Chapter 7

Galois Theory

Galois theory is named after the French mathematician Evariste Galois.

Galois was born in 1811, and had what could be called the life of a misunderstood genius. At the age of 15, he was already reading material written for professional mathematicians. He took the examination to the "Ecole Polytechnique" to study mathematics but failed and entered the "Ecole Normale" in 1828. He wrote his first paper at the age of 18. He tried to advertise his work, and sent his discoveries in the theory of polynomial equations to the Academy of Sciences, where Cauchy rejected his memoir. He did not get discouraged, and in 1830, he wrote again his researches to the Academy of Sciences, where this time Fourier got his manuscript. However, Fourier died before reading it.

A year later, he made a third attempt, and sent to the Academy of Sciences a memoir called "On the conditions of solvability of equations by radicals". Poisson was a referee, and he answered several months later, declaring the paper incomprehensible.

In 1832, he got involved in a love affair, but got rejected due to a rival, who challenged him to a duel. The night before the duel, he wrote a letter to his friend, where he reported his mathematical discoveries. He died during the duel with pistols in 1832.

It is after his death that his friend insisted to have his letter published, which was finally done by the mathematician Chevalier.

7.1 Galois group and fixed fields

Definition 7.1. If E/F is normal and separable, it is said to be a Galois extension, or alternatively, we say that E is Galois over F.

Take E/F a Galois extension of degree n. Since it is separable of degree n, we know that there are exactly n F-monomorphisms of E into an algebraic closure C. But E/F being also normal, every F-automorphism into C is actually and

Figure 7.1: Evariste Galois (1811-1832)

F-automorphism of E. Thus there are exactly $n = [E : F]$ F-automorphisms of E.

We can define the notion of a Galois group for an arbitrary field extension.

Definition 7.2. If E/F is a field extension, the Galois group of E/F, denoted by $\mathrm{Gal}(E/F)$, is the set of F-automorphisms of E. It forms a group under the composition of functions.

Example 7.1. If $E = \mathbb{Q}(\sqrt[3]{2})$, then $\mathrm{Gal}(E/\mathbb{Q}) = \{1\}$, that is the identity on E.

The above example illustrates the fact that though one can always define a Galois group, we need the extension to be actually Galois to say that the order of the Galois group is actually the degree of the field extension.

Definition 7.3. Let $G = \mathrm{Gal}(E/F)$ be the Galois group of the extension E/F. If H is a subgroup of G, the fixed field of H is the set of elements fixed by every automorphism in H, that is

$$\mathcal{F}(H) = \{x \in E,\ \sigma(x) = x \text{ for all } \sigma \in H\}.$$

Vice-versa, if K is an intermediate field, define

$$\mathcal{G}(K) = \mathrm{Gal}(E/K) = \{\sigma \in G,\ \sigma(x) = x \text{ for all } x \in K\}.$$

It is the group fixing K.

Galois theory has much to do with studying the relations between fixed fields and fixing groups.

Proposition 7.1. *Let E/F be a finite Galois extension with Galois group $G = \mathrm{Gal}(E/F)$. Then*

1. *The fixed field of G is F.*

2. *If H is a proper subgroup of G, then the fixed field $\mathcal{F}(H)$ of H properly contains F.*

Proof. 1. Let F_0 be the fixed field of G (and we have the field extensions $E/F_0/F$). We want to prove that $F_0 = F$.

We first note that if σ is an F-automorphism of E (that is σ is in G), then by definition of F_0, σ fixes everything in F_0, meaning that σ is an F_0-automorphism. Thus the F-automorphisms in the group G coincide with the F_0-automorphisms in the group G.

Now we further have that E/F_0 is Galois: indeed, we have $E/F_0/F$ with E/F Galois thus normal and separable, and E/F_0 inherits both properties.

We now look at the degrees of the extensions considered:

$$|\mathrm{Gal}(E/F_0)| = [E : F_0],\ |\mathrm{Gal}(E/F)| = [E : F],$$

since both are Galois. Furthermore by the first remark, the number of $F-$ and F_0- automorphisms in G coincide:

$$|\mathrm{Gal}(E/F_0)| = |\mathrm{Gal}(E/F)|$$

showing that

$$[E : F_0] = [E : F]$$

and by multiplicativity of the degrees

$$[E : F] = [E : F_0][F_0 : F] \Rightarrow [F_0 : F] = 1$$

and $F = F_0$.

2. In order to prove that $F \subsetneq \mathcal{F}(H)$, let us assume by contradiction that $F = \mathcal{F}(H)$.

Since we consider a finite Galois extension, we can invoke the Theorem of the Primitive Element and claim that

$$E = F(\alpha),\ \alpha \in E. \tag{7.1}$$

Consider the polynomial

$$f(X) = \prod_{\sigma\in H}(X - \sigma(\alpha)) \in E[X].$$

It is a priori in $E[X]$, but we will prove now that it is actually in $F[X]$. Since by contradiction we are assuming that $F = \mathcal{F}(H)$, it is enough to proof that $f(X)$ is fixed by H. Indeed, take $\tau \in H$, then

$$\prod_{\sigma\in H}(X - \tau\sigma(\alpha)) = \prod_{\sigma\in H}(X - \sigma(\alpha))$$

since $\tau\sigma$ ranges over all H as does σ.

Thus $f(X) \in F[X]$ and $f(\alpha) = 0$ (σ must be the identity once while ranging through H). Now on the one hand, we have

$$\deg f = |H| < |G| = [E : F]$$

since we assume that H is proper and E/F is Galois. On the other hand,

$$\deg f \geq [F(\alpha) : F] = [E : F]$$

since f is a multiple of the minimal polynomial of α over F (equality holds if f is the minimal polynomial of α over F), and $E = F(\alpha)$ by (7.1). We cannot possibly have $\deg f < [E : F]$ and $\deg f \geq [E : F]$ at the same time, which is a contradiction and concludes the proof.

□

7.2 The fundamental Theorem of Galois theory

The most significant discovery of Galois is that (surely not in these terms!) under some hypotheses, there is a one-to-one correspondence between

1. subgroups of the Galois group $\mathrm{Gal}(E/F)$
2. subfields M of E such that $F \subseteq M$.

The correspondence goes as follows:

- To each intermediate subfield M, associate the group $\mathrm{Gal}(E/M)$ of all M-automorphisms of E:

$$\begin{array}{rcl} \mathcal{G} = \mathrm{Gal} : \{\text{intermediate fields}\} & \to & \{\text{subgroups of } \mathrm{Gal}(E/F)\} \\ M & \mapsto & \mathcal{G}(M) = \mathrm{Gal}(E/M). \end{array}$$

- To each subgroup H of $\mathrm{Gal}(E/F)$, associate the fixed subfield $\mathcal{F}(H)$:

$$\begin{array}{rcl} \mathcal{F} : \{\text{subgroups of } \mathrm{Gal}(E/F)\} & \to & \{\text{intermediate fields}\} \\ H & \mapsto & \mathcal{F}(H). \end{array}$$

We will prove below that, under the right hypotheses, we actually have a bijection (namely $\mathcal{G}$ is the inverse of $\mathcal{F}$). Let us start with an example.

Example 7.2. Consider the field extension $E = \mathbb{Q}(i, \sqrt{5})/\mathbb{Q}$. It has four $\mathbb{Q}$-automorphisms, given by (it is enough to describe their actions on i and $\sqrt{5}$):

$$\begin{array}{rrl} \sigma_1 : & i \mapsto i, & \sqrt{5} \mapsto \sqrt{5} \\ \sigma_2 : & i \mapsto -i, & \sqrt{5} \mapsto \sqrt{5} \\ \sigma_3 : & i \mapsto i, & \sqrt{5} \mapsto -\sqrt{5} \\ \sigma_4 : & i \mapsto -i, & \sqrt{5} \mapsto -\sqrt{5} \end{array}$$

thus

$$\mathrm{Gal}(E/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}.$$

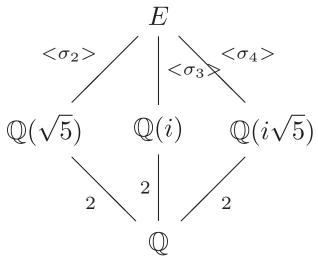
The proper subgroups of $\mathrm{Gal}(E/\mathbb{Q})$ are

$$\{\sigma_1\}, \{\sigma_1, \sigma_2\}, \{\sigma_1, \sigma_3\}, \{\sigma_1, \sigma_4\}$$

and their corresponding subfields are

$$E,\ \mathbb{Q}(\sqrt{5}),\ \mathbb{Q}(i),\ \mathbb{Q}(i\sqrt{5}).$$

We thus get the following diagram:



Theorem 7.2. *Let E/F be a finite Galois extension with Galois group G.*

1. *The map $\mathcal{F}$ is a bijection from subgroups to intermediate fields, with inverse $\mathcal{G}$.*
2. *Consider the intermediate field $K = \mathcal{F}(H)$ which is fixed by H, and $\sigma \in G$. Then the intermediate field*

   $$\sigma K = \{\sigma(x),\ x \in K\}$$

   is fixed by $\sigma H \sigma^{-1}$, namely $\sigma K = \mathcal{F}(\sigma H \sigma^{-1})$.

Proof. 1. We first consider the composition of maps

$$H \to \mathcal{F}(H) \to \mathcal{G}\mathcal{F}(H).$$

We need to prove that $\mathcal{G}\mathcal{F}(H) = H$. Take σ in H, then σ fixes $\mathcal{F}(H)$ by definition and $\sigma \in \mathrm{Gal}(E/\mathcal{F}(H)) = \mathcal{G}(\mathcal{F}(H))$, showing that

$$H \subseteq \mathcal{G}\mathcal{F}(H).$$

To prove equality, we need to rule out the strict inclusion. If H were a proper subgroup of $\mathcal{G}(\mathcal{F}(H))$, by the above proposition the fixed field $\mathcal{F}(H)$ of H should properly contain the fixed field of $\mathcal{G}\mathcal{F}(H)$ which is $\mathcal{F}(H)$ itself, a contradiction, showing that

$$H = \mathcal{G}\mathcal{F}(H).$$

Now consider the reverse composition of maps

$$K \to \mathcal{G}(K) \to \mathcal{F}\mathcal{G}(K).$$

This time we need to prove that $K = \mathcal{F}\mathcal{G}(K)$. But

$$\mathcal{F}\mathcal{G}(K) = \text{ fixed field by } \mathrm{Gal}(E/K)$$

which is exactly K by the above proposition (its first point).

2. It is enough to compute $\mathcal{F}(\sigma H \sigma^{-1})$ and show that it is actually equal to $\sigma K = \sigma \mathcal{F}(H)$.

$$\begin{aligned} \mathcal{F}(\sigma H \sigma^{-1}) &= \{x \in E,\ \sigma\tau\sigma^{-1}(x) = x \text{ for all } \tau \in H\} \\ &= \{x \in E,\ \tau\sigma^{-1}(x) = \sigma^{-1}(x) \text{ for all } \tau \in H\} \\ &= \{x \in E,\ \sigma^{-1}(x) \in \mathcal{F}(H)\} \\ &= \{x \in E,\ x \in \sigma(\mathcal{F}(H))\} = \sigma(\mathcal{F}(H)). \end{aligned}$$

□

We now look at subextensions of the finite Galois extension E/F and ask about their respective Galois group.

Theorem 7.3. *Let E/F be a finite Galois extension with Galois group G. Let K be an intermediate subfield, fixed by the subgroup H.*

1. *The extension E/K is Galois.*
2. *The extension K/F is normal if and only if H is a normal subgroup of G.*
3. *If H is a normal subgroup of G, then*

$$\mathrm{Gal}(K/F) \simeq G/H = \mathrm{Gal}(E/F)/\mathrm{Gal}(E/K).$$

4. *Whether K/F is normal or not, we have*

$$[K : F] = [G : H].$$

Proof. 1. That E/K is Galois is immediate from the fact that a subextension $E/K/F$ inherits normality and separability from E/F.

2. First note that σ is an F-monomorphism of K into E if and only if σ is the restriction to K of an element of G: if σ is an F-monomorphism of K into E, it can be extended to an F-monomorphism of E into itself thanks to the normality of E. Conversely, if τ is an F-automorphism of E, then $\sigma = \tau|_K$ is surely a F-monomorphism of K into E.

Now, this time by a characterization of a normal extension, we have

$$K/F \text{ normal } \iff \sigma(K) = K \text{ for all } \sigma \in G.$$

Since $K=\mathcal{F}(H)$, we just rewrite

$$K/F \text{ normal } \iff \sigma(\mathcal{F}(H))=\mathcal{F}(H) \text{ for all } \sigma\in G.$$

Now by the above theorem, we know that $\sigma(\mathcal{F}(H))=\mathcal{F}(\sigma H\sigma^{-1})$, and we have

$$K/F \text{ normal } \iff \mathcal{F}(\sigma H\sigma^{-1})=\mathcal{F}(H) \text{ for all } \sigma\in G.$$

We are almost there, we now use again the above theorem that tells us that $\mathcal{F}$ is invertible, with inverse $\mathcal{G}$, to get the conclusion:

$$K/F \text{ normal } \iff \sigma H\sigma^{-1}=H \text{ for all } \sigma\in G.$$

3. To prove this isomorphism, we will use the 1st isomorphism Theorem for groups. Consider the group homomorphism

$$\mathrm{Gal}(E/F)\to\mathrm{Gal}(K/F),\ \sigma\mapsto\sigma|_K.$$

This map is surjective (we showed it above, when we mentioned that we can extend $\sigma|_K$ to σ. Its kernel is given by

$$\mathrm{Ker}=\{\sigma,\ \sigma|_K=1\}=H=\mathrm{Gal}(E/K).$$

Applying the 1st isomorphism Theorem for groups, we get

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

4. Finally, by multiplicativity of the degrees:

$$[E:F]=[E:K][K:F].$$

Since E/F and E/K are Galois, we can rewrite

$$|G|=|H|[K:F].$$

We conclude by Lagrange Theorem:

$$[G:H]=|G|/|H|=[K:F].$$

□

7.3 Finite fields

We will provide a precise classification of finite fields.

Theorem 7.4. *Let E be a finite field of characteristic p.*

1. *The cardinality of E is*

$$|E|=p^n,$$

for some $n\geq 1$. It is denoted $E=\mathbb{F}_{p^n}$.

2. *Furthermore, E is the splitting field for the separable polynomial*

$$f(X) = X^{p^n} - X$$

over $\mathbb{F}_p$, so that any finite field with p^n elements is isomorphic to E. In fact, E coincides with the set of roots of f.

Proof. 1. Let $\mathbb{F}_p$ be the finite field with p elements, given by the integers modulo p. Since E has characteristic p, it contains a copy of $\mathbb{F}_p$. Thus E is a field extension of $\mathbb{F}_p$, and we may see E as a vector space over $\mathbb{F}_p$. If the dimension is n, then let $\alpha_1, \dots, \alpha_n$ be a basis. Every x in E can be written as

$$x = x_1\alpha_1 + \cdots + x_n\alpha_n$$

and there are p choices for each x_i, thus a total of p^n different elements in E.

2. Let $E^\times$ be the multiplicative group of non-zero elements of E. If $\alpha \in E^\times$, then

$$\alpha^{p^n-1} = 1$$

by Lagrange's Theorem, so that

$$\alpha^{p^n} = \alpha$$

for all α in E (including $\alpha = 0$). Thus each element of E is a root of f, and f is separable.

Now f has at most p^n distinct roots, and we have already identified the p^n elements of E as roots of f.

□

Corollary 7.5. *If E is a finite field of characteristic p, then $E/\mathbb{F}_p$ is a Galois extension, with cyclic Galois group, generated by the Frobenius automorphism*

$$\sigma : x \mapsto \sigma(x) = x^p, \ x \in E.$$

Proof. By the above proposition, we know that E is a splitting field for a separable polynomial over $\mathbb{F}_p$, thus $E/\mathbb{F}_p$ is Galois.

Since $x^p = x$ for all x in $\mathbb{F}_p$, we have that

$$\mathbb{F}_p \subset \mathcal{F}(\langle\sigma\rangle)$$

that is $\mathbb{F}_p$ is contained in the fixed field of the cyclic subgroup generated by the Frobenius automorphism σ. But conversely, each element fixed by σ is a root of $X^p - X$ so $\mathcal{F}(\langle\sigma\rangle)$ has at most p elements. Consequently

$$\mathbb{F}_p = \mathcal{F}(\langle\sigma\rangle)$$

and

$$\mathrm{Gal}(E/\mathbb{F}_p) = \langle\sigma\rangle.$$

□

This can be generalized when the base field is larger than $\mathbb{F}_p$.

Corollary 7.6. *Let E/F be a finite field extension with $|E| = p^n$ and $|F| = p^m$. Then E/F is a Galois extension and $m|n$. Furthermore, the Galois group is cyclic, generated by the automorphism*

$$\tau : x \mapsto \tau(x) = x^{p^m},\ x \in E.$$

Proof. If the degree $[E : F] = d$, then every x in E can be written as

$$x = x_1\alpha_1 + \cdots + x_d\alpha_d$$

and there are p^m choices for each x_i, thus a total of

$$(p^m)^d = p^n$$

different elements in E, so that

$$d = m/n \text{ and } m|n.$$

The same proof as for the above corollary holds for the rest. □

Thus a way to construct a finite field E is, given p and n, to construct $E = \mathbb{F}_{p^n}$ as a splitting field for $X^{p^n} - X$ over $\mathbb{F}_p$.

Theorem 7.7. *If G is a finite subgroup of the multiplicative group of an arbitrary field, then G is cyclic. Thus in particular, the multiplicative group $E^\times$ of a finite field E is cyclic.*

Proof. The proof relies on the following fact: if G is a finite abelian group, it contains an element g whose order r is the exponent of G, that is, the least common multiple of the orders of all elements of G.

Assuming this fact, we proceed as follows: if $x \in G$, then its order divides r and thus

$$x^r = 1.$$

Therefore each element of G is a root of $X^r - 1$ and

$$|G| \leq r.$$

Conversely, $|G|$ is a multiple of the order of every element, so $|G|$ is at least as big as their least common multiple, that is

$$|G| \geq r$$

and

$$|G| = r.$$

Since the order of $|G|$ is r, and it coincides with the order of the element g whose order is the exponent, we have that G is generated by g, that is $G = \langle g \rangle$ is cyclic. □

Since $E^\times$ is cyclic, it is generated by a single element, say α:

$$E = \mathbb{F}_p(\alpha)$$

and α is called a primitive element of E. The minimal polynomial of α is called a primitive polynomial.

Example 7.3. Consider the following irreducible polynomial

$$g(X) = X^4 + X + 1$$

over $\mathbb{F}_2$. Let α be a root of $g(X)$. A direct computation shows that α is primitive:

$$\alpha^0 = 1, \ldots, \ \alpha^4 = \alpha + 1, \ldots, \ \alpha^7 = \alpha^3 + \alpha + 1, \ldots, \ \alpha^{14} = 1 + \alpha^3.$$

7.4 Cyclotomic fields

Definition 7.4. A cyclotomic extension of a field F is a splitting field E for the polynomial

$$f(X) = X^n - 1$$

over F. The roots of f are called nth roots of unity.

The nth roots of unity form a multiplicative subgroup of the group $E^\times$ of non-zero elements of E, and thus must be cyclic. A primitive nth root of unity is an nth root of unity whose order in $E^\times$ is n. It is denoted ζ_n.

From now on, we will assume that we work in a characteristic char(F) such that char(F) does not divide n. (Otherwise, we have $n = m\text{char}(F)$ and $0 = \zeta_n^n - 1 = (\zeta^m - 1)^{\text{char}(F)}$ and the order of ζ_n is less than n.)

Example 7.4. The field $\mathbb{Q}(\zeta_p)$ where p is a prime and ζ_p is a primitive pth root of unity is a cyclotomic field over $\mathbb{Q}$.

Let us look at the Galois group Gal(E/F) of the cyclotomic extension E/F. Then $\sigma \in \text{Gal}(E/F)$ must map a primitive nth root of unity ζ_n to another primitive nth root of unity ζ_n^r, with $(r, n) = 1$. We can then identify σ with r, and this shows that

$$\text{Gal}(E/F) \simeq U_n$$

where U_n denotes the group of units modulo n. This shows that the Galois group is abelian.

Example 7.5. Consider the field extension $\mathbb{Q}(\zeta_3)/\mathbb{Q}$. We have

$$X^3 - 1 = (X - 1)(X^2 + X + 1).$$

The Galois group is given by:

$$\begin{array}{rcl} \sigma : \zeta_3 & \mapsto & \zeta_3^2 \\ \sigma^2 : \zeta_3 & \mapsto & \zeta_3 \end{array}$$

and the group U_3 of units modulo 3 is $U_3 = \{1, 2\}$. Thus

$$\mathrm{Gal}(\mathbb{Q}(\zeta_3)/\mathbb{Q}) = \{\sigma, 1\} \simeq \{2, 1\} = (\mathbb{Z}/3\mathbb{Z})^\times.$$

Finally, since E/F is Galois (under the above assumption)

$$[E : F] = |\mathrm{Gal}(E/F)| = \varphi(n)$$

where $\varphi(n)$ is the Euler totient function.

From now on, we fix the base field $F = \mathbb{Q}$. This means that a primitive nth root of unity ζ_n is given by

$$\zeta_n = e^{i2\pi r/n},\ (r, n) = 1.$$

Definition 7.5. The nth cyclotomic polynomial is defined by

$$\Psi_n(X) = \prod_{(i,n)=1} (X - \zeta_n^i),$$

where the product is taken over all primitive nth roots of unity in $\mathbb{C}$.

The degree of $\Psi_n(X)$ is thus

$$\deg(\Psi_n) = \varphi(n).$$

Example 7.6. For $n = 1, 2$, we have

$$\Psi_1(X) = X - 1,\ \Psi_2(X) = X - (-1) = X + 1.$$

Computing a cyclotomic polynomial is not that easy. Here is a formula that can help.

Proposition 7.8. *We have*

$$X^n - 1 = \prod_{d|n} \Psi_d(X).$$

In particular, if $n = p$ a prime, then d is either 1 or p and

$$X^p - 1 = \Psi_1(X)\Psi_p(X) = (X - 1)\Psi_p(X)$$

from which we get

$$\Psi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

Proof. We prove equality by comparing the roots of both monic polynomials.

If ζ is a nth root of unity, then by definition

$$\zeta_n^n = 0$$

and its order d divides n. Thus ζ is actually a primitive dth root of unity, and a root of $\Psi_d(X)$.

Conversely, if $d|n$, then any root of $\Psi_d(X)$ is a dth root hence a nth root of unity. □

Examples 7.7. For $n = 3$ and 5, we have a prime and thus we can use the above formula:

$$\begin{aligned}\Psi_3(X) &= X^2 + X + 1\\ \Psi_5(X) &= X^4 + X^3 + X^2 + X + 1.\end{aligned}$$

For $n = 4$ the primitive 4rth roots of unity are $\pm i$, and by definition

$$\Psi_4(X) = (X - i)(X + i) = X^2 + 1.$$

Finally for $n = 6$, the possible values for d are 1,2,3 and 6. Thus

$$\Psi_6(X) = \frac{X^6 - 1}{(X-1)(X+1)(X^2+X+1)} = X^2 - X + 1.$$

From the above examples, it is tempting to say that in general $\Psi_n(X)$ has integer coefficients. It happens to be true.

Proposition 7.9. *The nth cyclotomic polynomial $\Psi_n(X)$ satisfies*

$$\Psi_n(X) \in \mathbb{Z}[X].$$

Proof. We proceed by induction on n. It is true for $n = 1$ since $X - 1 \in \mathbb{Z}[X]$. Let us suppose it is true for $\Psi_k(X)$ where k is up to $n - 1$, and prove it is also true for n.

Using the above proposition, we know that

$$\begin{aligned}X^n - 1 &= \prod_{d|n} \Psi_d(X)\\ &= \Psi_n(X) \prod_{d|n, d<n} \Psi_d(X).\end{aligned}$$

The aim is to prove that $\Psi_n(X) \in \mathbb{Z}[X]$:

$$\Psi_n(X) = \frac{X^n - 1}{\prod_{d|n,d<n} \Psi_d(X)}.$$

First note that $\Psi_n(X)$ has to be monic (by definition), and both $X^n - 1$ and $\Psi_d(X)$ (by induction hypothesis) are in $\mathbb{Z}[X]$. We can thus conclude invoking the division algorithm for polynomials in $\mathbb{Z}[X]$. □

We conclude by proving the irreducibility of the cyclotomic polynomials.

Theorem 7.10. *The cyclotomic polynomial $\Psi_n(X)$ is irreducible over $\mathbb{Q}$.*

Proof. Let $f(X)$ be the minimal polynomial of ζ_n, a primitive nth root of unity over $\mathbb{Q}(X)$. We first note that by definition $f(X)$ is monic, and thus since $f(X)|X^n - 1$, we have

$$X^n - 1 = f(X)g(X) \tag{7.2}$$

and $f(X)$ and $g(X)$ must be in $\mathbb{Z}[X]$.

To prove that $\Psi_n(x)$ is irreducible, we will actually prove that

$$\Psi_n(X) = f(X).$$

To prove the equality, it is enough to show that every root of $\Psi_n(X)$ is a root of $f(X)$.

We need the following intermediate result: if p does not divide n, then

$$f(\zeta_n^p) = 0.$$

Let us prove this result. Suppose by contradiction that this is not the case, namely $f(\zeta_n^p) \neq 0$. By (7.2), we have

$$X^n - 1 = f(X)g(X),$$

which evaluated in $X = \zeta_n^p$ yields

$$(\zeta_n^p)^n - 1 = 0 = f(\zeta_n^p)g(\zeta_n^p)$$

implying by our assumption that $f(\zeta_n^p) \neq 0$ that

$$g(\zeta_n^p) = 0,$$

or in other words, ζ_n is a root of $g(X^p)$. But by definition of minimal polynomial, we have that $f(X)$ must then divide $g(X^p)$, that is

$$g(X^p) = f(X)h(X),\ h(X) \in \mathbb{Z}[X].$$

Since $g(X^p), f(X)$ and $h(X)$ are in $\mathbb{Z}[X]$, we can look at their reduction modulo p, that is work in $\mathbb{F}_p[X]$. We will denote $\bar{p}(X)$ the polynomial obtained from $p(X)$ by taking all its coefficients modulo p: if $p(X) = \sum_{i=0}^n a_i X^i$, then $\bar{p}(X) = \sum_{i=0}^n (a_i \mod p) X^i$. Therefore

$$\bar{g}(X^p) = \bar{f}(X)\bar{h}(X) \in \mathbb{F}_p[X].$$

By working in $\mathbb{F}_p[X]$, we are now allowed to write that

$$\bar{g}(X^p) = \bar{g}(X)^p$$

and thus

$$\bar{g}(X)^p = \bar{f}(X)\bar{h}(X) \in \mathbb{F}_p[X].$$

This tells us that any irreducible factor of $\bar{f}(X)$ divides $\bar{g}(X)$ and consequently $\bar{f}$ and $\bar{g}$ have a common factor. Looking at (7.2) in $\mathbb{F}_p[X]$ gives

$$X^n - \bar{1} = \bar{f}(X)\bar{h}(X) \in \mathbb{F}_p[X].$$

Since $\bar{f}$ and $\bar{g}$ have a common factor, $X^n - \bar{1}$ has a multiple root, which cannot be since we have assumed that p does not divide n. This proves the claim.

To summarize, we have just proven that if p does not divide n, then $f(\zeta_n^p)$ is another root of f. Since all primitive nth roots of unity can be obtained from ζ_n by successive prime powers, we have that all primitive nth roots of unity are actually roots of $f(X)$, and we know that there are $\varphi(n)$ of them, which is also the degree of $\Psi_n(X)$. This concludes the proof, since

$$\deg f(X) \geq \varphi(n) = \deg(\Psi_n(X)) \Rightarrow f(X) = \Psi_n(X).$$

□

7.5 Solvability by radicals

The question of solvability by radicals is the one of solving polynomial equations under the restriction that we are only allowed to perform addition, subtraction, multiplication, division, and taking nth roots.

For example, we know (Fontana-Tartaglia, 1535) that for a cubic equation

$$X^3 + pX = q,$$

the solution is given by

$$X = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}.$$

By the 16th century all polynomial equations of degree smaller or equal to 4 were solved. The natural question was then: what happens with quintic equations? Euler failed to give an answer, Lagrange (1770) proved that it depends on finding functions of the roots which are unchanged by certain permutations of the roots, and that this approach works up to degree 4 and fails for 5. Abel showed (1824) that quintics are insolvable by radicals. The next question thus became: decide whether or not a given equation can be solved by radicals. Liouville (1843) found the answer in Galois's papers.

The answer is to be found by connecting the problem with field theory as follows. We first need to define the notion of a radical extension. Informally, a radical extension is obtained by adjoining a sequence of nth roots. For example, to get a radical extension of $\mathbb{Q}$ containing

$$\sqrt[3]{11}\sqrt[5]{\frac{7+\sqrt{3}}{2}} + \sqrt[4]{1+\sqrt[3]{4}},$$

we must adjoin

$$\alpha = \sqrt[3]{11},\ \beta = \sqrt{3},\ \gamma = \sqrt[5]{\frac{7+\beta}{2}}, \delta = \sqrt[3]{4}, \epsilon = \sqrt[4]{1+\delta}.$$

This can be stated formally:

Definition 7.6. An extension E/F is radical if $E = F(\alpha_1, \ldots, \alpha_n)$ where for all $i = 1, \ldots, n$, there exists an integer $n(i)$ such that

$$\alpha_i^{n(i)} \in F(\alpha_1, \ldots, \alpha_{i-1}),\ i \geq 2.$$

The α_i's are said to form a radical sequence for E/F.

Example 7.8. The expression

$$\sqrt[3]{11}\sqrt[5]{\frac{7+\sqrt{3}}{2}} + \sqrt[4]{1+\sqrt[3]{4}}$$

is contained in $\mathbb{Q}(\alpha, \beta, \gamma, \delta, \epsilon)$, where

$$\alpha^3 = 11, \beta^2 = 3, \gamma^5 = \frac{7+\beta}{2}, \delta^3 = 4, \epsilon^4 = 1 + \delta.$$

Definition 7.7. Let f be a polynomial over a field F of characteristic zero (this is a simplifying assumption). We say that f is solvable (soluble) by radicals if there exists a field E containing a splitting field for f such that E/F is a radical extension.

We want to connect radical extensions and solvable groups. Here is the main theorem:

Theorem 7.11. *If F is a field of characteristic zero, and $F \subseteq E \subseteq M$ where M/F is a radical extension, then the Galois group of E/F is a solvable group.*

Thus a solvable (by radicals) polynomial has a solvable Galois group (of a splitting field over the base field).

Recall that a group G is solvable if G has a normal series

$$\{1\} = G_r \trianglelefteq G_{r-1} \trianglelefteq \ldots \trianglelefteq G_0 = G$$

with G_i/G_{i+1} abelian. The proof takes some fair amount of work, though the idea is simple. A radical extension is a series of extensions by nth roots. Such extensions have abelian Galois groups (to be proven though...), so the Galois group of a radical extension is made up by fitting together a sequence of abelian groups (unfortunately, the proof is not that simple...)

We can restate the above result in terms of polynomials.

Theorem 7.12. *Let f be a polynomial over a field E of characteristic zero. If f is solvable by radicals then its Galois group (that is the Galois group of its splitting field) over E is a solvable group.*

To find a polynomial which is not solvable by radicals, it suffices to find one whose Galois group is not solvable.

Lemma 7.13. *Let p be a prime, f an irreducible polynomial of degree p over $\mathbb{Q}$. Suppose that f has precisely two non-real zeros in $\mathbb{C}$. Then the Galois group of f over $\mathbb{Q}$ is the symmetric group S_p.*

Theorem 7.14. *The polynomial $X^5 - 6X + 3$ over $\mathbb{Q}$ is not solvable by radicals.*

The proof consists of showing that the polynomial is irreducible over $\mathbb{Q}$, by Eisenstein's criterion. Then f has exactly three real zeros with multiplicity 1 each, and the above lemma says that is Galois group is S_5. To conclude, we need to show that the symmetric group S_n is not solvable if $n \geq 5$.

7.6 Solvability by ruler and compasses

The ancient Greek philosopher Plato believed that the only perfect figures were the straight line and the circle, and this belief had a great impact in ancient Greek geometry: it restricted the instruments available for performing geometrical constructions to ruler and compasses.

Many constructions can be done just be using ruler and compasses, but three famous constructions could not be performed:

- duplication of the cube: find a cube twice the volume of a given cube.
- trisection of the angle: find an angle 1/3 the size of a given angle.
- quadrature of the circle: find a square of area equal to those of a given circle.

It is no wonder those problems remained unsolved (again, under these platonic constraints) since we will see, using our modern tools, that none of them are possible.

We start by formalizing the intuitive idea of a ruler and compass construction. Denote by P_0 the set of points in $\mathbb{R}^2$.

- operation 1 (ruler): through any 2 points of P_0, draw a straight line.
- operation 2 (compasses): draw a circle, whose center is a point of P_0 and whose radius is equal to the distance between some pairs of points in P_0.

Definition 7.8. The points of intersection of any two distinct lines or circles, drawn using operations 1 and 2 are said to be constructible from P_0 if there exists a sequence $r_1, \dots, r_n$ of points of $\mathbb{R}^2$ such that for each $i = 1, \dots, n$ the point r_i is constructible from the set $P_0 \cup \{r_1, \dots, r_{i-1}\}$, $P_i = P_{i-1} \cup \{r_i\}$.

We can now bring field theory into play. With each stage, we associate the subfield of $\mathbb{R}$ generated by the coordinates of the points constructed. Denote by K_0 the subfield of $\mathbb{R}$ generated by the x- and y-coordinates of the points in P_0. If r_i has coordinates (x_i, y_i), then inductively we define

$$K_i = K_{i-1}(x_i, y_i)$$

to get

$$K_0 \subseteq K_1 \subseteq \ldots \subseteq K_n \subseteq \mathbb{R}.$$

Lemma 7.15. *With the above notation, x_i and y_i are zeros in K_i of quadratic polynomials over K_{i-1}.*

Proof. There are 3 cases to consider: line meets line, line meets circle and circle meets circle. We only give the proof of line meets circle.

Take 3 points $A = (p, q)$, $B = (r, s)$, $C = (t, u)$ in K_{i-1}, then draw a line between A and B, and a circle of center C with radius w. The equation of the line AB is

$$\frac{x-p}{r-p} = \frac{y-q}{s-q}$$

while the equation of the circle is

$$(x-t)^2 + (y-u)^2 = w^2.$$

Solving them yields

$$(x-t)^2 + \left(\frac{s-q}{r-p}(x-p) + q - u\right)^2 = w^2.$$

Now x, the first coordinate of the intersection point, is a zero of a quadratic polynomial over K_{i-1}. □

We note that fields obtained by adjoining the zeroes of a quadratic polynomial are extensions of degree 2.

Theorem 7.16. *If $r = (x, y)$ is constructible from a subset $P_0 \in \mathbb{R}^2$, and if K_0 is the subfield of $\mathbb{R}$ generated by the coordinates of the points of P_0, then the degrees $[K_0(x) : K_0]$ and $[K_0(y) : K_0]$ are powers of 2.*

Proof. We have that

$$[K_{i-1}(x_i) : K_{i-1}] = 1 \text{ or } 2,\ [K_{i-1}(y_i) : K_{i-1}] = 1 \text{ or } 2.$$

Using multiplication of degrees, we get

$$[K_{i-1}(x_i, y_i) : K_{i-1}] = [K_{i-1}(x_i, y_i) : K_{i-1}(x_i)][K_{i-1}(x_i) : K_{i-1}] = 1 \text{ or } 2 \text{ or } 4$$

with $K_i = K_{i-1}(x_i, y_i)$. Thus $[K_n : K_0]$ is a power of 2 implying that $[K_n : K_0(x)][K_0(x) : K_0]$ is a power of 2 from which we conclude that $[K_0(x) : K_0]$ is a power of 2, and similarly for y. □

We are now ready to discuss the impossibility proofs.

Theorem 7.17. *The cube cannot be duplicated using ruler and compass constructions.*

Proof. Take a cube whose side is the unit interval, that is of volume 1. We have $P_0 = \{(0, 0), (1, 0)\}$ and $K_0 = \mathbb{Q}$. If we could duplicate the cube, then we can construct a point $(\alpha, 0)$ such that the volume α^3 is equal to 2, that is

$$\alpha^3 = 2.$$

Now $[\mathbb{Q}(\alpha):\mathbb{Q}]$ is a power of 2, but α is a zero of t^3-2 which is irreducible (by Eisenstein) over $\mathbb{Q}$. This gives that

$$[\mathbb{Q}(\alpha):\mathbb{Q}]=3,$$

a contradiction to the fact that it should be a power of 2. □

Theorem 7.18. *The angle $\pi/3$ cannot be trisected using ruler and compass constructions.*

Proof. Constructing an angle trisecting $\pi/3$ is equal to constructing the point $(\alpha,0)$ given $(0,0)$ and $(1,0)$ where $\alpha=\cos(\pi/9)$. Knowing $\alpha=\cos(\pi/9)$, we can construct

$$\beta=2\cos(\pi/9).$$

Using that $\cos(3\theta)=4\cos^3(\theta)-3\cos(\theta)$ and $\cos(3\theta)=1/2$ when $\theta=\pi/9$, we have

$$1=8\cos^3(\theta)-6\cos(\theta)\Rightarrow\beta^3-3\beta-1=0.$$

Now $f(t)=t^3-3t-1$ is irreducible over $\mathbb{Q}$ (apply Eisenstein on $f(t+1)$) thus

$$[\mathbb{Q}(\beta):\mathbb{Q}]=3$$

contradicting the fact that it should be a power of 2. □

Theorem 7.19. *The circle cannot be squared using ruler and compass constructions.*

Proof. Without loss of generality, we assume that the circle is the unit circle centered at $(0,0)$. Constructing a square with area π is equivalent to constructing a point $(\sqrt{\pi},0)$. Since the smallest field with 0 and 1 is $\mathbb{Q}$, the field obtained from adjoining $(\sqrt{\pi},0)$ is $\mathbb{Q}(\sqrt{\pi})$. Thus $[\mathbb{Q}(\sqrt{\pi}):\mathbb{Q}]$ should be a power of 2, and in particular it should be algebraic, which is a contradiction (Lindeman's Theorem shows the transcendence of π, 1882). □

The main definitions and results of this chapter are

- **(4.1).** Definitions of: Galois extension, Galois group, fixed field.
- **(4.2).** The fundamental theorem of Galois theory, Galois groups of intermediate fields.
- **(4.3).** Characterization of finite fields, their Galois group, their multiplicative group.
- **(4.4).** Definition of cyclotomic field, primitive root of unity, cyclotomic polynomial. The Galois group of a cyclotomic field.

Chapter 8

Exercises on Galois Theory

Exercises marked by (*) are considered difficult.

8.1 Galois group and fixed fields

Exercise 96. Compute the Galois group of $X^4 - 2$ over $\mathbb{Q}$ and $\mathbb{F}_3$, the finite field with 3 elements.

Answer. Over $\mathbb{Q}$, we have

$$X^4 - 2 = (X^2 - \sqrt{2})(X^2 + \sqrt{2}) = (X - 2^{1/4})(X + 2^{1/4})(X - i2^{1/4})(X + i2^{1/4}),$$

while over $\mathbb{F}_3$, let w be a root of the irreducible polynomial $X^2 + X + 2 = 0$, then

$$w^2 = -w + 1,\ w^4 = -1,\ w^8 = 1$$

and

$$X^4 - 2 = X^4 + 1 = (X^2 - w^2)(X^2 + w^2) = (X - w)(X + w)(X - w^3)(X + w^3).$$

8.2 The fundamental Theorem of Galois theory

Exercise 97.

1. Compute the splitting field K of the polynomial $f(x) = x^4 - 2 \in \mathbb{Q}(x)$.
2. Show that K is a Galois extension.
3. Compute the degree of $K/\mathbb{Q}$.
4. Compute the $\mathbb{Q}$-automorphisms of K.
5. Do you recognize $\text{Gal}(K/\mathbb{Q})$?

6. What are all the subgroups of $\mathrm{Gal}(K/\mathbb{Q})$?

7. What are all the intermediate subfields of $K/\mathbb{Q}$?

8. Among the intermediate subfields, which are normal?

Answer.

1. We have that $f(x) = (x^2-\sqrt{2})(x^2+\sqrt{2}) = (x-\sqrt[4]{2})(x+\sqrt[4]{2})(x+i\sqrt[4]{2})(x-i\sqrt[4]{2})$. Thus the splitting field of f is $\mathbb{Q}(i, \sqrt[4]{2})$.

2. It is a splitting field thus K is normal, it is separable because $\mathbb{Q}$ is of characteristic zero.

3. The degree is
$$[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})][\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}].$$
The minimum polynomial of i over $\mathbb{Q}(\sqrt[4]{2})$ is x^2+1, so $[\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}(\sqrt[4]{2})] = 2$. Since $f(x)$ is irreducible over $\mathbb{Q}$ (by Eisenstein), it is the minimal polynomial of $\sqrt[4]{2}$ over $\mathbb{Q}$, thus $[\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}] = 4$ and finally the total degree is 8.

4. There are 8 of them. We have
$$\sigma(i) = i,\ \sigma(\sqrt[4]{2}) = i\sqrt[4]{2},$$
and
$$\tau(i) = -i,\ \tau(\sqrt[4]{2}) = \sqrt[4]{2}$$
and we can find the others by combining these two, namely:
$$\begin{array}{rcl}
1: & \sqrt[4]{2} \mapsto \sqrt[4]{2}, & i \mapsto i \\
\sigma: & \sqrt[4]{2} \mapsto i\sqrt[4]{2} & i \mapsto i \\
\sigma^2: & \sqrt[4]{2} \mapsto -\sqrt[4]{2} & i \mapsto i \\
\sigma^3: & \sqrt[4]{2} \mapsto -i\sqrt[4]{2} & i \mapsto i \\
\tau: & \sqrt[4]{2} \mapsto \sqrt[4]{2} & i \mapsto -i \\
\sigma\tau: & \sqrt[4]{2} \mapsto i\sqrt[4]{2} & i \mapsto -i \\
\sigma^2\tau: & \sqrt[4]{2} \mapsto -\sqrt[4]{2} & i \mapsto -i \\
\sigma^3\tau: & \sqrt[4]{2} \mapsto -i\sqrt[4]{2} & i \mapsto -i
\end{array}$$

5. This is the dihedral group of order 8.

6.
   - order 8: G, order 1: $\{1\}$.
   - order 4: there are 3 of them
   $$S = \{1, \sigma, \sigma^2, \sigma^3\} \simeq C_4,\ T = \{1, \sigma^2, \tau, \sigma^2\tau\} \simeq C_2 \times C_2,\ U = \{1, \sigma^2, \sigma\tau, \sigma^3\tau\} \simeq C_2 \times C_2.$$

- order 2, there are 5 of them, all isomorphic to C_2:

$$A = \{1, \sigma^2\},\ B = \{1, \tau\},\ C = \{1, \sigma\tau\},\ D = \{1, \sigma^2\tau\},\ E = \{1, \sigma^3\tau\}.$$

7. By Galois correspondence, we obtain the intermediate fiels as fixed fields of the subgroups. The subfields of degree 2 are the easiest to find:

$$\mathbb{Q}(i),\ \mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(i\sqrt{2})$$

which are fixed by resp. S, T and U. By direct computation (that is, apply the automorphism on an element of the larger field, and solve the equation that describes that this element is fixed by this automorphism), we find that the others are:

$$\mathbb{Q}((1+i)\sqrt[4]{2}),\ \mathbb{Q}(i, \sqrt{2}),\ \mathbb{Q}(\sqrt[4]{2}).$$

fixed resp. by C, A and B.

8. The normal subgroups of G are G, S, T, U, A, I, thus their corresponding fixed fields are normal extensions of $\mathbb{Q}$.

Exercise 98. Let K be the subfield of $\mathbb{C}$ generated over $\mathbb{Q}$ by i and $\sqrt{2}$.

1. Show that $[K : \mathbb{Q}] = 4$.
2. Give a primitive element of K and its minimal polynomial.
3. Show that $\mathrm{Gal}(K/\mathbb{Q}) \simeq (\mathbb{Z}/2\mathbb{Z})^2$.
4. Give a list of all the subfields of K.

Answer.

1. Since $K = \mathbb{Q}(i, \sqrt{2})$, we can first build $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ which is of degree 2, because $x^2 - 2$ is irreducible, then we check that $x^2 + 1$ is irreducible over $\mathbb{Q}(\sqrt{2})$, so we obtain another extension of degree 2, by multiplicativity of the degrees, this gives an extension of degree 4.

2. For example, ζ_8, the primitive 8th root of unity, is a primitive element, with minimal polynomial $x^4 + 1$.

3. The Galois group is given by $\{1, \sigma, \tau, \sigma\tau\}$ where

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

4. There is one for each subgroup of the Galois group. Since there are only subgroups of order 2 (but for the whole group and the trivial subgroup), we get 3 quadratic field extensions:

$$\mathbb{Q}(i),\ \mathbb{Q}(\sqrt{2}),\ \mathbb{Q}(i\sqrt{2}).$$

Exercise 99.

1. Show that $X^4 - 3 = 0$ is irreducible over $\mathbb{Q}$.
2. Compute the splitting field E of $X^4 - 3 = 0$.
3. Compute the Galois group of $E/\mathbb{Q}$.
4. Can you recognize this group?
5. Choose two proper, non-trivial subgroups of the Galois group above, and compute their corresponding fixed subfields.

Answer.

1. Use Eisenstein with $p = 3$.
2. The roots of $X^4 - 3$ are $i^j \sqrt[4]{3}$, $j = 0, 1, 2, 3$, thus the splitting field is $\mathbb{Q}(\sqrt[4]{3}, i)$.
3. As in previous exercise, with $\sqrt[4]{3}$ instead of $\sqrt[4]{2}$.
4. It is the dihedral group.
5. Again as in previous exercise.

Exercise 100. Consider the field extensions $M = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ and $E = M(\alpha)$ where $\alpha = \sqrt{(2+\sqrt{2})(3+\sqrt{3})}$.

1. Show that M is a Galois extension of $\mathbb{Q}$ with Galois group $C_2 \times C_2$.
2. Denote by σ and τ the generators of the two cyclic groups of (1), so that the Galois group of M is written $\langle\tau\rangle \times \langle\sigma\rangle$.
   - Compute $\sigma(\alpha^2)/\alpha^2$ and deduce that $\alpha \notin M$. What is the degree of E over $\mathbb{Q}$?
   - Extend σ to an automorphism of E and show that this automorphism has order 4.
   - Similarly extend τ to an automorphism of E and compute its order. What is the Galois group of E over $\mathbb{Q}$?

Answer.

1. $M/\mathbb{Q}$ is clearly Galois because it is separable ($\mathbb{Q}$ is of characteristic 0) and normal.
2.
   - We have $\sigma(\alpha^2)/\alpha^2 = (\sqrt{2}-1)^2$ thus $\sigma(\alpha^2) = (\alpha(\sqrt{2}-1)^2$. If α were in M, then $\sigma(\alpha) = \pm\alpha(\sqrt{2}-1)$ and $\sigma^2(\alpha) = \alpha(\sqrt{2}-1)(-\sqrt{2}-1) = -\alpha$, a contradiction ($\sigma^2(\alpha) = \alpha$).
   - We have $\sigma^2(\alpha) = -\alpha$ thus $\sigma^4(\alpha) = \alpha$, $\sigma^4|M = 1$ and $\sigma^2 \neq 1$.

- We compute that $\tau(\alpha) = \frac{3-\sqrt{3}}{\sqrt{6}}\alpha$, we extend τ and its order is 4. We then compute that
$$\sigma\tau(\alpha) = \frac{3-\sqrt{3}}{-\sqrt{6}}(\sqrt{2}-1)\alpha,\ \tau(\sigma(\alpha) = (\sqrt{2}-1)\frac{3-\sqrt{3}}{\sqrt{6}}\alpha$$
so σ and τ anticommute, and they are both of order 3, so the Galois group is the quaternion group.

Exercise 101. Let L/K be a Galois extension of degree 8. We further assume that there exists a subextension M/K of degree 4 which is not a Galois extension.

- Show that the Galois group G of L/K cannot be abelian.
- Determine the Galois group G of L/K.

Answer.

- A subextension M/K of degree 4 which is not Galois, means that there is a subgroup of order 2 which is not normal in G. Thus G cannot be abelian, since all subgroups of an abelian group are all normal.
- The only groups of order 8 which are not abelian are D_4 and Q_8. All the subgroups of Q_8 are normal, thus it must be D_4.

Exercise 102. Assume that the polynomial $X^4+aX^2+b \in \mathbb{Q}[X]$ is irreducible. Prove that its Galois group is:

1. the Klein group if $\sqrt{b} \in \mathbb{Q}$.
2. the cyclic group of order 4 if $\sqrt{a^2-4b}\sqrt{b} \in \mathbb{Q}$.

Answer.

1. Set $Y = X^2$, then
$$Y^2 + aY + b = (Y - y_1)(Y - y_2)$$
with
$$y_1 = \frac{-a+\sqrt{a^2-4b}}{2}, y_2 = \frac{-a-\sqrt{a^2-4b}}{2}$$
and $X = \pm\sqrt{Y}$ so that the four roots are $\pm\sqrt{y_1}, \pm\sqrt{y_2}$. Now $y_1y_2 = b$ thus
$$\sqrt{y_1}\sqrt{y_2} = \sqrt{b} \in \mathbb{Q}$$
and if $\sigma(\sqrt{y_1}) = \sqrt{y_2}$, then we have that
$$\sigma(\sqrt{y_2}) = \sqrt{b}/\sigma(\sqrt{y_1}) = \sqrt{b}/\sqrt{y_2} = \sqrt{y_1}$$
and all the elements of the Galois group have order 2, so that it must be the Klein group.

2. We have
$$y_1 - y_2 = \sqrt{a^2 - 4b},$$
thus
$$\sqrt{y_1}\sqrt{y_2}(y_1 - y_2) = \sqrt{b}\sqrt{a^2 - 4b} \in \mathbb{Q}.$$
Now take $\sigma(\sqrt{y_1}) = \sqrt{y_2}$ and if it were of order 2, then $\sigma(\sqrt{y_2}) = \sqrt{y_1}$ and
$$\sigma(\sqrt{y_1}\sqrt{y_2}(y_1 - y_2)) = \sqrt{y_1}\sqrt{y_2}(y_2 - y_1)$$
which contradicts that $\sqrt{y_1}\sqrt{y_2}(y_1 - y_2) \in \mathbb{Q}$ thus σ is of order 4 and the Galois group must be the cyclic group of order 4.

8.3 Finite fields

Exercise 103. Identify the finite fields $\mathbb{Z}[i]/(2 + i)$ and $\mathbb{Z}[i]/(7)$.

Answer. $\mathbb{F}_5$ and $\mathbb{F}_{49}$

Exercise 104. Consider the following two polynomials $p(x) = x^2 - x - 1 \in \mathbb{F}_3[x]$ and $q(x) = x^2 + 1 \in \mathbb{F}_3[x]$. Consider the fields $\mathbb{F}_3[x]/(p(x)) \simeq \mathbb{F}_3(\alpha)$ where $p(\alpha) = 0$ and $\mathbb{F}_3[x]/(q(x)) \simeq \mathbb{F}_3(\beta)$ where $q(\beta) = 0$.

1. Compute $(\alpha + 1)^2$.

2. Deduce that the two fields $\mathbb{F}_3(\alpha)$ and $\mathbb{F}_3(\beta)$ are isomorphic.

Answer.

1. We have $(\alpha + 1)^2 = \alpha^2 - \alpha + 1 = (\alpha + 1) - \alpha + 1 = 2 = -1$.

2. We have that $\beta^2 = -1$ by definition of β and we have just shown above that $(\alpha+1)^2 = -1$, thus it is natural to map β to $\alpha+1$, that is $f : \mathbb{F}_3(\beta) \to \mathbb{F}_3(\alpha),\ a + b\beta \mapsto a + b(\alpha + 1)$. Check that f is a ring homomorphism. Then argue that a field homomorphism is always injective, and that both fields have same number of elements.

Exercise 105. Let $\mathbb{F}_2$ be the finite field with two elements.

1. Show that $\mathbb{F}_2(\beta) = \mathbb{F}_2[X]/(q(X))$ is a finite field, where $q(X) = X^2+X+1$ and $q(\beta) = 0$.

2. Consider the polynomial $r(Y) = Y^2 + Y + \beta \in \mathbb{F}_2(\beta)[Y]$, and set $L = \mathbb{F}_2(\beta)[Y]/(r(Y))$.
   - Is L a field? Justify your answer.
   - What is the cardinality of L? What is its characteristic? Justify your answers.

Answer.

1. It is enough to show that $q(X)$ is irreducible over $\mathbb{F}_2$, this generates the finite field $\mathbb{F}_4 \simeq \mathbb{F}_2(\beta)$.

2. - We have to see if $r(Y)$ is irreducible over $\mathbb{F}_4$. It is enough to evaluate it in β and $\beta + 1$ to see that it is not zero.
   - This creates an extension of degree 2 of $\mathbb{F}_4$, that is 16 elements. It has characteristic 2.

Exercise 106. - Let $\mathbb{F}_p$ be a finite field, $p \geq 3$ a prime number. Show that the sum of all the elements of $\mathbb{F}_p$ is 0.

- Let $q = p^n$, p a prime. Show that if $q \neq 2$, then the sum of all elements of $\mathbb{F}_q$ is 0.
- Let $q = p^n$, p a prime. Show that the product of all the non-zero elements of a finite field $\mathbb{F}_q$ is -1.

Answer.

- There are many ways of doing that. Modulo p, one could simply notice that $1+2+\ldots+p-1$ is $p(p-1)/2$, if $p \geq 3$, p is an odd prime, thus $p-1$ is even, $(p-1)/2$ is an integer and thus mod p we do get 0.
- An element a in $\mathbb{F}_q$ satisfies that $a^{p^n} = a$, that is, it is a root of $X^{p^n} - X$. Now all the roots of this polynomial exactly coincide with the elements of $\mathbb{F}_q$, that is, we can write
$$X^{p^n} - X = \prod_{a \in \mathbb{F}_q} (X - a).$$
If we develop the product, we get that the term in X^{p^n-1} has as coefficients exactly the sum of the elements of $\mathbb{F}_q$, which is thus 0.
- This follows from above. Now we just factor X from the polynomial $X^{p^n} - X$ to get
$$X^{p^n-1} - 1 = \prod_{a \in \mathbb{F}_q^*} (X - a).$$
Now -1 corresponds to the constant term of the product, which is exactly the product over all non-zero elements of the finite field.

Exercise 107. Consider the finite fields $\mathbb{F}_2, \mathbb{F}_3$ and $\mathbb{F}_4$, and the polynomial $P(Y) = Y^3 + Y + 1$. Over which of these finite fields is $P(Y)$ irreducible? If possible, construct the corresponding field extension.

Answer. Since this polynomial is of degree 3, if it is reducible, that means there is at least one linear term, that is one root in the base field. It is thus irreducible over $\mathbb{F}_2$, however over $\mathbb{F}_3$, we have that $P(1) = 0$, and over $\mathbb{F}_4$, we have no root. Over $\mathbb{F}_2$, we get an extension of degree 3, that is $\mathbb{F}_8$, over $\mathbb{F}_4$, we get an extension of degree 3, that is $\mathbb{F}_{4^3}$.

4.4 Cyclotomic fields

Exercise 108. Let ζ be a primitive 20th root of unity in $\mathbb{C}$, and let $E = \mathbb{Q}(\zeta)$.

- Compute the Galois group $\mathrm{Gal}(E/\mathbb{Q})$.
- How many subfields of E are there which are quadratic extensions of $\mathbb{Q}$?
- Determine the irreducible polynomial of ζ over $\mathbb{Q}$.

Answer.

- We know that $\mathrm{Gal}(E/\mathbb{Q}) \simeq (\mathbb{Z}/20\mathbb{Z})^*$.
- There are 3 of them: $\mathbb{Q}(i\sqrt{5})$, $\mathbb{Q}(\sqrt{5})$ and $\mathbb{Q}(i)$.
- It is $X^8 - X^6 + X^4 - X^2 + 1$.

4.5 Solvability by radicals

4.6 Solvability by ruler and compasses

Exercise 109. True/False.

Q1. An extension having Galois group of order 1 is normal.

Answer.

Q1. It's false! If there is only one element, then it's the identity. Again $\mathbb{Q}(\alpha)$ with $\alpha^3 = 2$ has a Galois group with only the identity, and it is not normal!