Notes on Galois Theory

Contents

7 Splitting fields and Galois groups **2**
7.1 Splitting fields . . . 2
7.2 The Galois group . . . 3
7.3 Galois extensions . . . 5
7.4 Exercises . . . 8

8 The Main Theorem of Galois theory **9**
8.1 Fixed fields . . . 9
8.2 Main Theorem . . . 10
8.3 Examples of Galois correspondences . . . 11
8.4 Extending Galois extensions . . . 14
8.5 Simple extensions . . . 14

9 Solving equations **16**
9.1 Symmetric polynomials . . . 16
9.2 Solution of the cubic equation . . . 16
9.3 Solution of the quartic equation . . . 17
9.4 Radical extensions . . . 17
9.5 Solvability . . . 18
9.6 Main Theorem . . . 20
9.7 Exercises . . . 21

7 Splitting fields and Galois groups

7.1 Splitting fields

In previous chapters we have considered fields extensions L/K and studied elements in L, algebraic over K, and their minimal polynomials. In this section we shall reverse the approach. Given a field K and a polynomial $f \in K[x]$, does there exist a field extension of K which contains a zero of f? More generally, does there exist a field extension which contains all zeros of f?
We begin by answering the first question.

Theorem 7.1.1 *Let K be a field and $f(X) \in K[X]$ a non-constant polynomial. Then there exists a finite field extension L/K such that L contains a zero of $f(X)$.*

Proof. When f is irreducible in $K[X]$ we know that $K[X]/(f)$ is a field which contains the element $X \pmod f$ as obvious zero.
Suppose f is reducible in $K[X]$. Let g be an irreducible factor of f. Then clearly $K[X]/(g)$ is again a finite extension of K which contains a zero of g, hence it contains a zero of f.

We now address the question if there is a field extension which contains all zeros of a given polynomial f. To put the question more precisely we use the term splitting field.

Definition 7.1.2 Let K be a field and $f \in K[X]$ a monic polynomial of degree $n > 0$. A field extension L of K is called a *splitting field* of f over K if

1. There exist $\alpha_1, \ldots, \alpha_n$ such that $f = \prod_{i=1}^{n}(X - \alpha_i)$ and
2. $L = K(\alpha_1, \ldots, \alpha_n)$.

Theorem 7.1.3 *Let K be a field and $f \in K[X]$ a non-constant polynomial. Then there exists a splitting field of f over K.*

Proof. We argue by induction on the degree of f, which we assume to be monic. When $\deg(f) = 1$ we see that K itself is a splitting field.
Suppose $n > 1$ and assume that we proved our statement for all polynomials of degree $n-1$. By theorem 7.1.1 we know that there exists a finite extension K_1/K and $\alpha \in K_1$ such that $f(\alpha) = 0$. Hence there exists $g \in K_1[X]$ such that $f(X) = (X-\alpha)g(X)$. The degree of g is $n-1$, hence by our induction hypothesis there is a splitting field L of g over K_1. A fortiori f factors into linear factors $X-\alpha_i$ in $L[X]$. For the splitting field of f over K we simply take the field extension $K(\alpha_1, \ldots, \alpha_n) \subset L$.

A question that arises immediately is whether the splitting field of a polynomial is uniquely determined. In answering this question it is important to state when two extensions are considered the same. Before dealing with the question of the uniqueness of a splitting field in Corollary 7.3.8 we first introduce the concept of field isomorphisms.

7.2 The Galois group

Definition 7.2.1 Let K, K' be two fields. A ring homomorphism $\phi : K \to K'$ is said to be a *field morphism* if in addition $\phi(1) = 1$. The kernel of ϕ is an ideal in K, hence either (0) or K itself. Since $\phi(1) = 1$ we get that $\ker(\phi) = (0)$ and so a field morphism is always injective. This is the reason we speak of a field morphism rather than a field homomorphism.
A field morphism is called a *field isomorphism* if it is a bijection.
A field isomorphism of a field K to itself is called a *field automorphism*.
The group of automorphisms of a field K is denoted by $\mathrm{Aut}(K)$.

Example 7.2.2 $\mathrm{Aut}(\mathbb{Q}) = \mathrm{id}$.

Example 7.2.3 Complex conjugation $z \mapsto \bar{z}$ is a field automorphism of $\mathbb{C}$.

Example 7.2.4 Let K be a finite field. Since K cannot contain $\mathbb{Q}$ it must have positive characteristic p. The map $F_p : K \to K$ given by $f_p(x) = x^p$ is a field morphism. Because a field morphism is injective and K finite, F_p is automatically a bijection and thus an element of $\mathrm{Aut}(K)$. We call F_p the *Frobenius automorphism* of K.
An example of a finite field other that $\mathbb{F}_p$ is $\mathbb{F}_3[X]/(X^2+1)$.

Example 7.2.5 Consider the subfields $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\omega\sqrt[3]{2})$ and $\mathbb{Q}(\omega^2\sqrt[3]{2})$ of $\mathbb{C}$. Here $\omega = e^{2\pi i/3}$ is a primitive cube root of unity. Notice that all three numbers $\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}$ are zeros of the polynomial $X^3 - 2$ which is irreducible in $\mathbb{Q}[X]$. By Theorem **??** all three fields are isomorphic to $Q[X]/(X^3-2)$. Notice that $\mathbb{Q}(\sqrt[3]{2})$ is a subfield of $\mathbb{R}$, whereas the other two are not. In spite of this all three fields are isomorphic. For example $\mathbb{Q}(\sqrt[3]{2})$ is isomorphic to $\mathbb{Q}(\omega\sqrt[3]{2})$ via the isomorphism σ determined by $\sigma(x) = x$ for all $x \in \mathbb{Q}$ and $\sigma(\sqrt[3]{2}) = \omega\sqrt[3]{2}$.

The above example is an example of an isomorphism between two extensions L, L' of $\mathbb{Q}$ which fixes the elements of $\mathbb{Q}$. Such isomorphisms, where $\mathbb{Q}$ can be any ground field K, are going to be the important maps in Galois theory.

Definition 7.2.6 Let K be a field and L, L' two finite extensions. An isomorphism $\sigma : L \to L'$ is called a *K-isomorphism* if it is a field isomorphism with the additional property that $\sigma(x) = x$ for all $x \in K$.
Let K be a field and L a finite extension. An automorphism $\sigma : L \to L$ is called a K-automorphism it is a field isomorphism with the additional property that $\sigma(x) = x$ for all $x \in K$.
The group of K-automorphisms of a finite extension L is called the *Galois group* of the extension L/K.
Notation: $\mathrm{Gal}(L/K)$.

Remark 7.2.7 Let K be a field, $f \in K[X]$ a non-constant polynomial and L a splitting field of f over K. Let $\alpha \in L$ be a zero of f and $\sigma \in \mathrm{Gal}(L/K)$. Since σ is a K-automorphism it fixes the elements of K. In particular, it follows from $\sigma(f(\alpha)) = 0$ that $f(\sigma(\alpha)) = 0$. This means that an element σ of $\mathrm{Gal}(L/K)$ permutes the zeros of f. Moreover, the action of σ is uniquely determined by the way in which the zeros of f are permuted.
However, not necessarily all permutations of the zeros of f occur as elements of $\mathrm{Gal}(L/K)$.

The following Proposition allows us to determine the Galois group in the case of simple extensions.

Proposition 7.2.8 *Let K be a field, and L an extension of K generated by one element α. So $L = K(\alpha)$. Let f be the minimal polynomial of α. Suppose that L contains another zero β of f. The field morphism σ determined by $\sigma(\alpha) = \beta$ and $\sigma(x) = x$ for all $x \in K$ is an element of $\mathrm{Gal}(L/K)$.*
Conversely, every element of $\mathrm{Gal}(L/K)$ is given in this way. In particular $|\mathrm{Gal}(L/K)|$ equals the number of distinct zeros of f.

Proof. From Lemma **??** we know that we have

$$K(\alpha) \cong K[X]/(f) \cong K[\beta]$$

via the K-isomorphisms given by $\alpha \mapsto X (\mathrm{mod}\ f) \mapsto \beta$. Hence the isomorphism σ determined by $\sigma(\alpha) = \beta$ and $\sigma(x) = x$ for all $x \in K$ is in $\mathrm{Gal}(L/K)$.
Conversely, every element $\sigma \in \mathrm{Gal}(L/K)$ maps α to another zero of f. If the number of distinct zeros of f in L is m, the number of K-automorphisms of L is also m.

Example 7.2.9 $|\mathrm{Gal}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})| = 2$. The automorphisms are given by $\sqrt{2} \mapsto \sqrt{2}$, which is the identity map and $\sqrt{2} \mapsto -\sqrt{2}$.

Example 7.2.10 $|\mathrm{Gal}(\mathbb{C}/\mathbb{R})| = 2$ and the group is generated by complex conjugation, which is an $\mathbb{R}$-automorphism of $\mathbb{C}$.

Example 7.2.11 Consider the fifth root of unity $\zeta = e^{2\pi i/5}$. Its minimal polynomial over $\mathbb{Q}$ is $(X^5 - 1)/(X - 1) = X^4 + X^3 + X^2 + X + 1$. The other zeros are given by $\zeta^k = e^{2\pi ki/5}$ for $k = 1, 2, 3, 4$ which clearly belong to $\mathbb{Q}(\zeta)$. Consider the K-automorphism σ given by $\sigma : \zeta \mapsto \zeta^3$. Notice that

$$\sigma^2(\zeta) = (\zeta^3)^3 = \zeta^4, \quad \sigma^3(\zeta) = (\zeta^3)^4 = \zeta^2$$

and finally $\sigma^4(\zeta) = (\zeta^3)^2 = \zeta$. So $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3\}$. This is example of a field over $\mathbb{Q}$ with a cyclic Galois group.

Example 7.2.12 Let $K = \mathbb{F}_p(t)$ the function field in one variable t and coefficients in $\mathbb{F}_p$. The polynomial $X^p - t$ is irreducible in $K[X]$ because it is an Eisenstein polynomial with respect to the irreducible element $t \in \mathbb{F}_p[t]$. Denote a zero of $X^p - t$ by $t^{1/p}$ and define $L = K(t^{1/p})$. Then, in L we have the factorisation $X^p - t = (X - t^{1/p})^p$. In other words, $X^p - t$ has precisely one distinct zero. Therefore the Galois group $\mathrm{Gal}(L/K)$ can map $t^{1/p}$ only to $t^{1/p}$. Hence $\mathrm{Gal}(L/K)$ consists of precisely one element, which is the identity map.

Example 7.2.13 Let $L = \mathbb{Q}(\sqrt[3]{2})$. Any element $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ maps $\sqrt[3]{2}$ to a zero of $X^3 - 2$. But L contains only one zero of $X^3 - 2$ namely $\sqrt[3]{2}$ itself. Hence $\mathrm{Gal}(L/\mathbb{Q})$ consists of only one element, namely the identity map.

Example 7.2.14 Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. This is an extension of degree 4 over $\mathbb{Q}$, but it is not written as a simple extension. Of course an element in $\mathrm{Gal}(L/\mathbb{Q})$ maps $\sqrt{2}$ to $\pm\sqrt{2}$ and $\sqrt{3}$ to $\pm\sqrt{3}$. But it is not clear if all choices of $\pm$-signs are possible.
To answer this question we note that $\sqrt{2} + \sqrt{3}$ is an element of L of degree 4. Hence $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$. The minimal polynomial of $\sqrt{2} + \sqrt{3}$ reads $f = X^4 - 10X^2 + 1$ and the complete set of zeros reads $\pm\sqrt{2}\pm\sqrt{3}$, each of which is contained in $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. According to Theorem 7.2.8 the Galois group consists of 4 elements. Hence for every choice of signs $\epsilon_2, \epsilon_3 \in \{\pm 1\}$ there exists $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ such that $\sigma(\sqrt{2}) = \epsilon_2\sqrt{2}$ and $\sigma(\sqrt{3}) = \epsilon_3\sqrt{3}$.
Let us define in particular $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ by $\sigma(\sqrt{2}) = -\sqrt{2}$ and $\sigma(\sqrt{3}) = \sqrt{3}$. We define τ by $\tau(\sqrt{2}) = \sqrt{2}$ and $\tau(\sqrt{3}) = -\sqrt{3}$. We easily check that $\sigma^2 = \tau^2 = \mathrm{id}$ and $\sigma\tau = \tau\sigma$. Thus we see that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q})$ is isomorphic to the fourgroup of F.Klein.

Motivated by the last example one might have the idea to determine the Galois group of a finite extension L/K in the following way. Determine an element $\alpha \in L$ such that $L = K(\alpha)$. Let $f \in K[X]$ be the minimal polynomial of α over K. Then determine the number of distinct zeros of f that are contained in L. This is precisely the order of $\mathrm{Gal}(L/K)$.
Although this is certainly a feasible approach, we shall not follow it here. Instead we prefer to get some more insight into general properties of Galois groups.

7.3 Galois extensions

We first show the following Theorem.

Theorem 7.3.1 *Let K be a field and L a finite extension. Then $|\mathrm{Gal}(L/K)| \leq [L : K]$.*
Moreover, if $|\mathrm{Gal}(L/K)| = [L : K]$ then for every $\alpha \in L$, the minimal polynomial f of α over K has precisely $\deg(f)$ distinct zeros in L.

Proof. We proceed by induction on $[L : K]$. For $[L : K] = 1$ the statement is obvious. Let now $n > 1$ and assume our Theorem is proved for all extensions L/K with $[L : K] < n$. Now assume that $[L : K] = n$. Let α be any element in L and not in K. Let $G = \mathrm{Gal}(L/K)$ and $H = \mathrm{Gal}(L/K(\alpha))$. Clearly H is a subgroup of G. Consider the right coset decomposition $G = \cup_{i=1}^{r} g_i H$ where $g_i \in G$ for $i = 1, \ldots, r$ and the sets $g_i H$ are pairwise disjoint. Let f be the minimal polynomial of α over K and suppose it has degree d. Now note that $g_i(\alpha)$ are zeros of f for $i = 1, \ldots, r$. Moreover, they are disjoint. For if $g_i(\alpha) = g_j(\alpha)$ for some $i \neq j$ we would get $g_i^{-1} g_j(\alpha) = \alpha$ and hence $g_i^{-1} g_j \in H$. This contradicts the definition in which g_i, g_j belong to different cosets. Since the $g_i(\alpha)$ are distinct elements in a set of at most d elements we find that $r \leq d$. By the induction hypothesis $|H| = |\mathrm{Gal}(L/K(\alpha))| \leq [L : K(\alpha)]$, so we get

$$|\mathrm{Gal}(L/K)| = |G| = r|H| \leq d|H| \leq [K(\alpha) : K][L : K(\alpha)] = [L : K].$$

This completes the induction step.
Moroever, if $|\mathrm{Gal}(L/K)| = [L : K]$ we infer that $r = d$. In other words, f has precisely d distinct zeros, as asserted.

We shall now be interested in those finite extensions L/K for which $|\mathrm{Gal}(L/K)| = [L : K]$. We call these extensions *Galois extensions*. Computation of their Galois group will be our main concern. Of course we need some easy criteria by which we can recognize Galois extensions.
Before we continue we need two more definitions.

Definition 7.3.2 Let L/K be a finite extension. Then L is called *normal* over K if every irreducible polynomial in $K[X]$ with a zero in L has all of its zeros in L.

Definition 7.3.3 Let L/K be a finite extension. An element $\alpha \in L$ is called *separable* over K if its minimal polynomial f has no multiple zeros in a splitting field of f. The element α is called *inseparable* over K if F has a multiple zero.
The extension L/K is called separable if all of its elements are separable over K.

An example of an inseparable extension is given by Example 7.2.12. There the element $t^{1/p}$ is inseparable over $\mathbb{F}_p(t)$. Notice that in $\mathbb{F}_p(t)$ the derivative of $X^p - t$ with respect to X is identically 0. This is the way to recognize inseparable elements.

Proposition 7.3.4 *Let L/K be a finite extension. Let $\alpha \in L$ and let f be its minimal polynomial over K. Then α is inseparable over K if and only if K has positive characteristic p and the derivative of f is identically zero. The latter condition is equivalent to $f \in K[X^p]$.*

Proof. Suppose f has a multiple common zero in some splitting field of f over K. Then f and its derivative f' have a common divisor. A fortiori they should have a common divisor in $K[X]$. Since f is irreducible in $K[X]$ this implies that f divides f'. Since $\deg(f') < \deg(f)$ this is only possible if $f' = 0$. Let $a_i X^i$ be any non-trivial term in f. Its derivative is $ia_i X^{i-1}$. This can only be zero if i is divisible by p. Hence $X^i = (X^p)^{i/p}$. We conclude that $f \in K[X^p]$.
Suppose conversely that $f(X) = g(X^p) \in K[X^p]$. Then $f(X) = f(X) - f(\alpha) = g(X^p) - g(\alpha^p) = (X^p - \alpha^p)h(X^p)$ for some $h \in L[X]$. Hence $f(X) = (X - \alpha)^p h(X^p)$ and f has a multiple zero α.

We see that separability questions only play a role if the ground field has positive characteristic. In characteristic zero, for example when $K = \mathbb{Q}$ we need not worry about (in)separability.
The main result of this section will be the following Theorem.

Theorem 7.3.5 *Let L/K be a finite extension. Then the following statements are equivalent,*

1. $|\mathrm{Gal}(L/K)| = [L : K]$ *(i.e. L/K is a Galois extension).*
2. *L/K is a normal and separable extension.*
3. *L is the splitting field over K of a polynomial $f \in K[X]$ with distinct zeros. (We call such f separable).*

Note that the implication 7.3.5(1)$\Rightarrow$ 7.3.5(2) follows immediately from the second part of Theorem 7.3.1.
The implication 7.3.5(2)$\Rightarrow$ 7.3.5(3) is also straightforward. Suppose that $L = K(\alpha_1, \ldots, \alpha_r)$. Let $g_i \in K[X]$ be the minimal polynomial of α_i for $i = 1, \ldots, r$. By the normality assumption all zeros of every g_i are in L and moreover, by the separability condition, these zeros are distinct for each g_i. Let now f be the product over the distinct elements in the set $\{g_1, g_2, \ldots, g_r\}$. Then f has distinct zeros and L is its splitting field.
The implication 7.3.5(3)$\Rightarrow$ 7.3.5(1) is the hardest part of the proof of Theorem 7.3.5 and the remainder of this Section will be devoted to it.
The fundamental tool will be the following Proposition.

Proposition 7.3.6 *Let K and K' be fields which are isomorphic via an isomorphism $\sigma : K \to K'$. Let L/K and L'/K' be two finite extensions. To any $p \in K[X]$ given by $p(X) = \sum_i p_i X^i$ we associate the polynomial $p^\sigma \in K'[X]$ given by $p^\sigma(X) = \sum_i \sigma(p_i) X^i$.*
Let $\alpha \in L$ and let f be the minimal polynomial of α over K. Suppose that L' contains a zero α' of f^σ. Then there is an isomorphism $\tau : K(\alpha) \to K'(\alpha')$ given by $\tau(\alpha) = \alpha'$ and $\tau(x) = \sigma(x)$ for all $x \in K$. In other words, τ is an extension of the isomorphism $\sigma : K \to K'$ to $K(\alpha)$.

Proof. By Theorem **??** we know that $K(\alpha) \cong K[X]/(f)$ and $K(\alpha') \cong K'[X]/(f^\sigma)$. We now show that $K[X]/(f) \cong K'[X]/(f^\sigma)$. Consider the homomorphism $\phi : K[X] \to K'[X]/(f^\sigma)$ given by $p \mapsto p^\sigma \pmod{f^\sigma}$. Notice that

$$p \in \ker(\phi) \iff f^\sigma | p^\sigma \iff f|p \iff p \in (f).$$

Hence $\ker(\phi) = (f)$ and via the isomorphism theorem we get $K[X]/(f) \cong K'[X]/(f^\sigma)$. Notice also that ϕ restricted to K is simply the morphism σ.
The resulting isomorphism is now given by $x \mapsto \sigma(x)$ for all $x \in K$ and $\alpha \mapsto X \pmod{f} \mapsto X \pmod{f^\sigma} \mapsto \alpha'$. This is precisely our desired map τ.

An important application is the following Proposition.

Proposition 7.3.7 *Let K, K' be two fields isomorphic via $\sigma : K \to K'$. Let $f \in K[X]$. Let L be a splitting field of f over K and L' a splitting field of f^σ over K'. Then the isomorphism σ can be extended to an isomorphism $\tau : L \to L'$ (in other words $\tau|_K = \sigma$).*

Proof. We proceed by induction on $[L : K]$. When $[L : K] = 1$ our statement is clear, we then have $L = K$ and $L' = K'$. Let $n > 1$ and suppose our Proposition is proven for all L/K with $[L : K] < n$. Suppose $[L : K] = n$.
Let g be an irreducible factor of f of degree > 1 and $\alpha \in L$ a zero of g. Let $\alpha' \in L'$ be a zero of g^σ. By Proposition 7.3.6 there exists an isomorphism $\rho : K(\alpha) \to K'(\alpha')$ such that $\rho|_K = \sigma$.
The degree of $[L : K(\alpha)]$ is less than n. Furthermore, L is a splitting field of f over $K(\alpha)$ and L' is a splitting field of f^σ over $K'(\alpha')$. Hence our induction hypothesis applies and we can extend ρ to an isomorphism $\tau : L \to L'$ such that $\tau|_L = \rho$ and, a fortiori, $\tau|_K = \sigma$.

When we take $K' = K$ and for σ the identity map we immediately get the following Corollary.

Corollary 7.3.8 *Let K be a field, $f \in K[X]$ a non-constant polynomial and L, L' two splitting fields of f over K. Then L, L' are K-isomorphic.*

Hence the splitting field of a polynomial over K is uniquely determined up to K-isomorphism. From now on we could also speak of *the* splitting field of a polynomial if one wants.

Proof. of 7.3.5(3)⇒ 7.3.5(1). We again proceed by induction on $[L : K]$. Again the case $[L : K] = 1$ is clear. Let $n > 1$ and suppose our statement is proven for all extensions of degree $< n$. Now assume that $[L : K] = n$. Let g be an irreducible factor of f of degree $d > 1$. Then by separability of f the polynomial g has d distinct zeros in L which we denote by $\alpha^{(1)}, \ldots, \alpha^{(d)}$. We abbreviate $\alpha^{(1)} = \alpha$. According to Proposition 7.3.6 with $K' = K$ there is a K-isomorphism $\sigma_i : K(\alpha) \to K(\alpha^{(i)})$ such that $\sigma_i(\alpha) = \alpha^{(i)}$ for $i = 1, \ldots, r$. According to Proposition 7.3.7 with $L' = L$ we can extend these isomorphisms to isomorphisms $g_i : L \to L$ such that $g_i|_K(\alpha) = \sigma_i$ for $i = 1, \ldots, d$. And a fortiori, since the σ_i are K-isomorphisms, the g_i are K-isomorphisms. Hence $g_1, \ldots, g_d \in \mathrm{Gal}(L/K)$.
Note that L is a splitting field of f over $K(\alpha)$. Hence our induction hypothesis applies and we find that $|\mathrm{Gal}(L/K(\alpha))| = [L : K(\alpha)]$. Denote $H = \mathrm{Gal}(L/K(\alpha))$. Of course H is a subgroup of $\mathrm{Gal}(L/K)$. We assert that all elements $g_i h$ with $i = 1, \ldots, d$ and $h \in H$ are distinct. Suppose two of them would be equal, say $g_i h = g_j h'$. Apply these two elements to α. We then get $g_i h(\alpha) = g_i(\alpha) = \alpha^{(i)}$. Similarly $g_j h'(\alpha) = \alpha^{(j)}$. Hence $\alpha^{(i)} = \alpha^{(j)}$ and so $i = j$. Consequently $h = h'$.
Hence we have found that

$$|\mathrm{Gal}(L/K)| \geq d|H| = [K(\alpha) : K][L : K(\alpha)] = [L : K].$$

Since also $|\mathrm{Gal}(L/K)| \leq [L : K]$ our desired equality follows.

An interesting Corollary of Theorem 7.3.5 is the equivalence of 7.3.5(2) and 7.3.5(3) which we explicitly state here.

Corollary 7.3.9 *Let K be a field. An extension of K is normal and separable if and only if it is a splitting field of a separable polynomial.*

It turns out, but we will not prove it here, that we can toss out the separability condition.

Theorem 7.3.10 *Let K be a field. An extension of K is normal if and only if it is a splitting field of a polynomial.*

In particular, in a splitting field L/K every polynomial in $K[X]$, which has a zero in L, factors completely into linear factors in $L[X]$.

7.4 Exercises

7.1. Bepaal een splijtlichaam van $X^3 - 7$ in $\mathbb{C}$, bepaal al zijn $\mathbb{Q}$-automorfismen en alle $\mathbb{Q}$-inbeddingen van de wortellichamen in het splijtlichaam.

7.2. Laat L een splijtlichaam zijn van f over K en $f = \prod_{i=1}^{n}(X - \alpha_i)$. Bewijs: $L = K(\alpha_1, ..., \alpha_{n-1})$ (dus met één alpha minder!).

7.3. Laat ζ een nulpunt zijn van $f = X^4 + X^3 + X^2 + X + 1$. Bewijs dat $\zeta^5 = 1$ en dat ζ^2, ζ^3 en ζ^4 de andere wortels zijn van f in $\mathbb{C}$. Bewijs dat $\mathbb{Q}(\zeta)$ een splijtlichaam is van f over $\mathbb{Q}$.

7.4. Toon aan dat $\mathbb{Q}(\sqrt[4]{2})$ en $\mathbb{Q}(i\sqrt[4]{2})$ twee $\mathbb{Q}$-isomorfe lichamen zijn.

Voor volgende opgaves mag je **??** gebruiken.

7.5. Zijn volgende lichamen splijtlichamen van een polynoom of niet (hierbij is t transcendent over $\mathbb{F}_3$):
(a) $\mathbb{F}_3(t)(\sqrt[3]{t})$ over $\mathbb{F}_3(t)$?
(b) $\mathbb{F}_3(t)(\sqrt[4]{t})$ over $\mathbb{F}_3(t)$?

7.6. Geef een voorbeeld van een toren van lichaamsuitbreidingen $F \subset K \subseteq E$ met K/F en E/K normaal, maar E/F niet normaal.
7.7 Zijn volgende polynomen separabel of niet?
(a) $x^3 + x^2 - x - 1$ over $\mathbb{Q}$?
(b) $x^4 + x^2 + 1$ over $\mathbb{F}_2$?
(c) $x^{10} + x^5 + 3$ over $\mathbb{F}_3$?
(d) $x^{10} + 4t$ over $\mathbb{F}_5(t)$ met t transcendent over $\mathbb{F}_5$?

8 The Main Theorem of Galois theory

8.1 Fixed fields

To prove the Main Theorem 8.2.1 we first need two important ingredients, namely the Theorems of Dedekind and Artin.
Let K, L be two fields. A *multiplicative function* $\chi : K^* \to L^*$ is a function with the property that $\chi(1) = 1$ and $\chi(ab) = \chi(a)\chi(b)$ for all $a, b \in K^*$. We sometimes call such functions *characters* on K^* with values in L. Automorphisms of a field L (so we let $K = L$) are examples of such multiplicative functions and this is the way they will arise in what follows.
The following Theorem states that distinct characters on K^* are L-linear independent in the space of functions on K^*.

Theorem 8.1.1 (Dedekind) *Let $\chi_1, \ldots, \chi_n$ be distinct multplicative functions from a field K to a field L. Suppose that there exist $a_1, \ldots, a_n \in L$ such that*

$$a_1\chi_1(x) + a_2\chi_2(x) + \cdots + a_n\chi_n(x) = 0$$

for all $x \in K$. Then $a_1 = a_2 = \cdots = a_n = 0$.

Proof. We proceed by induction on n. When $n = 1$ we see that $a_1\chi_1(x) = 0$ for all $x \in K$, in particular for $x = 1$. Hence $a_1 = 0$.
Let $n > 1$ and suppose our theorem is proved for every $n-1$-tuple of multiplicative functions. Choose an index i with $1 \leq i < n$. Since χ_i and χ_n are distinct functions, there exists $\xi \in K$ such that $\chi_i(\xi) \neq \chi_n(\xi)$. From $a_1\chi_1(x) + \cdots + a_n\chi_n(x) = 0$ for all $x \in K$ it follows that $a_1\chi_1(\xi x) + \cdots + a_n\chi_n(\xi x) = 0$ for all $x \in K$. Now use the multiplicative property of the χ_j to get $a_1\chi_1(\xi)\chi_1(x) + \cdots + a_n\chi_n(\xi)\chi_n(x) = 0$ for all $x \in K$. Subtract from this $\chi_n(\xi)$ times the original relation. We get

$$a_1(\chi_1(\xi) - \chi_n(\xi))\chi_1(x) + \cdots + a_{n-1}(\chi_{n-1}(\xi) - \chi_n(\xi))\chi_{n-1}(x) = 0$$

for all $x \in K$. According to our induction hypothesis all coefficients are zero, in particular $a_i(\chi_i(\xi) - \chi_n(\xi)) = 0$. Since $\chi_i(\xi) \neq \chi_n(\xi)$ this implies $a_i = 0$. This argument holds for all i with $i < n$ and we are left with $a_n\chi_n(x) = 0$ for all $x \in K$ which in its turn implies that $a_n = 0$.

The reason we have proved Dedekind's theorem is the following Corollary, which is the only thing we will need from Dedekind's theorem.

Corollary 8.1.2 *Let L be a field and $\sigma_1, \ldots, \sigma_n$ distinct automorphisms of L. Then there exists $\xi \in L$ such that $\sigma_1(\xi) + \cdots + \sigma_n(\xi) \neq 0$.*

Proof. Suppose on the contrary that $\sigma_1(x) + \cdots + \sigma_n(x) = 0$ for all $x \in L$. Then we have a contradiction with Dedekind's Theorem.

Notice that if L has characteristic zero, the proof of Corollary 8.1.2 is trivial, without need for Dedekind's Theorem. One simply takes $\xi = 1$ and notes that $\sigma_1(1) + \cdots + \sigma_n(1) = n \neq 0$. When L has a characteristic dividing n however, we get $\sigma_1(1) + \cdots + \sigma_n(1) = n = 0$. So we have to look for another element ξ and we need to take recourse to Dedekind's Theorem for that.
Corollary 8.1.2 plays an important role in the proof of the following crucial Theorem on fixed fields. Let L be a field and H a subgroup of the automorphism group of L, then we denote the *fixed field* under H by

$$L^H = \{x \in L |\ \sigma(x) = x \text{ for all } \sigma \in H\}.$$

Theorem 8.1.3 (E.Artin) *Let L be a field and H a finite subgroup of the automorphism group of L. Let L^H be its fixed field. Then L/L^H is a finite Galois extension with Galois group H. In particular $|H| = [L : L^H]$.*

Proof. Let $H = \{\sigma_1, \ldots, \sigma_h\}$. For any $x \in L$ we define $tr(x) = \sigma_1(x) + \cdots + \sigma_h(x)$. Note that $tr(x)$ is fixed under the action of each $\sigma_j \in H$ and therefore $tr(x) \in L^H$ for every $x \in L$.
Now suppose that L contains $h+1$ elements $\alpha_1, \ldots, \alpha_{h+1}$ which are L^H-linear independent. We derive a contradiction as follows. Consider the homogeneous system of h equations

$$\begin{aligned} x_1\sigma_1(\alpha_1) + \cdots + x_{h+1}\sigma_1(\alpha_{h+1}) &= 0 \\ &\vdots \\ x_1\sigma_h(\alpha_1) + \cdots + x_{h+1}\sigma_h(\alpha_{h+1}) &= 0 \end{aligned}$$

in the $h+1$ unknowns $x_i \in L$. According to linear algebra there must be a non-trivial solution. Choose such a solution. Without loss of generality we can assume that $x_1 \neq 0$ and after multiplication by a suitable factor if necessary we may assume that $\sigma_1(x_1) + \cdots + \sigma_h(x_1) \neq 0$. The possibility of this follows from Corollary 8.1.2. To the i-th equation above we apply σ_i^{-1} for $i = 1, 2, \ldots, n$. After renumbering we obtain the system of equalities

$$\begin{aligned} \sigma_1(x_1)\alpha_1 + \cdots + \sigma_1(x_{h+1})\alpha_{h+1} &= 0 \\ &\vdots \\ \sigma_h(x_1)\alpha_1 + \cdots + \sigma_h(x_{h+1})\alpha_{h+1} &= 0 \end{aligned}$$

Addition of these equalities yields

$$tr(x_1)\alpha_1 + \cdots + tr(x_{h+1})\alpha_{h+1} = 0.$$

We know that $tr(x_i) \in L^H$ for every i and $\alpha_1, \ldots, \alpha_{h+1}$ are L^H-linearly independent. Hence $tr(x_i) = 0$ for all i. But this contradicts our carefully doctored provision $tr(x_1) \neq 0$.
Hence $[L : L^H] \leq h = |H|$. On the other hand $|H| \leq [L : L^H]$ because $H \subset \mathrm{Gal}(L/L^H)$. Thus we conclude that $|H| = [L : L^H]$. In other words, L/L^H is a finite Galois extension with Galois group H.

8.2 Main Theorem

Let L/K be a Galois extension. The main theorem of Galois theory gives us a bijection between the subgroups of $\mathrm{Gal}(L/K)$ and the intermediate fields M such that $K \subset M \subset L$.
Note that for such an intermediate field M the extension L/M is again a Galois extension. This is clear, by Theorem 7.3.5 L is the splitting field of a separable polynomial f over K. But f can also be considered as polynomial in $M[X]$, so L is also a splitting field of f over M. The group $\mathrm{Gal}(L/M)$ is a subgroup of $\mathrm{Gal}(L/K)$. By Theorem 7.3.5 we have $|\mathrm{Gal}(L/M)| = [L : M]$.
Note that in general M is *not* a Galois extension of K. For example, the splitting field of $X^3 - 2$ over $\mathbb{Q}$ is given by $\mathbb{Q}(\sqrt[3]{2}, \omega)$ with $\omega = e^{2\pi i/3}$. But the subfield $\mathbb{Q}(\sqrt[3]{2})$ is not Galois over $\mathbb{Q}$ since it contains only one zero of $X^3 - 2$.

Theorem 8.2.1 *Let L/K be a Galois extension. Then the map from intermediate fields M of L/K and subgroups of $\mathrm{Gal}(L/K)$ given by $M \mapsto \mathrm{Gal}(L/M)$ is a bijection.*
The inverse map is given by $H \mapsto L^H$.

Proof. We show that $\phi : M \mapsto \mathrm{Gal}(L/M)$ is surjective and injective. Suppose H is a subgroup of $\mathrm{Gal}(L/K)$. From Artin's Theorem 8.1.3 we know that $H = \mathrm{Gal}(L/L^H)$. This shows surjectivity of ϕ.

Let now M, M' be two intermediate fields such that $\mathrm{Gal}(L/M) = \mathrm{Gal}(L/M')$. Denote the smallest subfield of L containing both M and M' by $M \cdot M'$. Since $\mathrm{Gal}(L/M) = \mathrm{Gal}(L/M')$, these groups also fix the elements of $M \cdot M'$. Hence $\mathrm{Gal}(L/M) = \mathrm{Gal}(L/M') = \mathrm{Gal}(L/(M \cdot M'))$, which implies $[L : M \cdot M'] = [L : M] = [L : M']$. Consequently M, M' and $M \cdot M'$ have the same degree over K, which implies that $M = M'$. Hence ϕ is injective.

We call the bijection in Theorem 8.2.1 the *Galois correspondence*. It turns out that under the Galois correspondence normal extensions of K correspond to normal subgroups of L. We can state this slightly more general as follows.

Theorem 8.2.2 *Let L/K be a finite Galois extension. Then an intermediate extension M with $K \subset M \subset L$ is normal over K if and only if $\mathrm{Gal}(L/M)$ is a normal subgroup of $\mathrm{Gal}(L/K)$. Moreover, we have the isomorphism*

$$\mathrm{Gal}(M/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M).$$

Proof. We first remark that an intermediate field M is normal over K if and only if $\sigma(M) = M$ for every $\sigma \in \mathrm{Gal}(L/K)$. Suppose that the intermediate field M is normal over K and let $\alpha \in M$. Let g be the minimal polynomial of α over K. Then $\sigma(\alpha)$ is also a zero of g. By the normality of M this zero is also contained in M. Hence σ maps elements of M to itself. Conversely suppose that $\sigma(M) = M$ for every $\sigma \in \mathrm{Gal}(L/K)$. Then, if an irreducible polynomial g has a zero $\alpha \in M$, all of its zeros are images of α under $\mathrm{Gal}(L/K)$ and hence all zeros are contained in M.
Now suppose that M is normal over K. We have just seen that this implies that $\sigma(M) = M$ for every $\sigma \in \mathrm{Gal}(L/K)$. So we can consider the restriction of σ to M, denoted by $\sigma|_M$, for every $\sigma \in \mathrm{Gal}(L/K)$. Clearly the map $\pi : \mathrm{Gal}(L/K) \to \mathrm{Gal}(M/K)$ given by $\sigma \mapsto \sigma|_M$ is a group homomorphism. It is surjective since any element of $\mathrm{Gal}(M/K)$ can be extended to an element of $\mathrm{Gal}(L/K)$ by Proposition **??**. Its kernel is $\mathrm{Gal}(L/M)$ and so this is a normal subgroup, as asserted. Moreover, by the isomorphsim theorem for groups we get

$$\mathrm{Gal}(M/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M).$$

Suppose conversely that H is a normal subgroup of $\mathrm{Gal}(L/K)$. Let $\alpha \in L^H$ and $\sigma \in \mathrm{Gal}(L/K)$. Then, for any $h \in H$ there is $h' \in H$ such that $h\sigma = \sigma h'$. Hence $h(\sigma(\alpha)) = \sigma(h'(\alpha) = \sigma(\alpha)$. So $\sigma(\alpha)$ is fixed under all $h \in H$ and hence $\sigma(L^H) = L^H$. This means that L^H is a normal extension of K.

8.3 Examples of Galois correspondences

Example 8.3.1 Let $L/\mathbb{Q}$ be the splitting field of $X^3 - 2$ over $\mathbb{Q}$. We are asked to determine $\mathrm{Gal}(L/\mathbb{Q})$. The first step is to determine the degree $[L : \mathbb{Q}]$. We have seen at earlier occasions that $L = \mathbb{Q}(\sqrt[3]{2}, \omega)$ where $\omega = e^{2\pi i/3}$ is a cube root of unity. The degrees over $\mathbb{Q}$ of $\sqrt[3]{2}$ and ω are 3 and 2 respectively. Hence $[L : \mathbb{Q}] = 2 \cdot 3 = 6$. By Theorem 7.3.5 we now know that $|\mathrm{Gal}(L/\mathbb{Q})| = 6$. An element of the Galois group maps $\sqrt[3]{2}$ to a zero of $X^3 - 2$, so $\sqrt[3]{2}, \omega\sqrt[3]{2}$ or $\omega^2\sqrt[3]{2}$. The element ω is mapped to ω or ω^2. In principle there are 6 possibilities. Since we know that the Galois group has precisely 6 elements, every possibility should occur. Let us consider two special elements $\sigma, \tau \in \mathrm{Gal}(L/\mathbb{Q})$ defined by

$$\sigma(\sqrt[3]{2}) = \omega\sqrt[3]{2}, \quad \sigma(\omega) = \omega, \quad \tau(\sqrt[3]{2}) = \sqrt[3]{2}, \quad \tau(\omega) = \omega^2.$$

Notice that

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

Similarly,

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

From these equalities we conclude that $\sigma \circ \tau = \tau \circ \sigma^2$. Similarly we can check that $\sigma^3 = \mathrm{id}$ and $\tau^2 = \mathrm{id}$ (please verify). These relations are precisely the defining relations for the symmetric group S_3. Hence $\mathrm{Gal}(L/\mathbb{Q}) \cong S_3$. The element σ plays the role of a cyclic permutation of order 3. In fact it permutes the zeros of $X^3 - 2$ in a cyclic way (check!). The element τ fixes $\sqrt[3]{2}$ and it interchanges the other two zeros of $X^3 - 2$. It coincides with complex conjugation on L if L is considered subfield of $\mathbb{C}$.
The group S_3 has 6 subgroups which we tabulate together with their invariant fields:

Group H	Invariant field L^H
$\{\mathrm{id}\}$	L
S_3	$\mathbb{Q}$
$A_3 = \{\mathrm{id}, \sigma, \sigma^2\}$	$\mathbb{Q}(\omega) = \mathbb{Q}(\sqrt{-3})$
$\{\mathrm{id}, \tau\}$	$\mathbb{Q}(\sqrt[3]{2})$
$\{\mathrm{id}, \sigma\tau\}$	$\mathbb{Q}(\omega^2\sqrt[3]{2})$
$\{\mathrm{id}, \sigma^2\tau\}$	$\mathbb{Q}(\omega\sqrt[3]{2})$

The subgroup A_3 is a normal subgroup of S_3 and its fixed field $\mathbb{Q}(\sqrt{-3})$ is normal over $\mathbb{Q}$.

Example 8.3.2 We compute the Galois group of the splitting field L of $X^4 - 4X^2 + 1$ over $\mathbb{Q}$ and determine the subgroups and the Galois correspondence.
First we need to find the degree of L. Notice that $X^4 - 4X^2 + 1 = (X^2 - 2)^2 - 3$. Hence the four zeros are given by $\pm\sqrt{2 \pm \sqrt{3}}$. The field L contains $\sqrt{2 + \sqrt{3}}$. Write $\alpha = \sqrt{2 + \sqrt{3}}$. From the very special form of the equation we easily see that $-\alpha, 1/\alpha, -1/\alpha$ are also zeros. Hence we conclude that $L = \mathbb{Q}(\sqrt{2 + \sqrt{3}}) = \mathbb{Q}(\alpha)$. So L is a simple extension and we can apply Proposition 7.2.8. Since $[L : \mathbb{Q}] = 4$ the Galois group has four elements. So $\mathrm{Gal}(L/\mathbb{Q})$ is either cyclic or it is Klein's fourgroup. Let us define the element σ by $\sigma(\alpha) = -\alpha$ and the element τ by $\tau(\alpha) = 1/\alpha$. Then note that $\sigma\tau(\alpha) = -1/\alpha$. In addition $\sigma\tau = \tau\sigma$ and $\sigma^2 = \tau^2 = \mathrm{id}$. So $\mathrm{Gal}(L/\mathbb{Q})$ is Klein's fourgroup, denoted by V_4.
Let us determine the fixed field under the subgroups of order 2. For example, the element $\alpha + 1/\alpha$ is fixed under τ. Notice that

$$(\alpha + 1/\alpha)^2 = \alpha^2 + 2 + 1/\alpha^2 = 2 + \sqrt{3} + 2 + 2 - \sqrt{3} = 6.$$

So, perhaps surprisingly, we discovered that $\sqrt{6} \in \mathbb{Q}(\alpha)$. Similarly $\alpha - 1/\alpha$ is fixed under $\sigma\tau$. Notice that

$$(\alpha - 1/\alpha)^2 = \alpha^2 - 2 + 1/\alpha^2 = 2\sqrt{3} - 2 + 2 - \sqrt{3} = 2.$$

Hence $\sqrt{2} \in \mathbb{Q}(\alpha)$. We now tabulate the subgroups of $\mathrm{Gal}(L/\mathbb{Q})$ and their fixed fields

Group H	Invariant field L^H
{id}	L
V_4	$\mathbb{Q}$
$\{\mathrm{id}, \sigma\}$	$\mathbb{Q}(\sqrt{3})$
$\{\mathrm{id}, \tau\}$	$\mathbb{Q}(\sqrt{6})$
$\{\mathrm{id}, \sigma\tau\}$	$\mathbb{Q}(\sqrt{2})$

Note that all subgroups and all fixed fields are normal.

Example 8.3.3 We compute the Galois group of the splitting field L of $X^4 - 2X^2 - 2$ over $\mathbb{Q}$ and determine the subgroups and the Galois correspondence.
The polynomial $X^4 - 2X^2 - 2$ is an Eisenstein polynomial with respect to $p = 2$, hence irreducible in $\mathbb{Q}[X]$. The zeros are given by $\pm\sqrt{1 \pm \sqrt{3}}$. The element $\sqrt{1 + \sqrt{3}}$ has degree 4 over $\mathbb{Q}$ but this time $\mathbb{Q}(\sqrt{1 + \sqrt{3}})$ is not a splitting field. For example the element $\sqrt{1 + \sqrt{3}}\sqrt{1 - \sqrt{3}} = \sqrt{1^2 - 3} = \sqrt{-2}$

should be in L. Clearly $\sqrt{-2} \notin \mathbb{Q}(\sqrt{1+\sqrt{3}})$ since the latter field is a subfield of $\mathbb{R}$ and $\sqrt{-2}$ is not a real number.
Write $\alpha = \sqrt{1+\sqrt{3}}$. The field $\mathbb{Q}(\sqrt{-2}, \alpha)$ has degree 8 over $\mathbb{Q}$. The zeros of $X^4 - 2X^2 - 2$ are $\alpha, -\alpha, \sqrt{-2}/\alpha, -\sqrt{-2}/\alpha$. So $L = \mathbb{Q}(\sqrt{-2}, \alpha)$ and $\mathrm{Gal}(L/\mathbb{Q})$ has order 8. Any element of the Galois group maps α to one of the four zeros of $X^4 - 2X^2 - 2$ and $\sqrt{-2}$ to $\pm\sqrt{-2}$. These are 8 possibilities and each actually occurs. Define the elements σ, τ of the Galois group by

$$\sigma(\alpha) = \sqrt{-2}/\sigma, \quad \sigma(\sqrt{-2}) = -\sqrt{-2}$$

and

$$\tau(\alpha) = \alpha, \quad \tau(\sqrt{-2}) = -\sqrt{-2}.$$

We can check that

$$\sigma(\alpha) = \sqrt{-2}/\alpha, \quad \sigma^2(\alpha) = -\alpha, \quad \sigma^3(\alpha) = -\sqrt{-2}/\alpha, \quad \sigma^4(\alpha) = \alpha.$$

Hence σ has order 4. It is easily seen that $\tau^2 = \mathrm{id}$. Moreover, we verify that $\sigma\tau = \tau\sigma^3 = \tau\sigma^{-1}$. The group generated by σ, τ, together with the given relations is precisely the symmetry group of the square, which is a group of order 8. We denote it by D_4 (dihedral group of order 8). The element σ permutes the zeros of $X^4 - 2X^2 - 2$ cyclically and τ interchanges the zeros $\sqrt{-2}/\alpha$ and $-\sqrt{-2}/\alpha$ and leaves the other two fixed.
To determine the Galois correspondence we first observe that L contains three quadratic fields, namely $\mathbb{Q}(\sqrt{3})$ (since $\alpha^2 = 1+\sqrt{3}$), $\mathbb{Q}(\sqrt{-2})$ and $\mathbb{Q}(\sqrt{-6})$. We now tabulate the subgroups of the Galois group together with the fixed fields.

Group H	Invariant field L^H
$\{\mathrm{id}\}$	L
D_4	$\mathbb{Q}$
$C_4 = \{\mathrm{id}, \sigma, \sigma^2, \sigma^3\}$	$\mathbb{Q}(\sqrt{-6})$
$\{\mathrm{id}, \tau, \sigma^2, \tau\sigma^2\}$	$\mathbb{Q}(\sqrt{3})$
$\{\mathrm{id}, \tau\sigma, \sigma^2, \tau\sigma^3\}$	$\mathbb{Q}(\sqrt{-2})$
$\{\mathrm{id}, \sigma^2\}$	$\mathbb{Q}(\sqrt{-2}, \sqrt{3})$
$\{\mathrm{id}, \tau\}$	$\mathbb{Q}(\alpha)$
$\{\mathrm{id}, \tau\sigma\}$	$\mathbb{Q}(\alpha - \sqrt{-2}/\alpha)$
$\{\mathrm{id}, \tau\sigma^2\}$	$\mathbb{Q}(\sqrt{-2}/\alpha)$
$\{\mathrm{id}, \tau\sigma^3\}$	$\mathbb{Q}(\alpha + \sqrt{-2}/\alpha)$

To check the fixed fields notice that $\sigma(\alpha^2) = -2/\alpha^2$. Hence $\sigma(1+\sqrt{3}) = -2/(1+\sqrt{3}) = 1-\sqrt{3}$. And so $\sigma(\sqrt{3}) = -\sqrt{3}$. By definition $\sigma(\sqrt{-2}) = -\sqrt{-2}$. Also by definition $\tau(\sqrt{-2}) = -\sqrt{-2}$ but $\tau(\sqrt{3}) = \sqrt{3}$. From this we conclude that $\sqrt{3}$ is fixed by σ^2 and τ, $\sqrt{-2}$ is fixed by $\tau\sigma$ and σ^2 and $\sqrt{-6}$ is fixed by σ. This explains the Galois correspondence for the subgroups of order four. In the case of subgroups of order two, we have indicated fourth degree extensions of $\mathbb{Q}$ whose generating elements are fixed under the corresponding subgroup, which is straightforward to verify.

Example 8.3.4 Let $p \in \mathbb{Z}_{>0}$ be a prime and L the splitting field of $X^p - 1$ over $\mathbb{Q}$. Let $\zeta = e^{2\pi i/p}$. Then the zeros of $X^p - 1$ are given by ζ^k for $k = 0, 1, \ldots, p-1$. So $\mathbb{Q}(\zeta)$ is the splitting field of $X^p - 1$. We have seen earlier that ζ is a zero of the irreducible polynomial $\phi_p(X) = X^{p-1} + \cdots + X^2 + X + 1$. Hence ζ has degree $p-1$ over $\mathbb{Q}$. The other zeros of $\phi_p(X)$ are ζ^k with $k = 1, 2, \ldots, p-1$. The Galois group is given by $\zeta \mapsto \zeta^k$ for any $k \in (\mathbb{Z}/p\mathbb{Z})^*$. Denote the latter element by σ_k. Then it is easily verified that $\sigma_{kl} = \sigma_k\sigma_l = \sigma_l\sigma_k$. Hence $\mathrm{Gal}(L/\mathbb{Q})$ is an abelian group of order $p-1$ which is isomorphic to $(\mathbb{Z}/p\mathbb{Z})^*$. A Theorem of Gauss states that such groups are cyclic, but we will not prove it here.

Example 8.3.5 We specialise the previous example to the case $p = 17$. So let $\zeta = e^{2\pi i/17}$. Consider the element $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ given by $\sigma(\zeta) = \zeta^3$. Notice that $\sigma^k(\zeta) = \zeta^{3^k}$. A simple computation shows that modulo 17 we have

$$3 \equiv 3,\ 3^2 \equiv 9,\ 3^3 \equiv 10,\ 3^4 \equiv 13,\ 3^5 \equiv 5,\ 3^6 \equiv 15,\ 3^7 \equiv 11,\ 3^8 \equiv 16$$

$$3^9 \equiv 14,\ 3^{10} \equiv 8,\ 3^{11} \equiv 7,\ 3^{12} \equiv 4,\ 3^{13} \equiv 12,\ 3^{14} \equiv 2,\ 3^{15} \equiv 6,\ 3^{16} \equiv 1.$$

Thus every element of $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ can be written in the form σ^k, so we have a cyclic group of order 16. For every divisor d of the order of a cyclic group there is exactly one subgroup of that order. So in our case we have subgroups of orders $16, 8, 4, 2, 1$ and they are generated by $\sigma, \sigma^2, \sigma^4, \sigma^8, \sigma^{16} = \mathrm{id}$. Via the Galois-correspondence there exist fields $K_1 = \mathbb{Q}, K_2, K_4, K_8, K_{16} = \mathbb{Q}(\zeta)$ such that $K_i \subset K_{2i}$ and $[K_{2i} : K_i] = 2$ for $i = 1, 2, 4, 8$. Hence the number ζ is contructible by Theorem **??** and so the regular 17-gon is construcible. This was the striking discovery made by Gauss and the first significant progress in classic ruler and straight-edge constructions in about 2000 years!

Example 8.3.6 Here we make some comments field extension by a general root of unity.
Let K be a field and $n \in \mathbb{Z}/n\mathbb{Z}$. Let $L = K(\alpha)$ where α is a zero of $X^n - 1$. Then L/K is a Galois extension with an abelian Galois group.
This can be seen as follows. Without loss of generality we can assume that n is the smallest number such that $\alpha^n = 1$. Then the zeros of $X^n - 1$ are given by α^k with $k = 0, 1, 2, \ldots, n-1$. So L is the splitting field of $X^n - 1$ over K. Moreover, the powers α^k are all distinct. If $\alpha^k = \alpha^l$ would hold for some $0 \leq l < k < n$ then, after divison by α^l we would get $\alpha^{k-l} = 1$. This contradicicts the minimality of n. Therefore $X^n - 1$ is a separable polynomial and L/K is Galois.
Any element $\sigma \in \mathrm{Gal}(L/K)$ maps α to α^k for some $k \in \mathbb{Z}$. Since the group order of α in L^* is n, the same is true for the group order of $\sigma(\alpha) = \alpha^k$. Hence $\gcd(k, n) = 1$. Let associate to σ the element $k \in (\mathbb{Z}/n\mathbb{Z})^*$. Then this gives an injective homomorphsim of $\mathrm{Gal}(L/K)$ into $(\mathbb{Z}/n\mathbb{Z})^*$. Hence $\mathrm{Gal}(L/K)$ is an abelian group.

8.4 Extending Galois extensions

In many situations the following Theorem is very useful.

Theorem 8.4.1 *Let L/K be a Galois extension and α an element algebraic over L. Then $L(\alpha)/K(\alpha)$ is again a Galois extension and $\mathrm{Gal}(L(\alpha)/K(\alpha))$ is isomorphic to a subgroup of $\mathrm{Gal}(L/K)$.*

Proof. Since L/K is a Galois extension it is a splitting field of a separabel polynomial $f \in K[X]$. Clearly $L(\alpha)$ is a splitting field of f over $K(\alpha)$. Hence $L(\alpha)/K(\alpha)$ is a Galois extension.
Let $\sigma \in \mathrm{Gal}(L(\zeta)/K(\zeta))$. Then, $\sigma(\beta)$ is a zero of f whenever β is a zero of f. This is because all zeros of f are contained in L and σ is also a K-automorphism. Hence $\sigma(L) = L$. Moreover, any element of $L \cap K(\alpha)$ is fixed by σ. Hence σ is a $L \cap K(\alpha)$-automorphism of L. Suppose σ restricted to L is the identity map. Then, since $\sigma(\alpha) = \alpha$, σ is the identity element in $\mathrm{Gal}(L(\alpha)/K(\alpha))$.
So we get an injective homomorphism of $\mathrm{Gal}(L(\alpha)/K(\alpha)) \to \mathrm{Gal}(L/L \cap K(\alpha)$ by the restriction map $\sigma \mapsto \sigma|_L$. The latter group is a subgroup of $\mathrm{Gal}(L/K)$.

8.5 Simple extensions

In Proposition 7.2.8 we showed how to compute $\mathrm{Gal}(L/K)$ for simple extensions L/K. We noted that this might be an approach to computing the Galois group for every extension, simply by writing the extension as a simple extension. This was the approach which Galois originally took. Although we did not adopt this approach, we complete these remarks here by showing that finite separable extensions are indeed simple.

Theorem 8.5.1 *Let L/K be a finite separable extension. Then*

1. *there are finitely many fields M such that $K \subset M \subset L$.*
2. *there exists $\alpha \in L$ such that $L = K(\alpha)$ (in other words, L is a simple extension of K).*

Proof. Suppose $L = K(\alpha_1, \ldots, \alpha_r)$. Let $g_i \in K[X]$ be the minimal polynomial of α_i for $i = 1, \ldots, r$. Let $f(X)$ be the product of the distinct elements in the set $\{g_1, \ldots, g_r\}$. Let N be the splitting field of f over K. Then N/K is a Galois extension. The number of subgroups of $\mathrm{Gal}(N/K)$ is finite and so, by Galois correspondence, there are at most finitely many intermediate fields M with $K \subset M \subset N$. Hence the first part of our Theorem follows.
The proof of the second part only applies when $|K| = \infty$. When K is finite it follows from the theory of finite fields. The proof is by induction on r where $L = K(\alpha_1, \ldots, \alpha_r)$. When $r = 1$ the statement is trivial. Let $r > 1$ and suppose that every finite separable extension generated by $r - 1$ elements is simple. By the induction hypothesis there exists $\beta \in L$ be such that $K(\alpha_1, \ldots, \alpha_{r-1}) = K(\beta)$. We now prove that $L = K(\beta, \alpha_r)$ is simple. Put $\alpha = \alpha_r$. Consider the fields $K(\alpha + c\beta)$ where c runs over K. Since K is infinite and there are at most finitely many subfields of L containing K there exist distinct c, c' such that $K(\alpha + c\beta) = K(\alpha + c'\beta)$. Clearly $\alpha + c\beta \in K(\alpha, \beta)$. On the other hand both $\alpha + c\beta - \alpha - c'\beta = (c - c')\beta \in K(\alpha + c\beta)$ and $c'(\alpha + c\beta) - c'(\alpha + c\beta) = (c' - c)\alpha \in K(\alpha + c\beta)$. Since $c - c' \neq 0$ this implies that $\alpha, \beta \in K(\alpha + c\beta)$. Hence $L = K(\alpha, \beta) = K(\alpha + c\beta)$, so L is a simple extension of K.

Remark 8.5.2 Theorem 8.5.1 need not be true for inseparable extensions. Consider for example the extension $L = \mathbb{F}_p(s^{1/p}, t^{1/p})$ of $K = \mathbb{F}_p(s, t)$ which has degree p^2. Every element of the extension L has degree p. So L cannot be a simple extension. Furthermore the elements $as^{1/p} + bt^{1/p}$ with $a, b \in K$ generate an infinite number of distinct extensions. So the number of intermediate fields of L/K is infinite.

Here we present a second proof of Theorem 8.5.1(2) which does not use the Galois correspondence. Again we assume that K is infinite. As we have seen in the proof of Theorem 8.5.1(2) it suffices to show that any separable extension of the form $K(\alpha, \beta)$ over K is simple. Let $f, g \in K[X]$ be the minimal polynomials of α respectively β over K. We work in a splitting field L of $f(X)g(X)$. Let $\alpha_1, \ldots, \alpha_n$ be the zeros of f and $\beta_1, \ldots, \alpha_m$ the zeros of g. Since the extension is separable, the β_i are distinct. Take $\alpha = \alpha_1, \beta = \beta_1$. Since K is infinite there exists $c \in K$ such that c is different from $(\alpha - \alpha_i)/(\beta_k - \beta)$ for all $1 \leq i \leq n, 1 < k \leq m$. Hence $\alpha + c\beta \neq \alpha_i + c\beta_k$ for all $1 \leq i \leq n, 1 < k \leq m$. Let $\delta = \alpha + c\beta$. We assert that $K(\delta) = K(\alpha, \beta)$. To that end we note that $f(\delta - cx)$ and $g(x)$ have the common zero β. By construction it is also the only zero. So the gcd of $f(\delta - cx)$ and $g(x)$ is $x - \beta$. Both polynomials are in $K(\delta)[x]$, hence $\beta \in K(\delta)$. Then also $\alpha = \delta - c\beta \in K(\delta)$. Hence $K(\alpha, \beta) \subset K(\delta)$. Since we already know that $\delta \in K(\alpha, \beta)$ the desired equality $K(\alpha, \beta) = K(\delta)$ follows.

9 Solving equations

9.1 Symmetric polynomials

Let K be a field and consider the polynomial ring $K[x_1, \ldots, x_n]$ in n x_i. A polynomial $g(x_1, \ldots, x_n)$ is called *symmetric* if $g(x_{\sigma(1)}, \ldots, x_{\sigma(n)}) = g(x_1, \ldots, x_n)$ for every permutation σ of $\{1, 2, \ldots, n\}$. Simple examples are $x_1 + x_2 + \cdots + x_n$ or $\sum_{i \neq j} x_i x_j$ or $x_1 x_2 \cdots x_n$. Let us write

$$(T - x_1)(T - x_2) \cdots (T - x_n) = T^n - s_1 T^{n-1} + s_2 T^{n-2} - \cdots + (-1)^n s_n.$$

Here the coefficients s_i are symmetric polynomials in $x_1, \ldots, x_n$. In particular $s_1 = x_1 + \cdots + x_n$, $s_2 = \sum_{i<j} x_i x_j$ and $s_n = x_1 x_2 \cdots x_n$. The coefficients s_i are called the *elementary symmetric functions*. We have the following Theorem.

Theorem 9.1.1 *Let K be a field. Then any symmetric polynomial in $K[x_1, \ldots, x_n]$ can be written as a polynomial in the elementary symmetric functions $s_1, s_2, \ldots, s_n$.*

For example, $x_1^2 + x_2^2 + \cdots + x_n^2$ is a symmetric polynomial. It can be written as $s_1^2 - 2s_2$ (please verify). Another example, $x_1^3 + x_2^3 + \cdots + x_n^3 = s_1^3 - 3s_2 s_1 + 3s_3$.
We use this theorem to derive a solution of the third and fourth degree equation.

9.2 Solution of the cubic equation

Consider the polynomial $X^3 - aX^2 + bX - c$ and let x_1, x_2, x_3 be its zeros. We assume that a, b, c lie in a field which contains the cube root of unity ω. Consider the expression $u_1 = x_1 + \omega x_2 + \omega^2 x_3$. Apply the cyclic substition $x_1 \to x_2 \to x_3 \to x_1$ represented by the cycle (123). Then u_1 changes into $\omega^2 u_1$. So u_1^3 is fixed under the cyclic substitution. Let similarly $u_2 = x_1 + \omega^2 x_2 + \omega x_3$ Then after the cyclic substitution u_2 is replaced by ωu_2. Under the substitution $x_2 \to x_3 \to x_2$ (represented by (23) the form u_1 changes into u_2 and vice versa. Hence $u_1 u_2$ and $u_1^3 + u_2^3$ are fixed under the group of permutations generated by (123) and (23), which is the full permutation group S_3. Hence they are symmetric polynomials in x_1, x_2, x_3. By Theorem 9.1.1 these polynomials can be expressed in the symmetric expressions a, b, c in the x_i. Straightforward calculation gives us

$$\begin{aligned} u_1^3 + u_2^3 &= 2(x_1^3 + x_2^3 + x_3^3) - 3(x_1^2 x_2 + x_1 x_2^2 + x_1^2 x_3 + x_1 x_3^2 + x_2^2 x_3 + x_2 x_3^2) \\ &= 2a^3 - 9ab + 27c \end{aligned}$$

and

$$u_1 u_2 = x_1^2 + x_2^2 + x_3^2 - x_1 x_2 - x_1 x_3 - x_2 x_3 = a^2 - 3b.$$

Without loss of generality we can assume that $a = 0$. So we see that u_1^3 and u_2^3 are solutions of the equation

$$(U - u_1^3)(U - u_2^3) = U^2 - 27cU + (-3b)^3 = 0.$$

Solution gives us

$$u_1^3 = (27c + \sqrt{27^2 c^2 + 4 \cdot 27 b^3})/2 = 27(c/2) + 27\sqrt{(c/2)^2 + (b/3)^3}.$$

Hence

$$u_1 = 3\sqrt[3]{\Big(c/2 - \sqrt{(c/2)^2 + (b/3)^3}\Big)}, \quad u_2 = -3b/u_1.$$

Now note that

$$3x_1 = (x_1 + x_2 + x_3) + u_1 + u_2 = a + u_1 + u_2 = u_1 + u_2$$

where u_1, u_2 are given above. These formulas are known as *Cardano's formulas* for the solution of the cubic equation.
The linear forms u_1, u_2 which made the solution possible are examples of *Lagrange resolvents*. We will see more of them later.

9.3 Solution of the quartic equation

Suppose we are given the equation

$$X^4 - aX^3 + bX^2 - cX + d = 0.$$

Let x_1, x_2, x_3, x_4 be the solutions. Consider the elements

$$\begin{aligned} y_1 &= (x_1 + x_2 - x_3 - x_4)^2 \\ y_2 &= (x_1 - x_2 - x_3 + x_4)^2 \\ y_3 &= (x_1 - x_2 + x_3 - x_4)^2 \end{aligned}$$

Observe that after any permutation of x_1, x_2, x_3, x_4 the expressions y_1, y_2, y_3 are also permuted. Hence the elementary symmetric functions in y_1, y_2, y_3 are symmetric in x_1, x_2, x_3, x_4. Straightforward calculation gives us

$$\begin{aligned} y_1 + y_2 + y_3 &= 3a^2 - 8b \\ y_1y_2 + y_1y_3 + y_2y_3 &= 3a^4 - 16a^2b + 16b^2 + 16ac - 64d \\ y_1y_2y_3 &= a^6 - 8a^4b + 16a^3c + 16a^2b^2 - 64abc + 64c^2 \end{aligned}$$

Let us assume for simplicity (and without loss of generality) that $a = 0$. Then y_1, y_2, y_3 are solutions of the equation

$$(Y - y_1)(Y - y_2)(Y - y_3) = Y^3 + 8bY^2 + (16b^2 - 64d)Y - 64c^2 = 0.$$

We know how to solve this equation by Cardano's formula. Having found y_1, y_2, y_3 we observe that

$$4x_1 = a + \sqrt{y_1} + \sqrt{y_2} + \sqrt{y_3}$$

and similarly for x_2, x_3, x_4. Thus we have recovered Ferrari's formula for the solution of the quartic equation.
The functions y_1, y_2, y_3 are fixed under the substitutions $(1), (12)(34), (13)(24), (14)(23)$ that is, Klein's fourgroup V_4.Note that V_4 is a normal subgroup of S_4 and that $S_3 \cong S_4/V_4$, which is the group by which the y_1, y_2, y_3 are permuted. In its turn S_3 has the alternating subgroup A_3 as normal subgroup and $S_3/A_3 \cong S_2$. The solution of the cubic equation is based on the construction of an invariant under A_3. In this way we see how group theoretic considerations arise in the ideas to solve polynomial equations. The step to Galois theory is a natural continuation.

9.4 Radical extensions

Of course similar considerations have been attempted to solve the equation of degree 5 (quintic equation). The goal of these attempts was to describe the zeros of a quintic polynomial as a result of repeated application of addition/subtraction, multiplication/division and taking n-th roots, starting with the coefficients of the polynomial equation. We call such a procedure *solution by radicals* where "radical" refers to taking n-th roots. In the case of cubic and quartic equations we have seen how this is done. As is known since the beginning of the 19-th century, the quintic equation cannot be solved by radicals. In order to prove this we have a closer look at field extensions by n-th roots (radicals).
More precisely, we discuss Galois groups of splitting fields of $X^n - a$. Formally we can write the zeros of $X^n - a$ by $\sqrt[n]{a}, \zeta\sqrt[n]{a}, \ldots, \zeta^{n-1}\sqrt[n]{a}$ where $\zeta = e^{2\pi i/n}$. In particular we see that the splitting field of $X^n - a$ contains the n-th roots of unity. We consider n-th roots as the simplest examples of radicals (of 1) and we will usually assume that they lie in the ground field we are considering.

Definition 9.4.1 Let K be a field. A finite extension L of K is called a *radical extension* if there exist $n \in \mathbb{Z}_{n>1}$ and $a \in K^*$ such that $L = K(\alpha)$ where α is a zero of $X^n - a$.

A particular case occurs if we take $a = 1$. Then it follows from Example **??** that the radical extension L/K is Galois with an abelian Galois group. In general, when $a \neq 1$, this is not true. For example, with $a = 2$, the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is certainly not Galois. However, it does become a Galois extension if we add in the cube root of unity ω. We have seen earlier that $\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}(\omega)$ is a Galois extension and it Galois group is cyclic of order 3. That this is a general phenomenon is shown by the following Theorem.

Theorem 9.4.2 *Let $n \in \mathbb{Z}_{>1}$ and let K be a field and let ζ be a generator of the zeros of $X^n - 1$ in some splitting field.*
Then, for any $a \in K^*$, the splitting field of $X^n - a$ over $K(\zeta)$ is a Galois extension of $K(\zeta)$ with a cyclic Galois group.
Conversely, let L/K be a Galois extension of degree n with a cyclic Galois group. Then $L(\zeta)/K(\zeta)$ is a radical extension.

Proof. Suppose L is the splitting field of $X^n - a$ over $K(\zeta)$. Denote one zero of $X^n - a$ by $\sqrt[n]{a}$. Then the other zeros are given by $\zeta^k \sqrt[n]{a}$ with $k = 0, 1, \ldots, n-1$. Furthermore, since K contains ζ, any Galois element sends $\sqrt[n]{a}$ to $\zeta^k \sqrt[n]{a}$ for some $k \in \mathbb{Z}/n\mathbb{Z}$. Denote this element by σ_k. One easily verifies that $\sigma_l\sigma_k(\sqrt[n]{a}) = \sigma_k\sigma_l(\sqrt[n]{a}) = \zeta^{k+l}\sqrt[n]{a}$. Hence $\mathrm{Gal}(L/K)$ is isomorphic to an additive subgroup of $\mathbb{Z}/n\mathbb{Z}$. Hence it is cyclic.
Suppose $\mathrm{Gal}(L/K)$ is cyclic of order n. Then, by Theorem 8.4.1, the extension $L(\zeta)/K(\zeta)$ is also Galois with a Galois group which is a subgroup of $\mathrm{Gal}(L/K)$, hence cyclic. So, without loss of generality we can assume that ζ is already contained in K, L and so, $K = K(\zeta)$ and $L = L(\zeta)$. By Theorem 8.5.1 there exists an element $\alpha \in L$ such that $L = K(\alpha)$. Let σ be a generator of $\mathrm{Gal}(L/K)$. Define for every $i = 0, 1, 2, \ldots, n-1$ the sum

$$\begin{aligned} s_i &= \alpha^i + \zeta\sigma(\alpha^i) + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha^i) \\ &= \alpha^i + \zeta\sigma(\alpha)^i + \cdots + \zeta^{n-1}\sigma^{n-1}(\alpha)^i \end{aligned}$$

Since the determinant of $(\sigma^j(\alpha)^i)_{i,j=0,\ldots,n-1}$ is non-zero at least one of the s_i is non-zero. Since, trivially, $s_0 = 1 + \zeta + \cdots + \zeta^{n-1} = 0$ we see that $s_i \neq 0 \Rightarrow i > 0$. Choose such an i. Notice that $\sigma(s_i) = \zeta^{-1}s_i$. Hence s_i has n distinct images under the Galois group and thus $K(s_i) = K(\alpha)$. Furthermore, $\sigma(s_i^n) = s_i^n$ and therefore $s_i^n \in K$. Let us now denote $a = s_i^n$. Then $L(\zeta) = L$ is the splitting field of $X^n - a$ over $K(\zeta) = K$.

9.5 Solvability

In talking about solvability it is convenient to speak of the Galois group of a polynomial.

Definition 9.5.1 Let $f \in K[X]$ be a separable polynomial. Then by the *Galois group* of f we mean the Galois group of the splitting field of f. Notation $\mathrm{Gal}(f/K)$.

We now formalise our concept of solvability by radicals.

Definition 9.5.2 Let K be a field and $f \in K[X]$. Denote its splitting field over K by L. Then we say that f is solvable by radicals if and only if there exists a tower of extensions

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_m$$

such that K_{i+1} is a radical extension of K_i for $i = 0, 1, 2, \ldots, m-1$ and such that $L \subset K_m$.

We like to translate solvability of a polynomial f by a property of the Galois group $\mathrm{Gal}(f/K)$.

Definition 9.5.3 A group G is called *solvable* If there is a finite tower of subgroups

$$\mathrm{id} = G_0 \subset G_1 \subset \cdots \subset G_r = G$$

such that

- For every $i = 0, 1, \ldots, r-1$ G_i is a normal subgroup of G_{i+1}.
- The quotients G_{i+1}/G_i are all cyclic.

We call the sequence $G_0, G_1, \ldots, G_r$ a *resolving sequence* of subgroups

A nice observation is that the solvability property of a group is inherited by its subgroups and quotients by normal subgroups.

Proposition 9.5.4 *Let G be a solvable group and H a subgroup. Then H is again solvable. Moreover, if H is a normal subgroup then G/H is again solvable.*

Proof. Let $\mathrm{id} = G_0 \subset G_1 \subset \cdots \subset G_r = G$ be the resolving sequence of subgroups. Then the sequence consisting of $G_i \cap H$ forms the resolving sequence of subgroups for H. To this end we need to show that $H \cap G_i$ is a normal subgroup of $H \cap G_{i+1}$ and $(H \cap G_{i+1})/(H \cap G_i)$ is cyclic. To this end end consider the group homomorphism $G_{i+1} \to G_{i+1}/G_i$ restricted to $H \cap G_{i+1}$. Clearly the kernel is $H \cap G_i$, which is normal, and the image, being a subgroup of the cyclic group G_{i+1}/G_i is cyclic. So $(G_{i+1} \cap H)/(G_i \cap H)$ is a cyclic group.
When H is normal in G consider the natural quotient map $\phi : G \to G/H$. For a resolving sequence $G_0, G_1, \ldots, G_r$ of G we define $H_i = \phi(\langle G_i, H \rangle)$ for $i = 0, \ldots, r$. Here $\langle G_i, H \rangle$ denotes the subgroup of G generated by the elements of G_i and H. We assert that $H_0, H_1, \ldots, H_r$ is a resolving sequence for G/H.
First note that $\langle G_i, H \rangle$ is a normal subgroup of $\langle G_{i+1}, H \rangle$. We leave this as an exercise. Then we have the following group theoretic isomorphisms

$$H_{i+1}/H_i \cong \langle G_{i+1}, H \rangle \,/\, \langle G_i, H \rangle \cong G_{i+1}/\langle G_i, G_{i+1} \cap H \rangle .$$

Hence H_{i+1}/H_i is isomorphic to a quotient group of G_{i+1}/G_i, which is cyclic. Hence H_{i+1}/H_i is also cyclic.

There exist groups which are not solvable, as is shown by the following Theorem.

Theorem 9.5.5 *The symmetric group S_n with $n \geq 5$ is not solvable.*

Proof. We assert that if H is a subgroup of S_n containing all 3-cycles, and N is a normal subgroup in H such that H/N is abelian, then N also contains all 3-cycles.
Indeed, suppose that $\sigma = (ijk)$ and $\tau = (krs)$ are 3-cycles for any five distinct i, j, k, r, s. By assumption, $\sigma \in H$ en $\tau \in H$. One easily verifies that $\sigma\tau\sigma^{-1}\tau^{-1} = (rki)$.
Consider the group homomorphsim $\phi : H \to H/N$ with kernel N. Since H/N is abelian, we have $\phi(\sigma\tau\sigma^{-1}\tau^{-1}) = 1$, so $\sigma\tau\sigma^{-1}\tau^{-1} \in \ker(\phi) = N$. As a consequence N contains the 3-cycle (rki) for all triples of distinct r, k, i.
Suppose S_n is solvable, then there is resolving sequence

$$S_n = H_0 \supseteq H_1 \supseteq \ldots \supseteq H_r = \{1\}$$

where the consecutive quotients are abelian groups. So by induction we find that H_r contains all 3-cycles. This is clearly not possible.

Remark 9.5.6 The argument only works if we can choose five distinct indices, so $n \geq 5$ in S_n. Furthermore S_n is sovable when $n \leq 4$: S_1 and S_2 are abelian. The group S_3 has the resolving sequence $\mathrm{id} \subset A_3 \subset S_3$. The group S_4 has the resolving sequence $\mathrm{id} \subset V_4 \subset A_4 \subset S_4$ with quotients $S_4/A_4 = \mathbb{Z}/2\mathbb{Z}$ en $A_4/V_4 = \mathbb{Z}/3\mathbb{Z}$. Here V_4 denotes Klein's fourgroup consisting of $\mathrm{id}, (12)(34), (13)(24), (14)(23)$.

9.6 Main Theorem

We now come to our main point.

Theorem 9.6.1 *A separable polynomial $f \in K[X]$ is solvable by radicals if and only if $\mathrm{Gal}(f/K)$ is solvable.*

Proof. We first set some notation. Let L/K be the splitting field of f and G its Galois group.
Suppose f is solvable. Then there exists a tower of fields

$$K = K_0 \subset K_1 \subset \cdots \subset K_m$$

such that K_{i+1} is a radical extension of K_i for $i = 0, 1, \ldots, m-1$ and $L \subset K_m$. First of all, by taking the Galois closure of K_m over K if necessary, we can assume that K_m/K is a Galois extension. Secondly, suppose the order of the radical extensions involved are $n_1, n_2, \ldots, n_m$ and $n = \mathrm{lcm}(n_1, \ldots, n_m)$. Let ζ be a primitive n-th root of unity. Then we can replace K_i by $K_i(\zeta)$ so that we get the chain $K \subset K(\zeta) \subset K_1(\zeta) \subset \cdots$ which is 1 element longer than the original chain.
Let $G_0 = \mathrm{Gal}(K_m(\zeta)/K(\zeta)) \supset G_1 \supset \cdots \supset G_m = \mathrm{id}$ be the corresponding sequence of subgroups of the Galois group, where $G_i = \mathrm{Gal}(K_m(\zeta)/K_i(\zeta))$. From Theorem 9.4.2 it follows that $K_{i+1}(\zeta)/K_i(\zeta)$ is a radical Galois extension with a cyclic Galois group. So G_{i+1} is a normal subgroup of G_i and G_i/G_{i+1} is cyclic. Hence the sequence of groups is solvable. We now extend the resolving sequence by $G_0 \subset \mathrm{Gal}(K_m(\zeta)/K)$. Note that $K(\zeta)/K$ is an extension by roots of unity, hence abelian and normal. So $\mathrm{Gal}(K_m(\zeta)/K(\zeta)$ is normal in $\mathrm{Gal}(K_m(\zeta)/K)$ with abelian quotient. Therefore $\mathrm{Gal}(K_m(\zeta)/K)$ is also solvable.
The field L is a normal extension of K. So $\mathrm{Gal}(K_m(\zeta)/L)$ is a normal subgroup of $\mathrm{Gal}(K_m(\zeta)/K)$ and $\mathrm{Gal}(L/K) \cong \mathrm{Gal}(K_m(\zeta)/K)/\mathrm{Gal}(K_m(\zeta)/L)$. Since $\mathrm{Gal}(K_m(\zeta)/K)$ is solvable, the same holds for the quotient group $\mathrm{Gal}(L/K)$.
Suppose conversely that $\mathrm{Gal}(L/K)$ is a solvable group. Suppose it is of order n. Let ζ be a generator of the zeros of $X^n - 1$ in some splitting field. Consider a resolving sequence $\mathrm{id} = G_0 \subset G_1, \ldots, G_r = \mathrm{Gal}(L/K)$. By Galois correspondence there is a sequence of subfields $L = K_0 \supset K_1 \supset \cdots \supset K_r = K$ such that $\mathrm{Gal}(L/K_i) = G_i$ for $i = 0, 1, \ldots, r$. Since G_i is a normal subgroup of G_{i+1} the extension $K_i \supset K_{i+1}$ is normal. Moreover, G_{i+1}/G_i is cyclic, so $\mathrm{Gal}(K_i/K_{i+1})$ is cyclic. Hence, by Theorem 9.4.2 the extension $K_i(\zeta)/K_{i+1}(\zeta)$ is a radical extension. So we get the sequence of radical extensions

$$K \subset K(\zeta) = K_r(\zeta) \subset K_{r-1}(\zeta) \subset \cdots \subset K_0(\zeta) \subset L(\zeta)$$

and $L \subset L(\zeta)$. Hence f is solvable by radicals.

Of course it is of interest to know if there are polynomial equations which are unsolvable by radicals. Here is a straightforward example.

Theorem 9.6.2 *Let k be a field and $L = k(t_1, \ldots, t_n)$ the function field in n variables. Let $K = k(s_1, s_2, \ldots, s_n)$ be the subfield of L generated by the elementary symmetric functions in $t_1, \ldots, t_n$. Then L/K is a finite extension of degree $n!$ with Galois group S_n.*

Proof. Note that L is the splitting field of $X^n - s_1X^{n-1} + s_2X^{n-2} - \cdots + (-1)^n s_n$ with zeros $t_1, \ldots, t_n$. The Galois group of L/K is a subgroup of S_n, the permutation group of $t_1, \ldots, t_n$. On the other hand, every permutation of $t_1, \ldots, t_n$ is a K-automorphism of L. Hence $\mathrm{Gal}(L/K) = S_n$.

Since S_n is unsolvable for $n \geq 5$, Theorem 9.6.1 implies that there cannot exist general formulas for the solution of the n-th degree equation with $n \geq 5$ of Cardano and Ferrari type. To make matters worse, we can also provide individual equations which cannot be solved by radicals.

Theorem 9.6.3 *The zeros of $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$ cannot be written as radical expressions in $\mathbb{Q}$.*

Proof. The polynomial f is irreducible by Eisenstein's criterion for $p = 3$. From the graph of f we see that f has at least 3 real zeros. If there would exist four real zeros, then by Rolle's Theorem f' would have at least three and f'' at least two distinct zeros. This contradicts $f'' = 20x^3$. So there must be a pair complex conjugate zeros as well. The next Lemma implies that $\mathrm{Gal}(f/\mathbb{Q}) \cong S_5$, which is not solvable.

Lemma 9.6.4 *Suppose that p is prime and $f \in \mathbb{Q}[x]$ a polynomial of degree p, irreducible in $\mathbb{Q}[X]$ with exactly $p - 2$ real zeros. Then $G := \mathrm{Gal}(f/\mathbb{Q}) \cong S_p$.*

Proof. Let α be a zero of f in in a splitting field L. Then $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \deg f = p$. So p divides $[L : \mathbb{Q}] = |G|$ where $G = \mathrm{Gal}(L/\mathbb{Q})$. Cauchy's theorem states that G contains an element σ of order p. G is a subgroup of S_p, so σ is a p-cycle in G.
Complex conjugation is an automorphism of $L/\mathbb{Q}$ which swaps the two complex zeros, but fixes the real zeros, so we get a transposition in G. In S_p any p-cycle and a transposition generate S_p and therefore $G = S_p$.

9.7 Exercises

??.1. (GALOISGROEP VAN DE VERGELIJKING VAN GRAAD 3) Stel dat $x^3 - px - q$ een vergelijking is van graad 3 over een lichaam K (niet van karakteristiek 2,3) en $G = \mathrm{Gal}(f/K)$. Stel dat $\{\alpha_i\}_{i=1}^3$ de drie wortels zijn van f in een splijtlichaam. De *discriminant* van f is bij definitie

$$D = \prod_{i<j}(\alpha_i - \alpha_j)^2 = -\prod_{i\neq j}(\alpha_i - \alpha_j).$$

(a) D is invariant onder G, dus $D \in K$.
(b) Bewijs dat D op een teken na (welk) gelijk is aan $\prod_{i=1}^{3} f'(\alpha_i)$, met f' de formele afgeleide van f. Bewijs vervolgens dat $D = 4p^3 - 27q^2$.
(c) Stel dat f irreducibel is over K en D een kwadraat in K, dan is $G \cong A_3$. (hint: als $D = d^2$ voor $d \in K$ dan is d invariant onder G, dus is elk element van G een even permutatie van de wortels; bovendien is $|G|$ deelbaar door $\deg(f)$.)
(d) Stel dat f irreducibel is over K en D geen kwadraat in K, dan is $G \cong S_3$. (hint: $[K(\sqrt{D}) : K] = 2$ en $deg(f) = 3$ delen allebei $|G|$.)

??.2. Geef een voorbeeld van een algebraïsch getal van graad 4 over $\mathbb{Q}$ dat *niet construeerbaar* is over $\mathbb{Q}$.

??.3. Geef een voorbeeld van een irreducibel polynoom van graad 7 over $\mathbb{Q}$ dat niet oplosbaar is in radicalen. Geef een voorbeeld van een irreducibel polynoom van graad 7 over $\mathbb{Q}$ dat wel oplosbaar is in radicalen.

??.4 In "Discours de la méthode pour bien conduire sa raison et chercher la verité dans les sciences; plus la dioptrique les meteores et la geometrie qui sont des essais de cete methode (Leiden, 1637) beslaat de sectie "La Geometrie" pp. 297-413. Aldaar staat op p. 323: *" Dont la raison est qu'il y a reigle generale pour reduire au cube toutes les difficultés qui vont au quarré de quarré, et au sursolide toutes celles qui vont au quarré de cube, de façon qu'on ne les doit point estimer plus composées."* Henk Bos interpreteert dit (in "Redefining geometrical exactness. Descartes' transformation of the early modern concept of construction", Springer-Verlag 2001, pp. 356 e.v.) als volgt: Descartes beweerde dat men de algemene vergelijking van graad 6 kan oplossen door toevoegen van radicalen en oplossingen van vergelijkingen van graad 5 (naar analogie met het resultaat van Ferrari dat de vierdegraadsvergelijking naar een vergelijking van graad 3 herleidt), maar zulk een reductie van graad 6 naar graad 5 is onmogelijk. Laat zien dat de bewering van Descartes, in deze interpretatie, inderdaad fout is.

??.5 Toon aan: voor elke eindige groep G bestaat er een lichaamsuitbreiding L/K zodat $\mathrm{Gal}(L:K) \cong G$ (je mag zowel L als K afhankelijk van G kiezen).

> **Opmerking.** Of het antwoord op deze vraag "ja" is met $K = \mathbf{Q}$ vast is één van de grote open problemen van de Galoistheorie.