Galois theory

Nicolas Mascot (mascotn@tcd.ie)

Version: December 6, 2019

Contents

Introduction: what is Galois theory about?

Describing Galois theory without some theoretical background is not easy. In order to give a short glimpse of what it is about, we can make the following (vague) observations:

The computation

$$\frac{2+i}{1+3i} = \frac{(2+i)(1-3i)}{(1+3i)(1-3i)} = \frac{2+3+i-6i}{10} = \frac{1-i}{2},$$

which takes place in $\mathbb{C}$, involves the somewhat mysterious quantity i. In order to perform this computation, all we need to know i that $i^2 = -1$. This means that if we replace i with another entity α satisfying $\alpha^2 = -1$, namely $\alpha = -i$, in other words, if we apply complex conjugation $\tau : \begin{array}{ccc} \mathbb{C} & \longrightarrow & \mathbb{C} \\ z & \longmapsto & \overline{z} \end{array}$, the identity

$$\frac{2-i}{1-3i} = \frac{1+i}{2}$$

that we obtain remains valid. Another way to phrase this is to say that since i and $= i$ are both "quantities" satisfying $\alpha^2 = -1$, exchanging them defines a *field automorphism* $\tau : \mathbb{C} \longrightarrow \mathbb{C}$.

In fact, this is not specific to complex conjugation. For instance, we can introduce $\mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} | a, b \in \mathbb{Q}\}$, which happens to be a subfield of $\mathbb{R}$, and compute there that

$$\frac{\sqrt{2}+2}{\sqrt{2}-1} = \sqrt{2};$$

in this computation, all we really used bout $\sqrt{2}$ is the fact that it is some number α such that $\alpha^2 = 2$, so that if we replace $\sqrt{2}$ by $-\sqrt{2}$, which also

satisfies $\alpha^2 = 2$, then we obtain the identity

$$\frac{-\sqrt{2}+2}{-\sqrt{2}-1} = -\sqrt{2}$$

which is equally valid. Again, this can be interpreted in terms of the existence of a field automorphism

$$\sigma : \begin{array}{ccc} \mathbb{Q}(\sqrt{2}) & \longrightarrow & \mathbb{Q}(\sqrt{2}) \\ a+b\sqrt{2} & \longmapsto & a-b\sqrt{2}. \end{array}$$

For a more complicated example, consider $f(x) = x^5 + 2x^2 + 3$. This polynomial has only one real root, which we will denote by α. It can be shown (cf. the proof of theorem 1.2.4 for details about how this identity was obtained) that

$$\frac{1}{\alpha^2 - 2\alpha + 2} = \alpha^3 + 2\alpha^2 + 2\alpha + 2;$$

but since establishing this identity only uses the relation $f(\alpha) = 0$ (and not the fact that α is the real root of $f(x)$), it remains valid if we replace α with any one of the complex roots of $f(x)$.

The upshot of the picture that thus emerges is that if we start with some set (field) of "basic" numbers ($\mathbb{R}$ in the first example, $\mathbb{Q}$ in the second one), when we throw in the roots of an (irreducible) polynomial, these roots behave as "alien" quantities that have the same algebraic properties as each other (they satisfy the same identities), which makes them somewhat indistinguishable from each other. We therefore expect that there exist field automorphisms that permute them.

Taking this idea the other way round, it is reasonable to think that the "basic" numbers we started with are characterized by the fact that they are *fixed* by all field automorphisms (cf. theorem 2.4.3) for a rigorous statement). Thus for instance in the first example we started with $\mathbb{R}$ as "basic" numbers, which we enlarged into $\mathbb{C}$ by throwing in the "alien" quantity i, an the elements of $\mathbb{R}$ are characterised among those of $\mathbb{C}$ by the fact that they are fixed under complex conjugation; similarly, in the second example we started with $\mathbb{Q}$, and enlarged it to $\mathbb{Q}(\sqrt{2})$, and the elements of $\mathbb{Q}$ are characterised by the fact that they are fixed by σ.

We could even try to refine this principle: if we have several automorphisms, we could sort numbers by "complexity", the most simple ones being

those fixed by some automorphisms, the slightly more complicated ones being those that are fixed by some automorphisms but not all, etc.

We thus get the idea behind the *Galois correspondence* (cf. theorem 2.5.2), which is the fundamental result of Galois theory an relates fields to groups of filed automorphisms, and thus allows one to turn (difficult) field theory problems into (easier) group theory problems.

Remark. You may have heard that Galois theory explains why there is no "formula" to solve equations of degree 5 and higher. This is in fact just a (rather anecdotic) application of Galois theory, the idea being that equations of high degree yield groups that are sufficiently complicated that no such "formula" can exist.

Chapter 1

Reminders about field extensions

Before we establish the main theorem of Galois theory, let us begin by reviewing filed and their extensions.

1.1 Preliminary reminders

1.1.1 Field morphisms

Definition 1.1.1. Let R and S be rings (note: all rings considered in these notes are assumed to be commutative). A *ring morphism* $f : R \longrightarrow S$ is a map such that for all $x, y \in R$, $f(x + y) = f(x) + f(y)$, $f(0) = 0$, $f(xy) = f(x)f(y)$, and $f(1) = 1$.

A *field morphism* is simply a ring morphism between fields.

Proposition 1.1.2. *Let $f : K \longrightarrow L$ be a field morphism. Then automatically*

1. *$f(x/y) = f(x)/f(y)$ for all $x, y \in K$, $y \neq 0$,*
2. *f is injective,*
3. *the image of f is a subfield of L.*

Proof. 1. $f(1/y)f(y) = f(1) = 1$ so $f(1/y) = 1/f(y)$, whence $f(x/y) = f(x)/f(y)$.

2. If $x \neq y$, then $x - y \neq 0$ so $f(\frac{1}{x-y})f(x-y) = 1$ so $f(x) - f(y) = f(x-y) \neq 0$. Alternatively, $\ker f \subseteq K$ is an ideal, but K is a field...

3. This can be checked directly; alternatively, since f is injective, it induces an isomorphism between the field K and its image.

□

1.1.2 Symmetric polynomials, resultants, and discriminants

Let us fix a field K, and n variables $x_1, \cdots, x_n$. We denote by $K[x_1, \cdots, x_n]$ the ring of polynomials in these n variables and with coefficients in K.

Definition 1.1.3. A polynomial $P(x_1, \cdots, x_n) \in K[x_1, \cdots, x_n]$ is *symmetric* if it is invariant under any permutation of the variables.

Definition 1.1.4. The elementary symmetric polynomials in $x_1, \cdots, x_n$ are

$$\begin{aligned}
&\sigma_1 = x_1 + \cdots + x_n, \\
&\sigma_2 = x_1x_2 + \cdots + x_1x_n + x_2x_3 + \cdots + x_2x_n + \cdots + x_{n-1}x_n, \\
&\vdots \\
&\sigma_k = \textstyle\sum_{i_1 < \cdots < i_k} x_{i_1} \cdots x_{i_k}, \\
&\vdots \\
&\sigma_n = x_1 \cdots x_n.
\end{aligned}$$

These polynomials are obviously symmetric. They are called *elementary* for the following reason:

Theorem 1.1.5. *Let $P(x_1, \cdots, x_n) \in K[x_1, \cdots, x_n]$. The P is symmetric if and only if it can be expressed as a polynomial in $\sigma_1, \cdots, \sigma_n$ with coefficients in K.*

Remark 1.1.6. The "only if" part is obvious; it is the "if" part that is useful.

Example 1.1.7. Take $n = 4$. The elementary symmetric polynomials are

$$\begin{aligned}
&\sigma_1 = x_1 + \cdots + x_n, \\
&\sigma_2 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4, \\
&\sigma_3 = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4, \\
&\sigma_4 = x_1x_2x_3x_4.
\end{aligned}$$

The polynomial $P = x_1^2 + x_2^2 + x_3^2 + x_4^2$ is symmetric, so it is expressible in terms of the σ_k; indeed

$$P = \sigma_1^2 - 2\sigma_2.$$

On the other hand, $Q = x_1 + x_2^2 + x_3^3 + x_4^4$ is not symmetric, and is therefore not expressible in terms of the σ_k.

Proposition 1.1.8 (Vieta's formulas)**.** *Let $\alpha_1, \cdots, \alpha_n \in K$, and expand*

$$\prod_{k=1}^{n}(x - \alpha_k) = \sum_{k=0}^{n} a_k x^k.$$

Then we have $a_n = 1$, $a_{n-1} = -\sigma_1(\alpha_1, \cdots, \alpha_n)$, $\cdots$, $a_{n-k} = (-1)^k \sigma_k(\alpha_1, \cdots, \alpha_n)$, $\cdots$, $a_0 = (-1)^n \sigma_n(\alpha_1, \cdots, \alpha_n)$.

Corollary 1.1.9. *Let $P(x) \in K[x]$, and let $\alpha_1, \cdots, \alpha_n$ be the roots of P (counted with multiplicity, and which lie in some larger field, not necessarily in K). Then the value of any symmetric polynomial in $\alpha_1, \cdots, \alpha_n$ and with coefficients in K lies in K (even though the α_k do not necessarily lie in K).*

Example 1.1.10. Let $P(x) = x^4+2x^3-x^2+5x-3 \in \mathbb{Q}[x]$, and let $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ be its complex roots (in some arbitrary order). Then we have

$$\begin{aligned}
\sigma_1(\alpha_1, \alpha_2, \alpha_3, \alpha_4) &= -2, \\
\sigma_2(\alpha_1, \alpha_2, \alpha_3, \alpha_4) &= -1, \\
\sigma_3(\alpha_1, \alpha_2, \alpha_3, \alpha_4) &= -5, \\
\sigma_4(\alpha_1, \alpha_2, \alpha_3, \alpha_4) &= -3,
\end{aligned}$$

so that

$$\alpha_1^2 + \alpha_2^2 + \alpha_3^2 + \alpha_4^2 = (-2)^2 - 2(-1) = 6 \in \mathbb{Q}$$

in view of example 1.1.7, whereas the value of

$$\alpha_1 + \alpha_2^2 + \alpha_3^3 + \alpha_4^4$$

depends on the ordering of the α_k and is not in general rational.

The moral of the story is that we can compute with the roots of a polynomial even if we do not have a formula for them, as long as we stick to symmetric expressions in them (a natural restriction since the roots are in general indistinguishable from each other).

Consider now the following problem: let $A(x), B(x) \in K[x]$ be polynomials, and let $\alpha_1, \cdots, \alpha_n$ be the roots of $A(x)$ (in some large enough field containing K). Then the expression

$$\prod_{k=1}^{n} B(\alpha_k)$$

is symmetric in the α_k, so it must be expressible in terms of $B(x)$ and of the coefficients of $A(x)$, and in particular lie in K, but how can we evaluate it? The answer to this question is *resultants*.

Definition 1.1.11. Let $A = \sum_{j=0}^{m} a_j x^j$ and $B = \sum_{k=0}^{n} b_k x^k$ be two polynomials with coefficients in K. The *resultant* of A and B is the $(m+n)\times(m+n)$ determinant

$$\mathrm{Res}(A,B) = \begin{vmatrix} a_m & a_{m-1} & \cdots & a_0 & 0 & \cdots & 0 \\ 0 & a_m & a_{m-1} & \cdots & a_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \ddots & 0 \\ 0 & \cdots & 0 & a_m & a_{m-1} & \cdots & a_0 \\ b_n & b_{n-1} & \cdots & b_0 & 0 & \cdots & 0 \\ 0 & b_n & b_{n-1} & \cdots & b_0 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & & \ddots & 0 \\ 0 & \cdots & 0 & b_n & b_{n-1} & \cdots & b_0 \end{vmatrix},$$

where the first n rows contain the coefficients of A and the m last ones contain those of B.

The main properties of the resultant are the following:

Theorem 1.1.12.

- $\mathrm{Res}(A,B) \in K$, *and in fact, if the coefficients of both* A *and* B *lie in a subring* $\mathcal{R}$ *of* K, *then* $\mathrm{Res}(A,B) \in \mathcal{R}$.
- *If we can factor (over* K *or over a larger field)* A *and* B *as*

$$A = a\prod_{j=1}^{\deg A}(x-\alpha_j) \text{ and } B = b\prod_{k=1}^{\deg B}(x-\beta_k),$$

then

$$\begin{aligned}\mathrm{Res}(A,B) &= a^{\deg B}\prod_{j=1}^{\deg A}B(\alpha_j) = a^{\deg B}b^{\deg A}\prod_{j=1}^{\deg A}\prod_{k=1}^{\deg B}(\alpha_j-\beta_k)\\ &= (-1)^{\deg A\deg B}b^{\deg A}\prod_{k=1}^{\deg B}A(\beta_k) = (-1)^{\deg A\deg B}\mathrm{Res}(B,A).\end{aligned}$$

- $\mathrm{Res}(A,B) = 0$ *if and only if* A *and* B *have a common root (possibly in some lager field than* K*).*

Example 1.1.13. Take $K=\mathbb{Q}$, $A = x^2-2 \in \mathbb{Q}[x]$ and $B = x^2+1 \in \mathbb{Q}[x]$. Since actually A and B lie in $\mathbb{Z}[x]$, we have $\mathrm{Res}(A,B) \in \mathbb{Z}$; this is simply because by definition,

$$\mathrm{Res}(A,B) = \begin{vmatrix}1 & 0 & -2 & 0\\ 0 & 1 & 0 & -2\\ 1 & 0 & 1 & 0\\ 0 & 1 & 0 & 1\end{vmatrix}.$$

Besides, since we have

$$A = (x-\sqrt{2})(x+\sqrt{2}) \text{ and } B = (x-i)(x+i)$$

over $\mathbb{C}$, we find that

$$\mathrm{Res}(A,B) = B(\sqrt{2})B(-\sqrt{2}) = A(i)A(-i) = (\sqrt{2}-i)(\sqrt{2}+i)(-\sqrt{2}-i)(-\sqrt{2}+i) = 9.$$

In this example, it was easier to compute the resultants by handling directly the roots of A or B rather than evaluating the determinant, but in general, the point of resultants is to evaluate such expressions without introducing the roots explicitly, so as to only perform exact calculations; cf. example 1.2.9 for a more exciting case.

Example 1.1.14. Suppose we have $A = BQ + R$ in $K[x]$, and let b be the leading coefficient of B. Then $A(\beta) = R(\beta)$ for all roots β of B, so that

$$\operatorname{Res}(A, B) = (-1)^{\deg A \deg B} b^{\deg A - \deg R} \operatorname{Res}(B, R).$$

This gives a way to compute $\operatorname{Res}(A, B)$ by performing successive Euclidean divisions, which is more efficient (at least for a computer) than computing a large determinant when the degrees of A and B are large.

The fact that the resultant vanishes iff. the polynomials have a common root is particularly useful in the following case:

Definition 1.1.15. Let $A(x) \in K[x]$ be a polynomial of degree $n \in \mathbb{N}$ and with leading coefficient $a \in K$. The *discriminant* of $A(x)$ is

$$\operatorname{disc} A = \frac{(-1)^{n(n-1)/2}}{a} \operatorname{Res}(A, A').$$

Example 1.1.16. Let $A(x) = ax^2 + bx + c$, $a \neq 0$. Then $A'(x) = 2ax + b$, so that

$$\operatorname{Res}(A, A') = \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = 4a^2c - ab^2,$$

so we recover the well-known formula

$$\operatorname{disc} A = \frac{-1}{a} \operatorname{Res}(A, A') = b^2 - 4ac.$$

Theorem 1.1.17. *Let $\Omega \supseteq K$ be a field large enough to contain all the roots of $A(x)$, and let $\alpha_1, \ldots, \alpha_n \in \Omega$ be these roots, repeated with multiplicity. Then*

$$\begin{aligned} \operatorname{disc} A &= (-1)^{n(n-1)/2} a^{n-2} \prod_{j=1}^{n} P'(\alpha_j) \\ &= (-1)^{n(n-1)/2} a^{2n-2} \prod_{j \neq k} (\alpha_j - \alpha_k) \\ &= a^{2n-2} \prod_{j<k} (\alpha_j - \alpha_k)^2. \end{aligned}$$

Proof. The first equality is just an application of theorem 1.1.12. Then, since

$$A(x) = a \prod_{j=1}^{n} (x - \alpha_j),$$

we have

$$P'(x) = a \sum_{j=1}^{n} \prod_{k \neq j} (x - \alpha_k)$$

so

$$P'(\alpha_j) = a \prod_{k \neq j} (\alpha_j - \alpha_k),$$

whence the result. □

Corollary 1.1.18. *$A(x)$ has multiple roots (in some large enough field) if and only if* $\operatorname{disc} A = 0$.

We also have the following property:

Proposition 1.1.19. *Let $P(x) \in \mathbb{R}[x]$ without multiple roots, so that* $\operatorname{disc} P \in \mathbb{R}^\times$. *If $P(x)$ has r_1 real roots and r_2 complex-conjugate pair of non-real roots (so that* $\deg P = r_1 + 2r_2$*), then the sign of* $\operatorname{disc} P$ *is* $(-1)^{r_2}$.

1.1.3 Reminders on PID's

Let R be a commutative ring.

Definition 1.1.20. R is a domain if for all $x, y \in R$, $xy = 0 \implies x = 0$ or $y = 0$.

Definition 1.1.21. A subset $I \subseteq R$ is an *ideal* if $i + j \in I$ for all $i, j \in I$ and $ri \in I$ for all $r \in R$ and $i \in I$. An ideal is *principal* if it is of the form

$$(r) = rR = \{rs, s \in R\}$$

for some $r \in R$. A domain R is a *PID* if all its ideals are principal.

Theorem 1.1.22. *Every PID is a UFD: their elements can be factored into a product of irreducibles, and this factorisation is unique up to reordering and to invertible elements. In particular, the notions of gcd and lcm make sense in a PID.*

Theorem 1.1.23. *Every PID R has the* Bézout property*: given $r, s \in R$, there exist $u, v \in R$ such that $ur + vs = \gcd(r, s)$.*

Theorem 1.1.24. *Let K be a field. Then $K[x]$ is* Euclidean*: given $A, B \in K[x]$ with $B \neq 0$, there exists a unique pair (Q, R) of elements of $K[x]$ such that $A = BQ + R$ and that* $\deg R < \deg B$ *(this covers the case $R = 0$, thanks to the convenient convention* $\deg 0 = -\infty$.

This implies that $K[x]$ is a PID, and therefore also a UFD.

1.2 Field extensions

1.2.1 Notation

Let K and L be fields such that $K \subseteq L$. One says that K is a *subfield* of L, and that L is an *extension* of K.

In what follows, whenever $\alpha \in L$ (resp. $\alpha_1, \alpha_2, \cdots \in L$), we will write $K(\alpha)$ (resp. $K(\alpha_1, \alpha_2, \cdots)$) to denote the smallest subfield of L containing K as well as α (resp. $\alpha_1, \alpha_2, \cdots$). For example, we have $\mathbb{C} = \mathbb{R}(i)$, and $K(\alpha) = K$ if anf only if $\alpha \in K$.

Also, when $\mathcal{R}$ is a subring of K, we will write

$$\mathcal{R}[\alpha] = \{P(\alpha),\ P \in \mathcal{R}[x]\}$$

to denote the smallest subring of L containing $\mathcal{R}$ as well as α, and similarly

$$\mathcal{R}[\alpha_1, \cdots, \alpha_n] = \{P(\alpha_1, \cdots, \alpha_n),\ P \in \mathcal{R}[x_1, \cdots, x_n]\}.$$

Example 1.2.1. The ring $K[\alpha]$ is a subring of the field $K(\alpha)$.

1.2.2 Algebraic elements, algebraic extensions

Definition 1.2.2. Let $\alpha \in L$. Then set of polynomials $P \in K[x]$ such that $P(\alpha) = 0$ is an ideal V_α of $K[x]$, and one says that α is *algebraic* over K if this ideal is nonzero, that is to say if there exists a nonzero $P \in K[x]$ which vanishes at α. Else one says that α is *transcendental* over K, or just transcendental (for short) when $K = \mathbb{Q}$.

In the case when α is algebraic over K, the ideal V_α can be generated by one polynomial since the ring $K[x]$ is a PID. This polynomial is unique up to scaling, so there is a unique *monic* polynomial $m_\alpha(x)$ that generates V_α. This polynomial $m_\alpha(x)$ is called the *minimal polynomial* of α over K. One then says that α is algebraic over K of *degree* n, where $n = \deg m_\alpha \in \mathbb{N}$, and one writes $\deg_K \alpha = n$. When $K = \mathbb{Q}$, one says for short that α is algebraic of degree n.

If every element of L is algebraic over K, one says that L is an *algebraic extension* of K.

Remark 1.2.3. Minimal polynomials (over a field K) are always irreducible (over the same field K). Indeed, let $m_\alpha(x) \in K[x]$ be the minimal polynomial of some $\alpha \in L$, and suppose we have a factorisation $m_\alpha(x) = A(x)B(x)$

with $A(x), B(x) \in K[x]$. Then $0 = m_\alpha(\alpha) = A(\alpha)B(\alpha)$, so without loss of generality we may assume that $A(\alpha) = 0$. By definition of the minimal polynomial, this means that $m_\alpha(x) \mid A(x)$; but since we also have $A(x) \mid m_\alpha(x)$, $B(x)$ must be a constant.

Theorem 1.2.4. *Let L/K be a field extension, and let $\alpha \in L$ be algebraic over K of degree n. Then $K[\alpha]$ is a field, so it agrees with $K(\alpha)$. It is also a vector space of dimension n over K, with basis*

$$1, \alpha, \alpha^2, \cdots, \alpha^{n-1},$$

which we write as

$$K(\alpha) = K[\alpha] = \bigoplus_{j=0}^{n-1} K\alpha^j.$$

Remark 1.2.5. On the other hand, if $\alpha \in L$ is transcendental over K, then it is not difficult to see that

$$K(\alpha) = \{r(\alpha),\ r \in K(x)\}$$

is isomorphic to the field $K(x)$ of rational fractions over K via

$$\begin{array}{ccc} K(x) & \xrightarrow{\sim} & K(\alpha) \\ \dfrac{P(x)}{Q(x)} & \longmapsto & \dfrac{P(\alpha)}{Q(\alpha)} \end{array}$$

(this is well-defined since, as α is transcendental, $Q(\alpha) \neq 0$ as soon as $Q(x)$ is not the 0 polynomial), whence the notation $K(\alpha)$. In particular, it is infinite-dimensional as a K-vector space, and $K[\alpha]$ is a strict subring of $K(\alpha)$.

Proof of theorem 1.2.4. Let us begin with the second equality. Let $m(x) = m_\alpha(x) \in K[x]$ be the minimal polynomial of α over K, an irreducible polynomial of degree n. For all $P(x) \in K[x]$, euclidean division in $K[x]$ tells us that we may write

$$P(x) = m(x)Q(x) + R(x)$$

where $Q(x), R(x) \in K[x]$ and $\deg R(x) < n$. Evaluating at $x = \alpha$, we find that $P(\alpha) = R(\alpha)$, so that

$$K[\alpha] = \left\{ \sum_{j=0}^{n-1} \lambda_j \alpha^j,\ \lambda_j \in K \right\}.$$

Besides, if we had a relation of the form

$$\sum_{j=0}^{n-1} \lambda_j \alpha^j = 0$$

with the λ_j in K and not all zero, this would mean that the nonzero polynomial

$$\sum_{j=0}^{n-1} \lambda_j x^j \in K[x]$$

vanishes at $x = \alpha$, and since its degree is $< n$, this would contradict the definition of the minimal polynomial.

Therefore, the $(\alpha^j)_{0 \leqslant j < n}$ span $K[\alpha]$ as a K-vector space and are linearly independent over K, so they form a K-basis of $K[\alpha]$.

For the first equality, we must prove that the ring $K[\alpha]$ is actually a field. Let us thus prove that any nonzero $\beta \in K[\alpha]$ is invertible in $K[\alpha]$. We know from the above that $\beta = P(\alpha)$ for some nonzero $P(x) \in K[x]$ of degree $< n$. Since $m(x)$ is irreducible over K and $\deg P(x) < \deg m(x) = n$, it follows that $P(x)$ and $m(x)$ are coprime, so that there exist $U(x)$ and $V(x)$ in $K[x]$ such that

$$U(x)P(x) + V(x)m(x) = 1.$$

Evaluating at $x = \alpha$, we find that $U(\alpha)P(\alpha)+0 = 1$, which proves that $U(\alpha) \in K[\alpha]$ is the inverse of $\beta = P(\alpha)$. □

Example 1.2.6. Let $\alpha = \sqrt{2}$. Then α is a root of $x^2 - 2 \in \mathbb{Q}[x]$. Since this polynomial is of degree only 2, if it were reducible, it would split into factors of degree 1; since $\alpha \notin \mathbb{Q}$, we conclude that $x^2 - 2$ is irreducible, so it is the minimal polynomial of α, which is thus is algebraic of degree 2. In particular, we have

$$\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] = \mathbb{Q} \oplus \mathbb{Q}\sqrt{2},$$

which means that every element of $\mathbb{Q}(\sqrt{2})$ can be written in a unique way as $a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$.

Similarly, since $i^2 = -1$, i is algebraic of degree 2, and its minimal polynomial is x^2+1. It is also algebraic of degree 2 over $\mathbb{R}$, with the same minimal polynomial $x^2 + 1$, but which is this time seen as lying in $\mathbb{R}[x]$. We deduce that

$$\mathbb{Q}(i) = \mathbb{Q}[i] = \mathbb{Q} \oplus \mathbb{Q}i$$

and that

$$\mathbb{C} = \mathbb{R}(i) = \mathbb{R}[i] = \mathbb{R} \oplus \mathbb{R}i.$$

We thus recover the well-known fact that every complex number can be written uniquely as $a + bi$ with $a, b \in \mathbb{R}$.

On the contrary, one can prove that π is transcendental over $\mathbb{Q}$ (but this is not easy). In particular, $\mathbb{R}$ is not an algebraic extension of $\mathbb{Q}$, and its subfield $\mathbb{Q}(\pi)$ is isomorphic to $\mathbb{Q}(x)$.

Finally, one can prove that $\sqrt{3}$ is algebraic of degree 2 over $\mathbb{Q}(\sqrt{2})$. This amounts to say that $x^2 - 3$, which is irreducible over $\mathbb{Q}$, remains irreducible over $\mathbb{Q}(\sqrt{2})$. Indeed, if it became reducible, then $\sqrt{3}$ would lie in $\mathbb{Q}(\sqrt{2})$. Theorem 1.2.4 tells us that $(1, \sqrt{2})$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{2})$, so there would exist $a, b \in \mathbb{Q}$ such that $\sqrt{3} = a + b\sqrt{2}$. Squaring yields $3 = (a^2 + 2b^2) + 2ab\sqrt{2}$, which (again by theorem 1.2.4) implies that $a^2 + 2b^2 = 3$ and that $2ab = 0$, which is clearly impossible.

It follows that

$$\mathbb{Q}(\sqrt{2})(\sqrt{3}) = \mathbb{Q}(\sqrt{2}) \oplus \mathbb{Q}(\sqrt{2})\sqrt{3}$$

as a vector space over $\mathbb{Q}(\sqrt{2})$, so that every element of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ can be written in a unique way as $a + b\sqrt{3}$ with $a, b \in \mathbb{Q}(\sqrt{2})$.

Remark 1.2.7. Let K be a field in which $1 + 1 \neq 0$ (i.e. $\operatorname{char} K \neq 2$, cf. definition 1.3.1), and let L be an extension of K such that $[L : K] = 2$. Then there exists $\alpha \in L$ such that $L = K(\alpha)$ and $\alpha^2 = a \in K$; in other words, any extension of degree 2 is of the form $K(\sqrt{d})$ for some $d \in K$ (which is not a square in K, else we would have $K(\sqrt{d}) = K$).

Indeed, since $[L : K] = 2$, we can find $\beta \in L$ such that $\{1, \beta\}$ is a K-basis of L. Then clearly $L = K(\beta)$. Besides, $\beta^2 \in L$ so we must have a K-linear dependency relation $a\beta^2 + b\beta + c = 0$ for some $a, b, c \in K$ with $a \neq 0$ (else 1 and β would not be K-independent). Since $2 \neq 0 \in K$, the usual formula applies and shows that $\beta = \frac{-b \pm \sqrt{\Delta}}{2a}$ where $\Delta = b^2 - 4ac \in K$, which shows that $K(\sqrt{\Delta}) = K(\beta) = L$. We can thus take $d = \Delta$.

Note that this result does *not* generalise to higher degrees, for instance most extensions of K of degree 3 are not of the form $K(\sqrt[3]{d})$ for any $d \in K$.

We now prove that the four basic operations preserve algebraicity.

Theorem 1.2.8. *Let L/K be a field extension. The sum, difference, product, and quotient*[1] *of two elements of L which are algebraic over K are algebraic*

[1] Not by 0, of course.

over K.

Proof. Let α (resp. β) be algebraic over K, so that there exists a nonzero polynomial $A(x) \in K[x]$ (resp. $B(x) \in K[x]$) such that $A(\alpha) = 0$ (resp. $B(\beta) = 0$). Factor $A(x)$ and $B(x)$ in some large enough extension of K,

$$A(x) = \prod_{j=1}^{m}(x - \alpha_j), \quad B(x) = \prod_{k=1}^{n}(x - \beta_k),$$

with $\alpha = \alpha_1$ and $\beta = \beta_1$, and consider the polynomials $A(y)$ and $B(x - y)$ as polynomials in y over the field $K(x)$. Their resultant

$$C(x) = \mathrm{Res}\big(A(y), B(x - y)\big)$$

lies in $K(x)$, and actually even in $K[x]$ according to theorem 1.1.12, since the coefficients of $A(y)$ and $B(x - y)$ (still seen as polynomials in y) lie in $K[x]$. Besides, still according to theorem 1.1.12, we have

$$C(x) = \prod_{j=1}^{m} B(x - y)|_{y=\alpha_j} = \prod_{j=1}^{m} B(x - \alpha_j) = \prod_{j=1}^{m}\prod_{k=1}^{n}(x - \alpha_j - \beta_k),$$

so that $\alpha + \beta$ is a root of $C(x)$ and is thus algebraic over K.

The cases of $\alpha - \beta$, $\alpha\beta$ and α/β can be dealt with similarly. □

A consequence of this theorem is that the set $\overline{\mathbb{Q}}$ of complex numbers which are algebraic over $\mathbb{Q}$ is actually a subfield of $\mathbb{C}$.

Example 1.2.9. According to this theorem, $\alpha = \sqrt{2}+\sqrt{3}$ is algebraic. More specifically, it is a root of

$$\begin{aligned}\mathrm{Res}_y(y^2 - 2, (x - y)^2 - 3) &= \mathrm{Res}_y(y^2 - 2, y^2 - 2xy + x^2 - 3)\\ &= \begin{vmatrix} 1 & 0 & -2 & 0\\ 0 & 1 & 0 & -2\\ 1 & -2x & x^2 - 3 & 0\\ 0 & 1 & -2x & x^2 - 3 \end{vmatrix}\\ &= x^4 - 10x^2 - 1.\end{aligned}$$

In fact, this polynomial happens to be irreducible over $\mathbb{Q}$, so it is the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$.

1.2.3 The degree of an extension

Let L be an extension of a field K. If we forget temporarily about the multiplication on L, so that only addition is left, then L can be seen as a vector space over K.

Definition 1.2.10. The *degree* of L over K is the dimension (finite or infinite) of L seen as a K-vector space. It is denoted by $[L : K]$.

If this degree is finite, one says that L is a *finite extension* of K.

Example 1.2.11. Let $\alpha \in L$. If α is algebraic over K with minimal polynomial $m_\alpha(x) \in K[x]$ of degree n, then theorem 1.2.4 tells us that

$$K(\alpha) = \left\{ \sum_{k=0}^{n-1} \lambda_k \alpha^k,\ \lambda_k \in K \right\} = K \oplus K\alpha \oplus \cdots \oplus K\alpha^{n-1},$$

so $[K(\alpha) : K] = n = \deg_K \alpha$. On the other hand, if α is transcendental over K, then $K(\alpha)$ is isomorphic to the rational fraction field $K(x)$, so $[K(\alpha) : K] = \infty$.

Remark 1.2.12. Clearly, the only extension L of a field K such that $[L : K] = 1$ is $L = K$ itself.

Theorem 1.2.13. *If an extension is finite, then it is algebraic.*

Proof. Let L be a finite extension of K. Attach to each $\alpha \in L$ the map

$$\begin{array}{rccc} \mu_\alpha \colon & L & \longrightarrow & L \\ & \xi & \longmapsto & \alpha\xi. \end{array}$$

This map is clearly an endomorphism (i.e. a K-linear map) of L seen as a K-vector space. Besides, we have $\mu_{\alpha+\beta} = \mu_\alpha + \mu_\beta$ and $\mu_{\alpha\beta} = \mu_\alpha \circ \mu_\beta$ for all $\alpha, \beta \in L$, so that $P(\mu_\alpha) = \mu_{P(\alpha)}$ for every polynomial $P \in K[x]$.

Take now $\alpha \in L$. We must show that it is algebraic over K. Consider the characteristic polynomial $\chi(x) \in K[x]$ of the endomorphism μ_α of L. By Cayley-Hamilton, we have $\chi(\mu_\alpha) = 0$, whence $0 = \chi(\mu_\alpha) = \mu_{\chi(\alpha)}$, which means that $\chi(\alpha) = \mu_{\chi(\alpha)}(1) = 0$. □

Example 1.2.14. Let L be an extension of K, and $\alpha \in L$ be algebraic over K. Then $K(\alpha)$ is a finite extension of K, so it is an algebraic extension of K, so that its elements are all algebraic over K.

Counter-example 1.2.15. The converse of theorem 1.2.13 is false. For (counter)-example, consider again the subfield $\overline{\mathbb{Q}}$ of $\mathbb{C}$ consisting of the complex numbers that ar algebraic over $\mathbb{Q}$. Then $\overline{\mathbb{Q}}$ is by definition an algebraic extension of $\mathbb{Q}$, but it is not a finite one. Indeed, one can show that in the chain

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5}) \subseteq \cdots$$

(throw in the square root of each prime number one by one), each extension is of degree 2, so that the n-th extension is of degree 2^n over $\mathbb{Q}$ by proposition 1.2.16, which forces $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$.

An important feature of the degree is that it is multiplicative. In fact, even more is true.

Proposition 1.2.16 (Multiplicativity of the degree)**.** *Let $K \subseteq L \subseteq M$ be finite extensions, let $(l_i)_{1 \leqslant i \leqslant [L:K]}$ be a K-basis of L, and let $(m_j)_{1 \leqslant j \leqslant [M:L]}$ be an L-basis of M. Then $(l_i m_j)_{\substack{1 \leqslant i \leqslant [L:K] \\ 1 \leqslant j \leqslant [M:L]}}$ is a K-basis of M. In particular, $[M : K] = [M : L][L : K]$.*

Proof. Let $m \in M$. Since $(m_j)_{1 \leqslant j \leqslant [M:L]}$ is an L-basis of M, we have

$$m = \sum_{j=1}^{[M:L]} \lambda_j m_j$$

for some $\lambda_j \in L$, and since $(l_i)_{1 \leqslant i \leqslant [L:K]}$ is a K-basis of L, each λ_j can be written

$$\lambda_j = \sum_{i=1}^{[L:K]} \mu_{i,j} l_i.$$

Thus we have

$$m = \sum_{j=1}^{[M:L]} \sum_{i=1}^{[L:K]} \mu_{i,j} l_i m_j,$$

which proves that the $l_i m_j$ span M over K.

Besides, if we had a linear dependency relation

$$\sum_{j=1}^{[M:L]} \sum_{i=1}^{[L:K]} \mu_{i,j} l_i m_j = 0$$

with $\mu_{i,j} \in K$, then we would have

$$\sum_{j=1}^{[M:L]} \lambda_j m_j = 0$$

where

$$\lambda_j = \sum_{i=1}^{[L:K]} \mu_{i,j} l_i \in L.$$

Since $(m_j)_{1 \leqslant j \leqslant [M:L]}$ is an L-basis of M, this would imply that

$$0 = \lambda_j = \sum_{i=1}^{[L:K]} \mu_{i,j} l_i \in L$$

for all j; and since $(l_i)_{1 \leqslant i \leqslant [L:K]}$ is a K-basis of L, this means that the $\mu_{i,j}$ are all zero. Thus the $l_i m_j$ are linearly independent over K. □

Example 1.2.17. According to example 1.2.6 above,

$$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2,$$

and

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

It then follows from proposition 1.2.16 that

$$[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 2 \times 2 = 4.$$

More precisely, since we know that $(1, \sqrt{2})$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{2})$ by theorem 1.2.4, and that $(1, \sqrt{3})$ is a $\mathbb{Q}(\sqrt{2})$-basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ by theorem 1.2.4 and example 1.2.6, we deduce from proposition 1.2.16 that $(1, \sqrt{2}, \sqrt{3}, \sqrt{6})$ is a $\mathbb{Q}$-basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$.

Application: constructible numbers

Suppose we are given an orthonormal coordinate frame (O, I, J) in the plane. A point is said to be *constructible* if we can obtain it from O, I, J in finitely many steps using only a ruler and a compass. A number $\alpha \in \mathbb{R}$ is said to be *constructible* if it is a coordinate of a constructible point; equivalently, α is constructible if $|\alpha|$ is the distance between two constructible points.

A bit of geometry shows that the set of constructible numbers is a *subfield* of $\mathbb{R}$, which is stable under radicals (of positive elements only, of course).

Conversely, suppose that we perform a ruler-and-compass construction in $n \in \mathbb{N}$ steps, and let K_j ($j \leq n$) be the subfield of $\mathbb{R}$ generated by the coordinates of the points constructed at the j-th step, so that $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n$. At each step j, we either construct the intersection of two lines, or the intersection of a line and a circle or of two circles. In the first case, the coordinates of the intersection can be found by solving a linear system, which can be done by field operations in K_j, so that $K_{j+1} = K_j$. In the second case, the coordinates of the intersection can be found by solving quadratic equations, so that $[K_{j+1} : K_j]$ is either 1 (if the solutions to these equations already lie in K_j) or 2 (if they do not, so that K_{j+1} is genuinely bigger than K_j). By removing the steps such that $K_{j+1} = K_j$, we thus see establish the following result:

Theorem 1.2.18. *Let $\alpha \in \mathbb{R}$. Then α is constructible iff. there exist fields $\mathbb{Q} = K_0 \subsetneq K_1 \subsetneq \cdots \subsetneq K_n$ such that $[K_{j+1} : K_j] = 2$ for all j and that $\alpha \in K_n$.*

Corollary 1.2.19. *If $\alpha \in \mathbb{R}$ is constructible, then α is algebraic over $\mathbb{Q}$, and $\deg_{\mathbb{Q}}(\alpha)$ is a power of 2.*

Proof. Since α is constructible, there exist fields $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n \ni \alpha$ such that $[K_{j+1} : K_j] = 2$ for all j. By proposition 1.2.16, we have $[K_j : \mathbb{Q}] = 2^j$ for all j, so in particular $[K_n : \mathbb{Q}] = 2^n$. It follows that K_n is a finite extension of $\mathbb{Q}$, which is therefore algebraic by theorem 1.2.13, so that α is algebraic over $\mathbb{Q}$. Besides,

$$\deg_{\mathbb{Q}}(\alpha) = [\mathbb{Q}(\alpha) : \mathbb{Q}] = \frac{[K_n : \mathbb{Q}]}{[K_n : \mathbb{Q}(\alpha)]}$$

divides $[K_n : \mathbb{Q}] = 2^n$, so it is also a power of 2. □

Remark 1.2.20. Beware that the converse of corollary 1.2.19 is false! For instance, the polynomial $x^4 - 8x^2 + 4x + 2$ is irreducible over $\mathbb{Q}$ since it is Eisenstein at 2, and is therefore the minimal polynomial of each of its roots over $\mathbb{Q}$, so that these roots are algebraic of degree 4 over $\mathbb{Q}$. It happens that these roots are all real, but that none of them is constructible!

The problem is that if α is such a root, then we do have $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$, but this does not imply the existence of an intermediate field K such that $\mathbb{Q} \subseteq$

$K \subseteq \mathbb{Q}(\alpha)$ where both extensions are of degree 2, i.e. the hypotheses of theorem 1.2.18 are not necessarily satisfied.

Later on, we will use Galois theory to prove that there exists no field K such that $\mathbb{Q} \subsetneq K \subsetneq \mathbb{Q}(\alpha)$ (cf. example 2.6.20), and we will also explain how to modify corollary 1.2.19 so that its converse holds (cf. theorem 2.6.18).

1.2.4 Abstract field extensions

Definition 1.2.21. Let $P(x) \in K[x]$ be irreducible. A *stem field* of $P(x)$ over K is an extension M of K in which $P(x)$ has a root $\alpha \in M$, and which is as small as possible in that $M = K(\alpha)$.

Definition 1.2.22. Let $F(x) \in K[x]$. A *splitting field* of $F(x)$ over K is an extension M of K in which $F(x)$ splits completely, and which is minimal in the sense that $M = K(\alpha_1, \alpha_2, \cdots)$ where $\alpha_1, \alpha_2, \cdots$ are the roots of $F(x)$ in M.

Example 1.2.23. Take $K = \mathbb{Q}$ and $F(x) = x^3 - 2$. Then $\mathbb{Q}(\sqrt[3]{2})$ is a stem field of F, but it is **NOT** a splitting field since it only contains one root of $F(x)$. A splitting field of $F(x)$ is $\mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$, where $\zeta_3 = e^{2\pi i/3}$. Although $F(x)$ splits completely in $\mathbb{C}$, $\mathbb{C}$ is not a splitting field of $F(x)$ over $\mathbb{Q}$ since it is too large: $\mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}) \subsetneq \mathbb{C}$.

That stem fields and splitting fields always exist is not completely clear a priori: so far, the field extensions (such as $\mathbb{Q} \subseteq \mathbb{Q}(i)$) that we have considered were obtained by cutting out a piece of a very large field (such as $\mathbb{C}$) containing all the fields we were interested in, but this large field had to come from somewhere! We now show that it is possible to construct extensions of any field "out of thin air", without taking elements from an already constructed larger field. While this may not seem useful when we work over $\mathbb{Q}$ since we can always embed everything into $\mathbb{C}$, this is especially reassuring where we are working in more unusual contexts that might be outside of our comfort zone (e.g. finite fields). It also gives us a clearer understanding of what is happening even when we can embed everything into $\mathbb{C}$; in particular, it shows that such an embedding is not canonical, which is a key point in Galois theory.

Before we show the existence of uniqueness of stem fields and splitting fields, we establish some terminology that we will use in the rest of these notes.

Definition 1.2.24. Let K be a field, and let L, M be extensions of K. A *K-morphism* from L to M is a field morphism from L to M inducing the identity on K. We similarly define the notions of *K-isomorphism* and of *K-automorphism*. We denote by $\mathrm{Hom}_K(L, M)$ the set of K-morphisms from L to M, and by $\mathrm{Aut}_K(L)$ the set of K-automorphisms of L.

Lemma 1.2.25. *Let K be a field, L, M extensions of K, $\sigma : L \longrightarrow M$ a K-morphism, $F(x) \in K[x]$, and $\alpha \in L$ a root of F. Then $\sigma(\alpha) \in M$ is also a root of F.*

Proof. Write $F(x) = \sum_i a_i x^i$. Then

$$0 = \sigma(0) = \sigma\big(F(\alpha)\big) = \sigma\left(\sum_i a_i \alpha^i\right) = \sum_i \sigma(a_i)\sigma(\alpha)^i = \sum_i a_i \sigma(\alpha)^i = F\big(\sigma(\beta)\big)$$

since $\sigma(a_i) = a_i$ as $a_i \in K$. □

We now show how to construct stem fields.

Theorem 1.2.26. *Let K be a field, and let $P \in K[x]$ be an irreducible polynomial with coefficients in K. The quotient ring $L = K[x]/P(x)K[x]$ is a field, which is a finite extension of K of degree $[L : K] = \deg P$, and the image of x in L is a root of P.*

Proof. Since $P(x)K[x]$ is an ideal of the ring $K[x]$, the quotient $L = K[x]/P(x)K[x]$ inherits a ring structure. We want to show that this ring is in fact a field, that it contains K as a subfield, and that its degree as an extension of K is $\deg P$.

The proof of the fact that that L is a field is the same as that of theorem 1.2.4. More precisely, let us consider a nonzero element $\alpha \in L$, and prove that it is invertible. This element α is represented by a polynomial $A(x) \in K[x]$, which is not divisible by $P(x)$ since $\alpha \neq 0$. As $P(x)$ is irreducible, the polynomials $A(x)$ and $P(x)$ are coprime, so by Bézout there exist $U(x), V(x) \in K[x]$ such that

$$A(x)U(x) + P(x)V(x) = 1.$$

Thus $A(x)U(x) \equiv 1 \bmod P(x)$, which means that $U(x)$ represents the inverse of $A(x)$ in the quotient $L = K[x]/P(x)K[x]$.

Furthermore, let $A(x) \in K[x]$ represent some element of L. Th Euclidean division $A = PQ + R$ of A by P shows that this element of L is represented by a polynomial (x) of degree $\deg P$, which is unique by uniqueness of the remainder in a Euclidean division. Therefore $\{1, x, x^2, \cdots, x^{\deg P - 1}\}$ is a K-basis of L, so L contains a copy of K as a subfield (namely the K-span of 1), and is a vector space of dimension $\deg P$ over K. □

Remark 1.2.27. In fact, $K[x]/P(x)K[x]$ is a field if and only if $P(x)$ is irreducible over K. Compare with $\mathbb{Z}/n\mathbb{Z}$ is a field if and only if n is prime (actually, this is exactly the same proof).

Remark 1.2.28. The notation $K[x]/P(x)K[x]$ is often abbreviated into $K[x]/\big(P(x)\big)$.

Lemma 1.2.29. *Let $P(x) \in K[x]$ be irreducible, and let $L = K[x]/\big(P(x)\big)$. The extension $K \subseteq L$ is* universal *for the extensions of K in which $P(x)$ has a root. In other words, given an extension M of K in which $P(x)$ has a root $\alpha \in M$, there exists a unique K-morphism $f : L \to M$ sending the image of x in L to $\alpha \in M$.*

Proof. Consider the map

$$\begin{array}{rccc} \mathrm{eval}_\alpha : & K[x] & \longrightarrow & M \\ & F(x) & \longmapsto & F(\alpha) \end{array}.$$

It satisfies $f(x) = x$ for all $x \in K$, and is clearly a ring morphism; in particular, its kernel is an ideal of $K[x]$, and since $K[x]$ is a PID, this ideal is of the form $Q(x)K[x]$ for some $Q(x) \in K[x]$ which we may rescale so that it is monic. Then $P(x) \in \ker \mathrm{eval}_\alpha$ since $P(\alpha) = 0$, so $Q \mid P$. Since P is irreducible, P and Q must therefore be proportional, so actually $P = Q$ since both are monic. The first isomorphism theorem then shows that there exists a unique ring morphism f such that eval_α factors as

$$\begin{array}{ccc} K[x] & \xrightarrow{\mathrm{eval}_\alpha} & M\ ; \\ \downarrow & \nearrow_{f} & \\ L = K[x]/P(x)K[x] & & \end{array}$$

in particular, f must be a K-morphism. Conversely, let $f : L \longrightarrow M$ be such a morphism, and let $\pi : K[x] \longrightarrow L = K[x]/\big(P(x)\big)$ be the canonical projection. Then $f \circ \pi = \mathrm{eval}_\alpha$, so f must be of the above form. □

Remark 1.2.30. Since f is a field morphism, it is injective, so it induces an isomorphism between L and its image $K[\alpha] \subseteq M$, which agrees with $K(\alpha) \subseteq M$ by theorem 1.2.4. In particular, in the special case when P is the minimal polynomial over K of some (necessarily algebraic over K) element α lying in some extension M of K, the ring morphism

$$\begin{array}{rcl} \mathrm{eval}_\alpha : K[x] & \longrightarrow & K(\alpha) \\ F(x) & \longmapsto & F(\alpha) \end{array}$$

factors through L and induces a field isomorphism between L and $K(\alpha)$:

$$\begin{array}{ccc} K[x] & \xrightarrow{\mathrm{eval}_\alpha} & K(\alpha) \\ \downarrow & \overset{\sim}{\nearrow} & \\ L = K[x]/\big(P(x)\big) & & \end{array}$$

Example 1.2.31. Take $K = \mathbb{R}$ and $P = x^2 + 1$. Then $L = \mathbb{R}[x]/(x^2+1)$ is a degree 2 extension of $\mathbb{R}$. In fact, $x^2 + 1$ is the minimal polynomial of i over $\mathbb{R}$, the map $\mathrm{eval}_i : F(x) \mapsto F(i)$ induces a field isomorphism between L and $\mathbb{R}(i) = \mathbb{C}$:

$$\begin{array}{ccc} \mathbb{R}[x] & \xrightarrow{\mathrm{eval}_i} & \mathbb{R}(i) = \mathbb{C}. \\ \downarrow & \overset{\sim}{\nearrow} & \\ \mathbb{R}[x]/(x^2+1) & & \end{array}$$

This isomorphism show that $\mathbb{C}$ is $\mathbb{R}$ adjoined some alien quantity x forced to satisfy $x^2 + 1 = 0$, namely i.

Example 1.2.32. Take $K = \mathbb{Q}$ and $P = x^3 - 2$, which is irreducible over $\mathbb{Q}$ as it is Eisenstein at $p = 2$. Therefore, $L = \mathbb{Q}[x]/(x^3-2)\mathbb{Q}[x]$ is a degree 3 extension of $\mathbb{Q}$, which is actually isomorphic to $\mathbb{Q}(\sqrt[3]{2})$ via

$$\begin{array}{ccc} \mathbb{Q}[x] & \xrightarrow{\mathrm{eval}_{\sqrt[3]{2}}} & \mathbb{Q}(\sqrt[3]{2})\,, \\ \downarrow & \overset{\sim}{\nearrow} & \\ \mathbb{Q}[x]/(x^3-2) & & \end{array}$$

but also to $\mathbb{Q}(\zeta_3\sqrt[3]{2})$ and to $\mathbb{Q}(\zeta_3^2\sqrt[3]{2})$ where $\zeta_3 = e^{2\pi i/3}$.

This illustrates the fact that which one of the 3 roots of x^3-2 we choose does not matter. The abstract extension $\mathbb{Q}[x]/(x^3-2)$ is thus a model for this extension that has the advantage of being canonical, since it does not pick a particular root of x^3-2: $\mathbb{Q}[x]/(x^3-2)$ is just $\mathbb{Q}(\alpha)$, where α is something having the property that $\alpha^3-2=0$ but whose nature does not matter. This reflects the fact that the roots of x^3-2 have the same properties as each other (cf. definition 1.2.39).

Besides, we get 3 embeddings of $\mathbb{Q}[x]/(x^3-2)$ into $\mathbb{C}$, one for each root of x^3-2 in $\mathbb{C}$.

Theorem 1.2.33. *Let $P(x) \in K[x]$ be irreducible. A stem field of $P(x)$ exists and is unique up to K-isomorphism.*

Proof. Existence: $L = K[x]/\big(P(x)\big)$ is a stem field of $P(x)$ over K since $P(x)$ has a root there (the image of x) and since L is generated by this root over K.

Uniqueness: Let L' be another stem field of $P(x)$ over K. Then L' contains a root α of $P(x)$, so there exists a K-morphism $L \longrightarrow L'$ sending the image of x in L to $\alpha \in L'$ by lemma 1.2.29. This K-morphism induces a K-isomorphism between L and its image, which is a subfield of L' containing α, and must therefore agree with L' by minimality of L'. □

Corollary 1.2.34. *Let $F(x) \in K[x]$. A splitting field of $F(x)$ exists.*

Proof. If $F(x)$ already splits into linear factors over K, we are done. Else, take an irreducible factor $P(x)$ of degree ≥ 2 of $F(x)$, and start over with $L = K[x]/\big(P(x)\big)$ instead of K. □

Example 1.2.35. Let us construct the splitting field of $F(x) = x^3-2$ over $\mathbb{Q}$. Since $F(x)$ is irreducible over K, we first enlarge K into $L = K[x]/(x^3-2)$, which we view as $K(\alpha)$ from now on, where α denotes the image of x in L. Since α is a root of $F(x)$, the quotient $F(x)/(x-\alpha)$ must be a polynomial, which turn out to be $x^2+\alpha x+\alpha^2$; we thus have the factorisation $F(x) = (x-\alpha)(x^2+\alpha x+\alpha^2)$ over L. If the factor $x^2+\alpha x+\alpha^2$ has both its roots in L, then L is a splitting field of F, so we stop; else, we need to further enlarge L.

Actually, $x^2+\alpha x+\alpha^2$ happens to be irreducible[2] over L, so we further enlarge L into $M = L[x]/(x^2+\alpha x+\alpha^2)$. Then $x^2+\alpha x+\alpha^2$ acquires a root

[2]This can be proved by computing that its discriminant is $-3\alpha^2$, which is not a square in L (e.g. because L can be embedded into $\mathbb{R}$, and then $-3\alpha^2 < 0$).

in M, so it must split in linear factor over M. Thus $F(x)$ splits into linear factors over M, so M is a splitting field of $F(x)$ over $\mathbb{Q}$.

We now show that splitting fields are unique up to isomorphism. In fact, we have a stronger statement:

Theorem 1.2.36. *Let $\sigma : K_1 \simeq K_2$ be a field isomorphism, let $F_1(x) \in K_1[x]$, and let $F_2(x) \in K_2[x]$ be the polynomial obtained by applying σ to the coefficients of $F_1(x)$, and finally let L_1 (resp. L_2) be a splitting field of $F_1(x)$ over K_1 (resp. of $F_2(x)$ over K_2). Then σ can be extended (in at least one way) into an isomorphism $\widetilde{\sigma} : L_1 \simeq L_2$.*

Proof. In the proof of corollary 1.2.34, we constructed splitting fields by throwing in one root at a time. To keep track of things, we do an induction on the degree $[L_1 : K_1]$.

If $[L_1 : K_1] = 1$, then $L_1 = K_1$, i.e. $F_1(x)$ already splits as $\prod_i (x - \alpha_i)$ where the α_i lie in K_1, so that $F_2(x) = \prod_i \big(x - \sigma(\alpha_i)\big) \in K_2[x]$, so $L_2 = K_2$ and we we can simply take $\widetilde{\sigma} = \sigma$.

Suppose now $[L_1 : K_1] > 1$. Then $F(x)$ does not split completely over K_1, so it has an irreducible factor $P_1(x) \in K_1[x]$. Let $P_2(x) \in K_2[x]$ be its image by σ, and for $i = 1, 2$, let $\alpha_i \in L_i$ be a root of $P_i(x)$, and set $E_i = K_i(\alpha_i) \subseteq L_i$. Then E_i is a stem field of $P_i(x)$ over K_i, so

$$E_1 = K_1(\alpha_1) \simeq K_1/\big(P_1(x)\big) \overset{\sigma}{\simeq} K_2[x]/\big(P_2(x)\big) \simeq K_2(\alpha_2) = E_2.$$

We thus obtain an isomorphism $\sigma' : E_1 \simeq E_2$. Besides $[L_1 : E_1] = [L_1 : K_1]/[E_1 : K_1] < [L_1 : K_1]$ by proposition 1.2.16, and L_1 (resp. L_2) is still a splitting field of $F_1(x)$ (resp. $F_2(x)$) over E_1 (resp. E_2), so the induction hypothesis grants us with an extension $\widetilde{\sigma} : L_1 \simeq L_2$ of σ' and thus of σ. □

Corollary 1.2.37. *Let $F(x) \in K[x]$. Splitting fields of F over K are unique up to K-isomorphism.*

Proof. Apply theorem 1.2.36 to the case $K_1 = K_2 = K$ and $\sigma = \mathrm{Id}$. □

Corollary 1.2.38. *Let K be a field, $F(x) \in K[x]$, L a splitting field of F over K, and $\alpha, \beta \in L$. Then the following conditions are equivalent:*

(i) α and β have the same minimal polynomial over K,

(ii) There exists a K-automorphism σ of L such that $\sigma(\alpha) = \beta$.

Proof.

- (i) $\implies$ (ii): $K_1 = K(\alpha)$ and $K_2 = K(\beta)$ are both stem fields of P over K, so they are both K-isomorphic to $K[x]/\big(P(x)\big)$ by lemma 1.2.29. In particular, there exits a K-isomorphism $\tau : K(\alpha) \simeq K(\beta)$ sending α to β. By theorem 1.2.36, τ extends into an automorphism σ of L, which is a K-automorphism since it extends τ.
- (ii) $\implies$ (i): Let $P(x) \in K[x]$ be the minimal polynomial of α. Then $P(\alpha) = 0$, so $P(\beta) = 0$ as well by lemma 1.2.25. Therefore the minimal polynomial of β over K divides P, so agrees with P since both are irreducible and monic.

□

Morally speaking, this says that if α and β have the same minimal polynomial, they are so indistinguishable from each other that there exists an automorphism that sends one to the other, and that conversely, if σ is an automorphism, then $\sigma(\alpha)$ and α have the same algebraic properties.

Definition 1.2.39. Two elements α and β satisfying the conditions of corollary 1.2.38 are said to be *conjugate* over K.

Example 1.2.40. Take $K = \mathbb{R}$, and $L = \mathbb{C}$, which is the splitting field of $F(x) = x^2 + 1$. Then $\alpha, \beta \in \mathbb{C}$ are conjugate in the above sense iff. they are equal or complex-conjugate.

Example 1.2.41. The conjugates of $\sqrt[3]{2}$ over $\mathbb{Q}$ are the $\zeta_3^k \sqrt[3]{2}$ for $k = 0, 1, 2$.

To conclude this section, we mention the existence of algebraic closures.

Theorem 1.2.42. *Let K be any field. There exists an extension $\overline{K}$ of K, called the* algebraic closure *of K, such that every polynomial with coefficients in K (and even in $\overline{K}$) splits into linear factors, and which is minimal in the sense that it is an algebraic extension of K. It is unique up to K-isomorphism.*

Proof. Same logic as above (throw in roots of irreducible polynomials, one at a time), but the details get a bit tedious, so we omit them. □

Example 1.2.43. The algebraic closure of $\mathbb{R}$ is (isomorphic to) $\mathbb{C}$.

Example 1.2.44. The algebraic closure of $\mathbb{Q}$ is **NOT** $\mathbb{C}$, which is not an algebraic extension of $\mathbb{Q}$ (i.e. way too big), but rather (isomorphic to)

$$\overline{\mathbb{Q}} = \{\alpha \in \mathbb{C} \mid \alpha \text{ algebraic over } \mathbb{Q}\}.$$

1.3 Finite fields

1.3.1 The characteristic of a field

Definition 1.3.1. Let R be a ring. The *characteristic* of R is the non-negative integer c such that the kernel of the ring morphism

$$\begin{array}{ccc} \mathbb{Z} & \longrightarrow & R \\ n & \longmapsto & \underbrace{1 + \cdots + 1}_{n \text{ times}} \end{array}$$

is $c\mathbb{Z}$.

In other words, it is the smallest integer n such that $\underbrace{1 + \cdots + 1}_{n \text{ times}} = 0$, or 0 if there is no such n.

Example 1.3.2. The characteristic of $\mathbb{Z}/n\mathbb{Z}$ is n. The characteristic of $\mathbb{R}[x]$ is 0.

Remark 1.3.3. If R is finite, then $\operatorname{char} R \neq 0$; indeed, $\mathbb{Z} \longrightarrow R$ cannot be injective.

Proposition 1.3.4. *If R is a domain (in particular, if R is a field), then* $\operatorname{char} R = 0$ *or is a prime number.*

Proof. Suppose $\operatorname{char} R = ab$. Then

$$0 = \underbrace{1 + \cdots + 1}_{ab \text{ times}} = (\underbrace{1 + \cdots + 1}_{a \text{ times}})(\underbrace{1 + \cdots + 1}_{b \text{ times}})$$

so $a = ab$ or $b = ab$ since R is a domain. □

Remark 1.3.5. Conversely, the examples $\operatorname{char}\mathbb{Q} = 0$ and $\operatorname{char}\mathbb{Z}/p\mathbb{Z} = p$ for any prime $p \in \mathbb{N}$ show that all these cases occur, even if we restrict ourselves to fields.

Definition 1.3.6. Let K be a field. The *prime subfield* of K is the smallest subfield of K, i.e. that generated by 0 and 1.

Proposition 1.3.7. *Let K be a field.*

1. *If $\operatorname{char} K = 0$, then K contains a copy of $\mathbb{Q}$.*
2. *If $\operatorname{char} K = p$, then K contains a copy of $\mathbb{Z}/p\mathbb{Z}$.*

Proof. Consider the prime subfield of K. □

In summary, if K is a finite field, then $\operatorname{char} K = p \neq 0$ is a prime number, and K contains a copy of the field $\mathbb{Z}/p\mathbb{Z}$. Therefore K is a (necessarily) finite extension of $\mathbb{Z}/p\mathbb{Z}$.

Theorem 1.3.8. *If K is a finite field, then there exists $d \in \mathbb{N}$ such that $\#K = p^d$, where $p = \operatorname{char} K$.*

Proof. We know that K is a finite extension of $\mathbb{Z}/p\mathbb{Z}$. Let $d = [K : \mathbb{Z}/p\mathbb{Z}]$. Then $K \simeq (\mathbb{Z}/p\mathbb{Z})^d$ as $(\mathbb{Z}/p\mathbb{Z})$-vector spaces; in particular, they have the same cardinal. □

Example 1.3.9. There does not exist a field with 6 elements.

1.3.2 The Frobenius

Proposition 1.3.10. *Let R be a commutative ring such that $\operatorname{char} R$ is a prime number p. Then*

$$(a+b)^p = a^p + b^p$$

for all $a, b \in R$.

Proof. Since $(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k}$, if suffices to prove that $p \mid \binom{p}{k}$ for $0 < k < p$. And indeed $p \mid p! = \binom{p}{k} k!(p-k)!$, but $p \nmid k!$ nor $(p-k)!$. □

Corollary 1.3.11. *If $\operatorname{char} R = p$, then the* Frobenius map

$$\text{Frob} : \begin{array}{ccc} R & \longrightarrow & R \\ x & \longmapsto & x^p \end{array}$$

is a ring morphism.

Proof. The identities $\mathrm{Frob}(xy) = \mathrm{Frob}(x)\,\mathrm{Frob}(y)$, $\mathrm{Frob}(0) = 0$, and $\mathrm{Frob}(1) = 1$ are all clear, and the fact that $\mathrm{Frob}(x+y) = \mathrm{Frob}(x) + \mathrm{Frob}(y)$ is proposition 1.3.10. □

Example 1.3.12. Take $R = (\mathbb{Z}/p\mathbb{Z})[x]$. By Fermat's little theorem, $a^p = a$ for all $a \in \mathbb{Z}/p\mathbb{Z}$, so that $\mathrm{Frob}\big(F(x)\big) = F(x^p)$ for all $F(x) \in R$.

1.3.3 Structure of finite fields

Theorem 1.3.13. *Let K be a field. Any finite subgroup of the multiplicative group $K^\times$ is cyclic.*

Corollary 1.3.14. *If K is a finite field with p^d elements, then*

1. $(K, +) \simeq (\mathbb{Z}/p\mathbb{Z})^d$*; in particular,* $\mathrm{char}\, K = p$*,*
2. $(K^\times, \times) \simeq \mathbb{Z}/(p^d - 1)\mathbb{Z}$*.*
3. $\mathrm{Frob} \in \mathrm{Aut}(K)$*.*

Proof.

1. results from the fact that $K \simeq (\mathbb{Z}/p\mathbb{Z})^d$ as $(\mathbb{Z}/p\mathbb{Z})$-vector spaces, so in particular as additive groups.
2. is a consequence of theorem 1.3.13.
3. We already know from corollary 1.3.11 that Frob is a field morphism from K to itself; as such, it is injective by proposition 1.1.2. Since K is finite, it must also be surjective.

□

Corollary 1.3.15 (Primitive element theorem for finite fields)**.** *If $K \subseteq L$ is an extension of finite fields*[3]*, then there exists $\alpha \in L$ such that $L = K(\alpha)$.*

Proof. Take $\alpha \in L$ to be a generator of the cyclic group $L^\times$. Then every element of $L^\times$ is a polynomial in (actually, a power of) α, and so is 0 (take the 0 polynomial). □

[3]Not to be confused with a finite field extension!

Lemma 1.3.16. *Let K be a finite field with q elements. Then $x^q = x$ for all $x \in K$.*

Proof. If $x = 0$, this is clear; else, $x \in K^\times$ which is a group of order $q - 1$, so $x^{q-1} = 1$ by Lagrange. □

Lemma 1.3.17. *Let K be a field, and let $\sigma : K \longrightarrow K$ be a field automorphism of K. Then $\{\alpha \in L \mid \sigma(\alpha) = \alpha\}$ is a subfield of K.*

Proof. Routine verification. □

Armed with these results, we can now state and prove the fundamental theorem about the structure of finite fields:

Theorem 1.3.18.

1. *The number of elements of a finite field is a prime power.*
2. *For each prime power $q = p^d$, there exists a finite field with q elements.*
3. *Two finite fields with the same number of elements are isomorphic.*
4. *Let K and L be two finite fields. Then L contains a copy of K iff. $\#L$ is a power of $\#K$.*

In view of this theorem, it is legitimate to use the notation $\mathbb{F}_q$ to denote "the" (unique up to isomorphism) finite field with q elements when q is a prime power. We shall do so from now on; in particular, we now write $\mathbb{F}_p$ for $\mathbb{Z}/p\mathbb{Z}$.

Proof. 1. Already seen (theorem 1.3.8).

2. Let $q = p^d$, and let $\overline{\mathbb{F}_p}$ be an algebraic closure of $\mathbb{F}_p$ (this exits and is unique up to isomorphism by theorem 1.2.42). In view of lemma 1.3.16, let us consider the subset

$$Z_q = \{\alpha \in \overline{\mathbb{F}}_p \mid \alpha^q = \alpha\}.$$

We are going to prove that Z_q is a subfield of $\overline{\mathbb{F}}_p$ with q elements.

First, Z_q is the set of roots in $\overline{\mathbb{F}}_p$ of the polynomial $F(x) = x^q - x$. Since $\overline{\mathbb{F}}_p$ is algebraically closed, $F(x)$ splits into linear factors over $\overline{\mathbb{F}}_p$, i.e. has all of it roots there. Besides, $F'(x) = -1$ since $q = p^d = 0$

in $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p \subseteq \overline{\mathbb{F}}_p$, so F and F' are coprime, so all these roots are distinct. Thus $\#Z_q = q$.

Next, recall that

$$\text{Frob} : \begin{array}{ccc} \overline{\mathbb{F}}_p & \longrightarrow & \overline{\mathbb{F}}_p \\ \alpha & \longmapsto & \alpha^p \end{array} .$$

is a field morphism by corollary 1.3.14. Besides, for all $\alpha \in \overline{\mathbb{F}}_p$, the polynomial $x^p - \alpha$ has a root in the algebrically closeed field $\overline{\mathbb{F}}_p$, so Frob is also surjective. It is therefore an automorphism of $\overline{\mathbb{F}}_p$.

Define Φ_q to be the d-fold composition of Frob with itself, so that $\Phi_q(\alpha) = \alpha^{p^d} = \alpha^q$ for all $\alpha \in \overline{\mathbb{F}}_p$. Then Z_q is the set of fixed points of the automorphism Φ_q, so that it is a subfield of $\overline{\mathbb{F}}_p$ by lemma 1.3.17.

3. It suffices to prove that any finite field with q elements is isomorphic to the subfield Z_q of $\overline{\mathbb{F}}_p$ constructed above. Let K be such a field. Then K is a (necessarily finite) extension of its prime subfield $\mathbb{F}_p$, so by corollary 1.3.15 there exists $\alpha \in K$ such that $K = \mathbb{F}_p(\alpha)$. Since the extension $\mathbb{F}_p \subseteq K$ is finite, it is algebraic by 1.2.13, so we can consider the minimal polynomial $\mu_\alpha(x) \in \mathbb{F}_p[x]$ of α over $\mathbb{F}_p$, and by remark 1.2.30 there is an isomorphism $K = \mathbb{F}_p(\alpha) \simeq \mathbb{F}_p[x]/\big(\mu_\alpha(x)\big)$ sending α on the image of x. Since $\overline{\mathbb{F}}_p$ is algebraically closed, $\mu_\alpha(x)$ has (at least one) root in $\overline{\mathbb{F}}_p$, so lemma 1.2.29 grants us with an $\mathbb{F}_p$-morphism $f : K \longrightarrow \overline{\mathbb{F}}_p$, whose image is a subfield of $\overline{\mathbb{F}}_p$ of cardinal q. Therefore, every element of this image satisfies $\gamma^q = \gamma$ by lemma 1.3.16, so this image is contained in Z_q; it must therefore agree with Z_q since both have cardinal q. As a result, f induces an isomorphism between K and its image Z_q.

4. Write $\#K = q = p^d$ and $\#L = q' = p'^{d'}$. If $K \subseteq L$, then L is a K-vector space, so $\#L = \#K^{[L:K]}$. Conversely, suppose that $\#L$ is a power of $\#K$, i.e. that $p = p'$ and $d \mid d'$. Up to isomorphism, we have

$$K = Z_q = \{\alpha \in \overline{\mathbb{F}}_p \mid \Phi_q(\alpha) = \alpha\}, \qquad L = Z_{q'} = \{\alpha \in \overline{\mathbb{F}}_p \mid \Phi_{q'}(\alpha) = \alpha\},$$

and it is clear that $Z_q \subseteq Z_{q'}$ since $\Phi_{q'}$ is the (d'/d)-fold composition of Φ_q with itself.

□

1.3.4 Explicit construction

The easiest way to construct explicitly $\mathbb{F}_q$ given a prime power $q = p^d$ is to find an irreducible polynomial $P(x) \in \mathbb{F}_p[x]$ of degree d. Indeed, such a polynomial must exist (consider the minimal polynomial of α where $\mathbb{F}_p(\alpha) = \mathbb{F}_q$), and then $\mathbb{F}_p[x]/\big(P(x)\big)$ will be a field extension of $\mathbb{F}_p$ of cardinal $p^d = q$.

Example 1.3.19. Let us construct $\mathbb{F}_q$ for $p = 2$ and $d \leqslant 4$.

1. For $d = 1$, simply
$$\mathbb{F}_2 \simeq \mathbb{Z}/2\mathbb{Z}.$$

2. For $d = 2$, consider $P(x) \in \mathbb{F}_2[x]$ of degree 2. Then if $P(x)$ is reducible, it must split into two linear factors, so it must have a root. A quick search reveals that $x^2 + x + 1$ has no root in $\mathbb{F}_2$ (and in fact it is the only one), so it is irreducible and we have
$$\mathbb{F}_4 \simeq \mathbb{F}_2[x]/(x^2 + x + 1).$$

3. For $d = 3$, consider $P(x) \in \mathbb{F}_2[x]$ of degree 3. Then if $P(x)$ is reducible, it must split into three linear factors or a linear and a quadratic factor, so either way it must have a root. A quick search reveals that x^3+x+1 has no root in $\mathbb{F}_2$ (the only other possibility is $x^3 + x^2 + 1$), so it is irreducible and we have
$$\mathbb{F}_8 \simeq \mathbb{F}_2[x]/(x^3 + x + 1).$$
Note that by theorem 1.3.18, $\mathbb{F}_8$ is **NOT** an extension of $\mathbb{F}_4$; indeed, actually the smallest field containing both $\mathbb{F}_4$ and $\mathbb{F}_8$ is $\mathbb{F}_{64}$.

4. Finally, let $P(x) \in \mathbb{F}_2[x]$ of degree 4. For $P(x)$ to be irreducible, it is necessary that it has no roots in $\mathbb{F}_2$, but in degree 4 this is no longer sufficient since $P(x)$ could also be a product of two irreducible factors of degree 2. Fortunately, we have seen that the only irreducible of degree 2 is $x^2 + x + 1$, so if $P(x)$ has no roots and is not equal to $(x^2+x+1)^2 = x^4+x^2+1$ (this identity follows from example 1.3.12), then it is irreducible. Thus for instance x^4+x+1 is irreducible, so that
$$\mathbb{F}_{16} \simeq \mathbb{F}_2[x]/(x^4 + x + 1).$$

Remark 1.3.20. We will see how to factor mod p polynomials of low degree thanks to proposition 3.3.6 below.

Chapter 2

The Galois correspondence

2.1 The global picture

Field automorphisms play a prominent rôle in Galois theory, so let u begin by a quick word about them.

Definition 2.1.1 ((Reminder))**.** Let $K \subseteq L$ be a field extension. Recall that A K-*automorphism* of L is an field automorphism $\sigma \in \mathrm{Aut}(L)$ satisfying $\sigma(x) = x$ for all $x \in K$.

The K-automorphisms of L for a subgroup of the group $\mathrm{Aut}(L)$ of all field automorphisms of L under composition, denoted by

$$\mathrm{Aut}_K(L) = \{\sigma \in \mathrm{Aut}(L) \mid \sigma_{|K} = \mathrm{Id}\}.$$

Remark 2.1.2. Suppose that $L = K(\alpha_1, \cdots, \alpha_r)$ for some $\alpha_1, \cdots, \alpha_r \in L$. Then the map

$$\begin{array}{ccc} \mathrm{Aut}_K(L) & \longrightarrow & L^r \\ \sigma & \longmapsto & \big(\sigma(\alpha_1), \cdots, \sigma(\alpha_r)\big) \end{array}$$

is injective, in other words, an element $\sigma \in \mathrm{Aut}_K(L)$ is completely determined by its behaviour on the generators $\alpha_1, \cdots, \alpha_r$ of L. Indeed, every element of $L = K(\alpha_1, \cdots, \alpha_r)$ is of the form

$$\beta = \frac{\displaystyle\sum_{i_1, \cdots, i_r} a_{i_1, \cdots, i_r} \alpha_1^{i_1} \cdots \alpha_r^{i_r}}{\displaystyle\sum_{i_1, \cdots, i_r} b_{i_1, \cdots, i_r} \alpha_1^{i_1} \cdots \alpha_r^{i_r}}$$

where the $a_{i_1,\cdots,i_r}$ and the $b_{i_1,\cdots,i_r}$ lie in K, so that

$$\sigma(\beta) = \frac{\sum_{i_1,\cdots,i_r} \sigma(a_{i_1,\cdots,i_r})\sigma(\alpha_1^{i_1}\cdots\alpha_r^{i_r})}{\sum_{i_1,\cdots,i_r} \sigma(b_{i_1,\cdots,i_r})\sigma(\alpha_1^{i_1}\cdots\alpha_r^{i_r})} = \frac{\sum_{i_1,\cdots,i_r} a_{i_1,\cdots,i_r}\sigma(\alpha_1)^{i_1}\cdots\sigma(\alpha_r)^{i_r}}{\sum_{i_1,\cdots,i_r} b_{i_1,\cdots,i_r}\sigma(\alpha_1^{i_1})\cdots\sigma(\alpha_r)^{i_r}}$$

is completely determined by the values $\sigma(\alpha_1),\cdots,\sigma(\alpha_r)$.

In particular, suppose that L is the splitting field over K of a polynomial $F(x) \in K[x]$ without multiple roots (we will see in theorem 2.4.3 below that this is a particularly interesting case), and that $\alpha_1,\cdots,\alpha_r$ are the roots of F in L (and re therefore distinct from each other). Then a K-automorphism $\sigma \in \mathrm{Aut}_K(L)$ is determined by its behaviour on the α_i as above; further more, $\sigma(\alpha_i) = \alpha_j$ is also a root of F for each i by lemma 1.2.25. We thus get an injective morphism from $\mathrm{Aut}_K(L)$ into the group of permutations of the roots of F. In other words, **the automorphisms of a splitting field can be represented by permutations of the roots**.

This mode of representation of automorphisms is extremely useful, both for conceptual understanding and for practical computations.

Finally, we note that if K_0 is the prime subfield (cf. definition 1.3.6) of K, then any automorphism of L induces the identity on K_0, and is therefore automatically a K_0-morphism. Indeed, K_0 is generated by 0 and 1, and any field automorphism fixes these elements. In particular, in the case $K = K_0$ (that is to say $K = \mathbb{Q}$ in characteristic 0, and $K = \mathbb{F}_p$) in characteristic p), then $\mathrm{Aut}_K(L)$ is simply $\mathrm{Aut}(L)$.

We can now give an example of Galois theory.

Example 2.1.3. Consider the extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$. It is the splitting field of $F(x) = (x^2-2)(x^2-3) \in \mathbb{Q}[x]$, so any $\mathbb{Q}$-automorphism of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ must permute its roots $\pm\sqrt{2},\pm\sqrt{3}$. Besides, such an automorphism must send $\sqrt{2}$ to a root of $x^2-2 \in \mathbb{Q}[x]$ by lemma 1.2.25, and conversely corollary 1.2.38 grants us with an automorphism σ such that $\sigma(\sqrt{2}) = -\sqrt{2}$, and thus $\sigma(-\sqrt{2}) = \sqrt{2}$; besides $\sigma(\sqrt{3}) = \pm\sqrt{3}$ since it must be a root of $x^2-3 \in \mathbb{Q}[x]$. Similarly, there exists an automorphism τ such that $\tau(\sqrt{3}) = -\sqrt{3}$, and thus $\tau(-\sqrt{3}) = \sqrt{3}$. After composing these automorphisms with themselves, we may assume that

$$\sigma(\sqrt{2}) = -\sqrt{2}, \quad \sigma(-\sqrt{2}) = \sqrt{2}, \quad \sigma(\sqrt{3}) = \sqrt{3}, \quad \sigma(-\sqrt{3}) = -\sqrt{3},$$

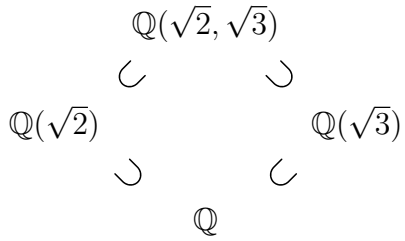
$$\tau(\sqrt{2}) = \sqrt{2}, \quad \tau(-\sqrt{2}) = -\sqrt{2}, \quad \tau(\sqrt{3}) = -\sqrt{3}, \quad \tau(-\sqrt{3}) = \sqrt{3};$$

in other words, σ moves $\sqrt{2}$ but not $\sqrt{3}$, and vice-versa for τ.

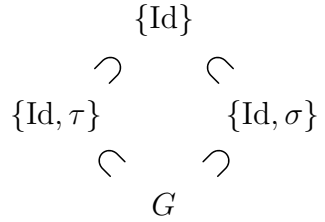
Since the elements of $\mathrm{Aut}_{\mathbb{Q}}\left(\mathbb{Q}(\sqrt{2},\sqrt{3})\right)$ are characterised by how they permute the roots $\pm\sqrt{2}$, $\pm\sqrt{3}$ of $F(x)$, we see that σ and τ have order 2, and that $\sigma\tau = \tau\sigma$. Thus the automorphism group (under composition) spanned by σ and τ is

$$\begin{array}{rccc} G = & \{\mathrm{Id}, \sigma, \tau, \sigma\tau\} & \simeq & \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \\ & \mathrm{Id} & \longmapsto & (0,0) \\ & \sigma & \longmapsto & (1,0) \\ & \tau & \longmapsto & (0,1) \\ & \sigma\tau & \longmapsto & (1,1). \end{array}$$

Consider now the following diagram of intermediate field extensions:



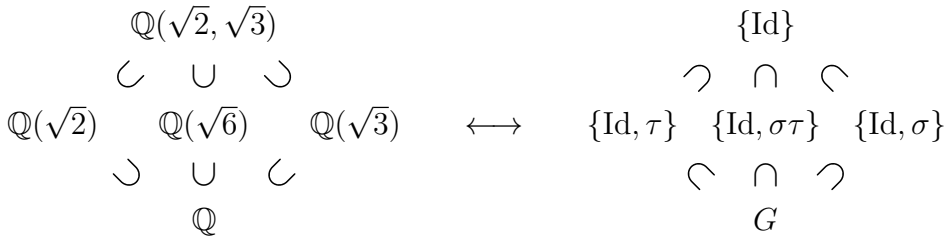
and the following diagram, which shows subgroups of G:



The key observation is that these diagrams are exact mirrors of each other: each subgroup of G corresponds to the subfield of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ fixed point-wise by its elements. We thus have an illustration of the *Galois correspondence*: a correspondence between subgroups and subfields.

Thanks to this correspondence, we can turn (difficult) problems of field theory in to (easier) problems of group theory. For instance, we forgot to include the subgroup $\{\mathrm{Id}, \sigma\tau\}$ in our subgroup diagram, so we must have forgotten a subfield in our subfield diagram. Namely, $\sigma\tau = \tau\sigma$ turns both $\sqrt{2}$

and $\sqrt{3}$ into their negatives, so it fixes $\sqrt{2}\sqrt{3} = \sqrt{6}$; the missing subfield is thus $\mathbb{Q}(\sqrt{6})$.



Furthermore, we will see that since there are no more subgroups of G, there are no more subfields between $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2},\sqrt{3})$.

In this example, all works out very nicely, but this is only because the extension $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{2},\sqrt{3})$ enjoys nice properties (it is a *Galois extension*, cf. below). Namely, it has sufficiently many automorphisms (to be precise, $\#G = 4 = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}]$...) so that only the elements of $\mathbb{Q}$ are fixed by all these automorphisms. In what follows, we will shed lights on two conditions that an extension must satisfy in order to be Galois, i.e. to have enough automorphisms: *separability*, and *normality*.

2.2 Characteristic p phenomena: inseparability

Proposition 2.2.1. *Let K be a field, and let $F(x) \in K[x]$ be a polynomial. The following conditions are equivalent:*

(i) *$F(x)$ and $F'(x)$ have a common factor in $K[x]$,*

(ii) *$F(x)$ and $F'(x)$ have a common root in some extension of K,*

(iii) $\operatorname{disc} F = 0$.

Proof. Obviously (i) $\Longrightarrow$ (ii), and conversely (ii) $\Longrightarrow$ (i) follows from the consideration of the minimal polynomial of a common root of F and F'. Finally, (ii) $\Longleftrightarrow$ (iii) is corollary 1.1.18. $\square$

Definition 2.2.2. A polynomial is said to be *inseparable* if it satisfies the conditions of proposition 2.2.1, and *separable* else.

In other words, $F(x)$ is separable if it has "no repeated root" (even after enlarging K).

Definition 2.2.3. Let L/K be an algebraic extension, and let $\alpha \in L$.

1. α is *separable over* K if its minimal polynomial over K is separable.
2. The extension $K \subseteq L$ is *separable* if all the elements of L are separable over K.

This definition feels weird: how could a minimal polynomial have multiple roots? Surely, it must be squarefree since it is irreducible, right? Well, in characteristic 0 this is true, but there is a catch in characteristic p. To see this, let us first establish

Lemma 2.2.4 (Factorisation of $x^p - a$ in characteristic p)**.** *Let K be a field of characteristic p, let $a \in K$, and let $F(x) = x^p - a$.*

1. *If there exists $b \in K$ such that $a = b^p$, then $F(x)$ factors as*

$$F(x) = (x - b)^p$$

   in $K[x]$.

2. *If there exists no such b, then $F(x)$ is irreducible in $K[x]$.*

Proof.

1. Immediate by proposition 1.3.10.
2. Let $P(x) \in K[x]$ be a non-constant factor of $F(x)$, and let b be a root of $F(x)$ in its splitting field. Then $F(x) = (x - b)^p$ as in the previous case, so $P(x) = (x - b)^n$ for some $1 \leqslant n \leqslant p$. Then the coefficient of x^{n-1} of $Q(x)$, which lies in K, is nb, whereas $b \notin K$ by assumption since $b^p = a$. Therefore we must have $n = 0$ in K, which forces $n = p$.

□

Example 2.2.5. Thanks to this result, we can give an example of an inseparable extension in characteristic p: let $K = \mathbb{F}_p(t)$ be the field of rational fractions in the indeterminate t over $\mathbb{F}_p$, and let $L = \mathbb{F}_p(t^{1/p})$, in other words, $L = K(u)$ where u is a root of $P(x) = x^p - t \in K[x]$. The p-th powers in K are the rational fractions in t^p (cf. example 1.3.12), so t is not a p-th power in K; therefore $P(x)$ is the minimal polynomial of u over K by lemma 2.2.4; but over L, this minimal polynomial factors as $P(x) = (x-u)^p$.

Remark 2.2.6. This example shows that the notion of being squarefree depends on the field over which one considers the polynomial. On the other hand, the notion of being separable does not, since it can be characterised by the discriminant not vanishing.

Remark 2.2.7. In the example, $L = K(u)$ is the splitting field of $P(x) = x^p - t \in K[x]$ over K, so the elements of $\mathrm{Aut}_K(L)$ are determined by their behaviour on the roots of P in L. However, u is the only such root as we have $P(x) = (x-u)^p$ over L; therefore the only element of $\mathrm{Aut}_K(L)$ is the identity. This is bad for Galois, since for instance $u \in L$ is fixed by all the elements of $\mathrm{Aut}_K(L)$ even though $u \notin K$.

In fact, example 2.2.5 is the generic example of inseparability:

Proposition 2.2.8. *Let K be a field of characteristic p, and let $P(x) \in K[x]$ be irreducible over K. The following are equivalent:*

(i) $P(x)$ *is inseparable,*

(ii) $P'(x) = 0$,

(iii) $P(x)$ *is a polynomial in* x^p.

Proof.

- (i) $\Longrightarrow$ (ii): If P is inseparable, then P and P' have a common factor, which can only P as P is irreducible, which forces $P' = 0$ since $\deg P' < \deg P$.
- (ii) $\Longrightarrow$ (iii): Write $P(x) = \sum_i a_i x^i$. Then $0 = P'(x) = \sum_i i a_i x^{i-1}$, so $ia_i = 0$ for all i, which means $a_i = 0$ unless $i = 0$ in K, i.e. unless $p \mid i$.

- (iii) $\Longrightarrow$ (i): If $P(x) = \sum_i a_i x^{pi}$, then $P'(x) = \sum_i pia_i x^{pi-1} = 0$ since $p = 0$ in K, so P and P' have a common factor, namely P itself.

□

Remark 2.2.9. Let $K \subseteq L$ be a separable extension, and let $K \subseteq E \subseteq L$ be an intermediate extension. Then $K \subseteq E$ is also separable (by definition), and so is $E \subseteq L$; indeed, for all $\alpha \in L$, the minimal polynomial $P_E(x) \in E[x]$ of α over E divides that $P_K(x) \in K[x]$ of α over K, and therefore P_E cannot have a multiple root (in any any extension of E) since P_K does not have any multiple root (in any extension of K).

Definition 2.2.10. A field K is *perfect* if all its algebraic extensions are separable.

As one may expect, inseparability and imperfection only come to annoy us in characteristic p:

Theorem 2.2.11.

1. *All fields of characteristic 0 are perfect.*
2. *A field of characteristic p is perfect if and only if the Frobenius*

$$\text{Frob} : \begin{array}{ccc} K & \longrightarrow & K \\ x & \longmapsto & x^p \end{array}$$

is surjective.

Remark 2.2.12. The Frobenius, being a field morphism, is always injective, so it is surjective if and only if it is an automorphism. In particular, **finite fields are all perfect**, even though they have positive characteristic. This explains why we had to make the complicated choice $K = \mathbb{F}_p(t)$ in example 2.2.5.

Proof.

1. Suppose K is not perfect. Then K has an inseparable extension L, so there exists $\alpha \in L$ whose minimal polynomial $P(x) \in K[x]$ over K is inseparable, whcih means that P and P' have a common factor. Since P is also irreducible, this common factor can only be P, so $P \mid P'$, whence $P' = 0$ by considering the degrees (same argument as the proof of proposition 2.2.8); but this cannot happen in characteristic 0.

2. If Frob is not surjective, then there exists $\in K$ which is not a p-th power, and then, as in example 2.2.5, the polynomial $P(x) = x^p - a$ is irreducible over K by lemma 2.2.4, and inseparable since $P' = 0$, so the extension $L = K[x]/\big(P(x)\big)$ of K is inseparable.

   Conversely, if Frob is surjective, then it is bijective, so every $a \in K$ admits a (unique) p-th root, namely $a^{1/p} = \mathrm{Frob}^{-1}(a)$. If K were not perfect, then as above there would exist an inseparable irreducible polynomial $P(x) \in K[x]$, which by proposition 2.2.8 would be of the form

$$P(x) = \sum_i a_i x^{pi}$$

   with $a_i \in K$. But then we would have

$$P(x) = \sum_i (a_i^{1/p})^p x^{pi} = \left(\sum_i a_i x^i \right)^p$$

   by proposition 1.3.10 since we are in characteristic p, which contradicts the fact that $P(x)$ is irreducible over K.

□

From now on, we fix a field K and an algebraically closed extension Ω of K (for instance its algebraic closure).

Theorem 2.2.13. *If $[L : K] < \infty$, then the set of K-morphisms $\mathrm{Hom}_K(L, \Omega)$ is finite, and its cardinal $N = \#\,\mathrm{Hom}_K(L, \Omega)$ satisfies*

$$1 \leqslant N \leqslant [L : K],$$

with equality $N = [L : K]$ if and only if the extension $K \subseteq L$ is separable.

Proof. We are going to construct K-morphisms $\iota : L \longrightarrow \Omega$ by starting by defining $\iota(x) = x$ on K, and enlarging our definition of ι to larger and larger extensions of K until we get to L. To keep track of our progress, we write $L = K(\alpha_1, \cdots, \alpha_r)$ where the $\alpha_i \in L$ (for instance, we could take α_i forming a K-basis of L), and we do an induction on r.

If $r = 0$, then $L = K$ and the only possible ι is the identity, so there is nothing to do.

Suppose now $r \geqslant 1$, and let $E = K(\alpha_1, \cdots, \alpha_{r-1})$, so that $L = E(\alpha_r)$. By induction hypothesis, the number $N_E = \#\operatorname{Hom}_K(E, \Omega)$ satisfies $N_E \leqslant [E : K]$, with equality if and only if $K \subseteq E$ is separable.

Let $P(x) \in E[x]$ be the minimal polynomial of α_r over E, so that we have an E-isomorphism

$$L = E(\alpha_r) \simeq E[x]/\big(P(x)\big).$$

Pick a $\iota \in \operatorname{Hom}_K(E, \Omega)$, let $P_\iota(x) \in \Omega[x]$ be the polynomial obtained by applying ι to the coefficients of P, and let N_ι be the number of roots of P_ι in Ω, so that

$$N_\iota \leqslant \deg P_\iota = \deg P = [L : E]$$

with equality if and only if P_ι is separable.

If $\iota' : L \to \Omega$ is a hypothetical extension of ι, then $\iota'(\alpha_r)$ must necessarily be one of the N_ι roots of P_ι in Ω by lemma 1.2.25. Conversely, given such a root $\beta \in \Omega$, then by lemma 1.2.29, the ring morphism $\operatorname{eval}_\beta : E[x] \longrightarrow \Omega$ factors into

$$\begin{array}{ccc} E[x] & \xrightarrow{\operatorname{eval}_\beta} & \Omega \\ \big\downarrow & \overset{\iota'}{\nearrow} & \\ L \simeq E[x]/\big(P(x)\big) & & \end{array}$$

where $\iota' \in \operatorname{Hom}_K(L, \Omega)$ extends ι. The number of ι' extending ι is therefore $N_\iota \leqslant [L : E]$; since the number N_E of ι is $\leqslant [E : K]$ by induction hypothesis, we have

$$N = \#\operatorname{Hom}_K(L, \Omega) \leqslant [E : K][L : E] = [L : K]$$

by proposition 1.2.16.

If we furthermore assume that $K \subseteq L$ is separable, then so are $K \subseteq E$ and $E \subseteq L$ by remark 2.2.9, whence $N_E = [E : K]$ and the fact that P is separable, so that $\operatorname{disc} P \neq 0$. Since $\operatorname{disc} P_\iota = \iota(\operatorname{disc} P)$ as the discriminant is a determinant in the coefficients of the polynomial, and since ι, being a field morphism, is injective, we also have $\operatorname{disc} P_\iota \neq 0$, so P_ι is separable, whence $N_\iota = \deg P_\iota = [L : E]$, so all the inequalities above are equalities and we get $N = [L : K]$.

Conversely, if $K \subseteq L$ is not separable, then we can suppose without loss of generality that α_1 is not separable over K. Then E is not separable over K, so $N_E < [E : K]$ by induction hypothesis, whence $N \leqslant N_E[L : E] < [L : K]$, and the induction is complete. □

Remark 2.2.14. By the same arguments, we see that if $K \subseteq E \subseteq L$ are extensions such that $K \subseteq E$ and $E \subseteq L$ are separable, then so is $K \subseteq L$. This is a converse to remark 2.2.9. In particular, the splitting field of a separable polynomial is a separable extension.

Example 2.2.15. Let $K = \mathbb{Q} \subseteq L = \mathbb{Q}(\sqrt[3]{2})$. This is a separable extension (since we are in characteristic 0) of degree 3, so we mut have 3 distinct embedding of L into $\Omega = \mathbb{C}$. Indeed, $L \simeq \mathbb{Q}[x]/(x^3 - 2)$, and lemma 1.2.29 grants us with 3 embeddings of $\mathbb{Q}[x]/(x^3 - 2)$ into $\mathbb{C}$ since $x^3 - 2$ has 3 roots in $\mathbb{C}$.

2.3 Normal extensions

Unlike separability, which may be regarded as a technical condition since it is only a problem in characteristic p, *normality* is a property that fails for many "reasonable extensions".

Definition 2.3.1 (Reminder: group actions)**.** Let G be a group with identity $1_G \in G$, and let X be a set.

1. A *left action of G on X* is a map

$$\begin{array}{ccc} G \times X & \longrightarrow & X \\ (g, x) & \longmapsto & g \cdot x \end{array}$$

   such that $g \cdot h \cdot x = gh \cdot x$ and $1_G \cdot x = x$ for all $g, h \in G$ and $x \in X$ (in other words, it is a group morphism from G into the group of bijections from X to itself).

2. A *right action of G on X* is a map

$$\begin{array}{ccc} X \times G & \longrightarrow & X \\ (x, g) & \longmapsto & x \cdot g \end{array}$$

   such that $x \cdot g \cdot h = x \cdot gh$ and $x \cdot 1_G = x$ for all $g, h \in G$ and $x \in X$ (in other words, it is a group "anti-morphism", i.e $\phi(gh) = \phi(h)\phi(g)$, from G into the group of bijections from X to itself).

   In what follows, we only consider left actions to simplify notations, but the definition still make sense for right actions.

3. Let $x \in X$. The *orbit* of x is the subset $G \cdot x = \{g \cdot x \mid g \in G\} \subseteq X$. The *stabiliser* G_x of x is the subgroup $\{g \in G \mid g \cdot x = x\} \subseteq G$.

4. The action is *transitive* if for all $x, y \in X$, there exists $g \in G$ such that $g \cdot x = y$, i.e. if there is only one orbit.

5. The action is *free* if $\forall x \in X$, $\forall g \in G, g \neq 1_G \Longrightarrow g \cdot x \neq x$.

Example 2.3.2. A Rubik's cube is not a group, but rather a set of configurations acted on by a group of rotations of the faces. This action is free. It is transitive if and only if we only include the configurations of the cube that are reachable without taking the cube apart in our set of configurations.

We observe that we have a right action of the group $\mathrm{Aut}_K(L)$ of K-automorphisms of L on the set $\mathrm{Hom}_K(L, \Omega)$ of K-morphisms from L to Ω, defined by

$$\iota \cdot \sigma = \iota \circ \sigma \qquad \big(\iota \in \mathrm{Hom}_K(L, \Omega),\ \sigma \in \mathrm{Aut}_K(L)\big).$$

Moreover, this action is free, as $\iota \circ \sigma = \iota$ implies $\sigma = \mathrm{Id}$ since ι is injective.

We suppose from now on that $[L : K] < \infty$. Then we know from theorem 2.2.13 that $\mathrm{Hom}_K(L, \Omega)$ is a finite set; since the action of $\mathrm{Aut}_K(L)$ is free, we deduce the inequality

$$\#\,\mathrm{Aut}_K(L) \leqslant \#\,\mathrm{Hom}_K(L, \Omega).$$

Definition 2.3.3. The extension $K \subseteq L$ is *normal* if we have the equality

$$\#\,\mathrm{Aut}_K(L) = \#\,\mathrm{Hom}_K(L, \Omega).$$

Example 2.3.4. Consider the extension $K = \mathbb{Q} \subseteq L = \mathbb{Q}(\sqrt[3]{2})$. An element of $\sigma \in \mathrm{Aut}_K(L)$ is completely determined by the value $\sigma(\sqrt[3]{2}) \in L$, which must be a root of $P(x) = x^3 - 2 \in \mathbb{Q}[x]$ by lemma 1.2.25. But we saw in example 1.2.23 that $\sqrt[3]{2}$ is the only root of $P(x)$ in L; therefore $\mathrm{Aut}_K(L)$ is reduced to the identity, so we have

$$\#\,\mathrm{Aut}_K(L) = 1 < 3 = \#\,\mathrm{Hom}_K(L, \mathbb{C})$$

(where the last equality follows from example 2.2.15), i.e. the extension $K \subseteq L$ is not normal. This is annoying because as mentioned in remark 2.2.7, the lack of automorphisms is bad for Galois: for instance $\sqrt[3]{2} \in L$ is fixed by all the elements of $\mathrm{Aut}_K(L)$, even though it does not lie in K. More precisely, unlike in example 2.2.5 the problem is not that P has too few roots, but that too few of these roots lie in L.

Theorem 2.3.5. *Let $K \subseteq L$ be a finite extension. The following are equivalent:*

(i) The extension $K \subseteq L$ is normal,

(ii) The free right action of $\mathrm{Aut}_K(L)$ on $\mathrm{Hom}_K(L, \Omega)$ is also transitive,

(iii) The elements of $\mathrm{Hom}_K(L, \Omega)$ all have the same image,

(iv) For all irreducible $P(x) \in K[x]$, if $P(x)$ has a root in L, then $P(x)$ splits into linear factors over L,

(v) There exits $F(x) \in K[x]$ such that L is (isomorphic to) the splitting field of $F(x)$.

Proof.

- (i) $\iff$ (ii) is clear.
- (ii) $\implies$ (iii): If there exists $\iota \in \mathrm{Hom}_K(L, \Omega)$ such that the elements of $\mathrm{Hom}_K(L, \Omega)$ are all of the form $\iota \circ \sigma$ for some $\sigma \in \mathrm{Aut}_K(L)$, then their images all agree with that of ι.
- (iii) $\implies$ (ii): Let $\iota_1, \iota_2 \in \mathrm{Hom}_K(L, \Omega)$. since they are injective (as field morphisms) and have the same image (by assumption), the map $\sigma = \iota_2^{-1} \circ \iota_1$ is well-defined,lies in $\mathrm{Aut}_K(L)$, and satisfies $\iota_2 = \iota_1 \circ \sigma$.
- (iii) $\implies$ (iv): Let $I \subseteq \Omega$ be the common image of the elements of $\mathrm{Hom}_K(L, \Omega)$. Then $I \simeq L$ by any $\iota \in \mathrm{Hom}_K(L, \Omega)$, so it suffices to prove that if P has a root in I, then P splits into linear factors over I.

  Since $K \subseteq L$ is finite, there exist $\alpha_1, \cdots, \alpha_r$ such that $L = K(\alpha_1, \cdots, \alpha_r)$. For each i, let $P_i(x) \in K[x]$ be the minimal polynomial of α_i over K, let $F(x) \in K[x]$ be the lcm of the $P_i(x)$ and of P, and let S be the subfield of Ω generated over K by the roots of F in Ω, so that S is a splitting field of F over K. Since $I = K\big(\iota(\alpha_1), \cdots, \iota(\alpha_r)\big)$ for any $\iota \in \mathrm{Hom}_K(L, \Omega)$, and since $\iota(\alpha_i)$ is a root of P_i (and hence of F) by lemma 1.2.25, we have $I \subseteq S$. Let $\beta_1, \beta_2 \in S$ be two roots of P; we want to show that if $\beta_1 \in I$, then β_2 in I as well. Since P is irreducible over K, it is the minimal polynomial over K of both of β_1 and β_2, which are thus conjugate over K, so that corollary 1.2.38

grants us with $\Phi \in \mathrm{Aut}_K(S)$ such that $\Phi(\beta_1) = \beta_2$. But then for all $\iota \in \mathrm{Hom}_K(L, \Omega)$, we also have $\Phi \circ \iota \in \mathrm{Hom}_K(L, \Omega)$, which shows that $\Phi(I) = I$. Therefore, $\beta_2 = \Phi(\beta_1) \in \Phi(I) = I$.

- (iv) $\Longrightarrow$ (v): Again, write $L = K(\alpha_1, \cdots, \alpha_r)$, let $P_i(x) \in K[x]$ be the minimal polynomial of α_i over K, and let $F(x) \in K[x]$ be the lcm of the $P_i(x)$ (there is no P this time). Then by assumption the P_i all split into linear factors over L, hence so does F; since furthermore L is generated by the α_i over K, it is a fortiori generated by the roots of F over K, so L is a splitting field of F.

- (v) $\Longrightarrow$ (iii): Let $F(x) \in K[x]$ be such that L is a splitting field of F. Then for any $\iota \in \mathrm{Hom}_K(L, \Omega)$, $\iota(L) \subseteq \Omega$ is a splitting field of F contained in Ω, which necessarily agrees with the extension of K generated by the roots of F in Ω.

□

Corollary 2.3.6. *Let $K \subseteq L$ be a finite extension. There exists a finite extension $L \subseteq N$ such that $K \subseteq N$ is normal, and which is the smallest possible in the sense that if $L \subseteq E \subseteq N$ is normal, then $E = N$. This N is unique up to K-isomorphism. This N is called the* normal closure *of the extension $K \subseteq L$.*

Proof. As above, write $L = K(\alpha_1, \cdots, \alpha_r)$ with $\alpha_1, \cdots, \alpha_r$, let $P_i(x) \in K[x]$ be the minimal polynomial of α_i over K, and let $F(x) \in K[x]$ be the lcm of the $P_i(x)$. Then N must be the splitting field of F over K. Indeed, this is necessary by part (iv) of theorem 2.3.5, and also sufficient by part (v). □

Example 2.3.7. As in example 2.3.4, let $K = \mathbb{Q} \subseteq L = \mathbb{Q}(\sqrt[3]{2})$. This extension is not normal, indeed $P(x) = x^3 - 2 \in K[x]$ is irreducible over K, has a root in L, but does not split completely over L. Its normal closure is the splitting field $N = \mathbb{Q}(\sqrt[3]{2}, \zeta_3\sqrt[3]{2}, \zeta_3^2\sqrt[3]{2}) = L(\zeta_3)$ of $P(x)$ over K.

The following remark is sometimes useful when determining Galois groups (cf. next section):

Corollary 2.3.8. *Let $K \subseteq L$ be a normal extension. Suppose that there are teo intermediate fields $K \subseteq E_1, E_2 \subseteq L$ such that there exits a K-isomorphism $\sigma : E_1 \simeq E_2$. Then σ can be extended to (i.e. is the restriction of an element of)* $\mathrm{Aut}_K(L)$ *(in at least one way).*

Proof. Since the extension $K \subseteq L$ is normal, there exists $F(x) \in K[x]$ such that L is the splitting field of F over K. We can view F as an element of $E_1[x]$, and the polynomial obtained by applying σ to its coefficients is again $F \in E_2[x]$ since σ is a K-morphism. The result now follows from theorem 1.2.36. □

2.4 Galois extensions

We have proved the inequalities

$$\#\operatorname{Aut}_K(L) \leqslant \#\operatorname{Hom}_K(L, \Omega) \leqslant [L : K]. \tag{2.4.1}$$

For the Galois correspondence to work, we want as many automorphisms as possible; we therefore make the following definition:

Definition 2.4.2. The extension $K \subseteq L$ is *Galois* if it is separable and normal.

Let us introduce some notation: Given a subset (in practice, a subgroup) $H \subseteq \operatorname{Aut}_K(L)$, we write

$$L^H = \{\alpha \in L \mid \sigma(\alpha) = \alpha \ \forall \sigma \in H\} \subseteq L.$$

This is a *subfield* of L (routine verification; alternatively, invoke lemma 1.3.17).

Theorem 2.4.3. *Let $K \subseteq L$ be a finite extension. The following are equivalent:*

(i) The extension $K \subseteq L$ is Galois,

(ii) $\#\operatorname{Aut}_K(L) = [L : K]$,

(iii) There exists a separable *$F(x) \in K[x]$ such that L is a splitting field of K,*

(iv) For all $\alpha \in L$, the minimal polynomial of α over K is

$$\prod_{\beta \in \operatorname{Aut}_K(L)\cdot\alpha} (x - \beta),$$

where $\operatorname{Aut}_K(L) \cdot \alpha$ denotes the set $\{\sigma(\alpha) \mid \sigma \in \operatorname{Aut}_K(L)\}$ (without multiplicities),

(v) For all $\alpha \in L$, we have

$$\alpha \in K \iff \sigma(\alpha) = \alpha \ \forall \sigma \in \mathrm{Aut}_K(L);$$

in other words, the obvious inclusion $K \subseteq L^{\mathrm{Aut}_K(L)}$ is actually an equality.

Remark 2.4.4. In particular, (iv) implies that all the conjugates of α over K lie in L, and are the $\sigma(\alpha)$ for $\sigma \in \mathrm{Gal}(L/K)$.

Remark 2.4.5. Before we prove theorem 2.4.3, it is instructive to see how each of the points fail if the extension is not separable, e.g.

$$K = \mathbb{F}_p(t) \subseteq L = \mathbb{F}_p(t^{1/p}) \tag{A}$$

(cf. example 2.2.5), or if it is not normal, e.g. in the case

$$K = \mathbb{Q} \subseteq L = \mathbb{Q}(\sqrt[3]{2}) \tag{B}$$

(cf. example 2.3.4).

- Let $\alpha = t^{1/p}$ in the first case, and $\alpha = \sqrt[3]{2}$ in the second case, so that in both cases, we have $L = K(\alpha)$ for some $\alpha \in L$. In view of remark 2.1.2, this implies that an element $\sigma \in \mathrm{Aut}_K(L)$ is completely determined by the value $\sigma(\alpha)$. Furthermore, this value must be a root of the minimal polynomial of α over K by lemma 1.2.25, and lie in L since $\sigma \in \mathrm{Aut}_K(L)$. We have seen (respectively in remark 2.2.7 and in example 2.3.4) that this implies that in both cases, the only element of $\mathrm{Aut}_K(L)$ is the identity, so (ii) is violated since $[L : K] > 1$.

- In case (A), L is the splitting field of $x^p - t \in K[x]$, but this polynomial is not separable. In case (B), the polynomial $x^3 - 2$ is separable, but L is not its splitting field, only its stem field (cf. example 1.2.23); in fact, condition (iv) of theorem 2.3.5 is violated.

- We have seen that $\mathrm{Aut}_K(L)$ is reduced to the identity in both cases, so (iv) is violated since the minimal polynomial of α over K is not $x - \alpha$ (it is $(x - t^{1/p})^p \neq x - t^{1/p}$ in case (A), and $(x - \sqrt[3]{2})(x - \zeta_3\sqrt[3]{2})(x - \zeta_3^2\sqrt[3]{2}) \neq x - \sqrt[3]{2}$ in case (B)).

- Finally, in both cases α is fixed by every element of $\mathrm{Aut}_K(L)$ since the latter only contains the identity, yet $\alpha \notin K$ so (v) is violated.

We now prove theorem 2.4.3.

Proof of theorem 2.4.3.

- (i) $\iff$ (ii) is clear, since in (2.4.1) the first inequality is an equality iff. the extension is normal, and the second one iff. the extension is separable.

- (i) $\implies$ (iii): Since L is normal over K, then by theorem 2.3.5 there exists $F(x) \in K[x]$ such that L is the splitting field of F over K. Then all the roots of F are in L. For each such root α, the minimal polynomial of α divides F since $F(\alpha) = 0$, and is separable since $\alpha \in L$ is separable over K. Replacing if necessary F by the lcm of these minimal polynomials (i.e. "clearing multiplicities" in F), we may assume that F is separable.

- (iii) $\implies$ (i): If L is the splitting field of F over K, then it is normal over K by theorem 2.3.5. If furthermore F is separable, then L is also separable over K by remark 2.2.14.

- (ii) $\implies$ (v): Let $E = L^{\mathrm{Aut}_K(L)}$. Then E is a field such that $K \subseteq E \subseteq L$, so that $[L : E] \leqslant [L : K]$; besides $\mathrm{Aut}_E(L) = \mathrm{Aut}_K(L)$ by definition of E, so $[L : K] = \#\,\mathrm{Aut}_K(L) = \#\,\mathrm{Aut}_E(L) \leqslant [L : E]$ by (2.4.1), whence $[L : E] = [L : K]$, which forces $E = K$ by proposition 1.2.16.

- (v) $\implies$ (iv): Let $\alpha \in L$, let $P(x) \in K[x]$ be its minimal polynomial over K, and let us set

$$Q(x) = \prod_{\beta \in \mathrm{Aut}_K(L)\cdot\alpha} (x - \beta) \in L[x].$$

  Then the β are permuted transitively by $\mathrm{Aut}_K(L)$. As the coefficients of Q are symmetric polynomials in these β by proposition 1.1.8, they are therefore fixed by $\mathrm{Aut}_K(L)$, and therefore lie in K by assumption. So $Q \in K[x]$, so $P \mid Q$ since $Q(\alpha) = 0$. Besides, all roots of Q are also roots of P by lemma 1.2.25, so $Q \mid P$. Therefore $P = Q$ as they are both monic.

- (iv) $\implies$ (i) Let $\alpha \in L$. Then the minimal polynomial of α is by assumption $\prod_{\beta \in \mathrm{Aut}_K(L)\cdot\alpha}(x-\beta)$, whose roots are all ditinct; therefore α is separable over K. This shows that L is separable over K.

Let now $P(x) \in K[x]$ be irreducible over K and have a root α in L. Then P is the minimal polynomial of α over K, so again by assumption by assumption it splits completely in L, which shows that L is normal over K.

□

Example 2.4.6. The extension $K = \mathbb{Q} \subseteq L = \mathbb{Q}(\sqrt{2})$ is Galois, as it is the splitting field of the separable polynomial $F(x) = x^2 - 2 \in K[x]$.

By corollary 1.2.38, there exists $\sigma \in \mathrm{Gal}(L/K)$ such that $\sigma(\sqrt{2}) = -\sqrt{2}$; more specifically, we know that

$$L = \{a + b\sqrt{2} \mid a, b \in K\},$$

and σ is given by $a + b\sqrt{2} \mapsto a - b\sqrt{2}$. Thus σ has order 2 since the elements of $\mathrm{Gal}(L/K)$ are determined by their behaviour on the roots $\pm\sqrt{2}$ of $F(x)$ in L.

Besides, $\#\,\mathrm{Gal}(L/K) = [L : K] = 2$, so we see that

$$\mathrm{Gal}(L/K) = \{\mathrm{Id}, \sigma\} \simeq \mathbb{Z}/2\mathbb{Z}.$$

As an application, consider an element $\alpha = a + b\sqrt{2}$ of L. If $b \neq 0$, then it has two images under $\mathrm{Gal}(L/K)$, namely itself and its conjugate $\beta = a - b\sqrt{2}$, so it does not lie in L since it is not fixed by $\mathrm{Gal}(L/K)$, and its minimal polynomial over K is $(x - \alpha)(x - \beta)$, which does lie in $K[x]$ since it is invariant under $\mathrm{Gal}(L/K)$. But if $b = 0$, then α is fixed by $\mathrm{Gal}(L/K)$, and indeed lies in K; in particular its minimal polynomial over K is $x - \alpha$.

Example 2.4.7. The extension $K = \mathbb{Q} \subseteq L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ studied in example 2.1.3 is Galois since it is the splitting field of $(x^2 - 2)(x^2 - 3)$, so $\#\,\mathrm{Gal}(L/K) = [L : K] = 4$. Therefore, the group

$$G = \{\mathrm{Id}, \sigma, \tau, \sigma\tau\} \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$$

is the whole of $\mathrm{Gal}(L/K)$. The element $\sqrt{2} + \sqrt{3} \in L$ has 4 images under $\mathrm{Gal}(L/K)$ (= conjugates), namely $\pm\sqrt{2} \pm \sqrt{3}$, so its minimal polynomial over K is the polynomial of degree 4 having these 4 roots.

Remark 2.4.8. Let $K \subseteq L$ be an extension which is separable, but not necessarily normal. Then there exists a smallest extension $K \subseteq L \subseteq N$ such that N is Galois over K, namely the normal closure (cf. corollary 2.3.6) of L over K, which is rather called the *Galois closure* of L over K in this context. Indeed, this normal closure is still separable over K by remark 2.2.14.

Example 2.4.9. We have seen in example 2.3.4 that $L = \mathbb{Q}(\sqrt[3]{2})$ is not a normal extension of $K = \mathbb{Q}$. By example 2.3.7, its Galois closure is $N = L(\zeta_3)$, the splitting field of $F(x) = x^3 - 2 \in K[x]$. The Galois group $\mathrm{Gal}(N/K)$ permutes the 3 roots $\sqrt[3]{2}$, $\zeta_3\sqrt[3]{2}$, $\zeta_3^2\sqrt[3]{2}$ of $F(x)$ in N, and therefore injects into the symmetric group S_3. But

$$\#\,\mathrm{Gal}(N/K) = [N : K] = [N : L][L : K] = 6 = \#S_3,$$

whence

$$\mathrm{Gal}(N/K) \simeq S_3.$$

Finally, here is a more delicate example of Galois group computation.

Example 2.4.10. Let $\alpha = \sqrt{5 + \sqrt{21}}$ and $L = \mathbb{Q}(\alpha)$. We have

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt{21}) \subseteq L,$$

with $[\mathbb{Q}(\sqrt{21}) : \mathbb{Q}] = 2$ and $[L : \mathbb{Q}(\sqrt{21})] \leq 2$. If we had $[L : \mathbb{Q}(\sqrt{21})] = 1$, then we would have $\alpha = u + v\sqrt{21} \in L$ with $u, v \in \mathbb{Q}$, whence

$$5 + \sqrt{21} = (u + v\sqrt{21})^2 = u^2 + 21v^2 + 2uv\sqrt{21}$$

so that $u^2 + 21v^2 = 5$ and $2uv = 1$. This implies $u^4 - 5u^2 + 21/4 = 0$, whence $u^2 = \frac{5\pm 2}{2}$, which is absurd since $u \in \mathbb{Q}$. Therefore $[L : \mathbb{Q}(\sqrt{21})] = 2$ and $[L : \mathbb{Q}] = 4$.

The number α is a root of $P(x) = (x^2 - 5)^2 - 21 \in \mathbb{Q}[x]$, which has degree 4; it is therefore the minimal polynomial of α over $\mathbb{Q}$. The conjugates of α, namely the other roots of P, are $\alpha' = -\alpha$, $\beta = \sqrt{5 - \sqrt{21}}$, and $\beta' = -\beta$; therefore the splitting field of P over $\mathbb{Q}$ is $\mathbb{Q}(\alpha, \beta)$, and L is Galois over $\mathbb{Q}$ iff. $\beta \in L$. since actually $\alpha\beta = \sqrt{(5 + \sqrt{21})(5 - \sqrt{21})} = \sqrt{4} = 2 \in \mathbb{Q}$, we do have $\beta \in L$. Therefore L is Galois over $\mathbb{Q}$, and its Galois group $\mathrm{Gal}(L/K)$ is a subgroup of order $[L : \mathbb{Q}] = 4$ of the symmetric group on the 4 roots $\alpha, \alpha', \beta, \beta'$.

An element $\sigma \in \mathrm{Gal}(L/K)$ is completely determined by what it does to these roots, and thus by the value $\sigma(\alpha)$ since the other roots can be expressed in terms of α as $\beta = 2/\alpha$. In particular, if $\sigma(\alpha) = \alpha$ then $\sigma = \mathrm{Id}$. If $\sigma(\alpha) = \alpha' = -\alpha$, then $\sigma^2(\alpha) = \alpha$ so $\sigma^2 = \mathrm{Id}$; similarly, if $\sigma(\alpha) = \beta = 2/\alpha$, then $\sigma^2(\alpha) = 2/\sigma(\alpha) = \alpha$ so $\sigma^2 = \mathrm{Id}$, and the same goes if $\sigma(\alpha) = \beta'$. Therefore every nontrivial element of $\mathrm{Gal}(L/K)$ has order 2, whence

$$\mathrm{Gal}(L/K) \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}).$$

This example illustrates the principle that the Galois group is the group of permutations of the roots that respect the *relations* between these roots, namely $\alpha' = -\alpha$, $\beta' = -\beta$, and $\alpha\beta = 2$ in this case.

2.5 The correspondence

Definition 2.5.1. From now on, if the extension $K \subseteq L$ is Galois, we write $\mathrm{Gal}(L/K)$ instead of $\mathrm{Aut}_K(L)$, and we call this group the *Galois group* of the extension $K \subseteq L$. We reserve this notation for Galois extensions, and still write $\mathrm{Aut}_K(L)$ when the extension $K \subseteq L$ is not assumed to be Galois.

Theorem 2.5.2 (**Galois correspondence (fundamental)**)**.** *Let $K \subseteq L$ be a finite Galois extension, with Galois group $G = \mathrm{Gal}(L/K)$.*

(i) If E is an intermediate extension $K \subseteq E \subseteq L$, then the extension $E \subseteq L$ is Galois, with Galois group

$$\mathrm{Gal}(L/E) = \{\sigma \in G \mid \sigma(\alpha) = \alpha \ \forall \alpha \in E\},$$

a subgroup of G.

(ii) Let

$$\mathcal{H} = \{H \subseteq G \text{ subgroup}\}$$

be the set of subgroups of $\mathrm{Gal}(L/K)$, and let

$$\mathcal{E} = \{E \text{ field} \mid K \subseteq E \subseteq L\}$$

be the set of intermediate extensions in the extension $K \subseteq L$. Then the maps

$$\Phi : \begin{array}{ccc} \mathcal{H} & \longrightarrow & \mathcal{E} \\ H & \longmapsto & L^H \end{array} \qquad \text{and} \qquad \Psi : \begin{array}{ccc} \mathcal{E} & \longrightarrow & \mathcal{H} \\ E & \longmapsto & \mathrm{Gal}(L/E) \end{array}$$

are bijections that are inverses of each other, and we have

$$[L : L^H] = \#H, \ [L^H : K] = [G : H],$$

$$\#\,\mathrm{Gal}(L/E) = [L : E], \text{ and } [G : \mathrm{Gal}(L/E)] = [E : K]$$

for all $H \in \mathcal{H}$ and $E \in \mathcal{E}$.

(iii) *Let $H \in \mathcal{H}$, let $E = L^H \in \mathcal{E}$ be the corresponding intermediate extension, and let $\sigma \in \mathrm{Gal}(L/K)$. Then the subgroup corresponding to $\sigma(E) \subseteq L$ is the conjugate $\sigma H \sigma^{-1}$ of H.*

(iv) *Let $E \in \mathcal{E}$ be an intermediate extension, and let $H = \mathrm{Gal}(L/E) \in \mathcal{H}$ be the corresponding subgroup. Then*

$$\begin{aligned} & \textit{The extension } K \subseteq E \textit{ is Galois} \\ \iff & \forall \sigma \in G,\ \sigma(E) = E \\ \iff & H \textit{is a } \text{normal } \textit{subgroup of } G, \end{aligned}$$

and in this case we have an isomorphism

$$\begin{array}{ccc} G/H & \simeq & \mathrm{Gal}(E/K) \\ \sigma & \longmapsto & \sigma_{|E} \end{array}.$$

Remark 2.5.3. In part (ii), the maps Φ and Ψ are *inclusion-reversing*: the larger E, the smaller $H = \mathrm{Gal}(L/E) = \mathrm{Aut}_E(L)$. In particular, $\Psi(K) = \mathrm{Gal}(L/K)$ and $\Psi(L) = \{\mathrm{Id}\}$. This observation makes the formulas

$$[L : L^H] = \#H,\ [L^H : K] = [G : H],$$

$$\#\,\mathrm{Gal}(L/E) = [L : E],\ \text{and } [G : \mathrm{Gal}(L/E)] = [E : K]$$

much easier to remember.

In order to streamline the proof of theorem 2.5.2, let us first isolate two lemmas, the first of which is really in the spirit of Galois theory.

Lemma 2.5.4. *Let $K \subseteq L$ be a Galois extension, and let*

$$\begin{cases} \displaystyle\sum_{j=1}^{n} a_{1,j} x_j = 0 \\ \qquad \vdots \\ \displaystyle\sum_{j=1}^{n} a_{m,j} x_j = 0 \end{cases}$$

be a homogeneous linear system of size $m \times n$ with coefficients $a_{i,j}$ in L. If this system has a nonzero solution in L^n, and if its equations are invariant

under $\mathrm{Gal}(L/K)$ *in that for all* $\sigma \in \mathrm{Gal}(L/K)$ *and for each* $i \leqslant m$*, there exists* $i' \leqslant m$ *such that* $\sigma(a_{i,j}) = a_{i',j}$ *for all* $j \leqslant n$*, then this system also has a nonzero solution in* K^n*.*

Proof. Let $(x_1, \cdots, x_n) \in L^n$ be a solution which is nonzero, but which is such that the number of j such that $x_j = 0$ is as large as possible. Let j_0 be the smallest j such that $x_j \neq 0$. Dividing by x_{j_0}, we may assume that $x_{j_0} = 1$. Then for each $\sigma \in \mathrm{Gal}(L/K)$, $\big(\sigma(x_1), \cdots, \sigma(x_n)\big) \in L^n$ is also a solution by assumption, and thus so is $\big(\sigma(x_1) - x_1, \cdots, \sigma(x_n) - x_n\big) \in L^n$. But $\sigma(x_{j_0}) - x_{j_0} = \sigma(1) - 1 = 0$ and $\sigma(0) - 0 = 0$, so this last solution has at least one more zero than $(x_1, \cdots, x_n)$, and must therefore be the zero solution by definition of $(x_1, \cdots, x_n)$. Thus $\sigma(x_j) = x_j$ for all $\sigma \in \mathrm{Gal}(L/K)$, whence $x_j \in K$ for all j. □

Lemma 2.5.5. *Let* $K \subseteq L$ *be a Galois extension, and let* $K \subseteq E \subseteq L$ *be an intermediate extension. Then* E *is Galois over* K *if and only if* $\sigma(E) = E$ *for all* $\sigma \in \mathrm{Gal}(L/K)$*.*

Proof. We already know that the extension $K \subseteq E$ is separable since $K \subseteq L$ is (remark 2.2.9), so it is Galois iff. it is normal.

Let $\sigma \in \mathrm{Gal}(L/K)$, and let $\iota : L \longrightarrow \Omega$ be a K-morphism to an algebraically closed extension Ω of L. Then Ω is also an extension of K. If E is normal, then the K-morphisms ι and $\iota \circ \sigma$ have the same image by theorem 2.3.5, so that $E = \sigma(E)$ since ι is injective.

Conversely, suppose $\sigma(E) = E$ for all $\sigma \in \mathrm{Gal}(L/K)$, and let $P(x) \in K[x]$ be irreducible over K and have a root $\alpha \in E$. Then P is the minimal polynomial of α over K, so by theorem 2.4.3, P has all its roots in L, and these roots are the $\sigma(\alpha)$ for $\sigma \in \mathrm{Gal}(L/K)$ by . But for each such σ, the root $\sigma(\alpha)$ lies in $\sigma(E) = E$, so $K \subseteq E$ is normal by theorem 2.3.5. □

Proof of theorem 2.5.2.

(i) Since $K \subseteq L$ is Galois, it is normal, so by theorem 2.3.5 there exists $F(x) \in K[x]$ such that L is the splitting field of F over K, i.e. is generated as a field by K and the roots of F. Then we also have $F(x) \in E[x]$, and L is still the splitting field of F over E since it is obviously generated by E and the roots of F. Therefore $E \subseteq L$ is normal and hence Galois. Its Galois group is by definition

$$\mathrm{Gal}(L/E) = \mathrm{Aut}_E(L) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(\alpha) = \alpha \ \forall \alpha \in E\}.$$

(ii) By (i), if $E \in \mathcal{E}$, then $E \subseteq L$ is Galois, so $\#\operatorname{Gal}(L/E) = [L : E]$ and $L^{\operatorname{Gal}(L/E)} = E$ by theorem 2.4.3. This shows that $\Phi \circ \Psi = \mathrm{Id}$. If we assume for now that $\Psi \circ \Phi = \mathrm{Id}$, then the formulas

$$[L : L^H] = \#H,\ [L^H : K] = [G : H],\ \text{and}\ [G : \operatorname{Gal}(L/E)] = [E : K]$$

follow immediately from the multiplicativity of the degree.

Let us now prove that $\Psi \circ \Phi = \mathrm{Id}$. Take $H \in \mathcal{H}$, and let $E = L^H$; then we know by i that the extension $E \subseteq L$ is Galois, and we want to show that $\operatorname{Gal}(L/E) = H$. Note that we have $H \subseteq \operatorname{Gal}(L/E)$ by definition of E, whence $\#H \leqslant \#\operatorname{Gal}(L/E) = [L : E]$ by (2.4.1). It is therefore enough to show that $[L : E] \leqslant \#H$.

Consider thus $n+1$ elements $\alpha_0, \alpha_n \in L$, where $n = \#H$. We want to show that they are linearly dependent over E, that is to say that there exist $\lambda_1, \cdots, \lambda_{n+1} \in E$ which are not all 0 and such that

$$\sum_{j=1}^{n+1} \lambda_j \alpha_j = 0.$$

Applying an element $\sigma \in H$ to this equation yields

$$0 = \sum_{j=1}^{n+1} \sigma(\lambda_j)\sigma(\alpha_j) = \sum_{j=1}^{n+1} \lambda_j \sigma(\alpha_j)$$

since the λ_j lie in $E = L^H$, so we are led to considering the linear system

$$\begin{cases} \displaystyle\sum_{j=1}^{n+1} \lambda_j \sigma_1(\alpha_j) = 0 \\ \qquad\qquad \vdots \\ \displaystyle\sum_{j=1}^{n+1} \lambda_j \sigma_n(\alpha_j) = 0 \end{cases}$$

where $H = \{\sigma_1, \cdots, \sigma_n\}$, and we want to show that this system has a nonzero solution in E^{n+1}.

It has $n+1$ unknowns $\lambda_1, \cdots, \lambda_{n+1}$, and n equations with coefficients in L, so it certainly has a nonzero solution in L^{n+1}. Besides, these

equations are invariant under $\mathrm{Gal}(L/E)$, so lemma 2.5.4 applied to the Galois extension $E \subseteq L$ ensures that it indeed has a nontrivial solution in E^{n+1}.

(iii) We know that $H = \mathrm{Gal}(L/E)$ by (ii). Let $\tau \in \mathrm{Gal}(L/K)$. Then

$$\begin{aligned}
\tau \in \mathrm{Gal}(L/\sigma(E)) &\iff \forall e \in E,\ \tau(\sigma(e)) = \sigma(e) \\
&\iff \forall e \in E,\ \sigma^{-1}\tau\sigma(e) = e \\
&\iff \sigma^{-1}\tau\sigma \in H \\
&\iff \tau \in \sigma H \sigma^{-1}.
\end{aligned}$$

(iv) Let $K \subseteq E \subseteq L$ be an intermediate extension, and let $H \subseteq G$ be the corresponding subgroup. We deduce from lemma 2.5.5 and from (iii) that

$$\begin{aligned}
K \subseteq E \text{ Galois} &\iff \forall \sigma \in G,\ \sigma(E) = E \\
&\iff \forall \sigma \in G,\ \sigma H \sigma^{-1} = H \\
&\iff H \subseteq G \text{ normal.}
\end{aligned}$$

Let us now suppose that H is normal in G, so that E is Galois over K. Then the map

$$\rho : \begin{array}{ccc} \mathrm{Gal}(L/K) & \simeq & \mathrm{Gal}(E/K) \\ \sigma & \longmapsto & \sigma_{|E} \end{array}$$

is well-defined since each $\sigma \in \mathrm{Gal}(L/K)$ leaves E globally invariant. It is also clearly a group morphism, whose kernel is precisely H. The first isomorphism theorem thus grants us with an injective morphism from G/H to $\mathrm{Gal}(E/K)$. Furthermore

$$\#(G/H) = [G : H] = [E : K] = \#\,\mathrm{Gal}(E/K)$$

since $G = \mathrm{Gal}(L/K)$ and $H = \mathrm{Gal}(L/E)$, so this injection must be a bijection.

□

Example 2.5.6. In example 2.1.3, the "symmetry" we observed between the diagrams

$$\begin{array}{ccccc} & & \mathbb{Q}(\sqrt{2},\sqrt{3}) & & \\ & \curvearrowleft & \cup & \curvearrowright & \\ \mathbb{Q}(\sqrt{2}) & & \mathbb{Q}(\sqrt{6}) & & \mathbb{Q}(\sqrt{3}) \\ & \curvearrowright & \cup & \curvearrowleft & \\ & & \mathbb{Q} & & \end{array} \quad \longleftrightarrow \quad \begin{array}{ccccc} & & \{\mathrm{Id}\} & & \\ & \curvearrowright & \cap & \curvearrowleft & \\ \{\mathrm{Id},\tau\} & & \{\mathrm{Id},\sigma\tau\} & & \{\mathrm{Id},\sigma\} \\ & \curvearrowleft & \cap & \curvearrowright & \\ & & G & & \end{array}$$

where

$$\sigma(\sqrt{2}) = -\sqrt{2}, \quad \sigma(-\sqrt{2}) = \sqrt{2}, \quad \sigma(\sqrt{3}) = \sqrt{3}, \quad \sigma(-\sqrt{3}) = -\sqrt{3},$$
$$\tau(\sqrt{2}) = \sqrt{2}, \quad \tau(-\sqrt{2}) = -\sqrt{2}, \quad \tau(\sqrt{3}) = -\sqrt{3}, \quad \tau(-\sqrt{3}) = \sqrt{3}$$

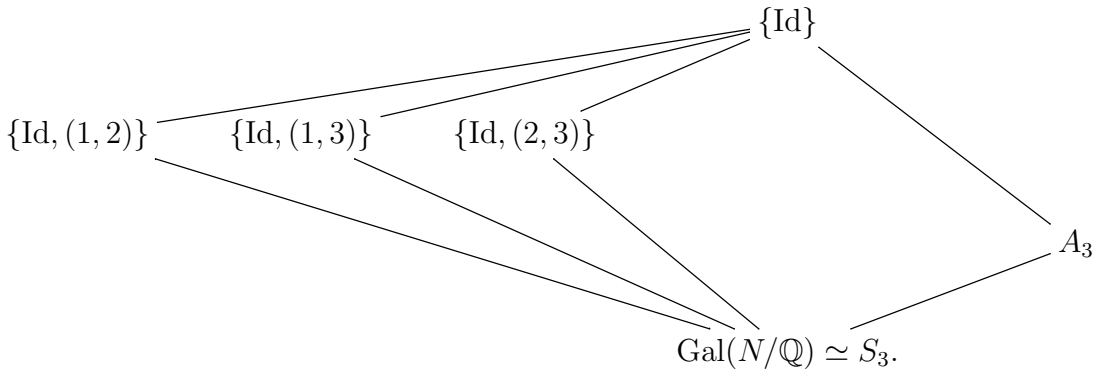
was an avatar of the Galois correspondence.

Example 2.5.7. Let $K = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt[3]{2})$. We have seen in example 2.4.9 that the extension $K \subseteq L$ is not Galois, so we cannot apply theorem 2.5.2 to it; but it applies to the extension $K = \mathbb{Q} \subseteq N$, where $N = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ is the Galois closure of L over K.

Since we have seen that $\mathrm{Gal}(N/\mathbb{Q})$ is isomorphic to the symmetric group S_3 permuting the conjugates

$$\alpha_1 = \sqrt[3]{2}, \quad \alpha_2 = \zeta_3\sqrt[3]{2}, \quad \alpha_3 = \zeta_3^2\sqrt[3]{2},$$

we can easily draw it subgroup diagram:



where $A_3 = \{\mathrm{Id}, (1,2,3), (1,3,2)\} \simeq \mathbb{Z}/3\mathbb{Z}$ is the alternate subgroup of S_3. Here, the lines mean inclusions, the smaller group being above the larger; in

fact, we have put subgroups of order 1 on the top row, subgroups of order 2 on the second one, then subgroups of order 3 on the third one, and finally S_3 itself on the last one.

Let us now find the corresponding subfield diagram. Let us begin with $H = \{\mathrm{Id}, (2,3)\}$. This is a subgroup of order 2 and therefore of index 3, so the corresponding subextension $E = N^H$ satisfies $[N : E] = 2$ and $[E : K] = 3$. Besides, α_1 is fixed by all of the elements of H, and therefore lies in E, whence

$$\mathbb{Q}(\alpha_1) = \mathbb{Q}(\sqrt[3]{2}) \subseteq E;$$

but then

$$[E : \mathbb{Q}(\sqrt[3]{2})] = \frac{[E : K]}{[\mathbb{Q}(\sqrt[3]{2}) : K]} = \frac{3}{3} = 1,$$

o we must actually have equality $E = \mathbb{Q}(\sqrt[3]{2})$.

We find similarly that the subextension corresponding to $\{\mathrm{Id}, (1,3)\}$ is $\mathbb{Q}(\alpha_2) = \mathbb{Q}(\zeta_3\sqrt[3]{2})$, and that the subextension corresponding to $\{\mathrm{Id}, (1,2)\}$ is $\mathbb{Q}(\alpha_3) = \mathbb{Q}(\zeta_3^2\sqrt[3]{2})$.

Finally, we observe that

$$\zeta_3 = \frac{\alpha_2}{\alpha_1} = \frac{\alpha_3}{\alpha_2} = \frac{\alpha_1}{\alpha_3},$$

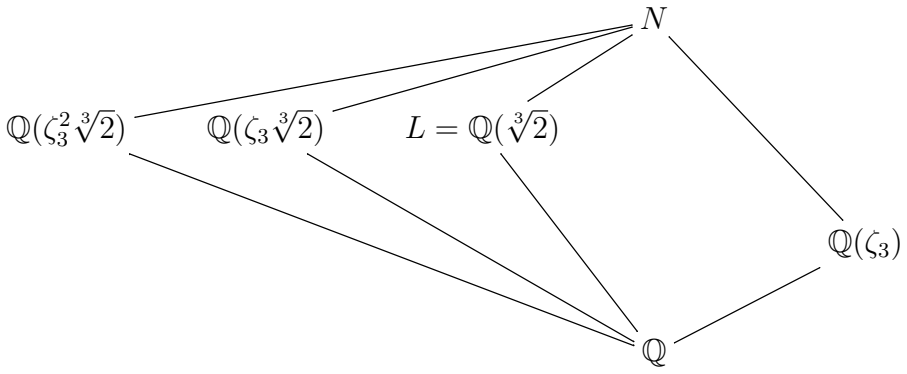
so that $\zeta_3 \in N^{A_3}$; since this extension has degree

$$[S_3 : A_3] = 2$$

over $K = \mathbb{Q}$, and since $\zeta_3 = \frac{-1+i\sqrt{3}}{2}$ is algebraic of degree 2 over $\mathbb{Q}$, we have

$$N^{A_3} = \mathbb{Q}(\zeta_3) = \mathbb{Q}(i\sqrt{3}).$$

The subfield diagram corresponding to the above subgroup diagram is thus



where lines still denote inclusion, but the larger fields are above the smaller ones this time (and in fac we have degree 6, 3, 2, 1 over $\mathbb{Q}$ on the first, second, third, and last row, respectively). These are all the fields between $\mathbb{Q}$ and N, ince we have considered all the subgroups of S_3.

Besides, for each intermediate extension E, the extension $E \subseteq N$ is Galois (it is actually the splitting field of $x^3 - 2$ over E); however, only the subgroup A_3 is normal in S_3, so $\mathbb{Q}(\zeta_3)$ is the only intermediate extension which is Galois over $K = \mathbb{Q}$. In fact, the other subgroups

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

are conjugate to each other (in the group-theoretic sense) in S_3, so that the corresponding intermediate extensions

$$\mathbb{Q}(\zeta_3^2 \sqrt[3]{2}), \quad \mathbb{Q}(\zeta_3 \sqrt[3]{2}), \quad \mathbb{Q}(\sqrt[3]{2})$$

are conjugate to each other (in the Galois-theoretic sense, i.e. they are taken to one another by automorphisms of $\mathrm{Gal}(N/K)$).

Example 2.5.8. Let $\alpha = \sqrt{5 + \sqrt{21}}$, and $L = \mathbb{Q}(\alpha)$. We have seen in example 2.4.10 that α is algebraic of degree 4 over $\mathbb{Q}$, that its conjugates are α, $-\alpha$, $\beta = \sqrt{5 - \sqrt{21}}$, and $-\beta$, and that $\beta \in L$ since $\alpha\beta = 2$, so that L is Galois over $\mathbb{Q}$ with Galois group

$$\mathrm{Gal}(L/\mathbb{Q}) = \{\mathrm{Id}, \sigma_1, \sigma_2, \sigma_3\} \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}),$$

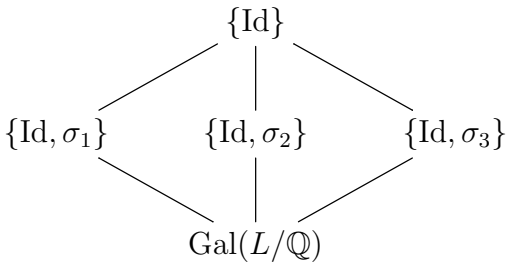
where

$$\sigma_1(\alpha) = -\alpha, \quad \sigma_2(\alpha) = \beta, \quad \sigma_3(\alpha) = -\beta$$

which in view of the relation $\beta = 2/\alpha$ implies

$$\sigma_1(\beta) = -\beta, \quad \sigma_2(\beta) = \alpha, \quad \sigma_3(\beta) = -\alpha.$$

The subgroup diagram of $\mathrm{Gal}(L/\mathbb{Q})$ is obviously



Let us now identify the corresponding subfields.

Write $H_i = \{\mathrm{Id}\,\sigma_i\}$ and $E_i = L^{H_i}$ for each $i \in \{1,2,3\}$. We have $\#H_i = 2$ for each i, whence

$$[E_i : \mathbb{Q}] = \frac{[L:\mathbb{Q}]}{[L:E_i]} = \frac{4}{\#H_i} = 2$$

for each i.

Since $\sigma_1(\alpha) = -\alpha$, the element $\alpha^2 = 5 + \sqrt{21}$ is fixed by al the elements of H_1, so that $\alpha^2 \in E_1$ whence $\mathbb{Q}(\alpha^2) = \mathbb{Q}(5+\sqrt{21}) = \mathbb{Q}(\sqrt{21}) \subseteq E_1$, and actually $\mathbb{Q}(\sqrt{21}) = E_1$ by comparing the degrees.

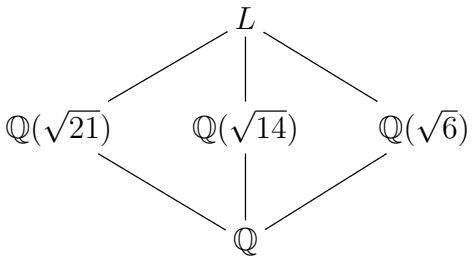
Similarly, since σ_2 swaps α and β, the elements $\alpha+\beta$ and $\alpha\beta$ lie in E_2. That $\alpha\beta = 2 \in E_2$ teaches us nothing; however we have $\alpha + \beta = \sqrt{14}$ since $(\alpha+\beta)^2 = \alpha^2+\beta^2+2\alpha\beta = 14$, whence $\mathbb{Q}(\sqrt{14}) \subseteq E_2$ and actually $E_2 = \mathbb{Q}(\sqrt{14})$ by checking the degrees.

Finally, $\alpha - \beta$ is fixed by σ_3 since

$$\sigma_3(\alpha-\beta) = \sigma_3(\alpha) - \sigma_3(\beta) = -\beta + \alpha,$$

so $\alpha - \beta \in E_3$. Besides, one computes that $\alpha - \beta = \sqrt{6}$, whence $E_3 = \mathbb{Q}(\sqrt{6})$ by the degrees.

The subfield diagram corresponding to the subgroup diagram is therefore



In particular, we discover the fact that $L = \mathbb{Q}(\sqrt{21},\sqrt{14},\sqrt{6})$; indeed the degree of $\mathbb{Q}(\sqrt{21},\sqrt{14},\sqrt{6})$ over $\mathbb{Q}$ is at least 4 since $\sqrt{14} \notin \mathbb{Q}(\sqrt{21})$ (this is proved as in example 2.4.10), but not 8 since

$$\sqrt{6} = \frac{\sqrt{21}\sqrt{14}}{7}.$$

Finally, we note that since $\mathrm{Gal}(L/\mathbb{Q})$ is Abelian, its subgroups are all normal; and indeed, the fields E_1, E_2, and E_3 are Galois over $\mathbb{Q}$.

Example 2.5.9. Let $\alpha = \sqrt{5+\sqrt{15}}$ and $L = \mathbb{Q}(\alpha)$. As in example 2.5.8, we check that $[L : \mathbb{Q}] = 4$, so that α is algebraic of degree 4 over $\mathbb{Q}$, and its 4 conjugates are $\pm\alpha$ and $\pm\beta$, where $\beta = \sqrt{5-\sqrt{15}}$. Clearly, $-\alpha \in L$, but this time (and this the fundamental difference with example 2.5.8), $\alpha\beta = \sqrt{10} \notin \mathbb{Q}$, so that is is not clear anymore whether $\beta \in L$ and thus whether L is Galois over $\mathbb{Q}$

Actually, we claim that $\beta \notin L$, so that L is not Galois over $\mathbb{Q}$. Let us prove this by contradiction. If we had $\beta \in L$, then also $-\beta$ in L, so L would be the splitting field of the minimal polynomial $(x^2-5)^2 - 15$ of α over $\mathbb{Q}$, and would therefore bye Galois over $\mathbb{Q}$. Since $[L : \mathbb{Q}] = 4$, $\mathrm{Gal}(L/\mathbb{Q})$ would be a group of order 4, and the intermediate extension

$$\mathbb{Q} \subseteq \mathbb{Q}(\alpha^2) = \mathbb{Q}(\sqrt{15}) \subseteq L$$

would correspond to a subgroup of order 2, thus of the form

$$H = \{\mathrm{Id}, \sigma\}$$

for some $\sigma \in \mathrm{Gal}(L/\mathbb{Q})$ or order 2. Since $\sigma(\alpha)^2 = \sigma(\alpha^2) = \alpha^2$, we would have $\sigma(\alpha) = \pm\alpha$. But $\alpha \notin L^H$ (since we would have $L = L^H$ else), so necessarily $\sigma(\alpha) = -\alpha$ and thus $\sigma(-\alpha) = \alpha$. Besides, σ permutes the conjugates $\pm\alpha$, $\pm\beta$ of α and is injective, so $\sigma(\beta)$ is either β or $-\beta$. We are going to how that both alternatives are absurd.

Indeed, if $\sigma(\beta) = \beta$, then $\beta \in L^H = \mathbb{Q}(\sqrt{15})$, whence $\mathbb{Q}(\beta) \subseteq \mathbb{Q}(\sqrt{15})$, which is impossible since one proves as above that $[\mathbb{Q}(\beta) : \mathbb{Q}] = 4$. If now $\sigma(\beta) = -\beta$, then

$$\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = (-\alpha)(-\beta) = \alpha\beta,$$

whence $\sqrt{10} = \alpha\beta \in \mathbb{Q}(\sqrt{15})$. But again this is impossible, since $(u + v\sqrt{15})^2 = 10$ yields the system

$$\begin{cases} u^2 + 15v^2 = 10 \\ 2uv = 0 \end{cases}$$

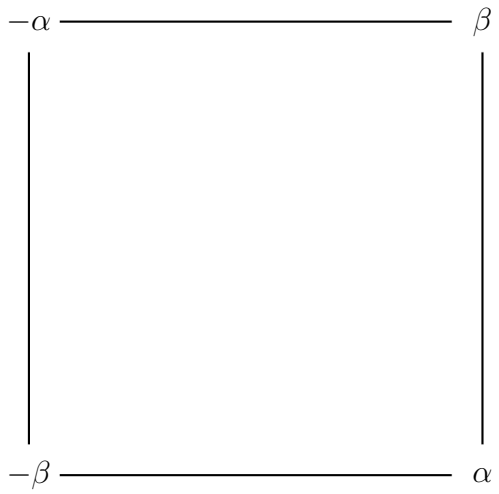
which has clearly no solutions in rationals.

So $\beta \notin L$, and L is not Galois over $\mathbb{Q}$. Its Galois closure is of course

$$N = \mathbb{Q}(\alpha, -\alpha, \beta, -\beta) = \mathbb{Q}(\alpha, \beta) = L(\beta),$$

which is thus a strict extension of L; but $\beta^2 = 5 - \sqrt{15} \in L$, so $[N : L] \leqslant 2$, whence $[N : L] = 2$ and $[N : \mathbb{Q}] = 8$. Therefore $\mathrm{Gal}(N/\mathbb{Q})$ has order 8.

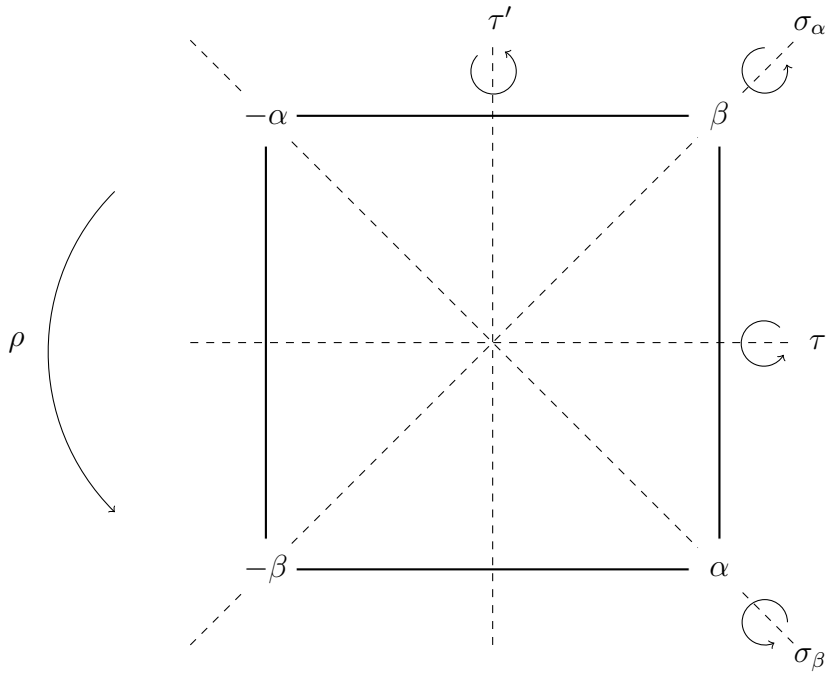
Let us identify this group. We know that it is a subgroup of the symmetric group S_4 acting on the 4 conjugates $\pm\alpha$, $\pm\beta$. But automorphisms must preserve negatives, so if we arrange these 4 conjugates as follows



then $\mathrm{Gal}(N/\mathbb{Q})$ must preserve the square. Therefore $\mathrm{Gal}(N/\mathbb{Q})$ is a subgroup of the group of symmetries of the square, which is the dihedral group D_8. Since both have order 8, we conclude that

$$\mathrm{Gal}(N/\mathbb{Q}) \simeq D_8.$$

Let us now check the Galois correspondence for the extension $\mathbb{Q} \subseteq N$. In order to list the subgroups of $\mathrm{Gal}(N/\mathbb{Q}) \simeq D_8$, let us name some of it elements:



Thus for instance

$$\sigma_\alpha : \alpha \mapsto -\alpha,\ -\alpha \mapsto \alpha,\ \beta \mapsto \beta,\ -\beta \mapsto -\beta$$

and

$$\rho : \alpha \mapsto \beta \mapsto -\alpha \mapsto -\beta \mapsto \alpha,$$

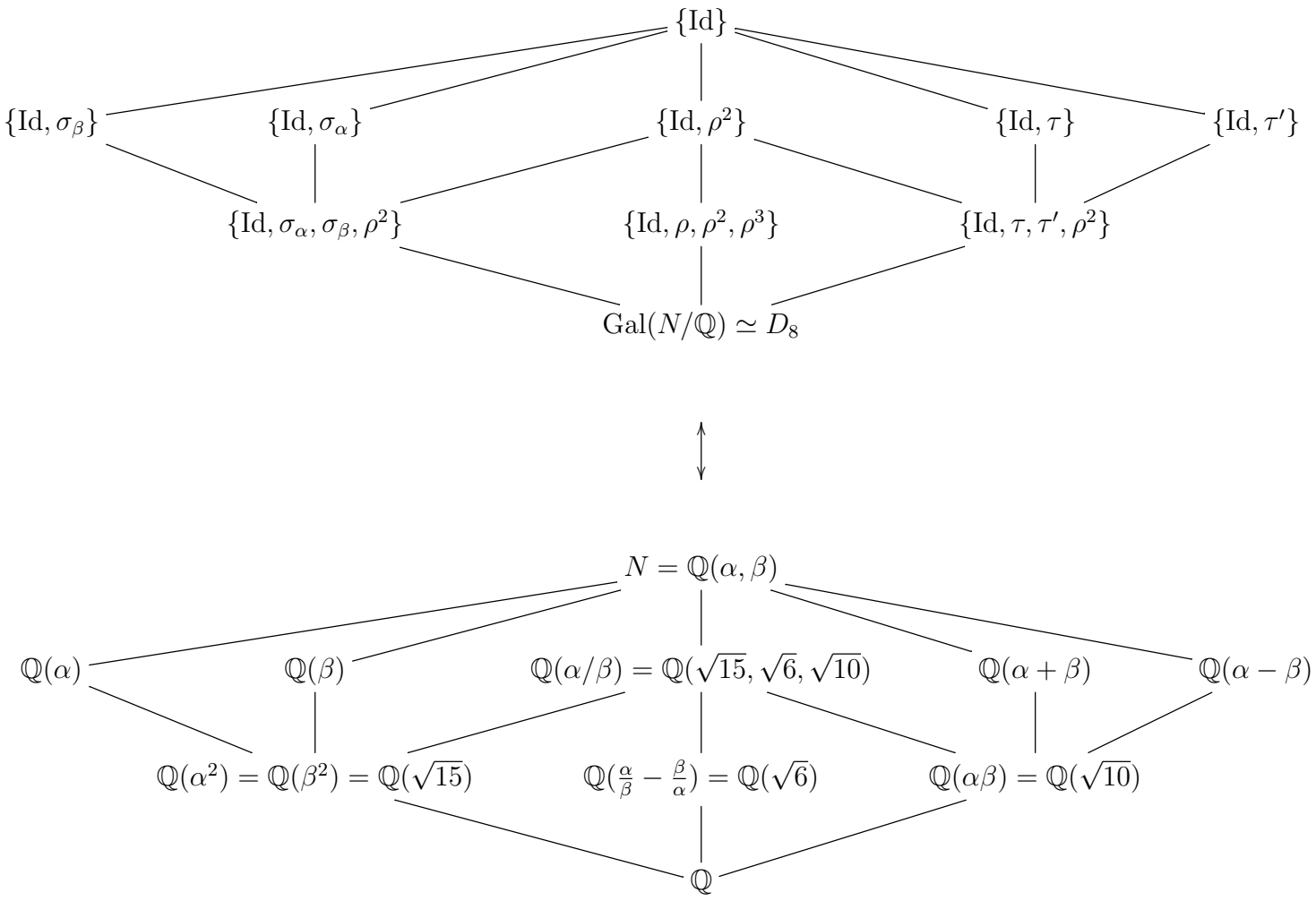
and the central symmetry is

$$\sigma_\alpha \sigma_\beta = \sigma_\beta \sigma_\alpha = \tau\tau' = \tau'\tau = \rho^2.$$

By Lagrange, the nontrivial subgroups of D_8 have order 2 or 4. Subgroups of order 2 are made of the identity nd of an element of order 2; whereas subgroups of order 4 are either isomorphic to $\mathbb{Z}/4\mathbb{Z}$ and thus spanned by an element of order 4, or to $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ and thus spanned by two elements of order 2 which commute with each other.

You should then convince yourself that the subgroup diagram of D_8 and

the corresponding subfield diagram are the following:



We also observe that the (group-theoretic) conjugates of σ_α are σ_α itself and σ_β; indeed $\sigma_\beta = \rho\sigma_\alpha\rho^{-1}$, as can be seen at the level of the action on $\pm\alpha$, $\pm\beta$. Therefore the subgroups $\{\mathrm{Id}, \sigma_\alpha\}$ and $\{\mathrm{Id}, \sigma_\beta\}$ are not normal, and are actually conjugate to each other; and indeed, the corresponding subextensions $\mathbb{Q}(\alpha)$ and $\mathbb{Q}(\beta)$ are not normal over $\mathbb{Q}$, and are conjugate in the sense that

$$\rho\big(\mathbb{Q}(\alpha)\big) = \mathbb{Q}\big(\rho(\alpha)\big) = \mathbb{Q}(\beta).$$

Similarly, the subgroups $\{\mathrm{Id}, \tau\}$ and $\{\mathrm{Id}, \tau'\}$ are not normal, and are actually conjugate to each other (by ρ again, in fact); and indeed, the corresponding subextensions $\mathbb{Q}(\alpha+\beta)$ and $\mathbb{Q}(\alpha-\beta)$ are not normal over $\mathbb{Q}$, and are actually conjugate to each other:

$$\rho\big(\mathbb{Q}(\alpha+\beta)\big) = \mathbb{Q}\big(\rho(\alpha+\beta)\big) = \mathbb{Q}(\alpha-\beta).$$

The other subgroups are normal, and Galois-correspondingly, the corresponding subextensions are Galois over $\mathbb{Q}$.

Example 2.5.10. So far, we have only give examples of extensions of $\mathbb{Q}$, but the Galois correspondence is much more general than that! For example, take $p \in \mathbb{N}$ a prime, $q = p^n$ for some $n \in \mathbb{N}$, and consider the extension of finite fields

$$K = \mathbb{F}_p \subseteq L = \mathbb{F}_q.$$

Recall from corollary 1.3.14 that

$$\mathrm{Frob} : \begin{array}{ccc} \mathbb{F}_q & \longrightarrow & \mathbb{F}_q \\ x & \longmapsto & x^p \end{array} \in \mathrm{Aut}_K(L).$$

Let m be its order; them $\mathrm{Frob}^m = \mathrm{Id}$, whence $x^{p^m} = x$ for all $x \in \mathbb{F}_q$. This means that the degree p^m polynomial $x^{p^m} - x$ has q roots in the field $\mathbb{F}_q$, so necessarily $p^m \geq q = p^n$ whence $m \geq n$. In particular,

$$\#\,\mathrm{Aut}_K(L) \geq m \geq n,$$

but on the other hand we know by (2.4.1) that

$$\#\,\mathrm{Aut}_K(L) \leq [L : K] = n.$$

We must therefore have equality everywhere, whence $m = n$, and $\mathrm{Aut}_K(L) \simeq \mathbb{Z}/n\mathbb{Z}$ is cyclic and generated by Frob. Since $\#\,\mathrm{Aut}_K(L) = [L : K]$, it follows that the extension $K \subseteq L$ is Galois by theorem 2.4.3(ii). Note that we already knew that it would be separable by remark 2.2.12; in fact, we may also argue that $K \subseteq L$ is Galois because it is the splitting field of $F(x) = x^q - x$ (cf. the contruction of $\mathbb{F}_q$ in the proof of theorem 1.3.18) and because $F(x)$ is separable as $F'(x) = -1$ has no common roots with $F(x)$ (since it does not have any roots).

The subgroups of $\mathbb{Z}/n\mathbb{Z}$ are the $d\mathbb{Z}/n\mathbb{Z}$ for $d \mid n$, so the subgroups of $\mathrm{Gal}(L/K) = \mathrm{Aut}_L(K) = \langle \mathrm{Frob} \rangle \simeq \mathbb{Z}/n\mathbb{Z}$ are the

$$H_d = \langle \mathrm{Frob}^d \rangle$$

for $d \mid n$. The corresponding subfields are the

$$\begin{aligned}\mathbb{F}_q^{H_d} &= \{x \in \mathbb{F}_q \mid \mathrm{Frob}^d(x) = x\} \\ &= \{x \in \mathbb{F}_q \mid x^{p^d} = x\} \\ &= \mathbb{F}_{p^d};\end{aligned}$$

we thus recover the fact (cf. theorem 1.3.18) that the subfields of $\mathbb{F}_{p^n}$ are the $\mathbb{F}_{p^d}$ for $d \mid n$.

2.6 Applications

2.6.1 The primitive element theorem

Proposition 2.6.1. *Let $K \subseteq L$ be a finite separable extension. There are only finitely many fields E such that $K \subseteq E \subseteq L$.*

Proof. We cannot use theorem 2.5.2 directly, since the extension might not be normal. We therefore introduce the Galois closure N of L over K. Then N is a finite Galois extension of K by construction, so its Galois group $\mathrm{Gal}(N/K)$ is a finite group. In particular, it has finitely many subfields, so there exist finitely many intermediate fields E such that $K \subseteq E \subseteq N$, and thus finitely many such that $K \subseteq E \subseteq L$. □

Theorem 2.6.2 (Primitive element theorem)**.** *Let $K \subseteq L$ be a finite separable extension. There exists $\alpha \in L$ such that $L = K(\alpha)$.*

Proof. If K is finite, then we already know this (corollary 1.3.15). We therefore suppose that K is infinite from now on.

We have

$$L = \bigcup_{\alpha \in L} K(\alpha).$$

For each $\alpha \in L$, $E = K(\alpha)$ is a field satisfying $K \subseteq E \subseteq L$, and there are finitely many such fields by proposition 2.6.1, so we can find finitely many $\alpha_1, \cdots, \alpha_r \in L$ such that

$$L = \bigcup_{i=1}^{r} K(\alpha_i).$$

Since each $K(\alpha_i)$ is a K-subspace of the K-vector space L and since we assume that K is infinite, the result follows from lemma 2.6.3 below. □

Lemma 2.6.3. *Let V be a vector space over a field K. If we can write*

$$V = \bigcup_{i=1}^{r} W_i$$

as a finite union of strict subspaces $W_i \subsetneq V$, then K is finite.

Proof. Suppose that

$$V = \bigcup_{i=1}^{r} W_i$$

where the W_i are strict subspaces. After removing some subspaces if necessary, we may assume that

$$\bigcup_{i=1}^{r-1} W_i \subsetneq \bigcup_{i=1}^{r} W_i = V.$$

Let $v \in V \setminus \bigcup_{i=1}^{r-1} W_i$, so that in particular $v \in W_r$; let also $a \in V \setminus W_r$, and consider the affine line

$$L = a + Kv = \{a + \lambda v \mid \lambda \in K\}.$$

If we had a point $p = a+\lambda v \in L \cap W_r$, then $a = p-\lambda v \in W_r$, which is absurd; thus $L \cap W_r = \emptyset$. Besides, we have $\#(L \cap W_i) \leqslant 1$ for all $i < r$; indeed, if $p_i = a + \lambda v$ and $q_i = a + \mu v$ both lie in W_i, then so does $\overrightarrow{p_i q_i} = (\mu - \lambda)v$, whence $\lambda = \mu$ as $v \notin W_i$. Since

$$L = \bigcup_{i=1}^{r} (L \cap W_i)$$

is in bijection with K, we must have $\#K \leqslant r - 1$. □

Remark 2.6.4. Theorem 2.6.2 can be proved without Galois theory. In particular, one can show that if K is infinite, then "most" $\alpha \in L$ satisfy $K(\alpha) = L$.

Remark 2.6.5. Both proposition 2.6.1 and theorem 2.6.2 can fail if L is not separable over K. Indeed, let u and v be independent indeterminates, $K = \mathbb{F}_p(u, v)$ the field of rational fractions in u and v with coefficients in $\mathbb{F}_p$, and $L = \mathbb{F}_p(u^{1/p}, v^{1/p})$. One checks as in example 2.2.5 that in the chain

$$K \subseteq \mathbb{F}_p(u^{1/p}, v) \subseteq L,$$

both extensions have degree p (in fact, the minimal polynomials of $u^{1/p}$ and $v^{1/p}$ are respectively $x^p - u$ and $x^p - v \in K[x]$), so $[L : K] = p^2$; yet for all $\alpha = R(u^{1/p}, v^{1/p}) \in L$, we have $\alpha^p = R(u, v)$ (cf. example 1.3.12), so the minimal polynomial of α over K divides $x^p - R(u, v) \in K[x]$, so that $[K(\alpha) : K] \leqslant p$ whence $K(\alpha) \subsetneq L$.

Besides, let $k \in K$, and define $E_k = K(u^{1/p} + kv^{1/p})$. Then the subextensions E_k are all distinct. Indeed, if we had

$$K(u^{1/p} + kv^{1/p}) = K(u^{1/p} + k'v^{1/p})$$

for $k \neq k' \in K$, then we would have

$$u^{1/p} + k'v^{1/p} \in K(u^{1/p} + kv^{1/p}),$$

whence

$$v^{1/p} = \frac{(u^{1/p} + k'v^{1/p}) - (u^{1/p} + kv^{1/p})}{k' - k} \in K(u^{1/p} + kv^{1/p})$$

and

$$u^{1/p} = (u^{1/p} + kv^{1/p}) - kv^{1/p} \in K(u^{1/p} + kv^{1/p})$$

as well, so that

$$L = K(u^{1/p}, v^{1/p}) \subseteq E_k = K(u^{1/p} + kv^{1/p})$$

and hence $L = E_k$, but this is absurd since $L \neq K(\alpha)$ for any $\alpha \in L$. Since K is clearly infinite, we have thus exhibited infinitely many intermediate fields

$$K \subseteq E_k \subseteq L.$$

2.6.2 Cyclotomic fields

Definition 2.6.6. Let $n \in \mathbb{N}$ and $\zeta \in \mathbb{C}$.

1. We say that ζ is an *n-th root of 1* if $\zeta^n = 1$.
2. We say that ζ is a a *primitive* n-th root of 1 if $\zeta^n = 1$ but $\zeta^m \neq 1$ for all $1 \leqslant m < n$, i.e. if the multiplicative order of ζ is *exactly* n.

Thus there are n n-th roots of 1, namely the

$$e^{2k\pi i/n}, \qquad k \in \{0, 1, \cdots, n-1\};$$

of these, $\phi(n)$ (Euler's totient function) are primitive, namely the

$$e^{2k\pi i/n}, \qquad k \in \{0, 1, \cdots, n-1\},\ \gcd(k, n) = 1.$$

The others are primitive d-th roots of unity for some strict divisor d of n.

Let us write

$$\zeta_n = e^{2\pi i/n}$$

from now on. We observe that since $\zeta_n^n = 1$, the value of ζ_n^k only depends on the class of k in $\mathbb{Z}/n\mathbb{Z}$. We therefore have a bijection

$$\begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} & \longmapsto & n\text{-th roots of 1} \\ k & \longmapsto & \zeta_n^k \end{array}$$

that is actually an isomorphism between $\mathbb{Z}/n\mathbb{Z}$ and the subgroup of $\mathbb{C}^\times$ formed by the n-th roots of 1, and that restricts to a bijection[1] between $(\mathbb{Z}/n\mathbb{Z})^\times$ and *primitive* n-th roots of 1.

Definition 2.6.7. The n-th *cyclotomic polynomial* is

$$\Phi_n(x) = \prod_{\substack{\zeta \text{ primitive} \\ n\text{-th root of 1}}} (x - \zeta) \quad = \prod_{\substack{k=0 \\ \gcd(k,n)=1}}^{n-1} (x - e^{2k\pi i/n}) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^\times} (x - \zeta_n^k).$$

We note that $\deg \Phi_n(x) = \phi(n)$ and that $\Phi_n(x) \mid (x^n - 1)$.

Definition 2.6.8. The n-th cyclotomic extension of $\mathbb{Q}$ is

$$\mathbb{Q}(\text{all } n\text{-th roots of 1}) = \mathbb{Q}(\text{all primitive } n\text{-th roots of 1}) = \mathbb{Q}(\zeta_n).$$

.

Theorem 2.6.9. *Let $n \in \mathbb{N}$.*

(i) $\Phi_n(x) \in \mathbb{Z}[x]$.

[1] Not an isomorphism anymore, since the source and target are no longer groups, but mere sets.

(ii) $\Phi_n(x)$ *is irreducible over* $\mathbb{Q}$.

(iii) The complete factorisation of $x^n - 1$ *over* $\mathbb{Q}$ *is*

$$x^n - 1 = \prod_{d|n} \Phi_d(x).$$

(iv) $\mathbb{Q}(\zeta_n)$ *is a Galois extension of* $\mathbb{Q}$.

(v) Its degree is $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$.

(vi) $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ *is canonically isomorphic to* $(\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. Let $F(x) = x^n - 1$. Then $\mathbb{Q}(\zeta_n)$ contains all the powers of ζ_n, i.e. all the roots of $F(x)$, so it is the splitting field of $F(x)$ over $\mathbb{Q}$. It is therefore normal, and also separable since we are in characteristic 0. This proves (iv).

Let

$$x^n - 1 = \prod_{i=1}^{r} P_i(x)$$

be the complete factorisation of $F(x) \in \mathbb{Q}[x]$, where the P_i are monic. We first prove that the P_i actually lie in $\mathbb{Z}[x]$ (this is an avatar of Gauss's lemma). Indeed, for each i, let $d_i \in \mathbb{N}$ be the smallest common denominator for the coefficients of P_i, so that $Q_i = d_i P_i \in \mathbb{Z}[x]$ and the gcd of its coefficients is 1. Then

$$\prod_{i=1}^{r} Q_i = \prod_{i=1}^{r} (d_i P_i) = \left(\prod_{i=1}^{r} d_i \right) (x^n - 1).$$

If at least one of the d_i were > 1, then we could find a prime $p \in \mathbb{N}$ dividing $\prod d_i$; but then we would have

$$\prod_{i=1}^{r} \overline{Q_i} = \overline{0} \cdot (x^n - \overline{1}) = \overline{0} \in \mathbb{F}_p[x],$$

where the bar denotes reduction mod p. This is absurd, as $\mathbb{F}_p[x]$ is a domain, and yet none of the $\overline{Q_i}$ is $\overline{0}$ since for each i, not all the coefficients of Q_i are divisible by p (else d_i would not be the smallest denominator). Therefore $d_i = 1$ and $P_i = Q_i \in \mathbb{Z}[x]$ for all i.

Write $\zeta = \zeta_n$ for simplicity. Then $F(\zeta) = 0$, so $P_i(\zeta) = 0$ for some i; without loss of generality, we will assume that $P_1(\zeta) = 0$. Since P_1 is irreducible over $\mathbb{Q}$, it is the minimal polynomial of ζ over $\mathbb{Q}$, and we want to show that $\Phi_n = P_1$.

Let $p \in \mathbb{N}$ be a prime not dividing n. Since $F(\zeta^p) = 0$, there exists a $j \leqslant r$ such that $P_j(\zeta_p) = 0$. We want to prove that actually, $j = 1$. For this, we first note that if we define $Q(x) = P_j(x^p)$, then $Q(\zeta) = P_j(\zeta^p) = 0$, so $P_1 \mid Q$ since P_1 is the minimal polynomial of ζ over $\mathbb{Q}$. We therefore have $Q(x) = P_1(x)R(x)$ for some $R \in \mathbb{Q}[x]$; and actually, one can prove as above (Gauss's lemma again) that $R \in \mathbb{Z}[x]$. Let us again denote reduction mod p by a bar. Then $\overline{F}(x) \in \mathbb{F}_p[x]$, so it has a splitting field S, which is a finite extension of $\mathbb{F}_p$. Besides, $\overline{F}$ is separable, since $\overline{F}' = \overline{n}x^{n-1}$ has no common factor with F in $\mathbb{F}_p[x]$; indeed, $p \nmid n$, so $\overline{n} \neq \overline{0}$, so the only factors of F' are the (up to scaling) the powers of x. Therefore $\overline{F}$ has $\deg F = n$ distinct roots in its splitting field S. Besides,

$$\overline{F} = \prod_{i=1}^{r} \overline{P_i},$$

so these roots are also the roots of the $\overline{P}_i$, and no two $\overline{P}_i$ can have a common root (else that root would be a multiple root of $\overline{F}$). Let $\overline{\alpha}$ be a root of $\overline{P}_1$. Since

$$\overline{P}_1(x)\overline{R}(x) = \overline{Q}(x) = \overline{P}_j(x^p) = \overline{P}_j(x)^p$$

by example 1.3.12, the fact that $\overline{P}_1(\overline{\alpha}) = \overline{0}$ implies that $\overline{P}_j(\overline{\alpha}) = \overline{0}$, i.e. that $\overline{\alpha}$ is a root of P_j as well; since the $\overline{P}_i$ have no common roots, we conclude that $j = 1$.

Therefore the minimal polynomial $P_1(x)$ of ζ is also that of ζ^p for all $p \nmid n$. By iterating the argument, we see that it is also the minimal polynomial of ζ^k for any $k \in \mathbb{N}$ which is a product of primes not dividing n, i.e. for any k coprime to n. Thus all the primitive n-th roots of 1 are roots of P_1.

Conversely, let β be a root of P_1 in $\mathbb{C}$. Since P_1 is the minimal polynomial of ζ, and since $\mathbb{Q}(\zeta_n)$ is Galois over $\mathbb{Q}$, there exists $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ such that $\sigma(\zeta) = \beta$ (and in particular, $\beta \in \mathbb{Q}(\zeta)$). Then

$$\beta^n = \sigma(\zeta)^n = \sigma(\zeta^n) = \sigma(1) = 1,$$

so β is actually an n-th root of 1; besides, if $0 < m < n$, then

$$\beta^m = \sigma(\zeta)^m = \sigma(\zeta^m) \neq \sigma(1) = 1$$

as σ is injective and as $\zeta^m \neq 1$ since ζ is a *primitive* n-th root of 1. Therefore, so is β. In summary, the roots of P_1 are exactly the primitive n-th roots of 1, so $P_1 = \Phi_n(x)$ since both are monic and have the same roots (both without multiplicities, since P_1, being irreducible over $\mathbb{Q}$, is separable by theorem 2.2.11). (i) and (ii) follow; and since $\Phi_n(x) = P_1$ is the minimal polynomial of ζ over $\mathbb{Q}$, we also have

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \deg \Phi_n(x) = \phi(n)$$

which is (v).

The roots of $F(x)$ that are not roots of $\Phi_n(x)$ are the n-th roots of 1 that are not primitive, so each of them is a primitive d-th root of 1 and has thus minimal polynomial $\Phi_d(x)$ for some $d \mid n$. (iii) follows.

Finally, let $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$. We know by theorem 2.4.3 that

$$\Phi_n(x) = \prod_{\alpha \in G \cdot \zeta} (x - \alpha).$$

Since any $\sigma \in G$ is completely determined by $\sigma(\zeta)$, we deduce bijections

$$(\mathbb{Z}/n\mathbb{Z})^\times \longleftrightarrow \{\text{Primitive } n\text{-th roots of } 1\} = \{\text{Roots of } \Phi_n(x)\} \longleftrightarrow G$$

by attaching to $k \in (\mathbb{Z}/n\mathbb{Z})^\times$ the primitive root ζ^k, and to it, the $\sigma_k \in G$ such that $\sigma_k(\zeta) = \zeta^k$. The composite bijection

$$\begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z})^\times & \longrightarrow & G \\ k & \longmapsto & (\sigma_k : \zeta \mapsto \zeta^k) \end{array}$$

is actually an isomorphism, since

$$\sigma_k \sigma_{k'}(\zeta) = \sigma_k(\zeta^{k'}) = \sigma_k(\zeta)^{k'} = (\zeta^k)^{k'} = \zeta^{kk'} = \sigma_{kk'}(\zeta),$$

whence (vi). □

Remark 2.6.10. The relation

$$x^n - 1 = \prod_{d \mid n} \Phi_d(x)$$

shows that $\Phi_1(x) = x - 1$ (this also follows from the definition) and that for $p \in \mathbb{N}$ prime,

$$\Phi_p(x) = \frac{x^n - 1}{\Phi_1(x)} = \frac{x^n - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1$$

(sum of geometric series). More generally, this relation can be used to compute $\Phi_n(x)$ for general $n \in \mathbb{N}$.

Example 2.6.11. To compute $\Phi_{12}(x)$, we use

$$\Phi_{12}(x) = \frac{x^{12}-1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)\Phi_4(x)\Phi_6(x)};$$

we already know that $\Phi_1(x) = x-1$, $\Phi_2(x) = x+1$, $\Phi_3(x) = x^2+x+1$, and then we must compute

$$\Phi_4(x) = \frac{x^4-1}{\Phi_1(x)\Phi_2(x)} = \frac{x^4-1}{(x-1)(x+1)} = x^2+1$$

and

$$\Phi_6(x) = \frac{x^6-1}{\Phi_1(x)\Phi_2(x)\Phi_3(x)} = \frac{x^6-1}{(x-1)(x+1)(x^2+x+1)} = x^2-x+1,$$

so that finally

$$\Phi_{12}(x) = \frac{x^{12}-1}{(x-1)(x+1)(x^2+x+1)(x^2+1)(x^2-x+1)} = x^4-x^2+1.$$

Since the structure of $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ is so transparent, it is easy to apply the Galois correspondence to the n-th cyclotomic extension, and to deduce identities involving ζ_n.

Example 2.6.12. Let us take $n = 9$. We have

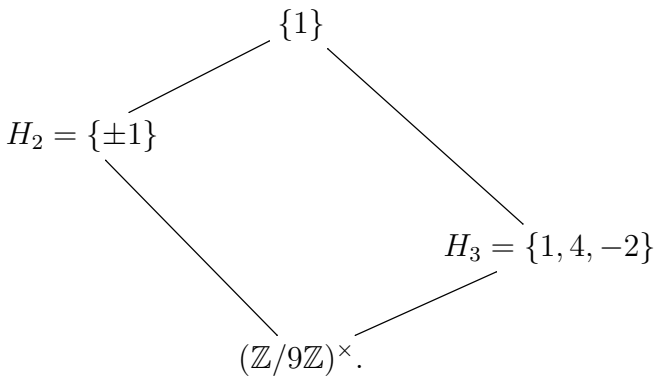
$$\Phi_9(x) = \frac{x^9-1}{\Phi_1(x)\Phi_3(x)} = \frac{x^9-1}{(x-1)(x^2+x+1)} = x^6+x^3+1,$$

and

$$\mathrm{Gal}(\mathbb{Q}(\zeta_9)/\mathbb{Q}) \simeq G = (\mathbb{Z}/9\mathbb{Z})^\times = \{1,2,4,-4,-2,-1\},$$

an Abelian group of order 6, which we identify with $\mathrm{Gal}(\mathbb{Q}(\zeta_9)/\mathbb{Q})$ from now on, remembering that $k \in (\mathbb{Z}/9\mathbb{Z})^\times$ means the automorphism of $\mathrm{Gal}(\mathbb{Q}(\zeta_9)/\mathbb{Q})$ sending ζ_9 to ζ_9^k. For instance, $-1 \in G$ is the complex conjugation.

The subgroup diagram is



Let us determine the corresponding intermediate extensions.

Let $E = \mathbb{Q}(\zeta_9)^{H_3}$. Then E is an extension of $\mathbb{Q}$ of degree $[G : H_3] = 2$ (the index of the subgroup) contains the elements

$$\zeta_9 + \zeta_9^4 + \zeta_9^{-2} = \frac{\zeta_9^3 + \zeta_9^6 + 1}{\zeta_9^2} = 0$$

(which teaches us nothing) and

$$\zeta_9 \zeta_9^4 \zeta_9^{-2} = \zeta_9^3 = \zeta_3,$$

so E is the third cyclotomic extension $\mathbb{Q}(\zeta_3)$.

Let now $F = \mathbb{Q}(\zeta_9)^{H_2} = \mathbb{Q}(\zeta_9) \cap \mathbb{R}$ since -1 is the complex conjugation. It is an extension of $\mathbb{Q}$ of degree 3, which contains $\zeta_9 \zeta_9^{-1} = 1$ (not interesting) and $\alpha = \zeta_9 + \zeta_9^{-1}$. We suspect that $\alpha \notin \mathbb{Q}$, and that actually $F = \mathbb{Q}(\alpha)$. In order to check this, we note that since G is Abelian, all its subgroups are normal, so F is Galois over $\mathbb{Q}$ (and so is E), of Galois group

$$\mathrm{Gal}(F/\mathbb{Q}) = G/H_2 = (\mathbb{Z}/9\mathbb{Z})^\times / \{\pm 1\} = \{1, 2, 4\}.$$

The elements

$$\beta = \zeta_9^2 + \zeta_9^{-2} = 2\cos(4\pi/9), \quad \gamma = \zeta_9^4 + \zeta_9^{-4} = 2\cos(8\pi/9)$$

are the images of α under $\mathrm{Gal}(F/\mathbb{Q})$; the fact (that can be checked with a calculator) that α, β, and γ are distinct means that $\alpha \notin F^{\mathrm{Gal}(F/\mathbb{Q})} = \mathbb{Q}$. Thus $\mathbb{Q} \subsetneq \mathbb{Q}(\alpha) \subseteq F$, and actually $F = \mathbb{Q}(\alpha)$ since $[F : \mathbb{Q}] = 3$ is prime.

The minimal polynomial of α over $\mathbb{Q}$ is

$$P(x) = \prod_{\sigma \in \mathrm{Gal}(F/\mathbb{Q})} \big(x - \sigma(\alpha)\big) = (x-\alpha)(x-\beta)(x-\gamma).$$

Its coefficientsare combinations of powers of ζ_9, ie. of roots of $\Phi_9(x)$, that must lie in $\mathbb{Q}$, so they must be combinations which are invariant by G, i.e. symmetric, so they should be expressible in terms of the coefficients of $\Phi_9(x)$ by proposition 1.1.8. More precisely, expanding

$$P(x) = (x - \zeta_9 - \zeta_9^{-1})(x - \zeta_9^2 - \zeta_9^{-2})(x - \zeta_9^4 - \zeta_9^{-4})$$

reveals that

- The coefficient of x^2 is

  $$-(\zeta_9 + \zeta_9^{-1} + \zeta_9^2 + \zeta_9^{-2} + \zeta_9^4 + \zeta_9^{-4})$$

  which is the negative of the sum of the roots of $\Phi_9(x)$, and therefore equal to the coefficient of x^5 of $\Phi_9(x)$, i.e. 0.

- The coefficient of x is the most annoying one. It is

  $$\begin{aligned}
  &(\zeta_9 + \zeta_9^{-1})(\zeta_9^2 + \zeta_9^{-2}) + (\zeta_9^2 + \zeta_9^{-2})(\zeta_9^4 + \zeta_9^{-4}) + (\zeta_9 + \zeta_9^{-1})(\zeta_9^4 + \zeta_9^{-4}) \\
  =&\zeta_9^3 + \zeta_9^{-1} + \zeta_9 + \zeta_9^{-3} + \zeta_9^6 + \zeta_9^{-2} + \zeta_9^2 + \zeta_9^{-6} + \zeta_9^5 + \zeta_9^{-3} + \zeta_9^3 + \zeta_9^{-5} \\
  =&\zeta_9^3 + \zeta_9^{-1} + \zeta_9 + \zeta_9^{-3} + \zeta_9^{-3} + \zeta_9^{-2} + \zeta_9^2 + \zeta_9^3 + \zeta_9^{-4} + \zeta_9^{-3} + \zeta_9^3 + \zeta_9^4 \\
  =&(\zeta_9 + \zeta_9^{-1} + \zeta_9^2 + \zeta_9^{-2} + \zeta_9^4 + \zeta_9^{-4}) + 3(\zeta_9^3 + \zeta_9^{-3}) \\
  =&\sum \text{Roots of } \Phi_9(x) + 3 \sum \text{Roots of } \Phi_3(x) \\
  =&(-\text{Coeff of } x^5 \text{ in } \Phi_9) + 3(-\text{Coeff of } x \text{ in } \Phi_3) \\
  =&-0 - 3 \\
  =&-3.
  \end{aligned}$$

- Finally, the constant coefficient is

$$\begin{aligned}
&-(\zeta_9+\zeta_9^{-1})(\zeta_9^2+\zeta_9^{-2})(\zeta_9^4+\zeta_9^{-4})\\
=&-(\zeta_9^2+\zeta_9^4+\zeta_9^6+\zeta_9^8+\zeta_9+\zeta_9^3+\zeta_9^5+\zeta_9^7) \quad (\text{Using } \zeta_9^9=1)\\
=&-\sum_{k=1}^{8}\zeta_9^k\\
=&1-\sum_{k=0}^{8}\zeta_9^k\\
=&1-\sum \text{Roots of } x^9-1\\
=&1-(\text{Coeff of } x^8 \text{ in } x^9-1)\\
=&1
\end{aligned}$$

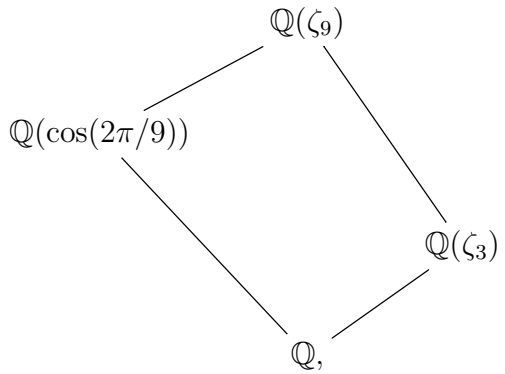
  (we could also have summed the geometric series).

Thus $P(x)=x^3-3x+1$.

It is also the minimal polynomial of β and γ, which are thus conjougate to α over $\mathbb{Q}$, so

$$F=\mathbb{Q}(\alpha)=\mathbb{Q}(\beta)=\mathbb{Q}(\gamma)=\mathbb{Q}\left(\cos\frac{2\pi}{9}\right)=\mathbb{Q}\left(\cos\frac{4\pi}{9}\right)=\mathbb{Q}\left(\cos\frac{8\pi}{9}\right).$$

In conclusion, the field diagram is



and we have discovered a polynomial relation satisfied by $\cos(2\pi/9)$, $\cos(4\pi/9)$, and $\cos(8\pi/9)$.

2.6.3 p-groups and constructibility

Definition 2.6.13. Let G be a group. The *centre* of G is the subset $Z(G)$ of elements which commute with all the elements of G:

$$Z(G) = \{z \in G \mid gz = zg \ \forall g \in G.\}$$

One checks easily that $Z(G)$ is actually a normal subgroup of G.

Definition 2.6.14. Let $p \in \mathbb{N}$ be prime. A *p-group* is a finite group whose order is of the form p^n for some integer $n \geqslant 1$.

Example 2.6.15. The dihedral group D_8 is a 2-group.

Proposition 2.6.16. *Let G be a p-group. Then the centre of $Z(G)$ contains elements other that the identity.*

Proof. Let $X = G$ viewed as a set, and define a left action of G on X by conjugation:

$$g \cdot x = gxg^{-1} \qquad (g \in G, x \in X = G).$$

Observe that a point $x \in X$ is fixed by all the element of G if and only if $x \in Z(G)$.

Write $\#G = p^n$. Let $x \in X$, and let $H_x \subseteq G$ be its stabiliser (i.e. the set of elements of g that commute with x). Then H_x is a subgroup, so $\#H_x = p^{m_x}$ for some $m_x \leqslant n$. This subgroup has no reason to be normal, so the set G/H_x of right classes of H_x is not a group in general, but we still have a bijection

$$\begin{array}{ccc} G/H_x & \longrightarrow & \text{Orbit of } x \\ gH_x & \longmapsto & g \cdot x, \end{array}$$

so the cardinal of the orbit of x is

$$\#(G/H_x) = \frac{\#G}{\#H_x} = p^{n-m_x}.$$

This is 1 if $m_x = n$, i.e. if $H_x = G$, i.e. if $x \in Z(G)$, and a multiple of p else.

The cardinal of the set X is p^n, which is a multiple of p. Besides, X is partitioned in orbits under G; of these orbits, exactly $\#Z(G)$ have size 1, and the others have size a multiple of p. Therefore $\#Z(G)$ is a multiple of p. In particular, $\#Z(G) \geqslant p$, so $Z(G)$ is not reduced to $\{1_G\}$. □

Corollary 2.6.17. *If $\#G = p^n$, then exists a chain of subgroups*

$$\{1_G\} = H_0 \subseteq H_1 \subseteq H_2 \subseteq \cdots \subseteq H_n = G$$

such that $\#H_i = p^i$ for all i.

Proof. We prove this by induction on n.

If $n = 0$, then $G = \{1_G\}$ and there is nothing to prove.

Let now $n \geqslant 1$, and suppose the corollary is true for $n-1$. Since G is a p-group, proposition 2.6.16 tells us that there exists a $z \neq 1_G$ in $Z(G)$. The order of z is thus > 1, and divides $\#G = p^n$, so it is of the form p^m for some $m \leqslant n$; then $z' = z^{p^{m-1}}$ is an element of order p of $Z(G)$. Let N be the subgroup generated by z'; then $N \simeq \mathbb{Z}/p\mathbb{Z}$, and N is normal since $z' \in Z(G)$ is invariant by conjugation. Let $\pi : G \longrightarrow G/N$ be the projection to the quotient group G/N. Then

$$\#(G/N) = \frac{\#G}{\#N} = \frac{p^n}{p} = p^{n-1},$$

so by the induction hypothesis, there exists a chain of subgroups

$$\{\overline{1_G}\} = \overline{H}_0 \subseteq \overline{H}_1 \subseteq \overline{H}_2 \subseteq \cdots \subseteq \overline{H}_{n-1} = G/N$$

where $\#\overline{H}_i = p^i$ for all i. Taking pre-images by π yields

$$N = \pi^{-1}(\overline{H}_0) \subseteq \pi^{-1}(\overline{H}_1) \subseteq \pi^{-1}(\overline{H}_2) \subseteq \cdots \subseteq \pi^{-1}(\overline{H}_{n-1}) = \pi^{-1}(G/N) = G,$$

where $\#\pi^{-1}(\overline{H}_i) = \#N\#\overline{H}_i = p^{i+1}$ for all i, so we complete the induction by setting $H_0 = \{1_G\}$ and $H_i = \pi^{-1}(\overline{H}_{i-1})$ for $i \geqslant 1$. □

Theorem 2.6.18. *Let $\alpha \in \mathbb{R}$ be algebraic over $\mathbb{Q}$, and let N be the Galois closure of $\mathbb{Q}(\alpha)$ over $\mathbb{Q}$. The following are equivalent:*

(i) $\mathrm{Gal}(N/\mathbb{Q})$ *is a 2-group,*

(ii) $[N : \mathbb{Q}]$ *is a power of 2,*

(iii) α *is constructible.*

Proof.

- (i) $\iff$ (ii) by theorem 2.4.3 since N is Galois over $\mathbb{Q}$ by definition.

- (i) $\Longrightarrow$ (iii): Let $G = \mathrm{Gal}(N/\mathbb{Q})$. If G is a 2-group, then by corollary 2.6.17 there exists a chain of subgroups

$$\{\mathrm{Id}\} = H_0 \subseteq H_1 \subseteq H_2 \subseteq \cdots \subseteq H_n = G$$

such that $[H_{i+1} : H_i] = 2$ for all i. By the Galois correspondence, we deduce that the subfields $E_i = N^{H_i}$ satisfy

$$\mathbb{Q} = E_n \subseteq E_{n-1} \subseteq \cdots \subseteq E_1 \subseteq E_0 = N$$

and that $[E_i : E_{i+1}] = 2$. Besides, we have $\mathbb{Q}(\alpha) \subseteq N$ by definition of N, whence $\alpha \in N = E_0$. By theorem 1.2.18, α is thus constructible.

- (iii) $\Longleftrightarrow$ (ii): Let $\alpha_1 = \alpha, \alpha_2, \cdots, \alpha_r$ be the conjugates of α in $\mathbb{C}$, so that we may take $N = \mathbb{Q}(\alpha 1, \cdots, \alpha_r)$. Since $\alpha = \alpha_1$ is constructible, theorem 1.2.18 ensures the existence of a chain of extensions

$$\mathbb{Q} = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = \mathbb{Q}(\alpha_1) \subseteq N \tag{2.6.19}$$

where for all i, $[K_{i+1} : K_i] = 2$, so that $K_{i+1} = K_i(\sqrt{k_i})$ for some $k_i \in K_i$ (cf. remark 1.2.7).

We now prove by induction on j that $\mathbb{Q}(\alpha_1, \alpha_2, \cdots, \alpha_j)$ for all $j \leqslant r$. Indeed, we have just seen that it is so for $j = 1$. Assume that it is the case for $j-1$, and let $E = \mathbb{Q}(\alpha_1, \cdots, \alpha_{j-1})$. By corollary 1.2.38, there exists $\sigma \in \mathrm{Gal}(N/\mathbb{Q})$ such that $\sigma(\alpha_1) = \alpha_j$. Applying this σ to (2.6.19) yields

$$\mathbb{Q} = \sigma(\mathbb{Q}) = K'_0 \subseteq K'_1 \subseteq \cdots \subseteq K'_n = \sigma(\mathbb{Q}(\alpha_1)) = \mathbb{Q}(\alpha_j) \subseteq \sigma(N) = N,$$

where $K'_i = \sigma(K_i)$. If we also define $k'_i = \sigma(k_i) \in K'_i$, then we have $K'_{i+1} = \sigma\big(K_i(\sqrt{k_i})\big) = K'_i(\sqrt{k'_i})$. Replacing $\mathbb{Q}$ with $E = \mathbb{Q}(\alpha_1, \cdots, \alpha_{j-1})$ then yields

$$E = E_0 \subseteq E_1 \subseteq \cdots \subseteq E_n = E(\alpha_j) = \mathbb{Q}(\alpha_1, \cdots, \alpha_{j-1}, \alpha_j),$$

where $E_i = K'_i(\alpha_1, \cdots, \alpha_{j-1})$ denotes the subfield of N generated by E and K'_i. In particular, we have $E_{i+1} = E_i(\sqrt{k'_i})$ for each i, so $[E_{i+1} : E_i] \leqslant 2$ (we had $\sqrt{k'_i} \notin K'_i$, but it may happen that $\sqrt{k'_i} \in E_i$). Therefore,

$$[\mathbb{Q}(\alpha_1, \cdots, \alpha_j) : \mathbb{Q}(\alpha_1, \cdots, \alpha_{j-1})] = [E_n : E_0] = \prod_{i<n} [E_{i+1} : E_i]$$

is a product of terms equal to 1 or 2, and is thus a power of 2, and so is

$$[\mathbb{Q}(\alpha_1, \cdots, \alpha_j) : \mathbb{Q})] = [\mathbb{Q}(\alpha_1, \cdots, \alpha_j) : \mathbb{Q}(\alpha_1, \cdots, \alpha_{j-1})][\mathbb{Q}(\alpha_1, \cdots, \alpha_{j-1}) : \mathbb{Q}]$$

by the induction hypothesis, which completes the induction step.

In the end, for $i = r$ we do find that $[N : \mathbb{Q}] = [\mathbb{Q}(\alpha_1, \cdots, \alpha_r) : \mathbb{Q}]$ is a power of 2.

□

Example 2.6.20. We can now explain what happened in remark 1.2.20: let $F(x) = x^4 - 8x^2 + 4x + 2 \in \mathbb{Q}[x]$, which is irreducible, and let $\alpha \in \mathbb{R}$ be one of its roots (they are all real). The $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$ is a power of 2, but its is not Galois over $\mathbb{Q}$! Its normal closure N is the splitting field of F, and we will prove in example 3.3.2 that $\mathrm{Gal}(N/\mathbb{Q})$ is isomorphic to the symmetric group S_4 acting by permutation on the 4 roots of F. Since $\#S_4 = 24$ is not a power of 2, α is not constructible!

In fact, let $\alpha_1 = \alpha, \alpha_2, \alpha_3, \alpha_4$ be the roots of F in N. To the (partial) subfield diagram

$$\begin{array}{c} N \\ | \\ \mathbb{Q}(\alpha) \\ | \\ \mathbb{Q} \end{array}$$

corresponds the (partial) subgroup diagram

$$\begin{array}{c} \{\mathrm{Id}\} \\ | \\ H \\ | \\ S_4, \end{array}$$

where $H \simeq S_3$ is the stabiliser of α_1 in S_4. If α were constructible, then by theorem 1.2.18, there would exist an intermediate field

$$\mathbb{Q} \subseteq E \subseteq \mathbb{Q}(\alpha)$$

such that both intermediate extensions have degree 2; this subfield would correspond to a subgroup H' of S_4 such that

$$H \subseteq H' \subseteq S_4$$

with both inclusions having index 2, but a little bit of group theory shows that no such subgroup of S_4 exists.

Example 2.6.21. On the contrary, let $\alpha = \sqrt{5+\sqrt{21}}$. We have seen in example 2.5.8 that $\mathbb{Q}(\alpha)$ is Galois over $\mathbb{Q}$, with Galois group $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ of order 2^2, and indeed α is constructible since square roots are constructible.

Similarly, for $\alpha = \sqrt{5+\sqrt{15}}$, we have seen in example 2.5.9 that the Galois group of the Galois closure of $\mathbb{Q}(\alpha)$ is the dihedral group D_8 of order 2^3, and indeed α is again constructible.

In fact, in both examples, we can see a chain of extensions of degree 2 from $\mathbb{Q}$ to $\mathbb{Q}(\alpha)$ on the subfield diagram.

Chapter 3

Methods to compute the Galois group

3.1 The Galois group of a polynomial

We now fix a field K and a monic, separable polynomial $F(x) \in K[x]$, and we denote by $\mathrm{Spl}_K(F)$ a splitting field of F over K (which is unique up to K-isomorphism by corollary 1.2.37). Then $\mathrm{Spl}_K(F)$ is a Galois extension of K by theorem 2.4.3.

Definition 3.1.1. The *Galois group of $F(x)$ over K* is

$$\mathrm{Gal}_K(F) \overset{\text{def.}}{=} \mathrm{Gal}(\mathrm{Spl}_K(F)/K).$$

This definition makes sense since $\mathrm{Spl}_K(F)$ is normal over K as it is a splitting field, and is separable over K since $F(x)$ is assumed to be separable. In what follows, we will denote by $\alpha_1, \cdots, \alpha_n$ the roots of $F(x)$ in $\mathrm{Spl}_K(F)$; thus $n = \deg F(X)$, and these roots are distinct.

Theorem 3.1.2. *$\mathrm{Gal}_K(F)$ is canonically isomorphic to a subgroup of the symmetric group S_n.*

Proof. The elements of $\mathrm{Gal}_K(F) = \mathrm{Gal}(\mathrm{Spl}_K(F)/K)$ preserve the roots of $F(x)$, so they permute them since they are injective. Besides, by definition $\mathrm{Spl}_K(F) = K(\alpha_1, \cdots, \alpha_n)$, so the elements of $\mathrm{Gal}_K(F)$ are completely determined by how they permute the α_i. □

Remark 3.1.3. In particular, $[\mathrm{Spl}_K(F) : K] = \#\,\mathrm{Gal}_K(F) \leqslant n!$. The fact that $[\mathrm{Spl}_K(F) : K] \leqslant n!$, and that this inequality is the best possible in general, is clear from the construction of $\mathrm{Spl}_K(F)$ given in example 1.2.35: enlarging K to $K(\alpha_1)$ results in an extension of degree $\leqslant \deg F(x) = n$, then enlarging $K(\alpha_1)$ to $K(\alpha_1, \alpha_2)$ results in an extension of degree $\leqslant \deg \frac{F(x)}{x-\alpha_1} = n - 1$, and so on.

Remark 3.1.4. One can show that "most" polynomials of degree n with coefficients in $\mathbb{Q}$ are irreducible, and have Galois group S_n.

Remark 3.1.5. Renumbering the roots of F amounts to conjugating $\mathrm{Gal}_K(F)$ by an element of S_n (the renumbering permutation). Since the ordering of the roots is not canonical, $\mathrm{Gal}_K(F)$ is technically speaking only defined as a subgroup of S_n up to conjugacy.

The way in which $\mathrm{Gal}_K(F)$ permutes the roots is reflected in the factorisation of $F(x)$ over K. More specifically,

Theorem 3.1.6. *Let*

$$\{\alpha_1, \cdots, \alpha_n\} = \coprod_{i=1}^{r} O_i$$

be the decomposition of the set of roots of $F(x)$ into a disjoint union of orbits under $\mathrm{Gal}_K(F)$. Then for each $i \leqslant r$, the polynomial

$$F_i(x) = \prod_{\alpha \in O_i} (x - \alpha)$$

lies in $K[x]$ and is irreducible over K. In particular,

$$F(x) = \prod_{i=1}^{r} F_i(x)$$

is the complete factorisation of $F(x)$.

Proof. This is because according to theorem 2.4.3 part (iv), $F_i(x)$ is the minimal polynomial of each of its roots. □

Corollary 3.1.7. $\mathrm{Gal}_K(F)$ *acts transitively on the roots of $F(x)$ iff. $F(x)$ is irreducible over K.*

Corollary 3.1.8. *If $F(x)$ factors as $F_1(x)F_2(x)\cdots F_r(x)$ over K, then*

$$\mathrm{Gal}_K(F) = \mathrm{Gal}_K(F_1) \times \mathrm{Gal}_K(F_2) \times \cdots \times \mathrm{Gal}_K(F_r).$$

We now wish to have recipes to determine $\mathrm{Gal}_K(F)$ as a subgroup of S_n, especially in the case $K = \mathbb{Q}$. We see from the above that we should start by checking if $F(x)$ is irreducible, and by determining its factorisation if it is not. For this, Eisenstein's criterion is often useful, and so is the following result:

Proposition 3.1.9. *Let $F(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. If $p/q \in \mathbb{Q}$ is a root of $F(x)$ written in lowest terms (i.e. $\gcd(p,q) = 1$), then $p \mid a_0$ and $q \mid a_n$.*

Proof. We have

$$0 = q^n F(p/q) = a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} + a_0 q^n.$$

Rewriting this as

$$a_n p^n = -a_{n-1}p^{n-1}q - \cdots - a_1 pq^{n-1} - a_0 q^n = -q(a_{n-1}p^{n-1} + \cdots + a_1 pq^{n-2} + a_0 q^{n-1})$$

shows that $q \mid a_n p^n$, whence $q \mid a_n$ since $\gcd(q, p^n) = 1$. Similarly, we have

$$a_0 q^n = -p(a_n p^{n-1} + a_{n-1}p^{n-2}q + \cdots + a_1 q^{n-1}),$$

so $p \mid a_0 q^n$, whence $p \mid a_0$ as $\gcd(p, q^n) = 1$. □

3.2 Method 1: The discriminant and Lagrange resolvents

3.2.1 Reminders on permutations

Recall that each element $\sigma \in S_n$ may be uniquely decomposed s a product of cycles with disjoint support (and that these cycles commute with each other since they have disjoint support). For instance, the element

$$\sigma\colon 1 \mapsto 6,\ 2 \mapsto 3,\ 3 \mapsto 2,\ 4 \mapsto 1,\ 5 \mapsto 5,\ 6 \mapsto 4 \tag{3.2.1}$$

of S_6 decomposes as $\sigma = (164)(23)$ (apply σ iteratively to 1, etc.), a product of a 3-cycle and of a 2-cycle.

Also recall that for any $\sigma \in S_n$, the *sign* of σ is

$$\epsilon(\sigma) = \prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

Then $\epsilon(\sigma) \in \{\pm 1\}$ for all $\sigma \in S_n$, and the map $\epsilon : S_n \longrightarrow \{\pm 1\}$ is a group morphism, which is surjective (unless $n = 1$ of course). Its kernel is called the *alternate* group, and is denoted by A_n. It is a normal subgroup of S_n since it is a kernel.

In practice, the sign of $\sigma \in S_n$ is easy to read off the decomposition of σ as a product of cycles, since the sign of a k-cycle is $(-1)^{k+1}$. For instance, the permutation σ defined by (3.2.1) has sign $(-1)^4(-1)^3 = +1 \cdot -1 = -1$, so $\sigma \notin A_6$.

3.2.2 The discriminant

The definition of the sign of the permutation has the following consequence:

Theorem 3.2.2. *Let $\Delta_F \in K$ be the discriminant of $F(x)$. Then $\mathrm{Gal}_K(F) \subseteq A_n$ iff. Δ_F is a square in K.*

Proof. Let $\delta_F = \prod_{1 \leqslant i < j \leqslant n} (\alpha_j - \alpha_i) \in \mathrm{Spl}_K(F)$. Then $\Delta_F = \delta_F^2$ by theorem 1.1.17; in particular, $\delta_F \neq 0$. Besides, the definition of the sign of a permutation shows that it is equal to the parity of the number of pairs (i, j) such that $1 \leqslant i < j \leqslant n$ but $\sigma(i) > \sigma(j)$, whence

$$\sigma(\delta_F) = \varepsilon(\sigma)\delta_F$$

for all $\sigma \in \mathrm{Gal}_K(F)$. Thus

$$\begin{aligned}
\mathrm{Gal}_K(F) \subseteq A_n &\iff \forall \sigma \in \mathrm{Gal}_K(F),\ \varepsilon(\sigma) = +1 \\
&\iff \forall \sigma \in \mathrm{Gal}_K(F),\ \sigma(\delta_F) = \delta_F \\
&\iff \delta_F \in \mathrm{Spl}(F)^{\mathrm{Gal}_K(F)} = K \\
&\iff \Delta_F \text{ is a square in } K.
\end{aligned}$$

□

Example 3.2.3. Suppose $F(x)$ has degree $n = 3$, so that $\mathrm{Gal}_K(F) \subseteq S_3$. In view of theorem 3.1.6, if $F(x)$ splits completely over K, then $\mathrm{Gal}_K(F) = \{\mathrm{Id}\}$, whereas if $F(x)$ splits over K as $(x - \alpha_1)G(x)$ where $G(x) \in K[x]$ is

irreducible of degree 2, then $\mathrm{Gal}_K(F) = \{\mathrm{Id}, \sigma\}$ where $\sigma = (23)$ permutes the roots of $G(x)$.

Suppose now that $F(x)$ is irreducible over K. Then $\mathrm{Gal}_K(F)$ acts transitively on its 3 roots, so it contains at least 3 elements; thus $\mathrm{Gal}_K(F)$ is either S_3 or $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$. Theorem 3.2.2 then allows us to tell these cases apart: indeed, if the discriminant of $F(x)$ is a square in K, then $\mathrm{Gal}_K(F) = A_3$, else $\mathrm{Gal}_K(F) = S_3$.

In general, discriminants are difficult to compute by hand. However, for depressed polynomials, we have the following formula:

Proposition 3.2.4. *(Non examinable) For all $n \in \mathbb{N}$ and $b, c \in K$, we have*

$$\mathrm{disc}(x^n + bx + c) = (-1)^{n(n-1)/2}\big((1-n)^{n-1}b^n + n^n c^{n-1}\big).$$

Proof. [1]

Let ζ be a primitive $(n-1)$-th root of 1, and β be such that $\beta^{n-1} = -b/n$ (both these elements lying in an algebraic closure of K containing $\mathrm{Spl}_K(x^n + bx + c)$).

According to theorem 1.1.12, the resultant of P and P' can be computed in two ways: as the product of the values of P at the roots of P' (essentially), and vice versa. Here, the first way is easier, because the roots of P' are easy to express and manipulate. Explicitly, we have $P'(x) = nx^{n-1} + b$, whose complex roots are the $\zeta^k\beta$, $0 \leqslant k < n-1$, and

$$P(\zeta^k\beta) = \zeta^{kn}\beta^n + b\zeta^k\beta + c = \zeta^k\left(-\frac{\beta}{n}\right) + b\zeta^k\beta + c = \left(1 - \frac{1}{n}\right)\beta\zeta^k b + c.$$

[1] In this proof, we assume for simplicity that K has characteristic 0, e.g so that we may divide by n; but the formula remains valid without this hypothesis.

Therefore,

$$\begin{aligned}
\operatorname{Res}(P,P') &= n^n \prod_{k=0}^{n-2} P(\zeta^k\beta) \qquad \text{because the leading coefficient of } P' \text{ is } n \\
&= n^n \prod_{k=0}^{n-2} \left(\left(1-\frac{1}{n}\right)\beta\zeta^k b + c \right) \\
&= n^n (-1)^{n-1} \prod_{k=0}^{n-2} \left(-c - \zeta^k \left(1-\frac{1}{n}\right)\beta b \right) \\
&= n^n (-1)^{n-1} \left(\big(-c\big)^{n-1} - \big((1-1/n)\beta b\big)^{n-1} \right) \text{ as } \prod_{k=0}^{n-2}(x-\zeta^k y) = x^{n-1}-y^{n-1} \\
&= n^n c^{n-1} - n^n \beta^{n-1} b^{n-1} (1/n-1)^{n-1} \\
&= n^n c^{n-1} - n\left(-\frac{b}{n}\right)(1-n)^{n-1} b^{n-1} \\
&= n^n c^{n-1} + (1-n)^{n-1} b^n.
\end{aligned}$$

The result then follows since $\operatorname{disc} P = (-1)^{n(n-1)/2} \operatorname{Res}(P,P')$. □

Corollary 3.2.5. *(Examinable) In particular, we obtain the important formulae*

$$\operatorname{disc}(x^2+bx+c) = b^2-4c, \qquad \operatorname{disc}(x^3+bx+c) = -4b^3-27c^2,$$

which you should learn by heart.

3.2.3 Lagrange resolvents

(Section 3.2.3 is not examinable.)

The argument of the proof of theorem 3.2.2 may be understood as follows: Let

$$\delta(x_1,\cdots,x_n) = \prod_{1\leqslant i<j\leqslant n} (x_j - x_i) \in K[x_1,\cdots,x_n].$$

If we apply a permutation $\sigma \in \S_n$ to the variables of δ, then δ is preserved if $\sigma \in A_n$, and negated else. Therefore, if we choose $\tau \in S_n \setminus A_n$, then the

polynomial

$$\begin{aligned} R_\delta(x; x_1, \cdots, x_n) &= \big(x - \delta(x_1, \cdots, x_n)\big)\big(x - \delta(x_{\tau(1)}, \cdots, x_{\tau(n)})\big) \\ &= x^2 - \delta(x_1, \cdots, x_n)^2 \in K[x, x_1, \cdots, x_n] \end{aligned}$$

is invariant under any permutation of $x_1, \cdots, x_n$. As a result, if we plug in $x_1 = \alpha_1, \cdots, x_n = \alpha_n$ where the α_i are the roots of $F(x)$, then we get $R_\delta(X; \alpha_1, \cdots, \alpha_n) \in K[x]$, and this polynomial splits over K iff. $\mathrm{Gal}_K(F) \subseteq A_n$.

This arguments can be generalised to other subgroups of S_n, by replacing $\delta(x_1, \cdots, x_n)$ by an appropriately "partially symmetric" polynomial. More specifically, fix a subgroup $H \subset S_n$, let $r = [S_n : H]$ be its index, and let $h(x_1, \cdots, x_n) \in K[x_1, \cdots, x_n]$ be such that the permutations of the variables $x_1, \cdots, x_n$ that leave $h(x_1, \cdots, x_n)$ invariant are exactly the elements of H. Then we can get exactly r distinct polynomials by permuting the variables $x_1, \cdots, x_n$ of h, i.e. the orbit of $h(x_1, \cdots, x_n)$ under S_n has exactly r elements. Let $\tau_1, \cdots, \tau_r \in S_n$ form a right transversal of H, i.e. be such that $S_n = \coprod_{i=1}^r \tau_i H$ is the disjoint union of the $\tau_i H$; then the r polynomials $h(x_{\tau_i(1)}, \cdots, x_{\tau_i(n)})$ are exactly the elements of the orbit of $h(x_1, \cdots, x_n)$ under S_n. We thus define

Definition 3.2.6. The *Lagrange resolvent of* $F(x)$ with respect to $h(x_1, \cdots, x_n)$ is

$$R_h(x) = \prod_{i=1}^{r} \big(x - h(\alpha_{\tau_i(1)}, \cdots, \alpha_{\tau_i(n)})\big).$$

By the same argument as above, the coefficients of $R_h(x)$ are invariant under $S_n \supseteq \mathrm{Gal}_K(F)$, so $R_h(x) \in K[x]$.

Theorem 3.2.7. *Suppose $R_h(x)$ has no repeated root. Then $R_h(x)$ has a root in K iff. $\mathrm{Gal}_K(F)$ is conjugate to a subgroup of H.*

Proof. Let S_n act on $K[x_1, \cdots, x_n]$ by $\sigma \cdot g(x_1, \cdots, x_n) = g(x_{\sigma(1)}, \cdots, x_{\sigma(n)})$,

and let $y_i = h(\alpha_{\tau_i(1)}, \cdots, \alpha_{\tau_i(n)})$ be a root of $R_h(x)$. Then

$$\begin{aligned}
y_i \in K &\iff \forall \sigma \in \mathrm{Gal}_K(F),\ \sigma(y_i) = y_i \\
&\iff \forall \sigma \in \mathrm{Gal}_K(F),\ h(\alpha_{\sigma\tau_i(1)}, \cdots, \alpha_{\sigma\tau_i(n)}) = h(\alpha_{\tau_i(1)}, \cdots, \alpha_{\tau_i(n)}) \\
&\iff \forall \sigma \in \mathrm{Gal}_K(F),\ h(x_{\sigma\tau_i(1)}, \cdots, x_{\sigma\tau_i(n)}) = h(x_{\tau_i(1)}, \cdots, x_{\tau_i(n)}) \\
&\iff \forall \sigma \in \mathrm{Gal}_K(F),\ \sigma\tau_i \cdot h = \tau_i \cdot h \\
&\iff \forall \sigma \in \mathrm{Gal}_K(F),\ \tau_i^{-1}\sigma\tau_i \cdot h = h \\
&\iff \forall \sigma \in \mathrm{Gal}_K(F),\ \tau_i^{-1}\sigma\tau_i \in H \\
&\iff \tau_i^{-1}\,\mathrm{Gal}_K(F)\tau_i \subseteq H \\
&\iff \mathrm{Gal}_K(F) \subseteq \tau_i H \tau_i^{-1},
\end{aligned}$$

where we have used the fact that the roots are pairwise distinct for the equivalence between the second and third lines. □

Remark 3.2.8. The resolvent $R_h(x)$ does not depend on the chosen ordering of the roots α_i of $F(x)$. Since choosing a different ordering amounts to replacing $\mathrm{Gal}_K(F)$ with a conjugate subgroup of S_n, it is not surprising that the theorem gives information on $\mathrm{Gal}_K(F)$ only up to conjugacy. However, the proof shows that once the ordering of the α_i has been fixed, determining which root of $R_h(x)$ lies in K shows which conjugate of H $\mathrm{Gal}_K(F)$ is contained in.

The point of this method is that one can determine $\mathrm{Gal}_K(F)$ as a subgroup of S_n by computing $R_h(x)$ for various $h(x_1, \cdots, x_n)$ corresponding to various subgroups $H \subset S_n$. Suitably optimised, this method is very efficient; it is due to Stauduhar (1973).

Example 3.2.9. The permutations of $\mathbb{F}_5$ induced by the maps $x \mapsto ax + b$ for $a \in \mathbb{F}_5\times$ and $b \in \mathbb{F}_5$ form a subgroup of S_5 of order $(\#\mathbb{F}_5^\times)(\#\mathbb{F}_5) = 20$ and thus of index 6, and it happens that the subgroup of S_5 leaving

$$\begin{aligned}
h = x_1^2(x_2x_5 + x_3x_4) + x_2^2(x_1x_3 + x_4x_5) + x_3^2(x_1x_5 + x_2x_4) \\
+ x_4^2(x_1x_2 + x_3x_5) + x_5^2(x_1x_4 + x_2x_3)
\end{aligned}$$

invariant is precisely H.

Let $F(x) = x^5 - x^4 + 2x^3 - 4x^2 + x - 1 \in \mathbb{Q}[x]$. With the help of a computer, we check that F is irreducible over $\mathbb{Q}$, so $\mathrm{Gal}_{\mathbb{Q}}(F)$ is a transitive

subgroup of S_5, and we find that

$$\{\mathrm{Id},\ (12),\ (13),\ (14),\ (15),\ (25)\}$$

is a right transversal for H, and that

$$R_h(x) = x^6 - 104x^4 + 2704x^2 - 35152x,$$

which has no repeated root. Since it obviously has a rational root, we conclude that $\mathrm{Gal}_{\mathbb{Q}}(F)$ is conjugate to a subgroup of H, i.e. that there exists an indexation of the 5 roots of $F(x)$ (in $\mathbb{C}$ for instance) by $\mathbb{F}_5$ such that the permutations induced by $\mathrm{Gal}_{\mathbb{Q}}(F)$ are all induced by maps from $\mathbb{F}_5$ to $\mathbb{F}_5$ of the form $x \mapsto ax + b$.

One also shows that the subgroups of H which are still transitive are H itself, the dihedral group D_{10} of symmetries of the pentagon (corresponding to restricting to $a \in \{\pm 1\}$, and the cyclic group $\mathbb{Z}/5\mathbb{Z}$ (corresponding to restricting to $a = 1$), which is contained in D_{10}. In particular, if the inclusion $\mathrm{Gal}_{\mathbb{Q}}(F) \subset H$ is strict, then $\mathrm{Gal}_{\mathbb{Q}}(F)$ is contained in D_{10}. However, one checks with a computer that the Lagrange resolvent attached to a polynomial h' with symmetry group D_{10} has no rational root (e.g. using proposition 3.1.9), so we can conclude that $\mathrm{Gal}_{\mathbb{Q}}(F) = H$.

3.3 Method 2: Reduction mod p

Although Stauduhar's method presented above is completely general, it is not well-suited to pen-and-paper calculations. We present another approach, due to Dedekind, which is less general but often allows one to conclude if $\deg F(x)$ is low.

Theorem 3.3.1. *Let $F(x) \in \mathbb{Z}[x]$ be monic and separable, and let $p \in \mathbb{N}$ be a prime.*

(i) $\mathrm{disc}(F) \in \mathbb{Z}$, *and we have* $\mathrm{disc}(F \bmod p) = \mathrm{disc}(F) \bmod p$; *in particular,* $F \bmod p$ *has no repeated factor for all but finitely many* p.

(ii) Suppose that $F \bmod p \in \mathbb{F}_p[x]$ *has no repeated factor, and let* $d_1, d_2, \cdots$ *be the degrees of its irreducible factors in* $\mathbb{F}_p[x]$. *Then* $\mathrm{Gal}_{\mathbb{Q}}(F)$ *contains an element whose decomposition into disjoint cycles is* $c_1 c_2 \cdots$ *where* c_1 *is a* d_1*-cycle,* c_2 *is a* d_2*-cycle, etc.*

Before we prove this theorem let us give an example of its use.

Example 3.3.2. Let $F(x) = x^4 - 8x^2 + 4x + 2$. Then F is irreducible over $\mathbb{Q}$ since it is Eisenstein at $p = 2$, so $\mathrm{Gal}_{\mathbb{Q}}(F)$ is a transitive subgroup of S_4. One can how that the transitive subgroups of the symmetric group S_4 are

- S_4 itself,
- the alternate group A_4,
- the dihedral group D_8 of symmetries of the square,
- the Klein group $V_4 = \{\mathrm{Id}, (12)(34), (13)(24), (14)(23)\} \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$,
- and the cyclic group $\mathbb{Z}/4\mathbb{Z}$,

so $\mathrm{Gal}_{\mathbb{Q}}(F)$ is one of these. Besides, one checks with a computer that

$$\mathrm{disc}\, F = 89344 = 2^3 \cdot 349,$$

which is not a square in $\mathbb{Q}$; so $\mathrm{Gal}_{\mathbb{Q}}(F) \not\subset A_4$ by theorem 3.2.2.

Mod $p = 2$, $F(x)$ factors as x^4, which has repeated factors so theorem 3.3.1 does not apply, and we cannot conclude anything.

Mod $p = 3$, $F(x)$ has the root -1, so factors as $(x+1)G(x)$ where $G(x) \in \mathbb{F}_3[x]$ has degree 3. We compute by Euclidean division in $\mathbb{F}_3[x]$ that $G(x) = x^3 - x^2 - x - 1$. Since neither of $0, 1, -1 \in \mathbb{F}_3$ is a root of $G(x)$, and since $\deg G(x) = 3$, we conclude that $G(x)$ is irreducible over $\mathbb{F}_3$. In summary, $F(x)$ factors mod 3 as $1 + 3$, so $\mathrm{Gal}_{\mathbb{Q}}(F)$ contains a 3-cycle.

The only groups in the list above that contain a 3-cycle are S_4 and A_4. Since we know that $\mathrm{Gal}_{\mathbb{Q}}(F) \not\subset A_4$, we conclude that $\mathrm{Gal}_{\mathbb{Q}}(F) = S_4$.

Theorem 3.3.1 is frequently used by factoring $F(x)$ mod various small primes p, and deducing that $\mathrm{Gal}_K(F)$ contains elements that imply that $\mathrm{Gal}_K(F) = S_n$. The following result goes in this direction:

Proposition 3.3.3. *Let $H \subseteq S_n$ be a transitive subgroup. If H contains a 2-cycle and an $(n-1)$-cycle, then $H = S_n$.*

Proof. After suitable relabelling, we may assume that the $(n-1)$ cycle is $\sigma = (12 \cdots n-1)$. Let (a, b) be the 2-cycle; then a and b are determined since we have fixed a relabelling, but we do not know their values. However, since H is

transitive, there exists $h \in H$ such that $h(b) = n$, so H contains $h(a,b)h^{-1} = (h(a), n)$; we may therefore assume without loss of generality that $b = n$, and thus that $a \neq n$.

Next, for each $x \in Z$, H contains $\sigma^x(a,n)\sigma^{-x} = (\sigma^x(a), n)$ since $\sigma(n) = n$. But σ acts transitively (and indeed cyclically) on

$$\{1, 2, \cdots, n-1\},$$

so we get that H contains $(1,n),\ (2,n),\ , \cdots,\ (n-1,n)$. It follows that for ll $i \neq j$ that are different from n, H contains

$$(i,n)(j,n)(i,n) = (i,j).$$

Thus H contains all the 2-cycles. Since the 2-cycles generate S_n, we conclude that $H = S_n$. □

Example 3.3.4. Let $F(x) = x^5 + x^2 + 1$. One checks that the complete factorisation of $F(x)$ mod 3 is

$$F(x) \equiv (x-1)(x^4 + x^3 + x^2 - x - 1) \bmod 3,$$

so that $\mathrm{Gal}(F)$ contains a 4-cycle, and that the complete factorisation of $F(x)$ mod 5 is

$$F(x) \equiv (x^2 - x + 2)(x^3 + x^2 - x - 2) \bmod 5,$$

so that $\mathrm{Gal}(F)$ contains an element σ which acts as the product of a 2-cycle and of a 3-cycle; in particular, σ^3 is a 2-cycle. By proposition 3.3.3, this forces

$$\mathrm{Gal}_{\mathbb{Q}}(F) = S_5.$$

Remark 3.3.5. Beware however that the information obtained by factoring mod different primes does not correlate. For instance, if $F(x)$ has a root mod p_1 and also a root mod p_2, then we get two elements of $\mathrm{Gal}_{\mathbb{Q}}(F)$ that each fix a root, but we cannot be sure if these are the same root.

In order to make full use of theorem 3.3.1, we must be able to factor polynomials mod p. The presentation of sophisticated methods such as Berlekamp's algorithm would take us too far from our topic, so we content ourselves with the following results:

Proposition 3.3.6.

(i) Let K be a perfect field, and let $F(x) \in K[x]$. Then $F(x)$ has repeated factors iff. $\gcd(F, F') \neq 1$.

(ii) Let $p \in \mathbb{N}$ be prime, let $n \in \mathbb{N}$, and let $q = p^n$. Then we have the identity

$$\prod_{\substack{P(x) \in \mathbb{F}_p[x] \\ \text{irreducible, monic,} \\ \deg(P) | n}} P(x) = x^q - x \in \mathbb{F}_p[x].$$

(iii) Let $F(x) \in \mathbb{F}_p[x]$, and let $n \in \mathbb{N}$. Then F has irreducible factors of degree dividing n iff. $\gcd(F, x^{p^n} - x) \neq 1$.

Proof.

(i) Suppose $P(x)$ is a nontrivial common factor of F and of F'. By replacing P with one of its irreducible factors, we may assume that P is irreducible. Since K is perfect, we then have $P' \neq 0$ by proposition 2.2.8, whence $\gcd(P, P') = 1$ by considering the degrees. Besides, $P \mid F$, so we can write $F = PQ$ with $Q \in K[x]$, and then $P \mid F' = P'Q + PQ'$ so $P \mid P'Q$, whence $P \mid Q$ since P and P' are coprime. As a result, $P^2 \mid F$.

Conversely, if we can factor $F = A^e B$ with $e > 1$, then $F' = eA'A^{e-1}B + A^e B'$, so A is a common factor of F and of F'.

(ii) Let $F(x) = x^q - x \in \mathbb{F}_p[x]$. Then $F' = qx^{q-1} - 1 = -1$ since $q = 0$ in $\mathbb{F}_p$, so F has no repeated factors by (i).

Recall from the proof of theorem 1.3.18 that

$$\mathbb{F}_q = \{\alpha \in \overline{\mathbb{F}}_p \mid \alpha^q = \alpha\} = \{\alpha \in \overline{\mathbb{F}}_p \mid F(\alpha) = 0\}.$$

So if $P(x) \in \mathbb{F}_p[x]$ is an irreducible factor of $F(x)$, and if $\alpha \in \overline{\mathbb{F}}_p$ is a root of P, then α is also a root of F, so $\alpha \in \mathbb{F}_q$, whence $\mathbb{F}_p(\alpha) \subseteq \mathbb{F}_q$ and

$$\deg P = [\mathbb{F}_p(\alpha) : \mathbb{F}_p] \mid [\mathbb{F}_q : \mathbb{F}_p] = n.$$

Conversely, let $P(x) \in \mathbb{F}_p[x]$ be irreducible of degree $d \mid n$, and let $\alpha \in \overline{\mathbb{F}_p}$ be one of its roots. Then $[\mathbb{F}_p(\alpha) : \mathbb{F}_p] = \deg P = d$ so $\mathbb{F}_p(\alpha) \simeq \mathbb{F}_{p^d}$, whence $\alpha^{p^d} = \alpha$, so that $\alpha^{p^{di}} = \alpha$ for all $i \in \mathbb{N}$; in particular, $\alpha^q = \alpha$, so $F(\alpha) = 0$. But since P is irreducible, it is the minimal polynomial of α, so $P \mid F$.

(iii) Follows immediately from (ii).

□

Example 3.3.7. Let us use proposition 3.3.6 to factor $F(x) = x^5 - x + 1$ mod 2, and then mod 3.

Mod $p = 2$, we find by the Euclidean algorithm that $\gcd(F, F') = 1$, so all factors of F are simple. We compute that $\gcd(F, x^2 - x) = 1$, so F has no roots mod 2 (it would have been easier to check directly that neither 0 nor 1 is a root mod 2!), and that $\gcd(F, x^4 - x) = x^2 + x + 1$, which shows that $x^2 + x + 1$ is the unique irreducible factor of degree 2 of F over $\mathbb{F}_2$. The cofactor $F/(x^2 + x + 1) = x^3 + x^2 + 1$ is prime because if it were not, it would have a factor of degree 1 or 2, but this factor would also be a factor of F so we would already have found it. In conclusion, the complete factorisation of F over $\mathbb{F}_2$ is

$$(x^2 + x + 1)(x^3 + x^2 + 1).$$

Mod $p = 3$, we see that F has no roots in $\mathbb{F}_3$, and we compute that

$$\gcd(F, x^9 - x) = 1,$$

so F has no irreducible factor of degree 2 either. As a result, F is irreducible mod 3 (for else it would have a factor of degree at most 2, since it has degree 5).

Remark 3.3.8. Conversely, *Cebotarev's density theorem* (which is beyond the scope of these notes) shows that if one picks p "at random", then one hits all the elements of $\mathrm{Gal}_{\mathbb{Q}}(F)$ with equal probability. In particular, in the previous example, we can predict that F will have 3 linear factors and one irreducible quadratic factor mod p for one prime p in $\#S_5/10 = 12$, since there are 10 transpositions in S_5, and that F will split completely mod p for one prime p in $\#S_5/\{\mathrm{Id}\} = 120$.

We are now going to prove theorem 3.3.1. First, we need two preliminary results about ideals.

Lemma 3.3.9 (Maximal ideals)**.** *Let R be a commutative ring, and $I \subset R$ an ideal. Then R/I is a field iff. I is* maximal*, in the sense that $I \subsetneq R$ and if $I \subseteq J \subseteq R$ is another ideal, then $J = I$ or $J = R$.*

Proof. Suppose I is maximal, and let $\overline{x} \in R/I$ be nonzero, i.e. $x \in R$ but $x \notin I$. Then the ideal $I + xR$ is strictly larger than I, so it is the whole of R by maximality of I. In particular, it contains 1, so we may write $1 = i + xy$ for some $i \in I$ and $y \in R$; but then $\overline{xy} = \overline{1}$, which shows that R/I is a field.

Conversely, suppose that R/I is a field, and let $J \supsetneq I$ be an ideal. We can find $x \in J$ such that $x \notin I$, but then $\overline{x} \neq \overline{0} \in R/I$; as R/I is a field, there exists an $y \in R$ such that $\overline{xy} = \overline{1} \in R/I$, whence $xy = 1 + i$ for some $i \in I$. But then $J \ni xy - i = 1$, so $J = R$. □

Lemma 3.3.10 (Chinese remainders)**.** *Let R be a commutative ring, let $I_1, \cdots, I_n$ be ideals of R with are* pairwise coprime*, i.e $I_i + I_j = R$ for all $i \neq j$, and let $I = \bigcap_{i=1}^{n} I_i$. Then for each I, we have $I \subseteq I_i$, whence a projection morphism $R/I \longrightarrow R/I_i$; and the morphism*

$$\varphi : R/I \longrightarrow \prod_{i=1}^{n} R/I_i$$

induced by these projections is a ring isomorphism.

Proof. By assumption, for each pair (i, j) with $i \neq j$, we may write

$$1 = e_{i,j} + e_{j,i}$$

where $e_{i,j} \in I_i$ and $e_{j,i} \in I_j$. Define

$$e_i = \prod_{j \neq i} e_{j,i}$$

for each i. Then clearly $e_i \in \bigcap_{j \neq i} I_j$, so $e_i \equiv 0 \bmod I_j$ for all $j \neq i$; besides $e_i \equiv 1 \bmod I_i$ as $e_i = \prod_{j \neq i}(1 - e_{i,j})$. In other words,

$$\varphi(e_i) = (0, \cdots, 0, \underset{\substack{\uparrow \\ i}}{1}, 0 \cdots, 0).$$

As a result, the morphism

$$\begin{array}{rcl} \displaystyle\prod_{i=1}^{r} R/I_i & \longrightarrow & R/I \\ (\overline{x}_1, \cdots, \overline{x}_r) & \longmapsto & \displaystyle\sum_{i=1}^{r} x_i e_i \end{array}$$

is well defined, since

$$\overline{x}_i = \overline{y}_i \Longrightarrow x_i - y_i \in I_i \Longrightarrow x_i e_i - y_i e_i \in I_i \cap \bigcap_{j \neq i} I_j = I,$$

and is the inverse of φ. □

Proof of theorem 3.3.1.

Write $F(x) = x^n + \sum_{k=0}^{n-1} a_k x^k$, so that $a_k \in \mathbb{Z}$ for each k. Also write $\overline{F}$ for $F \bmod p \in \mathbb{F}_p[x]$.

(i) Since F is monic, $\operatorname{disc}(F)$ is up sign the resultant of F and F', which is a determinant involving the a_k; the fact that $\operatorname{disc}(F) \in \mathbb{Z}$ and the relation $\operatorname{disc}(\overline{F}) = \operatorname{disc}(F) \bmod p$ follow. Besides $\operatorname{disc} F \neq 0$ as F is separable, so $\operatorname{disc} F$ has finitely many prime divisors. But by the above, $\overline{F}$ is inseparable iff. $\operatorname{disc}(F)$ is 0 mod p, i.e. iff. p is one of these prime divisors.

(ii) Consider the subring $\mathcal{O} = \mathbb{Z}[\alpha_1, \cdots, \alpha_n]$ of $\operatorname{Spl}_K(F)$ generated by the roots of F. It is stable under $\operatorname{Gal}_{\mathbb{Q}}(F)$ as the latter permutes the α_i. Since F is monic, we have

$$\alpha_i^n = -\sum_{k=0}^{n-1} a_k \alpha_i^k$$

for each i, so $\mathcal{O}$ is generated as a $\mathbb{Z}$-module by the $\alpha_1^{k_1} \cdots \alpha_n^{k_n}$ with $0 \leqslant k_i < n$ for all i; this shows that $\mathcal{O}$ is finitely generated as a $\mathbb{Z}$-module. Since $\mathcal{O}$ is also torsion-free (since it is contained in $\operatorname{Spl}_K(F)$), the fact that $\mathbb{Z}$ is a PID implies that $\mathcal{O}$ is free of finite rank over $\mathbb{Z}$, say

$$\mathcal{O} = \bigoplus_{j=1}^{r} \mathbb{Z}\omega_j$$

for some $\omega_j \in \mathcal{O}$ and $r \in \mathbb{N}$. Actually, it is easy to see that the ω_j form a $\mathbb{Q}$-basis of $\mathbb{Q}[\alpha_1, \cdots, \alpha_n] = \operatorname{Spl}_K(F)$, so

$$r = [\operatorname{Spl}_K(F) : \mathbb{Q}] = \#\operatorname{Gal}_{\mathbb{Q}}(F).$$

In particular, $p\mathcal{O} = \bigoplus_{j=1}^{r} \mathbb{Z}p\omega_j$ is a proper ideal of $\mathcal{O}$; furthermore, the proper ideals of $\mathcal{O}$ containing $p\mathcal{O}$ are in bijection with the proper ideals

of $\mathcal{O}/p\mathcal{O} \simeq \bigoplus_{j=1}^{r} \mathbb{F}_p\omega_j$, which is a finite ring; in particular, it has a nonzero but finite number of maximal ideals. Therefore, the set

$$\mathcal{M} = \{M \subset \mathcal{O} \text{ maximal ideal} \mid p\mathcal{O} \subseteq M\}$$

is nonempty and finite.

Let $M \in \mathcal{M}$, and write $\mathbb{F}_M = \mathcal{O}/M$, which is a field by lemma 3.3.9. Besides, since $p\mathcal{O} \subseteq M$, $\mathbb{F}_M$ is a quotient of the finite ring $\mathcal{O}/p\mathcal{O}$, and is therefore itself finite (whence the notation $\mathbb{F}_M$). Furthermore, the intersection $M \cap \mathbb{Z}$ is an ideal of $\mathbb{Z}$ containing p, which is thus of the form $n\mathbb{Z}$ for some $n \in \mathbb{Z}$ dividing p. If we had $n = 1$, then we would get $1 \in M$ whence $M = R$, which is absurd since maximal ideals are proper; thus $M \cap \mathbb{Z} = p\mathbb{Z}$. As a consequence, $\mathbb{F}_M$ has characteristic p, and is thus a finite field which is an extension of $\mathbb{F}_p$. Actually, since we have $F(x) = \prod_{i=1}^{n}(x - \alpha_i)$, the field $\mathbb{F}_M$ is a splitting field of $\overline{F}$ over $\mathbb{F}_p$; since $\overline{F}$ is separable by assumption, the roots α_i of F remain distinct in the quotient $\mathbb{F}_M$.

Example 2.5.10 tells us that since $\mathbb{F}_M$ is a finite extension of $\mathbb{F}_p$, this extension is Galois, and that $\mathrm{Gal}(\mathbb{F}_M/\mathbb{F}_p)$ is cyclic and generated by Frob : $\overline{x} \mapsto \overline{x}^p$. By theorem 3.1.6, the orbits of the $\overline{\alpha_i} \in \mathbb{F}_M$ under Frob thus correspond to the irreducible factors of $\overline{F}$. In order to conclude, we are going to construct an injective group morphism from $\mathrm{Gal}(\mathbb{F}_M/\mathbb{F}_p)$ into $\mathrm{Gal}_{\mathbb{Q}}(F)$ which is compatible with the permutation action of the Galois group on the roots of F.

In general, for $\sigma \in \mathrm{Gal}_{\mathbb{Q}}(F)$, $\sigma(M)$ is another element of $\mathcal{M}$. Define[2]

$$D_M = \{\sigma \in \mathrm{Gal}_{\mathbb{Q}}(F) \mid \sigma(M) = M\};$$

this is clearly a subgroup of $\mathrm{Gal}_{\mathbb{Q}}(F)$. The map

$$\rho_M : \begin{array}{ccc} D_M & \longrightarrow & \mathrm{Gal}_{\mathbb{F}_p}(\overline{F}) = \mathrm{Gal}(\mathbb{F}_M/\mathbb{F}_p) \\ \sigma & \longmapsto & (\overline{\sigma} : \overline{x} \mapsto \overline{\sigma(x)}) \end{array}$$

is well defined because if $\overline{x} = \overline{y}$ in $\mathbb{F}_M$, then $x = y + m$ for some $m \in M$, whence $\sigma(x) = \sigma(y) + \sigma(m)$ so $\overline{\sigma(x)} = \overline{\sigma(y)}$ as $\sigma(m) \in M$ by definition of D_M; besides, ρ_M is clearly a group morphism.

[2]This notation comes from the fact that D_M is called the *decomposition subgroup* of M in algebraic number theory.

We are now going to prove that ρ_M is an isomorphism. First of all, if $\sigma \in \ker \rho_M$, then $\bar{\sigma} = \rho_M(\sigma)$ is the identity, and thus fixes each of the roots $\overline{\alpha_i}$ of $\overline{F}$ in $\mathbb{F}_M$; since we have seen that reduction mod M is injective on the α_i, this means that σ fixes each of the α_i, whence $\sigma = \mathrm{Id}$. This proves that ρ_M is injective.

Let now $\mathrm{Gal}_{\mathbb{Q}}(F) \cdot M = \{\sigma(M) \mid \sigma \in \mathrm{Gal}_{\mathbb{Q}}(F)\}$ be the orbit of the maximal ideal M under $\mathrm{Gal}_{\mathbb{Q}}(F)$. It elements are also maximal ideals, and are thus pairwise coprime; besides, their intersection $I_M = \cap_{\sigma \in \mathrm{Gal}_{\mathbb{Q}}(F)} \sigma(M)$ contains $p\mathcal{O}$. We deduce from lemma 3.3.10 a surjective ring morphism

$$\mathcal{O}/p\mathcal{O} \twoheadrightarrow \mathcal{O}/I_M \xrightarrow{\sim} \prod_{M' \in \mathrm{Gal}_{\mathbb{Q}}(F) \cdot M} \mathcal{O}/M',$$

whence the inequality

$$\#\,\mathrm{Gal}_{\mathbb{Q}}(F) = r = \dim_{\mathbb{F}_p} \mathcal{O}/p\mathcal{O} \geqslant \dim_{\mathbb{F}_p} \prod_{M' \in \mathrm{Gal}_{\mathbb{Q}}(F) \cdot M} \mathcal{O}/M' = \sum_{M' \in \mathrm{Gal}_{\mathbb{Q}}(F) \cdot M} \dim_{\mathbb{F}_p} \mathcal{O}/M'.$$

But for each M', we know that $\mathcal{O}/M' = \mathbb{F}_{M'}$ is a splitting field of $\overline{F}$ over $\mathbb{F}_p$, so

$$\dim_{F_p} \mathcal{O}/M'. = [\mathbb{F}_{M'} : \mathbb{F}_p] = \#\,\mathrm{Gal}_{\mathbb{F}_p}(\overline{F});$$

besides, the map

$$\begin{array}{ccc} \mathrm{Gal}_{\mathbb{Q}}(F) & \longrightarrow & \mathrm{Gal}_{\mathbb{Q}}(F) \cdot M \\ \sigma & \longmapsto & \sigma(M) \end{array}$$

is $\#D_M$-to-1 by definition of D_M, so $\#(\mathrm{Gal}_{\mathbb{Q}}(F) \cdot M) = \frac{\#\,\mathrm{Gal}_{\mathbb{Q}}(F)}{\#D_M}$. We thus get

$$\#\,\mathrm{Gal}_{\mathbb{Q}}(F) \geqslant \frac{\#\,\mathrm{Gal}_{\mathbb{Q}}(F)}{\#D_M} \#\,\mathrm{Gal}_{\mathbb{F}_p}(\overline{F}),$$

which means that the source of ρ_M is not larger than its target. As ρ_M is injective, it must be bijective.

As a result, we get an injection

$$\mathrm{Gal}(\mathbb{F}_M/\mathbb{F}_p) = \mathrm{Gal}_{\mathbb{F}_p}(\overline{F}) \overset{\rho_M^{-1}}{\simeq} D_M \subseteq \mathrm{Gal}_{\mathbb{Q}}(F),$$

which is by construction compatible with the permutation action of the Galois group on the roots of F, and the proof is complete.

□

Chapter 4

Solvability by radicals

4.1 Solvable groups

In this section, G is a group with identity element 1_G.

Definition 4.1.1. A *commutator* in G is an element of G of the form

$$[x, y] = xyx^{-1}y^{-1}$$

for some $x, y \in G$.

The name comes form the fact that $x, y \in G$ commute iff. $[x, y] = 1$.

Definition 4.1.2. The *derived subgroup* $D(G)$ of G is the subgroup spanned by its commutators.

Remark 4.1.3. Since

$$z[x, y]z^{-1} = zxyx^{-1}y^{-1}z^{-1} = zxz^{-1}zyz^{-1}zx^{-1}z^{-1}zy^{-1}z^{-1} = [zxz^{-1}, zyz^{-1}]$$

for all $x, y, z \in G$, the derived subgroup is a *normal* subgroup of G. The quotient $G/D(G)$ is Abelian since all commutators are trivial in it; it is the "largest" Abelian quotient of G.

Example 4.1.4.

- $D(G) = \{1_G\}$ iff. G is Abelian.

- Take $G = S_n$. Then $\varepsilon([x,y]) = \varepsilon(xyx^{-1}y^{-1}) = 1$ for all $x, y \in G$, so $D(G) \subseteq A_n$. One can prove that in fact $D(S_n) = A_n$ for all n. Observe that $S_n/A_n \overset{\varepsilon}{\simeq} \mathbb{Z}/2\mathbb{Z}$ is Abelian.

Definition 4.1.5. A *normal series* for G of *length* $n \in \mathbb{N}$ is a sequence

$$\{1_G\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_n = G$$

where for all i, the G_i are subgroups of G, such that G_i is a *normal* subgroup of G_{i+1}. The quotients G_{i+1}/G_i are called the *factors* of the series.

Example 4.1.6.

- The sequence
$$\{1_G\} \triangleleft G$$
is a (boring) normal series of length 1 for any group G.

- If G is the symmetric group S_3, then
$$\{\mathrm{Id}\} \triangleleft A_3 \triangleleft G$$
is a normal series of length 2 for G, whose factors are $A_3/\{\mathrm{Id}\} = A_3 \simeq \mathbb{Z}/3\mathbb{Z}$ and $S_3/A_3 \simeq \mathbb{Z}/2\mathbb{Z}$ (but of course, S_3 is **NOT** isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, e.g. because it is not Abelian).

- If now $G = S_4$, then
$$\{\mathrm{Id}\} \triangleleft V_4 \triangleleft A_4 \triangleleft G$$
where
$$V_4 = \{\mathrm{Id}, (12)(34), (13)(24), (14)(23)\},$$
is a normal series of length 3, with factors
$$V_4 \simeq (\mathbb{Z}/2\mathbb{Z})^2, \ A_4/V_4 \simeq \mathbb{Z}/3\mathbb{Z}, \text{ and } S_4/A_4 \simeq \mathbb{Z}/2\mathbb{Z}.$$

- Finally, let G be any group, and define a sequence of subgroups by
$$D^0(G) = G, \ D^1(G) = D(G), \text{ and } D^{k+1}(G) = D(D^k(G)).$$
If there exits $n \in \mathbb{N}$ such that $D^n(G)$ is reduced to $\{1_G\}$, then the sequence
$$\{1_G\} = D^n(G) \triangleleft D^{n-1}(G) \triangleleft \cdots \triangleleft D^1(G) \triangleleft G$$
is a normal series with Abelian factors; indeed, for all i, all the elements of $D(D^i(G)) = D^{i+1}(G)$ are trivial in the quotient $D^i(G)/D^{i+1}(G)$.

Theorem 4.1.7. *Let G be a* finite *group. The following are equivalent:*

(i) G admits a normal series whose factors G_{i+1}/G_i are all Abelian,

(ii) G admits a normal series such that for all i, $G_{i+1}/G_i \simeq \mathbb{Z}/n_i\mathbb{Z}$ for some $n_i \in \mathbb{N}$,

(iii) There exists $n \in \mathbb{N}$ such that $D^n(G) = \{1_G\}$.

Proof.

- (i) $\Longrightarrow$ (ii): Let A be a finite Abelian group. We prove by induction on $\#A$ that A admits a normal series with cyclic factors. Indeed, if $\#A = 1$ there is nothing to prove; else, take an nontrivial element $a \in A$, and let $C = \langle a \rangle$ be the cyclic subgroup that it spans. This subgroup is normal since A is Abelian, so we get a projection morphism $\pi : A \longrightarrow A/C$. Since $\#(A/C) = \#A/\#C < \#A$, the induction hypothesis grants us with a normal series

$$\{\overline{1_A}\} = H_0 \subset H_1 \subset \cdots \subset H_r = A/C$$

  with cyclic factors. Pulling back by π yields

$$\{1_A\} \subset C = \pi^{-1}(H_0) \subset \pi^{-1}(H_1) \subset \cdots \subset \pi^{-1}(A/C) = A$$

  where all the inclusions are normal since A is Abelian, and with cyclic factors since C is cyclic.

  If now

$$\{1_G\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

  is a normal series with Abelian factors for G, then we may refine it into one with cyclic factors by applying the above with $A = G_{i+1}/G_i$ for $i = 0$, then for $i = 1$, etc.

- (ii) $\Longrightarrow$ (i) is trivial.

- (i) $\Longrightarrow$ (iii): Let

$$\{1_G\} = G_0 \lhd G_1 \lhd \cdots \lhd G_n = G$$

  have Abelian factors. Since G/G_{n-1} is Abelian, all the commutators of G are trivial in it, so $D(G) \subseteq G_{n-1}$. Iterating this argument show that $D^i(G) \subseteq G_{n-i}$ for all i; in particular, $D^n(G) \subseteq \{1_G\}$.

- (iii) $\Longrightarrow$ (i): We have already seen that the factors of

$$\{1_G\} = D^n(G) \triangleleft D^{n-1}(G) \triangleleft \cdots \triangleleft D^1(G) \triangleleft G$$

are Abelian.

□

Definition 4.1.8. If the equivalent conditions of theorem 4.1.7 are satisfied, we say that G is a *solvable* group.

Example 4.1.9.

- Abelian groups are solvable.
- We have seen in example 4.1.6 that S_3 and S_4 are solvable.
- On the other hand, one can prove that $D(A_n) = A_n$ for all $n \geqslant 5$, so S_n and A_n are *not* solvable for $n \geq 5$. In conclusion, S_n is solvable iff. $n \leqslant 4$.

Proposition 4.1.10. *Let G be a solvable group.*

(i) Any subgroup of G is also solvable.

(ii) If $f : G \longrightarrow H$ is a group morphism, then the image of f is solvable.

(iii) Any quotient of G is solvable.

Proof. Since G is solvable, theorem 4.1.7 ensures that there exists $n \in \mathbb{N}$ such that $D^n(G) = \{1_G\}$.

(i) It is clear that if $H \subseteq H'$ are groups, then $D(H) \subseteq D(H')$, whence $D^i(H) \subseteq D^i(H')$ for all $i \in \mathbb{N}$ by induction on i. As a result, if $H \subseteq G$, then $D^n(H) \subseteq D^n(G) = \{1_G\}$, so $D^n(H) = \{1_G\}$, so H is solvable.

(ii) After replacing H with the image of f, we may assume that f is surjective. Clearly the image of a commutator is a commutator, so $f(D(G)) = D(H)$, whence $f(D^i(G)) = D^i(H)$ for all $i \in \mathbb{N}$ by induction. In particular, $D^n(H) = f(D^n(G)) = f(\{1_G\}) = \{1_H\}$, so H is solvable.

(iii) follows immediately by taking f to be the projection to the quotient.

□

4.2 Radical extensions

Definition 4.2.1. Let $n \in \mathbb{N}$. A field extension $K \subseteq L$ is an *elementary radical extension* (of *order* n) if there exists $\alpha \in L$ such that $L = K(\alpha)$ and $\alpha^n \in K$ (i.e. $L = K(\sqrt[n]{a})$ for some $a \in K$).

A field extension $K \subseteq L$ is *radical* if there exist fields E_i such that

$$K = E_0 \subseteq E_1 \subseteq \cdots E_m = L$$

with $m \in \mathbb{N}$ and $E_i \subseteq E_{i+1}$ elementary radical for all $i < m$.

Example 4.2.2. The extension $\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt[7]{\sqrt{1+\sqrt[3]{2}}\sqrt{5}}\right)$ is radical because

$$\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{Q}\left(\sqrt{1+\sqrt[3]{2}}\right) \subseteq \mathbb{Q}\left(\sqrt{1+\sqrt[3]{2}}, \sqrt{5}\right) \subseteq \mathbb{Q}\left(\sqrt[7]{\sqrt{1+\sqrt[3]{2}}\sqrt{5}}\right).$$

Remark 4.2.3. For all $n \in \mathbb{N}$, the cyclotomic extension $\mathbb{Q} \subseteq \mathbb{Q}(\zeta_n)$ is elementary radical since $\zeta_n^n = 1 \in \mathbb{Q}$. (We will see in remark 4.3.8 below that it is actually also radical in a less frustrating sense).

Definition 4.2.4. Let K be a field, and let $F(x) \in K[x]$. We say that F is *solvable by radicals over* K if the splitting field of F over K is contained in a radical extension of K.

This formalises the concept of the roots of F being expressible by (nested) radicals.

4.3 Galois's theorem

The main theorem of this chapter is the following:

Theorem 4.3.1. *Let K be a field of characteristic 0, and let $F(x) \in K[x]$. Then F is solvable by radicals iff. its Galois group $\mathrm{Gal}_K(F)$ is a solvable group.*

Example 4.3.2. Let $F(x) = x^5 + x^2 + 1$. We have seen in example 3.3.4 that $\mathrm{Gal}_{\mathbb{Q}}(F) \simeq S_5$. Since S_5 is not a solvable group, F is not solvable over $\mathbb{Q}$, i.e. none of the 5 complex roots of F can be expressed using only rational numbers, the 4 field operations, and (iterated) n-th roots.

More generally, since "most" polynomials of degree n in $\mathbb{Q}[x]$ have Galois group S_n, for $n \geqslant 5$ there cannot exist formulas using only radicals and the 4 field operations to find their roots since S_n is not solvable.

The idea behind theorem 4.3.1 is clear: if $\mathrm{Spl}_K(F)$ can be obtained from K by a succession of elementary radical extensions, then the Galois correspondence should give us a chain of subgroups of $\mathrm{Gal}_K(F)$, which should show that it is solvable, and vice-versa. Unfortunately, the proof is now so straightforward, and requires taking care of roots of unity. The essential reason for that is n-th roots are not well-defined, since a number has n distinct n-th roots differing from each other by multiplication by an n-th root of 1; cf. example 4.3.7 for an illustration. A a result, we begin by proving a few lemmas about roots of 1.

Lemma 4.3.3 (n-th roots in characteristic 0)**.** *Let K be a field of characteristic 0, and let $a \in K$ be nonzero. Let also $n \in \mathbb{N}$, and Ω be an algebraically closed extension of K (e.g. $\Omega = \mathbb{C}$ if $K = \mathbb{Q}$). Then a has n distinct n-th roots in Ω; in particular, there are n n-th roots of 1 in Ω. The n-th roots of a differ from each other by multiplication by an n-th root of 1.*

Proof. Let $F(x) = x^n - a$. Then $F'(x) = nx^{n-1}$, so 0 is the only root of $F'(x)$ in Ω as $n \neq 0$ in K.Therefore F and F' have no common roots, so F' is separable.

Besides, if α and α' are both roots of $F(x)$, then $(\alpha'/\alpha)^n = 1$, so α'/α is an n-th root of 1. □

Remark 4.3.4. If $\mathrm{char}\, K$ is a prime p dividing n, the situation is totally different, cf. lemma 2.2.4.

Lemma 4.3.5 (Radical extensions are cyclic)**.** *Let K be a field of characteristic 0, and let L be an elementary radical extension of K of order n, i.e. $L = K(\alpha)$ for some $\alpha \in L$ such that $a = \alpha^n \in K$. If K contains the n-th roots of unity, then L is Galois over K, and $\mathrm{Gal}(L/K)$ is a cyclic group.*

Proof. Let $\mu_n = \{n\text{-th roots of } 1\} \subset K$; in view of lemma 4.3.3, this is a subgroup of $K^\times$ of order n; besides, it contains a primitive root (since the cyclotomic polynomial divides $x^n - 1$) and is therefore cyclic. The roots of polynomial $F(x) = x^n - a \in K[x]$ are the $z\alpha$ for $z \in \mu_n$ by lemma 4.3.3; in particular, they all lie in L, so $L = K(\alpha)$ is the splitting field of $F(x)$, which

is separable as seen in the proof of lemma 4.3.3. This proves that $K \subseteq L$ is Galois.

Define now

$$\begin{array}{rcl} \varphi : \mathrm{Gal}(L/K) & \longrightarrow & \mu_n \\ \sigma & \longmapsto & \dfrac{\sigma(\alpha)}{\alpha}. \end{array}$$

This is well defined, because $\sigma(\alpha)$ is always a root of $F(x)$, and is therefore of the form $z\alpha$ for some $z \in \mu_n$. It is also a morphism, since if $\varphi(\sigma) = z$ and if $\varphi(\sigma') = z'$, then

$$\frac{\sigma\sigma'(\alpha)}{\alpha} = \frac{\sigma(z'\alpha)}{\alpha} = \frac{z'\sigma(\alpha)}{\alpha} = \frac{z'z\alpha}{\alpha} = zz'$$

as σ must fix $z' \in \mu_n \subset K$. Finally, it is injective since $\frac{\sigma(\alpha)}{\alpha} = 1$ implies $\sigma = \mathrm{Id}$ as σ is completely determined by its action on the generator α of $L = K(\alpha)$.

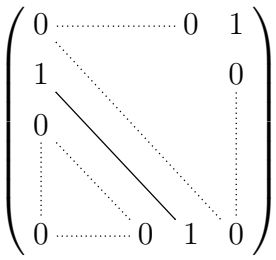
This shows that $\mathrm{Gal}(L/K)$ identifies with a subgroup of $\mu_n \simeq \mathbb{Z}/n\mathbb{Z}$, and is therefore itself cyclic. □

Lemma 4.3.6 (Cyclic extensions are radical)**.** *Let $n \in \mathbb{N}$, let K be a field of characteristic 0 containing the n-th roots of 1, and let L be a Galois extension of K of degree $[L : K] = n$. If $\mathrm{Gal}(L/K)$ is cyclic (i.e. isomorphic to $\mathbb{Z}/n\mathbb{Z}$), then there exist elements $\beta_1, \beta_2, \cdots$ of L such that $\beta_1^n, \beta_2^n, \cdots \in K$ and that $L = K(\beta_1, \beta_2, \cdots)$ (i.e. L is of the form $K(\sqrt[n]{b_1}, \sqrt[n]{b_2}, \cdots)$ for some $b_i = \beta_i^n \in K$).*

Proof. Write again $\mu_n \subset K^\times$ for the group of n-th roots of 1. Since $\mathrm{Gal}(L/K)$ is cyclic, is is generated by some element $\sigma \in \mathrm{Gal}(L/K)$. Besides, since K has characteristic 0, it is perfect, so the extension $K \subset L$ is separable; as a result, the primitive element theorem 2.6.2 ensures L is of the form $L = K(\alpha)$ for some $\alpha \in K$.

Define $\alpha_0 = \alpha$, $\alpha_1 = \sigma(\alpha)$, and inductively $\alpha_{i+1} = \sigma(\alpha_i)$; in other words, $\alpha_i = \sigma^i(\alpha)$ for all i. Since $\sigma \in \mathrm{Gal}(L/K) \simeq \mathbb{Z}/n\mathbb{Z}$, we have $\sigma^n = \mathrm{Id}$, so $\alpha_n = \alpha$. Besides, if the "period" of the α_i were less than n, i.e. if there existed $0 < m < n$ such that $\alpha_m = \alpha$, then we would have $\sigma^m = \mathrm{Id}$ since the elements of $\mathrm{Gal}(L/K)$ are completely determined by their action of the generator α of L; but this would say that σ has order $\leqslant m$, which contradicts the fact that σ is generator of $\mathrm{Gal}(L/K)$. Therefore, the α_i for $0 \leqslant i < n$ are all distinct, and σ permutes them cyclically.

The idea is now to "diagonalise"[1] the action of σ. This action can be represented by the cyclic permutation matrix



whose characteristic polynomial is $x^n - 1$. Its eigenvalues are thus the $z \in \mu_n$, and the corresponding "eigenvectors" are the

$$\beta_z = \sum_{i=0}^{n-1} z^{-i}\alpha_i = \alpha_0 + z^{-1}\alpha_1 + z^{-2}\alpha_2 + \cdots \in L;$$

indeed, for all $z \in \mu_n$, $z \in K$ so $\sigma(z) = z$, whence

$$\sigma(\beta_z) = \sum_{i=0}^{n-1} z^{-i}\sigma(\alpha_i) = z\sum_{i=0}^{n-1} z^{-(i+1)}\alpha_{i+1} = z\beta_z.$$

As a result, if we define $b_z = \beta_z^n$ for each $z \in \mu_n$, then we have

$$\sigma(b_z) = \sigma(\beta_z)^n = (z\beta_z)^n = \beta_z^n = b_z$$

since $z^n = 1$, whence $b_z \in L^{\mathrm{Gal}(L/K)} = K$ as σ generates $\mathrm{Gal}(L/K)$.

To conclude, let $L' = K(\beta_z \mid z \in \mu_n)$. Then $L' \subseteq L$ since the β_z lie in L, and we want to prove that actually $L' = L$. But for all $m \geqslant 2$, the m-th

[1] We do **NOT** claim that the α_i form a K-basis of L, since this is false in general. This diagonalisation tale is just here to explain the idea leading to the definition of the β_z. It is however true that since σ (seen as a field automorphism) has order n, σ (seen as a K-linear map from L to L) is killed by the polynomial $x^n - 1$ which is separable since we are in characteristic 0, so that σ is diagonalisable with eigenvalues μ_n. The same argument as in the proof them shows that the n-th powers of its eigenvectors lie in K, and one concludes by writing α as a linear combination of these eigenvectors. The advantage of this approach is that it shows that the lemma remains true if $\mathrm{Gal}(L/K)$ is only supposed to be Abelian instead of cyclic, since diagonalisable operators which commute with each other are simultaneously diagonalisable; its disadvantage is that it does not give an explicit form for the eigenvectors.

roots of 1 are the roots of $x^m - 1$, so their sum, which is the negative of the coefficient of x^{m-1}, is 0; in particular, $\sum_{z \in \mu_n} z^i = 0$ for all i not divisible by n, since

$$\{z^i \mid z \in \mu_n\} = \mu_{n/\gcd(n,i)}$$

with multiplicity $\gcd(n, i)$. Therefore

$$\sum_{z \in \mu_n} \beta_z = \sum_z \sum_{i=0}^{n-1} z^{-i} \alpha_i = \sum_{i=0}^{n-1} \alpha_i \sum_z z^{-i} = n\alpha_0 = n\alpha,$$

whence $\alpha = \frac{1}{n} \sum_{z \in \mu_n} \beta_z \in L'$ so that $L = K(\alpha) \subseteq L'$. □

Example 4.3.7. Let $\zeta = e^{2\pi i/11} \in \mathbb{C}$, and let $c = \zeta + \zeta^{-1} = 2\cos\frac{2\pi}{11}$. Then $\mathbb{Q}(\zeta)$ is the 11-th cyclotomic extension, which we know is Galois over $\mathbb{Q}$ with Galois group $(\mathbb{Z}/11\mathbb{Z})^\times$, which happens to be cyclic of order 10 and generated by $2 \in (\mathbb{Z}/11\mathbb{Z})^\times$. In particular, $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 10$. One proves as in example 2.6.12 that the subextension $\mathbb{Q}(c)$ corresponds to the subgroup $H = \{\pm 1\} \subset (\mathbb{Z}/11\mathbb{Z})^\times$, so that $[\mathbb{Q}(c) : \mathbb{Q}] = 5$, and that the conjugates of c are

$$\begin{aligned} c_0 = c &= 2\cos\frac{2\pi}{11}, \\ c_1 = \sigma_2(c) &= 2\cos\frac{4\pi}{11}, \\ c_2 = \sigma_2^2(c) &= 2\cos\frac{8\pi}{11}, \\ c_3 = \sigma_2^3(c) &= 2\cos\frac{6\pi}{11}, \\ \text{and } c_4 = \sigma_2^4(c) &= 2\cos\frac{10\pi}{11}, \end{aligned}$$

so that the minimal polynomial of c is $F(x) = \prod_{i=0}^4 (x - c_i)$, which evaluates (with the help of a computer) to

$$F(x) = x^5 + x^4 - 4x^3 - 3x^2 + 3x + 1.$$

In particular,

$$\mathrm{Gal}_{\mathbb{Q}}(F) = \mathrm{Gal}(\mathbb{Q}(c)/\mathbb{Q}) = (\mathbb{Z}/11\mathbb{Z})^\times/\{\pm 1\} \simeq \mathbb{Z}/5\mathbb{Z}$$

is cyclic, so we may use lemma 4.3.6 to express c by radicals, but over $\mathbb{Q}(\zeta_5)$ instead of $\mathbb{Q}$, where $\zeta_5 = e^{2\pi i/5}$.

More precisely, we know that if we define $\beta_j = \sum_{k=0}^{4} \zeta^{jk} c_k$, i.e.

$$\begin{aligned}
\beta_0 &= c_0 + c_1 + c_2 + c_3 + c_4, \\
\beta_1 &= c_0 + \zeta_5 c_1 + \zeta_5^2 c_2 + \zeta_5^3 c_3 + \zeta_5^4 c_4, \\
\beta_2 &= c_0 + \zeta_5^2 c_1 + \zeta_5^4 c_2 + \zeta_5^3 c_3 + \zeta_5 c_4, \\
\beta_3 &= c_0 + \zeta_5^3 c_1 + \zeta_5 c_2 + \zeta_5^4 c_3 + \zeta_5^2 c_4, \\
\beta_4 &= c_0 + \zeta_5^4 c_1 + \zeta_5^3 c_2 + \zeta_5^2 c_3 + \zeta_5 c_4,
\end{aligned}$$

then for all j, $\sigma_2(\beta_j) = \zeta_5^{-j}\beta_j$, so $\beta_j^5 \in \mathbb{Q}(\zeta_5)$. In fact, we already know that $\beta_0 = \sum$ roots of $F(x) = -$coeff. of $x^4 = -1$. The other β_j are permuted by $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$, so $G(y) = \prod_{j=1}^{4}(y - \beta_j^5)$ is fixed by $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q})$ and thus lies in $\mathbb{Q}[y]$. Still with the help of a computer, we determine that

$$G(y) = y^4 + 979y^3 + 467181y^2 + 157668929y + 25937424601,$$

and that $G(y)$ indeed has 4 roots in $\mathbb{Q}(\zeta_5)$, namely

$$\begin{aligned}
&-165\zeta_5^3 - 385\zeta_5^2 - 275\zeta_5 - 451, -110\zeta_5^3 + 110\zeta_5^2 + 275\zeta_5 - 176, \\
&-110\zeta_5^3 + 165\zeta_5^2 - 220\zeta_5 - 286, 385\zeta_5^3 + 110\zeta_5^2 + 220\zeta_5 - 66.
\end{aligned}$$

These are thus the β_j for $j \neq 0$ in some order, so we may conclude that

$$\begin{aligned}
c &= \frac{\beta_0 + \beta_1 + \beta_2 + \beta_3 + \beta_4}{5} \\
&= \frac{1}{5}\Big(-1 + \sqrt[5]{-165\zeta_5^3 - 385\zeta_5^2 - 275\zeta_5 - 451} + \sqrt[5]{-110\zeta_5^3 + 110\zeta_5^2 + 275\zeta_5 - 176} \\
&\qquad + \sqrt[5]{-110\zeta_5^3 + 165\zeta_5^2 - 220\zeta_5 - 286} + \sqrt[5]{385\zeta_5^3 + 110\zeta_5^2 + 220\zeta_5 - 66}\Big)
\end{aligned}$$

with the appropriate choices of complex 5-th roots.

Remark 4.3.8. We can then get a radical expression for c over $\mathbb{Q}$ by plugging in the value

$$\zeta_5 = \frac{-1 + \sqrt{5} + i\sqrt{10 + 2\sqrt{5}}}{4}$$

found in the homework.

More generally, the Galois group of the n-th cyclotomic extension is $(\mathbb{Z}/n\mathbb{Z})^\times$, which may be written as a product of cyclic group of order dividing $\#(\mathbb{Z}/n\mathbb{Z})^\times$

and thus strictly less than n. Therefore, lemma 4.3.6 shows that n-th roots of 1 may be expressed in terms of radicals and of m-th roots of 1 for various $m < n$. Iterating this argument then shows that they can be expressed by radicals over $\mathbb{Q}$.

Lemma 4.3.9. *Let $K \subset L$ be a Galois extension, and let α be some element of a larger field $\Omega \supseteq L$. Then the extension $K(\alpha) \subset L(\alpha)$ is also Galois, and its Galois group identifies with a subgroup of* $\mathrm{Gal}(L/K)$.

Proof. Since $K \subset L$ is Galois, L is the splitting field of some separable polynomial $F(x) \in K[x]$ by theorem 2.4.3 (iii). Then $L(\alpha)$ is clearly the splitting field of $F(x)$ over $K(\alpha)$, which shows that the extension $K(\alpha) \subseteq L(\alpha)$ is also Galois.

Consider now the restriction map

$$\rho : \begin{array}{ccc} \mathrm{Gal}(L(\alpha)/K(\alpha)) & \longrightarrow & \mathrm{Gal}(L/K) \\ \sigma & \longmapsto & \sigma_{|L} \end{array} .$$

This is well-defined, because if $\sigma \in \mathrm{Gal}(L(\alpha)/K(\alpha))$, then $\sigma_{|K} = \mathrm{Id}$ as $K \subseteq K(\alpha)$, and because $\sigma(L) = L$ by the same logic as in the proof of lemma 2.5.5. Besides, ρ is clearly a group morphism.

To conclude, we are going to prove that ρ is injective. Let $\sigma \in \mathrm{Ker}(\rho)$, i.e. $\sigma_{|L} = \mathrm{Id}$. Then σ fixes all the elements of L, and also fixes α since it fixes the elements of $K(\alpha)$. Since L and α generate $L(\alpha)$, σ fixes all the elements of $L(\alpha)$, i.e. $\sigma = \mathrm{Id}$. Thus $\mathrm{Ker}\,\rho = \{\mathrm{Id}\}$. □

Proof of theorem 4.3.1. Let us write $S = \mathrm{Spl}_K(F)$ for brevity.

- *F solvable by radicals $\Longrightarrow$ $\mathrm{Gal}_K(F)$ solvable:*

  By assumption, S is contained in a radical extension R of K, so we have

  $$K \subseteq S \subseteq R = K(\alpha_1, \cdots, \alpha_r)$$

  for some $r \in \mathbb{N}$, where the α_i are such that for each i, there exists $n_i \in \mathbb{N}$ such that $\alpha_i^{n_i} \in K(\alpha_1, \cdots, \alpha_{i-1})$, i.e. $K_i = K_{i-1}(\sqrt[n_i]{a_i})$ where we have defined $K_i = K(\alpha_1, \cdots, \alpha_i)$ and similarly for K_{i-1}, and where $a_i = \alpha_i^{n_i} \in K_{i-1}$.

  Furthermore, we may assume that $\alpha_1 = \zeta$ is a primitive n-th root of 1, where n is a common multiple of all the n_i; indeed, if this is not the case, then we can *define* α_1 this way, and keep the same α_i

(with indices shifted by 1 to make room for the new α_1), and we still have $S \subset R = K(\alpha_1, \cdots, \alpha_r)$ and $\alpha_i^{n_i} \in K(\alpha_1, \cdots, \alpha_{i-1})$ for all i. Then for all $i \geqslant 2$, K_{i-1} contains the n_i-th roots of 1, since these are the powers of ζ^{n/n_i}.

We now prove that the extension $K \subseteq K_i$ is Galois for all i. First of all, this extension is separable, since we are in characteristic 0. Besides, $K_1 = K(\zeta)$ contains all the powers of ζ and is thus normal as the splitting field of $x^n - 1$ over K. To prove $K \subseteq K_i$ is normal for $i \geqslant 2$, we fix an algebraically closed extension Ω of K, and we prove that all the elements of $\mathrm{Hom}_K(K_i, \Omega)$ have the same image by induction on i. For $i = 1$, we already know that since we have already proved that K_1 is normal over K. Let now $i \geqslant 2$, and assume that all the elements of $\mathrm{Hom}_K(K_{i-1}, \Omega)$ have the same image $I \subset \Omega$, and let $\iota \in \mathrm{Hom}_K(K_i, \Omega)$. Then $\iota_{|K_{i-1}} \in \mathrm{Hom}_K(K_{i_1}, \Omega)$, so $\iota(K_{i-1}) = I$, which shows that $\iota(K_i) = \iota\big(K_{i-1}(\sqrt[n_i]{a_i})\big)$ is an extension of $I \subset \Omega$ generated by an n_i-th root of $\iota(a_i) \in I$. But since I contains the n_i-th roots of 1 (since $K_{i-1} \supseteq K_1$ does), any such extension contains *all* these n_i-th roots by lemma 4.3.3; in particular, there is only one such extension, which completes the induction.

Let now $G = \mathrm{Gal}(R/K)$, and let $G_i = \mathrm{Gal}(R/K_i)$ for each i, so that

$$\{\mathrm{Id}\} = G_r \subseteq G_{r-1} \subseteq \cdots \subseteq G_1 \subseteq G. \tag{4.3.10}$$

The for all i, G_i is normal in G, since K_i is Galois over K. In particular, G_i is normal in G_{i-1} for all i, so (4.3.10) is actually a normal series. Besides, $G_{i-1}/G_i = \mathrm{Gal}(K_i/K_{i-1})$ is cyclic and therefore Abelian for all $i \geqslant 2$ by lemma 4.3.5, whereas for $i = 1$, we see that $G/G_1 = \mathrm{Gal}(K_1/K) = \mathrm{Gal}(K(\zeta)/K)$ injects into $(\mathbb{Z}/n\mathbb{Z})^\times$ by

$$\begin{array}{rcl} \mathrm{Gal}(K(\zeta)/K) & \longrightarrow & (\mathbb{Z}/n\mathbb{Z})^\times \\ \sigma & \longmapsto & \text{The } k \text{ such that } \sigma(\zeta) = \zeta^k \end{array}$$

by the same argument as for cyclotomic polynomials (the only difference is that here, this morphism may not be surjective, e.g. it may be that $\zeta \in K$).

Therefore G/G_1 is also Abelian, which shows that G is solvable.

Finally, since S is Galois over K by definition, the group $\mathrm{Gal}_K(F) = \mathrm{Gal}(S/K)$ is the quotient of G by $\mathrm{Gal}(R/S)$, and is therefore also solvable by proposition 4.1.10.

- $\mathrm{Gal}_K(F)$ solvable $\Longrightarrow$ F solvable by radicals:

  Let us slightly change the notation: ζ now denotes a primitive d-th root of 1, where $d = \#\,\mathrm{Gal}_K(F) = [S : K]$.

  Suppose first that $\zeta \in K$. This implies in particular that K contains the d'-th roots of unity for all $d'|d$, since these are some of the powers of ζ.

  Since $\mathrm{Gal}_K(F)$ is solvable, theorem 4.1.7 grants us with a normal series

  $$\mathrm{Gal}(S/K) = H_0 \triangleright H_1 \triangleright \cdots \triangleright H_r = \{\mathrm{Id}\}$$

  with H_i/H_{i+1} cyclic for all i. By the Galois correspondence, we deduce a tower of extensions

  $$K = E_0 \subset E_1 \subset \cdots \subset E_r = S$$

  with the extensions $E_i \subset E_{i+1}$ Galois of cyclic Galois group for each i. Then

  $$d = [\mathrm{Spl}_K(F) : K] = \prod_{i=0}^{r-1} [E_{i+1} : E_i],$$

  so for each i, the degree $d_i = [E_{i+1} : E_i]$ divides d. This implies that so E_i contains the d_i-th roots of 1 (since K does); it then follows from lemma 4.3.6 that the extension $E_i \subset E_{i+1}$ is radical for all i. In conclusion, $S = \mathrm{Spl}_K(F)$ is contained in an extension obtained as a succession of radical extensions of K, so tht F is solvable by radicals over K.

  Suppose now that $\zeta \notin K$. Let $K' = K(\zeta)$, $S' = S(\zeta)$, and $d' = [S' : K']$. Observe that S' is the splitting field of F over K'; in particular, the extension $K' \subseteq S'$ is normal, hence Galois since we are in characteristic 0. Furthermore, lemma 4.3.9 tells us that $\mathrm{Gal}(S'/K')$ is isomorphic to a subgroup of $\mathrm{Gal}(S/K) = \mathrm{Gal}_K(F)$. This has two consequences: first, proposition 4.1.10 implies that $\mathrm{Gal}(S'/K')$ is also solvable, and second, Lagrange tells us that

  $$d' = \#\,\mathrm{Gal}(S'/K') \mid \#\,\mathrm{Gal}(S/K) = d,$$

  so in particular K' contains the primitive d'-th root of unity $\zeta^{d/d'}$.

We may thus apply the above logic to the extension $K' \subseteq S'$ instead of $K \subseteq S$, and thus deduce that F is solvable by radicals over K', i.e. that there exists a radical extension R of K' containing all the roots of F. But then R is also a radical extension of K, since $K \subseteq K' \subseteq R$ and since $K' = K(\zeta)$ is an elementary radical extension of K (cf. remark 4.2.3), so F is actually also solvable by radicals over K.

□

Remark 4.3.11. The second part of the proof is based on lemma 4.3.6, of which we have given a constructive proof. We are therefore able to solve explicitly by radicals any polynomial equation whose Galois group is solvable (at least in theory), as demonstrated by example 4.3.7 above, and by the following example.

Example 4.3.12 (Cardano's formulas)**.** Suppose $F(x) \in K[x]$ is separable of degree 3, and let $\alpha_1, \alpha_2, \alpha_3$ be its roots in its splitting field S. Then $\mathrm{Gal}_K(F) = \mathrm{Gal}(S/K) \subseteq S_3$ is solvable (since S_3 is), so the α_i must be expressible by radicals.

Since $\mathrm{Gal}_K(F)$ is potentially the whole of S_3, the normal series

$$\{\mathrm{Id}\} \triangleleft A_3 \triangleleft S_3$$

with cyclic factors invites us to look for combinations of the roots that are invariant under the cyclic group A_3. Following lemma 4.3.6, we are led to defining

$$u = \alpha_1 + \zeta_3\alpha_2 + \zeta_3^2\alpha_3, \quad v = \alpha_1 + \zeta_3^2\alpha_2 + \zeta_3\alpha_3,$$

which have the property that u^3 and v^3 are fixed by A_3, and permuted by S_3. In particular, the polynomial

$$Q(x) = (x - u^3)(x - v^3)$$

is completely invariant by $\mathrm{Gal}_K(F)$, so it must lie in $K[x]$; in fact, its coefficients, being symmetric polynomials in the α_i, must be polynomials in the coefficients of F by proposition 1.1.8. By solving $Q(x) = 0$ by the quadratic formula, we can thus recover u^3 and v^3, hence u and v by taking cube roots, and finally $\alpha_1 = \frac{u+v}{3}$.

Unfortunately, the formulas expressing the coefficients of $Q(x)$ in terms of those of $F(x)$ are rather cumbersome in general. They are are considerably

simplified in the specific case where $F(x)$ is of the form x^3+bx+c (which we may always assume by translating x appropriately so a to kill the x^2 term), as we then have

$$Q(x) = x^2 + 3^3cx - 3^3b^3.$$

As a result, we get

$$u^3, v^3 = \frac{-27c \pm \sqrt{3^6c^2 + 4 \cdot 3^3b^3}}{2},$$

whence

$$\alpha_1 = \sqrt[3]{-\frac{c}{2} + \sqrt{\left(\frac{c}{2}\right)^2 + \left(\frac{b}{3}\right)^3}} + \sqrt[3]{-\frac{c}{2} - \sqrt{\left(\frac{c}{2}\right)^2 + \left(\frac{b}{3}\right)^3}}$$

for the appropriate choices of cube roots, and similarly for α_2 and α_3.

This identity was discovered by del Ferro and Tartaglia about 300 years before the advent of Galois theory, but Galois theory really helps understand where they come from.

To be honest, it should be pointed out that these formulas, although satisfying on the theoretical plan, are of limited practical use: For instance, they express the roots of

$$F(x) = x^3 - 7x + 6 = (x-1)(x-2)(x+3)$$

as

$$\sqrt[3]{-3 + \frac{10}{9}\sqrt{-3}} + \sqrt[3]{-3 - \frac{10}{9}\sqrt{-3}}.$$