathrm{Re}(\alpha) = \mathrm{Re}(\beta)$ and $\mathrm{Im}(\alpha) > \mathrm{Im}(\beta)$.

It is clear that this defines a total order on $\mathbb{C}$. Moreover, the following Lemma is clear.

Lemma 10.2.3. *If $\alpha_1 > \beta_1$ and $\alpha_2 > \beta_2$ then $\alpha_1 + \alpha_2 > \beta_1 + \beta_2$.*

The first step in the proof of the Lindemann-Weierstrass Theorem is the following reduction.

Lemma 10.2.4. *Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be distinct algebraic integers. Suppose e^{α_i} are linearly dependent over $\bar{\mathbb{Q}}$, that is, there is a relation $\sum_{i=1}^{n} \beta_i e^{\alpha_i} = 0$, where $\beta_i \in \bar{\mathbb{Q}}$ and $\beta_i \neq 0$. Then there exist distinct algebraic integers $\alpha'_1, \ldots, \alpha'_m$ such that $e^{\alpha'_i}$ are linearly dependent over $\mathbb{Q}$.*

Proof. Let K be a finite Galois extension containing all the β_i. Consider the ring $R := K[X_1, X_2, \ldots, X_n]$. For every $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ we have an automorphism $\tilde{\sigma}$ of R which acts on the coefficients by σ and sends X_i to X_i. Consider product

$$g(X_1, \ldots, X_n) := \prod_{\sigma \in \mathrm{Gal}(K/\mathbb{Q})} \tilde{\sigma}(\beta_1 X_1 + \ldots + \beta_n X_n)\,. \tag{10.2.5}$$

Clearly, this product is an element in $\mathbb{Q}[X_1, \ldots, X_n]$. This is obviously a nonzero polynomial and so we may write it as

$$g(X) := \sum_{\underline{a} \in (\mathbb{Z}_{\geqslant 0})^n} \gamma_{\underline{a}} X^{\underline{a}}, \qquad \gamma_{\underline{a}} \in \mathbb{Q}\,.$$

Here $\underline{a} = (a_1, \ldots, a_n)$ and $X^{\underline{a}} = X_1^{a_1} \ldots X_n^{a_n}$. Moreover, $\sum a_i = [K : \mathbb{Q}] =: r$. Let I denote the set of such indices $\underline{a}$ which can appear in the above sum.

The evaluation $g(e^{\alpha_1}, \ldots, e^{\alpha_n})$ is 0 since one of the terms in the product (10.2.5) evaluates to 0. Note that the monomial $X^{\underline{a}}$ evaluates to $e^{\sum a_i \alpha_i}$. Thus, we get an equation

$$\sum_{\underline{a} \in I} \gamma_{\underline{a}} e^{\sum a_i \alpha_i} = 0\,. \tag{10.2.6}$$

It is tempting to conclude that this gives the relation we are looking for. However, we still need to check that this is a nontrivial relation. For example, we could have an expression of the type

$$\gamma_1 M_1 + \gamma_2 M_2 + \ldots + \gamma_5 M_5\,,$$

where the $\gamma_i \in \mathbb{Q}$ and M_i are monomials $X^{\underline{a}}$. Let Θ denote the evaluation map, which sends $X_i \mapsto e^{\alpha_i}$. Then it may happen that $\Theta(M_1) = \Theta(M_2)$ and $\Theta(M_3) = \Theta(M_4) = \Theta(M_5)$ and $\gamma_1 + \gamma_2 = 0$ and $\gamma_3 + \gamma_4 + \gamma_5 = 0$. Then after evaluating we do not get a nontrivial relation. We need to show that after evaluation, such a cancellation of the coefficients does not happen. For

example, this will be the case if we can show that $\gamma_1 \neq 0$ and $\Theta(M_1) \neq \Theta(M_i)$ for $i \neq 1$.

We claim that if $\sum a_i\alpha_i \neq \sum b_i\alpha_i$ then $e^{\sum a_i\alpha_i} \neq e^{\sum b_i\alpha_i}$. If not, then we will have that $\sum_j \alpha_j(a_j - b_j) = 2i\pi n$ for some nonzero integer n. But this would imply that π is algebraic over $\mathbb{Q}$. This proves the claim.

We are now ready to prove the Lemma. Consider the evaluation of (10.2.5)

$$\prod_{\sigma\in \mathrm{Gal}(K/\mathbb{Q})} (\sigma(\beta_1)e^{\alpha_1} + \ldots + \sigma(\beta_n)e^{\alpha_n})\,.$$

Let α_1 be the largest among the α_i in the lexicographic order. Then the coefficient of $e^{r\alpha_1}$ is nonzero. Moreover, $r\alpha_1 > \sum a_i\alpha_i$ for every $\underline{a} \neq (r, 0, \ldots, 0)$. From the preceding para it follows that the value $e^{r\alpha_1}$ occurs only once in the expression (10.2.6) and it appears with a nonzero coefficient. This is the relation we are looking for. □

The next step in the proof is the following reduction.

Lemma 10.2.7. *Let $\alpha_1, \alpha_2, \ldots, \alpha_n$ be distinct algebraic integers. Suppose e^{α_i} are linearly dependent over $\mathbb{Q}$. Then there exists a set of distinct algebraic integers $\{\alpha'_1, \ldots, \alpha'_m\}$, which is left invariant by $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$, and a relation $\sum_{i=1}^m \gamma_i e^{\alpha'_i} = 0$ such that if α'_i and α'_j are conjugates then $\gamma_i = \gamma_j$.*

Proof. Again, we shall use a certain polynomial and evaluate it to get our result.

First, we can enlarge the set of α_i (by adding conjugates) and assume that the set $\alpha_1, \alpha_2, \ldots, \alpha_n$ is invariant under $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Then e^{α_i} are linearly dependent over $\mathbb{Q}$. Let $\sum \beta_i e^{\alpha_i} = 0$ be such a relation. Some of the β_i may be 0 now.

Consider the ring $\mathbb{Q}[X_1, \ldots, X_n, Y_1, \ldots, Y_n]$. Let g denote the polynomial in the Lemma 10.2.1, that is,

$$g = \prod_{\sigma\in S_n} (X_1Y_{\sigma(1)} + \ldots + X_nY_{\sigma(n)})\,.$$

Then g can be written as a sum of monomials in Y_i,

$$g = \sum_{M = Y_1^{j_1}Y_2^{j_2}\ldots Y_n^{j_n}} a_M Y_1^{j_1}Y_2^{j_2}\ldots Y_n^{j_n} \qquad a_M \in \mathbb{Q}[X_1, \ldots, X_n]\,. \tag{10.2.8}$$

Note that $\sum j_i = n!$. We evaluate g by putting $X_i \mapsto \beta_i$ and $Y_i \mapsto e^{\alpha_i}$. Let us denote this evaluation map by $\Theta : \mathbb{Q}[X_1, \ldots, X_n, Y_1, \ldots, Y_n] \to \mathbb{C}$.

Since one of the elements in the product, namely, $\sum \beta_i e^{\alpha_i} = 0$, it follows that the evaluation is 0. We claim that $\Theta(g)$ is the relation we are looking for. We need to check that this is a nontrivial relation and it has the property mentioned in the statement of the Lemma.

First we check that this is a nontrivial relation. The evaluation $\Theta(g)$ is the product

$$\prod_{\sigma \in S_n} \left(\beta_1 e^{\alpha_{\sigma(1)}} + \ldots + \beta_n e^{\alpha_{\sigma(n)}}\right). \tag{10.2.9}$$

When we open this out, this is a sum of terms, where each term looks like

$$\beta e^{\sum_\sigma \alpha_{\sigma(l_\sigma)}}, \qquad \beta \in \mathbb{Q}.$$

For each $\sigma \in S_n$, consider the expression

$$N_\sigma := \beta_1 e^{\alpha_{\sigma(1)}} + \ldots + \beta_n e^{\alpha_{\sigma(n)}}.$$

Then $\Theta(g)$ is the product of N_σ as σ varies. In N_σ, consider the set T of those i for which the coefficient of e^{α_i} in N_σ (that is, $\beta_{\sigma^{-1}(i)}$) is nonzero. There is a unique j_σ (which depends on σ) such that $\beta_{\sigma^{-1}(i)}$ is nonzero and for which $\alpha_{\sigma(j)}$ is largest in the lexicographic order in the set $\{\alpha_i \mid i \in T\}$. Let us write the product of these $e^{\alpha_{j_\sigma}}$, as σ varies, as e^δ. Then $\delta = \sum_\sigma \alpha_{j_\sigma}$.

If $e^{\delta'}$ is another term with nonzero coefficient which appears when we open out (10.2.9), then $\delta' = \sum_\sigma \alpha_{l_\sigma}$. For each σ, we have $\alpha_{j_\sigma} > \alpha_{l_\sigma}$ in the lexicographic order. In view of Lemma 10.2.3, it follows that $\delta > \delta'$. In particular, $\delta \neq \delta'$. It follows that $e^\delta \neq e^{\delta'}$ or else we get that π is algebraic over $\mathbb{Q}$, as both δ and δ' are algebraic over $\mathbb{Q}$. It follows that the coefficient of e^δ cannot get cancelled off. Thus, the relation is a nontrivial one.

Finally we have to show that this relation satisfies that property stated in the Lemma. Observe that every term $e^{\delta'}$ appears as $\Theta(M)$ for some monomial M. The coefficient of $e^{\delta'}$ is

$$\sum_{\Theta(M) = e^{\delta'}} \Theta(a_M).$$

Let $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Then σ defines a permutation of the α_i, which also we denote by σ. Let $M = Y_1^{j_1} \dots Y_n^{j_n}$. Then $\Theta(M) = e^{\sum j_i \alpha_i}$. Note that

$$\begin{aligned}\Theta(\tilde{\sigma}(M)) &= \Theta(Y_{\sigma(1)}^{j_1} \dots Y_{\sigma(n)}^{j_n}) \\ &= e^{\sum j_i \alpha_{\sigma(i)}} \\ &= e^{\sigma(e^{\sum j_i \alpha_i})}\,.\end{aligned}$$

Using this one easily checks that $\Theta(M) = e^{\delta'}$ iff $\Theta(\tilde{\sigma}(M)) = e^{\sigma(\delta')}$. By Lemma 10.2.1 the coefficient of $\tilde{\sigma}(M)$ in (10.2.8) is $a_{\tilde{\sigma}(M)} = a_M$. Thus, the coefficient of $e^{\sigma(\delta')}$ is

$$\begin{aligned}\sum_{\Theta(M)=e^{\sigma(\delta')}} \Theta(a_M) &= \sum_{\Theta(N)=e^{\delta'}} \Theta(a_{\tilde{\sigma}(N)}) \\ &= \sum_{\Theta(N)=e^{\delta'}} \Theta(a_N)\end{aligned}$$

This shows that the coefficients of $e^{\delta'}$ and $e^{\sigma(\delta')}$ are the same. This completes the proof of the Lemma. □

We are now ready to prove the Lindemann-Weierstrass Theorem.

Theorem 10.2.10 (Lindemann-Weierstrass)**.** *Let $\alpha_1, \dots, \alpha_n$ be distinct elements in $\bar{\mathbb{Q}}$. Then $e^{\alpha_1}, \dots, e^{\alpha_n}$ are linearly independent over $\bar{\mathbb{Q}}$.*

Proof. Let us assume that these are linearly dependent over $\bar{\mathbb{Q}}$. Applying Lemma 10.2.4 and Lemma 10.2.7 we may assume that there are distinct elements $\alpha_1, \dots, \alpha_n \in \bar{\mathbb{Q}}$ such that this collection is left invariant under $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ and there is a nontrivial relation $\sum_i \beta_i \alpha_i$, with $\beta_i \in \mathbb{Q}$, such that if α_i and α_j are conjugates then $\beta_i = \beta_j$. We renumber the α_i so that $\alpha_1, \alpha_2, \dots, \alpha_{n_1}$ are conjugates, $\alpha_{n_1+1}, \alpha_{n_1+2}, \dots, \alpha_{n_2}$ are conjugates, and so on. Thus,

$$\beta_{n_i+1} = \beta_{n_1+2} = \dots = \beta_{n_{i+1}}\,.$$

Let

$$\rho : \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{Aut}(\alpha_1, \dots, \alpha_n) \cong S_n$$

denote the permutation representation. Thus,

$$\beta_k = \beta_{\rho(\sigma)(k)}\,. \tag{10.2.11}$$

Let b be a positive integer such that $b\beta_i$ are integers and $b\alpha_i$ are algebraic integers. Define, for a prime p (to be made precise later)

$$g_i(X) := \frac{(Y - b\alpha_1)^p \dots (Y - b\alpha_n)^p}{(Y - b\alpha_i)} .$$

Let

$$f_i(X) := g_i(bX) \in \bar{\mathbb{Q}}[X] .$$

Recall that for $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ we have the automorphism $\tilde{\sigma} : \bar{\mathbb{Q}}[X] \to \bar{\mathbb{Q}}[X]$. Then $\tilde{\sigma}(f_i(X)) = f_{\rho(\sigma)(i)}(X)$.

Recall the definition of I from (10.1.1). For $\lambda \in \mathbb{C}$, let $I_i(\lambda) = I(\lambda, f_i)$. Let

$$J_i := \beta_1 I_i(\alpha_1) + \beta_2 I_i(\alpha_2) + \ldots + \beta_n I_i(\alpha_n) .$$

Using (10.1.2) we have that

$$\begin{aligned} J_i &= \sum_{k=1}^{n} \beta_k I_i(\alpha_k) \\ &= \sum_{k=1}^{n} \beta_k \left(e^{\alpha_k} \sum_{l=0}^{np-1} f_i^{(l)}(0) - \sum_{l=0}^{np-1} f_i^{(l)}(\alpha_k) \right) \\ &= -\sum_{k=1}^{n} \beta_k \sum_{l=0}^{np-1} f_i^{(l)}(\alpha_k) \\ &= -\sum_{l=0}^{np-1} \sum_{k=1}^{n} \beta_k f_i^{(l)}(\alpha_k) . \end{aligned}$$

Note that if $\sigma \in \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ then using (10.2.11) we get

$$\begin{aligned} \sigma(J_i) &= -\sum_{l=0}^{np-1} \sum_{k=1}^{n} \beta_k \sigma(f_i^{(l)}(\alpha_k)) \\ &= -\sum_{l=0}^{np-1} \sum_{k=1}^{n} \beta_k f_{\rho(\sigma)(i)}^{(l)}(\alpha_{\rho(\sigma)(k)}) \\ &= -\sum_{l=0}^{np-1} \sum_{k=1}^{n} \beta_{\rho(\sigma)(k)} f_{\rho(\sigma)(i)}^{(l)}(\alpha_{\rho(\sigma)(k)}) \\ &= J_{\rho(\sigma)(i)} . \end{aligned} \tag{10.2.12}$$

Next observe that if $l < p-1$ then $g_i^{(l)}(b\alpha_k) = 0$. This shows that if $l < p-1$ then $f_i^{(l)}(b\alpha_k) = 0$. If $l \geqslant p$ then $g_i^{(l)}(b\alpha_k) = p!\delta$, where δ is an algebraic integer. Thus, if $l \geqslant p$ then $f_i^{(l)}(\alpha_k) = b^l g_i^{(l)}(b\alpha_k) = b^l p!\delta$. Similarly, if $l = p-1$ then $f_i^{(p-1)}(\alpha_k) = b^{p-1} g_i^{(p-1)}(b\alpha_k) = 0$ if $k \neq i$ and

$$f_i^{(p-1)}(\alpha_i) = b^{p-1} g_i^{(p-1)}(b\alpha_i) = b^{p-1}(p-1)! \prod_{k\neq i}(b\alpha_k - b\alpha_i) \neq 0\,.$$

Combining these observations, we may write

$$\begin{aligned} J_i &= -\sum_{l=0}^{np-1}\sum_{k=1}^{n} \beta_k f_i^{(l)}(\alpha_k) = -\sum_{l=p-1}^{np-1}\sum_{k=1}^{n} \beta_k f_i^{(l)}(\alpha_k) \\ &= \beta_i f_i^{(p-1)}(\alpha_i) - \sum_{l=p}^{np-1}\sum_{k=1}^{n} \beta_k f_i^{(l)}(\alpha_k) \\ &= \beta_i b^{p-1} g_i^{(p-1)}(b\alpha_i) - \sum_{l=p}^{np-1}\sum_{k=1}^{n} \beta_k b^l g_i^{(l)}(b\alpha_k) \\ &= (p-1)!\delta_{i,1} + p!\delta_{i,2}\,, \end{aligned}$$

where $\delta_{i,1} = b^{p-1}\prod_{k\neq i}(b\alpha_k - b\alpha_i) \neq 0$ and $\delta_{i,2}$ are algebraic integers. Further note that

$$\sigma(\beta_i f_i^{(p-1)}(\alpha_i)) = \beta_{\rho(\sigma)(i)} f_{\rho(\sigma)(i)}^{(p-1)}(\alpha_{\rho(\sigma)(i)})\,.$$

This shows that $(p-1)!\delta_{i,1} = (p-1)!\delta_{\rho(\sigma)(i),1}$. As this equality holds in $\bar{\mathbb{Q}}$, we get that $\delta_{i,1} = \delta_{\rho(\sigma)(i),1}$. Using (10.2.12) we get $\delta_{i,2} = \delta_{\rho(\sigma)(i),2}$.

Now consider the product

$$\prod_{i=1}^{n} J_i = (p-1)!^n \prod_{i=1}^{n}(\delta_{i,1} + p\delta_{i,2})\,.$$

The product in the RHS is invariant under the Galois group and also an algebraic integer. Thus, it is an integer. It follows that $\prod_{i=1}^n J_i$ is an integer. Again, using similar arguments, it is easily checked that

$$\prod_{i=1}^{n}(\delta_{i,1} + p\delta_{i,2}) - \prod_{i=1}^{n}\delta_{i,1}$$

is an integer which is divisible by p. Thus, we get that

$$\prod_{i=1}^{n} J_i = (p-1)!^n \left(\prod_{i=1}^{n} \delta_{i,1} + p\tilde{\delta}_2 \right) .$$

Note that if $p \gg 0$ then p does not divide

$$\prod_{i=1}^{n} \delta_{i,1} = \prod_{i=1}^{n} \left(b^{p-1} \prod_{k \neq i} (b\alpha_k - b\alpha_i) \right) .$$

It follows that p does not divide $\prod_{i=1}^{n} J_i$ and so $\prod_{i=1}^{n} J_i \neq 0$. Thus, we get using (10.1.3)

$$(p-1)! \leqslant |J| \leqslant \max_i |J_i|^n \leqslant \max_{i,j} |n\beta_j I_i(\alpha_j)|^n \leqslant c c_1^p .$$

Here c, c_1 are constants independent of p. This gives a contradiction when $p \gg 0$. This completes the proof of the Theorem. □

Chapter 11

The Agrawal-Kayal-Saxena Algorithm

In this chapter we give a detailed exposition of the result of Agrawal, Kayal and Saxena. The reader who is not familiar with this result may find the following wiki article interesting.
`https://en.wikipedia.org/wiki/AKS_primality_test`
The proof uses results which we have seen in these notes. The last three sections of this chapter have been written keeping in mind people who have had no exposure to complexity theory. In particular, the bound on time complexity for A-K-S which we demonstrate is far from optimal. The last two sections briefly explain the class of problems **P** and **NP**. Both these sections are very informal. The reader interested in a rigorous exposition using terminology which is standard amongst computer scientists must consult other references. The original paper can be found here:
`https://www.cse.iitk.ac.in/users/manindra/algebra/primality_v6.pdf`

This chapter was written in collaboration with Aryaman Maithani. I thank him for his interest and enthusiasm. I also thank Swayam Shashank Chube for some interesting discussions.

11.1 Preliminaries

Lemma 11.1.1. *For* $N \geqslant 7$, $\mathrm{LCM}(N) \geqslant 2^N$.

Proof. For ease of notation denote by $l_n := \mathrm{LCM}(n)$. For $1 \leqslant m \leqslant n$, consider the following integral

$$I_{m,n} = \int_0^1 x^{m-1}(1-x)^{n-m}dx\,.$$

A direct computation yields

$$\begin{aligned} I_{m,n} &= \int_0^1 x^{m-1}(1-x)^{n-m}dx \\ &= \int_0^1 x^{m-1}\left(\sum_{r=0}^{n-m} {}^{n-m}C_r(-1)^r x^r\right)dx \\ &= \sum_{r=0}^{n-m}(-1)^r\,{}^{n-m}C_r \int_0^1 x^{m+r-1}dx \\ &= \sum_{r=0}^{n-m}(-1)^r\,{}^{n-m}C_r \frac{1}{m+r} \end{aligned}$$

Note that $m+r$ divides l_n for all $0 \leqslant r \leqslant n-m$ and so $I_{m,n}\cdot l_n \in \mathbb{N}$. Let $k_{n,m} := I_{m,n}l_n$. On the other hand, one may evaluate the integral using integration by parts repeatedly to obtain

$$\begin{aligned} I_{m,n} &= \int_0^1 x^{m-1}(1-x)^{n-m}dx \\ &= \frac{m-1}{n-m+1}\int_0^1 x^{m-2}(1-x)^{n-m+1}dx \\ &\vdots \\ &= \frac{(m-1)(m-2)\cdots 1}{(n-m+1)(n-m+2)\cdots(n-1)}\int_0^1 (1-x)^{n-1}dx \\ &= \frac{(n-m)!(m-1)!}{(n-1)!}\cdot\frac{1}{n} \\ &= \frac{(n-m)!(m-1)!}{(n-1)!}\cdot\frac{m}{n}\cdot\frac{1}{m} \\ &= \frac{1}{m\cdot\,{}^nC_m}. \end{aligned}$$

From the above we get that

$$k_{n,m}m \cdot {}^nC_m = I_{m,n}l_n m \cdot {}^nC_m = l_n\,.$$

This shows that $(m \cdot {}^nC_m)|l_n$ for all $1 \leqslant m \leqslant n$. In particular, $(n \cdot {}^{2n}C_n)|l_{2n}$ and $((n+1)\cdot {}^{2n+1}C_{n+1})|l_{2n+1}$. But note that $(n+1)\cdot {}^{2n+1}C_{n+1} = (2n+1)\cdot {}^{2n}C_n$, and so this shows that $((2n+1)\cdot {}^{2n}C_n)|l_{2n+1}$. Since $l_{2n}|l_{2n+1}$, we see that both $(2n+1)\cdot {}^{2n}C_n$ and $n\cdot {}^{2n}C_n$ divide l_{2n+1}. As $(n, 2n+1) = 1$, we deduce that $(n(2n+1)\cdot {}^{2n}C_n)|l_{2n+1}$. Thus,

$$l_{2n+1} \geqslant n(2n+1)\cdot {}^{2n}C_n\,.$$

Now note that ${}^{2n}C_n$ is larger than each of the $2n+1$ terms in the binomial expansion of $(1+1)^{2n}$. Thus, $(2n+1)\cdot {}^{2n}C_n \geqslant (1+1)^{2n} = 2^{2n}$. Thus, we get that

$$l_{2n+1} \geqslant n2^{2n}\,.$$

If $n \geqslant 2$ then we have

$$l_{2n+1} \geqslant 2\cdot 2^{2n} = 2^{2n+1}\,.$$

Moreover, if $n \geqslant 4$, then we have

$$l_{2n+2} \geqslant l_{2n+1} \geqslant n2^{2n} \geqslant 4\cdot 2^{2n} = 2^{2n+2}\,.$$

Thus, for $N \geqslant 9$, we have $l_N \geqslant 2^N$. For $N = 7, 8$ one can verify that $l_8 = 840 > 2^8$ and $l_7 = 420 > 2^7$. This proves the lemma. □

Lemma 11.1.2. *Let $n \geqslant 2$. There is an $r > 0$ such that*

(i) $(r, n) = 1$,

(ii) $o_r(n) > \log^2(n)$, *and*

(iii) $r \leqslant \max\{3, \lceil \log^5(n)\rceil\}$. *(Define $B := \lceil \log^5(n)\rceil$)*

Proof. When $n = 2$: $r = 3$ satisfies all conditions. Assume that $n > 2$. Let r_0 be the smallest positive integer which does not divide

$$N_0 := n^{\lfloor \log(B)\rfloor}\cdot \prod_{i=1}^{\lfloor \log^2(n)\rfloor}(n^i - 1)\,.$$

Step 1. We claim that r_0 has to be a prime power. If not, let us assume that $r_0 = ab$ where $(a, b) = 1$. Then since both $a, b < r_0$ it follows that both of them divide N_0. But since they are coprime it follows that their product, that is, r_0 divides N_0. Thus, r_0 has to be a prime power.

Step 2. Let us first consider the case when $r_0 \geqslant 8$. In this case $r_0 - 1 \geqslant 7$ and so $LCM(r_0 - 1)$ divides N_0. Now, note the following estimate:

$$N_0 = n^{\lfloor \log B \rfloor} \cdot \prod_{i=1}^{\lfloor \log^2 n \rfloor} (n^i - 1) < n^{\lfloor \log B \rfloor + \frac{1}{2} \log^n \cdot (\log^2 n - 1)} \leqslant n^{\log^4 n} \leqslant 2^{\log^5 n} \leqslant 2^B.$$

Using this and the above lemma on LCM, we see that $2^{r_0 - 1} < 2^B$. This shows that $r_0 \leqslant B$. From the previous step we may write $r_0 = p^a$. We next show that p does not divide n. Contrary to this assume that p divides n. Then this means that $p^{\lfloor \log(B) \rfloor}$ divides $n^{\lfloor \log(B) \rfloor}$. But as $r_0 = p^a$ does not divide N_0, it follows that $a > \lfloor \log(B) \rfloor$. On the other hand, taking logarithm of $r_0 = p^a \leqslant B$ one sees that $a \leqslant \lfloor \log(B) \rfloor$. This gives a contradiction. Thus, p does not divide n. It follows r_0 and n are coprime. Thus, if $r_0 \geqslant 8$, then the lemma follows by taking $r = r_0$.

Step 3. Consider the case when $r_0 \leqslant 7$. Clearly, 2 divides N_0. Thus, the only possibilities for r_0 are $r_0 = 3, 4, 5, 7$. If $r_0 \in \{3, 5, 7\}$ then again, since $B > 10$, all three assertions in the lemma follow by taking $r = r_0$. We claim $r = 4$ is not possible. Since $n > 2$, we have $\lfloor \log^2(n) \rfloor \geqslant 2$. If n is odd, then 4 divides N_0. If n is even then 4 divides N_0 since $\lfloor \log(B) \rfloor \geqslant 3$. This completes the proof of the lemma. □

Lemma 11.1.3. *Let $n \in \mathbb{N}$ and q be a prime factor of n. Suppose k is the largest natural number such that $q^k | n$. Then $q^k \nmid {}^nC_q$.*

Proof. Write $n = q^k m$ where $m \in \mathbb{N}$ such that $q \nmid m$.

$$\begin{aligned} {}^nC_q &= \frac{n(n-1)\cdots(n-(q-1))}{q(q-1)\cdots 1} \\ &= q^{k-1} m \frac{(n-1)(n-2)\cdots(n-(q-1))}{(q-1)(q-2)\cdots 1}. \end{aligned}$$

Note that $q \nmid m$. Moreover, no term of $n-1,\ n-2, \ldots, n-(q-1)$ is divisible by q as they are the $q-1$ terms between the successive multiples $n-q$ and n of q. Thus, $q^k \nmid {}^nC_q$. □

Lemma 11.1.4. *Let $a \in \mathbb{Z}$, $n \in \mathbb{N}$, $n \geqslant 2$ and $(a, n) = 1$. Then n is prime if and only if*

$$(X + a)^n = X^n + a \qquad \bmod n.$$

The above equality is to be interpreted as the equality of two elements of $(\mathbb{Z}/n\mathbb{Z})[X]$.

Proof. Suppose n is prime. We show that the equality holds. Indeed, we have $(X + a)^n = X^n + a^n$ in $(\mathbb{Z}/n\mathbb{Z})[X]$. Moreover, $(a, n) = 1$ tells us that $a^{n-1} = 1$ and hence, $a^n = a$, as desired.

Conversely, suppose that n is composite. Consider a prime factor q of n. Let k be the largest natural number such that $q^k | n$. Then by Lemma 11.1.3, q^k does not divide ${}^nC_q$. Further, since $(a, n) = 1$ it follows that q does not divide a and so q^k is coprime to a^{n-q}. However, note that the coefficient of X^q in $(X + a)^n - X^n - a$ is ${}^nC_q\, a^{n-q}$. This shows that $(X + a)^n - X^n - a$ is not the zero polynomial of $(\mathbb{Z}/n\mathbb{Z})[X]$ and thus we are done. □

11.2 The Algorithm

Input: integer n > 1
1. If ($n = a^b$ for some $a \in \mathbb{N}_{>1}$ and some $b > 1$), output COMPOSITE.
2. Find the smallest r such that $(r, n) = 1$ and $o_r(n) > \log^2 n$.
3. If $1 < (a, n) < n$ for some $a \leqslant r$, output COMPOSITE.
4. If $n \leqslant r$, output PRIME.
5. For $a = 1$ to $\lfloor \sqrt{\phi(r)} \log n \rfloor$ do
   if $(X + a)^n \neq X^n + a$ (mod $X^r - 1, n$), output COMPOSITE.
6. Output PRIME.

Proposition 11.2.1. *The above algorithm terminates in finitely many steps. It necessarily outputs exactly one of "COMPOSITE" or "PRIME".*

Proof. From Lemma 11.1.2, it follows that Step 2 terminates in finitely many steps. All the other steps terminate in finitely many steps. The second assertion is clear. Thus, the proposition follows. □

11.3 Proof of Correctness

Next we will show that if the algorithm outputs `COMPOSITE` then n is composite and if it outputs `PRIME` then n is prime.

11.3.1. Some easy preliminaries.

Lemma 11.3.2. *If the algorithm outputs `COMPOSITE`, then n is composite.*

Proof. Suppose the algorithm outputs `COMPOSITE`. This is possible only in Steps 1, 3, and 5. If this happens in Step 1 then clearly n is composite as $n = a^b$ for some $a, b \in \mathbb{N}$ and $b > 1$. If this happens in Step 3 then clearly n is composite as it has a divisor strictly between 1 and itself. If this happens in Step 5 then n is composite by Lemma 11.1.4. □

Lemma 11.3.3. *If the algorithm returns `PRIME` in Step 4, then n is prime.*

Proof. Suppose n is not prime. Let $p < n$ be a prime factor of n. Then since $n \leqslant r$ we have $p \leqslant r$ and $1 < (p, n) = p < n$. But then Step 3 would have returned `COMPOSITE` and the algorithm would have terminated, a contradiction. □

For the rest of this section** $n > 1$ **is such that the algorithm returns `PRIME` in Step 6. In particular, this implies that the algorithm did not terminate in Steps 3, 4 or 5.

Remark 11.3.4. Since $o_r(n) > 1$, there exists a prime divisor p of n such that $o_r(p) > 1$.

Lemma 11.3.5. $p > r$.

Proof. Indeed, if $p \leqslant r$, then the algorithm would have terminated in Step 3 or 4. □

Lemma 11.3.6. $(n, r) = 1$.

Proof. Assume that $(n, r) > 1$. Consider $a = r$ in Step 3. As the algorithm did not terminate by Step 3, we must have that $(r, n) \geqslant n$. This gives us that $(r, n) = n$ or $n \mid r$. However, this means that $n \leqslant r$ and thus, the algorithm would terminate at Step 4. □

11.3.7. Digression.

Thus, $(n, r) = 1$ and hence, $(p, r) = 1$. This shows that $p, n \in (\mathbb{Z}/r\mathbb{Z})^\times$. Let $l := \lfloor \sqrt{\phi(r)} \log n \rfloor$.

We fix p, r, and l for the rest of the section.

Step 5 of the equation verified l equations and did not output `COMPOSITE`, thus we must have the following:

$$(X + a)^n = X^n + a \pmod{X^r - 1, n}$$

for all $0 \leqslant a \leqslant l$. (Step 5 didn't check for $a = 0$ but it is obviously satisfied.) As $p|n$, the above implies:

$$(X + a)^n = X^n + a \pmod{X^r - 1, p} \tag{11.3.8}$$

for all $0 \leqslant a \leqslant l$. This is same as saying that $X^r - 1$ divides $(X+a)^n - X^n - a$ in $\mathbb{F}_p[X]$ for every a in the range $0 \leqslant a \leqslant l$. By Lemma 11.1.4, we have that

$$(X + a)^p = X^p + a \pmod{X^r - 1, p}$$

for all $0 \leqslant a \leqslant l$.

Lemma 11.3.9.

$$(X + a)^{\frac{n}{p}} = X^{\frac{n}{p}} + a \pmod{X^r - 1, p}$$

for all $0 \leqslant a \leqslant l$.

Proof. Let $g(X) = (X+a)^{\frac{n}{p}} - X^{\frac{n}{p}} - a$ and $f(X) = X^r - 1$ in the ring $\mathbb{F}_p[X]$. We wish to show that $f(X)$ divides $g(X)$ in $\mathbb{F}_p[X]$. Since $(p, r) = 1$, applying Lemma 5.1.1 we see that $f(X)$ is separable. However, note that

$$g(X)^p = (X + a)^n - X^n - a\,.$$

By (11.3.8) we see that $f(X)$ divides $g(X)^p$. As $f(X)$ is separable, this forces that $f(X)$ divides $g(X)$. □

Observing this property leads to the following definition.

Definition 11.3.10. *For a polynomial $g(X)$ and a natural number m, we say that m is* introspective *for $g(X)$ if*

$$g(X)^m = g(X^m) \pmod{X^r - 1, p}.$$

Remark 11.3.11. Thus, from the previous observations, it is clear that both $\frac{n}{p}$ and p are introspective for $X + a$ when $0 \leqslant a \leqslant l$.

We now show two closure properties.

Lemma 11.3.12. *If m and m' are introspective numbers for $g(X)$, then so is $m \cdot m'$.*

Proof. As before denote by $f(X) = X^r - 1 \in \mathbb{F}_p[X]$. By hypothesis, $f(X)$ divides $g(X)^m - g(X^m)$. This implies that $f(X^{m'})$ divides $g(X^{m'})^m - g(X^{mm'})$.

$$\begin{aligned} g(X^{m'})^m - g(X^{mm'}) &= [g(X^{m'}) - g(X)^{m'} + g(X)^{m'}]^m - g(X^{mm'}) \\ &= g(X)^{mm'} - g(X^{mm'}) + (g(X^{m'}) - g(X)^{m'})h(X) \end{aligned}$$

Since $f(X)$ divides $f(X^{m'})$ which divides the LHS, and since $f(X)$ divides $g(X^{m'}) - g(X)^{m'}$ by assumption, it follows that $f(X)$ divides $g(X)^{mm'} - g(X^{mm'})$. This proves that mm' is introspective for $g(X)$. □

Lemma 11.3.13. *If m is introspective for $g(X)$ and $h(X)$, then it also introspective for $g(X)h(X)$.*

Proof. As m is introspective for $g(X)$ and $h(X)$, we have that

$$(g(X))^m (h(X))^m = g(X^m)h(X^m) \pmod{X^r - 1, p}.$$

□

Thus, with the above two lemmas and Remark 11.3.11, we see the following.

Lemma 11.3.14. *Every number in the set*

$$I = \left\{ \left(\frac{n}{p}\right)^i \cdot p^j \,\middle|\, i, j \geqslant 0 \right\}$$

is introspective for every polynomial in the set

$$P = \left\{ \prod_{a=0}^{l} (X + a)^{e_a} \in \mathbb{Z}[X] \,\middle|\, e_a \geqslant 0 \right\}.$$

We now define two groups based on these sets. Define I_r as the set of all residues of I modulo r, that is,

$$I_r := \{\alpha \bmod r \mid \alpha \in I\}.$$

Lemma 11.3.15. *I_r is a subgroup of $(\mathbb{Z}/r\mathbb{Z})^\times$.*

Proof. This is obvious since $(r, n) = (r, p) = 1$. □

Corollary 11.3.16. *Define t to be the cardinality of the group I_r. Note that $n \in I_r$. Then $t \geqslant o_r(n) > \log^2 n$ (recall this from Lemma 11.1.2).*

The first group we wanted to define is the group I_r above. Now we define the second group. Recall the rth cyclotomic polynomial $\Phi_r(X) \in \mathbb{Z}[X]$. Since this divides $f(X) = X^r - 1$, and $f(X)$ is separable over $\mathbb{F}_p$, it follows that $\Phi_r(X)$ is separable over $\mathbb{F}_p$. Let $\mathbb{F}_p \subset K \subset \bar{\mathbb{F}}_p$ denote the field which contains all the roots of $f(X)$. Then K is a finite field and so $K^\times$ is a cyclic group. In particular, this shows that the group of rth roots of 1 in $\bar{\mathbb{F}}_p$ is a cyclic group with r distinct elements (since this set is precisely the set of roots of $f(X)$). Let us denote this set by $\mu_r \subset \bar{\mathbb{F}}_p^\times$. There are precisely $\phi(r)$ many primitive elements in this group (elements which generate the group), which follows from elementary group theory.

Each element of μ_r is forced to be a root of $\Phi_r(X) \in \mathbb{F}_p[X]$, which can be seen as follows. Reducing the equality

$$X^r - 1 = \prod_{d|r} \Phi_d(X)$$

modulo p we see that if a primitive rth root is a root of $\Phi_d(X)$ for some $d < r$, then it will be a root of $X^d - 1$, contradicting the fact that it was primitive. Since the degree of $\Phi_r(X)$ is $\phi(r)$, it follows that the set of roots of $\Phi_r(X)$ in $\bar{\mathbb{F}}_p$ is precisely μ_r.

Let us analyse how $\Phi_r(X)$ factors over $\mathbb{F}_p$. Write

$$\Phi_r(X) = \prod_{i=1}^{s} h_i(X),$$

where the $h_i(X)$ are irreducible over $\mathbb{F}_p$.

Lemma 11.3.17. *All the $h_i(X)$ have the same degree. This degree is equal to the order $o_r(p)$.*

Proof. Let θ_1 be a primitive rth root of 1 in $\bar{\mathbb{F}}_p$ which is a root of $h_1(X)$. Then $\mathbb{F}_p[X]/(h_1(X)) \cong \mathbb{F}_p[\theta_1]$. But any two primitive rth roots of 1 are powers of each other. Thus, if θ_2 is another such, which is a root of $h_2(X)$, then

$$\mathbb{F}_p[X]/(h_1(X)) \cong \mathbb{F}_p[\theta_1] = \mathbb{F}_p[\theta_2] \cong \mathbb{F}_p[X]/(h_2(X))\,.$$

This proves the claim that all the $h_i(X)$ have the same degree. Note that $\mathbb{F}_p[\theta_1]/\mathbb{F}_p$ is a finite separable and normal extension. To compute its extension degree, by the Galois correspondence, it suffices to compute the cardinality of $\mathrm{Aut}(\mathbb{F}_p[\theta_1]/\mathbb{F}_p) = \langle Fr \rangle$. That is, the degree of the extension is the smallest power k of the Frobenius such that $Fr^k = Id$ on $\mathbb{F}_p[\theta_1]$. But this happens iff $Fr^k(\theta_1) = \theta_1$ since the Frobenius is the identity on $\mathbb{F}_p$. Thus, the degree of the extension is the smallest k such that

$$\theta_1^{p^k-1} = 1\,.$$

Since θ_1 is a primitive rth root of 1, this is the smallest k such that $r \mid p^k - 1$, that is, $o_r(p)$. Thus, the degree of each $h_i(X)$ is precisely $o_r(p)$. □

Let us fix $h_1(X)$ and denote it by $h(X)$. Let $\mathcal{G}$ be the set of residues modulo $h(X)$ of the elements in P (see Lemma 11.3.14), that is,

$$\mathcal{G} := \{\alpha \,(\mathrm{mod}\, h(X), p) \mid \alpha \in P\}\,.$$

Thus, we may view elements of $\mathcal{G}$ as elements in the field $F = \mathbb{F}_p[X]/(h(X))$. In the group $(\mathbb{Z}/r\mathbb{Z})^\times$ the order of n is $o_r(n) > \log^2(n)$ (recall from Lemma 11.1.2 that r was chosen so that this happens). Thus,

$$\log^2(n) < o_r(n) \leqslant \phi(r) < r\,, \qquad \text{which implies that,} \qquad \log(n) < \sqrt{r}\,.$$

From this we get that $l = \lfloor \sqrt{\phi(r)}\log(n) \rfloor < \sqrt{r}\log(n) < r$. Since $p > r$ (see Lemma 11.3.5) it follows that $l < p$.

Let x denote the image of X in F. It follows (as $l < p$) that in the field F the elements $x, x+1, \ldots, x+l$ are all distinct. Also we have (recall from Remark 11.3.4) $1 < o_r(p) = \deg(h(X))$. From this it follows that $x + a \neq 0$ in the field F for $a \in \mathbb{F}_p$. Thus, the elements $x, x+1, \ldots, x+l$ are in $F^\times$. Since every element of $\mathcal{G}$ is a product of these elements, it clearly follows that $\mathcal{G}$ is a subgroup of the multiplicative group $F^\times$. Recall that t is the cardinality of the group I_r. Note that since $I_r \subset (\mathbb{Z}/r\mathbb{Z})^\times$, one has $t \leqslant \phi(r)$.

Lemma 11.3.18. $|\mathcal{G}| \geq {}^{t+l}C_{t-1}$.

Proof. Let $x \in F$ denote the image of X. Since $h(X)$ divides $\Phi_r(X)$, it follows that x is a primitive rth root of 1 in $\bar{\mathbb{F}}_p$.

If $f(X)$ and $g(X)$ are elements of P, both of degree $< t$, then we claim that their images in $\mathcal{G}$ are distinct. Assume that this is not the case. Then there are two polynomials $f(X), g(X)$, both of degree $< t$ in P such that their images in $\mathcal{G}$ are the same. That is, their images in $F = \mathbb{F}_p[X]/(h(X))$ are the same.

Consider the polynomial $q(Y) = f(Y) - g(Y) \in F[Y]$. Clearly, x is a root of $q(Y)$. We claim that $q(x^m) = 0$ for $m \in I$. Note that since m is introspective for $f(X)$, we have that $f(X)^m - f(X^m) = 0$ in $\mathbb{F}_p[X]/(X^r - 1)$ and so also in $\mathbb{F}_p[X]/(h(X))$. Similarly for $g(X)$. This shows that $f(x^m) = f(x)^m = g(x)^m = g(x^m)$ in F. Thus, x^m is a root of $q(Y)$ for every $m \in I$.

The x^m are distinct for m distinct in $\mathbb{Z}/r\mathbb{Z}$ and so for m distinct in I_r (this is because x is a primitive rth root of unity). Since the cardinality of I_r is t, it follows that $q(Y)$ has at least t roots. But the degree of $q(Y) < t$. This forces that $q(Y)$ is identically 0 in $F[Y]$. If we write $f(X) = \prod_{a=0}^{l}(X+a)^{e_a}$ and $g(X) = \prod_{a=0}^{l}(X+a)^{d_a}$ then we get that

$$\prod_{a=0}^{l}(Y+a)^{e_a} = \prod_{a=0}^{l}(Y+a)^{d_a} \in F[Y]\,.$$

Since $l < p$, as we saw above, all the $Y + a$ are distinct linear factors. It follows that $f(Y) = g(Y)$, that is, $f(X) = g(X)$, a contradiction. This proves the claim that if $f(X)$ and $g(X)$ are elements of P, both of degree $< t$, then their images in $\mathcal{G}$ are distinct.

The number of elements in P of degree $< t$ corresponds to the number of solutions of

$$e_0 + e_1 + \ldots + e_l < t$$

with $e_i \geqslant 0$. It is standard to see that the number of solutions to this is ${}^{t+l}C_{t-1}$. This proves the lemma. □

Lemma 11.3.19. *If n is not a power of p then $|\mathcal{G}| \leqslant n^{\sqrt{t}}$.*

Proof. If n is not a power of p then there is a prime $q \neq p$ and $k > 0$ such that $q^k \mid (n/p)$ and $q^{k+1} \nmid (n/p)$. Consider the set

$$\hat{I} = \{(n/p)^i p^j \mid 0 \leqslant i, j \leqslant \lfloor\sqrt{t}\rfloor\}\,.$$

By looking at the powers of p and q that divide element of $\hat{I}$, it follows that all the elements are distinct. Thus, $\hat{I}$ has exactly $(\lfloor\sqrt{t}\rfloor + 1)^2 > t$ elements. Since $|I_r| = t$ it follows that two of these are equal in I_r. Let these be m_1 and m_2, with $m_1 > m_2$. Then we have (since $r \mid (m_1 - m_2)$)

$$X^{m_1} = X^{m_2} \qquad (\mathrm{mod}\, X^r - 1)\,.$$

In particular, this means that in the field F, $x^{m_1} = x^{m_2}$. Let

$$q(Y) = Y^{m_1} - Y^{m_2} \in F[Y]\,.$$

We claim that all the elements of $\mathcal{G}$ are roots of $q(Y)$. Let $f(x) \in \mathcal{G}$, where $f(X) \in P$. We need to show that $f(x)^{m_1} = f(x)^{m_2}$. As we saw in the previous lemma, $f(x)^{m_1} = f(x^{m_1}) = f(x^{m_2}) = f(x)^{m_2}$. This proves that claim. Thus,

$$|\mathcal{G}| \leqslant \deg(q(Y)) = m_1 \leqslant (n/p)^{\lfloor\sqrt{t}\rfloor} p^{\lfloor\sqrt{t}\rfloor} \leqslant n^{\sqrt{t}}\,.$$

This completes the proof of the Lemma. □

11.3.20. Completing the proof of correctness.

We will need the following two simple lemmas in the proof.

Lemma 11.3.21. *Let $a, b, c, d \in \mathbb{N}$ with $a \geqslant b$ and $c \geqslant d$. Further assume that $a - c \geqslant b - d$. Then ${}^aC_c \geqslant {}^bC_d$.*

Proof. Repeatedly apply the following simple observations

$${}^bC_d \leqslant {}^{b+1}C_d \qquad \text{and} \qquad {}^bC_d \leqslant {}^{b+1}C_{d+1}.$$

Thus,

$${}^bC_d \leqslant {}^{b+c-d}C_{d+c-d} = {}^{b+c-d}C_c \leqslant {}^aC_c\,.$$

□

Lemma 11.3.22. *If $n > 1$, then $2^{n+1} < {}^{2n+1}C_n$.*

Proof. Note that it is certainly true for $n = 2$. We may assume $n \geqslant 3$ and hence, we have $2^{n-1} \geqslant n + 1$. We now note that ${}^{2n+1}C_r \leqslant {}^{2n+1}C_n$ for all $r \in \{0, \ldots, 2n+1\}$ and the inequality is strict for $r = 0$. This gives,

$$\begin{aligned} 2^{2n+1} &= (1+1)^{2n+1} \\ &= {}^{2n+1}C_0 + \cdots + {}^{2n+1}C_{2n+1} \\ &< (2n+2) \cdot {}^{2n+1}C_n \end{aligned}$$

Thus,

$$\begin{aligned} & \frac{2^{2n}}{n+1} < {}^{2n+1}C_n \\ \iff & \frac{2^{n-1}}{n+1} \cdot 2^{n+1} < {}^{2n+1}C_n \\ \implies & 2^{n+1} < {}^{2n+1}C_n \qquad (\because 2^{n-1} \geqslant n+1) \end{aligned}$$

□

Lemma 11.3.23. *If the algorithm returns* `PRIME` *in step 6 then n is prime.*

Proof. Let us assume that n is not a prime power. Thus, $n > 3$. Then by Lemma 11.3.19 we see that $|\mathcal{G}| \leqslant n^{\sqrt{t}}$. We will show that $|\mathcal{G}| > n^{\sqrt{t}}$ which gives a contradiction. Recall the following facts which have been proved earlier.

(a) $t > \log^2(n)$, see Corollary 11.3.16. This shows that $t > \sqrt{t}\log(n)$. Since t is an integer we get $t > \lfloor\sqrt{t}\log(n)\rfloor$, that is, $t - 1 \geqslant \lfloor\sqrt{t}\log(n)\rfloor$. It follows that $t + l \geqslant l + 1 + \lfloor\sqrt{t}\log(n)\rfloor$.

(b) $\phi(r) \geqslant t$, since $I_r \subset (\mathbb{Z}/r\mathbb{Z})^\times$. Recall that $l = \lfloor\sqrt{\phi(r)}\log(n)\rfloor$. Thus, we get $l \geqslant \lfloor\sqrt{t}\log(n)\rfloor$.

By Lemma 11.3.18 we have that

$$|\mathcal{G}| \geqslant {}^{t+l}C_{t-1}$$

(Using (a) and Lemma 11.3.21)

$$\geqslant {}^{l+1+\lfloor\sqrt{t}\log n\rfloor}C_{\lfloor\sqrt{t}\log n\rfloor}$$

(Using $l = \lfloor\sqrt{\phi(r)}\log n\rfloor \geqslant \lfloor\sqrt{t}\log n\rfloor$)

$$\begin{aligned} &\geqslant {}^{2\lfloor\sqrt{t}\log n\rfloor+1}C_{\lfloor\sqrt{t}\log n\rfloor} \\ &> 2^{\lfloor\sqrt{t}\log n\rfloor+1} \end{aligned}$$

(Since $\lfloor\sqrt{t}\log n\rfloor \geqslant \lfloor\log^2 n\rfloor > 1$ and Lemma 11.3.22)

$$\geqslant n^{\sqrt{t}}.$$

This gives us a contradiction. (We have used that $n > 3$ to say that $\lfloor \log^2 n \rfloor > 1$)

Thus, we conclude that if the algorithm returns `PRIME` in step 6, then n is a power of some prime. Writing $n = p^k$ for some prime p and $k > 0$, we note that if $k > 1$, then Step 1 would have returned `COMPOSITE`. Thus, we have $k = 1$ and hence, n is a prime. □

This completes the proof of the correctness of the algorithm.

11.4 Complexity Analysis

11.4.1. Big-O Notation.

Definition 11.4.2. *Let $f, g : \mathbb{N} \to \mathbb{R}^+$. We write $g(n) = O(f(n))$ if there exist $M \in \mathbb{R}^+$ and $n_0 \in \mathbb{N}$ such that*

$$g(n) \leqslant M \cdot f(n) \quad \forall n \geqslant n_0.$$

Note that since we demand a certain behaviour only for $n \gg 0$, we allow g and f to be functions defined on all but finitely many natural numbers.

11.4.3. Black-boxes. We shall assume the following standard complexities which may be easily verified by the reader:

1. Adding or subtracting two $n-$bit numbers takes $O(n)$ bit operations.
2. Multiplying two $n-$bit numbers takes $O(n^2)$ bit operations.
3. Division of two $n-$bit numbers takes $O(n^2)$ bit operations.

11.4.4. Fast Exponentiation Algorithm. We describe a method which computes $a^k \bmod n$. The idea is quite simple and is called "repeated squaring". The crux is that one may compute $s_i = a^{2^i} \bmod n$, $i \geqslant 0$, by the recursive formula

$$s_0 = a \bmod n; \quad s_i = s_{i-1}^2 \bmod n, \text{ for } i \geqslant 1.$$

Thus, to calculate a^{2^i}, i multiplications and divisions by n are sufficient. Now it is not necessary that k is a power of 2. So more generally, let $k = b_0 + 2b_1 + 2^2b_2 + \ldots + 2^rb_r$ be the binary representation of k. Then

$$\begin{aligned} a^k &= a^{b_0+2\lfloor\frac{k}{2}\rfloor} \\ &= a^{b_0}(a^2)^{\lfloor\frac{k}{2}\rfloor} \end{aligned}$$

It is clear that this sets up a recursive formula. The algorithm which implements the above is as follows:

Input: Integers a, k, n such that $n > a > 1$.
Algorithm:

```
1.  integers u, s, c
2.  u = k
3.  s = a  mod n
4.  c = 1
5.  while(u ⩾ 1)
6.     if(u is odd) c = (c·s) mod n
7.     s = s·s  mod n
8.     u = ⌊u/2⌋
9.  return c
```

Inside the while loop, we are multiplying, dividing, adding, subtracting integers, each of which is $\leqslant n^2$. Thus, the steps inside the while loop will take $O(\log^2(n))$ steps. The loop itself runs at most $\log(k) + 1$ times. It follows that the above algorithm takes at most $O(\log^2(n)\log(k))$ steps.

We will use the following modification of the above algorithm.

FEA-M(a,k,n):
Input: Integers a, k, n such that $n > a, k \geqslant 1$.
Algorithm:

```
1.  integers u, s, c
2.  u = k
3.  s = a
4.  c = 1
5.  while((u ⩾ 1) and (c<n))
6.     if(u is odd) c = (c·s)
```

```
7.      s = s·s
8.      u = ⌊u/2⌋
9.  return c
```

Let l_0 be the smallest integer such that $n \leqslant a^{l_0}$. Then it is clear that the above algorithm returns $\min\{a^k, a^{l_0}\}$. Since $k \leqslant n$, it is clear that this algorithm takes at most $O(\log^3(n))$ steps.

11.4.5. Complexity of Step 1. In this step we test if n is a perfect power, that is, if $n = a^b$ for some $a, b \geqslant 2$. It is clear that $2 \leqslant b \leqslant \log n$. The idea of the test is as follows. For each such b, we may perform a binary search in $\{1, \ldots, n\}$ for a number that satisfies $a^b = n$. The computation of a^b will be done using FEA-M(a,b,n).

Input: Integer $n \geqslant 2$
Algorithm:

```
01.  integers a, b, c, m
02.  b = 2
03.  while(2^b ⩽ n)
04.       a = 1, c = n
05.       while(c − a ⩾ 2)
06.           m = (a + c)/2
07.           p = min{FEA-M(m,b,n), n + 1}
08.           if(p = n) return 'perfect power'
09.           if(p < n) a = m
10.           else c = m
11.       b = b + 1
12.  return 'not a perfect power'
```

We now analyse the above algorithm. In steps 04 - 10, a binary search is carried. The complexity of the instructions in steps 06 - 10 is $O(\log^3(n))$. This is essentially the complexity of step 07. The while loop in step 05 runs at most $\log(n)$ times. Further, the while loop in step 03 runs at most $\log(n)$ times. We conclude that the complexity of the above algorithm is at most $\log^5(n)$.

11.4.6. Complexity of Step 2. The following algorithm computes the gcd of two integers a and n.

gcd(a,n):

```
Input:  integers 1<a<=n
1.  r=a
2.  while(r≠0)
3.      j = n-⌊n/r⌋r
4.      if j > r/2 then j = r-j
5.      if j = 0 then return r
6.      n=a and a=j
```

The instructions inside the while loop can take at most $O(\log^2(n))$ steps. The number of times this while loop can run is $\log(a)+1 \leqslant \log(n)+1$. Thus, computing $\gcd(a,n)$ will take at most $O(\log^3(n))$ many steps.

Step 2 may be achieved by the following algorithm

```
Input:  integer n
01.  r=2
02.  while(r⩾2)
03.      a = n mod r
04.      if (gcd(r,n)=1)
05.          b=1
06.          while(1 ⩽ i ⩽ ⌊log²(n)⌋)
07.              b=b*a
08.              if (b=1 mod r) then i=-1
09.              else i=i+1
10.          if (i=⌊log²(n)⌋+1) return r
11.       r=r+1
```

In this step we find an r such that $o_r(n) > \log^2(n)$. By Lemma 11.1.2, we may successively try out values of r till $\lceil \log^5(n) \rceil$. The complexity of the while loop at line 06 is $O(\log^2(r))$, which is $O(\log(n))$. The while loop at line 06 runs at most $\log^2(n)$ times and the outermost while loop runs at most $\log^5(n)$ times. Thus, there are at most $O(\log^8(n))$ steps in Step 2.

11.4.7. Complexity of Step 3. In this step we have

```
Input:  integer r
1.  for(2 ⩽ a ⩽ r)
```

```
2.      if (1 < gcd(a,n) < n) output 'COMPOSITE'
```

Clearly this step takes at most $O(\log^3(n)\log^5(n))$ since computing the gcd takes $O(\log^3(n))$ many steps and the for loop runs at most $\log^5(n)+1$ times. Thus, Step 3 takes at most $O(\log^8(n))$ many steps.

11.4.8. Complexity of Step 4. In this step, we compare n with another number. As we only need to check at most $\lfloor \log n \rfloor + 1$ bits, this step takes $O(\log n)$ bit operations.

11.4.9. Complexity of Step 5. Let us make the following observations on polynomial multiplication. Consider the ring $\mathbb{Z}/n\mathbb{Z}[X]$ and let $h(X)$ and $g(X)$ be two polynomials in this ring, whose degree is $< r$. To compute the coefficient of X^i in the product $h(X)g(X)$, we need to compute $\sum_s h_s g_{i-s}$. Computing the product takes $O(\log^2(n))$ steps and computing the sum will take $O(r\log^2(n))$ steps. The degree of the product is at most $2r$ and so computing the product $h(X)g(X)$ takes $O(r^2\log^2(n))$ steps. Next we want to go modulo $X^r - 1$. Since degree $h(X)g(X) < 2r$ and we are simply substituting $X^r = 1$, there will be at most r additions of coefficients in the ring $\mathbb{Z}/n\mathbb{Z}$. This will take $O(r\log(n))$ steps. Thus, we conclude that for two elements $h(X), g(X) \in \mathbb{Z}/n\mathbb{Z}[X]/(X^r - 1)$, the product can be computed in at most $O(r^2\log^2(n))$ steps.

In step 6, we verify $l = \lfloor \sqrt{\phi(r)} \log n \rfloor$ equations. Note that

$$l = \lfloor \sqrt{\phi(r)} \log n \rfloor \leqslant r^{1/2} \log n \leqslant \log^4 n$$

Using the same idea of fast modular exponentiation, one sees that calculating $(X+a)^n$ requires $O(\log n)$ multiplications in the ring $\mathbb{Z}[X]/(X^r - 1, n)$. Thus, computing $(X+a)^n$ requires at most $O(r^2\log^3(n))$ steps. Checking that the polynomials $(X+a)^n \neq X^n + a$ requires us to check if r coefficients are equal. This is easily checked to be $O(r\log(n))$. This gives us that this step requires $O(lr^2 \log^2 n) = O(\log^4 n \log^{10} n \log^2 n) = O(\log^{16} n)$ operations.

11.4.10. Conclusion. From the above analysis, it follows that the asymptotic time complexity of step 5 dominates that of all of the other steps. Thus, it follows that the asymptotic time complexity of the algorithm is $O(\log^{16} n)$. In particular, the algorithm can determine whether any given number is prime or composite within polynomial time.

11.5 Decision problems

The purpose of this section is to explain, by means of some examples, what a decision problem is.

11.5.1. Finding gcd. Let $1 < a \leqslant n$ be two integers. Consider the following question, which we denote $P_1(a, n)$:

Is there an integer f with $1 < f \leqslant a \leqslant n$ such that f divides a and n?

11.5.2. Primality testing. Let $n > 1$ be an integer. Let $P_2(n)$ be the question:

Is there an integer d such that $1 < d < n$ and d divides n?

11.5.3. Subset Sum Problem. Let $S \subset \mathbb{Z}$ be a finite subset. The question $P_3(S)$ is the following:

$$\text{Does there exist } T \subset S \text{ such that } \sum_{t \in T} t = 0?$$

A simple graph is a graph that does not have more than one edge between any two vertices and no edge starts and ends at the same vertex. A graph is said to be complete if any pair of vertices are connected by an edge. Let G be a simple graph. A clique of size k is a complete subgraph of G with k vertices.

11.5.4. Existence of Clique. Let G be a simple graph and let $k > 3$ be an integer. Let $EC(G, k)$ be the following question:

Does G contain a clique of size k?

11.5.5. Prime Factorization. Let $n > 1$ be an integer. Let $P_4(n)$ be the following question:

What is the prime factorization of n?

Definition 11.5.6. *A decision problem is a type of problem for which each problem instance has answer a 'YES' or a 'NO'.*

Note that when we say "a decision problem P", we actually mean a family of questions $\{P(I)\}$ where I is a problem instance (input). Given a problem instance I, we get a question $P(I)$ which has an answer 'YES' or 'NO'. For example, $P_2(2996863034895 \cdot 2^{1290000} + 1)$ asks:

Is the integer $2996863034895 \cdot 2^{1290000} + 1$ is composite?

Similarly, $P_2(2996863034895 \cdot 2^{1290000} - 1)$ asks:

Is the integer $2996863034895 \cdot 2^{1290000} - 1$ is composite?

The answer to both these questions is 'NO', see

`https://primes.utm.edu/top20/page.php?id=1`

In the above examples, only (11.5.5) is not a decision problem.

11.6 NP and P

In this section we will informally describe the *classes* of problems **NP** and **P**.

11.6.1. Problem instances. For a decision problem P let us denote by $\mathscr{I}(P)$ the set of all problem instances. For example, if we take $P = P_1$ (see (11.5.1)) then

$$\mathscr{I}(P_1) = \{(a, n) \in \mathbb{Z} \times \mathbb{Z} \,|\, 1 < a \leqslant n\}\,.$$

Similarly, if we take $P = P_2$ (see (11.5.2)) then

$$\mathscr{I}(P_2) = \{n \in \mathbb{Z} \,|\, n > 1\}\,.$$

11.6.2. Admissible inputs to an algorithm. Given an algorithm A, there is a set $\mathscr{A}(A)$ which consists of all possible "admissible" inputs to A. We are simply emphasizing the trivial point that one cannot feed in anything into an algorithm. In fact, when we specify an algorithm, part of the specification is what all can go into it. For example, consider the following algorithm which solves the problem $P_1(a, n)$ (11.5.1).

11.6.3. gcd-ineff(a,n):

```
Input:  integers 1<a<=n
```

```
1.  i=a
2.  while(i≥2)
3.      j = n-⌊n/i⌋i + a-⌊a/i⌋i
4.      if j = 0 then return YES
5.      i=i-1
6.  return NO
```

This algorithm runs through numbers from a to 2. If it finds an integer $2 \leqslant i \leqslant a$ which divides both a and n, then it returns 'YES'. Else it returns 'NO'. For the algorithm gcd-ineff we have

$$\mathscr{A}(\text{gcd-ineff}) = \{(a, n) \in \mathbb{Z} \times \mathbb{Z} \,|\, 1 < a \leqslant n\}\,.$$

It does not make sense to give the input (banana, apple) to gcd-ineff.

We will now informally describe what it means for a problem P to be in **NP**.

Definition 11.6.4. *Assume that the following conditions are satisfied.*

1. *P is a decision problem,*
2. *There is an algorithm $\mathbb{V}$ (the "verifier") and a surjective map*
$$i : \mathscr{A}(\mathbb{V}) \to \mathscr{I}(P)\,,$$
3. *There is a polynomial $q[T] \in \mathbb{Q}[T]$, which depends only on $\mathbb{V}$, such that the following holds: Let $J \in \mathscr{A}(\mathbb{V})$. The number of steps that $\mathbb{V}(J)$ takes is $\leqslant q(\text{size of } i(J))$,*
4. *Given any $I \in \mathscr{I}(P)$, the answer to $P(I)$='YES' iff there is a $J \in i^{-1}(I)$ such that the output of $\mathbb{V}(J)$='YES'.*

If the above conditions are satisfied then we say that P is in **NP**.

Let us see some examples.

1. Let us check that the problem P_1 (see (11.5.1)) is in **NP**. The input to P_1 is a pair of integers (a, n). The size of this input will be treated as $2\log(n)$ as we need at most $2\log(n)$ bits to represent this pair of integers. Consider the following algorithm.

11.6.5. gcd-eff(a,n):

```
Input:  integers 1<a<=n
1.  r=a
2.  while(r≠0)
3.      j = n-⌊n/r⌋r
4.      if j > r/2 then j = r-j
5.      if j = 0
6.          if r=1 then return 'NO'
7.          if r>1 then return 'YES'
8.      n=a and a=j
```

Take $\mathbb{V}$=gcd-eff. Then $i : \mathscr{A}(A) \to \mathscr{I}(P_1)$ is the identity map. The instructions inside the while loop can take at most $O(\log^2(n))$ steps, see §11.4.3. The number of times this while loop can run is $\log(a)+1 \leq \log(n)+1$. Thus, gcd-eff(a, n) will take at most $O(\log^3(n))$ many steps. One easily checks that all the conditions for P_1 to be in **NP** are satisfied.

We remark that if we were to take $\mathbb{V}$ =gcd-ineff, see 11.6.3, then we cannot conclude that P_1 is in **NP**. This is because this algorithm takes $O(n\log^2(n))$ many steps, and so is not in $O(q(\log(n)))$ for any polynomial q.

2. One may show in a different way that P_1 is in **NP**. Suppose we are given three integers $1 < f \leqslant a \leqslant n$. Consider the following algorithm.

11.6.6. div(f,a,n):

```
Input:  integers 1<f≤a≤n
1.  j = (n-⌊n/f⌋f) + (a-⌊a/f⌋f)
2.  if j = 0 then return YES
3.  return NO
```

We take the input size as $3\log(n)$, since we need these many bits to represent f, a, n. This algorithm takes $O(\log^2(n))$ many steps, see §11.4.3. Take $\mathbb{V}$ =div. Then $\mathscr{A}(\mathbb{V})$ consists of triples (f, a, n) such that $1 < f \leqslant a \leqslant n$. The map $i : \mathscr{A}(\mathbb{V}) \to \mathscr{I}(P_1)$ is given by $(f, a, n) \mapsto (a, n)$. The complexity of div(f,a,n) is $O(\log^2(n))$. One easily checks that all the conditions for P_1 to be in **NP** are satisfied.

3. The problem P_2 (see (11.5.2)) is in **NP**. Consider the following algorithm.

   11.6.7. divides(d,n):
   `Input:` integers $1<d\leq n$
   1. $j = n - \lfloor \frac{n}{d} \rfloor d$
   2. if $j = 0$ then return YES
   3. return NO

   Again, we take the input size to be $\log(n)$. Take $\mathbb{V}$ =divides. Then $\mathscr{A}(\mathbb{V})$ consists of pairs (d, n) such that $1 < d \leqslant n$. The set $\mathscr{I}(P_2)$ consists of integers $n > 1$. The map $i : \mathscr{A}(\mathbb{V}) \to \mathscr{I}(P_2)$ is given by $(d, n) \mapsto n$. This algorithm has complexity $O(\log^2(n))$, see §11.4.3. One easily checks that all the conditions for P_2 to be in **NP** are satisfied.

4. The reader will easily check that the problem P_3 (Subset sum problem, see (11.5.3)) is in **NP**.

5. Let us check that the Existence of Clique problem (see 11.5.4) is in **NP**. Consider the following algorithm. Let $V(G)$ denote the set of vertices of G and let $E(G)$ denote the set of edges in G.

   11.6.8. EC(G,k,U):
   `Input:` (G, k, U), $U \subset V(G)$
   1. for $1 \leqslant i \leqslant k-1$
   2. for $i+1 \leqslant j \leqslant k$
   3. if $(u_i, u_j) \notin E(G)$ return 'NO'
   4. return 'YES'

   There can be at most n^2 edges in a graph with n vertices. An edge can be represented by a pair of two integers, each integer corresponding to a vertex. Thus, the input size in this example can be taken to be $O(n^2\log(n))$. Take $\mathbb{V}$=EC(G,k,U). Then $\mathscr{A}(\mathbb{V})$ consists of triples (G, k, U) where $U \subset V(G)$ and $\mathscr{I}(EC)$ consists of tuples (G, k). The map $i : \mathscr{A}(\mathbb{V}) \to \mathscr{I}(EC)$ is simply $(G, k, U) \mapsto (G, k)$. One easily checks that all the conditions for EC to be in **NP** are satisfied.

Definition 11.6.9. *A decision problem P is said to be in* **P** *if there is an algorithm A with $\mathscr{A}(A) = \mathscr{I}(P)$ and a polynomial q such that for a given instance $I \in \mathscr{I}(P)$, $A(I)$ gives an answer to the problem $P(I)$ and $A(I)$ takes $\leqslant q$(size of I) many steps.*

1. The problem P_1 is in **P**, as is easily checked by taking A=gcd-eff.

2. The problem P_2 is in **P** is the content of the Theorem of Agarwal-Kayal-Saxena.

3. It is not known if P_3 (see (11.5.3)) is in **P**.

4. It is not known if EC (see (11.5.4)) is in **P**.

Prior to the Agrawal-Kayal-Saxena algorithm a "partial" result in this direction was the Miller-Rabin primality test. The correctness of the Miller-Rabin algorithm was however conditional on the truth of the Generalized Riemann Hypothesis (this is the sense in which this result is "partial"). Thus, if the Generalized Riemann Hypothesis (GRH) were true, then the Miller-Rabin primality test solved the problem $P_2(n)$ and has complexity a polynomial in $\log(n)$.

We remark that neither the Agrawal-Kayal-Saxena algorithm, nor the Miller-Rabin primality test produce a proper factor of n. In this sense, both are different from the algorithms that we saw above, gcd-eff(a, n), gcd-ineff(a, n). We further remark that for the problem of explicitly finding a prime factor of n, one does not expect to have an algorithm which has complexity a polynomial in $\log(n)$. Indeed, one often hears that cryptosystems are based on the hardness of this problem.

Proposition 11.6.10. $\mathbf{P} \subseteq \mathbf{NP}$.

Proof. Let $P \in \mathbf{P}$. Then there is an algorithm A which solves $P(I)$ in q(size of I) steps. In this case $\mathscr{A}(A) = \mathscr{I}(P)$. Take $i : \mathscr{A}(A) \to \mathscr{I}(P)$ to be the identity map. It is clear from the definition of **NP** that P is in **NP**. □

We may ask:

(11.6.11) Is $\mathbf{P} \neq \mathbf{NP}$?

This is the famous unsolved "**P** vs **NP**" problem in computer science. It is one of the original seven Millenium Prize Problems selected by the Clay Mathematics Institute. A correct solution to any of these problems results in a US $1 million prize being awarded to the solver. At the time of writing this, only one of these seven has been solved. Interestingly, and controversially, the solver declined the prize.

Before we end we make the following remark. Often the class of problems **NP** is informally described as,

(*) "NP is the class of problems which have efficient verifiers, that is, there is a polynomial time algorithm that can verify if a given solution is correct."

We wish to caution the reader that the above statement can be misleading. For example, one may conclude after reading the above statement, that to prove a problem P is in **NP**, one has to do the following:

1. Produce an algorithm A_1 whose inputs will be of the form (I, S), where S is a "proposed solution" to $P(I)$,
2. Produce a polynomial q such that the complexity of $A_1(I, S) \leqslant q(\text{size of } I)$,
3. The output of $A_1(I, S)$='YES' iff S is indeed a solution to $P(I)$.

We wish to warn the reader that the above interpretation of the sentence (*) is not correct. Indeed, if we look at the proof of Proposition 11.6.10, then we do not produce an algorithm which takes as inputs tuples (I, S), where S is a "proposed solution". Let us take another example. Recall the problem $P_1(a, n)$ (see (11.5.1)):

Is there an integer f with $1 < f \leqslant a \leqslant n$ such that f divides a and n?

Consider an algorithm A_1=gcd-eff-modified which we define next. The inputs to A_1 are in the set

$$\mathscr{A}(\text{gcd-eff}) \times \mathbb{Z}_{>1} = \{(a, n, f) \,|\, 1 < a \leqslant n\,,\ f \in \mathbb{Z}_{>1}\}$$

For (a, n, f) as above, we define

$$A_1(a, n, f) = \text{gcd-eff-modified}(a, n, f) := \text{gcd-eff}(a, n).$$

Then we claim that the algorithm A_1 satisfies all the conditions of Definition 11.6.4. However, it does not check if f divides a and n. In fact, if the output of $A_1(a, n, f)$ is 'YES' then we cannot conclude that f divides a and n.

However, in almost all cases of problems which are in **NP** and not known to be in **P**, the algorithm A which appears in the definition of **NP**, Definition 11.6.4, does indeed take as input tuples (I, S), where S is a "proposed solution", and tells us if S is a correct solution to $P(I)$. This is indeed the intuition behind Definition 11.6.4. The reader who is more curious may find the information here interesting.