5

Applications

We see in this chapter how Galois theory can be used to get a satisfactory answer to the problem of constructions with ruler and compass. By analogous methods, we discuss the problem of solving polynomial equations using radicals and we show how Galois theory allows us to understand the explicit resolution of equations of degrees up to 4*. Finally, we will study the behavior of the Galois group of an equation when we vary the coefficients.*

5.1 Constructibility with ruler and compass

Let us go back to the problem of geometric constructions with ruler and compass. We are mostly interested here in complex numbers which are constructible from the set $\{0,1\}$. By Wantzel's theorem (Theorem 1.4.1), these are the complex numbers z for which there is a sequence of extensions, $\mathbf{Q} = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_n$, such that $z \in K_n$ and such that for any i, $[K_i : K_{i-1}] = 2$. The main result is the following.

Theorem 5.1.1. *An algebraic number $z \in \mathbf{C}$ is constructible (from $\{0,1\}$) if and only if the degree of the extension of $\mathbf{Q}$ generated by z and its conjugates is a power of* 2*.*

To understand step by step what happens, let us begin by proving the following proposition.

Proposition 5.1.2. *Let $z \in \mathbf{C}$ be a constructible number. Then any conjugate of z is constructible.*

Proof. Let $\mathbf{Q} = K_0 \subset K_1 \subset \cdots \subset K_n$ be a sequence of quadratic extensions such that $z \in K_n$. Let $\mathbf{Q} \subset L$ be a Galois extension such that $K_n \subset L$. If z' is a conjugate of z, there exists an element $\sigma \in \mathrm{Gal}(L/\mathbf{Q})$ such that

$\sigma(z) = z'$. (This is essentially the content of the proof of Proposition 3.3.2; see Exercise 3.6.) Set $K'_j = \sigma(K_j)$ for $0 \leqslant j \leqslant n$. These are subfields of L and for any j, $K'_{j-1} \subset K'_j$, with $[K'_j : K'_{j-1}] = 2$. Since $z' \in K'_n$, this shows that z' is constructible. □

Proof of Theorem 5.1.1. Now let $z \in \mathbf{C}$ be a constructible number and let L be the extension of $\mathbf{Q}$ generated by the conjugates of z. By Theorem 1.1.3, any element in L is constructible. But $\mathbf{Q}$ having characteristic zero, it follows from the Primitive Element Theorem (Theorem 3.3.3) that there is $\alpha \in L$ such that $L = \mathbf{Q}[\alpha]$. This element α is constructible, so its degree is a power of 2, by Corollary 1.4.4. It follows that $[L : \mathbf{Q}]$ is a power of 2, which was to be shown.

Conversely, assume that $[L : \mathbf{Q}]$ is a power of 2. Since L is generated by the roots of the minimal polynomial of z, it is a splitting extension of a separable polynomial ($\mathbf{Q}$ has characteristic zero), hence a Galois extension (Proposition 3.2.7). The order of its Galois group $G = \mathrm{Gal}(L/K)$ is a power of 2. By Lemma 5.1.3 below, applied to $p = 2$, there exist subgroups $\{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$, each of index 2 in the next. They correspond to a sequence of extensions of $\mathbf{Q}$ contained in L, $\mathbf{Q} = L^G \subset L^{G_{n-1}} \subset \cdots \subset L^{G_0} = L$, with $[L^{G_j} : L^{G_{j+1}}] = (G_{j+1} : G_j) = 2$. By Wantzel's theorem 1.4.1, any element of L is then constructible. In particular, z is constructible. □

Lemma 5.1.3. *Let G be a finite group, the order of which is a power of a prime number p. Then G has a normal series*

$$\{1\} = G_0 \subset G_1 \subset \cdots \subset G_n = G$$

such that for any j, $(G_j : G_{j-1}) = p$.

Proof. We will argue by induction on the order of G. By Exercise 4.7, the center Z of G is a nontrivial commutative group. Let $g \in Z \setminus \{e\}$; the order of g divides $\mathrm{card}\, Z$, hence is a power of p, say p^a, with $a \geqslant 1$. It follows that $h = g^{p^{a-1}}$ is an element of Z of order p. Let G_1 denote the subgroup of G generated by h. It is a normal subgroup of order p in G. The cardinality of the group G/G_1 is a power of p, say p^m. By induction, there are subgroups $H_j \subset G/G_1$, for $0 \leqslant j \leqslant m$, such that H_{j-1} is a normal subgroup of H_j and $(H_j : H_{j-1}) = p$ for each j. For $2 \leqslant j \leqslant m+1$, let G_j denote the preimage of H_{j-1} in G/G_1. One has $G_1 \subset G_2 \subset \cdots \subset G_{m+1}$, G_{j-1} is a normal subgroup of G_j and $(G_j : G_{j-1}) = p$ for any $j \leqslant m+1$, and $G_{m+1} = G$. □

5.2 Cyclotomy

This name is the concatenation of two Greek roots, and it roughly means "cutting the circle." Consider a regular n-gon inscribed in the unit circle.

Its vertices divide the unit circle into n equal parts. By identifying points of the plane with the complex numbers, and assuming that one of the vertices is 1, these vertices correspond to nth roots of unity. Therefore, cyclotomy characterizes nowadays any study of mathematics that is related to roots of unity. For example, cyclotomic fields are fields generated by a root of unity, and the roots of the nth cyclotomic polynomial are exactly the primitive nth roots of unity.

We now obey the title of this section and begin by studying the Galois-theoretical properties of the equation $X^n = 1$.

Theorem 5.2.1. *Let K be a field, and let n be any positive integer. We assume that the characteristic of K does not divide n. Let $K \subset L$ be a splitting extension of the polynomial $X^n - 1$. It is a Galois extension, and its Galois group is isomorphic to a subgroup of the group $(\mathbf{Z}/n\mathbf{Z})^*$.*

More precisely, there is a canonical injective morphism of groups

$$\varphi\colon \mathrm{Gal}(L/K) \to (\mathbf{Z}/n\mathbf{Z})^*$$

such that for any nth root of unity $\zeta \in L$ and any $\sigma \in \mathrm{Gal}(L/K)$,

$$\sigma(\zeta) = \zeta^{\varphi(\sigma)}.$$

Proof. Fix a primitive nth root of unity ζ. Since the polynomial $X^n - 1$ is separable, the extension $K \subset L$ is Galois. The roots of $X^n - 1$ are the ζ^m, for $0 \leqslant m \leqslant n-1$, hence $L = K(\zeta)$.

Let $\sigma \in \mathrm{Gal}(L/K)$; it maps ζ to a nth root of unity, which is of the form ζ^m for some integer m whose class modulo m is well defined. Moreover, if $\sigma(\zeta)^k = 1$, one has $\zeta^k = 1$, hence $\sigma(\zeta)$ is still a primitive root, so that m is prime to n. This defines a map $\varphi\colon \mathrm{Gal}(K(\zeta)/K) \to (\mathbf{Z}/n\mathbf{Z})^*$.

Let θ be any nth root of unity, and fix an integer a such that $\theta = \zeta^a$. One has

$$\sigma(\theta) = \sigma(\zeta^a) = \sigma(\zeta)^a = (\zeta^m)^a = \zeta^{ma} = \theta^m,$$

and $\sigma(\theta) = \theta^{\varphi(\sigma)}$. This shows in particular that the map φ does not depend on the choice of a particular primitive root ζ.

If $\sigma, \tau \in \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$, with $\sigma(\zeta) = \zeta^m$ and $\tau(\zeta) = \zeta^n$, one has

$$(\sigma \circ \tau)(\zeta) = \sigma(\zeta^n) = \sigma(\zeta)^n = \zeta^{mn},$$

so that $\varphi(\sigma \circ \tau) = \varphi(\sigma)\varphi(\tau)$. This implies that φ is a morphism of groups. Moreover, if $\varphi(\sigma) = 1$, then $\sigma(\zeta) = \zeta$. Since ζ generates $\mathbf{Q}(\zeta)$, this implies $\sigma = \mathrm{id}$ and φ is injective. □

We saw in Chapter 1, Example 1.4.7, that it is impossible to construct a regular 9-gon with ruler and compass. However, C.-F. Gauss had shown that the regular polygon with 17 edges is actually constructible (as he wrote in his mathematical diary, March 30, 1796). He was barely 19 years old. We now prove a general result about the possibility of constructing regular polygons with ruler and compass.

Theorem 5.2.2. *A regular polygon with n sides is constructible with ruler and compass if and only if n is the product of a power of 2 and of distinct Fermat primes.*

Recall that a *Fermat prime* is a prime number of the form $F_m = 2^{2^m}+1$, where m is an integer. Among them are 3, 5, 17, 257 and 65537, corresponding to $m = 0, \dots, 4$. Fermat had conjectured that all F_m's are prime numbers but Euler showed that 641 divides F_5. (*Exercise*: prove it; show also that if n is not a power of 2, then 2^n+1 is not a prime number.) Actually, the five Fermat primes just listed above are the only known ones! It has also been proved that $F_6, \dots, F_{16}$ are not primes.

Proof. Let $\mathscr{P}$ be the set of integers $n \geqslant 3$ such that one can construct a regular n-gon with ruler and compass. In other words, an integer $n \geqslant 3$ belongs to $\mathscr{P}$ if and only if the algebraic number $\exp(2i\pi/n)$ is constructible. Its conjugates are among nth root of unity.

Using the following remarks, however, we reduce ourselves to the case where n is a prime or the square of a prime.

a) If $n \in \mathscr{P}$, then $2n \in \mathscr{P}$.

Indeed, if a regular n-gon is already drawn, one just needs, for each edge AB of it, to draw the perpendicular to AB passing through the center O of the n-gon, for it cuts the angle $\widehat{AOB}$ into two equal parts.

b) If $n \in \mathscr{P}$, then any integer $m \geqslant 3$ dividing n also belongs to $\mathscr{P}$.

To construct a regular m-gon, just join every (n/m)th vertex of a regular n-gon.

c) If m and n are two coprime integers belonging to $\mathscr{P}$, then their product mn belongs to $\mathscr{P}$.

That m and n belong to $\mathscr{P}$ means that the two complex numbers $\exp(2i\pi/m)$ and $\exp(2i\pi/n)$ are constructible. Since m and n are coprime, there are integers u and v such that $um + vn = 1$, hence

$$\exp(2i\pi/mn) = \exp\big(2i\pi\big(\frac{u}{n} + \frac{v}{m}\big)\big) = \big(\exp(2i\pi/n)\big)^u \big(\exp(2i\pi/m)\big)^v$$

is constructible, which in turns means that $mn \in \mathscr{P}$.

To prove the theorem, we now just need to prove that the only prime numbers in $\mathscr{P}$ are Fermat primes, and that $\mathscr{P}$ does not contain the square of any odd prime number. By Theorem 5.1.1, these two statements reduce to the following facts, where p is an odd prime number.

d) The complex number $\exp(2i\pi/p)$ *is an algebraic number of degree* $p-1$ *over* $\mathbf{Q}$. *The extension of* $\mathbf{Q}$ *generated by all* p*th roots of unity has degree* $p-1$.

Let P be the minimal polynomial of $\exp(2i\pi/p)$. It is a monic polynomial with integer coefficients and it divides $(X^p-1)/(X-1) = 1+X+\cdots+X^{p-1}$, hence there is $Q \in \mathbf{Z}[X]$ with

$$\frac{X^p-1}{X-1} = P(X)Q(X).$$

Set $a = \deg P$, $b = \deg Q$; in particular, $a+b = p-1$. Since $\exp(2i\pi/p)$ is not a rational number, $a \geqslant 2$.

Modulo p, one has $X^p - 1 \equiv (X-1)^p$. By uniqueness of decomposition into irreducible factors over $\mathbf{Z}/p\mathbf{Z}$, there are polynomials A and $B \in \mathbf{Z}[X]$ such that $P = (X-1)^a + pA(X)$, $Q = (X-1)^b + pB(X)$, Consequently,

$$\begin{aligned}\frac{X^p-1}{X-1} &= P(X)Q(X)\\ &= (X-1)^{a+b} + p\big(A(X)(X-1)^b + B(X)(X-1)^a\big) + p^2A(X)B(X).\end{aligned}$$

Now evaluate the two sides of this equality at 1. If one had $b \geqslant 1$, it would follow that $p = p^2AB(1)$, which is obviously a contradiction, for $AB(1)$ is an integer. Hence, $b = 0$, and $a = p-1$.

The last assertion comes from the fact that $\exp(2i\pi/p)$ generates the splitting extension over $\mathbf{Q}$ of the polynomial $X^p - 1$.

e) The complex number $\exp(2i\pi/p^2)$ *is an algebraic number of degree* $p(p-1)$ *over* $\mathbf{Q}$.

We do a similar analysis with the polynomial $X^{p^2}-1$ divided by its factor $X^p - 1$, which does not vanish at $\exp(2i\pi/p^2)$. If $P \in \mathbf{Z}[X]$ is the minimal polynomial of $\exp(2i\pi/p^2)$, there is as above a polynomial $Q \in \mathbf{Z}[X]$ such that

$$\frac{X^{p^2}-1}{X^p-1} = P(X)Q(X).$$

Since $X^{p^2} - 1 = (X-1)^{p^2}$ modulo p, we similarly find polynomials A and $B \in \mathbf{Z}[X]$ with $P = (X-1)^a + pA$ and $Q = (X-1)^b + pB$, where $a = \deg P \geqslant 2$ and $b = \deg Q$. Evaluating the resulting equality

$$\frac{X^{p^2}-1}{X^p-1} = (X-1)^{p^2-p} + p\big((X-1)^aB(X) + (X-1)^bA(X)\big) + p^2A(X)B(X)$$

at 1, we find as above that $b = 0$, hence the degree of $\exp(2i\pi/p^2)$ equals $a = p^2 - p$. □

Remark 5.2.3. These last two statements *d*) and *e*) are particular cases of a general theorem of Gauss, according to which the degree of $\exp(2i\pi/n)$ is equal to Euler's totient function $\varphi(n)$ (see Exercise 2.5). Together with Theorem 5.2.1, this shows that the Galois group of the extension $\mathbf{Q} \subset \mathbf{Q}(\exp(2i\pi/n))$ is isomorphic to $(\mathbf{Z}/n\mathbf{Z})^*$.

These particular cases, where $n = p^r$ is a power of a prime p, are usually proved using Eisenstein's criterion (Exercise 1.10). Indeed, applied to the polynomial $\Phi_{p^r}(Y+1)$ and the prime p, this criterion allows one to show that Φ_{p^r} is irreducible.

Corollary 5.2.4 (Gauss, 1801). *The regular polygon with* 17 *vertices is constructible with ruler and compass.*

Let us explain Gauss's explicit resolution of the equation $X^{17} = 1$. Let ζ be a primitive 17th root of unity in $\mathbf{C}$. The extension $\mathbf{Q} \subset \mathbf{Q}(\zeta)$ is Galois and its Galois group is isomorphic to $(\mathbf{Z}/17\mathbf{Z})^*$. Gauss's fundamental remark is that this group is cyclic, generated, for example, by the class of 3. Its powers modulo 17 are successively

$$1, 3, 9, 10, 13, 5, 15, 11, 16, 14, 8, 7, 4, 12, 2, 6, 1 \ldots$$

Let $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ be the corresponding generator, mapping ζ to ζ^3, and set

$$a_0 = \sum_{k=0}^{7} \sigma^{2k}(\zeta) = \zeta + \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16} + \zeta^8 + \zeta^4 + \zeta^2,$$
$$a_1 = \sum_{k=0}^{7} \sigma^{2k+1}(\zeta) = \zeta^3 + \zeta^{10} + \zeta^5 + \zeta^{11} + \zeta^{14} + \zeta^7 + \zeta^{12} + \zeta^6.$$

One has $\sigma(a_0) = a_1$ and $\sigma(a_1) = a_0$. It follows that a_0 and a_1 are the two roots of a quadratic equation in $\mathbf{Q}[X]$. Precisely, one has $a_0 + a_1 = -1$ and $a_0 a_1 = -4$, so that

$$a_0,\ a_1 = \frac{-1 \pm \sqrt{17}}{2}.$$

The choice of signs depends on the choice of ζ. If $\zeta = \exp(2i\pi/17)$, a numerical calculation shows that $a_0 = (-1 + \sqrt{17})/2$. Set $K_1 = \mathbf{Q}(\sqrt{17})$. The Galois group of the extension $K_1 \subset \mathbf{Q}(\zeta)$ is generated by σ^2.

We continue by defining, for $0 \leqslant i \leqslant 3$,

$$b_i = \sum_{k=0}^{3} \sigma^{4k+i}(\zeta),$$

so that $\sigma(b_i) = b_{i+1}$ if $i = 0, 1, 2$ and $\sigma(b_3) = b_1$. In particular, b_0 and b_2 are permuted by σ^2, they are the two roots of a quadratic equation in K_1. One has $b_0 + b_2 = a_0$ and $b_0 b_2 = -1$, so that

$$b_0,\ b_2 = \frac{1}{2}\big(a_0 \pm \sqrt{a_0^2 + 4}\big) = -\frac{1}{4} + \frac{1}{4}\sqrt{17} \pm \sqrt{34 - 2\sqrt{17}},$$

and again, choosing the positive square root for a positive real number, numerical calculations show that b_0 is given by the formula with the + sign. Similarly,

$$b_1,\ b_2 = -\frac{1}{4} - \frac{1}{4}\sqrt{17} \pm \sqrt{34 + 2\sqrt{17}}.$$

Set $K_2 = \mathbf{Q}(\sqrt{34 - 2\sqrt{17}})$. The extension $K_2 \subset \mathbf{Q}(\zeta)$ is Galois, with group generated by σ^4.

Now define, for $0 \leqslant i \leqslant 7$,

$$c_i = \sigma^i(\zeta) + \sigma^{i+8}(\zeta).$$

The quantities c_0 and c_4 are permuted under σ^4, hence are the two roots of a quadratic equation over K_2. Concretely, $c_0 + c_4 = a_0$ and $c_0 c_4 = b_1$, hence

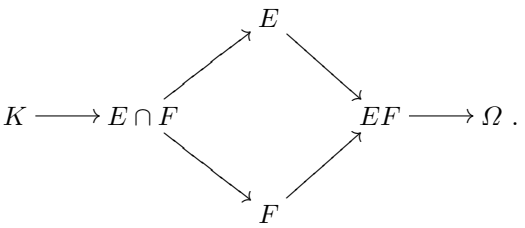
$$c_0,\ c_4 = \frac{1}{2}\big(a_0 \pm \sqrt{a_0^2 - 4b_1}\big).$$

Computing numerical values, with $\zeta = \exp(2i\pi/17)$, one then checks that $c_0 = 2\cos(2\pi/17)$ is given by the + sign, so that we have proved the following amazing formula:

$$2\cos(2\pi/17) = -\frac{1}{8} + \frac{1}{8}\sqrt{17} + \frac{1}{8}\sqrt{34 - 2\sqrt{17}} + \frac{1}{8}\sqrt{68 + 12\sqrt{17} - 2\sqrt{34 - 2\sqrt{17}} + 2\sqrt{34 - 2\sqrt{17}}\sqrt{17} - 16\sqrt{34 + 2\sqrt{17}}}.$$

5.3 Composite extensions

In this section, we study the following situation. Let K be a field; let Ω be an algebraic closure of K and let E, F be two extensions of K contained in Ω. We denote by EF the subfield of Ω generated by E and F. This is by definition the *composite extension* of E and F. Introduce also their intersection $E \cap F$, hence a diagram of fields as follows:



Lemma 5.3.1. *If the extension $K \subset E$ is Galois, then the extension $F \subset EF$ is Galois. If moreover the extension $K \subset F$ is Galois, the extensions $K \subset EF$ and $K \subset E \cap F$ are Galois.*

Proof. Assume that $K \subset E$ is a splitting extension of a separable polynomial $P \in K[X]$ (in other words, E is generated by the roots of P in Ω). Then $F \subset EF$ is a splitting extension of P over the field F, so is a Galois extension, by Proposition 3.2.7. If $K \subset F$ is itself a splitting extension of a separable polynomial $Q \in K[X]$, then $K \subset EF$ is a splitting extension of the polynomial PQ or, preferably, of the separable polynomial $\mathrm{l.c.m.}(P, Q)$ (see Exercise 3.2). In particular, the extension $K \subset EF$ is Galois. This shows the first two assertions of the lemma.

To prove that the extension $K \subset E \cap F$ is Galois, provided $K \subset E$ and $K \subset F$ are, it suffices to check that for any K-homomorphism $\sigma\colon E \cap F \to \Omega$, one has $\sigma(E \cap F) = E \cap F$, for then the result will follow from Proposition 3.2.7. By Theorem 3.1.6, such a morphism σ can be extended to a K-homomorphism $\tau\colon EF \to \Omega$. Since the extension $K \subset E$ is Galois, $\tau(E) = E$. Similarly, $\tau(F) = F$. Hence, $\tau(E \cap F) \subset E \cap F$. By Remark 3.2.3, $\tau(E \cap F) = E \cap F$.□

Assume now that $K \subset E$ is a Galois extension and let us show how one can identify $\mathrm{Gal}(EF/F)$ with a subgroup of $\mathrm{Gal}(E/K)$. An element $\sigma \in \mathrm{Gal}(EF/F)$ is an automorphism of EF which restricts to the identity on F. In particular, $\sigma|_K = \mathrm{id}_K$ and $\sigma \in \mathrm{Gal}(EF/K)$. Since the extension $K \subset E$ is Galois, $\sigma(E) = E$, so that σ defines an element in $\mathrm{Gal}(E/K)$ that we denote $i(\sigma)$. The map $i\colon \mathrm{Gal}(EF/F) \to \mathrm{Gal}(E/K)$ is a morphism of groups, because it is the composition of the two natural morphisms

$$\mathrm{Gal}(EF/F) \hookrightarrow \mathrm{Gal}(EF/K) \twoheadrightarrow \mathrm{Gal}(E/K).$$

Proposition 5.3.2. *The morphism i is injective; its image is* $\mathrm{Gal}(E/E \cap F)$.

Proof. If $\sigma \in \mathrm{Gal}(EF/F)$ satisfies $i(\sigma) = \mathrm{id}_E$, then σ restricts to the identity on E. One thus has $\sigma(x) = x$ for any x in F and for any x in E, so that $\sigma(x) = x$ for any x in the field generated by E and F, which is EF. This shows that $\sigma = \mathrm{id}$, hence i is injective.

Its image $i(\mathrm{Gal}(EF/F))$ is a subgroup H of $\mathrm{Gal}(E/K)$ and corresponds by Galois correspondence to the subfield E^H of E and one has $H = \mathrm{Gal}(E/E^H)$.

(Recall that E^H is the set of all $x \in E$ such that $\sigma(x) = x$ for any $\sigma \in \mathrm{Gal}(EF/F)$.) Therefore $E \cap F \subset E^H$, but conversely, if $x \in E \setminus (E \cap F)$, one has $x \in EF \setminus F$ and there is $\sigma \in \mathrm{Gal}(EF/F)$ with $\sigma(x) \neq x$, hence $x \notin E^H$. This shows that $E^H = E \cap F$; consequently $H = \mathrm{Gal}(E/E \cap F)$. □

An immediate corollary of this proposition is the following formula for the degrees of the various extensions we have been discussing.

Corollary 5.3.3. *Assume that the extension $K \subset E$ is Galois. Then,*

$$[EF : F] = [E : E \cap F].$$

In particular, $[EF : K] = [E : K]\,[F : K]$ if and only if $K = E \cap F$.

Proof. Indeed, $[EF : F]$ is the cardinality of $\mathrm{Gal}(EF/F)$. By the proposition, $\mathrm{card}\, i(\mathrm{Gal}(EF/F)) = \mathrm{card}\, \mathrm{Gal}(E/E \cap F)$, whence $[EF : F] = [E : E \cap F]$. Consequently,

$$[EF : K] = [E : E \cap F]\,[F : K] = \frac{[E : K]\,[F : K]}{[E \cap F : K]},$$

so that $[EF : K] = [E : F]\,[F : K]$ if and only if $E \cap F = K$. □

In the case where the two extensions $K \subset E$ and $K \subset F$ are Galois, we will compute the Galois group of EF over K in terms of the groups $\mathrm{Gal}(E/K)$ and $\mathrm{Gal}(F/K)$. First consider the homomorphism

$$j\colon \mathrm{Gal}(EF/K) \to \mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$$

deduced from the two surjective morphisms $\mathrm{Gal}(EF/K) \to \mathrm{Gal}(E/K)$ and $\mathrm{Gal}(EF/K) \to \mathrm{Gal}(F/K)$. (They are well defined, for the extensions $K \subset E$ and $K \subset F$ are Galois; see Proposition 3.2.9). If $\sigma \in \mathrm{Gal}(EF/K)$ restricts to the identity on E and on F, it induces the identity on the field generated by E and F in Ω, hence on EF. It follows that $\sigma = \mathrm{id}$ and j is injective.

First assume that $K = E \cap F$. By Corollary 5.3.3, one has $[EF : K] = [E : K][F : K]$. Since j is injective, it must be surjective.

In the general case, we have shown in Lemma 5.3.1 that the extension $K \subset E \cap F$ is Galois. Let us see what happens if we compose j with the surjective homomorphisms

$$\pi_1\colon \mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K) \to \mathrm{Gal}(E/K) \to \mathrm{Gal}(E \cap F/K)$$

and

$$\pi_2\colon \mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K) \to \mathrm{Gal}(F/K) \to \mathrm{Gal}(E \cap F/K).$$

By construction, $\pi_1 \circ j$ and $\pi_2 \circ j$ are both equal to the natural morphism

$$\mathrm{Gal}(EF/K) \to \mathrm{Gal}(E \cap F/K)$$

corresponding to the Galois subextension $K \subset E \cap F$ of $K \subset EF$. Therefore, the image of j is contained in the subgroup G of $\mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$ consisting of all (σ_1, σ_2) such that $\pi_1(\sigma_1) = \pi_2(\sigma_2)$.

If we show that $\operatorname{card} G = \operatorname{card} \mathrm{Gal}(EF/K)$, it will follow that j is an isomorphism from $\mathrm{Gal}(EF/K)$ onto G. If Δ denotes the diagonal subgroup in $\mathrm{Gal}(E \cap F/K) \times \mathrm{Gal}(E \cap F/K)$ consisting of all (σ, σ), with $\sigma \in \mathrm{Gal}(E \cap F/K)$, we see that G is the preimage of Δ by the surjective morphism

$$(\pi_1, \pi_2)\colon\ \mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K) \to \mathrm{Gal}(E \cap F/K) \times \mathrm{Gal}(E \cap F/K).$$

Therefore,

$$\begin{aligned}
\operatorname{card} G &= \operatorname{card} \mathrm{Gal}(E \cap F/K) \times \operatorname{card} \mathrm{Ker}(\pi_1, \pi_2) \\
&= [E \cap F : K] \times [E : E \cap F] \times [F : E \cap F] \\
&= [F : K] \times [E : E \cap F] \\
&= [F : K] \times [EF : F] \\
&= [EF : K].
\end{aligned}$$

We have thus proved the following theorem.

Theorem 5.3.4. *Let us consider a composite extension $K \subset EF$, where $K \subset E$ and $K \subset F$ are two Galois extensions contained in an algebraic closure of K. The extension $K \subset EF$ is Galois and its Galois group is isomorphic to the subgroup of $\mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$ consisting of all couples (σ, τ) such that σ and τ have the same image in $\mathrm{Gal}(E \cap F/K)$.*

In particular, if $E \cap F = K$, $\mathrm{Gal}(EF/K)$ can be identified with the direct product $\mathrm{Gal}(E/K) \times \mathrm{Gal}(F/K)$.

5.4 Cyclic extensions

By definition, a *cyclic extension* is a Galois extension whose Galois group is cyclic, hence isomorphic to $\mathbf{Z}/n\mathbf{Z}$, where n denotes the degree of the extension.

If K is a field, let us denote by $\mu_n(K)$, or μ_n in short, the (cyclic) group of nth roots of unity in K. In this section, we will often assume that μ_n has order n. In this case, it is generated by a primitive nth root of unity. If the characteristic of the field K is equal to a prime number p, this implies that n is not a multiple of p.

This section is devoted to the determination of the field extensions of K which are Galois with Galois group $\mathbf{Z}/n\mathbf{Z}$.

Let us begin by an example, which in fact is *the* example.

Theorem 5.4.1. *Let K be a field and let n be any integer with $n \geqslant 2$. We assume that* $\operatorname{card} \mu_n(K) = n$.

Let $a \in K^*$ and let $K \subset L$ be a splitting extension of the polynomial $P = X^n - a$; denote by x a root of P in L.

The extension $K \subset L$ is Galois. The map $i\colon \sigma \mapsto i(\sigma) = \sigma(x)/x$ defines an injective group morphism from $\mathrm{Gal}(L/K)$ *to $\mu_n(K)$. Let d be the smallest positive integer such that $x^d \in K$. Then d divides n, and the image of the morphism i is equal to $\mu_d(K)$.*

In particular, the following are equivalent:

a) *for any integer $m > 1$ dividing n, a is not an mth power in K;*
b) *the polynomial $X^n - a$ is irreducible in $K[X]$;*
c) $\mathrm{Gal}(L/K) \simeq \mathbf{Z}/n\mathbf{Z}$.

Proof. In $L[X]$, the polynomial $P = X^n - a$ can be factored as

$$P = X^n - a = \prod_{\zeta \in \mu_n} (X - \zeta x).$$

Since $\operatorname{card} \mu_n(K) = n$, the characteristic of K does not divide n and any root ζx of P in L is simple, for $P'(\zeta x) = n(\zeta x)^{n-1} = na/(\zeta x) \neq 0$. In other words, the polynomial P is separable and the extension $K \subset L$ is Galois.

Any K-automorphism σ of L is determined by the image $\sigma(x)$ of x, which is a root of $X^n - a$. Then $\sigma(x)/x$ is an nth root of unity. This defines a map $i\colon \mathrm{Gal}(L/K) \to \mu_n$, such that $i(\sigma) = \sigma(x)/x$.

Observe that i is a group homomorphism; if $\sigma(x) = ux$ and $\tau(x) = vx$ for $u, v \in \mu_n$, then

$$(\sigma \circ \tau)(x) = \sigma(vx) = v\sigma(x) = uvx,$$

since $v \in K$; hence $i(\sigma \circ \tau) = i(\sigma)i(\tau)$. The image of i in μ_n is a subgroup, necessarily of the form μ_d for some integer d dividing n. One has $[L : K] = \operatorname{card} \mathrm{Gal}(L/K) = d$, and d is the degree of the minimal polynomial of x over K, for $L = K[x]$. Notice also that $\mathrm{Gal}(L/K) \simeq \mu_d(K) \simeq \mathbf{Z}/d\mathbf{Z}$.

Let m be any integer. One has $x^m \in K$ if and only if $\sigma(x^m) = x^m$ for any $\sigma \in \mathrm{Gal}(L/K)$. Since $\sigma(x) = i(\sigma)x$, this holds if and only if $i(\sigma)^m = 1$ for any $\sigma \in \mathrm{Gal}(L/K)$, hence if and only if $\zeta^m = 1$ for any ζ in the image of $\mathrm{Gal}(L/K)$ by i. Since $i(\mathrm{Gal}(L/K)) = \mu_d(K)$, one has $x^m \in K$ if and only if d divides m. It follows in particular that $a = x^n = (x^d)^{n/d}$ is an (n/d)th power in K. If one assumes that a is not an mth power in K for any integer $m > 1$ dividing n, then $d = n$ and $P = X^n - a$ is irreducible in $K[X]$. Conversely, assuming that $a = b^e$ for some $b \in K$ and some integer $e > 1$ dividing n, the equality

$$P = X^n - a = X^{me} - b^e = (X^m - b)(X^{m(e-1)} + X^{m(e-2)}b + \cdots + b^{e-1})$$

shows that P is not irreducible in $K[X]$. □

Conversely, let $K \to L$ be any finite Galois extension, with Galois group $\mathbf{Z}/n\mathbf{Z}$. Let σ be any generator of $\mathrm{Gal}(L/K)$. The preceding proof suggests that we seek for an element $x \in L$ such that $L = K[x]$ and such that $\sigma(x)/x$ is an nth root of unity. Let $\zeta \in \mu_n$ be any primitive nth root of unity and let us define, for $t \in L$, the *Lagrange's resolvent* of t, by the formula

$$x = t + \zeta^{-1}\sigma(t) + \cdots + \zeta^{1-n}\sigma^{n-1}(t).$$

It is proved in Exercise 3.12 that the elements of $\mathrm{Gal}(L/K)$ are linearly independent over K. Consequently, one may find $t \in L$ such that $x \neq 0$. Then

$$\sigma(x) = \sigma(t) + \zeta^{-1}\sigma^2(t) + \cdots + \zeta^{1-n}\sigma^n(t) = \zeta x,$$

since $\sigma^n = \mathrm{id}$ and $\zeta^n = 1$. By induction, for any $k \in \{0, 1, \ldots, n-1\}$, one has

$$\sigma^k(x) = \zeta^k x.$$

It follows that for any integer k, $\sigma^k(x^n) = x^n$. Since $\mathrm{Gal}(L/K) = \{\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^{n-1}\}$, $a = x^n$ belongs to K.

Let

$$P = X^n - a = \prod_{k=0}^{n-1}(X - \zeta^k x) = \prod_{k=0}^{n-1}(X - \sigma^k(x)).$$

It is a separable polynomial in $K[X]$, split in L. Consequently, the extension $K \subset K(x)$ is a splitting extension of the polynomial P. Since $\mathrm{Gal}(L/K)$ acts transitively on its roots, this polynomial is irreducible. This implies $[K(x) : K] = n$, and since one has $[L : K] = n$, it follows necessarily that $L = K(x)$, hence x is a primitive element of the extension $K \subset L$, with minimal polynomial $X^n - a$. (See also Exercise 3.8.)

We finally have proved the following theorem.

Theorem 5.4.2. *Let K be a field and let n be any integer $\geqslant 2$ such that* $\mathrm{card}\,\mu_n(K) = n$.

If $K \subset L$ is a Galois extension whose Galois group is isomorphic to $\mathbf{Z}/n\mathbf{Z}$, there exists $a \in K$ such that L is a splitting extension of the irreducible polynomial $X^n - a \in K[X]$.

5.5 Equations with degrees up to 4

We are now going to analyse equations of degree $\leqslant 4$ in light of Galois theory. What will allow us to explicitly solve such equations is that in each of the

three groups $\mathfrak{S}_2$, $\mathfrak{S}_3$ and $\mathfrak{S}_4$, there is a normal series such that the successive quotients are cyclic (with order 2 or 3), i.e. , these groups are solvable. By Corollary 4.6.8, this does not happen in $\mathfrak{S}_n$ for $n > 4$. Recall that the symbol $\triangleleft$ means that the group on the left is normal in the next, and the number above it indicates the order of the quotient. Also recall that one denotes by V_4 the *Klein four-group* in $\mathfrak{A}_4$, the four elements of which are the permutations

$$\mathrm{id}, \quad (1,2)(3,4), \quad (1,3)(2,4), \quad (1,4)(2,3)$$

on the set $\{1,2,3,4\}$ (these are the products of two transpositions with disjoint supports, plus the identity). This group is isomorphic to $(\mathbf{Z}/2\mathbf{Z})^2$. Now, one has the following normal series:

$$\{1\} = \mathfrak{A}_2 \overset{2}{\triangleleft} \mathfrak{S}_2 = \mathbf{Z}/2\mathbf{Z}$$
$$\{1\} \overset{3}{\triangleleft} \langle (1,2,3) \rangle \overset{2}{\triangleleft} \mathfrak{A}_3 \overset{2}{\triangleleft} \mathfrak{S}_3$$
$$\{1\} \overset{2}{\triangleleft} \{1, (1,2)(3,4)\} \overset{2}{\triangleleft} V_4 \overset{3}{\triangleleft} \mathfrak{A}_4 \overset{2}{\triangleleft} \mathfrak{S}_4 \ .$$

Felix Klein (1849–1925)

In this section, we consider only fields whose characteristic is neither 2 *nor* 3.

Let K be such a field and let P be a monic polynomial in $K[X]$ with degree $n \leqslant 4$. Let $K \subset L$ be the splitting extension of P contained in some fixed algebraic closure Ω of K. (All extensions in this section will be assumed to live in Ω.) Denote by $x_1, x_2, \ldots, x_n$ the roots of P in L and let $G = \mathrm{Gal}(L/K)$. This is naturally a subgroup of $\mathfrak{S}_n$.

The intersections with G of the above-written subgroups of $\mathfrak{S}_n$ define a normal series in G, and the successive quotients are cyclic groups with order $\leqslant 3$ (they may be trivial). Such a series corresponds to a chain of Galois extensions. We already explained in Chapter 3, Prop. 3.4.2, how the subgroup $\mathfrak{A}_n \subset \mathfrak{S}_n$ corresponds to the extension generated by a square root of the discriminant of P.

Let us first consider degree 2. Then $P = X^2 + aX + b$ for $a, b \in K$ and the discriminant of P is equal to $\Delta = a^2 - 4b$. If Δ is a square in K, the roots of P belong to K and $G = \{1\}$. Otherwise, $L = K(\sqrt{\Delta})$ has degree 2 over K. We can order the roots so that $x_1 - x_2 = \sqrt{\Delta}$. Together with the relation $x_1 + x_2 = a$, this determines $x_1 = (a + \sqrt{\Delta})/2$ and $x_2 = (a - \sqrt{\Delta})/2$.

Assume now that P is a separable polynomial with degree 3 in $K[X]$:

$$P = X^3 + a_1 X^2 + a_2 X + a_3.$$

The change of variables $Y = X + a_1/3$ allows us to assume that the sum of its roots is equal to 0 or, in other words, that P is of the form $P = X^3 + pX + q$. Its discriminant is then equal to $D = -4p^3 - 27q^2$ (Example 3.4.1). Let us consider the extensions

$$K \overset{2}{\subset} K(\sqrt{\Delta}) \overset{3}{\subset} L,$$

where each extension is either trivial, or Galois with Galois group the cyclic group of cardinality indicated above the inclusion sign. If the polynomial P is irreducible, we already can deduce from this the Galois group of L over K. Indeed, the degree of the extension $K \subset L$ is a multiple of 3 and $\mathrm{Gal}(L/K)$ is $\mathfrak{S}_3$ when Δ is not a square, and is $\mathfrak{A}_3$ if Δ is a square in K.

To give explicit formulas for the roots of P, we first have to adjoin $\sqrt{\Delta}$. The remaining extension $K(\sqrt{\Delta}) \overset{3}{\subset} L$ is either trivial if the field $K(\sqrt{\Delta})$ contains the three roots of P, or cyclic with Galois group $\mathbf{Z}/3\mathbf{Z}$.

Proceeding as in the case of extensions with a cyclic Galois group (Section 5.4), let us first add to $K(\sqrt{\Delta})$ the cubic roots of unity ρ and ρ^2. These are the roots of the polynomial $X^2 + X + 1$. Recall that we may assume

$$\rho = -\frac{1}{2} + \frac{1}{2}\sqrt{-3}, \quad \rho^2 = -\frac{1}{2} - \frac{1}{2}\sqrt{-3}$$

where $\sqrt{-3}$ denotes a square root of -3 in $K(\sqrt{\Delta}, \rho)$. In particular, $\rho - \rho^2 = \sqrt{-3}$. Set $K' = K(\rho)$ and $L' = L(\rho)$.

The resulting extension $K'(\sqrt{\Delta}) \subset L'$ is either trivial or cyclic with order 3. Corresponding to the circular permutation $(1, 2, 3)$, there are two *Lagrange's resolvents* that one can introduce:

$$\alpha = x_1 + \rho x_2 + \rho^2 x_3 \quad \text{and} \quad \beta = x_1 + \rho^2 x_2 + \rho x_3.$$

Let us now compute α^3 and β^3:

$$\alpha^3 = x_1^3 + x_2^3 + x_3^3 + 6x_1x_2x_3 + 3\rho(x_1^2x_2 + x_2^2x_3 + x_3^2x_1) + 3\rho^2(x_1x_2^2 + x_2x_3^2 + x_3x_1^2)$$

and β^3 is given by the formula obtained by switching ρ and ρ^2. The first term in these expressions is a symmetric function of the roots, hence can be expressed with p and q. Explicitly:

$$\begin{aligned} x_1^3 + x_2^3 + x_3^3 + 6x_1x_2x_3 &= (x_1 + x_2 + x_3)^3 - 3(x_1^2x_2 + \dots) \\ &= -3\big(x_1x_2(x_1 + x_2) + \dots\big) \\ &= -3x_1x_2(-x_3) - \dots \\ &= 9x_1x_2x_3 = -9q. \end{aligned}$$

The two other terms are not symmetric functions, and we cannot hope for them to be, otherwise α^3 and β^3 would always belong to K'. However, we

know that they belong to $K'(\sqrt{\Delta})$ and the aim of the game is to find a formula for them! Since Δ has two square roots, we have to choose one of them and we set

$$\sqrt{\Delta} = (x_1-x_2)(x_1-x_3)(x_2-x_3) = (x_1^2x_2+x_2^2x_3+x_3^2x_1)-(x_1x_2^2+x_2x_3^2+x_3x_1^2).$$

Defining

$$A = x_1^2x_2 + x_2^2x_3 + x_3^2x_1 \quad \text{and} \quad B = x_1x_2^2 + x_2x_3^2 + x_3x_1^2,$$

we find the relations

$$A + B = 3q \quad \text{and} \quad A - B = \sqrt{\Delta},$$

hence

$$A = \frac{3}{2}q + \frac{1}{2}\sqrt{\Delta} \quad \text{and} \quad B = \frac{3}{2}q - \frac{1}{2}\sqrt{\Delta}.$$

Let us write down these expressions in the formulae for α^3 and β^3:

$$\begin{aligned}\alpha^3 &= -9q + 3\rho A + 3\rho^2 B \\ &= -9q + \frac{3}{2}q(3\rho + 3\rho^2) + \frac{1}{2}\sqrt{\Delta}(3\rho - 3\rho^2) \\ &= -\frac{27}{2}q + \frac{3}{2}\sqrt{-3}\sqrt{\Delta}\end{aligned}$$

and

$$\beta^3 = -\frac{27}{2}q - \frac{3}{2}\sqrt{-3}\sqrt{\Delta}.$$

Moreover, since $\sigma(\alpha) = \rho^{-1}\alpha$ and $\sigma(\beta) = \rho^{-2}\beta$, one has $\sigma(\alpha\beta) = \alpha\beta$ and $\alpha\beta \in K'$. Actually,

$$\begin{aligned}\alpha\beta &= (x_1 + \rho x_2 + \rho^2 x_3)(x_1 + \rho^2 x_2 + \rho x_3) \\ &= x_1^2 + x_2^2 + x_3^2 + (\rho + \rho^2)(x_1x_2 + x_2x_3 + x_3x_1) \\ &= (x_1 + x_2 + x_3)^2 + (\rho + \rho^2 - 2)(x_1x_2 + x_2x_3 + x_3x_1) \\ &= -3p.\end{aligned}$$

To derive explicit formulae for x_1, x_2 and x_3, it remains to note that one has a Cramer system with three linear equations in three unknowns:

$$\begin{cases} x_1 + x_2 + x_3 = 0 \\ x_1 + \rho x_2 + \rho^2 x_3 = \alpha \\ x_1 + \rho^2 x_2 + \rho x_3 = \beta. \end{cases}$$

Therefore,

$$\begin{cases} x_1 = \dfrac{1}{3}\alpha + \dfrac{1}{3}\beta \\ x_2 = \dfrac{1}{3}\rho^2\alpha + \dfrac{1}{3}\rho\beta \\ x_3 = \dfrac{1}{3}\rho\alpha + \dfrac{1}{3}\rho^2\beta. \end{cases}$$

Jerome Cardan (1501–1576)

These are "*Cardan's formulae*." (Concerning history, Jerome Cardan had bought them to Tartaglia under the promise of not publishing them, a promise which was broken when Cardan published his *Ars magna sive de regulis algebraicis liber unus* in 1545. Before that, Scipione del Ferro, an Italian like Cardan, had discovered how to solve equations of degree 3 but only at the moment of his death did he explain his method, and only for a particular case!)

In practice, if one wants to solve a cubic equation, this can all be ignored and one needs to remember only the following procedure: write one of the roots $x = u + v$ with $uv = -p/3$, then expand

$$0 = (u+v)^3 + p(u+v) + q = u^3 + v^3 + 3uv(u+v) + p(u+v) + q = u^3 + v^3 + q,$$

so that u^3 and v^3 are solutions of the quadratic equation

$$X^2 + qX - \frac{p^3}{27} = 0.$$

Therefore, the value of u^3 can be deduced from one of the square roots of the discriminant $q^2 + \dfrac{4}{27}p^3 = -\Delta/27$, then the value of u through a cubic root, and finally the value for $x = u - p/3u$. (This works well for $p \neq 0$, but the case $p = 0$ is easy.)

You might also notice that when x_1, x_2 and x_3 are real numbers, Δ is a positive real number, hence Cardan's formulae use complex numbers. This is the so-called *casus irreductibilis*, and there is no way to avoid it (see Exercise 7.2).

Let us finally explain how to solve equations of degree 4. Let

$$P = X^4 + pX^2 + qX + r$$

be a monic polynomial of degree 4, where the coefficient of X^3 is assumed to be 0 up to a linear change of variables. Let us recall the sequence of normal subgroups in $\mathfrak{S}_4$:

$$\{1\} \overset{2}{\lhd} \{1, (1,2)(3,4)\} \overset{2}{\lhd} V_4 \overset{3}{\lhd} \mathfrak{A}_4 \overset{2}{\lhd} \mathfrak{S}_4,$$

hence a chain of Galois extensions

$$K \overset{2}{\subset} K(\sqrt{\Delta}) \overset{3}{\subset} K_1 \overset{2}{\subset} K_2 \overset{2}{\subset} L.$$

(The numbers above the inclusion symbol mean that the extension is either trivial, or cyclic with corresponding degree.) We now can use a similar approach to the one we gave for degree 3.

Let us immediately introduce a resolvent polynomial corresponding to the extension $K \subset K_1$. The polynomial $R_1 = (X_1 + X_2)(X_3 + X_4)$ is invariant under the permutations of V_4, and its orbit under the symmetric group $\mathfrak{S}_4$ consists of the three polynomials

$$R_1, \quad R_2 = (X_1 + X_3)(X_2 + X_4) \quad \text{and} \quad R_3 = (X_1 + X_4)(X_2 + X_3).$$

It follows first that $\theta_1 = (x_1 + x_2)(x_3 + x_4)$, $\theta_2 = (x_1 + x_3)(x_2 + x_4)$, and $\theta_3 = (x_1 + x_4)(x_2 + x_3)$ belong to $K_1 = L^{V_4}$, and second that the degree 3 polynomial

$$Q(X) = (X - \theta_1)(X - \theta_2)(X - \theta_3)$$

has its coefficients in K. This polynomial is usually called the Lagrange's resolvent polynomial of the quartic equation. If P is separable, which we assume, then θ_1, θ_2 and θ_3 are distinct. In fact, one has

$$\theta_1 - \theta_2 = (x_4 - x_1)(x_2 - x_3),$$

and similar formulae for $\theta_2 - \theta_3$ and $\theta_1 - \theta_2$. This shows moreover that the discriminant of Q is equal to that of P.

Exercise 5.5.1. Show that $Q(X) = X^3 - 2pX^2 + (p^2 - 4r)X + q^2$.

Assume now that we have determined θ_1, θ_2 and θ_3, e.g. , using Cardan's formulae. By the relations $(x_1+x_2)(x_3+x_4) = \theta_1$ and $(x_1+x_2)+(x_3+x_4) = 0$, we see that $x_1 + x_2$ is a square root of $-\theta_1$, say $\sqrt{-\theta_1}$. Similarly, $x_1 + x_3$ and $x_1 + x_4$ are square roots of $-\theta_2$ and $-\theta_3$ respectively. Pay attention to the fact that these three square roots cannot be taken arbitrarily: the degree of

the extension $K_1 \subset L$ divides 4 and three "independent" square roots would make the degree a multiple of 8. Actually, one has

$$\sqrt{-\theta_1}\sqrt{-\theta_2}\sqrt{-\theta_3} = (x_1+x_2)(x_1+x_3)(x_1+x_4)$$
$$= x_1^3 + x_1^2(x_2+x_3+x_4) + x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4 = -q.$$

If $q = 0$, the quartic equation is "biquadratic" and can be solved easily. Otherwise, if $q \neq 0$, the θ_i are nonzero and this formula computes $\sqrt{-\theta_3} = -q/\sqrt{-\theta_1}\sqrt{-\theta_2}$. Then,

$$2x_1 = 3x_1 + x_2 + x_3 + x_4 = \sqrt{-\theta_1} + \sqrt{-\theta_2} + \sqrt{-\theta_3}$$

and analogous formulae for x_2, x_3 and x_4.

Assuming that P is irreducible in $K[X]$, let us determine the various possible Galois groups.

First observe that the extension $K(\sqrt{\Delta}) \subset K_1$ has degree either 1 or 3, for it is Galois and its Galois group is a subquotient of $\mathfrak{A}_4/V_4 \simeq \mathbf{Z}/3\mathbf{Z}$. This shows that the polynomial Q cannot have an irreducible factor of degree 2 over $K(\sqrt{\Delta})$. Therefore, it is either split or irreducible over $K(\sqrt{\Delta})$. In this last case, the degree $[L : K]$ is divisible by 3 and by Cauchy's lemma (Proposition 4.2.3, but you might want to prove it by hand here), $\mathrm{Gal}(L/K)$ contains an element of order 3, hence a subgroup of order 3. But there are precisely four such subgroups in $\mathfrak{S}_4$, denoted $H_1, \ldots, H_4$, where H_i is generated by any 3-cycle which fixes i. (For example, H_1 is generated by the 3-cycle $(2,3,4)$.) If $g \in \mathfrak{S}_4$ maps i to j, then $gH_jg^{-1} = H_i$; since $\mathrm{Gal}(L/K)$ acts transitively on $\{1,2,3,4\}$, as soon as $\mathrm{Gal}(L/K)$ contains one of the H_i, it contains the other three, hence all 3-cycles, hence all of $\mathfrak{A}_4$. We just proved that if Q is irreducible over $K(\sqrt{\Delta})$, then $\mathrm{Gal}(L/K)$ contains $\mathfrak{A}_4$.

If moreover Δ is a square in K, one has $\mathrm{Gal}(L/K) \subset \mathfrak{A}_4$, whence the equality. If Δ is not a square in K, one has $\mathrm{Gal}(L/K) = \mathfrak{S}_4$.

Let us now assume that the resolvent polynomial Q is split in $K(\sqrt{\Delta})$, i.e. , assume that $K_1 = K(\sqrt{\Delta})$. Since P is irreducible, $[L : K]$ is a multiple of 4. Moreover, $[L : K]$ divides 8, hence one has $[L : K] = 4$ or 8.

If Δ is a square in K, one then has $K_1 = K$ and $\mathrm{Gal}(L/K) \subset V_4$. Since no proper subgroup of V_4 acts transitively on $\{1,2,3,4\}$, one necessarily has $\mathrm{Gal}(L/K) = V_4$ in this case.

If Δ is not a square in K, one has $[K_1 : K] = 2$. Therefore, $[L : K] = 4$ if L is generated by one of the square roots of the $-\theta_j$, and $[L : K] = 8$ otherwise. In the first case, $\mathrm{Gal}(L/K)$ is a transitive subgroup of order 4 in $\mathfrak{S}_4$, not contained in $\mathfrak{A}_4$, which leaves only the cyclic group generated by a circular permutation. In the other case, $\mathrm{Gal}(L/K)$ has 8 elements and is isomorphic to the dihedral group D_4. (Remark: it is one of the 2-Sylow subgroups of $\mathfrak{S}_4$, generated by a 4-cycle (a,b,c,d) and the transposition (a,c).)

5.6 Solving equations by radicals

In this section, I explain the relationship discovered by Galois between the possibility of solving a polynomial equation with radicals and the solvability of its Galois group. This relationship simultaneously generalizes the following results:

– Theorem 5.1.1 concerning constructibility with ruler and compass (on one hand, a group with cardinality a power of 2 is solvable, see Exercise 4.11; on the other hand, constructible numbers are contained in an extension obtained by successively adding square roots);

– the explicit solution of equations with degree 2, 3 or 4 which I explained in the previous section (as I said there, the groups $\mathfrak{S}_2$, $\mathfrak{S}_3$ and $\mathfrak{S}_4$, and their subgroups, are solvable);

– Abel's theorem (see Corollary 5.6.5 below) that the general equation of degree $n \geqslant 5$ is not solvable by radicals.

To simplify, we will only consider in this section fields of characteristic zero.

Definition 5.6.1. *Let E be a field with characteristic zero, and let $E \subset F$ be a finite extension.*

We will say that the extension $E \subset F$ is elementary radical *with exponent n, if there is some $x \in F$ such that $F = E[x]$ and $x^n \in E$.*

We will say that the extension $E \subset F$ is radical *if there are subfields $E = E_0 \subset E_1 \subset \cdots \subset E_n = F$ such that the extension $E_{i-1} \subset E_i$ is elementary radical for any $i \in \{1, \ldots, n\}$.*

Finally, we will say that the extension $E \subset F$ is solvable by radicals, *or simply* solvable, *if there is a finite extension $F \subset F'$ such that the extension $E \subset F'$ is a radical extension.*

Proposition 5.6.2. a) *Let $E \subset F$ be a finite extension and K be any field such that $E \subset K \subset F$. If the extension $E \subset F$ is radical, then the extension $K \subset F$ is itself radical. If the extension $E \subset F$ is solvable, then both extensions $E \subset K$ and $K \subset F$ are solvable.*

b) *Let $E \subset F_1$ and $E \subset F_2$ be two finite isomorphic extensions. If $E \subset F_1$ is a radical extension (*resp. *a solvable extension), then so is $E \subset F_2$.*

c) *Let Ω be a field containing E and let $E \subset F$ and $E \subset F'$ be two radical (*resp. *solvable) extensions contained in Ω. Then the composite extension $E \subset FF'$ is radical (*resp. *solvable).*

d) *Let $E \subset F$ a finite radical (*resp. *solvable) extension. Then its Galois closure (in any algebraic closure), $E \subset F^{\mathrm{g}}$, is again radical (*resp. *solvable).*

Proof. *a*) is obvious from the Definition.

b) Assume the extension $E \subset F_1$ to be radical. Let $E = E_0 \subset E_1 \subset \cdots \subset E_n = F_1$ be a chain of subfields such that the extension $E_{i-1} \subset E_i$ is elementary radical for any integer i. Let $\sigma\colon F_1 \to F_2$ be any E-isomorphism. For any i, the extension $\sigma(E_{i-1}) \subset \sigma(E_i)$ is elementary radical, for if $E_i = E_{i-1}(x_i)$, with $x_i^{n_i} \in E_{i-1}$, one has $\sigma(E_i) = \sigma(E_{i-1})(\sigma(x_i))$ and $\sigma(x_i)^{n_i} \in \sigma(E_{i-1})$. This shows that the extension $\sigma(E) \subset \sigma(F_1)$ is radical.

Now assume that the extension $E \subset F_1$ is solvable and let F_1' be some extension of F_1 such that the extension $E \subset F_1'$ is radical. Fix an algebraic closure Ω of F_2; by Theorem 3.1.6, there is a field homomorphism $\sigma'\colon F_1' \to \Omega$ such that $\sigma'|_{F_1} = \sigma$. Consequently, the extension $E \subset \sigma'(F_1')$ is radical, and the extension $E \subset F_2$ is solvable.

c) Let $E = E_0 \subset E_1 \subset \cdots \subset E_n = F$ and $E = E_0' \subset E_1' \subset \cdots \subset E_{n'}' = F'$ be two chains of fields, the extensions $E_{i-1} \subset E_i$ and $E_{i-1}' \subset E_i'$ being elementary radical. If y_i is an element in E_i' such that $E_i' = E_{i-1}'(y_i)$, a power of which belongs to E_{i-1}', then the extension $FE_{i-1}' \subset FE_i'$ is elementary radical, for $FE_i' = FE_{i-1}'(y_i)$. The chain of elementary radical extensions

$$E = E_0 \subset E_1 \subset \cdots \subset E_n = F \subset FE_1' \subset FE_2' \subset \cdots \subset FE_n' = FF'$$

shows that the extension $E \subset FF'$ is radical.

Assume that the two extensions $E \subset F$ and $E \subset F'$ are solvable, and let $F \subset L$ and $F' \subset L'$ be extensions such that $E \subset L$ and $E \subset L'$ are radical. By assumption, the fields F and F' are contained in Ω, which we can assume to be algebraically closed. (Otherwise, replace Ω by any algebraic closure.) Then there is an F-homomorphism $\sigma\colon L \to \Omega$ and a F'-homomorphism $\sigma'\colon L' \to \Omega$. By *b*), the extensions $E \subset \sigma(L)$ and $E \subset \sigma'(L')$ are radical, and so is the extension $E \subset \sigma(L)\sigma'(L')$. Since $E \subset FF' \subset \sigma(L)\sigma'(L')$, the extension $E \subset FF'$ is solvable.

d) Let Ω be an algebraic closure of F. The Galois closure of an extension $E \subset F$ is the subfield of Ω generated by all $\sigma(F)$, with σ running along the set of all E-homomorphisms from F to Ω. By b), each extension $E \subset \sigma(F)$ is radical (*resp.* solvable). An obvious induction using c) now shows that the extension $E \subset \prod_\sigma \sigma(F)$ is radical (*resp.* solvable). □

Theorem 5.6.3. *Let E be a field of characteristic zero. A Galois extension $E \subset F$ is solvable if and only if its Galois group* $\mathrm{Gal}(F/E)$ *is solvable.*

Before proving this very important theorem, it might be worth recalling the Galois theory of elementary radical extensions given by Theorem 5.4.1 and its converse, Theorem 5.4.2, showing that that Galois extensions with Galois group $\mathbf{Z}/n\mathbf{Z}$ are elementary radical, since we assumed that $\operatorname{card} \mu_n(E) = n$.

Proposition 5.6.4. *Let E be a field such that* $\operatorname{card} \mu_n(E) = n$.

Any elementary radical extension $E \subset F$ of exponent n, is Galois and $\mathrm{Gal}(F/E)$ *can be identified to a subgroup of* $\mathbf{Z}/n\mathbf{Z}$. *(It follows that there is an integer d dividing n such that* $\mathrm{Gal}(F/E) \simeq \mathbf{Z}/d\mathbf{Z}$.*)*

Conversely, any Galois extension $E \subset F$ with Galois group $\mathbf{Z}/n\mathbf{Z}$ is elementary radical, of exponent n.

The *Proof of Theorem 5.6.3* involves four steps.

a) Let the extension $E \subset F$ be radical, Galois, and assume that E contains a root of unity of order $[F : E]$. Then $\mathrm{Gal}(F/E)$ *is a solvable group.*

Let us show this by induction on the degree $[F : E]$. Let $E \subset E_1 \subset \cdots \subset F$ be a chain of (nontrivial) elementary radical extensions. Set $G = \mathrm{Gal}(F/E)$ and $H = \mathrm{Gal}(F/E_1)$. The extension $E_1 \subset F$ is radical and Galois. Since $[F : E_1]$ and $[E_1 : E]$ both divide $[F : E]$, E contains a primitive root of unity of both orders. By induction, the group H is solvable; by the preceding proposition, the extension $E \subset E_1$ is Galois and its Galois group is cyclic. Consequently, H is a normal subgroup of G and $G/H \simeq \mathrm{Gal}(E/E_1)$ is a cyclic finite group. It now follows from Proposition 4.5.2, c), that G is a solvable group.

b) Let $E \subset F$ be a solvable Galois extension, then $\mathrm{Gal}(F/E)$ *is a solvable group.*

Let $F \subset F_1$ be a finite extension such that the extension $E \subset F_1$ is a radical extension. Let Ω be an algebraic closure of K containing F_1 and let L denote the Galois closure of the extension $E \subset F_1$ in Ω. The extension $E \subset L$ is radical and Galois. Denote also by K the extension of E generated in Ω by a primitive root of unity of order $[L : E]$.

By Proposition 5.6.2, c), the extension $K \subset KL$ is radical and Galois. Since its degree $[KL : K]$ divides $[L : E]$, a) implies that $\mathrm{Gal}(KL/K)$ is a solvable group. On the other hand, the extension $E \subset K$ is Galois, and its Galois group is a subgroup of $(\mathbf{Z}/N\mathbf{Z})^*$, where $N = [L : E]$ (see Section 5.2). Therefore, $\mathrm{Gal}(KL/K)$ is a normal subgroup of $\mathrm{Gal}(KL/E)$ and the quotient $\mathrm{Gal}(KL/E)/\mathrm{Gal}(KL/K)$ is abelian, because it is isomorphic to $\mathrm{Gal}(K/E)$. Since $\mathrm{Gal}(KL/K)$ is solvable, it follows from Prop. 4.5.2, c), that the group $\mathrm{Gal}(KL/E)$ is solvable. Since $E \subset F$ is a Galois extension with $F \subset KL$, $\mathrm{Gal}(F/E)$ is a quotient of $\mathrm{Gal}(KL/E)$. This shows that $\mathrm{Gal}(F/E)$ is a solvable group.

c) If $\mathrm{Gal}(F/E)$ *is a solvable group, and if E contains a primitive root of unity of order $[F : E]$. Then the extension $E \subset F$ is radical.*

Let us show this by induction on $[F : E]$. The group $G = \mathrm{Gal}(F/E)$ is solvable. By Proposition 4.5.3, G has a normal subgroup H, such that G/H is cyclic. Consequently, there exists an integer $d > 1$ dividing $[F : E]$ such that G/H is isomorphic to $\mathbf{Z}/d\mathbf{Z}$. Therefore, the field extension $E \subset F^H$ is

Galois, and its Galois group is $\mathbf{Z}/d\mathbf{Z}$; by Proposition 5.6.4, this extension is elementary radical. (Observe that E contains a primitive dth root of unity.) The extension $F^H \subset F$ is Galois and its Galois group is equal to H, so is solvable (Proposition 4.5.2, a). Since $[F : F^H]$ divides $[F : E]$, F^H contains a primitive root of unity of order $[F : F^H]$. By induction, the extension $F^H \subset F$ is a radical extension. This shows that the extension $E \subset F$ is radical.

d) If $\mathrm{Gal}(F/E)$ *is a solvable group, the extension* $E \subset F$ *is solvable.*

Let Ω be an algebraic closure of F and let K be the field generated in Ω by a primitive root of unity of order $[F : E]$. The extension $E \subset K$ is radical, Galois, and its Galois group is abelian. The extension $K \subset KF$ is Galois, and its Galois group is solvable, for it is a subgroup of $\mathrm{Gal}(F/E)$. Since $[KF : K]$ divides $[KF : E]$, K contains a primitive root of unity of order $[KF : K]$, it follows from c) that the extension $K \subset KF$ is radical. Therefore, the extension $E \subset KF$ is radical and the extension $E \subset F$ is solvable. □

Solving the "general equation of degree n" over some field K means being able to give formulae for solving any equation of degree n with arbitrary unspecified coefficients. In more precise terms, we want to solve the equation

$$X^n + a_1 X^{n-1} + \cdots + a_n,$$

in which coefficients $a_1, \ldots, a_n$ are indeterminates. This is a polynomial equation over the field of rational functions $K(a_1, \ldots, a_n)$ in n indeterminates. By Exercise 3.11, its Galois group is equal to the full symmetric group $\mathfrak{S}_n$. Since this group is not solvable for $n \geqslant 5$ (Corollary 4.6.8), it follows from Theorem 5.6.3 that the general equation of degree n is not solvable by radicals, a result which had been first anticipated by the Italian mathematician P. Ruffini in 1799 and proved by N. Abel in 1826.

Corollary 5.6.5 (Abel). *Let K be a field. For $n \geqslant 5$, the general equation of degree n,*

$$X^n + a_1 X^{n-1} + \cdots + a_n = 0,$$

viewed as a polynomial equation over the field $K(a_1, \ldots, a_n)$ of rational functions in n indeterminates and coefficients in K, is not solvable by radicals.

You will find below, and also in some exercises, explicit examples of polynomial equations (over the field of rational numbers) which are not solvable by radicals.

5.7 How (not) to compute Galois groups

In many actual applications, one considers a separable polynomial P, irreducible or not, with coefficients in a field K, and a splitting extension $K \subset L$ of the polynomial P, so that L is generated over K by the roots $x_1, \dots, x_n$ of P in an algebraic closure of K. As in Section 3.3, the Galois group $G = \mathrm{Gal}(L/K)$ is naturally a subgroup of the group of permutations of $\{x_1, \dots, x_n\}$, hence can be identified with a subgroup of the symmetric group $\mathfrak{S}_n$.

The first result of this section shows that, provided one knows how to factor polynomials with many indeterminates and coefficients in K, then one can explicitly determine the group G.

The group $G = \mathrm{Gal}(L/K)$ acts on the ring $L[Y_1, \dots, Y_n]$ coefficientwise, hence also on the the field of rational functions $L(Y_1, \dots, Y_n)$, which is its field of fractions. It also acts on the ring of polynomials $L[X, Y_1, \dots, Y_n]$. To simplify notation, we will write $\boldsymbol{Y}$ as an abbreviation for $Y_1, \dots, Y_n$. For example, we write $L[\boldsymbol{Y}]$ for $L[Y_1, \dots, Y_n]$ and $L(\boldsymbol{Y})$ for $L(Y_1, \dots, Y_n)$.

For any $\sigma \in \mathfrak{S}_n$, we let

$$\xi_\sigma = x_1 Y_{\sigma(1)} + \cdots + x_n Y_{\sigma(n)} \in L[\boldsymbol{Y}].$$

Lemma 5.7.1. a) *For any element τ in the Galois group* $\mathrm{Gal}(L/K)$*, one has*

$$\tau(\xi_\sigma) = \xi_{\sigma\tau^{-1}}.$$

b) *The extension $K(\boldsymbol{Y}) \subset L(\boldsymbol{Y})$ is Galois, with Galois group G.*

c) *Moreover, $\xi = x_1 Y_1 + \cdots + x_n Y_n$ is a primitive element.*

Proof. For any $\tau \in G$, one has

$$\tau(\xi_\sigma) = \sum_{i=1}^{n} \tau(x_i) Y_{\sigma(i)} = \sum_{i=1}^{n} x_{\tau(i)} Y_{\sigma(i)} = \sum_{j=1}^{n} x_j Y_{\sigma(\tau^{-1}(j))} = \xi_{\sigma\tau^{-1}},$$

which proves *a*).

b) If $R = P/Q \in L(Y)$, one can write

$$R = \frac{P}{Q} \prod_{\tau \in G \setminus \{1\}} \frac{\tau(Q)}{\tau(Q)} = \frac{P \prod_{\tau \neq 1} \tau(Q)}{\prod_{\tau} \tau(Q)},$$

a new fraction whose denominator D belongs to $K[\boldsymbol{Y}]$ since it is clearly invariant under any $\tau \in G$. Let $N = RD$ be its numerator, then R is invariant under G if and only if N is. It follows that $L(\boldsymbol{Y})^G = K(\boldsymbol{Y})$, and by Artin's lemma (Prop. 3.2.8), the extension $K(\boldsymbol{Y}) \subset L(\boldsymbol{Y})$ is Galois, with Galois group G.

c) Let $\xi = \xi_{\mathrm{id}} = x_1Y_1 + \cdots + x_nY_n$. For any $\tau \in G$, $\tau(\xi) = \xi_{\tau^{-1}}$, so that $\tau = \mathrm{id}$ is the only element of G such that $\tau(\xi) = \xi$. This shows that the extension $K(\boldsymbol{Y}) \subset L(\boldsymbol{Y})$ is generated by ξ. □

It follows from the Lemma that the minimal polynomial of ξ over $K(\boldsymbol{Y})$ is equal to

$$M_\xi(T) = \prod_{\tau\in G}(T - \tau(\xi)) = \prod_{\tau\in G}(T - \xi_\tau).$$

It belongs to $K[\boldsymbol{Y}, T]$ and is irreducible in $K(\boldsymbol{Y})[T]$, hence is irreducible in $K[\boldsymbol{Y}, T]$ for the ring $K[\boldsymbol{Y}]$ is a unique factorization domain.

Theorem 5.7.2. *Let us define a polynomial in variables $X, Y_1, \ldots, Y_n$ by the formula*

$$\mathscr{R}_P(T) = \prod_{\sigma\in\mathfrak{S}_n}(T - \xi_\sigma) = \prod_{\sigma\in\mathfrak{S}_n}(T - (x_1Y_{\sigma(1)} + \cdots + x_nY_{\sigma(n)})).$$

This is a separable polynomial with coefficients in K.

Let M be the unique irreducible factor of $\mathscr{R}_P$ in $K(\boldsymbol{Y})[T]$ which is monic in T and divisible by $T - \xi$ in $L(\boldsymbol{Y})[T]$.

Then $M = M_\xi$ and a permutation $\sigma \in \mathfrak{S}_n$ belongs to G if and only if

$$M(T, Y_1, \ldots, Y_n) = M(T, Y_{\sigma(1)}, \ldots, Y_{\sigma(n)}).$$

Proof. Any $\tau \in G$ induces a permutation of the roots of $\mathscr{R}_P$, since $\tau(\xi_\sigma) = \xi_{\sigma\tau^{-1}}$, hence $\tau(\mathscr{R}_P) = \mathscr{R}_P$ for any $\tau \in \mathrm{Gal}(L/K)$ and the coefficients of $\mathscr{R}_P$ belong to K.

Since M and M_ξ have the common factor $X - \xi$ in $L(\boldsymbol{Y})[T]$, it follows from Corollary 2.4.3 that M and M_ξ have a common factor in $K(\boldsymbol{Y})[T]$. Being both monic and irreducible in $K(\boldsymbol{Y})[T]$, they are equal and

$$M(T, Y_1, \ldots, Y_n) = \prod_{\tau\in G}(T - (x_1Y_{\tau(1)} + \cdots + x_nY_{\tau(n)})).$$

Finally, for $\sigma \in \mathfrak{S}_n$, one has

$$\begin{aligned} M(T, Y_{\sigma(1)}, \ldots, Y_{\sigma(n)}) &= \prod_{\tau\in G}\big(X - x_1Y_{\tau(\sigma(1))} - \cdots - x_nY_{\tau(\sigma(n))}\big) \\ &= \prod_{\tau\in G\sigma}\big(X - x_1Y_{\tau(1)} - \cdots - x_nY_{\tau(n)}\big), \end{aligned}$$

so that

$$M(X, Y_{\sigma(1)}, \ldots, Y_{\sigma(n)}) = M(X, Y_1, \ldots, Y_n)$$

if and only if $G\sigma = G$, which means exactly that $\sigma \in G$. □

However nice it may look, this theorem is of almost no practical use. For example, if K is the field of rational numbers, the complexity of factoring multivariate polynomials of large degree ($\deg \mathscr{R}_P = n!$) is tremendous and this approach rapidly fails, even on the fastest available computing systems. We will still deduce from it a fundamental theoretical consequence concerning the behaviour of the Galois group of a polynomial by *specialization* of its coefficients, which is the subject of the next section.

Observe that the polynomial $\mathscr{R}_P$ defined in the theorem is symmetric in $Y_1, \dots, Y_n$, and is independent of the particular numbering of the roots. On the contrary, its irreducible factor M depends on the chosen numbering, as well as the Galois group, viewed as a subgroup of a symmetric group. Let us make this dependence explicit.

Let $P \in K[X]$ be a separable polynomial of degree n and let $K \to L$ be a splitting extension of P. Let R be the set of roots of P in L. A numbering of R is a bijection $\nu\colon \{1, \dots, n\} \xrightarrow{\sim} R$; it defines an embedding $\lambda_\nu\colon \mathrm{Gal}(L/K) \hookrightarrow \mathfrak{S}_n$ such that

$$\nu(\lambda_\nu(g)(i)) = g(\nu(i)), \quad g \in \mathrm{Gal}(L/K), \quad i \in \{1, \dots, n\}.$$

Denote its image by $G_\nu = \lambda_\nu(\mathrm{Gal}(L/K))$. Observe that the polynomial $\mathscr{R}_P$ satisfies

$$\begin{aligned}\mathscr{R}_P(T) &= \prod_{\sigma \in \mathfrak{S}_n} \big(T - (x_{\sigma^{-1}(1)}Y_1 + \cdots + x_{\sigma^{-1}(n)}Y_n)\big) \\ &= \prod_{\text{numberings } \nu} \big(T - (\nu(1)Y_1 + \cdots + \nu(n)Y_n)\big),\end{aligned}$$

the last product being over all numberings of the roots of P. Let $\mathscr{R}_{P,\nu}$ denote the minimal polynomial of $\xi = \nu(1)Y_1 + \cdots + \nu(n)Y_n$ introduced above, so that

$$\begin{aligned}\mathscr{R}_{P,\nu}(T, Y_1, \dots, Y_n) &= \prod_{\tau \in G} \big(T - (\tau(\nu(1))Y_1 + \cdots + \tau(\nu(n))Y_n)\big) \\ &= \prod_{\sigma \in G_\nu} \big(T - (\nu(\sigma(1))Y_1 + \cdots + \nu(\sigma(n))Y_n)\big).\end{aligned}$$

If μ is another numbering, there is a permutation $\sigma \in \mathfrak{S}_n$ such that $\mu(i) = \nu(\sigma(i))$ for any $i \in \{1, \dots, n\}$. Then either $\mathscr{R}_{P,\mu}$ and $\mathscr{R}_{P,\nu}$ are coprime, or they have a factor in common. In this case, they are necessarily equal since they both are irreducible and monic; moreover, one has $\sigma \in G_\nu$. This implies that $\mathscr{R}_P$ is the product of $\mathscr{R}_{P,\nu\circ\sigma}$, the σ being some representatives in $\mathfrak{S}_n$ of all left cosets of G_ν. The embeddings of the Galois group into $\mathfrak{S}_n$ defined by μ and ν satisfy the relation

$$\lambda_\mu(g) = \sigma^{-1}\lambda_\nu(g)\sigma.$$

In particular, $G_\mu = \sigma^{-1}G_\nu\sigma$ is conjugate to G_ν in $\mathfrak{S}_n$.

5.8 Specializing Galois groups

Before I give a general definition, let me explain two important examples:

a) Let P be a monic polynomial with integer coefficients, and let G denote the Galois group of a splitting extension of P over $\mathbf{Q}$. For any prime number p, one can reduce the polynomial P modulo p; hence one obtains a new Galois group G_p corresponding to a finite extension of $\mathbf{Z}/p\mathbf{Z}$.

b) Let $P \in \mathbf{Q}(t)[X]$ be a polynomial with coefficients in the field $\mathbf{Q}(t)$ of rational functions, denote by G the Galois group of a splitting extension of P over $\mathbf{Q}(t)$. For any rational number α which is not a pole of the coefficients of P, one can evaluate the polynomial P at $t = \alpha$, and obtain a polynomial $P_\alpha \in \mathbf{Q}[X]$, hence a Galois group G_α.

We will see that the Galois groups of these specialized equations are, in a quite natural way, *subgroups* of the group G.

Definition 5.8.1. *A* place *of the field K is a map $\varphi\colon K \to k \cup \{\infty\}$, where k is a field, which satisfies the following properties:*

a) *if $\varphi(x)$ and $\varphi(y)$ are not both ∞, then $\varphi(x+y) = \varphi(x)+\varphi(y)$, with the convention $a + \infty = \infty$ for $a \in k$;*

b) *if $\{\varphi(x), \varphi(y)\} \neq \{0, \infty\}$, then $\varphi(xy) = \varphi(x)\varphi(y)$, with the convention $a\infty = \infty$ for $a \neq 0$.*

Example 5.8.2. Let us go back to the two previous examples.

a) Let p be a prime number. Let $x = a/b$ be a rational number, written in smallest terms. If p divides b, let us set $\varphi_p(x) = \infty$. If p does not divide b, let $\varphi_p(x)$ be the quotient in $\mathbf{Z}/p\mathbf{Z}$ of the classes of a and b modulo p. This map $\varphi_p\colon \mathbf{Q} \to (\mathbf{Z}/p\mathbf{Z}) \cup \{\infty\}$ is a place.

b) Let $\alpha \in \mathbf{Q}$. A rational function has a "value" at α, which is set to ∞ if α is a pole. This map $\varphi_\alpha\colon \mathbf{Q}(t) \to \mathbf{Q} \cup \{\infty\}$ is a place.

If $\varphi\colon K \to k \cup \{\infty\}$ is a place, let $A = \varphi^{-1}(K)$ be the set of $x \in K$ such that $\varphi(x) \neq \infty$. The definition of a place implies at once that A is a subring of K, which we will call the *valuation ring of* φ. (*Exercise:* check it! See also Exercise 5.15.) In the two examples above, any ideal in A is generated by a power of p, or of $X - \alpha$, accordingly. In particular, *in these two cases, the ring A is a principal ideal ring.*

Let us fix a place $\varphi\colon K \to k \cup \{\infty\}$ of the field K. Let A denote the valuation ring of φ. Let $P \in K[X]$ be a monic polynomial of degree n. Assume that $P \in A[X]$, and that its discriminant $\Delta \in A$ satisfies $\varphi(\Delta) \neq 0$, so that the polynomial $\varphi(P) \in k[X]$ is separable. Let G be the Galois group of a splitting extension L of P over K, and let H be the Galois group of a splitting extension ℓ of the polynomial $\varphi(P)$ over k.

Lemma 5.8.3. *The polynomial $\mathscr{R}_P$ belongs to $A[T, \boldsymbol{Y}]$, and $\mathscr{R}_{\varphi(P)} = \varphi(\mathscr{R}_P)$.*

Proof. Let us first consider the polynomial

$$R = \prod_{\sigma \in \mathfrak{S}_n} (T - (\sum_{i=1}^{n} X_{\sigma(i)} Y_i)).$$

We view it as a polynomial in $T, Y_1, \dots, Y_n$ with coefficients in $\mathbf{Z}[X_1, \dots, X_n]$, writing

$$R = \sum_{I=(i_0,\dots,i_n)} R_I(X_1, \dots, X_n) Y^{i_0} Y_1^{i_1} \dots Y_n^{i_n}.$$

The polynomial R is symmetric in $X_1, \dots, X_n$, hence each of its coefficients R_I is symmetric too. Therefore, there is for each I a polynomial $\tilde{R}_I \in \mathbf{Z}[S_1, \dots, S_n]$ such that

$$R_I(X_1, \dots, X_n) = \tilde{R}_I(S_1(X), \dots, S_n(X)).$$

Let us write $P = X^n + a_1 X^{n-1} + \dots + a_n$ and let $x_1, \dots, x_n$ denote the roots of P in L, so that $a_j = (-1)^j S_j(x_1, \dots, x_n)$. It follows that

$$\mathscr{R}_P = \sum_I \tilde{R}_I(-a_1, \dots, (-1)^n a_n) T^{i_0} Y_1^{i_1} \dots Y_n^{i_n}.$$

Since the coefficients a_j belong to the subring A, $\mathscr{R}_P \in A[T, \boldsymbol{Y}]$.

Moreover, one has $\varphi(P) = X^n + \varphi(a_1) X^{n-1} + \dots + \varphi(a_n)$, and the same argument shows that

$$\tilde{R}_{\varphi(P)} = \sum_I \tilde{R}_I(-\varphi(a_1), \dots, (-1)^n \varphi(a_n)) T^{i_0} Y_1^{i_1} \dots Y_n^{i_n}.$$

Consequently,

$$\varphi(R_P) = \sum_I \varphi(\tilde{R}_I(-a_1, \dots, (-1)^n a_n)) T^{i_0} Y_1^{i_1} \dots Y_n^{i_n} = \tilde{R}_{\varphi(P)}$$

is the polynomial attached to $\varphi(P)$, which proves the lemma. □

Lemma 5.8.4. *For any numbering ν of the roots of P in L, the polynomial $\mathscr{R}_{P,\nu}$ belongs to $A[T, \boldsymbol{Y}]$.*

Proof. If the ring A is a unique factorization domain, e.g. , in the two examples above, it follows from Theorem 2.4.7 that the polynomial $\mathscr{R}_{P,\nu}$ belongs to $A[T, \boldsymbol{Y}]$. That remains true in the general case, for "a valuation ring is integrally closed," but we shall not prove it here; see Exercise 5.16. □

We saw that the irreducible factors in $k[T, \boldsymbol{Y}]$ of the polynomial $\mathscr{R}_{\varphi(P)}$ were of the form $\mathscr{R}_{\varphi(P),\mu}$ for μ a numbering of the roots of $\varphi(P)$ in ℓ. Now, since $\mathscr{R}_{P,\nu}$ divides $\mathscr{R}_P$, the preceding lemmas show that $\varphi(\mathscr{R}_{P,\nu})$ is a divisor of $\mathscr{R}_{\varphi(P)}$ in $k[T, \boldsymbol{Y}]$. We shall say that a numbering ν of the roots of P and a numbering μ of the roots of $\varphi(P)$ are *compatible* if $\mathscr{R}_{\varphi(P),\mu}$ divides $\varphi(\mathscr{R}_{P,\nu})$.

Theorem 5.8.5. *Fix a numbering ν of the roots of P, hence an embedding $\lambda_\nu \colon \mathrm{Gal}(L/K) \to \mathfrak{S}_n$ of image G_ν.*

a) *There exists a numbering μ of the roots of $\varphi(P)$ which is compatible with ν. It defines an embedding of the Galois group H into $\mathfrak{S}_n$; its image H_μ is a subgroup of G_ν.*

b) *Let μ' be any numbering of the roots of $\varphi(P)$, and let σ be the unique permutation $\in \mathfrak{S}_n$ such that $\mu'(i) = \mu(\sigma(i))$ for any $i \in \{1, \dots, n\}$. Then μ' is compatible with ν if and only if $\sigma \in G_\nu$. In that case, $H_{\mu'} = \sigma^{-1} H_\mu \sigma$ is conjugate to H_μ in G_ν.*

This shows that "the" Galois group H of the specialized equation $\varphi(P)$ is in an almost natural way a *subgroup* of the Galois group G of the equation P. Moreover, if the group G is abelian, or if the group H appears to be normal in G, then the Galois group of the specialized equation is a *canonical* subgroup of the Galois group.

Proof. The irreducible factors of the polynomial $\varphi(\mathscr{R}_{P,\nu}) \in k[T, \boldsymbol{Y}]$ divide $\mathscr{R}_{\varphi(P)}$, hence are of the form $\mathscr{R}_{\varphi(P),\mu}$ for some numberings μ of the roots of $\varphi(P)$ in ℓ. These numberings are precisely those which are compatible with ν.

More precisely, with N denoting the set of numberings of the roots of $\varphi(P)$ which are compatible with ν, one has the formula

$$\varphi(\mathscr{R}_{P,\nu}) = \prod_{\mu \in N} (T - (\mu(1)Y_1 + \cdots + \mu(n)Y_n))$$

in $\ell[T, \boldsymbol{Y}]$. Let $\sigma \in G_\nu$; then

$$\mathscr{R}_{P,\nu}(T, Y_{\sigma(1)}, \dots, Y_{\sigma(n)}) = \mathscr{R}_{P,\nu}(T, Y_1, \dots, Y_n),$$

hence, taking the images of both sides by φ,

$$\prod_{\mu \in N} (T - (\mu(1)Y_{\sigma(1)} + \cdots + \mu(n)Y_{\sigma(n)})) = \prod_{\mu \in N} (T - (\mu(1)Y_1 + \cdots + \mu(n)Y_n)).$$

Writing $\mu(i) = \mu \circ \sigma^{-1}(\sigma(i))$, we find that $N\sigma^{-1} = N$; in other words, $N = NG_\nu$ is a right coset modulo G_ν. Since the cardinality of N is that of G_ν, one has $N = \mu G_\nu$ for any $\mu \in N$.

Fix such a μ. The polynomial $\mathscr{R}_{\varphi(P),\mu}$ divides $\varphi(R_{P,\nu})$. Looking in $\ell[T, \boldsymbol{Y}]$, one sees that $\mu H_\mu \subset N = \mu G_\nu$. Consequently, $H_\mu \subset G_\nu$.

If μ' is another numbering, one has $\mu' = \mu \circ \sigma$ for some $\sigma \in \mathfrak{S}_n$. Moreover, μ' is compatible with ν if and only if $\mu' \in N$, hence if and only if $\sigma \in G_\nu$. For such a numbering μ', we saw that $H_{\mu'} = \sigma^{-1} H_\mu \sigma$. The subgroups $H_{\mu'}$ and H_μ are therefore conjugate in G_ν. □

Let me now show some examples of how this theorem can be used to specify the shape of the Galois group of a polynomial with rational coefficients. Recall a remark from the end of Section 3.5 on finite fields. We define the *shape* of a permutation of $\{1, \dots, n\}$ as the partition of n that it defines (see p. 93).

Lemma 5.8.6. *Let P be a monic separable polynomial with coefficients in a finite field k. Let us denote by $n_1, \dots, n_r$ the degrees of the irreducible factors of P in $k[X]$. Let $k \to \ell$ be a splitting extension of P; the Frobenius automorphism $F \in \mathrm{Gal}(\ell/k)$ induces a permutation of the roots of P in ℓ. This permutation has shape $(n_1, \dots, n_r)$.*

Recall also from Prop. 4.6.1 that the conjugacy class of this permutation is characterized by these integers $(n_1, \dots, n_r)$. Consequently, this lemma and Theorem 5.8.5 allow one to exhibit *conjugacy classes* of elements in the Galois group. In some cases, this is even enough to compute the Galois group!

Example 5.8.7. Let us begin with the polynomial $P = X^5 - X - 1$. Denote by G its Galois group over $\mathbf{Q}$, considered as a subgroup of the group of permutations of the 5 roots, identified with $\mathfrak{S}_5$.

Reducing the polynomial modulo 2, we see that it has no root in $\mathbf{F}_2$, but it has two in $\mathbf{F}_4$. Indeed, the g.c.d. of $X^5 - X - 1$ and $X^4 - X$ is equal to $X^2 - X - 1$ over $\mathbf{F}_2$, so that $P \pmod 2$ has a factor of degree 2, the other being necessarily of degree 3. In particular, $P \pmod 2$ is separable over $\mathbf{F}_2$ and its Galois group over $\mathbf{F}_2$ is generated by an element of $\mathfrak{S}_5$ of shape $(2, 3)$. By Theorem 5.8.5, G contains a permutation of this shape, hence its cube, which is a transposition.

Let us now reduce modulo 3. By computing the g.c.d. of $P \pmod 3$ and $X^3 - X$, *resp.* $X^9 - X$ (computer algebra systems can be of great use in such calculations...), we check that $P \pmod 3$ has no root in $\mathbf{F}_3$, nor in $\mathbf{F}_9$. (*Exercise:* do it also by hand, using, for example, the fact that for any element $x \in \mathbf{F}_9$, one has $x^4 \in \{0, \pm 1\}$.) It follows that $P \pmod 3$ is irreducible over $\mathbf{F}_3$. By Theorem 5.8.5, G contains a 5-cycle. Incidentally, this shows that the polynomial P is irreducible.

It now follows from Proposition 4.6.2 that G is equal to the full symmetric group $\mathfrak{S}_5$. By the way, this gives an explicit example of a polynomial with rational coefficients which cannot be solved by radicals, for its Galois group, being $\mathfrak{S}_5$, is not solvable.

Example 5.8.8. Let us show in a similar way that the Galois group G of the polynomial $P = X^5 + 20X - 16$ over $\mathbf{Q}$, viewed as a subgroup of $\mathfrak{S}_5$, is equal to the alternating group $\mathfrak{A}_5$. Modulo 2, one has $P \equiv X^5$, which is not separable. Let us thus look modulo 3. One has $P \equiv X^5 - X - 1 \pmod 3$; as we saw in the previous example, $P \pmod 3$ is irreducible. As above, the group G contains a 5-cycle.

Modulo 7, one has $P \equiv X^5 - X - 2$ and its roots in $\mathbf{F}_7$ are 2 and 3; moreover, one has

$$P \equiv (X-2)(X-3)(X^3 - 2X^2 - 2X + 2) \qquad (\text{mod } 7).$$

The polynomial $X^3 - 2X^2 - 2X + 2$ has no root in $\mathbf{F}_7$ (check it!), hence is irreducible since its degree is 3. It follows that G contains a 3-cycle.

Modulo 23, one gets a factorization of P as the product of a linear factor and two polynomials of degree 2, hence there is a permutation of the form $(1)(2,3)(4,5)$ — a double transposition — in G.

Considering other prime numbers does not seem to give new information on G. We already know that the order of G is a multiple of 2, 3 and 5, hence of their l.c.m. 60, and since it is a subgroup of $\mathfrak{S}_5$, its order divides by $5! = 120$.

We now have to use another piece of information. Observe that the discriminant of P is equal to

$$5^5 \times (-16)^4 + 4^4 \times 20^5 = 1024000000 = 2^{16}\, 5^6 = (2^8\, 5^3)^2$$

(see Exercise 3.22), so is a square in $\mathbf{Q}$. By Proposition 3.4.2, this implies that G is a subgroup of $\mathfrak{A}_5$. Since $\operatorname{card} \mathfrak{A}_5 = 60$, one necessarily has $G = \mathfrak{A}_5$.

In more complicated examples, these two ingredients, reduction modulo prime numbers and the consideration of the discriminant, are not enough and one is forced to use more general resolvent polynomials (see Section 3.4).

Example 5.8.9. Computer algebra systems like Magma, Pari/Gp or Maple can compute Galois groups for you, at least if the degree is not too big. For instance, here is the output of a (verbose) Maple session when asked to compute the Galois group of the polynomial $t^5 - 5t + 12$ over the rationals.

```
> infolevel[galois]:=2;
> galois(t^5-5*t+12);
galois:   Computing the Galois group of    t^5-5*t+12
```

```
galois/absres:   64000000 = ``(8000)^2
galois/absres:   Possible groups:   {"5T2", "5T1", "5T4"}
galois/absres:   p = 3    gives shape   2, 2, 1
galois/absres:   Removing   {"5T1"}
galois/absres:   Possible groups left:   {"5T2", "5T4"}
galois/absres:   p = 7    gives shape   5
galois/absres:   p = 11   gives shape   5
galois/absres:   p = 13   gives shape   5
galois/absres:   p = 17   gives shape   2, 2, 1
galois/absres:   p = 19   gives shape   5
galois/absres:   p = 23   gives shape   5
galois/absres:   p = 29   gives shape   2, 2, 1
galois/absres:   p = 31   gives shape   2, 2, 1
galois/absres:   p = 37   gives shape   5
galois/absres:   p = 41   gives shape   5
galois/absres:   The Galois group is probably one of   {"5T2"}
galois/respol:   Using the orbit-length partition of 2-sets.
galois/respol:   Calculating a resolvent polynomial...
galois/respol:   Factoring the resolvent polynomial...
galois/respol:   Orbit-length partition is   5, 5
galois/respol:   Removing   {"5T4"}
galois/respol:   Possible groups left:   {"5T2"}
        "5T2", {"5:2", "D(5)"}, "+", 10, {"(1 4)(2 3)", "(1 2 3 4 5)"}
```

To understand these lines, one needs to know that, up to conjugacy, there are only 5 transitive subgroups of $\mathfrak{S}_5$. These are

a) the cyclic group C_5, generated by the 5-cycle $(1, 2, 3, 4, 5)$, isomorphic to $\mathbf{Z}/5\mathbf{Z}$ and denoted in this context as `5T1`;

b) the dihedral group D_5, generated by $(1, 2, 3, 4, 5)$ and $(2, 5)(3, 4)$, denoted as `5T2`;

c) the metacyclic group M_{20}, defined as the normalizer `5T3` of C_5 in $\mathfrak{S}_5$, of cardinality 20, also isomorphic to the group of all maps $\mathbf{F}_5 \to \mathbf{F}_5$ of the form $x \mapsto ax + b$ with $a \in \mathbf{F}_5^*$ and $b \in \mathbf{F}_5$;

d) the alternating group $\mathfrak{A}_5$, of cardinality 60 and denoted `5T4`;

e) the full symmetric group $\mathfrak{S}_5$, denoted `5T5`.

(In fact, all practical algorithms for computing Galois groups require the list of all transitive subgroups of $\mathfrak{S}_n$, which is known up to $n = 31$. The notations `5T1`, etc. come from this classification.)

First, the discriminant is computed. It is a square, $(64,000,000 = (8000)^2)$, hence the group must be a subgroup of the alternating group, which excludes M_{20} and $\mathfrak{S}_5$ (respectively `5T3` and `5T5`). Then, the program reduces our polynomial modulo small prime numbers and computes its factorization over the corresponding finite field, hence the shape of some permutation be-

longing to the Galois group; then, for any group which has not yet been excluded, the program simply checks whether it contains such a permutation. In fact, all nontrivial elements of the group generated by a 5-cycle are 5-cycles themselves, so that the group C_5 (5T1) is eliminated at once by reducing modulo $p = 3$. However, no new information is obtained in this way by reducing modulo prime numbers $\leqslant 41$.

Then, MAPLE indicates that the group would probably be equal to D_5 (5T2). Indeed, by Chebotarëv's density theorem, a profound and difficult theorem from algebraic number theory, all possible conjugacy classes of elements in the Galois group will appear by reducing modulo larger and larger prime numbers, and they will appear "in proportion" to their cardinalities. In fact, the shape of a permutation detects only its conjugacy class in the symmetric group, so that an easier result, due to Frobenius, is sufficient for our purposes. The number of permutations of a given shape in each group is given in Table 5.1. In our example, the shapes that appear are $(2, 2)$, 4 times, and (5), 7 times. If the group had been $\mathfrak{A}_5$ (5T4), the shape (3) would probably have already appeared, therefore MAPLE suggests that the group is D_5.

	C_5 (5T1)	D_5 (5T2)	M_{20} (5T3)	$\mathfrak{A}_5$ (5T4)	$\mathfrak{S}_5$ (5T5)
1,1,1,1,1	1	1	1	1	1
2,1,1,1					10
3,1,1				20	20
2,2,1		5	5	15	15
4,1			10		30
3,2					20
5	4	4	4	24	24
total	5	10	20	60	120

Table 5.1. Number of permutations inducing a given partition in subgroups of $\mathfrak{S}_5$

Since D_5 is a subgroup of $\mathfrak{A}_5$, it remains to check whether G is, up to conjugacy, a subgroup of D_5. This requires a resolvent polynomial like

$$X_1X_2 + X_2X_3 + X_3X_4 + X_4X_5 + X_5X_1,$$

whose stabilizer is exactly D_5. (Can you see why? Remember that D_5 is the symmetry group of the regular pentagon.) Computing the complex roots of the polynomial $t^5 - 5t + 12$ with large accuracy, one can evaluate the above resolvent polynomial at all permutations of the roots. Some of these evaluations are integers and Prop. 3.4.5 implies that the Galois group is equal to D_5. In fact, a floating point calculation does not really *prove* that the

numbers obtained are integers, only that they are up to the given precision. However, using results such as Liouville's theorem (Exercise 1.2), one can prove that the numbers obtained are actually integers.

5.9 Hilbert's irreducibility theorem

This section explains some facts concerning the variation of the Galois group of a polynomial equation depending on a parameter. Any of the three theorems below constitute what is generally known as Hilbert's irreducibility theorem.

Let us consider a monic polynomial P with coefficients in the field $\mathbf{Q}(T)$ of rational functions. Let us assume that P is irreducible as a polynomial in $\mathbf{Q}(T)[X]$. We will first show that for "many" values $t \in \mathbf{Z}$, the polynomial $P(t, X) \in \mathbf{Q}[X]$ has no root in $\mathbf{Q}$. We will then show that in fact, for "many" integers t, the polynomial $P(t, X)$ is even irreducible. Recall from Theorem 5.8.5 that, essentially, the Galois group over $\mathbf{Q}$ of the polynomial $P(t, X)$ is a subgroup of the Galois group over $\mathbf{Q}(T)$ of the polynomial $P(T, X)$. The last result, Theorem 5.9.7, claims that for "many" integers t, these two groups are in fact *equal!*

This is a theorem in *arithmetic*, as opposed to algebra, and it relies on properties of the field $\mathbf{Q}$ of rational numbers. It is obviously false if one replaces $\mathbf{Q}(T)$ by $\mathbf{C}(T)$ in its statement: there are irreducible polynomials $P \in \mathbf{C}(T)[X]$ of any degree but for any t, the polynomial $P(t, X)$ is split in $\mathbf{C}$, for the field of complex numbers is algebraically closed. The Galois group of the specialized equation is therefore trivial.

The heart of the arithmetic arguments will be in the proof of Prop. 5.9.1, at the point when we bound from below by 1 the absolute value of a nonzero integer. Remark that such a lower bound was also the crucial point in the proof that e and π are transcendental numbers (Theorems 1.6.3 and 1.6.6). However, the arguments we will use to prove Theorems 5.9.4, 5.9.6 and 5.9.7 from that proposition are essentially of algebraic nature.

Proposition 5.9.1. *Let e be any positive integer and let $\varphi = \sum_{n \geqslant -n_0} a_n u^{-n/e}$ be a Laurent series in the variable $u^{-1/e}$ which is not a polynomial in u. (In other words, there is a nonzero coefficient a_n such that either $n > 0$ or e does not divide n.) Assume that $\varphi(u)$ converges for $|u| \geqslant B_0$. Denote by $N(B)$ the number of integers $u \in [B_0, B]$ such that $\varphi(u) \in \mathbf{Z}$. Then, there exists a real number $\alpha < 1$ such that $N(B)/B^\alpha$ remains bounded when $B \to \infty$.*

From now on, we shall use the big-O notation and write $N(B) = \mathrm{O}(B^\alpha)$ to mean that $N(B)/B^\alpha$ remains bounded when $B \to \infty$.

Proof. It suffices to separately consider the real and imaginary parts of φ, for at least one of them is not a polynomial. We will therefore assume that φ has real coefficients. Observe that φ defines a $\mathscr{C}^\infty$ function from the interval $(B_0, +\infty)$ to $\mathbf{R}$, its derivatives of any order being obtained by deriving the series term by term. Hence, for $m > n_0/e$, $\varphi^{(m)}(u)$ decreases to 0 when $u \to +\infty$ Since φ is not a polynomial, $\varphi^{(m)}$ is not the zero-function and, when $u \to \infty$, $\varphi^{(m)}(u)$ is then equivalent to its first term, which is of the form $cu^{-\mu}$ for some real number $c \neq 0$ and some positive real number μ. In particular, for u large enough, say $u \geqslant B_1$, one has an inequality $c_1 u^{-\mu} \leqslant \left|\varphi^{(m)}(u)\right| \leqslant c_2 u^{-\mu}$.

Let S denote the set of integers $\geqslant B_0$ such that $\varphi(u) \in \mathbf{Z}$. Consider $m+1$ elements in S, $u_0 < \cdots < u_m$, with $u_0 > B_1$ and let us introduce the determinant

$$D = \begin{vmatrix} 1 & \dots & 1 \\ u_0 & \dots & u_m \\ \vdots & & \vdots \\ u_0^{m-1} & \dots & u_m^m \\ \varphi(u_0) & \dots & \varphi(u_m) \end{vmatrix}.$$

This determinant is an integer, for it is the determinant of a matrix with integer coefficients. By Lemma 5.9.3 below, there exists a real number $\xi \in (u_0, u_m)$ such that

$$D = \frac{1}{m!}\varphi^{(m)}(\xi)\prod_{i>j}(u_i - u_j).$$

Since $u_0 \geqslant B_1$, $\varphi^{(m)}(\xi) \neq 0$; in particular $D \neq 0$. Since D is an integer, one has $|D| \geqslant 1$, hence a lower bound

$$\prod_{i>j}(u_i - u_j) \geqslant \frac{m!}{\left|\varphi^{(m)}(\xi)\right|} \geqslant \frac{m!}{c_2}\xi^\mu,$$

and, *a fortiori*,

$$(u_m - u_0)^{m(m+1)/2} \geqslant \frac{m!}{c_2}u_0^\mu.$$

We thus have shown the existence of positive real numbers b and β such that, for any $m+1$ elements $u_0 < \cdots < u_m$ in S with $u_0 > B_1$, one has

$$u_m \geqslant u_0 + bu_0^\beta. \tag{5.9.2}$$

Now we set $\alpha = 1/(1+\beta)$ and we split the interval $[B_0, B]$ as $[B_0, B^\alpha] \cup [B^\alpha, B]$. The interval $[B_0, B^\alpha]$ contains at most B^α elements of S. For B large enough, $B^\alpha \geqslant B_1$ and the lower bound (5.9.2) implies that the interval $[B^\alpha, B]$ contains at most $(m/b)B^{1-\alpha\beta} = (m/b)B^\alpha$ elements of S. Finally, for $B \geqslant B_1^{1/\alpha}$, $N(B) \leqslant (1 + m/b)B^\alpha$, as we had to prove. □

Lemma 5.9.3. *Let I be an interval in $\mathbf{R}$, and $f\colon I \to \mathbf{R}$ a function with $\mathscr{C}^n$-regularity. Let $x_0, \dots, x_n$ be elements in I. Then, there is $\xi \in I$ such that*

$$\begin{vmatrix} 1 & \dots & 1 \\ x_0 & \dots & x_n \\ \vdots & & \vdots \\ x_0^{n-1} & \dots & x_n^{n-1} \\ f(x_0) & \dots & f(x_n) \end{vmatrix} = \frac{f^{(n)}(\xi)}{n!} \prod_{i>j} (x_i - x_j).$$

Proof. It suffices to consider the case where all x_i are distinct. Let us consider x_0 as a parameter and denote by $D(x_0)$ the determinant above. For $A \in \mathbf{R}$, let $F_A\colon I \to \mathbf{R}$ be the function defined by $F_A(x) = D(x) - A \prod_{i=1}^{n} (x - x_i)$. This function F_A vanishes at $x_1, \dots, x_n$; let us choose A so that it vanishes at $x = x_0$ too.

By Rolle's Lemma, the derivative of F_A vanishes at n distinct points on I, then its second derivative $(n-1)$ times, and so on. Finally, there is at least one $\xi \in I$ such that $F_A^{(n)}(\xi) = 0$. Moreover,

$$\begin{aligned} F_A^{(n)}(\xi) = D^{(n)}(\xi) - An! &= \begin{vmatrix} 0 & 1 & \dots & 1 \\ x_0 & \dots & x_n & \\ \vdots & \vdots & & \vdots \\ 0 & x_1^{n-1} & \dots & x_n^{n-1} \\ f^{(n)}(\xi) & f(x_1) & \dots & f(x_n) \end{vmatrix} - An! \\ &= (-1)^n f^{(n)}(\xi) \begin{vmatrix} 1 & \dots & 1 \\ x_0 & \dots & x_n \\ \vdots & & \vdots \\ x_1^{n-1} & \dots & x_n^{n-1} \end{vmatrix} - An!, \end{aligned}$$

hence $A = (-1)^n \dfrac{f^{(n)}(\xi)}{n!} \prod\limits_{i>j\geqslant 1} (x_i - x_j)$ and

$$D(x_0) = A \prod_{i=1}^{n} (x_0 - x_i) = \frac{f^{(n)}(\xi)}{n!} \prod_{i>j} (x_i - x_j).$$

This proves the lemma. □

Theorem 5.9.4. *Let P be a monic polynomial in $\mathbf{Q}(T)[X]$. Let $N(B)$ denote the number of integers $t \in [0, B]$ such that $P(t, X)$ has a root in $\mathbf{Q}$. If P has no root in $\mathbf{Q}(T)$, then there is a real number $\alpha < 1$ such that, when $B \to \infty$, $N(B) = \mathrm{O}(B^\alpha)$.*

Lemma 5.9.5. *Let n denote the degree of P. There exist an integer $e \geqslant 1$, Laurent series $x_1, \ldots, x_n$ with complex coefficients, and a nonzero radius of convergence, such that for any complex number t of large enough modulus, the n complex roots of $P(t^e, X)$ are the $x_j(1/t)$, for $1 \leqslant j \leqslant n$.*

Proof. Since we look at the roots of $P(t, X)$ for t large, let us make a change of variables $t = 1/u$. Let R denote a common denominator to the coefficients of the polynomial $P(1/U, X) \in \mathbf{Q}(U)[X]$, so that $R(U)P(1/U, X) \in \mathbf{Q}[U, X]$. Multiplying by $R(U)^{n-1}$, we can then find a polynomial $Q \in \mathbf{Q}[U, Y]$, monic and of degree n with respect to Y, such that $P(1/U, X)R(U)^n = Q(U, R(U)X)$. By Puiseux's theorem (Theorem 2.6.1), there are power series $y_1, \ldots, y_n$ with positive radius of convergence, and an integer $e \geqslant 1$ such that, for $|u|$ small enough, the roots of the polynomial $Q(u^e, Y)$ are the $y_j(u)$, for $1 \leqslant j \leqslant n$. Let us set $x_j(u) = R(u)^{-e}y_j(u)$. Expanding $R(u)^{-e}$ as a Laurent series around $u = 0$, one sees that the x_j are Laurent series, converging for $|u|$ small enough, but $u \neq 0$. Making the change of variables $t = 1/u$ again, the $x_j(1/t)$ are the roots of $P(t^e, X)$ provided $|t|$ is large enough. □

Proof of Theorem 5.9.4. Let $D \in \mathbf{Z}[T]$ be a common denominator of the coefficients of P, so that $P(T, X)D(T) \in \mathbf{Z}[T, X]$. There is a polynomial $Q \in \mathbf{Z}[T, X]$, monic as a polynomial in X, such that $P(T, X)D(T)^n = Q(T, D(T)X)$. The polynomial Q has no root in $\mathbf{Q}(T)$ (if $R(T)$ were a root of Q in $\mathbf{Q}(T)$, then $R(T)/D(T)$ would be a root of P in $\mathbf{Q}(T)$). Similarly, if $D(t) \neq 0$, then the polynomial $P(t, X) \in \mathbf{Z}[X]$ has a root in $\mathbf{Q}$ if and only if $Q(t, X)$ has a root in $\mathbf{Q}$. Therefore, it suffices to prove the theorem for the polynomial Q, which allows us to assume that $P \in \mathbf{Z}[T, X]$. Then, for any $t \in \mathbf{Z}$, the polynomial $P(t, X)$ is monic with integer coefficients. By Exercise 1.5, its roots in $\mathbf{Q}$ are necessarily integers.

Let $x_1, \ldots, x_n$ be the series given by Lemma 5.9.5. Since P has no root in $\mathbf{Q}(T)$, none of these series is a polynomial. It is now enough to apply Proposition 5.9.1 to each of them and to add up the upper bounds obtained, so that we get the desired upper bound for $N(B)$. □

Theorem 5.9.6. *Let $P \in \mathbf{Q}(T)[X]$ be any monic irreducible polynomial with coefficients in $\mathbf{Q}(T)$. Let $N(B)$ denote the cardinality of the set of integers $t \in [0, B]$ such that t is not a pole of any coefficient of P and such that $P(t, X)$ is reducible in $\mathbf{Q}[X]$. Then there exists $\alpha < 1$ such that $N(B) = \mathrm{O}(B^\alpha)$.*

Proof. As in the proof of the preceding theorem, we assume that P belongs to $\mathbf{Z}[T, X]$. Let $x_1, \ldots, x_n$ be the Laurent series given by Lemma 5.9.5. If t is large enough, say $t \geqslant B_0$, any monic factor of $P(t, X) \in \mathbf{Z}[X]$ has the form

$$P_I(t) = \prod_{i \in I}(X - x_i(t^{-1/e})),$$

where I is a subset of $\{1, \dots, n\}$. If $I \neq \emptyset$ and $I \neq \{1, \dots, n\}$, it is thus enough to show that the set of all integers $t \in [B_0, B]$ such that $P_I(t)$ belongs to $\mathbf{Z}[X]$ has cardinality $\mathrm{O}(B^\alpha)$.

But we may view the polynomial P_I as a polynomial with coefficients in the field K of converging Laurent series in a variable $T^{-1/e}$, and P_I is a factor of P in $K[X]$. Since P is irreducible in $\mathbf{Q}[T, X]$, the polynomial P_I does not belong to $\mathbf{Q}(T)[X]$ and at least one of its coefficients, say φ_I, is not a polynomial in T. Proposition 5.9.1 then implies that the set of all integers $t \in [B_0, B]$ such that $\varphi_I(t)$ is an integer has cardinality $\mathrm{O}(B^\alpha)$ for some $\alpha < 1$. The theorem is then proved. □

More generally, the following theorem says that the Galois group over $\mathbf{Q}$ of the polynomial $P(t, X)$, with $t \in \mathbf{Z}$, quite often coincides with the Galois group over $\mathbf{Q}(T)$ of the polynomial $P(T, X)$.

Theorem 5.9.7. *Let $P \in \mathbf{Q}(T)[X]$ be a monic polynomial with coefficients in $\mathbf{Q}(T)$. Let G denote its Galois group over $\mathbf{Q}(T)$. Let $N(B)$ be the cardinality of the set of all integers $t \in [0, B]$ such that either t is a pole of $P(T, X)$ or the Galois group of the polynomial $P(t, X)$ over $\mathbf{Q}$ is not isomorphic to G. Then, there exists $\alpha < 1$ such that $N(B) = \mathrm{O}(B^\alpha)$.*

Proof. As in the proof of Theorem 5.9.7, we assume that the coefficients of P are polynomials in T. Let us denote by n the degree of P in the variable X. Let $\mathbf{Q}(T) \to K$ be a splitting extension of the polynomial P and let $\kappa \in K$ be any primitive element. If $N = \operatorname{card} G$, then $N = [K : \mathbf{Q}(T)]$, and N is the degree of the minimal polynomial Q of κ over $\mathbf{Q}(T)$. The coefficients of Q are a priori rational functions in T. However, denoting by $D \in \mathbf{Q}[T]$ a common denominator of its coefficients, the minimal polynomial of $D(T)\kappa$ is equal to the polynomial $D(T)^N Q(T, D(T)^{-1}X)$ and therefore belongs to $\mathbf{Q}[T, X]$. This allows us to assume that $Q \in \mathbf{Q}[T, X]$.

Over $\mathbf{Q}(T)$, the polynomials P and Q have a common splitting extension, hence have the same Galois group, even if, as permutation groups, they look distinct (they do not act on the same set).

By the following lemma, there is a finite subset $S \subset \mathbf{Q}$ such that for any $t \notin S$, the polynomials $Q(t, X)$ and $P(t, X)$ are separable and have a common splitting extension $\mathbf{Q} \subset K_t$. By Theorem 5.8.5, the Galois group $\mathrm{Gal}(K_t/\mathbf{Q})$ can be considered as a subgroup of the Galois group $\mathrm{Gal}(K/\mathbf{Q}(T))$, so that $[K_t : \mathbf{Q}] \leqslant [K : \mathbf{Q}(T)] = N$. By Theorem 5.9.6 applied to the polynomial Q, there exists $\alpha < 1$ such that the number $N(B)$ of all integers $t \in [0, B]$ such that $t \notin S$ and such that $Q(t, X)$ is irreducible in $\mathbf{Q}[X]$, satisfies $N(B) = \mathrm{O}(B^\alpha)$. For such t, $[K_t : \mathbf{Q}] \geqslant N$, so that one has $[K_t : \mathbf{Q}] = N$ and $\mathrm{Gal}(K_t/\mathbf{Q})$ is isomorphic to $\mathrm{Gal}(K/\mathbf{Q}(T))$. □

Lemma 5.9.8. *Let $P \in \mathbf{Q}(T)[X]$ be a monic polynomial, let $\mathbf{Q}(T) \subset K$ be a splitting extension of P. Let $y \in K$ be a primitive element and denote by $Q \in \mathbf{Q}(T)[X]$ its minimal polynomial. There exists a finite subset $\Sigma \subset \mathbf{Q}$ such that for any $t \notin \Sigma$, the polynomials $Q(t, X)$ and $P(t, X)$ are separable and have a common splitting extension.*

Proof. Let us denote by $x_1, \ldots, x_n$ the roots of P in K. One can find polynomials $A_i \in \mathbf{Q}(T)[Y]$ such that for any i, $x_i = A_i(y)$, in other words,

$$P(T, X) = \prod_{i=1}^{n} (X - A_i(T, y)).$$

Replacing y by a formal variable Y, this implies that $Q(T, Y)$ divides the coefficients of the polynomial

$$P(T, X) - \prod_{i=1}^{n} (X - A_i(T, Y)),$$

for these coefficients vanish at y and Q is the minimal polynomial of y. Therefore, there is a polynomial $R \in \mathbf{Q}(T)[X, Y]$ such that

$$P(T, X) = \prod_{i=1}^{n} (X - A_i(T, Y)) + R(T, X, Y)Q(T, Y). \tag{5.9.9}$$

Similarly, there exists a polynomial $B \in \mathbf{Q}(T)[X_1, \ldots, X_n]$ such that $y = B(T, x_1, \ldots, x_n)$ and, again, $Q(T, Y)$ divides the coefficients of the polynomial $Y - B(T, A_1(Y), \ldots, A_n(Y))$, hence there is a polynomial $S \in \mathbf{Q}(T)[Y]$ such that

$$Y = B(T, A_1(T, Y), \ldots, A_n(T, Y)) + S(T, Y)Q(T, Y). \tag{5.9.10}$$

Finally, the polynomial Q is split in K. We thus can find polynomials $C_i \in \mathbf{Q}(T)[Y]$ satisfying

$$Q(T, X) = \prod_{i=1}^{N} (X - C_i(T, y)).$$

As before, it follows that there is a polynomial $U \in \mathbf{Q}(T)[X, Y]$ such that

$$Q(T, X) = \prod_{i=1}^{N} (X - C_i(T, Y)) + U(T, X, Y)Q(T, Y). \tag{5.9.11}$$

The coefficients of the polynomials $P, Q, A_1, \ldots, A_n, B, C_1, \ldots, C_N, R, S$ belong to $\mathbf{Q}(T)$. Let Σ denote the set of all $t \in \mathbf{Q}$ such that either t is a pole of one of these coefficients, or such that the discriminant of P or Q vanishes

at t. By assumption, for any $t \notin \Sigma$, the polynomials $P(t, X)$ and $Q(t, X)$ are separable and the preceding relations hold when evaluated at $T = t$.

Let $t \in \mathbf{Q} \setminus \Sigma$. To prove the lemma, it now suffices to show that the polynomial $P(t, X)$ is split in any extension where $Q(t, X)$ is split, and conversely.

Thus let L be an a extension of $\mathbf{Q}$ in which $Q(t, X)$ has a root η. For any $i \in \{1, \ldots, n\}$, let us set $\xi_i = A_i(t, \eta)$. Relation (5.9.9) shows that $P(t, X) = \prod_{i=1}^{n} (X - \xi_i)$, hence $P(t, X)$ is split in L.

Conversely, let L be any extension of $\mathbf{Q}$ in which $P(t, X)$ is split. Denote its roots by $\xi_1, \ldots, \xi_n$. Let η be a root of $Q(t, X)$ in some extension L' of L. The roots of P in L' are then given by the $A_i(t, \eta)$, for $1 \leqslant i \leqslant n$, so that there is a permutation $\sigma \in \mathfrak{S}_n$ with $A_i(t, \eta) = \xi_{\sigma(i)}$ for all i. The relation (5.9.10) implies that

$$\eta = B(t, \xi_{\sigma(1)}, \ldots, \xi_{\sigma(n)}).$$

It follows that $\eta \in L$ and that $Q(t, X)$ has a root in L.

Now, relation (5.9.11) implies that $Q(t, X) = \prod_{i=1}^{N} (X - C_i(t, \eta))$ is split in L. □

Exercises

Exercise 5.1. **a)** Let G be a finite group and let H be a subgroup of G such that $(G : H) = 2$. Show that H is normal in G.

b) How does this relate to Lemma 5.1.3?

c) More generally, if $(G : H)$ is equal to the smallest prime number dividing card G, show that H is normal in G.

Exercise 5.2. Let $K \subset E$ and $K \subset F$ be two finite extensions with coprime degrees, contained in a common extension Ω of K. Show that $E \cap F = K$ and that $[EF : K] = [E : K][F : K]$.

Exercise 5.3. Let α and β be two distinct complex roots of the polynomial $X^3 - 2$. Let $E = \mathbf{Q}(\alpha)$, $F = \mathbf{Q}(\beta)$.

a) Show that the composite extension $\mathbf{Q} \subset EF$ is a splitting extension of the polynomial $X^3 - 2$ over $\mathbf{Q}$.

b) Show that $E \cap F = \mathbf{Q}$, although $[EF : \mathbf{Q}] \neq [F : \mathbf{Q}]\,[E : \mathbf{Q}]$. (This shows that one cannot remove the hypothesis that one of the extensions E or F is Galois in Corollary 5.3.3.)

Exercise 5.4. This is a sequel to Exercise 1.13, where we showed that the two real roots of the polynomial $P = X^4 - X - 1$ cannot be both constructible with ruler and compass.

a) Show that in fact no root of P is constructible with ruler and compass.

b) What is the Galois group of the extension generated by the complex roots of P?

Exercise 5.5. Let p be a prime number and let $P \in \mathbf{Q}[X]$ be any irreducible polynomial of degree p which has 2 conjugate complex roots, x_1, x_2, and $p-2$ real roots, $x_3, \ldots, x_p$. Let us denote by $K = \mathbf{Q}(x_1, \ldots, x_p)$ the subfield of $\mathbf{C}$ generated by the roots of P. We identify $\mathrm{Gal}(K/\mathbf{Q})$ with a subgroup of $\mathfrak{S}_p$.

a) Show that the transposition $\tau = (1, 2)$ belongs to $\mathrm{Gal}(K/\mathbf{Q})$. (Think about the complex conjugation.)

b) Show that $\mathrm{Gal}(K/\mathbf{Q})$ contains a p-cycle σ.

c) Show that σ and τ generate $\mathfrak{S}_p$. Conclude that $\mathrm{Gal}(K/\mathbf{Q}) = \mathfrak{S}_p$.

d) *Application*: $P = X^5 - 6X + 3$. (To prove that P is irreducible, use Exercise 1.10 or reduce mod 5.)

Exercise 5.6 (Artin-Schreier's theory). Let p be a prime number. Let K be a field of characteristic p and let $a \in K$. We assume that the polynomial $P = X^p - X - a$ has no root in K. Let $K \subset L$ be any splitting extension of P.

a) If x is a root of P in L, show that the roots of P are $x, x+1, x+2, \ldots, x+p-1$. In particular, P is separable.

b) Show that P is irreducible in $K[X]$. (If a degree d polynomial Q divides P, look at the term of degree $d-1$ in Q.)

c) (Another proof that P is irreducible.) Let $x + u$ (for $1 \leqslant u < p$) be another root of the minimal polynomial of x over K. Show that there is $\tau \in \mathrm{Gal}(L/K)$ with $\tau(x) = x + u$. Deduce from this that there is some $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(x) = x + 1$, hence that all roots of P are conjugates of x. Conclude.

d) Show that $L = K[x]$ and that $\mathrm{Gal}(L/K) \simeq \mathbf{Z}/p\mathbf{Z}$.

Exercise 5.7 (Cyclic extensions of degree p in characteristic p). Let K be a field of characteristic $p > 0$, and let $K \subset L$ be a finite Galois extension with Galois group $\mathbf{Z}/p\mathbf{Z}$. Let σ be a generator of $\mathrm{Gal}(L/K)$.

a) Show the existence of $t \in L$ such that $\sum_{i=0}^{p-1} \sigma^i(t) = 1$.

Then, set $x = \sum_{i=0}^{p-1} i\sigma^i(t)$.

b) Compute $\sigma(x)$. Show that $x \notin K$ but that $a = x^p - x$ belongs to K.

c) Show that $L = K[x]$ and that $X^p - X - a$ is the minimal polynomial of x over K.

Exercise 5.8. In this exercise, we will determine the Galois group over $\mathbf{Q}$ of the polynomial $P = X^7 - X - 1$, using reduction modulo primes.

a) Show that P has no root in the finite field $\mathbf{F}_8$. Deduce that it is irreducible, when viewed as a polynomial over $\mathbf{F}_2$.

b) Show that the only roots of P in $\mathbf{F}_9$ are the roots of the polynomial X^2+X-1, and that they are simple. Conclude that over $\mathbf{F}_3$, P splits as the product of two irreducible polynomials of degrees 2 and 5.

c) Show that the Galois group of P over the field of rational numbers contains a 7-cycle and a transposition, hence that it is isomorphic to the symmetric group $\mathfrak{S}_7$.

Remark. In fact, for any integer n, the Galois group of the polynomial $X^n - X - 1$ over $\mathbf{Q}$ is equal to $\mathfrak{S}_n$. You may try to prove this by analogous methods for small values of n. If you find the computations too hard, do not hesitate to rely on computer algebra systems, for they often provide routines to factor polynomials modulo prime numbers. For example, the answer to the first question is obtained in less than 1 ms by entering `factormod(x^7-x-1,2)` in PARI/GP, or `Factor(x^7-x-1) mod 2` in MAPLE.

Exercise 5.9 (Another proof of Theorem 5.4.2). Let $K \subset L$ be a finite extension of degree $n \geqslant 2$. Assume that it is Galois and that its Galois group is generated by $\sigma \in \mathrm{Gal}(L/K)$. Assume moreover that $\mathrm{card}\,\mu_n(K) = n$.

a) Show that $\sigma\colon L \to L$ is a morphism of K-vector spaces, and that its eigenvalues are nth roots of unity.

b) Show that L is the direct sum of the eigenspaces $L_\zeta = \{x \in L\,;\, \sigma(x) = \zeta x\}$, for $\zeta \in \mu_n(K)$.

c) If $y \in L_\zeta \setminus \{0\}$, show that the map $x \mapsto x/y$ is an injective K-linear map $L_\zeta \to L_1$.

d) Show that $L_1 = K$ and conclude that $\dim L_\zeta = 1$ for any $\zeta \in \mu_n(K)$. In particular, if ζ is any primitive nth root of unity, there is a nonzero element $x \in L^*$ such that $\sigma(x) = \zeta x$.

Exercise 5.10. Let $K \subset E$ be a splitting extension of an irreducible separable polynomial $P \in K[X]$. Assume that P has degree n and let $x_1, \ldots, x_n$ denote the roots of P in E. One assumes moreover that $\mathrm{Gal}(E/K)$ is cyclic; let σ be a generator.

a) Show that $[E : K] = n$.

b) Assume that $\mathrm{card}\,\mu_n(K) = n$. For any nth root of unity $\zeta \in K$, define a Lagrange's resolvent by

$$R(\zeta) = x_1 + \zeta\sigma(x_1) + \cdots + \zeta^{n-1}\sigma^{(n-1)}(x_1).$$

Show that $R(1) \in K$. For any $\zeta \in \mu_n(K)$, show that $R(\zeta)^n \in K$.

c) Show that E is generated by the $R(\zeta)$ for $\zeta \in \mu_n(K)$.

d) If n is a prime number, show that there is $j \in \{1, \ldots, n-1\}$ such that $E = K(\sqrt[n]{R(\zeta)^n})$.

Exercise 5.11. Let K be a field and consider a polynomial $P = X^n - a$, for some $a \in K^*$. Assume that n is not a multiple of the characteristic of K and observe that P is separable.

a) Let L be a splitting extension of K. Show that L contains a primitive nth root of unity ζ. Let $K_1 = K(\zeta)$ and write $\mu_n = \mu_n(K_1)$.

If $m \in \mathbf{Z}$ is prime to n, show that the map $u \mapsto u^m$ is an automorphism of μ_n. Show conversely that any automorphism of μ_n is of this form. Conclude that there is an isomorphism $(\mathbf{Z}/n\mathbf{Z})^* \simeq \mathrm{Aut}(\mu_n)$.

b) Show that the extensions $K \subset K_1$ and $K_1 \subset L$ are Galois, and that their Galois groups are naturally subgroups $A \subset (\mathbf{Z}/n\mathbf{Z})^*$ and $B \subset \mu_n$. (Fix $x \in L$ with $x^n = a$ and look at the action of $\mathrm{Gal}(L/K)$ on x and ζ.)

c) Show that the isomorphism of Question b) restricts to a morphism $\varphi\colon A \to \mathrm{Aut}(B)$ and prove that $\mathrm{Gal}(L/K)$ is isomorphic to the semi-direct product $A \rtimes_\varphi B$.

d) Assume that $[K_1 : K]$ is prime to n and that P is irreducible over K. Show that P is still irreducible over K_1 and that $B = \mu_n$.

e) *Numerical application:* $K = \mathbf{Q}$ and $P = X^7 - 2$. Show that $\mathrm{Gal}(L/K)$ has order 42 and is isomorphic to the group of permutations of $\mathbf{Z}/7\mathbf{Z}$ of the form $n \mapsto an + b$ for $a \in (\mathbf{Z}/7\mathbf{Z})^*$ and $b \in \mathbf{Z}/7\mathbf{Z}$.

Exercise 5.12. This exercise proposes a Galois-theoretic proof of the fundamental theorem of algebra.

Let $\mathbf{R} \subset K$ be a Galois extension of the field of real numbers containing the field of complex numbers $\mathbf{C}$. Let $G = \mathrm{Gal}(K/\mathbf{R})$ and let P be a 2-Sylow subgroup of G. Set $\mathrm{card}\, P = 2^n$.

a) Using the fact that $\mathbf{R}$ has no finite extension of odd degree, show that $G = P$.

b) Let $P_1 = \mathrm{Gal}(K/\mathbf{C})$. By Lemma 5.1.3, P has a normal series

$$\{1\} = P_n \subset \cdots \subset P_2 \subset P_1 \subset P$$

with $(P_{j+1} : P_j) = 2$ for any j. Define $K_j = K^{P_j}$. Show that the extension $K_j \subset K_{j+1}$ is a quadratic extension. Using the fact that any complex number is a square, show that $n = 1$, hence $K = \mathbf{C}$.

Exercise 5.13. This exercise will let you prove Theorem 5.1.1 without any group theory, using instead ideas from the second proof of the fundamental theorem of algebra.

Let z be any algebraic number, and assume that the degree of the extension of $\mathbf{Q}$ generated by its conjugates $z_1, \ldots, z_d$ is a power of 2.

Observe that d is itself a power of 2. By induction on d, prove as follows that z is constructible.

a) Fix $c \in \mathbf{Q}$, set $z_{i,j,c} = z_i + z_j + c z_i z_j$ and $Q_c = \prod_{i<j} (X - z_{i,j,c})$. Show that Q_c is a polynomial with rational coefficients, and that the degrees of its irreducible factors are powers of 2. Show that at least one of these degrees divides $d/2$, hence that there are $i < j$ such that $z_i + z_j + c z_i z_j$ is constructible.

b) Show that there are i and j such that $z_i + z_j$ and $z_i z_j$ are constructible. Conclude that z_i and z_j are both constructible.

c) Show that z is constructible.

Exercise 5.14. Let n be an integer, with $n \geqslant 5$. Let $K \subset L$ be a finite Galois extension with Galois group $\mathfrak{S}_n$.

a) Show that there is only one quadratic extension $K \subset K_1$ contained in L. What is the Galois group of the extension $K_1 \subset L$? (Use Exercise 4.17.)

b) Show that the degree of any $x \in L \setminus K_1$ is at least n.

Exercise 5.15. Let K be a field, and let $\varphi\colon K \to k \cup \{\infty\}$ be a place of K. Recall that we defined the valuation ring of φ as the set $A = \{x \in K\,;\, \varphi(x) \neq \infty\}$.

a) Show also that for any $x \in K \setminus \{0\}$, either x or $1/x$ belongs to A (this is the general definition of a valuation ring).

b) Let $\mathfrak{m} = \varphi^{-1}(0)$. Show that $\mathfrak{m}$ is an ideal of A and that an element $a \in A$ is invertible in A if and only if $a \notin \mathfrak{m}$.

c) Deduce from this that $\mathfrak{m}$ is the unique maximal ideal in A, that $A/\mathfrak{m}$ is a field, and that φ induces a field homomorphism $A/\mathfrak{m} \to k$.

d) In the two examples given in the text (Example 5.8.2), show that the ideal $\mathfrak{m}$ is generated by one element π. Show moreover that any ideal in A is generated by a power of π. (In fact, one can set $\pi = p$ in case *a*) and $\pi = X - \alpha$ in case *b*).) In particular, in these two cases, the ring A is a principal ideal ring.

Exercise 5.16. Let K be a field and let A be a subring in K. Fix an algebraic closure Ω of K. One says that an element $x \in \Omega$ is *integral* over A if there is a monic polynomial $P \in A[X]$ such that $P(x) = 0$.

a) Let x and y be two elements in Ω which are integral over A. Let P and $Q \in A[X]$ be monic polynomials such that $P(x) = Q(y) = 0$. Factor P and Q in Ω as

$$P = \prod_{i=1}^{n}(X - x_i) \quad \text{and} \quad Q = \prod_{j=1}^{m}(X - y_j).$$

Show that the coefficients of the polynomial $R = \prod_{i,j}(X - x_i - y_j)$ belong to A. (Write $R = \prod_i Q(X - x_i)$ and use the theorem on symmetric polynomials.) Conclude that $x + y$ is integral over A. Similarly, show that xy is integral over A.

b) Show that the set of elements of Ω which are integral over A form a subring of Ω.

c) Assume that A is a valuation ring. Show that an element $x \in K$ is integral over A if and only if $x \in A$. ("A valuation ring is integrally closed.")

d) Let P and Q be two monic polynomials in $K[X]$. Assume that $P \in A[X]$ and that Q divides P in $K[X]$. Show that the coefficients of Q are integral over A.

e) Assuming that A is a valuation ring, conclude that $Q \in A[X]$. ("Gauss's lemma for valuation rings.")