NOTES FOR MODULE 3419
"GALOIS THEORY"
MICHAELMAS TERM 2015

VLADIMIR DOTSENKO

CONTENTS

Preface

These notes roughly correspond to the module "Galois Theory" I taught at Trinity College Dublin in the autumn semester of 2015/16. Galois theory is a mathematical theory which attempts, to an extent, make solving equations with one unknown x, say $f(x) = 0$, easy. "Easy", and one cannot find quotation marks large enough to emphasize the futility of that notion here, can mean a few different things:

- writing down exact formulas for solutions,
- reducing solving the given equation to solving some simpler equations,
- establishing some properties of solutions,
- or, even worse, proving that there is no reasonable exact formula for solutions (except for the formula "x is a solution to $f(x) = 0''$, which is not too useful).

The main idea behind Galois theory is to study equations via their symmetries, and use abstract group theory to encode properties of solutions. Throughout this module, we shall explore more and more of this philosophy.

Rather than faithfully representing the module lecture by lecture, I tried to give a slightly polished version of the exposition best suited for learning and revising the material. I am grateful to Adam Keilthy and Conor McMeel who kindly provided me with their notes (some of my own notes did not survive the semester), this was of great help.

Some of the arguments in these notes follow various Galois theory materials available online, e.g. [1, 2, 3]. This is a draft version for students to revise the module, and I did not attempt to attribute any arguments precisely to the sources where I encountered them; in many cases, it happened so long ago that precise attribution would be impossible.

1. Introduction

Let us recall how polynomial equations of low degrees are solved. We shall always assume the polynomial $f(x)$ monic, since dividing by the leading coefficient does not alter the equation. In this section, we usually assume the ground field to be complex numbers, so that extracting roots of all degrees is possible, for instance.

1.1. **Quadratic equations.**

For the equation $x^2 + ax + b = 0$, we write

$$x^2 + ax + b = \left(x + \frac{a}{2}\right)^2 + b - \frac{a^2}{4},$$

so if we denote $x + \frac{a}{2}$ by y, our equation becomes $y^2 + b - \frac{a^2}{4}$, which is easy to solve, leading to solutions

$$x = -\frac{a}{2} \pm \sqrt{\frac{a^2}{4} - b}.$$

1.2. **Cubic equations.**

For the equation $x^3 + ax^2 + bx + c = 0$, we first apply the same strategy as in the quadratic case: denote $x + \frac{a}{3}$ by y, then the next-to-leading coefficient disappears, and our equation becomes

$$y^3 + py + q = 0$$

for some p and q, which are expressed via a, b, and c by simple however unremarkable formulas. The next step is a bit of a trick, invented by Italian mathematicians a few centuries ago. Suppose we want to find a solution $y = z_1 + z_2$, where z_1 and z_2 are “simpler” than y. Then we have

$$0 = y^3 + py + q = z_1^3 + 3z_1^2 z_2 + 3z_1 z_2^2 + z_2^3 + pz_1 + pz_2 + q = \left(z_1^3 + z_2^3 + q\right) + (z_1 + z_2)\left(3z_1 z_2 + p\right).$$

Hence, we may find a solution if we put

$$\begin{cases} z_1^3 + z_2^3 = -q, \\ z_1 z_2 = -\frac{p}{3}, \end{cases}$$

which implies

$$\begin{cases} z_1^3 + z_2^3 = -q, \\ z_1^3 z_2^3 = -\frac{p^3}{27}. \end{cases}$$

Thus, z_1^3 and z_2^3 are roots of the quadratic equation

$$t^2 + qt - \frac{p^3}{27} = 0.$$

Solving this equation, we have six different values for z_1 (two values for z_1^3, and three values of the cube root), each of these leads to exactly one $z_2 = -\frac{p}{3z_1}$ due to the constraints above, and these produce three different values for the sum $z_1 + z_2$, which are roots of the given equation.

1.3. **Quartic equations.** For the equation $x^4 + ax^3 + bx^2 + cx + d = 0$, we first apply the same strategy as in the quadratic case: denote $x + \frac{a}{4}$ by y, then the next-to-leading coefficient disappears, and our equation becomes

$$y^4 + py^2 + qx + r = 0$$

for some p, q, and r. If y_1, y_2, y_3, y_4 are roots of this polynomial, then we have $y^4 + py^2 + qx + r = (y - y_1)(y - y_2)(y - y_3)(y - y_4)$, so

$$y_1 + y_2 + y_3 + y_4 = 0,$$
$$y_1 y_2 + y_1 y_3 + y_1 y_4 + y_2 y_3 + y_2 y_4 + y_3 y_4 = p,$$
$$y_1 y_2 y_3 + y_1 y_2 y_4 + y_1 y_3 y_3 + y_2 y_3 y_4 = -q$$
$$y_1 y_2 y_3 y_4 = r.$$

We now use an even more bizarre trick which will be explained in a while once we develop the general theory. Let us introduce new unknowns u, v, and w, related to y_1, y_2, y_3, and y_4 as follows:

$$\begin{cases} y_1 = \frac{u+v+w}{2}, \\ y_2 = \frac{u-v-w}{2}, \\ y_3 = \frac{-u+v-w}{2}, \\ y_4 = \frac{-u-v+w}{2} \end{cases}$$

Note that this way $y_1 + y_2 + y_3 + y_4 = 0$ automatically. Substituting this above and doing some elementary calculations yields

$$u^2 + v^2 + w^2 = -2p,$$
$$uvw = -q,$$
$$u^2 v^2 + u^2 w^2 + v^2 w^2 = p^2 - 4r.$$

Replacing the second equation by its consequence $u^2 v^2 w^2 = q^2$, we see that u^2, v^2, and w^2 are roots of the cubic equation

$$t^3 + 2pt^2 + (p^2 - 4r)t - q^2 = 0.$$

Using results of the previous section, we can solve that cubic equation, extract square roots subject to $uvw = -q$, and obtain formulas for $y_1, \ldots, y_4$.

Already here we can give some hints as to what exactly just happened. Note that we can easily express u, v, and w in terms of the roots:

$$\begin{aligned} u &= y_1 + y_2 = -(y_3 + y_4), \\ v &= y_1 + y_3 = -(y_2 + y_4), \\ w &= y_1 + y_4 = -(y_2 + y_3). \end{aligned}$$

Therefore we can write

$$\begin{aligned} u^2 &= -(y_1 + y_2)(y_3 + y_4), \\ v^2 &= -(y_1 + y_3)(y_2 + y_4), \\ w^2 &= -(y_1 + y_4)(y_2 + y_3). \end{aligned}$$

If we let the symmetric group S_4 permute the roots, the quantities $(y_1 + y_2)(y_3 + y_4)$, $(y_1 + y_3)(y_2 + y_4)$, and $(y_1 + y_4)(y_2 + y_3)$ are all invariant under the permutations $(12)(34)$, $(13)(24)$, and $(14)(23)$, which together generate the Klein 4-group $K_4 \subset S_4$. The subgroup K_4 is normal, and this is a very rare thing for a symmetric group. The existence of a normal subgroup is precisely what is behind the solution mechanism we just presented.

An important remark that we certainly must make here is that while we could reduce solving a cubic equation to solving a quadratic equation and extracting some cube roots, and as well could reduce solving a quartic equation to solving a cubic equation, starting from quintic equation onwards no reduction to lower degrees is possible, as we shall see later in this module.

2. Background material

2.1. **Polynomials and equations.** The following result on univariate polynomials and their roots is very useful.

Proposition 1.

(i) *For a polynomial $f(x)$, the remainder after division by $x - a$ is equal to the scalar $f(a)$. In particular, a is a root of $f(x)$ if and only if $f(x)$ is divisible by $x - a$. This holds for $f(x) \in R[x]$, where R is any commutative ring.*

(ii) *If $x_1, x_2, \ldots, x_k$ are distinct roots of a polynomial $f(x)$, we have $f(x) = (x - x_1)\cdots(x - x_k)g(x)$ for some polynomial $g(x)$. In particular, a polynomial of degree n has at most n roots. This holds for $f(x) \in F[x]$, where F is any field.*

Proof. The first claim follows by inspecting $f(x) = (x - a)g(x) + c$, where $c \in R$ is the remainder (a constant polynomial, since $x - a$ is of degree 1), and setting $x = a$ there. The second claim follows from the first by induction on n. □

Corollary 1. *Let F be an infinite field, and let $f(x_1, \ldots, x_n) \in F[x_1, \ldots, x_n]$ be a nonzero polynomial. Then there exist elements $a_1, \ldots, a_n \in K$ for which $f(a_1, \ldots, a_n) \neq 0$.*

Proof. Induction on n. If $n = 1$, the result follows from Proposition 1 (ii). For $n > 1$, write $f(x_1, \ldots, x_n) = f_k(x_1, \ldots, x_{n-1})x_n^k + \cdots + f_0(x_1, \ldots, x_{n-1})$. Since $f(x_1, \ldots, x_n)$ is a nonzero polynomial, one of the polynomials $f_i(x_1, \ldots, x_{n-1})$ is a nonzero polynomial, and thus by induction there exist $a_1, \ldots, a_{n-1}$ such that $f_i(a_1, \ldots, a_{n-1}) \neq 0$. This in turn implies that $f(a_1, \ldots, a_{n-1}, x_n)$ is a nonzero polynomial in x_n, and Proposition 1 (ii) applies again. □

The following result (the Vieta theorem) we used in the particular case $n = 4$ (and in fact $n = 2$) above; the proof is trivial.

Proposition 2. *Suppose that $f(x) = x^n + q_1 x^{n-1} + \cdots + q_{n-1}x + q_n \in F[x]$ is a univariate polynomial of degree n with exactly n (possibly repeating) roots $x_1, \ldots, x_n$, so that by Proposition 1 we have*

$$f(x) = (x - x_1)(x - x_2)\cdots(x - x_n).$$

Then

$$\sum_{1\le i\le n} x_i = -q_1,$$
$$\sum_{1\le i<j\le n} x_i x_j = q_2,$$
$$\sum_{1\le i<j<k\le n} x_i x_j x_k = -q_3,$$
$$\dots,$$
$$\sum_{1\le i_1<i_2<\dots<i_k\le n} x_{i_1}x_{i_2}\cdots x_{i_k} = (-1)^k q_k,$$
$$\dots,$$
$$x_1x_2\cdots x_n = (-1)^n q_n,$$

and vice versa, if $x_1, \dots, x_n$ and $q_1, \dots, q_n$ are related by these formulas, the elements $x_1, \dots, x_n$ are roots of $f(x)$.

Definition 1. Suppose that $x_1, \dots, x_n$ are formal variables. The polynomial

$$e_k(x_1,\dots,x_n) := \sum_{1\le i_1<i_2<\dots<i_k\le n} x_{i_1}x_{i_2}\cdots x_{i_k}$$

is called the k-th *elementary symmetric polynomial* in $x_1, \dots, x_n$.

The relevance of elementary symmetric polynomials is clear for the following result.

Theorem 1 (Main theorem on symmetric polynomials)**.** *Suppose that a polynomial h in $x_1, \dots, x_n$ is symmetric, that is,*

$$h(x_1,\dots,x_n) = h(x_{\sigma(1)},\dots,x_{\sigma(n)})$$

for all permutations $\sigma \in S_n$. Then h can be expressed as a polynomial in elementary symmetric polynomials, that is there exists a polynomial $r(y_1,\dots,y_n)$ for which

$$h(x_1,\dots,x_n) = r(e_1(x_1,\dots,x_n),\dots,e_n(x_1,\dots,x_n)).$$

Proof. We begin with noticing that for every symmetric polynomial h, if $x_1^{a_1}\cdots x_n^{a_n}$ occurs in h with a certain coefficient, then $x_{\sigma(1)}^{a_1}\cdots x_{\sigma(n)}^{a_n}$ occurs with the exact same coefficient (for each permutation $\sigma \in S_n$). Thus, if we define for each non-increasing sequence of nonnegative integers $r_1 \ge r_2 \ge \dots \ge r_n \ge 0$, the polynomial

$$m_{r_1,\dots,r_n} = \sum_{\sigma\in S_n} x_{\sigma(1)}^{r_1}\cdots x_{\sigma(n)}^{r_n},$$

these polynomials form a basis of the vector space of all symmetric polynomials.

Let us define a dictionary order on monomials in $x_1, \dots, x_n$ as follows: we say

$$x_1^{a_1}\cdots x_n^{a_n} \prec x_1^{b_1}\cdots x_n^{b_n},$$

if for the largest k such that $a_k \ne b_k$, we have $a_k < b_k$. For example, we have

$$1 \prec x_1 \prec x_1^2 \prec x_1^3 \prec x_2 \prec x_1x_2 \prec x_1^2x_2 \prec x_1x_2^2 \prec x_1x_2x_3.$$

We call the smallest (with respect to the dictionary order) monomial appearing in a polynomial $h(x_1,\dots,x_n)$ with a nonzero coefficient the *lowest term* of h. Note that for each polynomial $m_{r_1,\dots,r_n}$ defined as above, the lowest term is $x_1^{r_1}\cdots x_n^{r_n}$.

A very important, even if obvious, property of the dictionary order is that whenever for four monomials we have $m_1 \prec m_2$ and $m_3 \prec m_4$, it implies $m_1m_3 \prec m_2m_4$. This easily implies that the lowest term of the product of two polynomials is equal to the product of their lowest terms. This implies that for nonnegative integers $a_1, \dots, a_n$, the lowest term of the polynomial $e_1^{a_1}\cdots e_n^{a_n}$ is

$$x_1^{a_1+\dots+a_n}x_2^{a_2+\dots+a_n}\cdots x_n^{a_n}.$$

Thus, the polynomials $e_1^{a_1}\cdots e_n^{a_n}$ have distinct lowest terms, and among their terms, every monomial $x_1^{r_1}x_2^{r_2}\cdots x_n^{r^n}$ with $r_1 \ge r_2 \ge \dots \ge r_n$ occurs (to see that, we put $a_n = r_n$, $a_k = r_k - r_{k+1}$ for $k < n$). This easily implies that each $m_{r_1,\dots,r_n}$ is a polynomial in $e_1, \dots, e_n$, since we can keep subtracting scalar multiples of $e_1^{a_1} \cdots e_n^{a_n}$ to increase the lower term without increasing the degree of the polynomial (hence after finitely many steps this procedure will terminate). Since the elements $m_{r_1,\dots,r_n}$ form a basis, the theorem follows. □

Remark 1. In fact, this theorem holds when coefficients of the polynomials belong to any ring, not necessarily a field.

This theorem makes it clearer why some formulas like

$$u^2 + v^2 + w^2 = -2p,$$
$$u^2 v^2 w^2 = q^2,$$
$$u^2 v^2 + u^2 w^2 + v^2 w^2 = p^2 - 4r$$

from Section 1.3 must exist. Indeed, since

$$u^2 = -(y_1 + y_2)(y_3 + y_4),$$
$$v^2 = -(y_1 + y_3)(y_2 + y_4),$$
$$w^2 = -(y_1 + y_4)(y_2 + y_3),$$

it is easy to see that elementary symmetric polynomials in u, v, w are symmetric in y_1, y_2, y_3, y_4, and therefore are polynomial expressions in elementary symmetric polynomials.

2.2. **Groups.** Galois theory uses groups to study equations, and therefore it is not surprising that some group theory will prove very useful. Let us collate some useful results on groups that will be occasionally used in this module.

Let us recall some definitions and notation.

Definition 2.

- For an element g of a group G, the order $o(g)$ is the smallest positive integer such that $g^{o(g)} = e$. (If such an integer exists).
- If a group G acts on a set X, we denote by $\mathcal{O}_x$ the *orbit* of $x \in X$, that is $\{g.x \colon g \in G\}$.
- If a group G acts on a set X, the *stabiliser* S_x of $x \in X$ under the action of G is $\{g \in G \colon g.x = x\}$.
- In particular, if $X = G$ and the action is $g.x = gxg^{-1}$, orbits are *conjugacy classes*, and we use the notation $\mathcal{C}_g$ for the conjugacy class of g. In this particular case, S_x is denoted $Z(x)$ and called the *centraliser* of x; alternatively, $Z(x) = \{g \in G \colon gx = xg\}$.
- The *centre* of G, denoted $Z(G)$, is the intersection of all centralisers, in other words, it consists of elements that commute with all elements of G.

Proposition 3 (Useful facts of basic group theory)**.**

(i) *For a finite group G and its subgroup H, we have $\#H \mid \#G$. In particular, we have $o(g) \mid \#G$.*
(ii) *The stabiliser S_x is always a subgroup of G. For all $g \in G$, we have $S_{g.x} = gS_xg^{-1}$.*
(iii) *We have $\#\mathcal{O}_x \cdot \#S_x = \#G$.*
(iv) *The centre $Z(G)$ is a normal subgroup of G.*

Proof. See any introductory group theory course. □

The next proposition will be used several times in this module, and sometimes is not covered by introductory courses.

Proposition 4. *Let p be a prime number, and let G be a group of p^n elements. Then G has a nontrivial centre.*

Proof. Consider G with the action on itself by the formula $g.x = gxg^{-1}$, as above. Let us choose representatives of conjugacy classes and form a set I consisting of these representatives. Since G is the disjoint union of conjugacy classes, we have

$$p^n = \#G = \sum_{x \in I} \#\mathcal{C}_x = \sum_{x \in I} \frac{\#G}{\#S_x}.$$

Note that $\#S_x \mid \#G = p^n$, so $\frac{\#G}{\#S_x}$ is a power of p. There is one term in $\sum_{x\in I}\frac{\#G}{\#S_x}$ equal to 1, the term corresponding to the conjugacy class of the identity element. Since the sum is equal to p^n, and we add powers of p, there must be other terms equal to 1. But $\frac{\#G}{\#S_x} = 1$ means $\#S_x = \#G$, so $x \in Z(G)$. □

The next proposition is a list of all groups of small orders. With group theory being as abstract as it is, one should ensure they have a large repertoire of examples and counterexamples, and in particular have a working knowledge of "small" groups.

Proposition 5 (Groups of small orders)**.** *Up to isomorphism, the following are all groups of order at most* 10*:*

(1) $\{e\}$,
(2) $\mathbb{Z}/2\mathbb{Z}$,
(3) $\mathbb{Z}/3\mathbb{Z}$,
(4) $\mathbb{Z}/4\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$,
(5) $\mathbb{Z}/5\mathbb{Z}$,
(6) $\mathbb{Z}/6\mathbb{Z}$, $S_3 \cong D_3$,
(7) $\mathbb{Z}/7\mathbb{Z}$,
(8) $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$, D_4, Q_8,
(9) $\mathbb{Z}/9\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}\times\mathbb{Z}/3\mathbb{Z}$,
(10) $\mathbb{Z}/10\mathbb{Z}$, D_5

Here $\mathbb{Z}/n\mathbb{Z}$ is the additive group of integers modulo n (this group is of order n), S_k is the symmetric group consisting of all permutations of k elements (this group is of order $k!$), D_m is the dihedral group consisting of all symmetries of a regular m-gon (this group is of order $2m$), Q_8 is the quaternion group of order 8 *consisting of ±1, $\pm i$, $\pm j$, $\pm k$ with the well known product rule $i^2 = j^2 = k^2 = ijk = -1$.*

Proof. First, note that if p is prime, then for any element $g \in \mathbb{Z}/p\mathbb{Z}$ that is different from the identity element, we have $o(g) = p$ since $o(g) \mid p$ and $o(g) \neq 1$. Thus, a group of prime order is cyclic, hence cases of order 2, 3, 5, 7 are covered.

Next, let us consider a group of order p^2. From Proposition 4, we already know that G has a non-trivial centre. Since $\#Z(G) \mid \#G = p^2$, we see that $\#Z(G)$ is equal to p or p^2. In the latter case, $Z(G) = G$, so G is Abelian. In that case, there are two possibilities: either G has an element of order p^2, in which case it is cyclic, or all elements are of order p, in which case G may be regarded as a vector space over the field $\mathbb{Z}/p\mathbb{Z}$ of p elements, so choosing a basis shows $G \cong \mathbb{Z}/p\mathbb{Z}\times\mathbb{Z}/p\mathbb{Z}$. If $\#Z(G) = p$, note that $\#(G/Z(G)) = p$, so it is cyclic. Let $gZ(G)$ be a generator of $G/Z(G)$. Note that $G/Z(G)$ consists of the elements $Z(G)$, $gZ(G)$, $g^2Z(G)$, ..., $g^{p-1}Z(G)$, and hence

$$G = Z(G) \sqcup gZ(G) \sqcup g^2Z(G) \sqcup \ldots \sqcup g^{p-1}Z(G)$$

is Abelian, hence $G = Z(G)$, a contradiction. This covers the cases of order 4 and 9.

The remaining cases 6, 8, 10 are left to the reader; carefully going through groups of order 8 is a very good exercise to check fluency with basic group theory. □

Let us also mention a couple of useful results about Abelian groups.

Proposition 6. *Let G be a finite Abelian group.*

(i) *Suppose $a, b \in G$, and* $\gcd(o(a), o(b)) = 1$. *Then* $o(ab) = o(a)o(b)$.
(ii) *Suppose $a \in G$ is an element of the largest possible order. Then the order of any other element in G divides $o(a)$.*

Proof. The statement (i) is quite trivial: if $(ab)^k = e$, then $a^k = b^{-k}$. Suppose that $a^k \neq e$. Then $(a^k)^{o(b)} \neq e$, since $\gcd(o(a), o(b)) = 1$. But $(a^k)^{o(b)} = (b^{-k})^{o(b)} = e$, so $a^k = b^{-k} = e$, which implies that k is divisible by both $o(a)$ and $o(b)$.

To prove (ii), suppose that $x \in G$ is such that $o(x)$ does not divide $o(a)$. This means that for some prime p and some $n > 0$ p^n divides $o(x)$ but does not divide $o(a)$. Let m be the maximal exponent such that p^m divides $o(a)$. Denote

$$y = x^{\frac{o(x)}{p^n}}, \quad b = a^{p^m}.$$

Clearly, $o(y) = p^n$, and $o(b) = \frac{o(a)}{p^m}$. Since $\gcd(p^n, \frac{o(a)}{p^m}) = 1$, we have

$$o(yb) = o(a)p^{n-m} > o(a),$$

a contradiction. □

2.3. **Fields and rings.** Throughout this module, by a *ring* we mean a commutative ring.

The relevance of fields for Galois theory which we shall see throughout this module is very apparent: for an equation $f(x) = 0$, where $f(x)$ is a polynomial with coefficients in some field K, it will be beneficial to consider a field L obtained from K by adjoining all roots of $f(x)$; studying that field L instead of studying roots directly can be very useful.

Example 1 (Examples of fields and rings)**.**

- The set of integers $\mathbb{Z}$ is a ring.
- For each ring R and its ideal I, the cosets R/I form a ring.
- For each ring R without zero divisors (an integral domain), the field of fractions $\mathrm{Frac}(R)$ is defined; as the name suggests, it is a field.
- For each ring R and its maximal ideal I, the cosets R/I form a field.
- In particular, $\mathbb{Q} = \mathrm{Frac}(\mathbb{Z})$ is a field, $\mathbb{Z}/p\mathbb{Z}$ is a field when p is a prime number, $\mathbb{C} \cong \mathbb{R}[x]/(x^2+1)$ is a field.

Proposition 7. *Let k be a field. The ring of polynomials $k[x]$ is a principal ideal domain and a unique factorisation domain. Nonzero prime ideals of $k[x]$ are maximal. Every prime ideal of $k[x]$ is of the form $(f(x))$, where $f(x)$ is an irreducible polynomial.*

Proof. See any introductory ring theory course. □

The following classical result will be used later in this module.

Proposition 8. *Suppose F is a field, and G is a finite subgroup of $F^\times$. Then G is cyclic. In particular, $(\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic.*

Proof. Let a be an element of G of maximal order. If $o(a) = \#G$, then G is cyclic. If $o(a) < \#G$, then by Proposition 6, $x^{o(a)} = 1$ for all $x \in G$, so the polynomial $x^m - 1$ has more than m roots in F, which is a contradiction. □

We also mention without proof the following more general result which will be useful once or twice:

Proposition 9.

- *If $n = p_1^{a_1} \cdots p_k^{a_k}$ where p_i are distinct primes, we have*
$$(\mathbb{Z}/n\mathbb{Z})^\times \cong (\mathbb{Z}/p_1^{a_1}\mathbb{Z})^\times \times \cdots \times (\mathbb{Z}/p_k^{a_k}\mathbb{Z})^\times.$$
- *If p is an odd prime, we have $(\mathbb{Z}/p^k\mathbb{Z})^\times \cong \mathbb{Z}/p^{k-1}(p-1)\mathbb{Z}$.*
- *We have $(\mathbb{Z}/2^k\mathbb{Z})^\times \cong \mathbb{Z}/2^{k-2}\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ for $k \geq 3$.*

The following result will also be important for us later; similarly to the previous one, it is based on the interplay between group theory and ring / field theory.

Proposition 10 (Linear independence of homomorphisms)**.** *Suppose that G is an Abelian group, and $\chi_1, \dots, \chi_k$ are distinct homomorphisms from G to $F^\times$, where F is a field. Then $\chi_1, \dots, \chi_k$ are linearly independent over F, that is if*

$$c_1\chi_1(g) + \cdots + c_k\chi_k(g) = 0 \textit{ for all } g \in G,$$

then $c_1 = \cdots = c_k = 0$.

Proof. Induction on k. Basis $k = 1$ is trivial. Suppose that we already proved it for all values strictly less than k. Suppose that

$$c_1\chi_1(g) + \cdots + c_k\chi_k(g) = 0 \text{ for all } g \in G,$$

and all the coefficients c_i are nonzero (otherwise, we get a shorter linear combination, and the induction hypothesis applies). Note that we clearly have

$$c_1\chi_1(g)\chi_1(h)+\cdots+c_k\chi_k(g)\chi_k(h)=c_1\chi_1(gh)+\cdots+c_k\chi_k(gh)=0 \text{ for all } g,h\in G.$$

Therefore,

$$c_1\chi_1(g)\chi_1(h)+\cdots+c_k\chi_k(g)\chi_k(h)-(c_1\chi_1(g)+\cdots+c_k\chi_k(g))\chi_k(h)=0 \text{ for all } g,h\in G,$$

which can be written as

$$c_1(\chi_1(h)-\chi_k(h))\chi_1(g)+\cdots+c_k(\chi_{k-1}(h)-\chi_k(h))\chi_{k-1}(g)=0 \text{ for all } g,h\in G.$$

and since the homomorphisms χ_1, ..., chi_k are distinct, there exists h for which $\chi_1(h)\neq\chi_k(h)$. Therefore, we have a linear dependence between $\chi_1,\dots,chi_{k-1}$ with nontrivial coefficients $c_1(\chi_1(h)-\chi_k(h)),\dots,c_k(\chi_{k-1}(h)-\chi_k(h))$, a contradiction. □

The following result is at the core of the notion of characteristic of a field.

Proposition 11. *Let K be a field. There exists a unique ring homomorphism $\lambda\colon\mathbb{Z}\to K$ for which $\lambda(1)=1$. The kernel* $\operatorname{Ker}\lambda$ *of this homomorphism is a prime ideal in $\mathbb{Z}$.*

Proof. The first statement is trivial. The second follows from the absence of zero divisors in K. □

Definition 3. In the setup of the previous result we have $\operatorname{Ker}\lambda=\{0\}$ or $\operatorname{Ker}\lambda=(p)$ for a prime number p. In the first case, we say that K has *characteristic* 0 ($\operatorname{char}k=0$), in the second case — that K has characteristic p ($\operatorname{char}K=p$).

Example 2. We have $\operatorname{char}(\mathbb{Q})=\operatorname{char}(\mathbb{R})=\operatorname{char}(\mathbb{C})=0$, and $\operatorname{char}(\mathbb{Z}/p\mathbb{Z})=p$.

Definition 4. Let k be a field, and let K be a another field containing k. Suppose that $a\in K$. The smallest subring of K containing k and a will be denoted by $k[a]$, the smallest subfield of K containing k and a will be denoted by $k(a)$.

Note that $k(a)=\operatorname{Frac}(k[a])$.

Proposition 12. *Let k be a field, and let K be a another field containing k. Suppose that $a\in K$. There exists a unique ring homomorphism $v_a\colon k[x]\to K$ satisfying the following two conditions:*

- *$v_a(c)=c$ for $c\in k$,*
- *$v_a(x)=a$.*

The kernel $\operatorname{Ker}v_a$ *of this homomorphism is a prime ideal in $k[x]$.*

Proof. Clearly, the only homomorphism satisfying these is

$$v_a(f(x))=f(a).$$

The kernel is a prime ideal since the target is a field, and hence has no zero divisors. □

Definition 5. If in the setting of the previous result we have $\operatorname{Ker}v_a=\{0\}$, the element a is said to be *transcendental over k*. Otherwise, the element a is said to be *algebraic over k*; $\operatorname{Ker}v_a=(f(x))$ for some monic irreducible polynomial $f(x)$ (in other words, every polynomial with coefficients in k having a as a root is divisible by $f(x)$); that polynomial $f(x)$ is called the *minimal polynomial of a over k*.

Example 3.

(1) $a=\sqrt{2}$ is algebraic over $\mathbb{Q}$, its minimal polynomial is x^2-2 since $\sqrt{2}$ is famously irrational;
(2) $a=\sqrt{3}$ is algebraic over $\mathbb{Q}(\sqrt{2})$ since $x^2-3\in\operatorname{Ker}v_a$ (exercise: find its minimal polynomial);
(3) $a=\sqrt{2}+\sqrt{3}$ is algebraic over $\mathbb{Q}$ and in general sums and products of algebraic elements are algebraic, as main theorem on symmetric polynomials easily implies (exercise);
(4) it is known (but not too easy to prove) that the base of natural logarithms e and the number π are transcendental over $\mathbb{Q}$.

Proposition 13. *If a is algebraic over k, then $k[a]=k(a)$.*

Proof. Clearly, we have $k[a] = \operatorname{Im} v_a \cong k[x]/\ker v_a$ by First Homomorphism Theorem. Also, $\operatorname{Ker} v_a = (f(x))$, and as $f(x)$ is irreducible, $\operatorname{Ker} v_a$ is a maximal ideal, so $k[x]/\operatorname{Ker} v_a$ is a field. Thus, $k(a) \subset k[a]$, since $k(a)$ is the smallest subfield containing k and a. But we also have $k[a] \subset k(a)$, hence $k(a) = k[a]$. □

Remark 2.

(1) If a is algebraic over k, then $k[a]$ is a finite-dimensional vector space over k, where the dimension is equal to n, the degree of the minimal polynomial of a. Indeed, 1, a, …, a^{n-1} are easily seen to form a spanning set (as long division by $f(x)$ shows) which is also linearly independent (because of minimality of $f(x)$).

(2) In practice, to convert $\frac{g(a)}{h(a)}$ into a polynomial expression in a, we note that $h(x)$ must be coprime to $f(x)$ if we can divide by $h(a)$. Thus, since $k[x]$ is a principal ideal domain, there exist polynomials $p(x), q(x) \in k[x]$ for which $p(x)f(x) + q(x)h(x) = 1$. Substituting $x = a$ we get $q(a)h(a) = 1$, so $\frac{1}{h(a)} = q(a)$, and $\frac{g(a)}{h(a)} = g(a)q(a)$.

The following definition formalises the intuition of adjoining roots of polynomials to existing fields.

Definition 6. Suppose k is a field, and $f(x) \in k[x]$ is an irreducible polynomial, so that $k[x]/(f(x))$ is a field. That field is said to be obtained from k by *adjoining a root of the polynomial* $f(x)$.

This is justified by the observation that the coset of x in $k[x]/(f(x))$ is a root of $f(x)$: $f(x+(f(x))) = f(x) + (f(x)) = 0 + (f(x)) = 0 \in k[x]/(f(x))$.

The central notion of Galois theory is that of a field extension. Before we recall the definition, note that a ring homomorphism from a field to any ring is injective, since a field has no nontrivial ideals. In what follows, we shall always identify a field with its image under such embedding.

Definition 7. If K and L are fields and $K \subset L$, we call L a *field extension of* K. An extension of the form $K(a)$ is called *simple*.

The following innocent result is at the core of many results of Galois theory.

Proposition 14.

(i) *Let k be a field, and let K, L be two extensions of k. Suppose that $a \in K$ and $b \in L$ are both algebraic over k with the same minimal polynomial. Then ther exists a unique homomorphism $\phi\colon k[a] \to k[b]$ satisfying the following two conditions:*
- *$\phi(c) = c$ for $c \in k$,*
- *$\phi(a) = b$.*

This homomorphism ϕ is an isomorphism.

(ii) *Let $k \subset K$ be a field extension, and let $a \in L$ be algebraic over k with the minimal polynomial $f(x) \in k[x]$. Assume that $k \subset L$ is another field extension. The field homomorphisms $\eta\colon k(a) \to L$ with $\eta(c) = c$ for all $c \in k$ are in one-to-one correspondence with roots of $f(x)$ in L.*

Proof. The first one is similar to Proposition 12, the second one is completely analogous, if we note that $\eta(a)$ must be a root of $f(x)$, since $\eta(f(a)) = f(\eta(a))$ for a homomorphism that is identical on k. □

Proposition 15 (Tower Law)**.**

(i) *If $K \subset L$ is a field extension, L has a natural structure of a vector space over K.*

(ii) *If $K \subset L \subset M$ is a tower of field extensions, then*

$$\dim_K(M) = \dim_L(M) \cdot \dim_K(L).$$

Proof. The first statement is obvious.

If $a_1 \ldots, a_k$ form a basis of L over K, and $b_1, \ldots, b_l$ form a basis of M over L, then $a_i b_j, 1 \le i \le k$, $1 \le j \le l$ form a basis of M over K (easy exercise). □

Definition 8. If $K \subset L$ is a field extension, the dimension of L as a vector space over K is often referred to as the *degree* of L over K, and is denoted $[L : K]$. Thus, the Tower Law can be written as

$$[M : K] = [M : L] \cdot [L : K].$$

EXERCISES FOR CHAPTER 2

Exercise 1.

(i) Give an example of a non-Abelian group G for which $G/Z(G)$ is Abelian. (As we discussed above, it cannot be cyclic).

(ii) Let $R = \mathbb{Z}/6\mathbb{Z}$. Give an example of a polynomial $x^2 + ax + b \in R[x]$ which has three distinct roots in R. Does such an example exist for $R = \mathbb{Z}/4\mathbb{Z}$?

(iii) Show that the equation $x^2+1 = 0$ has infinitely many solutions in the (noncommutative) ring $\mathbb{H}$ of quaternions.

Exercise 2.

(i) Show that if in a group G we have $g^2 = e$ for all g, then G is Abelian.

(ii) Show that a non-Abelian group G of order 6 must have an element of order 3. Use that to demonstrate that every non-Abelian group of order 6 is isomorphic to S_3. [Hint: if $g \in G$ is of order 3, and $h \in G$ is distinct from e, g, g^2, show that $h^2 = e$, and that $G = \{e, g, g^2, h, hg, hg^2\}$; then determine the possible multiplication tables of G.]

Exercise 3.

(i) Prove that x^2+x+1 is irreducible in $\mathbb{F}_2[x]$, and use this to prove that there exists a field $\mathbb{F}_4$ with 4 elements; write out its multiplication table.

(ii) Similarly, show that $x^2 + 1$ is irreducible in $\mathbb{F}_3[x]$, and that there is a field $\mathbb{F}_9$ with 9 elements; show that you multiply elements of $\mathbb{F}_9$ by the familiar rule

$$(a+bi)(c+di) = ac-bd+(ad+bc)i.$$

Exercise 4.

(i) List all irreducible polynomials with coefficients in $\mathbb{Z}/2\mathbb{Z}$ of degree at most 4.

(ii) Use the results of (i) to explain how to construct a field with 8 elements and a field with 16 elements.

Exercise 5. Prove that the polynomial ring $k[x]$ over any field k has infinitely many irreducible polynomials. [Hint: Imitate Euclid's proof that $\mathbb{Z}$ has infinitely many primes.]

Exercise 6.

(i) Show that $x^3 - 2x - 2$ is irreducible in $\mathbb{Q}[x]$.

(ii) Let a denote the image of x in $\mathbb{Q}[x]/(x^3 - 2x - 2)$; write each of $1/a$, $1/(1+a)$ and $1/(1+a^2)$ in the form $c_2a^2 + c_1a + c_0$ with $c_i \in \mathbb{Q}$.

Exercise 7. Show that $x^{105} - 9$ is irreducible in $\mathbb{Q}[x]$. [Hint: we know all complex roots of this polynomial; use them to show that it is impossible to factorise this polynomial into a product of two polynomials of positive degrees with integer coefficients.]

Exercise 8. Find the minimal polynomial of $\sqrt{2} + \sqrt{3}$ over $\mathbb{Q}$.

3. BASIC GALOIS THEORY

3.1. **Splitting fields.** Among field extensions, a class of utmost importance for Galois theory is given by splitting fields.

Definition 9. Let k be a field, and let $f(x) \in k[x]$. A field extension K of k is called a *splitting field of* $f(x)$ if over K the polynomial $f(x)$ splits as a product of linear factors $f(x) = (x-a_1)(x-a_2)\cdots(x-a_m)$, and $K = k(a_1, \dots, a_m)$.

Proposition 16.

(i) *For each polynomial $f(x) \in k[x]$, there exists a splitting field.*

(ii) *A splitting field of any polynomial is an extension of k of finite degree.*

Proof. To prove (i), we proceed by induction on degree of $f(x)$. We may assume that $f(x)$ has no linear factors. Suppose that $h(x)$ is an irreducible factor of $f(x)$. Consider the field $k[x]/(h(x))$; in that field $f(x)$ has at least one roots, hence a linear factor that we can factor out and proceed by induction.

To prove (ii), we note that a splitting field can be represented as a tower of simple extensions $[k(a_1,\dots,a_i)] = [k(a_1,\dots,a_{i-1})(a_i) : k(a_1,\dots,a_{i-1})]$. Since a_i is a root of $f(x)$, it is an algebraic element; by Remark 2, it generates an extension of finite degree. Applying Tower Law inductively completes the proof. □

Theorem 2 (Uniqueness of splitting fields)**.** *Let k be a field, $f(x) \in k[x]$. Suppose that K is a splitting field of $f(x)$ over k Consider a field extension $k \subset L$ where $f(x)$ splits as a product of linear factors. Then there is a homomorphism $\rho\colon K \to L$ extending the identity map on k. In particular, if K_1 and K_2 are two different splitting fields of $f(x)$ over k, then there exists an isomorphism between K_1 and K_2 extending the identity map on k.*

Proof. Induction on $[K : k]$ (which is finite by Proposition 16). We may assume that $f(x)$ has no linear factors. Let a be a root of $f(x)$ in K, and let us consider the corresponding simple extension $k_1 = k(a)$. Then $k_1 = k[x]/(g(x))$, where $g(x)$ is the minimal polynomial of a over k; note that $f(x)$ is divisible by $g(x)$. Since $f(x)$ splits as a product of linear factors over L, the polynomial $g(x)$ has roots in L; let b be one of those roots. By Proposition 14, we can extend the embedding $k \to L$ to an embedding $k_1 \to L$ by sending a to b. Thus, we now work with the extension $k_1 \subset K$ with $[K : k_1][k_1 : k] = [K : k]$, so $[K : k_1] < [K : k]$, and induction applies. The rest follows, since there can be injective maps in both directions between two k-vector spaces if these vector spaces are isomorphic, and the injections in questions are bijections. □

Definition 10. Let $k \subset K$ be a field extension. A *normal closure of K over k* is a tower of extensions $k \subset K \subset L$ where L is the smallest normal extension of k containing K.

Similarly to the previous results, it is possible to prove the following theorem.

Theorem 3. *For each finite extension $k \subset K$, a normal closure exists and is unique up to isomorphism.*

3.2. **Classification of finite fields.** In this section, we use basic Galois theory to classify finite fields.

Proposition 17.

(i) *A finite field has characteristic $p > 0$.*
(ii) *The number of elements in a finite field F is p^n for some n; here $p = \mathrm{char}(F)$.*

Proof. If $\mathrm{char}(F) = 0$, the homomorphism $\lambda\colon \mathbb{Z} \to F$ is injective, and F is infinite.

If $\mathrm{char}(F) = p$, we have $\mathrm{Im}(\lambda) \cong \mathbb{Z}/p\mathbb{Z}$, so F is a vector space over $\mathbb{Z}/p\mathbb{Z}$, which is of finite dimension because it is even a finite set; choosing a basis leads to an isomorphism $F \cong (\mathbb{Z}/p\mathbb{Z})^n$, where $n = \dim_{\mathbb{Z}/p\mathbb{Z}} F$, so $\#F = p^n$. □

Theorem 4. *Let p be a prime number. For each $q = p^n$, there exists a field of q elements, unique up to isomorphism.*

Proof. Let us do some educated guessing. Suppose that $\#F = q$. Then $F^\times$ is a finite group of order $q-1$, so $x^{q-1} = 1$ for $x \in F^\times$, and therefore $x^q = x$ for $x \in F$. Thus, the polynomial $x^q - x$ has q roots in F, so it splits as a product of linear factors over F. This suggests that F is somehow related to the splitting field of $x^q - x$ over $\mathbb{Z}/p\mathbb{Z}$. Let us make it precise.

Lemma 1. *Let L be an extension of $\mathbb{Z}/p\mathbb{Z}$ where $x^q - x$ splits as a product of linear factors. The set A of all roots of $x^q - x$ in L is a finite field of order q.*

Proof. Let us show that $\#A = q$. For that, we just need to show that all roots of $x^q - x$ are distinct. But if that were not the case, $x^q - x$ would have common roots with its derivative $qx^{q-1} - 1 = -1$ (since $q = p^n$ and $\mathrm{char}(L) = p$), a contradiction. Let us show that A is a subfield of L. It is very easy to see that if a, b are roots of $x^q - x$, then ab and a^{-1} are roots of $x^q - x$ as well; e.g., $(ab)^q = a^q b^q = ab$. For $a + b$ the argument is a bit more subtle: we have $(a+b)^p = a^p + b^p$ since all binomial coefficients $\binom{p}{i}$

for $0 < i < p$ are divisible by p, and hence $(a+b)^{p^2} = ((a+b)^p)^p = a^{p^2} + b^{p^2}, \ldots, a^q + b^q = a^{p^n} + b^{p^n} = a^q + b^q = a + b$. □

This lemma establishes existence of a finite field of q elements, and shows that any finite field of q elements is a splitting field of $x^q - x$ over $\mathbb{Z}/p\mathbb{Z}$. This implies uniqueness up to isomorphism, by Theorem 2. Note that the latter theorem deals with isomorphism identical on $\mathbb{Z}/p\mathbb{Z}$; in our case, $\mathbb{Z}/p\mathbb{Z}$ is the subfield generated by 1, so that qualifier is redundant. □

In what follows, we denote by $\mathbb{F}_q$ the(unique up to isomorphism) finite field of q elements.

3.3. **Normal extensions.**

Definition 11. Let $k \subset K$ be a field extension. It is said to be *normal* if every irreducible polynomial $f(x) \in k[x]$ that has a root in K splits as a product of linear factors in $K[x]$.

Example 4. Consider $\mathbb{Q}(\sqrt[3]{2})$ as an extension of $\mathbb{Q}$. The minimal polynomial of $\sqrt[3]{2}$ is $x^3 - 2$; this polynomial does not split over $\mathbb{Q}(\sqrt[3]{2})$, since two of its roots are complex.

It turns out that normal extensions of finite degree are precisely splitting fields.

Theorem 5. *An extension $k \subset K$ is a normal extension of finite degree if and only if K is a splitting field of some polynomial $f(x) \in k[x]$.*

Proof. Suppose that $k \subset K$ is a normal extension of finite degree. Of course, we have $K = k(a_1, \ldots, a_m)$ for some $a_1, \ldots, a_m$ (e.g. a basis of K over k). Since $k(a_i) \subset K$ and $[K : k]$ is finite, it follows that $[k(a_i) : k]$ is finite, so a_i must be algebraic. Let $g_i(x) \in k[x]$ be the minimal polynomial of a_i over k. By construction, $g_i(x)$ has a root in K, so by the normality assumption, $g_i(x)$ splits as a product of linear factors over K. Thus, L is a splitting field of $g_1(x) \cdots g_m(x)$.

Conversely, let K be a splitting field of some polynomial $f(x)$. We know that it automatically implies that $[K : k]$ is finite. Suppose $g(x) \in k[x]$ is irreducible, and that $g(x)$ has a root in K. Let L be some extension of K over which $g(x)$ splits as a product of linear factors, and let a_1 and a_2 be two roots of $g(x)$ in L. We know that $k(a_1) \cong k(a_2) \cong k[x]/(g(x))$. By Theorem 2, this isomorphism extends to $K(a_1) \cong K(a_2)$ since $K(a_1)$ is the splitting field of $f(x)$ over $k(a_1)$ and $K(a_2)$ is the splitting field of $f(x)$ over $k(a_2)$. We see that $[K(a_1) : K][K : k] = [K(a_1) : k] = [K(a_2) : k] = [K(a_2) : K][K : k]$, so $[K(a_1) : K] = [K(a_2) : K]$. (Note that this twisted argument is necessary since there is no good reason that $K(a_1) \cong K(a_2)$ as extensions of K.) Thus, $a_1 \in K$ if and only if $a_2 \in K$, so if one of the roots of $g(x)$ is in K, all of them are in K. Therefore, K is a normal extension. □

The theorem we proved implies the following technical result that will be useful later.

Corollary 2. *Let $k \subset K$ be a normal extension of finite degree.*

(i) *Suppose that there is a tower of extensions $k \subset F \subset K$. Then any k-homomorphism $\tau\colon F \to K$ extends to a k-automorphism $\tilde{\tau}\colon K \to K$.*

(ii) *Suppose that $a \in K$, and that $g(x)$ is the minimal polynomial of a over k. If b is another root of $g(x)$, then there exists a k-automorphism $\sigma\colon K \to K$ for which $\sigma(a) = b$. In other words, k-automorphisms of normal extensions act on roots of irreducible polynomials transitively.*

Proof. To prove (i), let $f(x)$ be a polynomial for which K is a splitting field over k (as we just established, such a polynomial exists). Clearly, K is also a splitting field of $f(x)$ over the field F, and over the field $\tau(F)$. This means that we can use the uniqueness of a splitting field, and conclude that there exists an isomorphism of K with $\tau(K) = K$ extending the isomorphism τ between F and $\tau(F)$. Claim (ii) follows from (i) if we put $F = k(a)$, and let τ be the map $k(a) \to K$ sending a to b. □

3.4. **Separable extensions.**

Definition 12. Let $k \subset K$ be a field extension of finite degree.

- An irreducible polynomial $f(x) \in k[x]$ is said to be *separable* if all its roots in the splitting field are distinct.
- An element $a \in K$ is said to be separable over k if its minimal polynomial is separable.

- The extension $k \subset K$ is said to be separable if every element of K is separable.

Example 5. Suppose F is a field of characteristic $p > 0$, and suppose that $t \in F$ is not a p-th power. (For instance, take $F = \mathbb{Z}/p\mathbb{Z}(t)$, where t is transcendental.) Then $x^p - t$ is irreducible and not separable, and as a consequence $F(\sqrt[p]{t})$ is not a separable extension of F. First of all, over $F(\sqrt[p]{t})$, we have $x^p - t = (x - \sqrt[p]{t})^p$ due to the binomial formula, so this polynomial has multiple roots. Irreducibility is proved as follows. Suppose that $x^p - t = g(x)h(x)$, where $g(x), h(x) \in F[x]$ are monic polynomials of positive degrees. Over $F(\sqrt[p]{t})$, due to uniqueness of factorisation, we must have $g(x) = (x - \sqrt[p]{t})^k$, $h(x) = (x - \sqrt[p]{t})^l$ with $0 < k, l < p$. Comparing constant terms, we see that $(\sqrt[p]{t})^k \in F$. It remains to find k' for which $kk' = 1$ in $\mathbb{Z}/p\mathbb{Z}$ to conclude that $\sqrt[p]{t} = ((\sqrt[p]{t})^k)^{k'} \in F$, a contradiction.

Proposition 18. *A polynomial $f(x) \in k[x]$ has multiple roots in its splitting field if and only if $f(x)$ and $f'(x)$ have a common factor of positive degree.*

Proof. It is well known that $f(x) \in k[x]$ has multiple roots in its splitting field if and only if $f(x)$ and $f'(x)$ have common roots in the splitting field, which of course happens if and only if $f(x)$ and $f'(x)$ have common factors of positive degree. □

Corollary 3.

(i) *Over a field k of characteristic zero, every irreducible polynomial is separable.*

(ii) *Over a field k of characteristic $p > 0$, a non-separable polynomial is of the form $f(x) = g(x^p)$, where $g(x) \in k[x]$.*

(iii) *Over a field k of characteristic $p > 0$ in which every element is a p-th power, every irreducible polynomial is separable.*

(iv) *Every finite extension of a finite field is separable.*

Proof. If $f(x)$ is irreducible, the only way for $f(x)$ and $f'(x)$ to have common factors of positive degree is when $f'(x) = 0$ (the zero polynomial), since otherwise $f'(x)$ is a polynomial of degree less than $f(x)$ which cannot have common factors with the (irreducible) polynomial $f(x)$. Over a field of characteristic zero, the derivative of a non-constant polynomial is never zero (proving (i)), and over a field of characteristic p it only happens when all the exponents of the powers of x present in the polynomial are divisible by p (proving (ii)). To prove (iii), we note that if $\mathrm{char}(F) = p$ and $f(x) = a_n x^{k_n p} + a_{n-1} x^{k_{n-1} p} + \cdots + a_0 x^{k_0 p}$, and we have $a_i = b_i^p$ for all i, then $f(x) = (b_n x^{k_n} + b_{n-1} x^{k_{n-1}} + b_0 x^{k_0})^p$ due to the divisibility of binomial coefficients, so $f(x)$ is not irreducible. Finally, a finite field consists of p^n elements for some n, and every element of such a field satisfies $x^{p^n} = x$, so each element $a \in F$ is a p-th power of $a^{p^{n-1}}$. □

3.5. **Automorphism groups.**

Definition 13.

- Let K be a field. The group of all automorphisms of K is denoted $\mathrm{Aut}(K)$.
- Let K and L be two extensions of a field k. A field homomorphism $\phi\colon K \to L$ is said to be a *k-linear homomorphism*, or simply a *k-homomorphism*, if it is identical on k.
- Let $k \subset K$ be a field extension. The group of all k-automorphisms of K is called the *Galois group* of K over k, and is denoted $\mathrm{Gal}(K : k)$.

Example 6.

(i) We have $\mathrm{Aut}(\mathbb{Q}) = \{e\}$. Indeed, for an automorphism ϕ, we have $\phi(1) = 1$, so $\phi(n) = \phi(1 + \cdots + 1) = \phi(1) + \cdots + \phi(1) = n\phi(1) = n$, $\phi(m/n) = \phi(m)/\phi(n) = m/n$.

(ii) We have $\mathrm{Aut}(\mathbb{R}) = \{e\}$. Indeed, note that for an automorphism ϕ, if $a - b = c^2$, then $\phi(a) - \phi(b) = \phi(c)^2$, and noticing that

$$\{x \in \mathbb{R}, x \geq 0\} = \{x \in \mathbb{R}, x = y^2 \text{ for some } y\},$$

we see that if $a \geq b$ then $\phi(a) \geq \phi(b)$. Since $\phi(1) = 1$, arguing as in (i), we see that ϕ is identical on $\mathbb{Q}$. Together with the order preserving property, this implies that ϕ is identical on $\mathbb{R}$.

(iii) We have $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})) \cong \mathbb{Z}/2\mathbb{Z}$, as such an automorphism is automatically identical on $\mathbb{Q}$, so Proposition 14 applies.

(iv) We have $\operatorname{Aut}(\mathbb{Q}(\sqrt[3]{2})) \cong \{e\}$, as such an automorphism is automatically identical on $\mathbb{Q}$, so Proposition 14 applies (and unlike (iii), only one root of x^3-2 is contained in $\mathbb{Q}(\sqrt[3]{2})$.

(v) The field of complex numbers behaves drastically different to either of the examples above. First of all, there is an obvious nontrivial automorphism, the complex conjugation. However, assuming Axiom of Choice, there are uncountably many other automorphisms of $\mathbb{C}$; for instance, there exists an automorphism that maps π to e, or to any other transcendental number, and there exists an automorphism extending any automorphism of any subfield of $\mathbb{C}$, for example, the automorphism of (iii).

Exercises for Chapter 3

Exercise 9. Let $\alpha \in \mathbb{C}$ be one of the roots of x^3-x-1, and $\beta \in \mathbb{C}$ be one of the roots of $x^3-x-\alpha$. Write some polynomial with rational coefficients that has β as a root.

Exercise 10. Let $k \subset K$ be a field extension, and let $\alpha, \beta \in K$. Suppose that $[k(\alpha)\colon k] = m$ and $[k(\beta)\colon k] = n$. Show that $[k(\alpha,\beta)\colon k(\alpha)] = n$ if and only if $[k(\alpha,\beta)\colon k(\beta)] = m$. Does either of these equivalent condition hold for $\alpha = \sqrt[3]{2}$ and $\beta = \omega\sqrt[3]{2}$, where ω is the primitive complex cube root of 1?

Exercise 11. Compute the degree of the splitting field of x^4-2 over $\mathbb{Q}$, and find a nice basis for that extension as a $\mathbb{Q}$-vector space.

Exercise 12. Compute the degree of the splitting field of $x^{12}-1$ over $\mathbb{Q}$, and find a nice basis for that extension as a $\mathbb{Q}$-vector space. Show that this extension is also the splitting field of $(x^4-1)(x^3-1)$ over $\mathbb{Q}$.

Exercise 13. Let p be a prime number, let k be a field, and let $a \in k$.

(i) Show that $x^p - a$ is either irreducible in $k[x]$ or has a root in k. (*Hint*: this essentially was proved in one example above).

(ii) Let $k \subset K$ be a field extension, and assume that p is coprime to $[K\colon k]$. Prove that a is a p-th power in k if and only if it is a p-th power in K.

Exercise 14.

(i) Determine the Galois group $\operatorname{Gal}(\mathbb{C}\colon \mathbb{R})$.

(ii) Determine the Galois group $\operatorname{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3})\colon \mathbb{Q})$.

4. Galois groups and the Galois correspondence

In this section, we discuss the central result of Galois theory, the correspondence between subfields and subgroups of automorphism groups.

4.1. Galois extensions.

The following theorem is one of central results of Galois theory; it connects properties of a field extension with properties of the corresponding Galois group.

Theorem 6. *Let $k \subset K$ be a finite extension. Then*

$$\#\operatorname{Gal}(K:k) \le [K:k],$$

moreover $\#\operatorname{Gal}(K:k) = [K:k]$ if and only if $k \subset K$ is a normal and separable extension.

Instead of proving this theorem, we shall prove a more general result which is easy to prove, as it offers more flexibility by separating the source and the target of a map. We already saw this strategy when proving uniqueness of a splitting field in Theorem 2.

Theorem 7. *Let K and L be two extensions of a field K, and assume that K is a finite degree extension. The number of k-homomorphisms $\phi\colon K \to L$ does not exceed $[K:k]$, and is equal to $[K:k]$ of and only if every irreducible polynomial $f(x) \in k[x]$ that has a root in K splits as a product of distinct linear factors in $L[x]$.*

Proof. Let us prove that the number of k-homomorphisms $\phi\colon K \to L$ does not exceed $[K:k]$, arguing by induction on $[K:k]$. Let $a \in K \setminus k$, and consider $k_1 = k(a)$. Suppose that $f(x)$ is the minimal polynomial of a over k, and $\deg(f) = n$. Any k-homomorphism $\tau\colon K \to L$, once restricted to k_1, gives a homomorphism $\sigma\colon k_1 \to L$. Note that once such a homomorphism is fixed, its extension to a homomorphism from K to L is a k_1-homomorphism from K to L. Indeed, $[K:k_1] < [K:k]$, so we may assume that the number of k_1-homomorphisms from K to L does not exceed $[K:k_1]$. By Proposition 14, k-homomorphisms $\phi\colon k_1 \to L$ are in one-to-one correspondence with roots of $f(x)$ in L. Thus, the number of k-homomorphisms from k_1 to L does not exceed $\deg(f) = n = [k_1:k]$. A k-homomorphism from K to L is uniquely determined by its restriction to k_1 and the extension of the latter, so the number of k-homomorphisms does not exceed $[K:k_1][k_1:k] = [K:k]$.

Suppose that the number number of k-homomorphisms $\phi\colon K \to L$ equals $[K:k]$. The above argument shows that it can only happen if the number of k_1-homomorphisms from K to L is equal to $[K:k_1]$ and at the same time the number of k-homomorphisms from k_1 to L is equal to $[k_1:k]$. The latter condition holds if and only if $f(x)$ splits as a product of distinct linear factors over L. Since this is holds for any a, the desired implication follows.

Now let us assume that for every irreducible polynomial $f(x) \in k[x]$ that has a root in K splits as a product of distinct linear factors over $L[x]$. Once again, take some $a \in K \setminus k$, and consider $k_1 = k(a)$. Suppose that $f(x)$ is the minimal polynomial of a over k, and $\deg(f) = n$. Let $b \in K$; consider the minimal polynomials of β over k and over k_1, call them $g(x)$ and $g_1(x)$. Being the minimal polynomial over a larger field k_1, $g_1(x)$ divides $g(x)$. Since $g(x)$ splits as a product of distinct factors over L, it follows that $g_1(x)$ must split as a product of distinct factors. This is sufficient: by Proposition 14, the number of k-homomorphisms from k_1 to L is equal to $\deg(f) = n = [k_1:k]$, and by induction the number of k_1-homomorphisms from K to L is equal to $[K:k_1]$, so the number of k-homomorphisms from K to L is equal to $[K:k_1][k_1:k] = [K:k]$. □

Definition 14. A field extension $k \subset K$ is called a *Galois extension* if it is finite, normal, and separable.

Let us state one very useful result that is essentially contained in the proof of Theorem 7.

Proposition 19. *If $k \subset K$ is a Galois extension, and F is a field in a tower of extensions $k \subset F \subset K$, then $F \subset K$ is always a Galois extension.*

The extension $k \subset F$ is not necessarily Galois: for instance, when K is the splitting field of some polynomial $f(x)$, F may contain just one root of that polynomial, and as such not be normal. However, it is of course always separable.

4.2. **Fixed subfields.**

Definition 15. Let K be a field, and let G be a subgroup of $\mathrm{Aut}(K)$. We define the *fixed subfield K^G* by the formula

$$K^G = \{a \in K\colon g(a) = a \text{ for all } a \in G\}.$$

As it says on the tin, a fixed subfield of any subgroup of $\mathrm{Aut}(G)$ is, in particular, a subfield of K; this immediately follows from the fact that G consists of automorphisms of K.

Theorem 8. *A field extension $k \subset K$ is a Galois extension if and only if $k = K^G$ for some finite subgroup $G \subset \mathrm{Aut}(K)$. Moreover, in that case* $\mathrm{Gal}(K:k) = G$.

Proof. Suppose $k \subset K$ is a Galois extension. Let $G = \mathrm{Gal}(K:k)$. Consider $K^G \subset K$; according to our definition of G, we have $k \subset K^G \subset K$, so $[K:k] \ge [K:K^G]$. By Theorem 6, we have $\#G = \#\mathrm{Gal}(K:k) = [K:k]$ and $\#\mathrm{Gal}(K:K^G) \le [K:K^G]$. It remains to note that since $G \subset \mathrm{Gal}(K:K^G)$, so

$$[K:k] = \#G = \le \#\mathrm{Gal}(K:K^G) \le [K:K^G].$$

Thus, $[K:k] = [K:K^G]$, so $k = K^G$.

Let us now assume that G is a finite subgroup of $\mathrm{Aut}(K)$; we shall prove that K is a Galois extension of K^G. First, we establish that $\#G \ge [K:K^G]$. Let $G = \{g_1, \ldots, g_n\}$; it is enough to prove that if

$x_1, \dots, x_{n+1} \in K$ are any elements, then they are linearly dependent over K^G. Such a linear dependency $\sum_{j=1}^{n+1} u_j x_j$, if exists, would produce n different consequences

$$\sum_{j=1}^{n+1} g_i(x_j) u_j = 0, \quad i = 1, \dots, n.$$

We consider these consequences as n linear equations with $n+1$ unknowns u_j. This system has nontrivial solutions over K. Among all nontrivial solutions, let us choose one with as few nonzero coordinates as possible. Re-numbering variables if necessary, we may assume that $u_1, \dots, u_r$ are nonzero, and $u_j = 0$ for $j > r$; moreover, we may re-scale to ensure $u_1 = 1$. Take some $h \in G$. Applying it to the equations above, we have

$$\sum_{j=1}^{n+1} hg_i(x_j) h(u_j) = 0, \quad i = 1, \dots, n.$$

Since $\{hg_1, \dots, hg_n\} = \{g_1, \dots, g_n\}$, the $(n+1)$-tuple $(h(u_1), \dots, h(u_{n+1}))$ is also a solution to our system of equations. Of course, the difference of two solutions to a homogeneous system of equations is also a solution, so the $(n+1)$-tuple $(h(u_1) - u_1, \dots, h(u_{n+1}) - u_{n+1})$ is a solution. However, $h(u_j) - u_j = 0$ for $j > r$ since for such j we have $u_j = 0$, and $h(u_1) - u_1 = h(1) - 1 = 0$, so we found a solution with fewer nonzero coordinates; such solution must therefore be trivial, so that $h(u_i) = u_i$ for all i (and all h), in other words $u_i \in K^G$ for all i. Thus, the $n+1$ elements $x_1, \dots, x_{n+1} \in K$ are linearly dependent over K^G.

Clearly, G is a subgroup of $\mathrm{Gal}(K : K^G)$, so together with the result $\#G \geq [K : K^G]$ we just proved, Theorem 6 implies that

$$\#G \leq \#\mathrm{Gal}(K : K^G) \leq [K : K^G] \leq \#G.$$

Thus, all inequalities here are in fact equalities, in particular by the same Theorem 6 we see that K is a normal and separable extension of K^G. □

Example 7. Consider the extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Note that $3 \notin \mathbb{Q}(\sqrt{2})$, since if there exist $a, b \in \mathbb{Q}$ for which $a + b\sqrt{2} = \sqrt{3}$, then $a^2 + 2b^2 + 2ab\sqrt{2} = 3$, and since $\sqrt{2}$ is irrational, we conclude $ab = 0$, so either $\sqrt{3}$ is rational or $\sqrt{\frac{3}{2}}$ is rational, a contradiction. Therefore, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] > 2$. Since $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$, the degree $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}]$ is even and at most 4. Thus, $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

The dimension counting shows that the spanning set $1, \sqrt{2}, \sqrt{3}, \sqrt{6}$ is a basis, and therefore the automorphisms

$$\sigma\colon \begin{cases} \sqrt{2} \to \sqrt{2}, \\ \sqrt{3} \to -\sqrt{3}, \\ \sqrt{6} \to -\sqrt{6}, \end{cases} \qquad \tau\colon \begin{cases} \sqrt{2} \to -\sqrt{2}, \\ \sqrt{3} \to \sqrt{3}, \\ \sqrt{6} \to -\sqrt{6}, \end{cases} \qquad \sigma\tau\colon \begin{cases} \sqrt{2} \to -\sqrt{2}, \\ \sqrt{3} \to -\sqrt{3}, \\ \sqrt{6} \to \sqrt{6}, \end{cases}$$

are well defined, and together with the identity automorphism give four different automorphisms of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$, implying that it is a Galois extension. Examining these automorphisms directly, we deduce that $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Alternatively, one can note that $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is the splitting field of $(x^2 - 2)(x^2 - 3)$, and therefore a Galois extension of $\mathbb{Q}$ (finite, separable since characteristic 0, normal since a splitting field). Then the above candidates for automorphisms give an exhaustive list of possibilities, since for any automorphism α, we have $\alpha(\sqrt{2}) = \pm\sqrt{2}$, $\alpha(\sqrt{3}) = \pm\sqrt{3}$, and $\alpha(\sqrt{6}) = \alpha(\sqrt{2} \cdot \sqrt{3}) = \alpha(\sqrt{2})\alpha(\sqrt{3})$. Being a Galois extension, this extension must have as many automorphisms as its degree, so all these automorphisms must be well defined.

4.3. **Galois correspondence.** In this section, we establish the main result connecting properties of extensions to properties of automorphism groups.

Theorem 9 (Galois correspondence). *Let $k \subset K$ be a Galois extension, denote $G = \mathrm{Gal}(K : k)$. Consider the sets*

$$\mathscr{F} = \{k \subset F \subset K\colon\ F \text{ a field}\},$$
$$\mathscr{G} = \{H \subset G\colon\ H \text{ a subgroup}\}.$$

Then the maps

$$\gamma\colon \mathscr{F} \to \mathscr{G}, \quad \gamma(F) = \mathrm{Gal}(K:F)$$

and

$$\phi\colon \mathscr{G} \to \mathscr{F}, \quad \phi(H) = K^H$$

satisfy the following properties:

(i) *If $F_1 \subset F_2$, then $\gamma(F_1) \supset \gamma(F_2)$.*

(ii) *If $H_1 \subset H_2$, then $\phi(H_1) \supset \phi(H_2)$.*

(iii) *For all $F \in \mathscr{F}$, we have $\phi(\gamma(F)) = F$.*

(iv) *For all $H \in \mathscr{G}$, we have $\gamma(\phi(H)) = H$.*

(v) *For all $F \in \mathscr{F}$, we have*

$$[K:F] = \#\gamma(F), \quad [F:k] = \frac{\#G}{\#\gamma(F)}.$$

(vi) *If $F \in \mathscr{F}$, the extension $k \subset F$ is normal if and only if $\gamma(F)$ is a normal subgroup of G; in the latter case, we have* $\mathrm{Gal}(F:k) \cong G/\gamma(F)$.

Proof. If $F_1 \subset F_2$, then automorphisms that fix F_2 must fix F_1, therefore $\gamma(F_1) \supset \gamma(F_2)$, proving (i).

If $H_1 \subset H_2$, then elements fixed by H_2 must be fixed by H_1, therefore $\phi(H_1) \supset \phi(H_2)$, proving (ii).

By Proposition 19, the field extension $F \subset K$ is Galois, hence by Theorem 8, we have

$$\phi(\gamma(F)) = \phi(\mathrm{Gal}(K:F)) = K^{\mathrm{Gal}(K:F)} = F,$$

proving (iii).

The equations

$$\gamma(\phi(H)) = \gamma(K^H) = \mathrm{Gal}(K:K^H) = H$$

follow from Theorem 8 as well, proving (iv).

To prove (v), we note that since the field extension $F \subset K$ is Galois, we have $[K:F] = \#\mathrm{Gal}(K:F) = \gamma(F)$. By Tower Law, $[F:k] = \frac{[K:k]}{[K:F]} = \frac{\#G}{\#\gamma(F)}$.

To prove (vi), let us establish a property of the map γ.

Lemma 2. *Let $g \in G$, and let $F \in \mathscr{F}$. Then $\gamma(g(F)) = g\gamma(F)g^{-1}$.*

Proof. We have $h \in \gamma(g(F))$ if and only if $h((g(a)) = g(a)$ for all $a \in F$, which happens if and only if $g^{-1}(h(g(a))) = a$ for all $a \in F$, that is $g^{-1}hg \in \gamma(F)$. Thus, $g^{-1}\gamma(g(F))g = \gamma(F)$, or in other words $\gamma(g(F)) = g\gamma(F)g^{-1}$, as required. □

Thus, $\gamma(F)$ is a normal subgroup of G if and only if $\gamma(g(F)) = \gamma(F)$ for all $g \in G$, which is equivalent to $g(F) = F$ for all $g \in G$.

Let us assume $k \subset F$ is a normal extension, and take $a \in F$ with the minimal polynomial $f(x)$ over k. For each $g \in G$, the element $g(a)$ is also a root of $f(x)$, so because of normality we have $g(a) \in F$. Hence $g(F) = F$.

Conversely, suppose that $g(F) = F$ for all $g \in G$. Let us take $a \in F$ with the minimal polynomial $f(x)$ over k. By normality of $k \subset K$, $f(x)$ splits as a product of linear factors over K. If b is another root of $f(x)$, then by the second part of Corollary 2 there exists $g \in G$ for which $g(a) = b$. Since $g(F) = F$, this implies $b \in F$, so F is a normal extension.

Finally, if F is a normal extension of k, then $g(F) = F$ for all $g \in G$, therefore elements of G restrict to k-automorphisms of F; this gives a homomorphism

$$\pi\colon\ \mathrm{Gal}(K:k) \to \mathrm{Gal}(F:k).$$

Note that by the first part of Corollary 2, this homomorphism is surjective, and that

$$\mathrm{Ker}\,\pi = \{g \in G\colon\ g \text{ restricts to identity on } F\} = \mathrm{Gal}(K:F) = \gamma(F),$$

so our last claim follows from First Homomorphism Theorem. □

Example 8. We continue discussing the extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$. The subgroups of the Galois group $G = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} = \{e, \sigma, \tau, \sigma\tau\}$ are

(1) $H = \{e\}$, $\phi(H) = \mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \sqrt{3})$,

(2) $H = \{e, \sigma\}$, $\phi(H) = \mathbb{Q}(\sqrt{2})$,
(3) $H = \{e, \tau\}$, $\phi(H) = \mathbb{Q}(\sqrt{3})$,
(4) $H = \{e, \sigma\tau\}$, $\phi(H) = \mathbb{Q}(\sqrt{6})$,
(5) $H = G$, $\phi(H) = \mathbb{Q}$.

Example 9. The following problem was offered to participants of a famous international mathematics olympiad, "Tournament of Towns", in the autumn competition of 1997:

> Consider the product of all possible expressions
>
> $$\Pi = \pm\sqrt{1} \pm \sqrt{2} \pm \cdots \pm \sqrt{99} \pm \sqrt{100}$$
>
> (for all possible choices of the ± signs). Prove that this product is an integer, and moreover a perfect square.

First of all, note that this product is clearly the square of the product of all possible expressions

$$\Pi' = \sqrt{1} \pm \sqrt{2} \pm \cdots \pm \sqrt{99} \pm \sqrt{100}$$

where the first sign is plus. So it is enough to show that this latter product is an integer. Clearly, this product is an element of $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \ldots, \sqrt{99})$, the splitting field of $\prod_{k=2}^{99}(x^2 - \sqrt{k})$. Being a splitting field, this extension is clearly a Galois extension. Each automorphism of this extension sends each of the square roots either to itself or to its negative, and therefore fixes the product Π'. Thus the Galois correspondence implies that $\Pi' \in \mathbb{Q}$. However, Π' is a product of sums of algebraic integers (roots of monic polynomials with integer coefficients), and hence is an algebraic integer itself. A rational number that is an algebraic integer must be an integer.

Exercises for Chapter 4

Exercise 15. Determine the Galois group of the splitting field of $x^{12} - 1$ over $\mathbb{Q}$.

Exercise 16. Find the splitting field and the Galois group of $x^3 - 5$ over $\mathbb{Q}(\sqrt{2})$.

Exercise 17. Find the splitting field and the Galois group of $x^4 - 2x^2 - 5$ over $\mathbb{Q}$.

Exercise 18. Let K be the splitting field of $f = x^4 - 3$ over $\mathbb{Q}$. Describe the Galois group $G = \mathrm{Gal}(K\colon \mathbb{Q})$ and its action on the 4 roots of f. List all the subgroups of G and use this to write down all the intermediate fields between $\mathbb{Q}$ and K. Explain which of those intermediate fields are Galois extensions of $\mathbb{Q}$.

Exercise 19. Compute the Galois groups of the splitting fields of the polynomial $x^4 - 3$ over $\mathbb{F}_5$, $\mathbb{F}_7$, $\mathbb{F}_{11}$ and $\mathbb{F}_{13}$.

Exercise 20. Let $k \subset K$ be a Galois extension with the Galois group $G = \{g_1, \ldots, g_n\}$, and let $a \in K$. Show that $K = k(a)$ if and only if $g_1(a), \ldots, g_n(a)$ are distinct elements of K.

Exercise 21.

(i) Show that if $\mathbb{F}_{p^n}$ is isomorphic to an extension of $\mathbb{F}_{(p')^{n'}}$ (where p and p' are primes) then $p = p'$ and n is divisible by n'.
(ii) Explain why $\mathbb{F}_{p^n}$ is a Galois extension of $\mathbb{F}_p$.
(iii) Show that the Galois group $\mathrm{Gal}(\mathbb{F}_{p^n} : \mathbb{F}_p)$ is the cyclic group $\mathbb{Z}/n\mathbb{Z}$. (*Hint*: show that $x \mapsto x^p$ is an automorphism, and that it is of order n in the Galois group).
(iv) Show that if n is divisible by n' then $\mathbb{F}_{p^n}$ is isomorphic to a field extension of $\mathbb{F}_{p^{n'}}$. Moreover, show that in that case $\mathbb{F}_{p^n}$ is a Galois extension of $\mathbb{F}_{p^{n'}}$, and describe the Galois group $\mathrm{Gal}(\mathbb{F}_{p^n} : \mathbb{F}_{p^{n'}})$.

5. Applications of the Galois correspondence

5.1. Cyclotomic fields and construction of regular polygons.

5.1.1. *Roots of unity of degree five.* As a first example, let us discuss the splitting field of $x^5-1=(x-1)(x^4+x^3+x^2+x+1)$ over $\mathbb{Q}$. We denote by ζ a root of $x^4+x^3+x^2+x+1$; this polynomial is irreducible over $\mathbb{Q}$ (by Eisenstein criterion after setting $x=y+1$). We have $\mathbb{Q}(\zeta)=\mathbb{Q}[x]/(x^4+x^3+x^2+x+1)$. Note that other roots of this polynomial are ζ^2, ζ^3, and ζ^4, so the splitting field is $\mathbb{Q}(\zeta)$, a degree 4 extension. If $\psi\in\mathrm{Gal}(\mathbb{Q}(\zeta):\mathbb{Q})$, then ψ is completely determined by the value of $\psi(\zeta)$, which can be any of the four roots of $x^4+x^3+x^2+x+1$. If we let $\sigma(\zeta)=\zeta^2$, we have $\sigma^2(\zeta)=\sigma(\zeta^2)=(\sigma(\zeta))^2=\zeta^4$, $\sigma^3(\zeta)=\sigma(\zeta^4)=\zeta^8=\zeta^3$, and $\sigma^4(\zeta)=\zeta$. Thus, $\mathrm{Gal}(\mathbb{Q}(\zeta):\mathbb{Q})=\mathbb{Z}/4\mathbb{Z}$ and is generated by the automorphism σ we just defined.

As an illustration of the Galois correspondence, $\mathbb{Z}/4\mathbb{Z}$ has only one nontrivial subgroup, $2\mathbb{Z}/4\mathbb{Z}$, which in our case is generated by σ^2, the automorphism sending ζ to ζ^4. If we consider the obvious basis $1,\zeta,\zeta^2,\zeta^3$ of $\mathbb{Q}(\zeta)$, we note that

$$\sigma^2(a+b\zeta+c\zeta^2+d\zeta^3)=a+b\zeta^4+c\zeta^3+d\zeta^2=a+b(-1-\zeta-\zeta^2-\zeta^3)+c\zeta^3+d\zeta^2,$$

and imposing the condition $\sigma^2(a+b\zeta+c\zeta^2+d\zeta^3)=a+b\zeta+c\zeta^2+d\zeta^3$ implies $b=0, c=d$. Thus,

$$\mathbb{Q}(\zeta)^{\langle\sigma^2\rangle}=\mathbb{Q}(\zeta^2+\zeta^3).$$

In fact, this can be simplified: if we denote

$$\begin{cases} A=\zeta^2+\zeta^3,\\ B=\zeta+\zeta^4,\end{cases}$$

we note that $A+B=-1$, and $AB=\zeta+\zeta^2+\zeta^3+\zeta^4=-1$, so A and B are roots of t^2+t-1, i.e. $\frac{-1\pm\sqrt{5}}{2}$. In particular, $\mathbb{Q}(\zeta)^{\langle\sigma^2\rangle}=\mathbb{Q}(\sqrt{5})$. Also, from this computation, it is easy to figure out how to construct the regular pentagon using a ruler and compass.

5.1.2. *General cyclotomic fields.*

Definition 16. Suppose n is a positive integer. Consider $\zeta_n=e^{2\pi i/n}$, a primitive n-th root of unity. We call $\mathbb{Q}(\zeta_n)$ the *n-th cyclotomic field.* We also introduce the *cyclotomic polynomial*

$$\Phi_n(x)=\prod_{1\le k\le n, \gcd(k,n)=1}(x-e^{2\pi ik/n}).$$

Proposition 20.

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

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

Proof. To establish (i), note that every root of unity of degree n is a primitive root of unity of some degree $d\mid n$, therefore

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

From this, the integrality of $\Phi_d(x)$ follows by easy induction.

The proof of (ii) is more complicated. Assuming the contrary, we may write $\Phi_n(x)=g(x)h(x)$, where $g(x)$ and $h(x)$ are monic polynomials with integer coefficients. Without loss of generality, $g(x)$ is irreducible; denote by ζ one of its roots. Let us take a prime p not dividing n, and prove that ζ^p is also a root of $g(x)$. Since p does not divide n, ζ^p is a primitive root, so is a root of $g(x)$ or $h(x)$, so if our assertion fails, it is a root of $h(x)$. Thus, ζ is a root of $h(x^p)$, so $h(x^p)$ is divisible by $g(x)$, $h(x^p)=g(x)h_1(x)$. Considering this modulo p, and denoting by $\bar{f}(x)$ the class modulo p of a polynomial $f(x)\in\mathbb{Z}[x]$, we get $\bar{h}(x)^p=\bar{g}(x)\bar{h}_1(x)$. This shows that $\bar{h}(x)$ and $\bar{g}(x)$ have common factors, so $\bar{\Phi}_n(x)$ has repeated factors, so $\overline{x^n-1}$ has repeated factors, therefore it has common roots with its derivative. But the derivative of $\overline{x^n-1}$ is $\overline{nx^{n-1}}$, and since p does not divide n, the only irreducible factor of the derivative is x, which is not a factor of $\overline{x^n-1}$, a contradiction. Thus, for a prime p not dividing n, ζ^p is also a root of $g(x)$, and iterating this, we see that ζ^k is a root of $g(x)$ for any k with $\gcd(k,n)=1$, so all primitive roots are roots of $g(x)$. It follows that $g(x)=\Phi_n(x)$ is irreducible. □

Corollary 4. *We have* $\mathrm{Gal}(\mathbb{Q}(\zeta_n):\mathbb{Q})\cong(\mathbb{Z}/n\mathbb{Z})^\times$.

Proof. Clearly, $\mathbb{Q}(\zeta_n)$ is the splitting field of $x^n - 1$ over $\mathbb{Q}$, so it is a Galois extension, and the number of automorphisms is equal to the degree of the extension, which is the degree of $\Phi_n(x)$. Automorphisms must send ζ_n to one of the roots of the same irreducible polynomial, so all automorphisms are $\sigma_k\colon \zeta_n \mapsto \zeta_n^k$ with $\gcd(k,n) = 1$. Note that $\sigma_k(\sigma_l(\zeta_n)) = \sigma_k(\zeta_n^l) = (\sigma_k(\zeta_n))^l = \zeta_n^{kl}$, so the assignment $\sigma_k \mapsto k + n\mathbb{Z}$ is a group isomorphism of $\mathrm{Gal}(\mathbb{Q}(\zeta_n) : \mathbb{Q})$ with $(\mathbb{Z}/n\mathbb{Z})^\times$. □

5.1.3. *Ruler and compass constructions.* Recall from module 2215 "Fields, Rings, and Modules" that for a complex number a that can be constructed using a ruler and compass, we have $[\mathbb{Q}(a) : \mathbb{Q}] = 2^m$ for some m. Suppose that $n = p_1^{a_1} \cdots p_s^{a_s}$ is the prime decomposition of n. Then

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg \Phi_n(x) = \phi(n) = p_1^{a_1-1} \cdots p_s^{a_s-1}(p_1 - 1)\cdots(p_s - 1).$$

For it to be a power of two, we need that whenever p_i is odd, we have $a_i = 1$, and $p_i - 1 = 2^{b_i}$ for some i. Note that $2^{(2s+t)t} + 1$ is divisible by $2^t + 1$, and therefore is not prime. This implies one half of the following result.

Theorem 10. *The regular n-gon can be constructed by a ruler and compass if and only if*

$$n = 2^s p_1 p_2 \cdots p_r,$$

where p_i are distinct "Fermat primes" (prime numbers of the form $2^{2^k} + 1$).

Proof. We already established that no other n could possibly work. Suppose that $n = 2^s p_1 p_2 \cdots p_r$ as above.

Note that if the regular m-gon can be constructed, the regular $2m$-gon can be constructed by bisecting the angle $2\pi/m$. Also, if $\gcd(m_1, m_2) = 1$, and both the regular m_1-gon and the regular m_2-gon can be constructed, then the regular m_1m_2-gon can be constructed. Indeed, we can find a and b for which $am_1 + bm_2 = 1$, and write $\frac{2b\pi}{m_1} + \frac{2a\pi}{m_2} = \frac{2\pi}{m_1m_2}$, which shows how to construct the corresponding angle.

Thus, it is enough to prove that the regular m-gon can be constructed when $m = p = 2^{2^k} + 1$ is a Fermat prime. For that, recall that by Proposition 8 we have

$$\mathrm{Gal}(\mathbb{Q}(\zeta_p) : \mathbb{Q}) = (\mathbb{Z}/p\mathbb{Z})^\times \cong \mathbb{Z}/(p-1)\mathbb{Z} = \mathbb{Z}/2^{2^k}\mathbb{Z}.$$

Note that $\mathbb{Z}/2^{2^k}\mathbb{Z}$ has a sequence of subgroups

$$\{e\} \subset G_{2^k-1} = 2^{2^k-1}\mathbb{Z}/2^{2^k}\mathbb{Z} = \{e, 2^{2^k-1}\} \subset \cdots \subset G_1 = 2\mathbb{Z}/2^{2^k}\mathbb{Z} \subset G_0 = \mathbb{Z}/2^{2^k}\mathbb{Z}.$$

By the Galois correspondence, this sequence corresponds to a sequence of subfields

$$\mathbb{Q}(\zeta_p) \supset \mathbb{Q}(\zeta_p)^{G_{2^k-1}} \supset \cdots \supset \mathbb{Q}(\zeta_p)^{G_1} \supset \mathbb{Q}.$$

Note that the degree of each extension $[\mathbb{Q}(\zeta_p)^{G_i} : \mathbb{Q}(\zeta_p)^{G_{i-1}}]$ is equal to the index of the corresponding subgroup, that is 2, so at each step the extension is obtained by solving a quadratic equation, hence the result. □

Remark 3. Fermat conjectured that all numbers of the form $2^{2^k} + 1$ were primes, but, for instance, $2^{2^5} + 1 = 4294967297$ is divisible by 641, as discovered by Euler. The only currently known Fermat primes are 3, 5, 17, 257, and 65537; it is unknown if there exist any other Fermat primes.

5.1.4. *Roots of unity of degree 17.* Let us discuss another example of a Fermat prime, $p = 17$; hopefully this would bring the proof above closer to reality. Note that $(\mathbb{Z}/17\mathbb{Z})^\times$ is generated by 3: we have the following table:

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
3^k	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

Let us denote $\zeta = \zeta_{17}$. We shall consider invariants of subgroups of $(\mathbb{Z}/17\mathbb{Z})^\times$ generated by $\sigma_3\colon \zeta \mapsto \zeta^3$. Such subgroups are constrained by divisibility by powers of 2 of the exponents of powers of 3 that emerge. On the first step, we separate the odd exponents from the even ones, introducing the quantities

$$A_0 = \zeta^9 + \zeta^{13} + \zeta^{15} + \zeta^{16} + \zeta^8 + \zeta^4 + \zeta^2 + \zeta,$$
$$A_1 = \zeta^3 + \zeta^{10} + \zeta^5 + \zeta^{11} + \zeta^{14} + \zeta^7 + \zeta^{12} + \zeta^6.$$

We have $A_0 + A_1 = \sum_{j=1}^{16} \zeta^j = -1$. The element A_0A_1 is also invariant under the whole Galois group (half of it preserves both A_0 and A_1, half of it swaps them), so it is an integer. In its expansion, 1 does not appear, and all primitive roots appear with the same coefficient, so since there are 16 primitive roots and 64 summands, $A_0A_1 = -4$. Thus, A_0 and A_1 are roots of $t^2 + t - 4 = 0$.

Further, we separate exponents depending on remainder modulo 4:

$$B_0 = \zeta^{13} + \zeta^{16} + \zeta^4 + \zeta,$$
$$B_2 = \zeta^9 + \zeta^{15} + \zeta^8 + \zeta^2,$$
$$B_1 = \zeta^3 + \zeta^5 + \zeta^{14} + \zeta^{12},$$
$$B_3 = \zeta^{10} + \zeta^{11} + \zeta^7 + \zeta^6.$$

Clearly, $B_0 + B_2 = A_0$, $B_1 + B_3 = A_1$, and also by direct inspection we have $B_0B_2 = -1$, $B_1B_3 = -1$, so we have quadratic equations for these quantities.

Next step is separating exponents depending on remainder modulo 8:

$$C_0 = \zeta^{16} + \zeta,$$
$$C_4 = \zeta^{13} + \zeta^4,$$
$$C_2 = \zeta^9 + \zeta^8,$$
$$C_6 = \zeta^{15} + \zeta^2,$$
$$C_1 = \zeta^3 + \zeta^{14},$$
$$C_5 = \zeta^5 + \zeta^{12},$$
$$C_3 = \zeta^{10} + \zeta^7,$$
$$C_7 = \zeta^{11} + \zeta^6.$$

We have $C_0 + C_4 = B_0$, $C_2 + C_6 = B_2$, $C_1 + C_5 = B_1$, $C_3 + C_7 = B_3$. Also, by direct inspection, we have $C_0C_4 = B_1$, $C_2C_6 = B_3$, $C_1C_5 = B_2$, $C_3C_7 = B_0$, so we have quadratic equations for these quantities also.

Finally, $C_0 = \zeta^{16} + \zeta = \zeta^{-1} + \zeta$, and we can easily derive a quadratic equation for ζ.

5.2. **Solvability of equations in radicals.** In this section, we discuss one of the starting points of Galois theory, application of group theory to solvability of equations in radicals.

Definition 17. A field extension $k \subset K$ is said to be *radical* if there exists a tower of field extensions

$$k = k_0 \subset k_1 \subset k_2 \cdots \subset k_{r+1} = K,$$

where for each $1 \le i \le r+1$ there exists a prime number p_i and an element $a_i \in k_i$ for which $a_i^{p_i} \in k_{i-1}$ and $k_i = k_{i-1}(a_i)$. (Note that $a_i^{p_i}$ might be a p_i-th power in k_{i-1}, in which case we are essentially adjoining a root of unity.)

This definition covers all fields that can be obtained from the ground field k by a sequence of simple extensions each of them adjoins a root of some power (without loss of generality, those powers may be assumed prime, since extracting a root of a composite power may be accomplished by extracting several roots of prime powers). Usually, we would care about specific elements being expressed in radicals, which means that we also need to consider subfields of radical extensions.

Definition 18. A field extension $k \subset K$ is said to be *solvable* if it can be included in a tower of extensions $k \subset K \subset F$, where the extension $k \subset F$ is radical.

In other words, an extension is solvable if its elements can be expressed via elements of the ground field k using arithmetic operations and extracting roots, which is exactly what we aim to detect.

Example 10.

(i) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}, \omega)$ where $\omega^2 + \omega + 1$ is a radical extension, since $\omega^3 = 1$.
(ii) $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2} + \sqrt{3})$ is a radical extension since we know that $\mathbb{Q}(\sqrt{2} + \sqrt{3}) = \mathbb{Q}(\sqrt{2}, \sqrt{3})$.
(iii) The extension $\mathbb{Q} \subset \mathbb{Q}(a)$, where a is a root of $x^3 - 9x + 9$, is not radical. To establish that, one can show that this polynomial has three real roots, that $\mathbb{Q}(a)$ is the splitting field of $x^3 - 9x + 9$ over $\mathbb{Q}$, that an extension of degree 3 that is radical is obtained by adjoining one cube root, and that a degree 3 extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt[3]{b})$ with $b \in \mathbb{Q}$ is not normal, hence cannot be a splitting field. However, the general process of solving cubic equations shows that $\mathbb{Q} \subset \mathbb{Q}(a)$ is a solvable extension.

5.2.1. *Solvable groups.*

Definition 19. Let G be a group. Recall that $G' = [G, G]$, the *derived subgroup*, or the *commutator subgroup*, is the subgroup of G generated by all commutators $ghg^{-1}h^{-1}$, $g, h \in G$. The *derived series* of G is the sequence of subgroups

$$G^{(0)} = G, \quad G^{(k+1)} = [G^{(k)}, G^{(k)}].$$

A group G is called *solvable* if $G^{(k)} = \{e\}$ for some k.

Example 11.

(i) If G is Abelian, then $G^{(1)} = \{e\}$, so G is solvable.
(ii) If $G = S_3$, then $G^{(1)} = A_3 \cong \mathbb{Z}/3\mathbb{Z}$, so $G^{(2)} = \{e\}$, and G is solvable.
(iii) If $G = A_5$, then in fact $G^{(1)} = G$. Indeed, $(ijk) = (ijl)(ikm)(ijl)^{-1}(ikm)^{-1}$, and $(ij)(kl) = (ijk)(ijl)(ijk)^{-1}(ijl)^{-1}$, and these (together with e) are all possible cycle types of permutations of five elements. Hence, G is not solvable.

Let us first establish some basic properties of solvable groups.

Proposition 21.

(i) *If G is a solvable group, and H is a subgroup of G, then H is solvable.*
(ii) *If G is a solvable group and H is a normal subgroup of G, then G/H is solvable.*
(iii) *If H is a normal subgroup of G and both H and G/H are solvable, then G is solvable.*

Proof. (i) : if $H \subset G$, then$H^{(k)} \subset G^{(k)}$, hence the derived series of H must collapse.

(ii) : clearly, $(G/H)^{(k)}$ is the image of $G^{(k)}$ under the canonical projection $\pi \colon G \to G/H$, hence the derived series of G/H must collapse.

(iii) : if $(G/H)^{(k)} = \{eH\}$ for some k, then by the remark made in (ii), for that k we have $G^{(k)} \subset H$, hence for each m we have $G^{(k+m)} \subset H^{(m)}$, and the derived series of G must collapse. □

Corollary 5. *The symmetric group S_n is not solvable for $n \geq 5$.*

Proof. Indeed, for such n the symmetric group S_n contains A_5 as a subgroup. □

The following result will be very useful later, as it encodes solvability in a way suited for applying the Galois correspondence.

Theorem 11. *For a finite group G, the following are equivalent:*

(1) *G is solvable;*
(2) *There exists a sequence of subgroups*

$$G = G_0 \supset G_1 \supset \cdots \supset G_l = \{e\}$$

where G_{i+1} is a normal subgroup of G_i for all i, and G_i/G_{i+1} is Abelian.

(3) *There exists a sequence of subgroups*

$$G = G_0 \supset G_1 \supset \cdots \supset G_l = \{e\}$$

where G_{i+1} is a normal subgroup of G_i for all i, and G_i/G_{i+1} is cyclic of prime order.

Proof. (1) implies (2), since we can take $G_i = G^{(i)}$, as $[H,H]$ is norma in H, and $H/[H,H]$ is Abelian.

To prove that (2) implies (3), consider one of the inclusions $G_i \supset G_{i+1}$, and assume that $G_i \neq G_{i+1}$ (else, remove G_{i+1}). Denote by $H_i^{(1)}$ the maximal proper subgroup of G_i containing G_{i+1}. If $H_i^{(1)} = G_{i+1}$, stop, else denote by $H_i^{(2)}$ the maximal proper normal subgroup of $H_i^{(1)}$ containing G_{i+1}, etc. We get a sequence

$$G_i = H_i^{(0)} \supset H_i^{(1)} \supset \cdots \supset H_i^{(k)} = G_{i+1}.$$

Since $H_i^{(j+1)}$ is a maximal normal subgroup of $H_i^{(j)}$, the quotient $H_i^{(j)}/H_i^{(j+1)}$ is a simple group. Also, $H_i^{(j)}$ is a subgroup of G_i, $H_i^{(j+1)}$ contains G_{i+1}, and G_i/G_{i+1} is Abelian, so $H_i^{(j)}/H_i^{(j+1)}$ must be Abelian. Hence, it is cyclic of prime order. Joining all these sequences together, we get a sequence prescribed by (3).

Finally, (3) implies (1) by a simple induction on l using Proposition 21 (iii). □

5.2.2. *Radical and solvable extensions.* The following result is our first step towards relating solvability of equations in radicals and solvability of Galois groups.

Theorem 12. *Suppose that $k \subset K$ is a Galois extension with the Galois group G. Assume that k contains p roots of unity of degree p for each prime $p \mid \#G$. Then G is solvable if and only if $k \subset K$ is a radical extension.*

Proof. First of all, note that due to the third equivalent definition of solvability of Theorem 11 and the Galois correspondence, G is solvable if and only if there exists a tower of field extensions

$$k = k_0 \subset k_1 \subset k_2 \cdots \subset k_{r+1} = K,$$

such that each extension $k_i \subset k_{i+1}$ is a Galois extension with the Galois group that is cyclic of prime order.

Next, Proposition 23 guarantees in our case that an extension $k_i \subset k_{i+1}$ has a cyclic Galois group of prime order p_i if and only if k_{i+1} is obtained from k_i by adjoining a p_i-th root of some element. □

Let us demonstrate that the assumption of K being a Galois extension in Theorem 12 is not too restrictive.

Proposition 22. *If $k \subset K$ is a radical field extension, the normal closure of K over k is radical as well.*

Proof. If the extension is radical, $K = k(a_1, \ldots, a_r)$ with $a_i^{p_i} \in k(a_1, \ldots, a_{i-1})$ for some prime p_i. Let $f_i(x)$ be the minimal polynomial of a_i over k. Then the normal closure L of K over k is the splitting field of $f(x) = f_1(x)f_2(x)\cdots f_r(x)$. Let us denote by $b_j^{(i)}$, $j = 1, \ldots, m_i$, the roots of $f_i(x)$, and define $K_i = k(\beta_j^{(s)} : s \leq i) \supset k(a_1, \ldots, a_i)$. Since for each $j = 1, \ldots, m_i$, the elements a_i and $b_j^{(i)}$ of K_i have the same minimal polynomial $f_i(x)$, there exists a k-automorphism $\tau_j^{(i)}$ of L for which $\tau_j^{(i)}(a_i) = b_j^{(i)}$. Since $a_i^{p_i} \in K_{i-1}$, we see that $(b_j^{(i)})^{p_i} = \tau_j^{(i)}(a_i)^{p_i} = \tau_j^{(i)}(a_i^{p_i}) \in \tau_j^{(i)}(K_{i-1})$. But K_{i-1} is a normal extension of k, hence is preserved by any k-automorphism, so $(b_j^{(i)})^{p_i} \in K_{i-1}$, and this immediately implies that L is a radical extension. □

Let us deal with the matter of roots of unity. Let us start with a useful auxiliary result.

Proposition 23. *Suppose that a field k contains n distinct roots of unity of degree n, for some given $n \geq 2$. A Galois extension $k \subset K$ with $[K:k] = n$ has the Galois group $\mathbb{Z}/n\mathbb{Z}$ if and only if there exists $a \in K$ for which $a^n \in k$ and $K = k(a)$.*

Proof. Suppose that there exists $a \in K$ for which $a^n \in k$ and $K = k(a)$. Then $f(x) = x^n - a^n$ must be irreducible over k, for otherwise we have $[K:k] = [k(a):k] < n$. Since k-automorphisms of K are in one-to-one correspondence with roots of $f(x)$ in K, and the latter are $\zeta \cdot a$ where ζ is an n-th root of unity, the Galois group is isomorphic to the subgroup of n-th roots of unity in $k^\times$, which is cyclic by Proposition 8.

Suppose that $\mathrm{Gal}(K:k)=\langle\sigma\rangle$. Denote by $\epsilon\in k$ a primitive n-th root of unity. For each $b\in K$, we may consider the element $a=b+\epsilon^{-1}\sigma(b)+\cdots+\epsilon^{1-n}\sigma^{n-1}(b)$. By Proposition 10, we may choose b for which $a\neq 0$. Clearly, we have

$$\sigma(a)=\sigma(b)+\epsilon^{-1}\sigma^2(b)+\cdots+\epsilon^{1-n}\sigma^n(b)=\sigma(b)+\epsilon^{-1}\sigma^2(b)+\cdots+\epsilon b=\epsilon a,$$

so $\sigma(a^n)=(\sigma(a))^n=y^n$, so $a^n\in K^{\langle\sigma\rangle}=k$. Moreover, we have $\sigma^k(a)=\epsilon^k a$, so by Exercise 20, we have $K=k(a)$. □

In what follows, we will have to restrict ourselves to the case of zero characteristic: $\operatorname{char}k=0$.

Proposition 24. *Suppose that $k\subset K$ is a Galois extension, that and $n>2$ is an integer. Let k' and K' be, respectively, the splitting fields of x^n-1 over k and over K. Then*

(i) *If one of the three groups $H=\mathrm{Gal}(K':k)$, $G=\mathrm{Gal}(K:k)$, $G_1=\mathrm{Gal}(K':k')$ is solvable, then all three of them are.*

(ii) *The degree $[K':k']$ divides the degree $[K:k]$.*

Proof. Let us first remark that for $\operatorname{char}k=0$ and for any field extension $k\subset K$, there is a natural restriction map $\rho\colon \mathrm{Gal}(K':K)\to\mathrm{Gal}(k':k)$. Moreover, since an F-automorphism of $F(\zeta_n)$ is determined by the image of ζ_n, this map is injective, hence $\mathrm{Gal}(K':K)$ is isomorphic to a subgroup of $\mathrm{Gal}(k':k)$.

Since $k\subset K'$ is a tower of Galois extensions $k\subset K\subset K'$, it is a Galois extension itself, and by Galois correspondence we know that both $\mathrm{Gal}(K':K)$ and G' are normal subgroups of H. Moreover, $G\cong H/\mathrm{Gal}(K':K)$ and $\mathrm{Gal}(k':k)\cong H/G_1$. It remains to notice that $\mathrm{Gal}(K':K)$ and $\mathrm{Gal}(k':k)$ are Abelian groups, as by the remark above they are subgroups of $\mathrm{Gal}(\mathbb{Q}(\zeta_n):\mathbb{Q})\cong(\mathbb{Z}/n\mathbb{Z})^\times$. Now, $G\cong H/\mathrm{Gal}(K':K)$ shows that G is solvable if and only if H is solvable, and $\mathrm{Gal}(k':k)\cong H/G_1$ shows that H is solvable if and only if G_1 is solvable, proving (i).

By the remark above, $\mathrm{Gal}(K':K)$ is isomorphic to a subgroup of $\mathrm{Gal}(k':k)$, so

$$[K':K]=\#\mathrm{Gal}(K':K)\mid\#\mathrm{Gal}(k':k)=[k':k].$$

By Tower Law, $[K':K][K:k]=[K':k'][k':k]$, so $[K':k']$ divides $[K:k]$, proving (ii). □

We are now ready to state and prove the main result of this section.

Theorem 13. *Suppose that* $\operatorname{char}k=0$, *and that $k\subset K$ is a finite field extension. This extension is solvable if and only if the normal closure L of K over k has a solvable Galois group over k.*

Proof. First, suppose that $\mathrm{Gal}(L:k)$ is solvable. Consider the field L' which is the splitting field of $x^{[L:k]}-1$ over L. Then by Proposition 24 (i) L' is a Galois extension of k with a solvable Galois group. By Proposition 24 (ii), $[L':k']\mid[L:k]$, hence by Theorem 12 the extension $k'\subset L'$ is radical. Clearly, $k\subset k'$ is a radical extension, so $k\subset L'$ is radical, and $k\subset K$ is solvable.

Suppose that $k\subset K$ is solvable, so that it can be included in a tower of extensions $k\subset K\subset F$, where the extension $k\subset F$ is radical. Denote by M the normal closure of F over k; by Proposition 22, the extension $k\subset M$ is radical. Moreover, let M' be the splitting field of $x^{[M:k]}-1$ over M, which still is a radical extension of k. By Proposition 24 (ii), $[M':k']\mid[M:k]$, so by Theorem 12, the group $\mathrm{Gal}(M':k')$ is solvable. By Proposition 24 (i), the group $\mathrm{Gal}(M:k)$ is solvable, and therefore its quotient $\mathrm{Gal}(L:k)$ is solvable. □

Corollary 6. *Suppose that* $\operatorname{char}k=0$. *Roots of polynomials $f(x)\in k[x]$ can be expressed in terms of coefficients of $f(x)$ by arithmetic operations and extracting roots if and only if the Galois group of the splitting field of $f(x)$ over k is solvable.*

5.2.3. *Cubics revisited.* Consider a cubic polynomial $f(x)=x^3+ax^2+bx+c\in k[x]$. We assume it irreducible and separable; otherwise, solving it would be reduced to solving a quadratic equation. Let x_1,x_2,x_3 be its roots, $K=k(x_1,x_2,x_3)$, and $G=\mathrm{Gal}(K:k)$. Since f is irreducible, G is a transitive subgroup of S_3, so $G=A_3$ or $G=S_3$.

If $G=A_3$, the general approach to extensions with cyclic Galois group (Proposition 23) suggests to consider $X=x_1+\omega x_2+\omega^2x_3$. We have $(123)X=\omega^2X$ and $(132)X=\omega X$, so X^3 is invariant under the Galois group, $X^3 \in k$. Similarly, for $Y = x_1 + \omega^2 x_2 + \omega x_3$, we have $Y^3 \in k$, and from knowing $x_1 + x_2 + x_3 = -a$, X, and Y, we can recover x_1, x_2, and x_3.

If $G = S_3$, then X^3 and Y^3 are still fixed by A_3 but are exchanged by the transposition (23) (and hence all transpositions), therefore $X^3 + Y^3$ and $X^3 Y^3$ are fixed by the Galois group and hence belong to k, and we have a quadratic equation for X^3 and Y^3 that we can solve. From there we proceed in the same way to recover x_1, x_2, and x_3.

5.2.4. *Discriminant.* How to distinguish between the two cases $G = A_3$ and $G = S_3$ above? Suppose that $\mathrm{char}(k) \neq 2$. For a separable polynomial $f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in k[x]$ with roots $x_1, \ldots, x_n$, we define its *discriminant*

$$D(f) = \prod_{i<j} (x_i - x_j)^2.$$

Clearly, $D(f)$ as an expression is a symmetric polynomial in $x_1, \ldots, x_n$, therefore $D(f) \in k$. Moreover, if we consider

$$\sqrt{D(f)} = \prod_{i<j} (x_i - x_j),$$

then it is clear that for each $\sigma \in S_n$ we have $\sigma(\sqrt{D(f)}) = \pm\sqrt{D(f)}$, and that $\sigma(\sqrt{D(f)}) = \sqrt{D(f)}$ if and only if σ is even. Thus, the Galois group of the splitting field of f over k is contained in A_n if and only if $D(f)$ is a square in k.

5.2.5. *Quartics revisited.* Let $f(x) = x^4 + ax^3 + bx^2 + cx + d \in k[x]$ be a quartic polynomial which we again assume irreducible and separable. Let x_1, x_2, x_3, x_4 be the roots of $f(x)$, and let $K = k(x_1, x_2, x_3, x_4)$. We recall that S_4 has a nontrivial normal subgroup $H = \{e, (12)(34), (13)(24), (14)(23)\}$. If $\mathrm{Gal}(K : k)$ contains H, we may consider $L = K^H$ which is a Galois extension of k. There are two different choices of formulas one can find in textbooks: either $\{x_1x_2 + x_3x_4, x_1x_3 + x_2x_4, x_1x_4 + x_2x_3\}$ or $\{(x_1 + x_2)(x_3 + x_4), (x_1 + x_3)(x_2 + x_4), (x_1 + x_4)(x_2 + x_3)\}$ are H-invariant and generate K^H. The first choice suggests to look at the polynomial $R(x) = (x - x_1x_2 - x_3x_4)(x - x_1x_3 - x_2x_4)(x - x_1x_4 - x_2x_3)$ called the cubic resolution of $f(x)$. It is easy to check that $R(x) \in k[x]$, and that $D(R) = D(f)$. Solving this cubic, we may assume we already know $x_1x_2 + x_3x_4$. However, $x_1x_2x_3x_4 = d \in k$, so we can compute x_1x_2 and x_3x_4 individually by solving a quadratic equation. Similarly, we can compute x_1x_3 and x_1x_4. Finally, $(x_1x_2)(x_1x_3)(x_1x_4) = x_1^2(x_1x_2x_3x_4)$, and we obtain the solution x_1.

5.2.6. *Cubic resolvent of a quartic equation.* Let us discuss how to distinguish between different Galois groups of quartics. Since $f(x)$ is assumed irreducible, the Galois group is a transitive subgroup of S_4. These are easy to classify: S_4, A_4, D_4, $\mathbb{Z}/4\mathbb{Z}$, and $H \cong (\mathbb{Z}/2\mathbb{Z})^2$. Note that D_4 and $\mathbb{Z}/4\mathbb{Z}$ are only unique up to conjugation. It turns out that one can distinguish between these cases as follows:

- if $D(f)$ is not a square and $R(x)$ is irreducible, we have $\mathrm{Gal}(K : k) = S_4$ (since it is not a subgroup of A_4, and its order is divisible by 3);
- if $D(f)$ is a square and $R(x)$ is irreducible, we have $\mathrm{Gal}(K : k) = A_4$ (since it is a subgroup of A_4, and its order is divisible by 3);
- if $D(f)$ is a square and $R(x)$ is reducible, we have $\mathrm{Gal}(K : k) = H$, (since it is a subgroup of A_4, and it cannon contain a 3-cycle, for a 3-cycle would act transitively on roots of R);
- if $D(f)$ is not a square and $R(x)$ is reducible, we have $\mathrm{Gal}(K : k) = D_4$ or $\mathrm{Gal}(K : k) = \mathbb{Z}/4\mathbb{Z}$ (for the same reason as we just mentioned, it cannot contain a 3-cycle).

Finally, we mention without a proof the following result:

Proposition 25. *Suppose that $D(f)$ is not a square, and $R(x)$ is reducible. Then $R(x)$ may only have one root in k. Moreover, if we denote this root by r, then if $x^2 + ax + b - r$ and $x^2 - rx + d$ split over $k(D(f))$, then* $\mathrm{Gal}(K : k) = \mathbb{Z}/4\mathbb{Z}$, *else* $\mathrm{Gal}(K : k) = D_4$.

5.2.7. *Impossibility results for solving equations in radicals.* Let us use the results that we established to show that occasionally it is impossible to solve equations of higher degrees in radicals. Our first result will show that a general formula, such as the formulas we have for quadratic, cubic and quartic equations, is impossible for degree 5 and higher.

Theorem 14. *Let ground field k be $\mathbb{Q}$. Suppose that $x_1, \dots, x_n$, $n \geq 5$, are formal variables, and write*

$$(x - x_1)\cdots(x - x_n) = x^n + q_1 x^{n-1} + \cdots + q_{n-1}x + q_n.$$

There is no formula expressing $x_1, \dots, x_n$ via $q_1, \dots, x_n$ by arithmetic operations and extracting roots of various degrees.

Proof. As usual, we denote by $e_1, \dots, e_n$ the elementary symmetric polynomials in these variables. Note that $\mathbb{Q}(x_1,\dots,x_n)^{S_n} = \mathbb{Q}(e_1,\dots,e_n)$. (For that, note that since each x_i is algebraic over $\mathbb{Q}(e_1,\dots,e_n)$, every element of $\mathbb{Q}(x_1,\dots,x_n)$ is of the form $\frac{g(x_1,\dots,x_n)}{h(e_1,\dots,e_n)}$, and such element is in $\mathbb{Q}(x_1,\dots,x_n)^{S_n}$ if and only if $g(x_1,\dots,x_n) \in \mathbb{Q}[x_1,\dots,x_n]^{S_n} = \mathbb{Q}[e_1,\dots,e_n]$.) Moreover, by Theorem 8, the field extension $\mathbb{Q}(e_1,\dots,e_n) \subset \mathbb{Q}(x_1,\dots,x_n)$ is a Galois extension with $\mathrm{Gal}(\mathbb{Q}(x_1,\dots,x_n) : \mathbb{Q}(e_1,\dots,e_n)) = S_n$. Since S_n is not solvable for $n \geq 5$, the statement follows from Corollary 6. □

This result, however, can be substantially improved; we shall show that there are many specific polynomials whose roots are not expressible via the coefficients using arithmetic operations and radicals. Let us give one such example right away.

Proposition 26. *Roots of the polynomial $f(x) = x^5 - 6x + 3$ are not expressible over $\mathbb{Q}$ using arithmetic operations and extracting roots of various degrees.*

Proof. Note that this polynomial is irreducible (Eisenstein for $p = 3$), and that it has three real roots and two complex roots (since $f(x) < 0$ for $x \ll 0$, $f(0) > 0$, $f(1) < 0$, and $f(x) > 0$ for $x \gg 0$, there are at least 3 real roots by Intermediate Value Theorem; if there were more roots, the derivative $f'(x) = 5x^4 - 6$ would have at least 3 real roots by Rolle Theorem).

Let K be the splitting field of $f(x)$ over $\mathbb{Q}$. Each automorphism of K over $\mathbb{Q}$ is uniquely determined by its action on the roots of $f(x)$, hence $\mathrm{Gal}(K : \mathbb{Q})$ may be identified with a subgroup G of S_5. By Corollary 2, G acts transitively on $1, \dots, 5$. Also, since $f'(x)$ has two complex roots, the complex conjugation as an automorphism of K is represented by a transposition in S_5. Let us prove the following general statement.

Lemma 3. *A transitive subgroup G of S_5 containing a transposition is equal to S_5.*

Proof. Without loss of generality, the transposition contained in G is (12). Due to transitivity of G, for each $k = 1,\dots,5$, we can find $\sigma \in G$ for which $\sigma(1) = k$, so $\sigma(12)\sigma^{-1} = (jk) \in G$, where $j = \sigma(2)$. Thus, every $k = 1,\dots,5$ is involved in at least one transposition in G, so there are at least three transpositions in G, and therefore some element is involved in two different transpositions. Since the transpositions (ik) and (jk) generate all permutations of i, j, k, G contains a subgroup isomorphic to S_3. Discarding the choice of notation made before, we may assume that G contains the standard S_3 permuting $1, 2, 3$. Clearly, we can find $\sigma \in G$ such that $\sigma(1) = 4$. Notably, $\sigma' = \sigma \cdot (23)$ also has $\sigma'(1) = 4$. Therefore, $\sigma(12)\sigma^{-1} = (4\sigma(2))$ and $\sigma'(12)(\sigma')^{-1} = (4\sigma'(2))$, so 4 is involved in two different transpositions. At least one of them is different from (45), and that transposition together with the subgroup S_3 generates the standard subgroup S_4. Finally, 5 is involved in some transposition, and that transposition together with the subgroup S_4 generates all of S_5. Thus, $G = S_5$. □

Our statement now follows from Corollary 6. □

5.3. **Fundamental theorem of algebra.** Let us use Galois theory to establish the following famous result.

Theorem 15 (Fundamental theorem of algebra)**.** *Every polynomial $f(x)$ with complex coefficients has a complex root.*

Proof. Let $f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$. We consider

$$g(x) = f(x)(\bar{a}_n x^n + \bar{a}_{n-1}x^{n-1} + \cdots + \bar{a}_1 x + \bar{a}_0)(x^2 + 1) \in \mathbb{R}[x].$$

Let K be the splitting field of $g(x)$ over $\mathbb{R}$. It suffices to show that $K = \mathbb{C}$.

Let $G = \mathrm{Gal}(K : \mathbb{R})$, write $\#G = 2^m q$, where q is odd. By Sylow's First Theorem (see any group theory textbook if you do not know what it is), G has a subgroup H of order 2^m; we put $L = K^H$. The extension $L \subset K$ is a Galois extension with the Galois group H, so $[K:L] = \#H = 2^m$, and Tower Law implies that $[L:\mathbb{R}] = q$. Let us first show that $L = \mathbb{R}$; assume $a \in \mathbb{L} \setminus \mathbb{R}$ with the minimal polynomial of degree $d > 1$ over $\mathbb{R}$. By Tower Law, $d = [\mathbb{R}(a):\mathbb{R}] \mid [L:\mathbb{R}] = q$, so d is odd. However, a polynomial of an odd degree must have a real root, which is a contradiction, so $L = \mathbb{R}$, and $\#\mathrm{Gal}(K:\mathbb{R}) = 2^m$. If $m = 1$, K is a quadratic extension of $\mathbb{R}$ containing $\mathbb{C}$, hence $K = \mathbb{C}$. Suppose that $m > 1$. Since K contains $\mathbb{C}$, we have $[K:\mathbb{C}] = 2^{m-1}$. By Proposition 4, $\mathrm{Gal}(K:\mathbb{C})$, being a group of order 2^{m-1}, has a nontrivial centre, and an easy induction utilising Proposition 21 shows that this group is solvable. By Theorem 11, $\mathrm{Gal}(K:\mathbb{C})$ has a subgroup of index two. By Galois correspondence, the field of invariants of such a subgroup is a quadratic extension of $\mathbb{C}$. However, $\mathbb{C}$ has no quadratic extensions, since every complex number has a square root. This contradiction completes the proof. □

Exercises for Chapter 5

Exercise 22. Explain how to compute $\cos(2\pi/13)$ by solving quadratic and cubic equations only.

Exercise 23.

(i) Determine the Galois group of the splitting field of $x^5 - 4x + 2$ over $\mathbb{Q}$.

(ii) Same question for the Galois group of the splitting field of $x^4 - 4x + 2$ over $\mathbb{Q}$.

Exercise 24. Prove that a subgroup of A_5 that contains a 3-cycle and acts transitively on $1, 2, 3, 4, 5$ coincides with A_5.

6. Further results in Galois theory

In this chapter, we shall establish some further results in Galois theory, and outline further directions that will not be touched in this course.

6.1. Primitive element theorem.

Definition 20. Let $K \subset L$ is a field extension. The element $a \in L$ is said to be a *primitive element* of this extension if $L = K(a)$.

Example 12. Consider the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Neither of the elements $\sqrt{2}$ and $\sqrt{3}$ is a primitive element, but, as we saw before, $\sqrt{2} + \sqrt{3}$ is a primitive element; $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$.

Theorem 16 (Primitive element theorem)**.** *A finite separable extension of an infinite field is simple.*

Remark 4. This theorem also holds for finite fields; we leave it as an exercise for the reader to prove it in that case.

Proof. We may include our separable extension $K \subset L$ into a tower $K \subset L \subset M$, where $K \subset M$ is a Galois extension. Let $G = \mathrm{Gal}(M:K)$. Because of the Galois correspondence, intermediate subfields between K and M are in one-to-one correspondence with subgroups of G; in particular, the set of intermediate subfields is finite. Let us consider all the proper intermediate subfields between K and L, denoting them by $F_1, \ldots, F_k$. Those subfields are subspaces of L, and we claim that their union is not the whole of L. To show that, we include each of them in a hyperplane (a subspace of dimension $\dim L - 1$); if we choose coordinates $x_1, \ldots, x_n$, the i-th hyperplane is defined by a linear equation $g_i(x_1, \ldots, x_n) = 0$. Consider $f = g_1 g_2 \cdots g_k$. By Corollary 1, there exist elements $a_1, \ldots, a_n$ for which $f(a_1, \ldots, a_n) \neq 0$, and hence the point with the coordinates $a_1, \ldots, a_n$ is not in the union $F_1 \cup \cdots \cup F_k$. Call that point $a \in L$, and consider $K(a)$. It cannot be a proper subfield of L, so it must coincide with L. □

6.2. Normal basis theorem.

Definition 21. Let $K \subset L$ be a Galois extension. A K-basis of L is said to be *normal* if it is a single orbit of the Galois group $\mathrm{Gal}(L:K)$.

Example 13. Consider the extension $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2})$. The elements 1 and $\sqrt{2}$ do not form a normal basis since they do not form a single orbit of the Galois group (the nontrivial element of the Galois group fixes 1 and negates $\sqrt{2}$). The orbit of $\sqrt{2}$ consists of two linearly dependent elements, so it is not a normal basis either. The orbit of $1 + \sqrt{2}$ forms a basis $e_1 = 1 + \sqrt{2}$, $e_2 = 1 - \sqrt{2}$.

Theorem 17 (Normal basis theorem)**.** *A Galois extension L of an infinite field K has a normal basis.*

Remark 5. This theorem also holds over finite fields; we leave it as an exercise for the reader to prove it in that case.

Proof. Let us establish the following auxiliary result.

Lemma 4. *Suppose that $K \subset L$ is a Galois extension with the Galois group* $\mathrm{Gal}(L:K) = \{e = \sigma_1, \sigma_2, \dots, \sigma_n\}$, *and let $e_1, \dots, e_n$ be a basis of L over K. Then the n-tuples*

$$v_i = (\sigma_1(e_i), \dots, \sigma_n(e_i)), \quad 1 \le i \le n,$$

form a basis of L^n over L.

Proof. Let W be the linear span of $v_1, \dots, v_n$. Suppose that W is a proper subspace of L^n. Then there exists a nonzero linear function ξ on L^n for which $\xi(w) = 0$ for all $w \in W$, or in other words, if we implement ξ as $\xi(v) = c \cdot v$, there exist $c_1, \dots, c_n \in L$ for which

$$c_1\sigma_1(e_i) + \cdots + c_n\sigma_n(e_i) = 0$$

for all $1 \le i \le n$. Since e_i form a basis, and Galois groups act K-linearly, this means that

$$c_1\sigma_1(x) + \cdots + c_n\sigma_n(x) = 0$$

for all $x \in L$, so by Proposition 10, $c_1 = \ldots = c_n = 0$, a contradiction. □

To prove our result, it is of course enough to show that $\sigma_1(x), \dots, \sigma_n(x)$ are linearly independent for some $x \in L$, since we know that $[L:K] = \#\mathrm{Gal}(L:K)$. If it were not the case, then for each x we would be able to find $a_1, \dots, a_n \in K$ which are not simultaneously equal to zero such that $a_1\sigma_1(x) + \cdots + a_n\sigma_n(x) = 0$. Applying the elements σ_i^{-1} to this, we get

$$a_1\sigma_i^{-1}\sigma_1(x) + \cdots + a_n\sigma_i^{-1}\sigma_n(x) = 0, \quad 1 \le i \le n.$$

We may regard these as a system of linear equations; by our assumptions, it has a nontrivial solution, so $\det A(x) = 0$ for all x, where

$$A(x) = \begin{pmatrix} \sigma_1^{-1}\sigma_1(x) & \sigma_1^{-1}\sigma_2(x) & \dots & \sigma_1^{-1}\sigma_n(x) \\ \sigma_2^{-1}\sigma_1(x) & \sigma_2^{-1}\sigma_2(x) & \dots & \sigma_2^{-1}\sigma_n(x) \\ \vdots & \ddots & \dots & \vdots \\ \sigma_n^{-1}\sigma_1(x) & \sigma_n^{-1}\sigma_2(x) & \dots & \sigma_n^{-1}\sigma_n(x) \end{pmatrix}.$$

Let us show that there exists x for which $\det A(x) \ne 0$. Note that if we choose a basis $e_1, \dots, e_n$ of L over K, then for each $x = x_1e_1 + \cdots + x_ne_n$ we manifestly have $A(x) = x_1A(e_1) + \cdots + x_nA(e_n)$, and $\det A(x)$ is a polynomial in $x_1, \dots, x_n$. Since K is assumed infinite, it is enough to show that $\det(x_1A(e_1) + \cdots + x_nA(e_n))$ is a nonzero polynomial. Note that $A(x) = x_1A(e_1) + \cdots + x_nA(e_n)$ only when $x_1, \dots, x_n \in K$, but after doing that rewriting, we may take values $x_1, \dots, x_n$ from either K or L to establish that this polynomial assumes nonzero values.

By Lemma 4, we can find some coefficients $c_1, \dots, c_n \in L$ for which $c_1v_1 + \cdots + c_nv_n = (1, 0, \dots, 0)$. Since by our choice of notation, $\sigma_1 = e$, this means that

$$c_1e_1 + \cdots + c_ne_n = 1,$$
$$c_1\sigma(e_1) + \cdots + c_n\sigma(e_n) = 0, \quad \sigma \ne e,$$

or in other words putting $\sigma = \sigma_i^{-1}\sigma_j$

$$\sigma_i^{-1}\sigma_j(e_1) + \cdots + \sigma_i^{-1}\sigma_j(e_n) = \begin{cases} 1, & i = j, \\ 0, & i \ne j. \end{cases}$$

This demonstrates that $c_1A(e_1) + \cdots + c_nA(e_n) = I_n$, the identity $n \times n$ matrix, hence $\det(c_1A(e_1) + \cdots + c_nA(e_n)) = 1 \ne 0$, as required. □

6.3. Kronecker theorem for computing Galois groups.

Theorem 18 (Kronecker, 1882)**.** *Let k be a field, and let $f(x) \in k[x]$ be a separable polynomial with the splitting field K over k. Let $a_1, \dots, a_n$ be the roots of $f(x)$ in K, and take n formal variables $t_1, \dots, t_n$, one for each root, which we use to form the polynomial*

$$F(x, t_1, \dots, t_n) = \prod_{\sigma \in S_n} (x - t_{\sigma(1)} a_1 - \cdots t_{\sigma(n)} a_n).$$

(i) *We have $F(x, t_1, \dots, t_n) \in k[x, t_1, \dots, t_n]$.*

(ii) *Let $F_1(x, t_1, \dots, t_n)$ be the irreducible factor of F in $k[x, t_1, \dots, t_n]$ which is divisible by $x - t_1 a_1 - \cdots t_n a_n$. Then* Gal$(K : k)$ *is isomorphic to the subgroup of S_n consisting of all permutations τ for which $\tau F_1 = F_1$, where τ acts by permutations of $t_1, \dots, t_n$.*

Proof. For each permutation $\tau \in S_n$, we denote by τ_t and τ_a the action of τ on

$$\prod_{\sigma \in S_n} (x - t_{\sigma(1)} a_1 - \cdots t_{\sigma(n)} a_n)$$

by permuting $t_1, \dots, t_n$ and $a_1, \dots, a_n$, respectively. We note that $\tau_a F(x, t_1, \dots, t_n) = F(x, t_1, \dots, t_n)$, since applying τ_a merely amounts to replacing the variable σ by $\sigma\tau^{-1}$. Thus, the coefficients of this polynomial can be expressed using elementary symmetric polynomials in $a_1, \dots, a_n$, which, up to signs, are coefficients of $f(x)$, and therefore elements of k. Hence, $F(x, t_1, \dots, t_n) \in k[x, t_1, \dots, t_n]$, proving (i).

Let us denote $\theta = t_1 a_1 + \cdots + t_n a_n$. If $\tau_t F_1 = F_1$, then $x - \tau_t \theta$ is a factor of F_1. Conversely, if $x - \tau_t \theta$ is a factor of F_1, then $\tau_t F_1$ and F_1 have common factors, so since F_1 is irreducible we must have $\tau_t F_1 = F_1$. Therefore, the group which we are to prove is the Galois group is

$$\{\tau \in S_n \colon x - \tau_t \theta \text{ is a factor of } F_1\}.$$

Note that $\tau_a \tau_t(\theta) = \theta$, so $\tau_t \theta = \tau_a^{-1} \theta$, and we can rewrite the above as

$$\{\tau \in S_n \colon x - \tau_a^{-1} \theta \text{ is a factor of } F_1\}.$$

We also note (and leave it as an exercise for the reader to fill in the details) that since $t_1, \dots, t_n$ are formal variables, θ is a primitive element of $K(t_1, \dots, t_n)$ over $k(t_1, \dots, t_n)$. Hence $\tau \in$ Gal$(K : k)$ if and only if $\tau_a \theta$ and θ have the same minimal polynomial over $k(t_1, \dots, t_n)$, that is if and only if $x - \tau_a \theta$ is a factor of F_1. It remains to notice that this condition is stable under replacing τ by τ^{-1}. □

This theorem is not too useful for computing Galois groups since it requires factorisation of multivariate polynomials of very high degrees ($n!$ if $\deg f(x) = n$). However, it has the following extremely useful corollary.

Corollary 7. *Suppose R is a UFD (for example, $\mathbb{Z}$), P is a prime ideal in R; denote $k =$ Frac(R), and $k_P =$ Frac(R/P). Let $f(x) \in R[x]$ be a monic polynomial, and denote by $f_P(x)$ the coset of $f(x)$ in $R/P[x]$. If both $f(x)$ and $f_P(x)$ are separable, the Galois group of the splitting field K_P of $f_P(x)$ over k_P is a subgroup of the Galois group of the splitting field K of $f(x)$ over k.*

Proof. Consider the polynomial $F(x) \in K[x, t_1, \dots, t_n]$ as above. Note that since the main theorem on symmetric polynomials holds over a ring, we have $F(x) \in R[x, t_1, \dots, t_n]$. Similarly, we can form a polynomial $F_P(x, t_1, \dots, t_n)$, and in fact we can form it in two different ways, starting from $f_P(x)$, and taking the coset of F in $R/P[x, t_1, \dots, t_n]$. It is not hard to check that these two constructions coincide. Since R is a UFD, there is no difference between factorisation of polynomials with coefficients in R in the ring $R[x, t_1, \dots, t_n]$ and in the ring Frac$(R)[x, t_1, \dots, t_n]$, due to Gauss' Lemma. Note that over R/P the polynomial $F_1 \in R[x, t_1, \dots, t_n]$ may become reducible, and modulo P we deal with permutations preserving of one irreducible factor of F_P only. From the proof of Theorem 18, it is not hard to infer that a permutation preserving one irreducible factor of F preserves each of them individually, and this ensures that Gal$(K_P : k_P)$ is a subgroup of Gal$(K : k)$. □

Let us show how this result can be applied, showing that for each n there exists a polynomial with rational coefficients whose Galois group is S_n. [In fact, as proved by van der Waerden in 1930s, if we pick at random a polynomial of degree n whose coefficients do not exceed N in absolute value, the probability of it to have Galois group *different from S_n* decays at least as $\frac{C_d}{\sqrt[6]{N}}$ (for some scalar factor C_d) as $N \to \infty$.]

Proposition 27. *For each $n \geq 2$, there exists a polynomial $f(x) \in \mathbb{Z}[x]$ for which the Galois group of the splitting field over $\mathbb{Q}$ is isomorphic to S_n.*

Proof. For each prime p and each integer $n > 0$, there exists a monic irreducible polynomial over $\mathbb{F}_p$ of degree exactly n; we may, for instance, take the minimal polynomial of ξ, where ξ is the generator of the multiplicative group $\mathbb{F}_{p^n}^\times$, which exists by Proposition 8. Let us pick the following polynomials:

$$\begin{cases} f_2(x) \text{ irreducible of degree } n \text{ over } \mathbb{F}_2, \\ f_3(x) = xg(x),\ g(x) \text{ irreducible of degree } n-1 \text{ over } \mathbb{F}_3, \\ f_5(x) = (x^2+2)h(x),\ h(x) \text{ irreducible of degree } n-2 \text{ over } \mathbb{F}_5, \text{ if } n \text{ is odd}, \\ f_5(x) = x(x^2+2)h(x),\ h(x) \text{ irreducible of degree } n-3 \text{ over } \mathbb{F}_5, \text{ if } n \text{ is even}. \end{cases}$$

Now lift these to monic polynomials $u_2(x)$, $u_3(x)$, $u_5(x)$ in $\mathbb{Z}[x]$, and consider

$$f(x) = -15u_2(x) + 10u_3(x) + 6f_5(x).$$

Then $f(x)$ is monic, and is congruent to $f_i(x)$ modulo i for $i = 2, 3, 5$. Considering it modulo 2, we conclude that it is irreducible over $\mathbb{Z}$, considering it modulo 3 we see that the Galois group contains a cycle of length $(n-1)$, and finally considering it modulo 5, we see that the Galois group contains a product of a transposition and a cycle of odd length, hence contains a transposition. The result follows now from this auxiliary lemma from group theory:

Lemma 5. *Suppose that a subgroup G of S_n acts transitively on $1, 2, \ldots, n$, and contains an $(n-1)$-cycle and a transposition. Then $G = S_n$.*

Proof. Without loss of generality, the $(n-1)$-cycle is $\sigma = (123\ldots(n-1))$, and the transposition is (ij) for some $1 \leq i < j \leq n$. By transitivity, there exists $\tau \in G$ for which $\tau(j) = n$, so that $\tau(ij)\tau^{-1} = (kn)$, where $k = \tau(i)$. But $\sigma(kn)\sigma^{-1}$ is $((k+1)n)$ if $k < n-1$ and is $(1n)$ if $k = n-1$, so we can obtain all transpositions (kn), and they can be easily seen to generate S_n. □

□

6.4. **Inverse problem of Galois theory.** A very interesting question that is quite natural in the context of Galois theory is the so called *inverse problem of Galois theory*:

> For which finite groups G there exists an extension $K : \mathbb{Q}$ with the Galois group $\mathrm{Gal}(K : \mathbb{Q})$ isomorphic to G?

Interestingly enough, however hard this problem may be, if we replace $\mathbb{Q}$ by $\mathbb{C}(t)$, the answer is known to be yes, and it can be proved geometrically, with just a little bit of algebraic topology. I shall not discuss it in details in this module, mentioning only that it concerns geometry of ramified coverings of $\mathbb{CP}^1$ (complex projective line, which is geometrically the same as the two-dimensional sphere).

Let us discuss examples of realising small groups as Galois groups.

$\mathbb{Z}/2\mathbb{Z}$ for instance $\mathbb{Q}(\sqrt{2})$ would work;

$\mathbb{Z}/3\mathbb{Z}$ for instance $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ would work, as $\mathrm{Gal}(\mathbb{Q}(\zeta_7) : \mathbb{Q}) = \mathbb{Z}/6\mathbb{Z}$, and $\mathbb{Q}(\zeta_7 + \zeta_7^{-1})$ is the fixed subfield of the involution $\zeta_7 \mapsto \zeta_7^{-1}$;

$\mathbb{Z}/4\mathbb{Z}$ for instance $\mathbb{Q}(\zeta_5)$ would work;

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ for instance $\mathbb{Q}(\zeta_8)$ would work, see 9, or alternatively $\mathbb{Q}(\sqrt{2}, \sqrt{3})$;

$\mathbb{Z}/5\mathbb{Z}$ for instance $\mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$ would work, as $\mathrm{Gal}(\mathbb{Q}(\zeta_{11}) : \mathbb{Q}) = \mathbb{Z}/10\mathbb{Z}$, and $\mathbb{Q}(\zeta_{11} + \zeta_{11}^{-1})$ is the fixed subfield of the involution $\zeta_{11} \mapsto \zeta_{11}^{-1}$;

$\mathbb{Z}/6\mathbb{Z}$ for instance $\mathbb{Q}(\zeta_7)$ would work;

S_3 for instance, the splitting field of $x^3 - 2$ would work, as we saw before;

$\mathbb{Z}/7\mathbb{Z}$ we know that $\mathrm{Gal}(\mathbb{Q}(\zeta_{29}) : \mathbb{Q}) = (\mathbb{Z}/29\mathbb{Z})^\times \cong \mathbb{Z}/28\mathbb{Z}$; the group $\mathbb{Z}/28\mathbb{Z}$ has a subgroup $0, 7, 14, 21$ of order 4, and the field of invariants of this therefore has the Galois group $\mathbb{Z}/7\mathbb{Z}$;

$\mathbb{Z}/8\mathbb{Z}$ for instance $\mathbb{Q}(\zeta_{17} + \zeta_{17}^{-1})$ would work, as $\mathrm{Gal}(\mathbb{Q}(\zeta_{17}) : \mathbb{Q}) = \mathbb{Z}/16\mathbb{Z}$, and $\mathbb{Q}(\zeta_{17} + \zeta_{17}^{-1})$ is the fixed subfield of the involution $\zeta_{17} \mapsto \zeta_{17}^{-1}$;

$\mathbb{Z}/4\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$ for instance $\mathbb{Q}(\zeta_{16})$ would work, see 9;
$(\mathbb{Z}/2\mathbb{Z})^3$ for instance $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5})$ would work;
D_4 for instance, the splitting field of x^4-3 would work, as we saw before;
Q_8 is more interesting, we shall see one example now.

Proposition 28. *The Galois group of* $\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{(2+\sqrt{2})(3+\sqrt{3})})$ *is isomorphic to* Q_8.

Proof. We denote $L=\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{(2+\sqrt{2})(3+\sqrt{3})})$, $K=\mathbb{Q}(\sqrt{2},\sqrt{3})$. Let us first establish that $L\neq K$. Recall that $\mathrm{Gal}(K:\mathbb{Q})$ is $\mathbb{Z}/2\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z}$; it is generated by σ and τ for which

$$\begin{cases}\sigma(\sqrt{3})=\sqrt{3},\\ \sigma(\sqrt{2})=-\sqrt{2},\end{cases}\qquad \begin{cases}\tau(\sqrt{3})=-\sqrt{3},\\ \tau(\sqrt{2})=\sqrt{2},\end{cases}$$

Suppose that $L=K$, so that $a=\sqrt{(2+\sqrt{2})(3+\sqrt{3})}\in K$. Then $\sigma(a)$ is defined. We have

$$\sigma(a)^2=\sigma(a^2)=\sigma((2+\sqrt{2})(3+\sqrt{3}))=(2-\sqrt{2})(3+\sqrt{3})=\frac{2-\sqrt{2}}{2+\sqrt{2}}a^2=\frac{\sqrt{2}-1}{\sqrt{2}+1}a^2=(\sqrt{2}-1)^2a^2,$$

so $\sigma(a)=\pm(\sqrt{2}-1)a$, and $\sigma^2(a)=\sigma(\pm(\sqrt{2}-1)a)=(-\sqrt{2}-1)(\sqrt{2}-1)a=-a$. However $\sigma^2=\mathrm{id}$, so $a=-a$, $a=0$, a contradiction. Thus $L\neq K$, and since clearly $[L:K]\leq 2$, we have $[L:K]=2$ and $[L:\mathbb{Q}]=8$.

Let σ' be an extension of σ to an automorphism of L. By the same argument, we have $\sigma'(a)=\pm(\sqrt{2}-1)a$, $\sigma^2(a)=-a$, and $\sigma^4(a)=a$, so $\sigma^4(a)=\mathrm{id}$. We also note that if $\sigma'(a)=-(\sqrt{2}-1)a$, then $(\sigma')^3(a)=(\sqrt{2}-1)a$, so without loss of generality, $\sigma'(a)=(\sqrt{2}-1)a$.

Consider also some extension τ' of τ to an automorphism of L. We have

$$\tau'(a)^2=\tau'(a^2)=\tau'((2+\sqrt{2})(3+\sqrt{3}))=(2+\sqrt{2})(3-\sqrt{3})=\frac{\sqrt{3}-1}{\sqrt{3}+1}a^2=(\frac{\sqrt{3}-1}{\sqrt{2}})^2a^2,$$

so $\tau'(a)=\pm\frac{\sqrt{3}-1}{\sqrt{2}}a$, and $(\tau')^2(a)=\tau'(\pm\frac{\sqrt{3}-1}{\sqrt{2}}a)=\frac{\sqrt{3}-1}{\sqrt{2}}\frac{-\sqrt{3}-1}{\sqrt{2}}a=-a$. Again, without loss of generality, $\tau'(a)=\frac{\sqrt{3}-1}{\sqrt{2}}a$. Note that $\sigma'\tau'(a)=\sigma'(\frac{\sqrt{3}-1}{\sqrt{2}}a)=\frac{\sqrt{3}-1}{-\sqrt{2}}(\sqrt{2}-1)a$, and $\tau'\sigma'(a)=\tau'((\sqrt{2}-1)a)=(\sqrt{2}-1)\frac{\sqrt{3}-1}{\sqrt{2}}a$, so $\tau'\sigma'(a)\neq\sigma'\tau'(a)$. We conclude that the Galois group of L over $\mathbb{Q}$ is not Abelian. Of the two non-Abelian groups of order 8, D_4 is ruled out because we have four distinct elements $\sigma',\tau',(\sigma')^3,(\tau')^3$ of order 4. Thus, the group in question is Q_8. □

The list of realisations above suggests that Abelian Galois groups tend to appear in the context of cyclotomic fields. That is quite easy to establish using Proposition 9 and a fundamental result of Dirichlet stating that every arithmetic series $an+b$ with $\gcd(a,b)=1$ contains a prime. A much more interesting result is the famous Kronecker–Weber theorem: every Galois extension of $\mathbb{Q}$ with an Abelian Galois group is a subfield of some cyclotomic field! It is also known (Shafarevich, 1954) that every solvable group appears as a Galois group over $\mathbb{Q}$.

Let us conclude with mentioning a very peculiar result of Serre (1992): if all finite groups appear as Galois groups of extensions of $\mathbb{Q}$, then they already appear as Galois groups of *real* extensions of $\mathbb{Q}$ (i.e. those that are subfields of $\mathbb{R}$).

Exercises for Chapter 6

Exercise 25.

(i) Explain why for every extension $K\subset L$ of finite fields the primitive element theorem holds.
(ii) Find a normal basis for the field extensions $\mathbb{F}_2\subset\mathbb{F}_{2^k}$ for $k=2,3,4$.

Exercise 26.

(i) Let k be a field of characteristic p, $K=k(x,y)$ the field of rational functions in two variables, and $L=K(\sqrt[p]{x},\sqrt[p]{y})$. Show that the extension $K\subset L$ does not have a primitive element.

(ii) Let k be an infinite field of characteristic p, $K = k(x, y)$ the field of rational functions in two variables, and $L = K(\sqrt[p]{x}, \sqrt[p]{y})$. Show that there are infinitely many intermediate fields between K and L.

Exercise 27. Find a normal basis of $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbb{Q}$, and a normal basis of the splitting field of $x^4 - 2$ over $\mathbb{Q}$.

Exercise 28. For which values of $n < 16$ do the primitive n-th roots of unity form a normal basis of the splitting field of $x^n - 1$ over $\mathbb{Q}$?

Exercise 29.

(i) Considering $x^5 - x - 1$ over $\mathbb{F}_2$ and over $\mathbb{F}_5$, establish that the Galois group of the splitting field of $x^5 - x - 1$ over $\mathbb{Q}$ is $\mathbb{S}_5$.

(ii) Let p be a prime number. Show that for large N the polynomial

$$x^p - N^3 p^3 x(x-1)\cdots(x-(p-4)) - p$$

has $p - 2$ real roots. Use it to deduce that for such values of N the Galois group of the splitting field of this polynomial over $\mathbb{Q}$ is S_p.

Exercise 30. Show that there exist some complex numbers roots of unity $\xi_1, \dots, \xi_s$, and some rational numbers $a_1, \dots, a_s$, so that the number $\alpha = a_1\xi_1 + \cdots + a_s\xi_s$ satisfies $\mathrm{Gal}(\mathbb{Q}(\alpha) : \mathbb{Q}) \cong \mathbb{Z}/720\mathbb{Z}$.

References

[1] Galois theory section in the list of expository notes of Keith Conrad http://www.math.uconn.edu/~kconrad/blurbs/.

[2] Online lecture notes of J.S.Milne, http://www.jmilne.org/math/CourseNotes/ft.html.

[3] Online lecture notes of Miles Reid, http://homepages.warwick.ac.uk/~masda/MA3D5/.