GALOIS THEORY

1. Introduction

Galois theory grows out of attempts to solve polynomial equations. Let's have a brief history of this important problem.

(1) **Quadratic equations.** Recall how one solves the quadratic equation

$$x^2 + bx + c = 0.$$

We 'complete the square':

$$(x + \frac{b}{2})^2 + c - \frac{b^2}{4} = 0,$$

and solve for x:

$$x = -\frac{b}{2} + \sqrt{\frac{b^2}{4} - c}.$$

This was known to the Babylonians (2000 - 1600 BC, algorithmic), to Euclid (300BC, geometric), and to Brahmagupta (6th century AD, allowing negative quantities, using letters for unknowns).

(2) **Cubic equations.** We next consider a cubic equation

$$x^3 + bx^2 + cx + d = 0.$$

This was first solved (at least in special cases) by del Ferro in 1515. He kept his methods secret for 11 years before passing his knowledge to his student Fior. By 1535 Tartaglia had a 'general' solution, and defeated Fior in public competition. Cardano convinced Tartaglia to divulge his solution, and breaking an oath of secrecy, published it in his volume *Ars Magna*.

The general equation above can be reduced to the case $y^3 + my = n$ (why?). Then Cardano's formula is

$$y = \sqrt[3]{\sqrt{\frac{n^2}{4} + \frac{m^3}{27}} + \frac{n}{2}} - \sqrt[3]{\sqrt{\frac{n^2}{4} + \frac{m^3}{27}} - \frac{n}{2}}.$$

Remarkably, negative numbers were not understood at the time; the formula 'makes sense' when m and n are nonnegative.

(3) **Quartic equations.** These were solved by Cardano's student Ferrari.

(4) **Quintic equations.** Abel proved in 1824 that there is no general formula for x satisfying the equation

$$x^5 + bx^4 + cx^3 + dx^2 + ex + f = 0$$

in terms of b, c, d, e, f combined using $+, -, \times, \div, \sqrt[n]{}$.

Galois (1811-1831) was the pioneer in this field. He showed that solutions of a polynomial equation are governed by a group. To illustrate this, let us consider the polynomial

$$x^4 = 2.$$

One solution is the positive real fourth root $\alpha = \sqrt[4]{2}$ of 2. The other three are then $\beta = i \cdot \sqrt[4]{2}$, $\gamma = -\sqrt[4]{2}$, and $\delta = -i \cdot \sqrt[4]{2}$. Let us list some equations that these four roots satisfy:

$$\alpha + \gamma = 0, \quad \alpha\beta\gamma\delta = -2, \quad \alpha\beta - \gamma\delta = 0, \quad \ldots.$$

What happens if we swap α and γ in this list? We get

$$\gamma + \alpha = 0, \quad \gamma\beta\alpha\delta = -2, \quad \gamma\beta - \alpha\delta = 0, \quad \ldots,$$

which are all still valid equations. If we perform the permutation $\alpha \mapsto \beta \mapsto \gamma \mapsto \delta \mapsto \alpha$ to the original list, we obtain

$$\beta + \delta = 0, \quad \beta\gamma\delta\alpha = -2, \quad \beta\gamma - \delta\alpha = 0, \quad \ldots,$$

which again are all true. We begin to get the impression that anything goes. But swapping α and β in the original list gives

$$\beta + \gamma = 0, \quad \beta\alpha\gamma\delta = -2, \quad \beta\alpha - \gamma\delta = 0, \quad \ldots,$$

and the first of these equations is false.

The set of permutations of the solutions $\alpha, \beta, \gamma, \delta$ which preserve the validity of all polynomial equations forms a group, the *Galois group* of the equation $x^4 = 2$. It turns out that this group is isomorphic to the symmetric group of the square (which one can see by identifying successive vertices of a square with the roots $\alpha, \beta, \gamma, \delta$).

To deal with $\alpha, \beta, \gamma, \delta$ it is natural to work in $\mathbb{C}$. Better yet, and more efficient is to use just the subset of $\mathbb{C}$ we get by performing arithmetic to these four numbers. This subset forms a 'field extending $\mathbb{Q}$ '. Galois theory brings together the study of polynomials equations, the abstract study of fields and field extensions, and group theory.

2. Background.

2.1. **Rings.** A *commutative ring with* 1 is a set R equipped with two binary operations, $+$ (called addition) and $\cdot$ (called multiplication), such that

- $(R, +)$ is an abelian group [write 0 for the additive identity],
- $(R, \cdot)$ is associative and commutative, and there exists $1 \in R$ such that $1 \cdot a = a = a \cdot 1$ for all $a \in A$ (a multiplicative identity),
- the distributive law
$$a \cdot (b + c) = a \cdot b + a \cdot c$$
holds for $a, b, c \in R$.
- $0 \neq 1$

Write ab for $a \cdot b$.

In this course *ring* means *commutative ring with* 1.

An *integral domain* is a ring in which $ab = 0$ implies that $a = 0$ or $b = 0$.

A *field* is a ring F in which every nonzero element $b \in F$ has a multiplicative inverse b^{-1}. The set $F^\times$ of nonzero elements of F form a group, called the *multiplicative group* of F. It is customary to write a/b or $\frac{a}{b}$ instead of ab^{-1}.

Exercise 1. *Show that any field is an integral domain.*

Example 2. $\mathbf{Z}$ *is an integral domain;* $\mathbf{Q}, \mathbf{R}, \mathbf{C}$ *are fields.*

A *subring* of a ring R is a subset containing 1 closed under $+, \cdot$ and $-$. A *subfield* of a field is a subring whose nonzero elements are closed under $^{-1}$. An *ideal* in a ring R is an additive subgroup I of R such that $1 \notin I$ and such that if $i \in I$ and $r \in R$ then $ri \in I$.

If I is and ideal in a ring R we can form the quotient ring R/I, whose elements $r + I$ are cosets of I in R (as an additive group) and with $+$ and $\cdot$ defined as follows:

$$(r + I) + (s + I) = (r + s) + I,$$
$$(r + I)(s + I) = rs + I.$$

A important example: The ideal $n\mathbf{Z}$ of multiples of n in $\mathbf{Z}$. The quotient ring $\mathbf{Z}_n = \mathbf{Z}/n\mathbf{Z}$ is the ring of integers modulo n.

Lemma 3. $\mathbf{Z}_n$ *is a field if and only if* n *is a prime number.*

Proof. Suppose $n = kl$ where k, l are positive integers less than n. Then in $\mathbf{Z}_n$,

$$(k + n\mathbf{Z})(l + n\mathbf{Z}) = kl + n\mathbf{Z} = n\mathbf{Z},$$

so $\mathbf{Z}_n$ is not an integral domain and hence not a field.

If p is prime and k is an integer not divisible by p, then there exist integers a and b such that $ap + bk = 1$. Thus

$$(b + p\mathbf{Z})(k + p\mathbf{Z}) = (bk + p\mathbf{Z}) = 1 + p\mathbf{Z},$$

so $k + p\mathbf{Z}$ is invertible in $\mathbf{Z}_p$. □

The elements of $\mathbf{Z}_n$ will be denoted by $0, 1, \ldots, n-1$ or $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ instead of the cumbersome $n\mathbf{Z}, 1 + n\mathbf{Z}, \ldots, (n-1) + n\mathbf{Z}$.

If R and S are rings, then a *homomorphism* from R into S is a map $\phi : R \longrightarrow S$ such that $\phi(1) = 1$, and such that for all $r_1, r_2 \in R$ we have $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$ and $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$. If ϕ is injective, surjective, or bijective it is called a *monomorphism*, *epimorphism*, or *isomorphism*, respectively.

$\mathrm{Im}(\phi)$ is a subring of S and $\ker(\phi)$ is an ideal in R, and

$$\overline{\phi} : \frac{R}{\ker(\phi)} \longrightarrow \mathrm{Im}(\phi)$$

defined by $\overline{\phi}(r + \ker(\phi)) = \phi(r)$ is an isomorphism of rings.

2.2. **Prime subfields.** Let K be a field. The intersection of all subfields of K is a subfield, called the *prime subfield* of K.

Note that $\mathbf{Q}$ and $\mathbf{Z}_p$ (where p is prime) are their own prime subfields. The following basic fact is left as an exercise.

Proposition 4. *The prime subfield of any field K is isomorphic to either $\mathbf{Z}_p$ for some prime p (in which case we say K has characteristic p) or to $\mathbf{Q}$ (in which case we say K has characteristic 0).*

2.3. **Fields of fractions.** The rational numbers can be constructed from the integers by forming fractions. We try to generalise this procedure as follows.

Let R be a ring. We consider the set Ω of pairs (r, s) of elements of R, with $s \neq 0$. (Think of these as fractions r/s.) We define an equivalence relation on Ω as follows: $(r, s) \sim (t, u)$ if and only if $ru = st$. It is easy to verify that this is an equivalence relation. Denote the equivalence class of (r, s) by $[r, s]$. The set F of equivalence classes is the *field of fractions* of R. Addition and multiplication are defined as follows:

$$[r, s] + [t, u] = [ru + st, su]$$
$$[r, s][t, u] = [rt, su].$$

Note that in order for this to make sense we must assume that R is an integral domain!

We need to check that these operations are well-defined. For example, suppose $(r, s) \sim (r', s')$. Then we want

$$(ru + st, su) \sim (r'u + s't, s'u).$$

Indeed,

$$\begin{aligned}(ru + st)s'u &= rus'u + sts'u \\ &= r'usu + s'tsu \\ &= (r'u + s't)su.\end{aligned}$$

The fact that every nonzero element of F has a multiplicative inverse is left as an easy exercise.

We may identify R with the subring of F consisting of elements of the form $[r, 1]$, i.e. we have a natural monomorphism $i : R \longrightarrow F$ taking r to $[r, 1]$.

Exercise 5. *Show that if K is any field and $\phi : R \to K$ is a monomorphism then ϕ extends uniquely to F, i.e. there is a unique homomorphism $\widetilde{\phi} : F \longrightarrow K$ such that $\phi = \widetilde{\phi} \circ i$.*

2.4. **Polynomial rings.** Let R be a ring. A *polynomial over R in the indeterminate t* is an expression

$$a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0 \tag{1}$$

where $0 \leq n \in Z$ and $a_0, \ldots, a_n \in R$. We call a_i the coefficient of t^i (if i is greater than n, the coefficient of t^i is 0).

Given two polynomials

$$\sum a_i t^i$$

and

$$\sum b_i t^i$$

we define their sum to be

$$\sum (a_i + b_i) t^i$$

and their product to be

$$\sum c_i t^i$$

where

$$c_i = \sum_{i=j+k} a_j b_k.$$

With this addition and multiplication, the set of polynomials over R in the indeterminate t is a ring, which we denote by $R[t]$ and call *the ring of polynomials over R in the indeterminate t.*

Example 6. *Let $R = \mathbf{Z}$. If $f = 3t+4$ and $g = t^2+t-2$ then $f+g = t^2+4t+2$ and $fg = 3t^3+7t^2-2t-8$.*

Any nonzero polynomial f can be written in the form (1) with $a_n \neq 0$. Then we say f has *degree* n (writing $\delta f = n$), and has *leading coefficient* a_n. The degree of the zero polynomial is taken to be $-\infty$, for convenience's sake.

We say that f is *monic* if its leading coefficient is 1.

Any element $a \in R$ can be thought of as polynomial $\ldots + 0t^2 + 0t + a$. This defines a ring monomorphism $R \longrightarrow R[t]$. The image consists of *constant polynomials* or *constants.*

If $f \in R[t]$ is as in (1) and $\alpha \in R$, then the *evaluation of f at α* is

$$f(\alpha) = a_n\alpha^n + a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 \in R.$$

For each fixed $\alpha \in R$ we have an *evaluation homomorphism*

$$\begin{aligned} R[t] &\longrightarrow R \\ f &\mapsto f(\alpha). \end{aligned}$$

Lemma 7. *Suppose R is an integral domain. Then so is $R[t]$.*

Proof. If f and g are nonzero polynomials with leading coefficients a and b respectively, then their product fg has leading coefficient $ab \neq 0$, and is hence nonzero. □

As $R[t]$ is an integral domain we can consider its field of fractions, which we denote by $R(t)$. Every element of this field, which is called the *field of rational functions over R in the indeterminate t*, is expressible as the quotient of polynomials.

If $\phi : R \longrightarrow S$ is a homomorphism of rings we get an induced map $R[t] \longrightarrow S[t]$ by 'applying ϕ to coefficients'. This is clearly a ring homomorphism; we will often abuse notation and call it ϕ as well.

2.5. **Polynomial rings over fields.** Throughout this section we fix a field K. In many ways $K[t]$ behaves like the ring of integers $\mathbf{Z}$.

Proposition 8. *(Division Algorithm for polynomials over a field.) Let f and g be polynomials over K, and suppose f is nonzero. Then there exist unique polynomials q and r over K such that*

$$g = qf + r$$

and $\delta r < \delta f$.

Proof. Induct on the δg. If $\delta g < \delta f$ then $g = 0f + g$ and we are done.

So assume

$$f = a_m t^m + \cdots + a_0$$

and

$$g = b_n t^n + \cdots + b_0$$

with a_m and b_n both nonzero and $m \leq n$.

Set

$$g_1 = g - b_n a_m^{-1} t^{n-m} f.$$

Then $\delta g_1 < \delta g$, so by induction

$$g_1 = q_1 f + r_1,$$

where $\delta r_1 < \delta f$. Then

$$\begin{aligned} g &= g_1 + b_n a_m^{-1} t^{n-m} f \\ &= (q_1 + b_n a_m^{-1} t^{n-m}) f + r_1, \end{aligned}$$

as desired.

Now we prove the uniqueness. Suppose we also have

$$g = q' f + r',$$

where $\delta r' < \delta f$. Then

$$(q - q')f = r - r'.$$

If the LHS is nonzero, then it has degree at least δf, whereas the RHS has degree less than δf. Hence both sides are 0, and therefore $q = q'$ and $r = r'$. □

Definition 9. *Let f and g be polynomials over K. We say that f* divides *g (and write $f|g$, if there is a polynomial h over K such that $g = fh$. If f does not divide g we write $f \nmid g$. A polynomial d is a* highest common factor (hcf) *of f and g if $d|f$ and $d|g$ and furthermore if $e|f$ and $e|g$ implies that $e|d$. We say f and g are* relatively prime *if 1 is a hcf of f and g.*

Exercise 10. *If d is a highest common factor of f and g, then so is λd, for any nonzero $\lambda \in K$. Conversely if d and d' are both highest common factors of f and g, then $d = \lambda d'$ for some nonzero $\lambda \in K$.*

In order to show that hcf's exist, we use an analogue of the Euclidean algorithm. We start with two nonzero polynomials f and g. We set $f = r_{-1}$ and $g = r_0$ and use the division algorithm repeatedly:

$$\begin{array}{ll} r_{-1} = q_1 r_0 + r_1 & \delta r_1 < \delta r_0 \\ r_0 = q_2 r_1 + r_2 & \delta r_2 < \delta r_1 \\ \cdots & \cdots \\ r_i = q_{i+2} r_{i+1} + r_{i+2} & \delta r_{i+2} < \delta r_{i+1} \\ \cdots & \end{array}$$

The degrees of the r_i's are strictly decreasing, so for some s we get

$$r_s = q_{s+2} r_{s+1}.$$

Now note that among r_i and r_{i+1} and r_{i+2}, a polynomial dividing any two of r_i, r_{i+1} and r_{i+2}, must divide the third. Because r_{s+1} divides r_s, we have that r_{s+1} is a hcf of r_s and r_{s+1},which is a hcf of r_{s-1} and r_s, etc. By induction r_{s+1} is a hcf of f and g.

Proposition 11. *Let h be a hcf of $f, g \in K[t]$. Then there exists polynomials a and b such that*

$$h = af + bg.$$

Proof. We argue by induction on s in the Euclidean algorithm. This statement is certainly true for $s = -1$, for $r_0 = 0 \cdot r_{-1} + 1 \cdot r_0$. For $s \geq 0$, Euclidean algorithm applied to r_0 and r_1 has length $s - 1$, and produces the same hcf so there exist a' and b' such that

$$h = a' r_0 + b' r_1.$$

Therefore

$$\begin{aligned} h &= a' r_0 + b'(r_{-1} - q_1 r_0) \\ &= b' r_{-1} + (a' - b' q_1) r_0, \end{aligned}$$

as desired. □

Definition 12. *An irreducible polynomial over a ring R is a nonconstant polynomial which cannot be written as the product of two polynomials of smaller degree.*

Example 13. *All polynomials of degree 1 are irreducible. The polynomial $t^2 - 2$ is irreducible over $\mathbf{Q}$ but reducible over $\mathbf{R}$.*

Clearly any nonconstant polynomial $f \in R[t]$ is expressible as the product of irreducible polynomials. One can see this by induction on the degree. Also, if f is monic, we can express it as a product of monic irreducibles.

We return our attention to the case where $R = K$ is a field.

Lemma 14. *Suppose $f, g, h \in K[t]$ and f is irreducible. If $f|gh$ then either $f|g$ or $f|h$.*

Proof. A hcf of f and g is a polynomial dividing f, so must be either λ or λf (where $\lambda \in K^\times$). If the latter holds, $f|g$. Otherwise f and g are relatively prime so by Lemma 11 there exist polynomials a and b such that

$$af + bg = 1.$$

Then

$$\begin{aligned} h &= h(af + bg) \\ &= haf + hbg. \end{aligned}$$

Certainly $f|haf$ and $f|hbg$ because $f|hg$. Thus $f|h$.

Theorem 15. *Every $f \in K[t]$ with $\delta f \geq 1$ can be written as a product of irreducible polynomials, unique up to order and multiplication by constants. If f is monic, it is a product of monic irreducible polynomials, unique up to order.*

□

Proof. Suppose $f = g_1 \cdots g_r = h_1 \cdots h_s$, where all factors are irreducible. We have $g_1|h_1 \cdots h_s$, so by an inductive argument based on Lemma 14, g_1 divides one of the h_i. By reordering the h's we may assume that $g_1|h_1$, and as h_1 and g_1 are irreducible we must have $h_1 = \lambda_1 g_1$, where $\lambda_1 \in K^\times$. So $\lambda_1 g_1 h_2 \cdots h_s = g_1 g_2 \cdots g_r$. Now $g_1(g_2 \cdots g_r - \lambda_1 h_2 \cdots h_s) = g_1 \cdots g_r - h_1 \cdots h_s = 0$, and as $g_1 \neq 0$ and $K[t]$ is an integral domain (by Lemma 7), this implies that $g_2 \cdots g_r = \lambda_1 h_2 \cdots h_s$.

Using the same argument, we obtain, after reordering the h's, $h_2 = \lambda_2 g_2, \ldots, h = \lambda_r g_r$, for some $\lambda_2, \ldots, \lambda_r \in K^\times$, and $1 = \lambda_1 \cdots \lambda_r h_{r+1} \cdots h_s$. This forces $r = s$ and we are done.

If each of the g's and h's are monic then each of the λ's must be 1. □

How does one test whether or not a polynomial f is irreducible? The most basic question is whether or not f has any linear factors.

Definition 16. *Let R be a ring. We say that $\alpha \in R$ is a zero or root of $f \in R[t]$ if $f(\alpha) = 0$.*

Lemma 17. *Suppose $\alpha \in K$ and $f \in K[t]$. Then $f(\alpha) = 0$ if and only if $(t - \alpha)|f$.*

Proof. If $f = (t - \alpha)g$ for some $g \in K[t]$, then $f(\alpha) = (\alpha - \alpha)g(\alpha) = 0$.

Suppose conversely that $f(\alpha) = 0$. By the division algorithm (8), there exist $q, r \in K[t]$ such that $f = q(t - \alpha) + r$, where r is a constant. Then $0 = f(\alpha) = q(\alpha)(\alpha - \alpha) + r = r$. Hence $(t - \alpha)|f$. □

Example 18. *Let $f \in K[t]$ be a a polynomial of degree $\delta f \leq 3$. Then f is irreducible if and only if $f(\alpha) \neq 0$ for all $\alpha \in K$. For example $f = t^3 + t^2 + 2 \in \mathbf{Z}_3[t]$ is irreducible because $f(0) = 2$, $f(1) = 1$, $f(2) = 2$.*

2.6. **Irreducibility over the rational field.** Here the main interest is polynomials over $\mathbf{Q}$. We begin with a theorem relating irreducibility over $\mathbf{Q}$ to irreducibility over $\mathbf{Z}$.

Proposition 19. *(Gauss's Lemma) Any irreducible polynomial over $\mathbf{Z}$ remains irreducible over $\mathbf{Q}$.*

Proof. Suppose that f is a polynomial over $\mathbf{Z}$ which is the product of two polynomials g and h over $\mathbf{Q}$, of strictly smaller degree. We want to show that f is not irreducible over $\mathbf{Z}$. By multiplying through by denominators of all the coefficients of g and h, we get

$$nf = g'h'.$$

for some $n \in \mathbf{Z}$ and some $g', h' \in \mathbf{Z}[t]$, with $\delta g' = \delta g$ and $\delta h' = \delta h$. If $n = 1$ we are done. Otherwise we try to 'get rid of' prime factors of n one by one. So suppose p is a prime factor of n.

We claim that if

$$g' = a_r t^r + \cdots + a_1 t + a_0,$$
$$h' = b_s t^s + \cdots + b_1 t + b_0,$$

then either p divides all the a's or p divides all the b's. If not then choose i and j smallest such that $p \nmid a_i$ and $p \nmid b_j$. Now because $nf = g'h'$, p divides all the coefficients in $g'h'$, in particular the coefficient of t^{i+j}, which is

$$a_0 b_{i+j} + \cdots + a_{i+j} b_0.$$

But in this sum each term is divisible by p except for $a_i b_j$, and this yields a contradiction.

So without loss of generality assume that $p|a_i$ for all i. Then $g' = pg''$ where $g'' \in \mathbf{Z}[t]$ and $\delta g'' = \delta g'$, and

$$(n/p)f = g''h'.$$

Continuing this way we eventually get $f = \tilde{g}\tilde{h}$ with $\tilde{g}, \tilde{h} \in \mathbf{Z}[t]$, and $\delta\tilde{g} = \delta g$ and $\delta\tilde{h} = \delta h$. This shows that f is not irreducible over $\mathbf{Z}$, as desired. □

Having reduced the problem of irreducibility over $\mathbf{Q}$ to irreducibility over $\mathbf{Z}$, we now want techniques to identify polynomials irreducible over $\mathbf{Z}$. Here is one.

Theorem 20. *(Eisenstein's criterion) Suppose $f = a_n t^n + \cdots + a_0 \in \mathbf{Z}[t]$ and there is a prime number p for which the following hold:*

$$p \nmid a_n$$
$$p|a_i \ (i = 0, \ldots, n-1)$$
$$p^2 \nmid a_0.$$

Then f is irreducible over $\mathbf{Z}$ (and therefore over $\mathbf{Q}$, by (19)).

Proof. Suppose that $f = gh$ where

$$g = b_r t^r + \cdots + b_0 \in \mathbf{Z}[t],$$
$$h = c_s t^s + \cdots + c_0 \in \mathbf{Z}[t],$$

with $\delta g < \delta f$ and $\delta h < \delta f$. Note that $b_r c_s = a_n$, so neither b_r or c_s is divisible by p. Choose i smallest such that $p \nmid b_i$. We have $a_i = b_i c_0 + \cdots + b_0 c_i$ where $i < n$. By assumption p divides $a_i, b_0, \ldots, b_{i-1}$ but not b_i, so $p|c_0$. A similar argument leads to $p|b_0$, and therefore p^2 divides $b_0 c_0 = a_0$, contradicting the assumptions in the statement of the theorem. □

Example 21. (1) *The polynomial $f = \frac{2}{9}t^5 + \frac{5}{3}t^4 + t^3 + \frac{1}{3}$ is irreducible over $\mathbf{Q}$ if and only if $9f = 2t^5 + 15t^4 + 9t^3 + 3$ is irreducible over $\mathbf{Q}$, and this is the case, by Eisenstein's criterion for $p = 3$.*

(2) *The polynomial $f = t^3 + t^2 - 5t + 1$ is irreducible over $\mathbf{Q}$ if and only if $g = (t+1)^3 + (t+1)^2 - 5(t+1) + 1 = t^3 + 4t^2 - 2$ is irreducible over $\mathbf{Q}$. This is true by Eisenstein's criterion for $p = 2$.*

We now introduce the idea of *reduction* modulo a prime number p. The natural quotient homomorphism

$$\_ : \mathbf{Z} \longrightarrow \mathbf{Z}_p : n \longmapsto \overline{n} = n + p\mathbf{Z}$$

extends uniquely to a ring homomorphism

$$\_ : \mathbf{Z}[t] \longrightarrow \mathbf{Z}_p[t] : f \longmapsto \overline{f},$$

in which

$$f = a_r t^r + \cdots + a_1 t + a_0$$

is mapped to

$$\overline{f} = \overline{a_r} t^r + \cdots + \overline{a_1} t + \overline{a_0}.$$

This can be exploited as follows.

Lemma 22. *Suppose f is a polynomial over $\mathbf{Z}$ whose leading coefficient is not divisible by p and such that $\overline{f} \in \mathbf{Z}_p[t]$ is irreducible. Then f is irreducible over $\mathbf{Q}$ (and therefore over $\mathbf{Z}$, by Proposition 19).*

Proof. Suppose $f = gh$ where $g, h \in \mathbf{Z}[t]$, $\delta g < \delta f$, and $\delta h < \delta f$. Then $\overline{f} = \overline{g}\overline{h}$, and $\delta\overline{g} \leq \delta g < \delta f = \delta\overline{f}$ and similarly $\delta\overline{h} < \delta\overline{f}$. This contradicts the irreducibility of $\overline{f}$. □

Example 23. *Consider $f = t^4 + 15t^3 + 7$ over $\mathbf{Z}$. Over $\mathbf{Z}_5$ we get $\overline{f} = t^4 + 2$. This has no zeroes in $\mathbf{Z}_5$, so by Lemma 17 $\overline{f}$ has no linear factors. So if $\overline{f}$ is not irreducible then*

$$t^4 + 2 = (t^2 + at + b)(t^2 + ct + d),$$

with $a, b, c, d \in \mathbf{Z}_5$. Comparing coefficients on both sides, we get $a + c = 0$, $ac + b + d = 0$, and $bd = 2$. Then $b + d = a^2$ and therefore $b(a^2 - b) = 2$. Well, $a^2 = 0$, 1, or 4, and $b = 0$, 1, 2, 3, or 4. None of these possibilities work.

Thus $\overline{f}$ is irreducible over Z_5 and therefore, by Lemma 22, f is irreducible over $\mathbf{Z}$ and therefore over $\mathbf{Q}$.

Note that over $\mathbf{Z}_3$ we get $t^4 + 1$ which factors $(t^2 + t - 1)(t^2 - t - 1)$, so one may need to choose the prime p carefully.

3. Field extensions

Definition 24. *A field extension is a homomorphism $i : K \longrightarrow L$ of a field K into a field L.*

The homomorphism i is a monomorphism because of the following.

Exercise 25. *If $\phi : K \longrightarrow R$ is a homomorphism of a field K into a ring R, then ϕ is a monomorphism.*

So $i(K)$ is a subfield of L isomorphic to K. We often identify K with $i(K)$ in L, and write

$$K \subset L, \quad L \supset K, \quad L/K, \quad \text{or} \quad L : K.$$

The 3rd is perhaps the most widespread notation, but has the disadvantage of looking like a quotient object.

Example 26. (1) $i : \mathbf{Q} \longrightarrow \mathbf{R}$, $i : \mathbf{R} \longrightarrow \mathbf{C}$, $i : \mathbf{Q} \longrightarrow \mathbf{C}$.
(2) $i : \mathbf{Q} \longrightarrow \{a + b\sqrt{3} \mid a, b \in \mathbf{Q}\} \subset \mathbf{R}$.
(3) *Let K be a field. Composing the natural homomorphisms $K \longrightarrow K[t]$ and $K[t] \longrightarrow K(t)$ we obtain an extension $i : K \longrightarrow K(t)$.*

Definition 27. *If $L \supset K$ is a field extension, and A is a subset of L, we write $K(A)$ for the intersection of all subfields of L containing K and A. We say that $K(A)$ is the field obtained by* adjoining *A to K. If $A = \{\alpha_1, \ldots, \alpha_n\}$, write $K(\alpha_1, \ldots, \alpha_n)$ for $K(A)$.*

It's easy to see that $K(A)$ consists of all elements of L which can be obtained by performing a finite number of successive field operations on the set $K \cup A$.

Example 28. (1) *If $L \supset K$ and $A \subset K$ then $K(A) = K$.*
(2) *Consider $\mathbf{R} \supset \mathbf{Q}$ and $A = \{2 + \sqrt{3}, 2 - \sqrt{3}\}$. It's easy to see that $\mathbf{Q}(A) = \{a + b\sqrt{3} \mid a, b \in \mathbf{Q}\} \subset \mathbf{R}$.*
(3) *Consider $\mathbf{C} \supset \mathbf{R}$. We have $\mathbf{R}(i) = \{a + bi \mid a, b \in \mathbf{R}\} = \mathbf{C}$.*
(4) *Consider $K(t) \supset K$, where K is any field and $K(t)$ is the field of rational functions over K, and let $A = \{t\} \subset K$. There is a potential notational confusion here, but luckily the intersection of all fields containing K and A is all of $K(t)$.*

Definition 29. *The extension $K \subset L$ is a* simple extension *if $L = K(\alpha)$ for some $\alpha \in L$.*

Note that in this definition the α realizing a simple extension may not be unique. For example we have $\mathbf{Q}(\sqrt{3}) = \mathbf{Q}(2 + \sqrt{3}) = \mathbf{Q}(2 - \sqrt{3})$.

Some simple extensions are not self-evidently simple. Consider the extensions $\mathbf{R} \supset \mathbf{Q}(\sqrt{2}, \sqrt{3}) \supset \mathbf{Q}$ and let $\alpha = \sqrt{2} + \sqrt{3} \in \mathbf{R}$. Since $\alpha \in \mathbf{Q}(\sqrt{2}, \sqrt{3})$ we clearly have $\mathbf{Q}(\alpha) \subset \mathbf{Q}(\sqrt{2}, \sqrt{3})$. On the other hand the field $\mathbf{Q}(\alpha)$ contains $(\alpha^2 - 5)/2 = \sqrt{6}$, $\sqrt{6}\alpha = 2\sqrt{3} + 3\sqrt{2}$, $(2\sqrt{3} + 3\sqrt{2}) - 2\alpha = \sqrt{2}$, and $\alpha - \sqrt{2} = \sqrt{3}$, and therefore $\mathbf{Q}(\alpha) \supset \mathbf{Q}(\sqrt{2}, \sqrt{3})$. So $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\alpha)$ is a simple extension of $\mathbf{Q}$.

Definition 30. *Let $K \subset L$ be a field extension, and let $\alpha \in L$. Then α is* algebraic *over K if it is a zero of some nonzero $f \in K[t]$. Otherwise it is* transcendental *over K.*

Example 31. (1) *$2 + \sqrt{3} \in \mathbf{R}$ is algebraic over $\mathbf{Q}$ because $f(2 + \sqrt{3}) = 0$ when $f = t^2 - 4t + 1 \in \mathbf{Q}[t]$.*
(2) *$e, \pi \in \mathbf{R}$ are transcendental over $\mathbf{Q}$.*

(3) $t \in K(t)$ *is transcendental over* K.

Theorem 32. *Suppose* $\alpha \in L \supset K$ *is algebraic over* K. *Then there is a unique nonzero monic polynomial* $m \in K[t]$ *of smallest degree such that* $m(\alpha) = 0$, *called the* minimal polynomial *of* α *over* K. *It is irreducible and it divides any* $g \in K[t]$ *satisfying* $g(\alpha) = 0$.

Proof. Let $m \in K[t]$ be a nonzero polynomial of smallest degree such that $m(\alpha) = 0$. By scaling by an element of $K^\times$, we may assume m is monic. If $m = gh$, where $g, h \in K[t]$, then $0 = g(\alpha)h(\alpha) = m(\alpha) = 0$ which implies that $g(\alpha) = 0$ or $h(\alpha) = 0$. Thus m is an irreducible polynomial. Now if $m' \in K[t]$ is another monic polynomial with $m'(\alpha) = 0$ and $\delta m' = \delta m$, then $\delta(m-m') < \delta m$ while $(m-m')(\alpha) = 0$, so $m-m' = 0$ by our choice of m.

Suppose $g \in K[t]$ and $g(\alpha) = 0$. By the division algorithm (8) there exists $q, r \in K[t]$, $\delta r < \delta m$, such that $g = qm + r$. Then $r(\alpha) = g(\alpha) - q(\alpha)m(\alpha) = 0$, so by our choice of m we have $r = 0$ and therefore m divides g. □

Example 33. *Consider* $\alpha = \sqrt{2} + \sqrt{3} \in \mathbf{R} \supset \mathbf{Q}(\sqrt{2}, \sqrt{3})$. *We have* $\alpha^2 = 5 + 2\sqrt{6}$ *and* $(\alpha^2 - 5)^2 = 24$. *So* $f(\alpha) = 0$ *where* $f = t^4 - 10t^2 + 1 \in \mathbf{Q}[t]$. *By Theorem 32, the minimal polynomial of* α *over* $\mathbf{Q}$ *divides* f. *Show that* f *is irreducible. Indeed, if it had a root then it would have a root over* $\mathbf{Z}_3$ *and an easy inspection shows that this is not the case. If* f *is a product of two quadratic polynomials then* α *must be a root of a (monic) quadratic polynomial. So suppose that*

$$(\sqrt{2} + \sqrt{3})^2 + a(\sqrt{2} + \sqrt{3}) + b = 0$$

where a, b *are rational numbers. We have*

$$2\sqrt{6} + a\sqrt{2} = -a\sqrt{3} - c$$

where $c = 5 + b$. *Further,*

$$24 + 4a\sqrt{12} + 2a^2 = c^2 + 3a^2 + 2\sqrt{3}ca.$$

We conclude that either $a = 0$ *or* $c = 4$. *If* $a = 0$ *then* $24 = c^2$ *which is impossible. If* $c = 4$ *then* $24 - a^2 = c^2 = 16$ *and* $a^2 = 8$, *again a contradiction.*

So f *is irreducible and therefore it is the minimal polynomial of* α.

Every monic irreducible polynomial over a field occurs as the minimal polynomial of an element of some extension field.

Theorem 34. *Let* K *be a field and* $f \in K[t]$ *be a monic irreducible polynomial. Then there exists a simple extension* $K(\alpha) \supset K$ *such that* f *is the minimal polynomial of* α *over* K.

Proof. Let I be the ideal in $K[t]$ consisting of all polynomials divisible by f. We claim that the quotient ring $K[t]/I$ is a field. Suppose $g + I \in K[t]/I$ is nonzero, so that $g \notin I$. As f is irreducible and does not divide g, there exist $a, b \in K[t]$ such that $1 = af + bg$, by the division algorithm (11). Then in $K[t]/I$ we have $(b + I)(g + I) = 1 + I - (a + I)(f + I) = 1 + I$, so $g + I$ is an inverse to $b + I$.

The composition of the natural inclusion $K \longrightarrow K[t]$ and the natural quotient map $K[t] \longrightarrow K[t]/I$ give us an extension $K \longrightarrow K[t]/I$ of fields. Once we identify K with its image in $K[t]/I$, we have $K[t]/I = K(\alpha)$ where $\alpha = t + I$, and $f(\alpha) = f(t) + I = 0$. As f is irreducible over K this means that f is the minimal polynomial of α over K. □

We would like to give a complete description of simple field extensions. To do this we shall need the following notion.

Definition 35. *Two extensions* $i : K \longrightarrow L$ *and* $i' : K' \longrightarrow L'$ *are* isomorphic *if there exist isomorphisms* $\phi : L \widetilde{\longrightarrow} L'$ *and* $\psi : K \widetilde{\longrightarrow} K'$ *such that* $\phi i = i'\psi$. *(If we identify* K *with* $i(K)$ *and* K' *with* $i(K')$ *then* ϕ *is an isomorphism of* L *onto* L' *which sends* K *onto* K'.*)*

Let $K(\alpha) \supset K$ be an arbitrary simple field extension. Consider the evaluation homomorphism

$$\phi : K[t] \longrightarrow K(\alpha) : f \mapsto f(\alpha).$$

We separate into two cases:

- α **is transcendental:** In this case ϕ is a monomorphism so by the exercise 5 ϕ extends to a monomorphism $\tilde{\phi} : K(t) \longrightarrow K(\alpha)$ which is the identity on K and sends t to α. Now $\mathrm{Im}(\phi)$ is a subfield of $K(\alpha)$ containing K and α so it must be all of $K(\alpha)$. So $\tilde{\phi}$ is an isomorphism which restricts to the identity on K. We conclude that any simple extension of a field K obtained by adjoining a transcendental element is isomorphic to the extension $K(t) \supset K$.
- α **is algebraic:** By Theorem 32, the ideal $I = \ker(\phi)$ consists of all polynomials divisible by m, the minimal polynomial of α over K. Thus we have an induced homomorphism $\overline{\phi} : K[t]/I \longrightarrow K(\alpha)$ which is the identity on K and sends $t + I$ to α. We saw in the proof of (34) that $K[t]/I$ is a field, and therefore $\overline{\phi}$ is a monomorphism. Moreover the image of $\overline{\phi}$ is subfield of $K(\alpha)$ containing K and α so it must be all of $K(\alpha)$. So $\overline{\phi}$ is an isomorphism which restricts to the identity on K. We conclude that any simple extension of a field K obtained by adjoining an algebraic element α is isomorphic to the extension $K[t]/I \supset K$, where I is the ideal generated by the minimal polynomial of the α.

In the algebraic case, we have seen that every element of $K(\alpha)$ is expressible as $f(\alpha)$ for some $f \in K[t]$. Of course f can be replaced with its remainder upon division by m (see (8)), so we may assume $\delta f < \delta m$. Moreover if $f, g \in K[t]$, $f(\alpha) = g(\alpha)$, and $\delta f, \delta g < \delta m$ then $(f - g)(\alpha) = 0$ and $\delta(f - g) < \delta m$ which implies that $f - g = 0$. So we've proved the existence of a 'standard form' for elements in a simple extension.

Proposition 36. *Let $K(\alpha) \supset K$ be a simple extension in which α in algebraic over K. Let $m \in K[t]$ be the minimal polynomial of α over K. Each element of $K(\alpha)$ is uniquely expressible as $f(\alpha)$ for a unique polynomial $f \in K[t]$ with $\delta f < \delta m$.*

It will be useful to have the following formulation of part of the second half of the foregoing discussion.

Theorem 37. *Let $K(\alpha) \supset K$ and $K(\beta) \supset K$ be simple field extensions and suppose that α and β have the same minimal polynomial m over K. Then the extensions are isomorphic, and we can choose an isomorphism which takes α to β.*

Proof. Let I be the ideal in $K[t]$ consisting of polynomials divisible by m. We've shown that there exists isomorphisms $\overline{\phi} : K[t]/I \longrightarrow K(\alpha)$ and $\overline{\psi} : K[t]/I \longrightarrow K(\beta)$ which restrict to the identity on K and such that $\overline{\phi}(t + I) = \alpha$ and $\overline{\psi}(t + I) = \beta$. The composition $\overline{\psi}\overline{\phi}^{-1}$ gives the desired isomorphism of extensions. □

We should point out that if $K(\alpha) \supset K$ and $K(\beta) \supset K$ are isomorphic simple extensions of K by algebraic elements, it does not necessary follow that that α and β have the same minimal polynomial. For example $\alpha + 1 \in K(\alpha)$ and $K(\alpha + 1) = K(\alpha)$, but α and $\alpha + 1$ do not in general have the same minimal polynomial.

Exercise 38. *Describe the minimal polynomial of $\alpha + 1$ over K in terms of the minimal polynomial of α over K. Show that these polynomials are different provided that K has characteristic 0.*

We record, for future reference, a more flexibly notated version of Theorem 37. The proof, which is similar, is left as an exercise.

Theorem 39. *Let $i : K \widetilde{\longrightarrow} K'$ be an isomorphism of fields. Let $K(\alpha) \supset K$ and $K'(\beta) \supset K'$ be simple extensions, and let $m_\alpha \in K[t]$ and $m_\beta \in K'[t]$ be the minimal polynomials of α and β over K and K'. Suppose that $i(m_\alpha) = m_\beta$. Then there exists an isomorphism $\hat{\imath} : K(\alpha) \widetilde{\longrightarrow} K'(\beta)$ such that $\hat{\imath}|_K = i$ and $\hat{\imath}(\alpha) = \beta$.*

4. Degree of an extension

Let $L \supset K$ be an extension of fields. Then L can be given the structure of a vector space over K as follows. If $v, w \in L$, define $v + w \in L$ by using the field addition in L. If $\lambda \in K$ and $v \in L$, define $\lambda v \in L$ by using the field multiplication in L.

The dimension of L as a K-vector space is called the *degree* of the extension and denoted by $[L : K]$.

Proposition 40. *Let $K(\alpha) \supset K$ be a simple extension. If α is transcendental over K then $[K(\alpha) : K]$ is infinite. If α is algebraic over K with minimal polynomial m, then $[K(\alpha) : K] = \delta m$; in fact $1, \alpha, \ldots, \alpha^{\delta m - 1}$ is a basis for $K(\alpha)$ over K.*

Proof. If α is transcendental over K, then $1, \alpha, \alpha^2, \ldots$ are linearly independent over K.

In the algebraic case, Proposition 36 tells us that each element of $K(\alpha)$ is uniquely expressible as $\lambda_0 + \lambda_1\alpha + \lambda_2\alpha^2 + \cdots + \lambda_{\delta m-1}\alpha^{\delta m-1}$, where $\lambda_i \in K$. This means that $1, \alpha, \ldots, \alpha^{\delta m-1}$ is a basis for $K(\alpha)$ over K. □

Example 41. (1) *Consider $\mathbf{Q}(\alpha) \supset \mathbf{Q}$ where $\alpha = \sqrt[3]{2} \in \mathbf{R}$. The polynomial $f = t^3 - 2$ is irreducible over $\mathbf{Q}$ (e.g., by Eisenstein's criterion, Theorem 20) and $f(\alpha) = 0$, so f is the minimal polynomial of α over $\mathbf{Q}$. Thus $[\mathbf{Q}(\alpha) : \mathbf{Q}] = \mathbf{3}$.*

(2) *Consider a simple extension $\mathbf{Q}(\alpha) \supset \mathbf{Q}$ where α has minimal polynomial $t^3 + t + 1$ over $\mathbf{Q}$. We have $\mathbf{Q}(\alpha) = \{\lambda_0 + \lambda_1\alpha + \lambda_2\alpha^2 \mid \lambda_0, \lambda_1, \lambda_2 \in \mathbf{Q}\}$. How can we express $(\alpha - 1)^{-1} \in \mathbf{Q}(\alpha)$ in this form? We apply Euclid's algorithm to $t^3 + t + 1$ and $t - 1$:*

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

So

$$3 = (\alpha^3 + \alpha + 1) - (\alpha^2 + \alpha + 2)(\alpha - 1)$$

and therefore

$$(\alpha - 1)^{-1} = -\frac{2}{3} - \frac{1}{3}\alpha - \frac{1}{3}\alpha^2.$$

Proposition 42. *(Tower Law) Suppose $M \supset L \supset K$. Then $[M : K] = [M : L][L : K]$.*

Proof. Let $(x_i)_{i\in I}$ be a basis for L over K and $(y_j)_{j\in J}$ be a basis for M over L. We claim that $(x_iy_j)_{i\in I, j\in J}$ is a basis for M over K. Suppose that $\sum_{i,j} \lambda_{ij}x_iy_j = 0$ where $\lambda_{ij} \in K$. Then $\sum_j \left(\sum_i \lambda_{ij}x_i\right) y_j = 0$, which implies that $\sum_i \lambda_{ij}x_i = 0$ for all j, and this in turn implies that $\lambda_{ij} = 0$ for all i and j. We've shown that (x_iy_j) is linearly independent over K.

Given any $z \in M$, we have $z = \sum_j \mu_j y_j$ for some $\mu_j \in L$, and each of these μ_j can be expressed $\mu_j = \sum_i \lambda_{ij}x_i$ for some $\lambda_{ij} \in K$. So $z = \sum_{i,j} \lambda_{ij}x_iy_j$ is in the K-span of (x_iy_j). □

Example 43. *Here we consider the tower $\mathbf{Q}(\sqrt{2}, \sqrt{3}) \supset \mathbf{Q}(\sqrt{2}) \supset \mathbf{Q}$. Firstly $\sqrt{2}$ has minimal polynomial $t^2 - 2$ over $\mathbf{Q}$, so $\{1, \sqrt{2}\}$ is a basis for $\mathbf{Q}(\sqrt{2})$ over $\mathbf{Q}$. Note that $\mathbf{Q}(\sqrt{2}, \sqrt{3}) = \mathbf{Q}(\sqrt{2})(\sqrt{3})$ is a simple extension of $\mathbf{Q}(\sqrt{2})$, and the minimal polynomial of $\sqrt{3}$ over $\mathbf{Q}(\sqrt{2})$ is $t^2 - 3$, because $\sqrt{3} \notin \mathbf{Q}(\sqrt{2})$ (check!). So $\{1, \sqrt{3}\}$ is a basis for $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbf{Q}(\sqrt{2})$. By the proof of the Tower Law, $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ is a basis for $\mathbf{Q}(\sqrt{2}, \sqrt{3})$ over $\mathbf{Q}$. If we're just interested in degrees and not bases, we can just calculate $[\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}] = [\mathbf{Q}(\sqrt{2}, \sqrt{3}) : \mathbf{Q}(\sqrt{2})][\mathbf{Q}(\sqrt{2}) : \mathbf{Q}] = 2 \cdot 2 = 4$.*

Definition 44. *An extension $L \supset K$ is*

- algebraic *if every $\alpha \in L$ is algebraic over K.*
- finite *if $[L : K]$ is finite.*
- finitely generated if $L = K(\alpha_1, \ldots, \alpha_n)$ *for some $\alpha_1, \ldots, \alpha_n \in L$.*

Lemma 45. *An extension $L \supset K$ is finite if and only if it is algebraic and finitely generated.*

Proof. Suppose $[L : K] = n < \infty$. If $\alpha \in K$, then $1, \alpha, \ldots, \alpha^n$ are linearly dependent over K so there exist $\lambda_0, \ldots, \lambda_n \in K$, not all zero, such that $\lambda_n\alpha^n + \cdots + \lambda_1\alpha + \lambda_0 = 0$, and therefore α is algebraic over K. Furthermore, if $\alpha_1, \ldots, \alpha_n$ is a basis for L over K then $L = K(\alpha_1, \ldots, \alpha_n)$.

Suppose on the other hand that $L = K(\alpha_1, \ldots, \alpha_n)$ is algebraic over K. We show that $L \supset K$ is finite by induction on n. By Proposition (42) we have $[L : K] = [L : K(\alpha_1, \ldots, \alpha_{n-1})][K(\alpha_1, \ldots, \alpha_{n-1}) : K]$. The second term in this product is finite, by induction, and the first is finite by Proposition 40 because $L = K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n)$ and α_n algebraic over K and therefore over $K(\alpha_1, \ldots, \alpha_{n-1})$. □

The simple transcendental extension $K(t) \supset K$ is an example of a finitely generated extension which is not finite. We now describe an algebraic extension which is not finite.

Let A be the set of complex numbers algebraic over $\mathbf{Q}$. By Prop. 40 a complex number α is in A if and only if $[\mathbf{Q}(\alpha) : \mathbf{Q}] < \infty$. Given any $\alpha, \beta \in A$, we have $[\mathbf{Q}(\alpha, \beta) : \mathbf{Q}] = [\mathbf{Q}(\alpha, \beta) : \mathbf{Q}(\alpha)][\mathbf{Q}(\alpha) : \mathbf{Q}] < \infty$ by Prop. 40 and 42 and therefore $\mathbf{Q}(\alpha, \beta) \subset A$. But $\alpha + \beta, -\alpha, \alpha\beta, \alpha^{-1} \in \mathbf{Q}(\alpha, \beta)$, so we've shown that A is a field extension of $\mathbf{Q}$.

Let $\alpha_n \in \mathbf{C}$ be a root of $f_n = t^n - 2$ for each $n \geq 1$, so that $\alpha_n \in A$. The f_n are irreducible by Eisenstein's' criterion, so $[\mathbf{Q}(\alpha_n) : \mathbf{Q}] = n$ by Prop. 40. So $[A : \mathbf{Q}] \geq [\mathbf{Q}(\alpha_n) : \mathbf{Q}] = n$ for all n.

5. Compass and straightedge constructions

This section, a detour from the main thrust of the course, demonstrates the power of the theory of field extensions.

The Greeks showed how to perform some geometric constructions, such as bisecting angles or dividing segments into any number of equal parts, using just a compass and straightedge under certain constraints.

There are some constructions that aren't possible in this setting: duplicating the cube (constructing a length whose cube is twice the cube of a given length), trisecting an angle, and squaring a circle. The impossibility of these constructions can be deduced fairly easily using the theory of field extensions.

We work in the plane $\mathbf{R}^2$. We assume that two points are given: $p_0 = (0,0)$ and $p_1 = (1,0)$. We say that $p \in \mathbf{R}^2$ is *constructible* if there exists a sequence of points $p_0, p_1, \ldots, p_n = p$ such that setting $S_j = \{p_0, p_1, \ldots, p_j\}$, we have for each $2 \leq j \leq n$ that p_j is either

- the intersection of two distinct lines, each joining two points in S_{j-1},
- the intersection of a line joining two points in S_{j-1} with a circle centered at a point of S_{j-1} and with a point of S_{j-1} on its circumference, or
- the intersection of two circles with distinct centers in S_{j-1} and each with a point of S_{j-1} on its circumference.

Theorem 46. *If $p = (x,y)$ is constructible then $[\mathbf{Q}(x,y) : \mathbf{Q}] = 2^r$ some integer r.*

Proof. Let $p_0, \ldots, p_n = p$ be as in definition of constructible and $p_j = (x_j, y_j)$. Let $K_j = \mathbf{Q}(x_0, y_0, x_1, y_1, x_2, \ldots, x_j, y_j)$, so that $K_j = K_{j-1}(x_j, y_j)$. We will prove that $[K_j : K_{j-1}] = 1$ or 2 for $j = 1, \ldots, n$. It will follow by Prop. 42 that $[K_n : K]$ is a power of 2. Then again by tower law, we have $[K_n : \mathbf{Q}] = [K_n : \mathbf{Q}(x,y)][\ \mathbf{Q}(x,y) : \mathbf{Q}]$, so that $[\mathbf{Q}(x,y) : \mathbf{Q}]$ is a power of 2 as well.

We need to consider 3 cases; we will handle the most interesting one, leaving the other cases as an exercise. Say $p_j = (x_j, y_j)$ is the intersection of the line through (a,b) and (c,d) and circle centered at (e,f) through (g,h), where $a, \ldots, h \in K_{j-1}$.

The line has equation $\frac{X-a}{Y-b} = \frac{c-a}{d-b}$ and the circle has equation $(X-e)^2 + (Y-f)^2 = (g-e)^2 + (h-f)^2$. Substituting $X =$ linear expression in Y into the second equation, we see that y_j is a root of a quadratic polynomial with coefficients in K_{j-1}. So the minimal polynomial of y_j over K_{j-1} has degree 1 or 2, so $[K_{j-1}(y_j) : K_{j-1}] = 1$ or 2. Now using the linear equation, we see that $x_j \in K_{j-1}(y_j)$, so $K_j = K_{j-1}(y_j)$ and $[K_j : K_{j-1}] = 1$ or 2, as desired.

Now we can consider each of the famous problems in turn.

Duplication of cube: We are given p_0 and p_1 and thus basically the length 1. We want to construct the length whose cube is twice this, so the question becomes 'Can we construct the point $(\alpha, 0)$, where $\alpha^3 = 2$'? The answer is no because $[\mathbf{Q}(\alpha, 0) = \mathbf{Q}(\alpha)\colon \mathbf{Q}] = 3$ is not a power of 2.

Trisection of the angle: We can construct $\pi/3$, but can't trisect it. If we could then we could construct $(\cos(\pi/9), 0)$ and hence $(\alpha, 0)$, where $\alpha = 2\cos(\pi/9)$. Now from elementary trigonometry we have $\cos(3\theta) = 4\cos^3(\theta) - 3\cos(\theta)$. Putting $\theta = \frac{\pi}{9}$, we deduce that α is a zero of $t^3 - 3t - 1$, which is irreducible over $\mathbf{Q}$ (check!). So $[\mathbf{Q}(\alpha, 0) = \mathbf{Q}(\alpha)\colon \mathbf{Q}] = 3$ is not a power of 2.

Square the circle: This means constructing the point $(\sqrt{\pi}, 0)$, from which one could also construct $(\pi, 0)$. For the latter to be possible $[\mathbf{Q}(\pi) : \mathbf{Q}]$ would have to be power of two. But this degree is actually infinite, i.e. π is transcendental. This is theorem of Lindemann.

6. The Galois group of an extension

We have associated to any extension a vector space, and this gave a way of measuring the size of an extension. To get at our main application, namely solving polynomial equations, we need some better way of understanding structure of extension.

Let L be a field. An *automorphism* of L is an isomorphism $\sigma : L \longrightarrow L$. The set of such forms a group $\mathrm{Aut}(L)$ under composition.

Let K be a subfield of L. A *K-automorphism* of L is an automorphism σ of L such that $\sigma(x) = x$ for all $x \in K$. These form a subgroup of $\mathrm{Aut}(L)$ which is denoted by $Gal(L : K)$ or $Gal(L \supset K)$ or $Gal(L/K)$ and called the *Galois group of L over K*. When it is clear from context what L is we will also use the shorthand notation $K^* = Gal(L \supset K)$.

Example 47. (1) *The extension* $\mathbf{C} \supset \mathbf{R}$. *Let* σ *be an* $\mathbf{R}$*-automorphism of* $\mathbf{C}$. *Let* $i = \sqrt{-1}$ *Then* $\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$ *because* $-1 \in \mathbf{R}$. *So either* $\sigma(i) = i$ *or* $\sigma(i) = -i$. *Then for any* $r, s \in \mathbf{R}$, *we have* $\sigma(r + si) = \sigma(r) + \sigma(s)\sigma(i) = r + s\sigma(i)$. *Hence there are two possibilities for* σ, *the identity map* $\sigma(z) = z$ *and the complex conjugation* $\sigma(z) = \overline{z}$. *Both are indeed* $\mathbf{R}$*-automorphisms of* $\mathbf{C}$, *so the Galois group of* $\mathbf{C} \supset \mathbf{R}$ *is a cyclic group of order* 2.

(2) *The extension* $\mathbf{Q}(\alpha) \supset \mathbf{Q}$ *where* α *is the real cube root of* 2. *Let* $\sigma \in Gal(\mathbf{Q}(\alpha) \supset \mathbf{Q})$. *Then* $\sigma(\alpha)^3 = \sigma(\alpha^3) = \sigma(2) = 2$ *which implies that* $\sigma(\alpha) = \alpha$ *and therefore that* σ *is the identity map on* $\mathbf{Q}(\alpha)$. *So the Galois group of* $\mathbf{Q}(\alpha)$ *over* $\mathbf{Q}$ *is the trivial group.*

In these two examples we have essentially used the following key lemma.

Lemma 48. *Suppose* $L \supset K$. *If* $\alpha \in L$ *is a zero of* $f \in K[t]$ *then so is* $\sigma(\alpha)$ *for any* $\sigma \in Gal(L \supset K)$. *In particular (*$f$ *is the minimal polynomial of* α *over* K*)* $\Longrightarrow$*(* f *is the minimal polynomial of* $\sigma(\alpha)$ *over* K*).*

Proof. Write $f = \lambda_n t^n + \ldots + \lambda_1 t + \lambda_0$. Then

$$\begin{aligned}\sigma(f(\alpha)) &= \sigma(\lambda_n)\sigma(\alpha)^n + \ldots + \sigma(\lambda_1)\sigma(\alpha) + \sigma(\lambda_0) \\ &= \lambda_n\sigma(\alpha)^n + \ldots + \lambda_1\sigma(\alpha) + \lambda_0 \\ &= f(\sigma(\alpha)).\end{aligned}$$

Thus $f(\alpha) = 0$ implies $f(\sigma(\alpha)) = 0$. □

To each subfield K of a given field L we have associated a subgroup $K^* \subset \mathrm{Aut}(L)$. We can go in the other direction, too. If G is a subgroup of $\mathrm{Aut}(L)$ we denote by L^G the set of $x \in L$ such that $\sigma(x) = x$ for all $\sigma \in G$. It is easily verified that L^G is a subfield of L, called the *fixed field* of G. If it is clear from context what L is we will write $G^\dagger$ instead of L^G.

So we have maps in both directions:

$$\begin{aligned}* &: \text{subfields of } L \longrightarrow \text{subgroups of } Aut(L). \\ \dagger &: \text{subgroups of } Aut(L) \longrightarrow \text{ subfields of } L.\end{aligned}$$

Proposition 49. a) $*$ *and* $\dagger$ *reverse inclusions.*

b) $K \subset K^{*\dagger}$ *and* $G \subset G^{\dagger *}$.

c) $K^* = K^{*\dagger *}$ *and* $G^\dagger = G^{\dagger *\dagger}$

d) *The image of* $*$ *consists of those* G *such that* $G = G^{\dagger *}$ *and the image of* $\dagger$ *consists of those* K *such that* $K^{*\dagger}$. *The maps* $*$ *and* $\dagger$ *induce inverse bijections between the image of* $*$ *and the image of* $\dagger$.

Proof. (a) and (b) are easily checked. This sets up a very general situation in which (c) and (d) are standard easy deductions. □

It is actually the case that $G^{\dagger *} = G$ for any finite subgroup G. We will prove this below. But it is *not* true that $K^{*\dagger} = K$ for any subfield K. These are special.

Definition 50. *An extension* $L \supset K$ *is called* Galois *if* $K^{*\dagger} = K$, *i.e. if the fixed field of* $Gal(L \supset K)$ *is* K.

Example 51. (1) $L = \mathbf{C}$ *and* $K = \mathbf{R}$. *Then* $\mathbf{R}^{*\dagger} = \mathbf{R}$, *as the only complex numbers fixed by complex conjugation are the reals. So* $\mathbf{C} \supset \mathbf{R}$ *is a Galois extension.*

(2) $L = \mathbf{Q}(\alpha)$,*where* α *a real cube root of* 3 *and* $K = \mathbf{Q}$. *Then* $\mathbf{Q}^{*\dagger} = \mathbf{Q}(\alpha)$, *so* $\mathbf{Q}(\alpha) \supset \mathbf{Q}$ *is not Galois.*

(3) $L = \mathbf{Q}(\sqrt{2}, \sqrt{3})$ *and* $K = \mathbf{Q}$. *If* $\sigma \in Aut(L)$ *then* $\sigma(1) = 1$ *so* $\sigma(\lambda) = \lambda$ *for all* $x \in \mathbf{Q}$. *Also* $\sigma(\sqrt{2}) = \pm\sqrt{2}$ *and* $\sigma(\sqrt{3}) = \pm\sqrt{3}$. *Recall that* $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ *is a basis for* L *over* $\mathbf{Q}$. *So there are at most 4 elements of* $Aut(L)$, *given by the formulas*

$$\begin{aligned}id(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}, \\ \sigma_1(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}, \\ \sigma_2(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}, \\ \sigma_3(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) &= a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}.\end{aligned}$$

where $a, b, c, d \in \mathbf{Q}$. It is straightforward albeit slightly tedious to check directly these are field automorphisms (we shall find an easier method eventually). Each nonidentity element squares to id so $\mathrm{Aut}(L)$ *is isomorphic to the Klein four group $C_2 \times C_2$.*

Let us calculate the fixed fields of all subgroups of $\mathrm{Aut}(L)$.

$$\begin{aligned} L^{\mathrm{Aut}(L)} &= \mathbf{Q}, \\ L^{\{id,\sigma_1\}} &= \mathbf{Q}(\sqrt{2}), \\ L^{\{id,\sigma_2\}} &= \mathbf{Q}(\sqrt{3}), \\ L^{\{id,\sigma_3\}} &= \mathbf{Q}(\sqrt{6}), \\ L^{\{id\}} &= L. \end{aligned}$$

Question: are there any other subfields of L other than the five listed here?

Next we seek a relationship between the degree of an extension and the size of its Galois group.

Theorem 52. *Let L be a field and let G be a group of automorphisms of L. Then $[L : G^\dagger] = |G|$.*

Corollary 53. a) *If $L \supset K$ is a finite extension then $|Gal(L \supset K)| \leq [L : K]$. Equality holds if and only if $L \supset K$ is a Galois extension.*

b) *If G is a finite subgroup of $Aut(L)$ then $G = G^{\dagger *}$.*

So we have a numerical characterisation of (finite) Galois extensions: they are extensions whose Galois groups are 'as large as possible'.

Proof. (of Corollary). We have $K \subset K^{*\dagger}$ by Prop. 49b). So $[L : K] \geq [L : K^{*\dagger}] = |Gal(L \supset K)|$, because $K^{*\dagger}$ is the fixed field of $K^* = Gal(L \supset K)$, and (a) is proven. For (b) we have $|G| = [L : G^\dagger] = [L : G^{\dagger *\dagger}] = |G^{\dagger *}|$ by Theorem 52 and Prop. 49c). The desired result follows because $G \subset G^{\dagger *}$, by Prop. 49b), (and because G is finite). □

To prove the theorem we will need a lemma. In order to understand its statement, first note that if S is a set and L a field, then the set of all maps $f : S \longrightarrow L$ is a vector space over L: if f, g are maps and $\lambda \in L$ then we define $(f + g)(s) = f(s) + g(s)$ and $(\lambda f)(s) = \lambda f(s)$.

Lemma 54. *(Dedekind). Let K and L be fields. The set of monomorphisms $K \to L$ is linearly independent over L.*

Proof. Suppose not. Then we have a linear relation

$$\lambda_1\sigma_1 + \cdots + \lambda_n\sigma_n = 0,$$

where $\sigma_1, \ldots, \sigma_n : K \to L$ are distinct monomorphisms and $\lambda_1, \ldots, \lambda_n \in L$, are all nonzero. Choose n to be as small as possible.

We have

$$\text{(A)} \qquad \lambda_1\sigma_1(x) + \lambda_2\sigma_2(x) \cdots + \lambda_n\sigma_n(x) = 0 \quad (\forall x \in K)$$

Choose $y \in K$ such that $\sigma_1(y) \neq \sigma_2(y)$. Replacing x by xy we get

$$\text{(B)} \qquad \lambda_1\sigma_1(x)\sigma_1(y) + \lambda_2\sigma_2(x)\sigma_2(y) \cdots + \lambda_n\sigma_n(x)\sigma_n(y) = 0 \quad (\forall x \in K)$$

Now consider $(B) - \sigma_1(y)(A)$:

$$\lambda_2(\sigma_2(y) - \sigma_1(y))\sigma_2(x) + \cdots + \lambda_n(\sigma_n(y) - \sigma_1(y))\sigma_n(x) = 0 \quad (\forall x \in K)$$

As $\lambda_2(\sigma_2(y) - \sigma_1(y)) \neq 0$, this gives a nontrivial relation among $\sigma_2, \ldots, \sigma_n$, contradicting our choice of n. □

Now we can prove Theorem 52: Set $L_0 = G^\dagger$. Suppose $[L : L_0] = m \leq \infty$, and let $(x_1, \ldots, x_m)$ be a basis for L over L_0. Let $g_1, \ldots, g_n$ be distinct elements of G. If $n > m$ then consider the system of homogeneous linear equations in y's:

$$g_1(x_j)y_1 + \cdots + g_n(x_j)y_n = 0$$

for $j = 1, \ldots, m$. There are more unknowns than equations, so there are y_i's in L, not all zero satisfying these equations. Then $(y_1g_1 + \cdots + y_ng_n)(x_j) = 0$ for $j = 1, \ldots, m$. Note that any $g \in G$ is a L_0-linear

map from L to L. Therefore so is $y_1g_1 + \cdots + y_ng_n$. It is zero on a basis for L over L_0, hence zero. This contradicts linear independence of monomorphisms.

So we've shown that if G is infinite then so is $[L : L_0]$, and if G is finite then $|G| \leq [L : L_0]$.

So now suppose $G = \{g_1, \ldots, g_n\}$ is finite and let $x_1, \ldots, x_m \in L$ be linearly independent over L_0 , where $n < m$. We consider the system of homogeneous linear equations

$$g_j(x_1)y_1 + g_j(x_2)y_2 + \cdots + g_j(x_m)y_m = 0 \tag{C}$$

for $j = 1, \ldots, n$. There are more unknowns than equations so there exist $y_i \in L$, not all zero, satisfying these equations. Choose these so that number of nonzero y_i's is as small as possible, and relabel the x_i's so that $y_1 \neq 0$. For any $g \in G$ we can apply g to the equation above to get

$$gg_j(x_1)g(y_1) + \cdots + gg_j(x_m)g(y_m) = 0$$

for $j = 1, \ldots, n$. From group theory we know that $\{gg_1, \ldots, gg_n\} = \{g_1, \ldots, g_n\}$ so the n equations above can simply be written

$$g_j(x_1)g(y_1) + g_j(x_2)g(y_2) \cdots + g_j(x_m)g(y_m) = 0 \tag{D}$$

Next consider $g(y_1)(C) - y_1(D)$:

$$g_j(x_2)(y_2g(y_1) - g(y_2)y_1) + \cdots + g_j(x_m)(y_mg(y_1) - g(y_m)y_1) = 0.$$

This is a solution of the system (C), but with fewer nonzero terms (as $y_i = 0$ implies that $y_ig(y_1) - g(y_i)y_1 = 0$). So we get a contradiction unless $y_jg(y_1) - g(y_j)y_1 = 0$ for $j = 2, \ldots, m$. If so then $g(y_iy_1^{-1}) = y_iy_1^{-1}$ for all $g \in G$, so $y_iy_1^{-1} \in L_0$.

Now taking g_j to be the identity in equation (C) and multiplying by y_1^{-1} we get a linear relation among the x_j's with coefficients in L_0, a contradiction.

7. Digression: adjoint functors

The material in this section is optional and uses some concepts and ideas which you may or may not be familiar with. The goal is to put the notion of the Galois extension into a broader perspective.

Let $\mathcal{A}$ and $\mathcal{B}$ be two categories and $L : A \to B, R : B \to A$ be functors between them . We say that L is left adjoint to R or that R is right adjoint to L if there is a natural bijection for all A in $\mathcal{A}$ and B in $\mathcal{B}$:

$$\tau = \tau_{AB} : Hom_{\mathcal{B}}(L(A), B) \longrightarrow Hom_{\mathcal{A}}(A, R(B)).$$

The naturality here means that the bijection τ behaves functorially with respect to any morphisms $A \to A'$ and $B \to B'$. (You can try to figure out what it means or look in any book on category theory).

Examples of adjoint functors abound. Here we'll give a few examples. You should be able to extend this list.

(1) The functor which associates to any set free group generated by this set is left adjoint to the forgetful functor from groups into sets.
(2) The forgetful functor from complete metric spaces is right adjoint to the functor associating to a metric space its completion.
(3) The functor associating to a vector space its dual vector space is a functor from vector spaces to the *opposite* category of vector spaces (i.e. the category having the same class of objects where all arrows are reversed.) This functor is its own left and right adjoint.
(4) If categories $\mathcal{A}, \mathcal{B}$ are equivalent via two quasi-inverse functors R, L then these functors are adjoint (both left and right) to each other.

Exercise 55. *Let L, R be an adjoint pair of functors between categories $\mathcal{A}$ and $\mathcal{B}$. For any object $A \in \mathcal{A}$ define a morphism $L(A) \to LRL(A)$ and a morphism $LRL(A) \to L(A)$ such that its composition is the identity morphism $L(A) \to L(A)$. Similarly for B in $\mathcal{B}$ define morphisms $R(B) \to RLR(B) \to R(B)$ whose composition is the identity morphism $R(B) \to R(B)$.*

Let L, R be a pair of adjoint functors as above and consider and arbitrary object A in $\mathcal{A}$. Then the set $Hom_{\mathcal{A}}(A, RL(A)) = Hom_{\mathcal{B}}(L(A), L(A))$ contains a preferred element corresponding to the identity morphism in $Hom_{\mathcal{B}}(L(A), L(A))$. In other words, there is a canonical morphism $A \to RL(A)$. This morphism

is called the unit of the adjunction L, R. Similarly the counit of the adjunction is the map $LR(B) \to B$ in $\mathcal{B}$ where B is an object in $\mathcal{B}$.

Note that any contravariant functor $\mathcal{A} \to \mathcal{B}$ could be considered as a usual (covariant) functor $\mathcal{A}^o \leftarrow \mathcal{B}^o$ where the superscript o denotes the opposite category. Therefore we can consider the notion of adjoint contravariant functors. The definitions of the unit and the counit will be modified accordingly (work it out!)

You can find much more information on adjoint functors in Mac Lane's book 'Categories for working mathematicians'.

Now consider the category $\mathcal{S}G$ of subgroups of a fixed group G. The objects of $\mathcal{S}G$ are subgroups of G and for two subgroups H_1 and H_2 there is an arrow $H_1 \to H_2$ if and only if H_1 is a subgroup of H_2.

Similarly for a field L consider the category $\mathcal{S}L$ of subfields of L. Again, the arrows correspond to inclusions of subfields.

Assume that $G = Aut(L)$. Then the functor $* : \mathcal{S}L \to \mathcal{S}G$ is right adjoint to the functor $\dagger : \mathcal{S}G \to \mathcal{S}L$. Check this. Note that this is pretty much the content of Prop. 49.

However Theorem 52 goes beyond general nonsense: it shows effectively that the composition of adjoint functors $\dagger *$ is isomorphic to the identity functor. If the composition $*\dagger$ were (isomorphic to) the identity functor that would imply that $*$ and $\dagger$ were mutually inverse equivalences of categories $\mathcal{S}G$ and $\mathcal{S}L$. This is not the case and in fact the category $\mathcal{S}G$ is equivalent to the subcategory in $\mathcal{S}L$ formed by 'good' subfields, i.e. those subfields K for which $L \supset K$ is a Galois extension.

This situation is typical. Recall Hilbert's Nullstellensatz. Let I is an ideal in the ring $R = k[x_1, \ldots, x_n]$ where k is an algebraically closed field and denote by $V(I)$ the set of common zeroes of all polynomials $f \in I$ in the affine space k^n. Then if a polynomial $f \in R$ vanishes at all points in $V(I)$ then $f^r \in I$ for some r.

Here we have the correspondence which associates to any ideal I the set $V(I)$. Conversely, to any algebraic set $V \subset k^n$ (i.e. the set defined by a system of polynomial equations) we associate the ideal $I(V)$ of polynomials which vanish on V. The composition $V \to I(V) \to V(I(V))$ gives us back the set V. However the composition $I \to V(I) \to I(V(I))$ gives $\sqrt{I}$, the *radical* of I, i.e. the set of polynomials $f \in R$ such that $f^r \in I$ for some r. This gives a $1-1$ correspondence between algebraic sets in k^n and the set of radical ideals in R, i.e. such ideals I for which $I = \sqrt{I}$.

This correspondence can also be considered as an example of a pair of adjoint functors.

The last example which we mention plays a prominent role in algebraic geometry. It is the construction of an associated sheaf for a presheaf. The discussion of this example would take us too far afield and an interested student is recommended to look in any book on algebraic geometry or sheaf theory.

8. Normality and separability

Our eventual goal will be to develop a criterion for Galoisness of an extension which does not involve explicitly calculating automorphisms. Instead, following the suggestion of Lemma 48 we will use polynomials.

We consider the idea of *normality* first. So far we've been studying extensions $K(\alpha) \supset K$ in which we adjoin a single zero α of a polynomial f to K. We really want to study all the zeros together, and the relations between them.

Let's make a few general observations about zeroes of polynomials. We saw (Lemma 17) that $\alpha \in K$ is a zero of $f \in K[t]$ if and only if $(t-\alpha)|f$. We define the *multiplicity* of α as the largest integer k for which $(t-\alpha)^k|f$. If $k > 1$ we say that α is a multiple zero of f in K. Now by unique factorisation, f can be written

$$f = g(t-\alpha_1)^{k_1} \cdots (t-\alpha_r)^{k_r},$$

uniquely (up to reordering of the α_i's), where g has no zeros in K. Then $\alpha_1, \ldots, \alpha_r$ are the zeroes of f in K, with multiplicities $k_1, \ldots, k_r$. In particular note that f has at most δf zeros.

If $\delta g = 0$, then we say that f *splits* over K.

Let f be a polynomial over K. Then a *splitting field* for f over K is a field Σ containing K such that

(1) f splits over Σ, and

(2) if $K \subset \Sigma' \subset \Sigma$ and f splits over Σ', then $\Sigma' = \Sigma$.

Note that if (1) holds, then f will split over Σ' if and only if it contains all the zeros of f in Σ. So in the presence of (1), (2) is equivalent to

(2') $\Sigma = K(\alpha_1, \ldots, \alpha_r)$, where $\alpha_1, \ldots, \alpha_r$ are the zeros of f in Σ.

Example 56. (1) *Suppose f has degree 2. If f has a zero over K then it splits. So if Σ is a splitting field for f over K, then either $[\Sigma : K] = 1$ or $[\Sigma : K] = 2$.*

(2) *Consider $f = t^3 - 2$ over $\mathbf{Q}$. Let α be the real cube root of 2. Then letting $\omega = e^{2\pi i/3} \in \mathbf{C}$, we have $f = (t-\alpha)(t-\omega\alpha)(t-\omega^2\alpha)$. So $\mathbf{Q}(\alpha, \omega\alpha, \omega^2\alpha) = \mathbf{Q}(\alpha, \omega)$ is a splitting field for f over $\mathbf{Q}$. Note that this is strictly larger than $\mathbf{Q}(\alpha)$ because the latter is contained in $\mathbf{R}$.*

(3) *Consider $f = t^3 + t^2 + 1$ over Z_2. By (34) there exists a simple extension $Z_2(\alpha) \supset Z_2$ such that f is the minimal polynomial of α over Z_2. Does f split over $Z_2(\alpha)$? Well, $0 = (\alpha^3 + \alpha^2 + 1)^2 = \alpha^6 + \alpha^4 + 1 = (\alpha^2)^3 + (\alpha^2)^2 + 1$, so α^2 is also a zero of f in $Z_2(\alpha)$. Therefore $\alpha^4 = (\alpha^2)^2$ is a zero as well. These three zeroes are distinct. Indeed, $\alpha \neq \alpha^2$ since otherwise α would have been a root of a quadratic polynomial. Likewise, it is easy to see that $\alpha \neq \alpha^4$ and $\alpha^2 \neq \alpha^4$. Therefore $\mathbf{Z}_2(\alpha)$ is a splitting field for f over $\mathbf{Z}_2$.*

Theorem 57. *Splitting fields exist.*

Proof. Using conditions (1)+(2'), we see that it suffices to find an extension field L in which f splits. By Theorem 34 there exists an extension $K(\alpha) \supset K$ where α has minimal polynomial f_1. Now $f_1(\alpha) = 0$, so over $K(\alpha)$, $(t-\alpha)|f_1$, so $(t-\alpha)|f$. Write $f = (t-\alpha)g$ where g is a polynomial over $K(\alpha)$ and $\delta(g) = \delta(f) - 1$. By induction there is an extension $\Sigma \supset K(\alpha)$ in which g splits. Then f splits in Σ as well. □

Actually splitting fields are unique up to isomorphism.

Lemma 58. *Let $i : K \widetilde{\longrightarrow} K'$ be an isomorphism of fields, f a polynomial over K, Σ a splitting field for f over K, and L' and extension of K' in which $i(f)$ splits. Then there exists a monomorphism $j : \Sigma \longrightarrow L'$ such that $j|_K = i$.*

Proof. Induct on δf. Let α be a zero of f in K. If m is the minimal polynomial of α over K, then $m|f$. Thus $i(m)|i(f)$. As $i(f)$ splits in L', so does $i(m)$. In particular $i(m)$ has a zero β in L', and as $i(m)$ is monic irreducible, it is the minimal polynomial of β. It follows by Thm. 39 that there exists $\hat{\imath} : K(\alpha) \longrightarrow K'(\beta)$ such that $\hat{\imath}|_K = i$ (and $\hat{\imath}(\alpha) = \beta$). Now $f = (t-\alpha)f_1$, where $f_1 \in K(\alpha)[t]$ and $\delta f_1 < \delta f$, and Σ is a splitting field for f_1 over $K(\alpha)$. Moreover $i(f) = \hat{\imath}(f) = \hat{\imath}(t-\alpha)\hat{\imath}(f_1)$ so $\hat{\imath}(f_1)$ splits over L'. Therefore by induction there exists $j : \Sigma \longrightarrow L'$ such that $j|_{K(\alpha)} = \hat{\imath}$. Then $j|_K = \hat{\imath}|_K = i$. □

Proposition 59. *(Uniqueness of splitting fields) Let $i : K \widetilde{\longrightarrow} K'$ be an isomorphism, let f be a polynomial over K, and let Σ and Σ' be splitting fields for f over K and $i(f)$ over K'. Then there exists an isomorphism $j : \Sigma \widetilde{\longrightarrow} \Sigma'$ such that $j|_K = i$. In particular the extensions $\Sigma \supset K$ and $\Sigma' \supset K'$ are isomorphic.*

Proof. By Lemma 58 we get at least a monomorphism j with the right properties. Then $K' \subset j(\Sigma) \subset \Sigma'$, and $j(\Sigma)$ is a splitting field for $i(f)$. By definition of splitting field $j(\Sigma) = \Sigma'$, so j is surjective. □

We now make the key definition.

Definition 60. *An extension $L \supset K$ is* normal *if every irreducible polynomial f over K which has a zero in L splits over L.*

Theorem 61. *An extension $L \supset K$ is normal and finite if and only if it is a splitting field for some polynomial over K.*

Proof. Suppose $L \supset K$ is normal and finite. Let $\alpha_1, \ldots, \alpha_n$ be a basis for L over K. Then $L = K(\alpha_1, \ldots, \alpha_n)$, where the α's are algebraic over K. If m_i is the minimal polynomial of α_i over K, then by assumption m_i splits over L. Hence L is a splitting field for $m = m_1 \cdots m_n$ over K.

Conversely, assume L is a splitting field for a polynomial g over K. Clearly $[L : K]$ is finite. We now show it is normal. Let f be an irreducible polynomial over K, and let M be an extension field of L in which f splits (e.g. a splitting field). We claim that if α and β are zeroes of f in M then $[L(\alpha) : L] = [L(\beta) : L]$.

If the claim is true then $\alpha \in L \Longrightarrow \beta \in L$ as desired. To prove it, consider this picture:

$$\begin{array}{ccccc} & & M & & \\ & \swarrow & & \searrow & \\ L(\alpha) & & \xrightarrow[j]{\sim} & & L(\beta) \\ & \nwarrow & & \nearrow & \\ | & & L & & | \\ K(\alpha) & & \xrightarrow[i]{\sim} & & K(\beta) \\ & \nwarrow & | & \nearrow & \\ & & K & & \end{array}$$

By Theorem 37 there exists an isomorphism $i : K(\alpha) \xrightarrow{\sim} K(\beta)$ such that $i(x) = x$ for all $x \in K$. In particular

$$[K(\alpha) : K] = [K(\beta) : K].$$

Now $L(\alpha)$ is a splitting field for g over $K(\alpha)$, and $L(\beta)$ is a splitting field for $i(g) = g$ over $K(\beta)$. So by Prop. 59 there exists an isomorphism $j : L(\alpha) \xrightarrow{\sim} L(\beta)$ such that $j|_{K(\alpha)} = i$. Thus

$$[L(\alpha) : K(\alpha)] = [L(\beta) : K(\beta)].$$

So using the tower law (Prop. 42) twice we get

$$[L(\alpha) : K] = [L(\beta) : K],$$

and

$$[L(\alpha) : L] = [L(\beta) : L].$$

□

Lemma 62. *Let $L \supset M \supset K$ be a tower of field extensions and suppose $L \supset K$ is finite normal extension. Then $L \supset M$ is a finite normal extension as well.*

Proof. By Theorem 61 there exists $f \in K[t]$ such that L is a splitting field for f over K. Then f is a splitting field for f over M, and therefore by Thm 61 again, $L \supset M$ is a finite normal extension. □

We turn now to separability.

Definition 63. *An irreducible polynomial f over a field K is* separable *over K if it has no multiple zeroes in a splitting field. If f is not separable over K we say it is* inseparable *over K.*

Here is an example of an inseparable polynomial. Let $K = \mathbf{Z}_p(u)$ be the field of rational functions over $\mathbf{Z}_p$ in the indeterminate u, and let $f = t^p - u \in K[t]$. Note that u is in the field of coefficients. Suppose that τ is a zero of f in some splitting field of f over K.

We have

$$(t - \tau)^p = t^p + \binom{p}{1} t^{p-1}(-\tau) + \cdots + (-\tau)^p.$$

All the terms except the first and last are zero, because the binomial coefficients are divisible by p, so

$$(t - \tau)^p = t^p - \tau^p = t^p - u = f.$$

Hence τ is the only zero of f , with multiplicity p.

Now let's check that f is irreducible. If $f = gh$ in $K[t]$ is a nontrivial factorisation, then $g = (t - \tau)^s$ where $1 \leq s \leq p - 1$. So its constant term τ^s is in K, and choosing $a, b \in \mathbf{Z}$ so that $as + bp = 1$, we get $\tau = (\tau^s)^a \cdot (\tau^p)^b \in K$. Recall that $K = \mathbf{Z}_p(u)$, so that $\tau = v/w$ where v and w are polynomials in u. Then $\tau^p = u$ implies that $v^p = w^p u$. But $\delta(v^p) \equiv 0 \bmod p$ while $\delta(w^p u) \equiv 1 \bmod p$, a contradiction.

Next, we seek a way to detect the existence of multiple zeroes. Borrowing ideas from real analysis, we introduce the idea of *formal differentiation.*

If $f = a_n t^n + \cdots + a_1 t + a_0 \in K[t]$, then define

$$Df = n a_n t^{n-1} + (n-1) a_{n-1} t^{n-2} + \cdots + a_1 \in K[t].$$

It is easy to check that the usual rules of differentiation hold in this context: $D(f + g) = Df + Dg$ and $D(fg) = (Df)g + f(Dg)$ for all $f, g \in K[t]$.

Lemma 64. *A nonzero polynomial f over a field K has a multiple zero in a splitting field if and only if f and Df have a common factor of degree ≥ 1.*

Proof. Suppose $f = (t-\alpha)^2 g$ in some splitting field Σ. Then $Df = 2(t-\alpha)g + (t-\alpha)^2 g$, so α is a zero of both f and Df. Thus the minimal polynomial of α over K divides both f and Df.

Conversely, suppose that in a splitting field, $f = \lambda(t-\alpha_1)\cdots(t-\alpha_r)$, where the α_i's are distinct. Then $Df = \lambda\sum_{i=1}^{r}(t-\alpha_1)\cdots\widehat{(t-\alpha_i)}\cdots(t-\alpha_r)$. So $Df(\alpha_i) = (\alpha_i-\alpha_1)\cdots\widehat{(\alpha_i-\alpha_i)}\cdots(\alpha_r-\alpha_i) \neq 0$, so by (17), $(t-\alpha_i)$ does not divide Df. Thus f and Df are relatively prime over any splitting field, and hence relatively prime over K (check this!). □

Lemma 65. *Over a field of characteristic zero, all irreducible polynomials are separable. Over a field of characteristic p, an irreducible polynomial is inseparable if and only if it has the form*

$$\lambda_r t^{rp} + \lambda_{r-1} t^{(r-1)p} + \cdots + \lambda_1 t^p + \lambda_0.$$

Proof. Let f be an irreducible polynomial over a field K. The degree of Df is less than that of f. As f is irreducible, this means f and Df do not have a common factor of degree ≥ 1 unless $Df = 0$. So by (64), f is inseparable if and only if $Df = 0$, i.e., if and only if $ia_i = 0$ for all $i \geq 0$, where

$$f = a_n t^n + \cdots$$

If K has characteristic 0 this doesn't occur because $ia_i = 0$ implies $a_i = 0$ for all $i > 0$. If the characteristic of K is p then this occurs if and only if $a_i = 0$ whenever i is not a multiple of p. □

Definition 66. *A polynomial over K is* separable *if all its irreducible factors are separable. An algebraic element α in an extension field L over K is* separable *over K if its minimal polynomial over K is separable over K. An algebraic extension $L \supset K$ is* separable *if every $\alpha \in L$ is separable over K.*

Lemma 67. *Let $L \supset M \supset K$ be a tower of field extensions and suppose $L \supset K$ is a separable algebraic extension. Then $M \supset K$ and $L \supset M$ are separable algebraic extensions as well.*

Proof. Clearly $M \supset K$ is separable. If $\alpha \in L$, let m_M and m_K be its minimal polynomial over M and K. Then m_M divides m_K in $M[t]$. So m_K separable implies m_M separable. □

9. Galois $\Longleftrightarrow$Normal +Separable.

Given an extension $L \supset K$, we want to construct K-automorphisms of L. We do this by building up automorphisms through intermediate fields $L \supset M \supset K$. This motivates the following.

Definition 68. *Let M and L be fields containing K. A K-monomorphism from M into L is a monomorphism $\phi : M \to L$ such that $\phi(x) = x$ for all $x \in K$.*

Lemma 69. *Let $L \supset M \supset K$ be a tower of fields such that $L \supset K$ is a finite normal extension, and let $\tau : M \to L$ be a K-monomorphism. Then there exists a K-automorphism $\sigma : L\widetilde{\to}L$ with $\sigma|_M = \tau$.*

Proof. By Theorem 61, L is a splitting field over K for some $f \in K[t]$. Therefore it is a splitting field for f over M and over $\sigma(M)$. As $\tau(f) = f$, the desired result follows from Prop. 59. □

Proposition 70. *Let $L \supset K$ be a finite normal extension and let $\alpha, \beta \in L$ be zeroes of an irreducible polynomial $f \in K[t]$. Then there exists a K-automorphism $\sigma : L\widetilde{\to}L$ taking α to β.*

Proof. By Thm. 37, there exists $\tau : K(\alpha) \to K(\beta)$ such that τ is the identity on K and $\tau(\alpha) = \beta$. Then we can apply Lemma 69, view τ as monomorphism $K(\alpha) \longrightarrow L$. □

Lemma 71. *Suppose $L \supset K$ is finite. Then there exists an extension $N \supset L$ such that $N \supset K$ is normal and finite.*

Proof. Let $\alpha_1, \ldots, \alpha_n$ be a basis for L over K. Let m_i be minimal polynomial for α_i over K, and let N be a splitting field for $m = m_1 \ldots m_n$ over L. Then N is also a splitting field for m over K so is finite and normal by Thm. 61. □

Theorem 72. *Suppose $N \supset L \supset K$ is a tower of fields, with $N \supset K$ finite and normal. If $L \supset K$ is separable then there are exactly $[L : K]$ K-monomorphisms from L into N. If $L \supset K$ is inseparable then there are strictly fewer than $[L : K]$ such.*

Proof. We first consider the case where $L \supset K$ is separable. Induct on $[L : K]$. Choose $\alpha \in L - K$, and let f be the minimal polynomial of α over K so that $[K(\alpha) : K] = \delta f$ by Lemma 40. Now by Prop. 67, $L \supset K(\alpha)$ is separable, and by Lemma 62 N is a normal finite extension over $K(\alpha)$. So by induction there are $s = [L : K(\alpha)]$ distinct $K(\alpha)$-monomorphisms $\rho_1, \ldots \rho_s : L \to N$.

Now because $N \supset K$ is normal, f splits in N; let $\alpha = \alpha_1, \ldots, \alpha_r$ be the zeroes of f in N. As $L \supset K$ is separable, f is separable, so we have $r = \delta f$. So by Prop. 70 there exists K-automorphisms $\sigma_1, \ldots \sigma_r : N \widetilde{\to} N$ such that $\sigma_i(\alpha) = \alpha_i$. Now set

$$\phi_{ij} = \sigma_i \rho_j : L \to N.$$

These are $rs = (\delta f)s = [K(\alpha) : K][L : K(\alpha)] = [L : K]$ K-monomorphisms $L \to N$, and they are all distinct, for if $\phi_{ij} = \phi_{i'j'}$ then $\alpha_i = \phi_{ij}(\alpha) = \phi_{i'j'}(\alpha) = \alpha_{i'}$ implies $i = i'$, and then $\rho_j = \sigma_i^{-1}\phi_{ij} = \sigma_i^{-1}\phi_{ij'} = \rho_{j'}$ implies $j = j'$.

On the other hand if $\phi : L \to N$ is an arbitrary K-monomorphism then $\phi(\alpha) = \alpha_i$ for some i by Lemma 48. So $\sigma_i^{-1}\phi : L \to N$ is K-monomorphism and $\sigma_i^{-1}\phi(\alpha) = \alpha$ so it is actually a $K(\alpha)$-mono. Therefore it must be equal to ρ_j for some j and then $\phi = \phi_{ij}$. This completes the proof when $L \supset K$ is separable.

Now if $L \supset K$ is not separable, we use the same argument as above, but taking care to choose $\alpha \in L$ inseparable over K. Then we have $r < \delta f$ and by induction $s \leq [L : K(\alpha)]$ so the total number of K-automorphisms of L is rs which is strictly less that $[L : K]$. □

We are ready for our main theorem.

Theorem 73. *Let $L \supset K$ be a finite extension. Then $L \supset K$ is Galois if and only if it is normal and separable.*

Proof. Suppose $L \supset K$ is normal and separable. Then we can take $N = L$ in Thm. 72, to get $[L : K]$ distinct K-monomorphisms $\phi : L \to L$. But $L \supset \phi(L) \supset K$ and $[L : K] = [\phi(L) : K]$, so $L = \phi(L)$ and every K-monomorphism is actually a K-automorphism. So the Galois group of L over K has size $[L : K]$, so $L \supset K$ is Galois by Corollary 53a.

To prove the converse first use Lemma 71 to find an extension $N \supset L$ so that $N \supset K$ is normal and finite. Then we have an injective map

$$Gal(L \supset K) \longrightarrow \{K\text{-monomorphisms } L \longrightarrow N\}.$$

If $L \supset K$ is not separable then by Thm. 72 the RHS has $< [L : K]$ elements, so $L \supset K$ is not Galois by Corollary 53a.

Finally suppose $L \supset K$ is separable but not normal. By Thm 72 there are $[L : K]$ monos $L \longrightarrow N$, which are given by certain ϕ_{ij}'s described in its proof. As $L \supset K$ is not normal we can choose α so that $\alpha_i \notin L$ for some i. Then for all j, $\phi_{ij}(\alpha) = \alpha_i \notin L$ so ϕ_{ij} is not a K-automorphism of L. So by Cor. 53a again $L \supset K$ is not Galois. □

So if $L \supset K$ is a finite extension, we have 3 equivalent ways of defining Galoisness:
(1) (fixed fields) the fixed field of $Gal(L \supset K)$ is K.
(2) (numerical) $|Gal(L \supset K)| = [L : K]$
(3) (zeros of polynomials) $L \supset K$ is normal and separable.

Lemma 74. *If $L \supset K$ is a finite Galois extension, and $L \supset M \supset K$, then $L \supset M$ is Galois as well.*

Proof. By Thm. 73 just need that finite normal separable $L \supset K$ implies same for $L \supset M$. Just use Lemmas 62 and 67. □

Proposition 75. *If $L = K(\beta_1, \ldots, \beta_n)$ where each β_i is separable algebraic over K, then $L \supset K$ is a separable extension.*

Proof. Let $N \supset L$ be an extension so that $N \supset K$ is finite normal (provided by Lemma 71). Without knowing that $L \supset K$ is a separable extension we can use the argument in the proof of Thm. 72, always taking α to be one of β_i's, to construct $[L : K]$ monos $L \longrightarrow N$. So by Thm. 72 the extension $L \supset K$ is separable. □

10. The fundamental theorem

Recall the following situation from an earlier section. We consider a field L and its group of automorphisms $Aut(L)$. If K is any subfield of L, we define $K^* = Gal(L \supset K)$, the group of K-automorphisms of L (the Galois group of L over K). Conversely given any subgroup G of $Aut(L)$, we define the fixed field $G^\dagger = L^G \subset L$. These two operations have nice properties with respect to each other. In particular they induce an inclusion reversing bijections between subfields $im(\dagger)$ and $im(*)$.

Now is fix a subfield K of L, such that $L \supset K$ is finite and Galois.

We let $G = K^* = Gal(L \supset K)$. If $L \supset M \supset K$ then $M^* \subset K^* = G$. Conversely, if $H \subset G$, then $H^\dagger \supset G^\dagger = K$. So from now on we can think of $*$ as a map from the set of fields between L and K to the set of subgroups of G, and $\dagger$ as a map in the other direction.

Theorem 76. *(Galois correspondence)*

1. *$*$ and $\dagger$ induce inverse, inclusion-reversing bijections between intermediate fields M (i.e. fields M such that $L \supset M \supset K$) and subgroups of $G = Gal(L \supset K)$.*
2. *If M is an intermediate field then $[L : M] = |M^*|$ and $[M : K] = |G|/|M^*|$.*
3. *If M is an intermediate field then $M \supset K$ is a normal extension if and only if $M^*$is a normal subgroup of G. And in this case $Gal(M \supset K) \cong G/M^*$.*

By the above arguments $*$ and $\dagger$ induced bijections between intermediate fields M such that $L \supset M$ is Galois and all subgroups of G. But for *any* intermediate field, $L \supset M$ is Galois because $L \supset K$ is Galois, by (74). This proves the first statement.

If $L \supset M$ is Galois then $[L : M] = |M^*|$ by (53a), and $[M : K] = [L : K]/[L : M] = |G|/|M^*|$. So the second statement holds.

To prove the third we need a lemma.

Lemma 77. *Let $L \supset K$ be a field extension, M an intermediate field, τ a K-automorphism of L. Then $(\tau(M))^* = \tau M^* \tau^{-1}$.*

Proof. Suppose $\sigma \in M^*$. Then for all $x \in M$, $\tau\sigma\tau^{-1}(\tau(x)) = \tau\sigma(x) = \tau(x)$; thus $\tau\sigma\tau^{-1} \in \tau(M)^*$. Hence $\tau M^* \tau^{-1} \subset (\tau(M))^*$. Replacing M by $\tau(M)$ and τ by τ^{-1} in this argument, we get $\tau^{-1}(\tau(M))^*\tau \subset M^*$ which implies $(\tau(M))^* \subset \tau(M)^*\tau^{-1}$. □

Suppose M is an intermediate field and $M \supset K$ is normal. Let $\tau \in G$. If $x \in M$ and x has minimal polynomial f over K, then $\tau(x)$ is a zero of f, so by normality, we have $\tau(x) \in M$. So we've shown $\tau(M) \subset M$. As $[\tau(M) : K] = [M : K]$ we have $\tau(M) = M$. So by the lemma $\tau M^* \tau^{-1} = (\tau(M))^* = M^*$. Hence M^* is normal in G.

On the other hand, if $M \supset K$ is not normal, there exists an irreducible polynomial f over K which has a root α in M but does not split over M. As $L \supset K$ is normal f splits in L, so it has a zero β in L which is not in M. By Prop. 70 there exists a K-automorphism $\tau : L \to L$ such that $\tau(\alpha) = \beta$. We have $\tau(M) \neq M$, so $M^* \neq (\tau(M))^* = \tau M^* \tau^{-1}$, and $M^*$is not normal.

Given any $\tau \in G$, define $\phi(\tau) = \tau|_M : M \to M$, so $\phi : G \to Gal(M \supset K)$. This is clearly a group homomorphism. It is surjective by Lemma 69. And its kernel is clearly M^*, so by standard group theory, $G/M^* \cong Gal(M \supset K)$.

Now suppose that $M \supset K$ is a not necessarily normal extension. Recall that $N(H)$, the *normalizer* of a subgroup $H \subset G$ is the collection of all elements $g \in G$ for which $gHg^{-1} = H$. Then $N(H)$ is a subgroup in G and H is a normal subgroup in $N(H)$. We have the following addendum to Theorem 76. Its proof is almost verbatim a repetition of that of part 3 of Theorem 76.

Proposition 78. $Gal(M \supset K) \cong N(M^*)/M^*$.

Proof. Given any $\tau \in N(M^*) \subset G = Gal(L \supset K)$ define $\phi(\tau) = \tau|_M$. Since conjugating by the element τ maps M^* into itself the automorphism τ maps M into itself. Thus, ϕ determines a homomorphism of groups $N(M^*) \to Gal(M \supset K)$. By Lemma 69 any K-automorphism of M comes from an automorphism of L, but a K-automorphism of L mapping M into itself must belong to $N(M^*)$. Therefore ϕ is surjective and its kernel is clearly M^* which finishes the proof. □

11. The fundamental theorem as an equivalence of categories

This section contains a reformulation of Fundamental Theorem 76 as an equivalence between certain categories. This reformulation is not hard, but uses some concepts which may be new to you. Therefore this material is optional.

First suppose that $L \supset K$ is a (finite) Galois extension with Galois group G. Let us introduce the category Int whose objects are the intermediate fields, i.e. the fields M which are included in the following tower of field extensions: $L \supset M \supset K$. A morphism $M \to M'$ in Int is a K-monomorphism of fields $M \to M'$.

Further denote by $Sub(G)$ the category whose objects are the subgroups of G. Let H_1 and H_2 be two objects in $Sub(G)$. For every element $g \in G$ such that $g^{-1}H_1g$ is a subgroup of H_2 we put an arrow $H_1 \to H_2$. Two elements $g, \tilde{g}$ determine the same morphism if $g^{-1}\tilde{g} \in H_2$.

The category $Sub(G)$ is built from $\mathcal{S}G$ consisting of subgroups of G and inclusions by adding some extra morphisms, namely conjugations by the elements in G, In particular, there are nontrivial isomorphisms between different subgroups of G.

The category $Sub(G)$ might look artificial, but it is equivalent to the much more natural category of transitive G-sets GS which we now describe. The set S with an action of G is called *transitive* if for any $s_1, s_2 \in S$ there exists $g \in G$ such that $gs_1 = s_2$. A morphism between two G-sets S_1 and S_2 is a map of sets $f : S_1 \to S_2$ such that for any $s \in S_1$ $f(gs) = sf(g)$.

Example 79. *Let H be a subgroup in G. Then the set of right cosets G/H is a transitive G-set. Indeed, for a coset $gH \in G/H$ and $g' \in G$ set $g'(gH) = g'gH$.*

Exercise 80. *Check that the action of G on G/H is transitive.*

Recall that the *stabilizer* of the point s in a G-set S is the subgroup $Stab(s)$ of G consisting of those elements g for which $gs = s$. Clearly in the example above the stabilizer of the coset H is the subgroup H of G.

Exercise 81. *Show that an arbitrary transitive G-set S has the form G/H for some subgroup H in G. Show that the stabilizers of different points of a transitive G-set are conjugate subgroups in G.*

Let us consider two G-sets of the form G/H_1 and G/H_2 where H_1 and H_2 are two subgroups of G. Let f be a G-map $G/H_1 \to G/H_2$. Suppose that $f : H_1 \to gH_2$. The element g determines f since then $f(aH_1) = af(H_1) = agH_2$ where $a \in G$. However g cannot be arbitrary. Indeed, if $h \in H_1$ then $hH_1 = H_1$ and therefore $f(hH_1) = f(H_1) = gH_2 = hgH_2$ for any $h \in H_1$. Therefore $g^{-1}H_1g \subset H_2$. Conversely, if an element $g \in G$ has this property then $f : g'H_1 \to g'gH_2$ will be a G-map $G/H_1 \to G/H_2$.

Exercise 82. *Show that the elements $g, \tilde{g} \in G$ determine the same G-map $G/H_1 \to G/H_2$ iff $g^{-1}\tilde{g} \in H_2$. Deduce that for $H_1 = H_2 = H$ the set of all G-maps $G/H \to G/H$ will form a group under composition; this group is isomorphic to $N(H)/H$ where $N(H)$ is the normalizer of H in G.*

From this description it is clear that the category of transitive G-sets GS for a finite group G is equivalent to the category $Sub(G)$. Then we have the following form of Fundamental theorem:

Theorem 83. *Let $L \supset K$ be a Galois extension with Galois group G. Then the categories* Int *and GS are (anti-)equivalent. Namely, the functor* Int $\mapsto GS$ *associates to an intermediate field M the G-set G/M^* and the inverse functor $GS \mapsto$* Int *associates to any transitive G-set G/H the field $H^\dagger \subset L$.*

Exercise 84. *Prove this theorem.*

Remark 85. *There is an amazing analogy between the theory of covering spaces in algebraic topology and Galois theory. (Concerning covering spaces you could consult almost any book on algebraic topology, e.g. W.Massey. Algebraic topology. An introduction.) Namely, consider a pointed topological space X and the*

category $Cov(X)$ consisting of connected coverings of X. For a covering $Y \to X$ define a subgroup in $\pi_1(X)$ as the image of $\pi_1(Y)$ under p. Then (under some mild hypotheses on X) this correspondence induces an equivalence of categories $Cov(X)$ and $Sub(\pi_1(X))$. The latter category is, as we saw, equivalent to the category of transitive $\pi_1(X)$-sets. This explains many formal similarities between Galois theory and covering spaces. In some cases it is possible to establish some direct links but discussion of such matters would take us too far afield.

12. A worked-out example

Let $f(t) = t^4 - 2$ over $\mathbf{Q}$ and let K be the splitting field of f inside $\mathbf{C}$. In $\mathbf{C}$ we can factorize f as $f(t) = (t-\xi)(t+\xi)(t-i\xi)(t+i\xi)$ where ξ is a real positive fourth root of 2. Therefore $K = \mathbf{Q}(\xi, i)$. In characteristic 0 every extension is separable and K is a splitting field of f, so $\mathbf{Q} \subset K$ is a Galois extension.

By the tower law we have

$$[K : \mathbf{Q}] = [\mathbf{Q}(\xi, i) : \mathbf{Q}(\xi)][\mathbf{Q}(\xi) : \mathbf{Q}].$$

It is easy to see that the minimal polynomial of i over $\mathbf{Q}(\xi)$ is $t^2 + 1$ so $[\mathbf{Q}(\xi, i) : \mathbf{Q}(\xi)] = 2$. Further, $[\mathbf{Q}(\xi) : \mathbf{Q}] = \delta f = 4$. We conclude that $[K : \mathbf{Q}] = 2 \cdot 4 = 8$.

Consider the automorphism σ of the field K such that $\sigma(i) = i, \sigma(\xi) = i\xi$ and the automorphism τ for which $\tau(i) = -i, \tau(\xi) = \xi$ (why are these automorphisms?)

It is easy to check that various products of ξ and τ yield 8 distinct $\mathbf{Q}$-automorphisms of K:

$$1, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau.$$

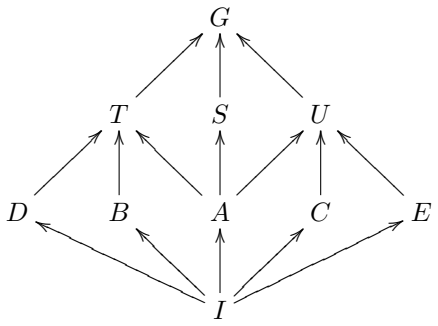
There are no more $\mathbf{Q}$-automorphisms of K since $|Gal(K/\mathbf{Q})| = 8$. So we listed all elements of $G = Gal(K/\mathbf{Q})$. Inspection shows that $\sigma^4 = \tau^2 = 1$ and $\tau\sigma = \sigma^3\tau$. It follows that $G = D_8$, the dihedral group of order 8.

Let us find the subgroups of G. First, there is the trivial subgroup I and the whole group G. The elements of order 2 are $\sigma^2, \tau, \sigma\tau, \sigma^2\tau$ and $\sigma^3\tau$. These generate cyclic subgroups of order 2 which we denote by A, B, C, D, E respectively.

The elements σ, σ^3 are the only elements of order 4, they generate the same subgroup which will be denoted by S.

The remaining subgroups of order 4 are isomorphic to $\mathbf{Z}_2 \times \mathbf{Z}_2$ and consist of the elements $\{1, \sigma^2, \tau, \sigma^2\tau\}$ and $\{1, \sigma^2, \sigma\tau, \sigma^3\tau\}$ (check this). We denote these two subgroups by T and U respectively.

Thus, we have the following diagram where the arrows denote inclusions of subgroups:



Under the Galois correspondence we obtain the intermediate fields. Let us describe them explicitly. First, there are three subfields of K of degree 2 over $\mathbf{Q}$, namely $\mathbf{Q}(i), \mathbf{Q}(\sqrt{2}), \mathbf{Q}(i\sqrt{2})$. These are the fixed fields K^S, K^T and K^U respectively.

Fields of degree 4 over $\mathbf{Q}$. The field $\mathbf{Q}(\sqrt{2}, i)$ is the only extension of $K^S = \mathbf{Q}(i)$ of degree 2 and we conclude that $K^A = \mathbf{Q}(\sqrt{2}, i)$.

The field $K^T = \mathbf{Q}(\sqrt{2})$ has three distinct extensions of degree 2: $\mathbf{Q}(\sqrt{2}, i), \mathbf{Q}(\sqrt{2}, \xi)$ and $\mathbf{Q}(\sqrt{2}, i\xi)$. These correspond to adjoining to K^T the roots of the polynomials $t^2 + 1, t^2 - \sqrt{2}$ and $t^2 + \sqrt{2}$ respectively. We have $K^B = \mathbf{Q}(\sqrt{2}, \xi) = \mathbf{Q}(\xi)$ and necessarily $K^D = \mathbf{Q}(\sqrt{2}, i\xi) = \mathbf{Q}(i\xi)$.

Similarly the field $K^U = \mathbf{Q}(i\sqrt{2})$ has three distinct extensions $\mathbf{Q}(i, i\sqrt{2}) = K^A$, $\mathbf{Q}(\xi(\frac{1}{\sqrt{2}} + \frac{i}{\sqrt{2}}), i\sqrt{2})$ and $\mathbf{Q}(\xi(\frac{i}{\sqrt{2}} - \frac{1}{\sqrt{2}}), i\sqrt{2})$. These are obtained by adjoining to K^U the roots of the polynomials $t^2 + 1, t^2 -$

$i\sqrt{2}, t^2 + i\sqrt{2}$. We have $\mathbf{Q}(\xi(\frac{i}{\sqrt{2}} + \frac{1}{\sqrt{2}}), i\sqrt{2}) = \mathbf{Q}(\xi(i-1), i\sqrt{2})) = \mathbf{Q}(\xi(i-1)) = K^E$ and the remaining field $\mathbf{Q}(\xi(\frac{1}{\sqrt{2}} - \frac{i}{\sqrt{2}}), i\sqrt{2}) = \mathbf{Q}(\xi(i+1), i\sqrt{2}) = \mathbf{Q}(\xi(i+1))$ will necessarily be K^C.

Furthermore, among the intermediate fields only T, S, U, A will be normal extensions of $\mathbf{Q}$ (why?). These completes our analysis of the extension $K \supset \mathbf{Q}$.

13. The Galois group of a polynomial.

Let $f \in K[t]$ and let L be a splitting field for f over K. Then the *Galois group* of f (over K) is defined to be the Galois group $G = Gal(L \supset K)$ of L over K. Note that this only depends on f and K, by the uniqueness of splitting fields (Prop. 59).

Let Z be the set of zeroes of f in L. Then by Lemma 48, each $\sigma \in G$ determines a permutation of Z. This gives a group homomorphism from G in the group S_Z of permutations of Z. This is injective because If $\sigma \in G$ fixes all the zeroes of f it fixes every element of L and is therefore the identity automorphism on L.

So G can be viewed as a subgroup of S_Z, i.e. as a group of permutation of the zeroes of f. For example we saw that the Galois group of $t^4 - 2$ over $\mathbf{Q}$ is the symmetry group of the square, a subgroup of the full group of permutations on the 4 zeros of $t^4 - 2$.

We record an important consequence of Prop. 70:

Proposition 86. *If f is irreducible, then G is a transitive group of permutations, that is, if α and β are zeros of $f \in L$ then there exists $\sigma \in G$ such that $\sigma(\alpha) = \beta$.*

Suppose K is a field of characteristic 0 and f is an irreducible cubic. Then $L \supset K$ is finite, separable (by Lemma 65) and normal (by Prop. 61), and hence Galois (Thm. 73). G is a transitive subgroup of S_Z of permutations of the zeros $\alpha_1, \alpha_2, \alpha_3$ of f, which may be identified with S_3. The subgroups of S_3 are S_3, $A_3 =< (123) >$, $< (12) >$, $< (23) >$, $< 13 >$, and $\{\mathrm{id}\}$. The only transitive subgroups are S_3 and A_3. So $G = S_3$ or A_3.

Consider $\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1) \in L$. If $\sigma \in G$, then $\sigma(\delta) = \pm\delta$, and $\sigma(\delta) = \delta$ if and only if $\sigma \in A_3$. So if $G = A_3$ then δ is in the fixed field of G and therefore $\delta \in K$. If $G = S_3$ then δ is not in the fixed field so $\delta \notin K$. On the other hand $\Delta = \delta^2$ is always in K, for $\sigma(\Delta) = \sigma(\delta^2) = \sigma(\delta)^2 = (\pm\delta)^2 = \Delta$.

So $G = A_3$ if and only if Δ has a square root in K.

If $G = A_3$ then $[L : K] = 3$. So $L = K(\alpha_1) = K(\alpha_2) = K(\alpha_3)$. So any zero is expressible as a polynomial in any other zero. What about intermediate fields? None, because A_3 has no nontrivial subgroups.

If $G = S_3$ then $[L : K] = 6$. Then there are three distinct intermediate fields $K(\alpha_1), K(\alpha_2), K(\alpha_3)$ of degree 3 over K, corresponding to the 3 subgroups of order 2 of S_3. (For example, take the polynomial $f = t^3 - 2$ over $\mathbf{Q}$. Then these fields are obtained by adjoining to $\mathbf{Q}$ the three roots of f.)

There should also be a intermediate field of degree 2, the fixed field of A_3. This contains and therefore is equal to $K(\delta)$. The minimal polynomial of δ is $t^2 - \Delta$.

Let $f = t^3 + at^2 + bt + c$. Can we express Δ in terms of a, b, and c? First of all the quadratic term can be eliminated by making the substitution $t \to t - a/3$. So we may assume that $f = t^3 + pt + q$, where $p, q \in K$ and try to express Δ in terms of p and q. If $f = (t - \alpha_1)(t - \alpha_2)(t - \alpha_3)$, then multiplying out we get

$$\begin{aligned} \alpha_1 + \alpha_2 + \alpha_3 &= 0 \\ \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 &= p \\ \alpha_1\alpha_2\alpha_3 &= -q \end{aligned}$$

and some calculation shows that $\Delta = -4p^3 - 27q^2$.

If we just randomly choose some irreducible cubic, chances are that Δ will not be square. So usually $G = S_3$. If $f = t^3 - 3t + 1$ then $\Delta = 81$. So the Galois group of f over $\mathbf{Q}$ is A_3 and that means $L = \mathbf{Q}(\alpha_1)$ so α_2 and α_3 are expressible as polynomials in α_1 over $\mathbf{Q}$. One can check directly that in this example $\alpha_2 = \alpha_1^2 - 2$ and $\alpha_3 = -\alpha_1^2 - \alpha_1 + 2$.

14. Some group theory

A group G is *soluble* if it is has a series

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

such that for $i = 0, \ldots, n-1$, $G_i \lhd G_{i+1}$ and G_{i+1}/G_i is abelian .

Notice that it isn't necessarily the case that $G_i \lhd G$, as the relation 'is a normal subgroup of' is not transitive.

Example 87. (1) *If G is abelian it is soluble: $1 \subset G$.*
(2) *S_3 is soluble: $1 \subset A_3 \subset S_3$.*
(3) *D_8 is soluble: $1 \subset< \sigma >\subset D_8$, or $1 \subset< \sigma^2 >\subset D_8$. This shows that the series of subgroups demonstrating solubility may not be unique.*
(4) *S_4 is soluble: $1 \subset V \subset A_4 \subset S_4$. Here A_4 is the alternating group consisting of even permutations and $V = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \cong C_2 \times C_2$. The quotients of successive terms in the series are $V/1 = V \cong C_2 \times C_2$, $A_4/V \cong C_3$, and $S_4/A_4 \cong C_2$.*

Proposition 88. *Let G be a group, H a subgroup and N a normal subgroup.*
(1) *If G soluble, then so is H.*
(2) *If G is soluble, then so is G/N.*
(3) *If N and G/N are soluble then so is G.*

Proposition 89. *If $n \geq 5$, then neither the alternating group A_n nor the symmetric group S_n is soluble. (In fact, A_n is a nonabelian simple group).*

Lemma 90. *The symmetric group S_n is generated by the n-cycle $(12\ldots n)$ and the transposition (12).*

Proof. Conjugating (12) by $(12\ldots n)$, we get $(23), (34)$,etc. Then conjugating (12) by (23) we get (13), and this by (34) we get (14), and continuing in this way we obtain every transposition of the form $(1i)$. Finally, conjugating $(1i)$ by $(1j)$ we get (ij), so every transposition, and hence all of S_n. □

Definition 91. *Let p be a prime number. A finite group G is a p-group if its order is a power of p.*

Definition 92. *The center $Z(G)$ of a group G is the set of elements of G which commute with every element of G.*

Lemma 93. *If G is a nontrivial p-group, then G has nontrivial center.*

Proof. Every conjugacy class of elements of G must have order dividing the order of G, hence must be a power of p. As G is the disjoint union of its conjugacy classes, and the conjugacy class of the identity has size 1, there must be at least p conjugacy classes of size 1, and each of these contains a central element. □

Proposition 94. *If G is a p-group of order p^n then G has a series of normal subgroups*

$$1 = G_0 \subset G_1 \subset \cdots \subset G_n = G,$$

such that $|G_i| = p^i$ for $i = 0, \ldots, n$. In particular G is soluble.

Proof. By induction on n. If $n = 0$, fine. Otherwise by Lemma 93 G has a nontrivial center $Z(G)$. By Lagrange's theorem $Z(G)$ contains an element of order p, and hence a subgroup K of order p. As K is central it is normal in G. Now G/K is a p-group of order p^{n-1}, so by induction there is a series of normal subgroups

$$K/K = G_1/K \subset G_2/K \subset \cdots \subset G/K,$$

where $|G_i/K| = p^{i-1}$. Then $|G_i| = p^i$ and $G_i \lhd G$. Taking $G_0 = 1$, we get the desired result. Each quotient G_i/G_{i+1}has order p, and is hence cyclic, and thus abelian. □

Theorem 95. *(Sylow's Theorems) Let G be a group of order $p^\alpha r$ where p is prime and p does not divide r. Then*
(1) *G has at least one subgroup of order p^α.*
(2) *All such subgroups (called Sylow p-subgroups) are conjugate in G.*
(3) *The number of Sylow p-subgroups is 1 modulo p.*

Example 96. *Let $L \supset K$ be a finite Galois extension with $[L : K] = 30$. Suppose M_1 and M_2 are intermediate fields with $[M_i : K] = 6$. By the Galois correspondence, M_1^* and M_2^* are subgroups of $G = Gal(L \supset K)$ of order 5. As G has order $[L : K] = 30$, these are Sylow 5-subgroups of G. Therefore there exists $\sigma \in G$ such that $\sigma M_1^* \sigma^{-1} = M_2^*$. Then*

$$M_2 = M_2^{*\dagger} = (\sigma M_1^* \sigma^{-1})^\dagger = \sigma(M_1^{*\dagger}) = \sigma(M_1)$$

by Thm. 95. Thus $M_1 \supset K$ and $M_2 \supset K$ are isomorphic extensions. I n particular M_1 and M_2 are isomorphic fields.

15. Solving Equations by radicals.

What is a radical expression? One which involves only the usual arithmetic operations of addition, subtraction, multiplication, division, as well as the extraction of n-th roots.

We can make this more precise:

Definition 97. *An extension $L \supset K$ is* radical *if $L = K(\alpha_1, \ldots, \alpha_n)$, where for each $i = 1, \ldots, n$, some power $\alpha_i^{r(i)}$ of α_i lies in $K(\alpha_1, \ldots, \alpha_{i-1})$.*

The sequence $\alpha_1, \ldots, \alpha_n$ is called a radical sequence *for L over K.*

Note that radical extensions are finite. Also, we can always assume that the powers $r(i)$ are prime (possibly increasing the length of the sequence).

Example 98.

(1) *Suppose $L \supset K$ is an extension of degree 2, where $char(K) \neq 2$. Choose an element β in L not in K. Then $\beta^2 + r\beta + s = 0$ for some $r, s \in K$. Let $\alpha = \beta + r/2 \in L$. Clearly $\alpha \notin K$, because $\beta \notin K$, and $\alpha^2 = \beta^2 + r\beta + r^2/4 = -s + r^2/4 \in K$. So $L = K(\alpha)$ is a radical extension of K.*

(2) *Let L be the splitting field for $f = t^3 - 2$ over $\mathbf{Q}$. Then we saw that*

$$L = \mathbf{Q}(\alpha, \omega) \supset \mathbf{Q}(\alpha) \supset \mathbf{Q}.$$

where $\alpha^3 = 2 \in \mathbf{Q}$, and $\omega^3 = 1 \in \mathbf{Q}(\alpha)$. So $L \supset \mathbf{Q}$ is radical.

Definition 99. *Let f be a polynomial over K, a field of characteristic 0. We say that f is* soluble by radicals *if there is a radical extension of K in which f splits.*

Note that this does not necessarily mean that a splitting field for f has to be a radical extension; only that a splitting field is contained is some radical extension. For example if L is a splitting field for $f = t^3 - 3t + 1$ over $\mathbf{Q}$, then $L \supset \mathbf{Q}$ is *not* radical, but $L(\omega) \supset \mathbf{Q}$ is, where $\omega^3 = 1$.

The main theorem of this section is the following.

Theorem 100. *Let K be a field of characteristic zero, and let L be a finite normal (and hence Galois) extension of K. Then $G = Gal(L \supset K)$ is soluble if and only if there is an extension M of L such that $M \supset K$ is a radical extension.*

Corollary 101. *A polynomial f is soluble by radicals if and only if its Galois group is a soluble group.*

Lemma 102. *Let $L \supset K$ is a finite extension and M is a normal closure of $L \supset K$. Then M is generated by subfields $L_1, \ldots, L_r$ containing K, such that each extension $L_i \supset K$ is isomorphic to $L \supset K$.*

Proof. . $L = K(\alpha_1, \ldots, \alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in L$, algebraic over K. Let m_i be the minimal polynomial of α_i. Let N be a splitting field for $m = m_1 \ldots m_n$ over L. Then by proof of Lemma 71, N is a normal closure of $L \supset K$. As normal closures are unique (Lemma 71), we may assume that $M = N$. If β_i is any root of m_i, then by Prop. 70 exists K-auto σ of N taking α_i to β_i So $\sigma(L) \supset K$ is an extension isomorphic to $L \supset K$, and $\sigma(L)$ contains β_i. Carrying out this procedure we get any root of any m_i in some extension $\sigma(L)$ where σ is K-auto. The statement follows. □

Lemma 103. *If $L \supset K$ is radical then there exists $N \supset L$ such that $N \supset K$ is normal and radical.*

Proof. Let $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$ be as in Definition 97. Let N be a splitting field for $m = m_1 \cdots m_n$ over L. Then N is also a splitting field for m over K and hence $N \supset K$ is a normal extension by Thm. 61. Let $\sigma_1, \ldots, \sigma_r$ be the elements of $Gal(N \supset K)$. Then by Prop. 70 the sequence

$$\sigma_1(\alpha_1), \sigma_1(\alpha_2), \ldots, \sigma_1(\alpha_n); \sigma_2(\alpha_1), \ldots, \sigma_2(\alpha_n); \ldots; \sigma_r(\alpha_1), \ldots, \sigma_r(\alpha_n)$$

contains all the zeros of m and furthermore is a radical sequence for N over K, because $\sigma_j(\alpha_i)^{r(i)} \in K(\sigma_j(\alpha_1), \ldots \sigma_j(\alpha_{i-1}))$. □

Lemma 104. *Let K be a field of characteristic 0. Let L be a splitting field for $t^p - 1$ over K, where p is prime. Then the Galois group of $L \supset K$ is abelian.*

Proof. As we are in characteristic 0, $t^p - 1$ is separable (Lemma 65), so has p distinct zeroes. Now if α and β are zeroes of $t^p - 1$, then so are $\alpha\beta$ and α^{-1}. So the zeroes of $t^p - 1$ form a group under multiplication. This must be cyclic group of order p; choose a generator ω. Then $L = K(\omega)$, so that every K-automorphism σ of L is determined by its effect on ω. If $\sigma(\omega) = \omega^i$ and $\tau(\omega) = \omega^j$, then it is easy to check that both $\sigma\tau$ and $\tau\sigma$ send ω to ω^{ij}, so must be equal. Hence $Gal(L \supset K)$ is abelian. □

Lemma 105. *Suppose K is a field of characteristic 0 in which $t^n - 1$ splits. Let L be a splitting field for $t^n - a$ over K, where $a \in K$. Then $Gal(L \supset K)$ is abelian.*

Proof. Let α be a zero of $t^n - a$ in K. If β is another zero, then $\varepsilon = \alpha^{-1}\beta$ is a zero of $t^n - 1$. Thus $\beta = \varepsilon\alpha \in K(\alpha)$. Hence $L = K(\alpha)$ and any K-automorphism σ of L is determined by its value on α. Now if $\sigma, \tau \in Gal(L \supset K)$,and $\sigma(\alpha) = \varepsilon\alpha$ and $\tau(\alpha) = \eta\alpha$, where ε and η are zeros of $t^n - 1$ and hence are elements of K, then $\sigma\tau(\alpha) = \sigma(\eta\alpha) = \eta\sigma(\alpha) = \eta\varepsilon\alpha$, while $\tau\sigma(\alpha) = \varepsilon\eta\alpha$, so $\sigma\tau$ and $\tau\sigma$ agree on α and are hence equal. Thus $Gal(L \supset K)$ is abelian. □

Now we are ready to prove the 'if' half of Thm. 100. We assume that $M \supset L \supset K$ is a tower of extensions, where K has characteristic zero, $L \supset K$ is normal and $M \supset K$ is radical. By Lemma 103 we may assume that M is a normal extension of K. Then the Galois correspondence applies to the Galois extension $M \supset K$. The Galois group of $L \supset K$ is a quotient of the Galois group of $M \supset K$, so by Prop. 88 it suffices to show that $G = Gal(M \supset K)$ is soluble.

We write $M = K(\alpha_1, \ldots, \alpha_n)$ as in Definition 99, with $\alpha_i^{r(i)} \in K(\alpha_1, \ldots, \alpha_{i-1})$ for $i = 1, \ldots, n$. Following the remark after Def. 97, we may assume that all the $r(i)$'s are prime. In particular $\alpha_1^p \in K$ for some prime p.

We induct on the number n. If $\alpha_1 \in K$ then $M = K(\alpha_2, \ldots, \alpha_n)$ and we are done by induction. Otherwise let m_1 be the minimal polynomial of α_1 over K. It divides $t^p - \alpha_1^p$, has degree at least 2, and because M is normal over K, m has another zero $\beta_1 \in M$ with $\beta_1 \neq \alpha_1$. Then $\alpha_1^p = \beta_1^p$ so $\varepsilon = \alpha_1\beta_1^{-1} \neq 1$ is a zero of $t^p - 1$ in M. By the proof of Lemma 104 $K(\varepsilon)$ is a splitting field for $t^p - 1$ over K and by Lemma 104 itself $Gal(K(\varepsilon) \supset K)$ is abelian. Next, by the proof of Lemma 105, $K(\varepsilon, \alpha_1)$ is a splitting field for $t^p - \alpha_1^p$ over $K(\varepsilon)$, and $Gal(K(\varepsilon, \alpha_1) \supset K(\varepsilon))$ is abelian.

By the Galois correspondence (Thm. 76), $Gal(K(\varepsilon, \alpha_1) \supset K(\varepsilon))$ is a normal subgroup of $Gal(K(\varepsilon, \alpha_1) \supset K)$ with quotient isomorphic to $Gal(K(\varepsilon) \supset K)$. Thus by Prop. 88, $Gal(K(\varepsilon, \alpha_1) \supset K)$ is soluble.

Now $M = K(\varepsilon, \alpha_1)(\alpha_2, \ldots, \alpha_n)$. So by induction $Gal(M \supset K(\varepsilon, \alpha_1))$ is soluble. and by the Galois correspondence $Gal(M \supset K(\varepsilon, \alpha_1))$ is a normal subgroup of $Gal(M \supset K)$ with quotient isomorphic to $Gal(K(\varepsilon, \alpha_1) \supset K)$. Therefore by Prop. 88 again, $Gal(M \supset K)$ is soluble.

Proposition 106. *Let p be a prime, and f an irreducible polynomial of degree p over $\mathbf{Q}$. Suppose that f has precisely 2 nonreal zeros in $\mathbf{C}$. Then the Galois group of f over $\mathbf{Q}$ is the symmetric group S_p.*

Proof. By the fundamental theorem of algebra, $\mathbf{C}$ contains a splitting field L for f over $\mathbf{Q}$. Let G be the Galois group of L over $\mathbf{Q}$, viewed as a group of permutations of the zeros of f in L (as in section 8). By Lemma 65 f has p distinct roots, so G is a subgroup of S_p. Let α be a zero of f in L. Then $L \supset K(\alpha) \supset K$, and $[K(a) : K] = p$, so p divides $|G| = [L : K]$. As $S_p = p!$, a Sylow p-subgroup of G has order p. Thus G has an element of order p, so must contain a p-cycle. Complex conjugation restricts to a $\mathbf{Q}$-automorphism of L which fixes the $p - 2$ real zeros and interchanges the other two zeros. So G contains a 2-cycle. By

reordering the zeroes and taking a power of the p-cycle, we may assume G contains (12) and (12...p). Then by Prop. 89, $G = S_p$, as desired. □

Example 107. *Let $f = t^5 - 6t + 3 \in \mathbf{Q}[\mathbf{t}]$. This is an irreducible by Eisenstein's criterion (Thm. 20). We have $f(-2) = -17$, $f(-1) = 8$, $f(1) = -2$, and $f(2) = 23$, so by the Intermediate value theorem, f has at least 3 real zeros. On the other hand $df/dt = 5t^4 - 6$ has only 2 real zeros, namely $\pm\sqrt[4]{6/5}$, so by Rolle's Theorem f has at most 3 real zeros. So f has precisely 2 nonreal zeros, and therefore by (106) has Galois group S_5 over $\mathbf{Q}$. But by Prop. 89 S_5 is not soluble, so by Cor. 101 f is not soluble by radicals.*

Now we work our way towards a proof of the 'only if' implication in Thm. 100.

Lemma 108. *Let K be a field of characteristic not equal to p, and let $L \supset K$ be a finite Galois extension of prime degree p. Suppose that $t^p - 1$ splits in K. Then $L = K(\beta)$ where β is a zero of an irreducible polynomial $t^p - \theta$, for some $\theta \in K$. In particular $L \supset K$ is a radical extension.*

Proof. Let $\omega \neq 1$ be a zero of $t^p - 1$ in K (this exists by Lemma 65 as the characteristic is not p). Choose $\sigma \neq 1$ in $G = Gal(L \supset K)$. Then $1, \sigma, \ldots \sigma^{p-1}$ are distinct K-automorphsism of L, so by Dedekind's Theorem (Lemma 54), these are linearly independent over K, so $1 + \omega\sigma + \omega^2\sigma^2 + \cdots + \omega^{p-1}\sigma^{p-1} \neq 0$. Thus there exists $\alpha \in L$ such that $\beta = \alpha + \omega\sigma(\alpha) + \omega^2\sigma^2(\alpha) + \cdots + \omega^{p-1}\sigma^{p-1}(\alpha) \neq 0$.

Now

$$\begin{aligned}\sigma(\beta) &= \sigma(\alpha) + \omega\sigma^2(\alpha) + \cdots + \omega^{p-2}\sigma^{p-1}(\alpha) + \omega^{p-1}\alpha \\ &= \omega^{-1}(\omega\sigma(\alpha) + \omega^2\sigma^2(\alpha) + \cdots + \omega^{p-1}\sigma^{p-1}(\alpha) + \alpha) \\ &= \omega^{-1}\beta.\end{aligned}$$

So $\beta \notin K$, but $\sigma(\beta^p) = \sigma(\beta)^p = \omega^{-p}\beta^p = \beta^p$. As the extension is Galois, we get $\theta = \beta^p \in K$. Now $L \supset K(\beta) \supset K$, and $[L : K] = p$, so $[K(\beta) : K] = p$. Therefore the minimal polynomial of β over L has degree p, and therefore $t^p - \theta$ is the minimal polynomial of β and is therefore irreducible. □

Finally, we prove the 'only if' implication in Thm. 100: Let K be a field of characteristic zero. Let $L \supset K$ be a finite normal extension with soluble Galois group G. Our aim: find a extension $M \supset L$ such that $M \supset K$ is a radical extension.

We induct on the order of G. If $G = 1$ fine. Otherwise let H be a maximal proper normal subgroup. Then G/H is abelian and simple, and is therefore a cyclic group of order p, where p is some prime. In order to apply Lemma 108 we need p-th roots of 1.

So let $\tilde{L}$ be a splitting field for $t^p - 1$ over L, and let $\tilde{K}$ be the subfield of $\tilde{L}$ generated by K and the zeros of $t^p - 1$, so that $\tilde{K}$ is a splitting field for $t^p - 1$ over K. Now $\tilde{K}$ is radical over K so it suffices to find an extension $M \supset \tilde{L}$ such that $M \supset \tilde{K}$ is radical.

Note that $\tilde{L}$ is obtained from K by first adjoining all roots of a certain polynomial f (to get L) and then adjoining pth roots of unity. It is thus a splitting field of the polynomial $f(t^p - 1)$ and therefore normal. This in turn implies that $\tilde{L}$ is normal over $\tilde{K}$.

We now show that $\tilde{G} = Gal(\tilde{L} \supset \tilde{K})$ is a subgroup of $G = Gal(L \supset K)$. If $\sigma \in \tilde{G}$ then $\sigma(L) = L$ because $L \supset K$ is normal, and σ fixes every element of K, so by restriction we get a group homomorphism $\phi : \tilde{G} \longrightarrow G$. This is injective: if $\phi(\sigma) = \mathrm{id}$, then σ fixes every element of L; But σ also fixes every element of $\tilde{K}$, and as $\tilde{L}$ is generated by L and $\tilde{K}$, this would imply that σ fixes every element of $\tilde{L}$.

Thus ϕ is injective. If ϕ is not surjective, then $\tilde{L} \supset \tilde{K}$ is a finite normal extension and $\tilde{G}$ is a soluble group of order strictly less than G, so by induction we are done.

If ϕ is surjective, then let $I = \phi^{-1}(H)$, so that I is a normal subgroup of $\tilde{G}$ of index p. Let $I^\dagger$be the fixed field of I in $\tilde{L}$. Then the Galois correspondence (Thm. 76) tells us that $I^\dagger \supset \tilde{K}$ is a Galois extension with Galois group $\tilde{G}/I$, which has order p. Thus by Lemma 108 $I^\dagger \supset \tilde{K}$ is a radical extension. Now also by the Galois correspondence $\tilde{L} \supset I^\dagger$is a normal extension with Galois group I soluble of order strictly less than G. So by induction there exists $M \supset \tilde{L}$ such that $M \supset I^\dagger$is radical. But then $M \supset \tilde{K}$ is radical.

Theorem 109. *Let f be a polynomial of degree ≤ 4 over a field of characteristic 0. Then f is soluble by radicals.*

Proof. The Galois group G of f is a subgroup of S_n where $n \leq 4$. As these are soluble groups, and any subgroup of a soluble group is soluble by Prop. 88, G is soluble. So by Thm. 100 f is soluble by radicals. □

16. Cubics.

Let K be a field of characteristic 0.

Let f be a monic polynomial of degree 3 over K.

Let L be a splittiing field for f over K. Suppose that $f = (t-\alpha_1)(t-\alpha_2)(t-\alpha_3)$ in L. We try to give radical expressions for these zeroes, by following the proof of (Thm 100). First of all, to carry this out we need a cube root of 1. So adjoint an element $\omega \neq 1$, $\omega^3 = 1$. Then $L(\omega)$ is the splitting field for f over $K(\omega)$. Let G be the Galois group of $L(\omega) \supset K(\omega)$. Then G is a subgroup of the permutation group on $\{\alpha_1, \alpha_2, \alpha_3\}$ which is S_3. Let $H = G \cap A_3$. Then $1 \lhd H \lhd G$, and $H = 1$ or A_3 and $G/H \cong 1$ or C_2.

Following the proof of Thm. 100 we consider $K(\omega) \subset H^\dagger \subset L(\omega)$. By 108 both $K(\omega) \subset H^\dagger$ and $H^\dagger \subset L(\omega)$ should be radical extensions.

Now $H = 1$ or A_3, so looking at proof of Lemma 108 we set

$$\beta = \alpha_1 + \omega\alpha_2 + \omega^2\alpha_3$$

and

$$\gamma = \alpha_1 + \omega^2\alpha_2 + \omega\alpha_3.$$

(Taking $\alpha = \alpha_1$, and $\sigma = (123)$ or (132).)

We have $\beta^3, \gamma^3 \in H^\dagger$ and $[H^\dagger : K(\omega)] = 1$ or 2, so they are zeroes of quadratics over $K(w)$. In fact $(t-\beta^3)(t-\gamma^3) = t^2 - (\beta^3+\gamma^3)t + \beta^3\gamma^3$, and the coefficients of this quadratic are in K, because any permutation of $\alpha_1, \alpha_2, \alpha_3$ either fixes or interchanges β^3 and γ^3.

So we can get β and γ by first adjoining the zeroes of $t^2 - (\beta^3+\gamma^3)t + \beta^3\gamma^3$ to $K(\omega)$ and then adjoining cube roots of these zeroes. Then the zeroes of f can be expressed in terms of β and γ.

Suppose $f = t^3 + mt - n$. Then

$$\begin{aligned} \alpha_1 + \alpha_2 + \alpha_3 &= 0. \\ \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 &= m. \\ \alpha_1\alpha_2\alpha_3 &= n. \end{aligned}$$

So

$$\begin{aligned} \beta\gamma &= \alpha_1^2 + \alpha_2^2 + \alpha_3^2 + (\omega+\omega^2)(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1) \\ &= (\alpha_1+\alpha_2+\alpha_3)^2 - 3(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1) \\ &= -3m. \end{aligned}$$

and $\beta^3\gamma^3 = -27m^3$.

Next

$$\begin{aligned} \beta^3 + \gamma^3 &= (\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3)^3 + \left(\alpha_1 + \omega^2\alpha_2 + \omega\alpha_3\right)^3 + (\alpha_1+\alpha_2+\alpha_3)^3 \\ &= 3(\alpha_1^3 + \alpha_2^3 + \alpha_3^3) + 18\alpha_1\alpha_2\alpha_3 \\ &= 3[(\alpha_1+\alpha_2+\alpha_3)^3 - 3(\alpha_1+\alpha_2+\alpha_3)(\alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1) \\ &+ 3\alpha_1\alpha_2\alpha_3] + 18\alpha_1\alpha_2\alpha_3 \\ &= 27n. \end{aligned}$$

So β^3 and γ^3 are zeros of $t^2 - 27nt - 27m^3$, which are

$$27\left(\frac{n}{2} \pm \sqrt{\frac{n^2}{4} + \frac{m^3}{27}}\right).$$

So

$$\beta, \gamma = 3\sqrt[3]{\frac{n}{2} \pm \sqrt{\frac{n^2}{4} + \frac{m^3}{27}}},$$

where the cube roots are chosen so that $\beta\gamma = -3m$. And

$$\begin{aligned}\alpha_1 &= \frac{1}{3}\left[\left(\alpha_1 + \omega\alpha_2 + \omega^2\alpha_3\right) + \left(\alpha_1 + \omega^2\alpha_2 + \omega\alpha_3\right) + (\alpha_1 + \alpha_2 + \alpha_3)\right] \\ &= \frac{1}{3}(\beta + \gamma),\end{aligned}$$

which gives Cardano's formula. Similarly $\alpha_2 = \frac{1}{3}(\omega^2\beta + \omega\gamma)$ and $\alpha_2 = \frac{1}{3}(\omega\beta + \omega^2\gamma)$.

Note that we are always working in $L(\omega)$, so β and γ actually may not be in L. This is the case for example for $f = t^3 - 3t + 1$ over $\mathbf{Q}$, a case where the Galois group is A_3.

17. Quartics

Let K be a field of characteristic zero, and $f \in K[t]$ be a polynomial of degree 4 over K. Let $L = K(f)$ be the splitting field of f. Then L/K is a Galois extension with the Galois group $G(f) = Gal(L/K)$.

Our first aim is to compute $G = G(f)$.

Assume that all four roots of f (in $K(f)$) are different. For example, it will be so, if f is irreducible. Then $G(f)$ acts on the set of roots, and is a subgroup of $S_{\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}} \cong S_4$. Let us first study the possible subgroups of S_4. Since $|S_4| = 4! = 24$, the size of the subgroup $H \subset S_4$ should be one of the numbers: $1, 2, 3, 4, 6, 8, 12, 24$. The following table lists all possible subgroups **up to conjugation**:

(1) 1 - trivial subgroup;
(2) $\mathbb{Z}/2 = \{Id, (12)\}$ - there are 6 such;
(3) $\mathbb{Z}/2 = \{Id, (12)(34)\}$ - there are 3 such;
(4) $\mathbb{Z}/3 = \{Id, (123), (132)\}$ - there are 4 such;
(5) $\mathbb{Z}/2 \times \mathbb{Z}/2 = \{Id, (12), (34), (12)(34)\}$ - there are 3 such;
(6) $\mathbb{Z}/2 \times \mathbb{Z}/2 = V_4 = \{Id, (12)(34), (13)(24), (14)(23)\}$ - only one such;
(7) $\mathbb{Z}/4 = \{Id, (1234), (13)(24), (1432)\}$ - there are 3 such;
(8) $S_3 = S_{\{1,2,3\}}$ - there are 4 such;
(9) D_8 - the Dihedral group, generated by V_4, and by one elementary permutation (say (12))- there are 3 such;
(10) A_4 - the subgroup of even permutations;
(11) S_4 itself.

Remark 110. *Below we will see that there is polynomial f of degree 4 with the Galois group S_4 (infact, the generic polynomial will be of this sort, so it is very easy to produce such examples). This shows that all the above subgroups are realised as the Galois groups of the same polymial but over other ground fields. Indeed, if $L = K(f)$ is a splitting field of f, and $H \subset Gal(L/K)$ is arbitrary subgroup, then by the Main theorem of Galois theory, $Gal(L/L^H) = H$, while L is a splitting field of f over L^H as well.*

Notice, that among the listed subgroups only $1, V_4, A_4$ and S_4 are normal. And the *solving tower* for S_4 is exactly $1 \lhd V_4 \lhd A_4 \lhd S_4$. Intersecting this tower with G we get the *solving tower* for G: $1 \lhd (G \cap V_4) \lhd (G \cap A_4) \lhd G$. Due to the Main Theorem of Galois theory (Theorem 76), one obtains the dual tower of subfields: $L \supset L^{(G\cap V_4)} \supset L^{(G\cap A_4)} \supset K$. How to describe $L^{(G\cap A_4)}$ and $L^{(G\cap V_4)}$? The description of the first one comes from the general statement:

Proposition 111. *Let $f \in K[t]$ be polynomial of degree n over the field of characteristic 0 having pairwise different roots α_i. Let $\delta = \prod_{i<j}(\alpha_i - \alpha_j)$, and $\Delta = \delta^2$. Then $L^{(G(f)\cap A_n)} = K(\delta) = K(\sqrt{\Delta})$.*

Proof. For arbitrary $\sigma \in S_n$, we have: $\sigma(\delta) = (-1)^{sgn(\sigma)}\delta$. Since $\delta \neq 0$, we get: for arbitrary $g \in G(f)$, $g(\delta) = \delta$ if and only if $g \in A_n$. Thus, $Gal(L/K(\delta)) = G(f) \cap A_n = Gal(L/L^{G(f)\cap A_n})$. By the Main theorem of Galois theory (Theorem 76), $K(\delta) = L^{G(f)\cap A_n}$. □

In particular, we get that $Gal(K(\sqrt{\Delta})/K) = G(f)/(G(f) \cap A_n)$, and so $G(f)$ belongs to A_n if and only if the *discriminant* $\Delta(f)$ is a square in K.

To describe the second extension, let us introduce the elements

$$u = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4),\ \ v = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4),\ \text{ and }\ w = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)\ \text{ in }\ L.$$

The first observation is that, under our conditions, u, v and w are pairwise different. Indeed, $(u-v) = (\alpha_1-\alpha_4)(\alpha_3-\alpha_2)$, $(u-w) = (\alpha_1-\alpha_3)(\alpha_4-\alpha_2)$, and $(v-w) = (\alpha_1-\alpha_2)(\alpha_4-\alpha_3)$. Next, any permutation of $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ gives the permutation of u, v, w, and we get the group homomorphism: $S_{\{\alpha_1,\alpha_2,\alpha_3,\alpha_4\}} \to S_{\{u,v,w\}}$. Clearly, this homomorphism is surjective, and the kernel is $V_4 \subset S_4$. Thus, the element $g \in G(f)$ belongs to V_4 if and only if it acts identically on u, v, w, or, which is the same, it acts identically on $K(u, v, w)$. So, we obtain the following:

Proposition 112. *In our situation,* $L^{G(f)\cap V_4} = K(u, v, w)$.

Proof. Indeed, we saw that $Gal(L/K(u, v, w)) = G(f)\cap V_4 = Gal(L/L^{G(f)\cap V_4})$. Thus, $L^{G(f)\cap V_4} = K(u, v, w)$. □

In particular, $Gal(K(u, v, w)/K) = G(f)/(G(f) \cap V_4)$. On the other hand, u, v and w are roots of the polynomial $(t-u)(t-v)(t-w)$, which is stable under all permutations from S_4, and hence, under G, so should have coefficients in K. Thus, $K(u, v, w)$ is just the splitting field of some cubic polynomial $g(t)$, called *cubic resolvent*. Let us find this polynomial. We have: $g(t) = t^3 - (u+v+w)t^2 + (uv+vw+wu)t - uvw$. Hence, the coefficients of g are symmetric functions in $\alpha_1, \alpha_2, \alpha_3, \alpha_4$, and by the Theorem on Symmetric Functions are polynomials in *elementary symmetric functions* $s_1(\alpha), \dots, s_4(\alpha)$. Up to sign, $s_1(\alpha), \dots, s_4(\alpha)$ are just the coefficients of f at t^3, t^2, t, and 1.

From this point, let us assume that f has no t^3-term (one can always reduce to such a case, and the reduction does not change the Galois group), and is given by: $f(t) = t^4 + qt^2 + rt + s$. Then $s_1(\alpha) = \alpha_1+\alpha_2+\alpha_3+\alpha_4 = 0$, $s_2(\alpha) = \prod_{i<j}\alpha_i\alpha_j = q$, $s_3(\alpha) = \prod_{i<j<k}\alpha_i\alpha_j\alpha_k = -r$, and $s_4(\alpha) = \alpha_1\alpha_2\alpha_3\alpha_4 = s$. So, we get that the coefficients of $g(t)$ can be expressed as polynomials in q, r, s. Since u, v and w themselves are quadratic polynomials in α's, and q, r, s have degrees 2, 3 and 4, respectively, we have:

$$u+v+w = \lambda\cdot q;$$
$$uv+vw+wu = \mu\cdot q^2 + \nu\cdot s;$$
$$uvw = \epsilon\cdot q^3 + \eta\cdot qs + \theta\cdot r^2,$$

where $\lambda, \mu, \nu, \epsilon, \eta, \theta$ are some integers (notice, that we can work with the formal expressions in α's with integral coefficients, keeping in mind that the Theorem on Symmetric Functions is valid over **any** commutative ring). It remains to find the constants $\lambda, \dots$. We can now plug $\mathbb{C}$-values of α's into our formal expressions. We only need to make sure that $\alpha_1+\alpha_2+\alpha_3+\alpha_4 = 0$ (since we used this condition in the computations above).

1) Plug $\alpha_1 = \alpha, \alpha_2 = -\alpha, \alpha_3 = 0, \alpha_4 = 0$. Then: $u = 0, v = -\alpha^2, w = -\alpha^2$. At the same time, $q = -\alpha^2$, $r = 0$, $s = 0$. Thus, $\lambda = 2$, $\mu = 1$, and $\epsilon = 0$.
2) Plug $\alpha_1 = \alpha, \alpha_2 = \omega\alpha, \alpha_3 = \omega^2\alpha, \alpha_4 = 0$, where ω is a nontrivial cubic root of 1 in $\mathbb{C}$. Then $u = \alpha^2(1+\omega^2)$, $v = \alpha^2(1+\omega)$, $w = \alpha^2(\omega+\omega^2)$. At the same time, $q = 0$, $r = -\alpha^3$, $s = 0$. This gives: $\theta = -1$.
3) Finally, plug $\alpha_1 = \alpha_3 = \alpha$, $\alpha_2 = \alpha_4 = -\alpha$. Then $u = 0$, $v = -4\alpha^2$, $w = 0$. At the same time, $q = -2\alpha^2$, $r = 0$, $s = \alpha^4$. Consequently, $\nu = -4$, and $\eta = 0$.

Putting everything together, we obtain the formula for the cubic resolvent:

$$g(t) = t^3 + (-2q)t^2 + (q^2-4s)t + (r^2).$$

Since $G(g) = Gal(K(u, v, w)/K) = G(f)/(G(f) \cap V_4)$, the problem of computing the latter quotient is reduced to computing the Galois group of a cubic. Notice, however, that g is not in a *reduced form* - it has (possibly) nontrivial coefficient at t^2. So, one may need to reduce it at some point (to compute Δ, for example). For $G(g)$ we have 4 cases:

1) 1, if $g(t)$ is split;
2) $\mathbb{Z}/2$, if $g(t)$ is a product of a linear term and an irreducible quadratic factor;
3) $\mathbb{Z}/3$, if $g(t)$ is irreducible, and $\Delta(g)$ is a square in K;
4) S_3, if $g(t)$ is irreducible, and $\Delta(g)$ is not a square in K.

Notice, that $\delta(g) = (u-v)(u-w)(v-w) = \pm\prod_{i<j}(\alpha_i-\alpha_j) = \pm\delta(f)$, and so $\Delta(g) = \Delta(f)$.

Now we have almost all the needed information to compute $G(f)$. First of all, we need to separate two cases: I) f is decomposable; II) f is irreducible.

I) Here either a) f has a linear factor, or b) f is a product of two irreducible quadratics.

a) If $f = f_1 f_2$, where f_1 is linear, then $G(f) = G(f_2)$ and everything is reduced to the computation of the Galois group of a cubic.

b) An easy computation shows that $G(f) = \mathbb{Z}/2$, if $\frac{\Delta_1}{\Delta_2}$ is a square, and $G(f) = \mathbb{Z}/2 \times \mathbb{Z}/2$, if $\frac{\Delta_1}{\Delta_2}$ is not a square (here Δ_1, Δ_2 are discriminants of quadratic factors).

II) If f is irreducible, then all the roots of f are different. It follows from Proposition 70 that the Galois group of an irreducible polynomial acts transitively on the set of its roots. In particular, since there are 4 different roots, $|G|$ should be divisible by 4.

Theorem 113. *Let $f(t)$ be an irreducible polynomial of degree 4 over a field of characteristic zero. Let $g(t)$ be its cubic resolvent. Then $G(f)$ is:*

(1) *S_4, if $g(t)$ is irreducible, and $\Delta(g) = \Delta(f)$ is not a square;*
(2) *A_4, if $g(t)$ is irreducible, and $\Delta(g) = \Delta(f)$ is a square;*
(3) *$\mathbb{Z}/2 \times \mathbb{Z}/2$, if $g(t)$ is split;*
(4) *either $\mathbb{Z}/4$, or D_8, if $g(t)$ is a product of an indecomposable quadratic and a linear factor.*

Proof. We know that $G(f)/(G(f) \cap V_4) = G(g)$ is either S_3, or A_3, or $\mathbb{Z}/2$, or 1. But the only subgroup in S_4 which projects onto S_3 under the identification $S_3 \cong S_4/V_4$ is S_4 itself. Similarly, the only subgroup which projects onto $A_3 \subset S_3$ is A_4. Thus, we get cases (1) and (2). For the case (3), observe that g is split if and only if $G(g) = 1$, if and only if $G(f) \subset V_4$. Since $|G(f)|$ is divisible by 4, the latter happens if and only if $G(f) = V_4$ and if and only if $G \cong \mathbb{Z}/2 \times \mathbb{Z}/2$. Finally, $g(t)$ is a product of an indecomposable quadratic and a linear factor if and only if $G(g) \cong \mathbb{Z}/2$. And the only subgroups $G \subset S_4$ having the property $G/(G \cap V_4) = \mathbb{Z}/2 \subset S_3$ are $\mathbb{Z}/4$ and D_8. □

Example 114. (1) *$K = \mathbb{Q}$, $f(t) = t^4 - 2t + 2$. Then f is irreducible by the Eisenstein criterion. The cubic resolvent will be $g(t) = t^3 - 8t + 4$, and it is also irreducible, since it has no rational roots (the only possible roots would be $\pm 1, \pm 2, \pm 4$). And $\Delta(g) = -4(-8)^3 - 27(4)^2 = 2^{11} - 3^3 \cdot 2^4 = (4)^2(128 - 27) = (4)^2 \cdot 101$ is not a square. Thus, $G(f) = S_4$.*

(2) *$K = \mathbb{Q}$, $f(t) = t^4 - 10t^2 + 1$. We already checked that f is irreducible. The cubic resolvent will be $g(t) = t^3 + 20t^2 + 96t = t(t^2 + 20t + 96) = t(t + 8)(t + 12)$. Thus, $G(f) = \mathbb{Z}/2 \times \mathbb{Z}/2$.*

In the ambiguous case $G(g) = \mathbb{Z}/2$ the possibilities can be distinguished as follows. Here g has a linear factor, which means that one of the elements u, v, w above belongs to K. Assume, it is u. Then $g(t) = (t - u)(t^2 + bt + c)$, where $(b^2 - 4c)$ is not a square in K.

Proposition 115. *In the above situation, $G(f)$ is*

(1) *$\mathbb{Z}/4$, if $c(b^2 - 4c)$ is a square in K;*
(2) *D_8, if $c(b^2 - 4c)$ is not a square in K.*

Proof. Since $G(f)$ acts trivially on u, it must belong to D_8 generated by V_4 and (12), or, which is the same, by (12) and the cycle (1324). Notice that the cycle (1324) generates the subgroup $\mathbb{Z}/4$, which is normal in D_8 (but not in S_4!). This is the only subgroup isomorphic to $\mathbb{Z}/4$ inside the given D_8, and we know that $\mathbb{Z}/4 \subset G(f) \subset D_8$. To separate our cases, it is sufficient to compute $G(f)/(\mathbb{Z}/4) = Gal(L^{\mathbb{Z}/4}/K)$, where $L^{\mathbb{Z}/4}/K$ is either quadratic, or trivial extension. Consider the element $\varepsilon := (\alpha_1 + \alpha_3)(\alpha_1 + \alpha_4)(\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4)$. Clearly, $\varepsilon \neq 0$, since otherwise, either v, or w would be zero, and $g(t)$ would be completely split. Using the fact that $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$, we obtain: $(12)(\varepsilon) = (\alpha_2 + \alpha_3)(\alpha_2 + \alpha_4)(\alpha_2 - \alpha_1)(\alpha_3 - \alpha_4) = -(\alpha_1 + \alpha_4)(\alpha_1 + \alpha_3)(\alpha_2 - \alpha_1)(\alpha_3 - \alpha_4) = -\varepsilon$, while $(1324)(\varepsilon) = (\alpha_3 + \alpha_2)(\alpha_3 + \alpha_1)(\alpha_3 - \alpha_4)(\alpha_2 - \alpha_1) = (\alpha_1 + \alpha_4)(\alpha_1 + \alpha_3)(\alpha_3 - \alpha_4)(\alpha_1 - \alpha_2) = \varepsilon$. Thus, $Gal(L/K(\varepsilon)) = \mathbb{Z}/4 = Gal(L/L^{\mathbb{Z}/4})$, which implies that $L^{\mathbb{Z}/4} = K(\varepsilon)$. Notice, that $\varepsilon^2 = (-v)(-w)(v - w)^2 = c(b^2 - 4c)$. Consequently, $G(f)/(\mathbb{Z}/4)$ is $\mathbb{Z}/2$, if $c(b^2 - 4c)$ is not a square in K, and is trivial otherwise. □

As a corollary we get the computation of the Galois group of a *biquadratic* polynomial.

Proposition 116. *Let $f(t) = t^4 + qt^2 + s$ be an irreducible polynomial over a field of characteristic zero. Then $G(f)$ is:*

(1) *$\mathbb{Z}/2 \times \mathbb{Z}/2$, if s is a square;*
(2) *$\mathbb{Z}/4$, if s is not a square, but $s(q^2 - 4s)$ is;*

(3) D_8, *if neither* s, *nor* $s(q^2-4s)$ *is a square.*

Proof. The cubic resolvent is $g(t) = t^3 - 2qt^2 + (q^2-4s)t = t(t^2 - 2qt + (q^2-4s))$, so we always have the linear factor, and $g(t)$ will be split if and only if $16s$ is a square in K. If s is not a square, then we get $\mathbb{Z}/4$ and D_8 cases depending on, is $c(b^2-4c) = (q^2-4s)16s$ a square, or not. □

Remark 117. *Notice, that while the Galois extension L/K produces naturally the group $Gal(L/K)$, it does not provide any embedding of this group into a symmetric group. Such an embedding appears only when one realises L as a splitting field of some polynomial f (and the respective group then is a symmetry group of roots of f). In particular, the same extension can be realised as a splitting field of various polynomials, and the respective embeddings into a symmetry group could be completely different, and not even conjugate.*

Example 118. *Let $K = \mathbb{Q}$, and $L = \mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2}+\sqrt{3})$. Then L is simultaneously a splitting field of $(t^2-2)(t^2-3)$ and of $t^4 - 10t^2 + 1$ (the minimal polynomial of $\sqrt{2}+\sqrt{3}$). Then $Gal(L/K) \cong \mathbb{Z}/2 \times \mathbb{Z}/2$, and it embeds as a subgroup $\{Id, (12), (34), (12)(34)\}$ of S_4, in the first case, and as a subgroup V_4, in the second. These subgroups are not conjugate in S_4 (one is normal, another is not, for example).*

It remains to express the roots of our quartic $f(t)$ in radicals. Since u, v, w are roots of the cubic resolvent $g(t)$ we can express them in radicals using Cardano's formula obtained in the previous section. Now, since $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$, we obtain: $(\alpha_1 + \alpha_2)^2 = -u$, and $(\alpha_1 + \alpha_2) = \sqrt{-u}$. In the same way, $(\alpha_1 + \alpha_3) = \sqrt{-v}$, and $(\alpha_1 + \alpha_4) = \sqrt{-w}$. Notice, that the choice of square roots here is not independent, since $(\alpha_1 + \alpha_2)(\alpha_1 + \alpha_3)(\alpha_1 + \alpha_4) = \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \alpha_1\alpha_3\alpha_4 + \alpha_2\alpha_3\alpha_4 = -r$. But if this condition is satisfied, then the (concerted) change of signs gives only the permutation of roots. We can solve the system of 4 linear equations in 4 variables to obtain:

$$\alpha_1 = \frac{1}{2}(\sqrt{-u} + \sqrt{-v} + \sqrt{-w});$$
$$\alpha_2 = \frac{1}{2}(\sqrt{-u} - \sqrt{-v} - \sqrt{-w});$$
$$\alpha_3 = \frac{1}{2}(-\sqrt{-u} + \sqrt{-v} - \sqrt{-w});$$
$$\alpha_4 = \frac{1}{2}(-\sqrt{-u} - \sqrt{-v} + \sqrt{-w})$$

18. Cyclotomic extensions

Let K be arbitrary field, and n be an integer. In this section we will study the extensions L/K, where $L = K(f)$ is a splitting field of $f(t) = t^n - 1$. Such extensions are called *cyclotomic*.

Let $\alpha_1, \ldots, \alpha_m$ are all different roots of f in L. Clearly, $\alpha_i \neq 0$, and we have the inclusion of sets: $\{\alpha_1, \ldots, \alpha_m\} \subset L^*$. If α, β are roots, then $\alpha \cdot \beta$ is also a root, since $(\alpha\beta)^n = \alpha^n\beta^n = 1 \cdot 1 = 1$, and similarly, 1 is a root, and α^{-1} is a root. Thus $\{\alpha_1, \ldots, \alpha_m\} \subset L^*$ is actually a subgroup of the multiplicative group of a field. Clearly, m is finite, since the number of roots of a polynomial in the field is no more than its degree. Thus, we have a finite subgroup of a multiplicative group.

Proposition 119. *Let $H \subset L^*$ be a finite subgroup in the multiplicative group of a field. Then H is cyclic.*

Proof. The multiplicative group of a field is commutative, hence H is finite commutative group. Thus, $H = C_1 \times \ldots \times C_r$, where $C_i \cong \mathbb{Z}/k_i$ are cyclic groups. Let $k = |H| = \prod_i k_i$. If integers a, b are relatively prime, then $\mathbb{Z}/a \times \mathbb{Z}/b \cong \mathbb{Z}/ab$ is again cyclic. So, if H would not be cyclic, then there would exist $i \neq j$ such that $G.C.D.(k_i, k_j) = d > 1$. Then, k_i and k_j divide $\frac{k_i k_j}{d}$, and thus, all k_l divide $\frac{k}{d}$. Denote $m := \frac{k}{d}$. Then all $h \in H$ will be roots of $t^m - 1$ over L. This is impossible, since the degree is m, while $|H| = k > m$. Consequently, H is cyclic. □

Thus, the roots $\{\alpha_1, \ldots, \alpha_m\}$ form a subgroup $\mathbb{Z}/m \subset L^*$. What is the relation between n and m? This depends on characteristic of a base field. Really, f has no multiple roots if and only if it is relatively prime with its derivative $f'(t) = nt^{n-1}$.

I) If either $char(K) = 0$, or $char(K) = p$, and $G.C.D.(p, n) = 1$, then n is invertible, $1 = -f(t) + \frac{t}{n}f'(t)$, which means that $G.C.D.(f, f') = 1$, and so f has no multiple roots. Thus, $m = n$.

II) If $char(K) = p$, and $n = p^k \cdot l$, where $G.C.D.(l, p) = 1$, then $t^n - 1 = t^{l \cdot p^k} - 1 = (t^l - 1)^{p^k}$, and the roots of $t^n - 1$ are exactly the roots of $t^l - 1$ (although, with different multiplicity). Thus, in this case, $m = l$.

The case of positive characteristic will be considered in the next section. Let us assume now that $char(K) = 0$. Then $m = n$, and we can choose one of the roots, say α as a generator of the multiplicative subgroup $\mathbb{Z}/n$. Since all the roots are powers of α, we have: $K(f) = K(\alpha)$, and any element of the Galois group is determined by its action on α. For any $g \in G(f)$, $g(\alpha) = \alpha^{d_g}$, where the integer d_g is unique modulo n, and can be considered as an element of $\mathbb{Z}/n$. Observe that, for $h, g \in G(f)$, $(h \circ g)(\alpha) = h(\alpha^{d_g}) = (h(\alpha))^{d_g} = (\alpha^{d_h})^{d_g} = \alpha^{d_h \cdot d_g} = (g \circ h)(\alpha)$. So, we have proved:

Proposition 120. *If $char(K) = 0$, then the assignment $g \mapsto d_g$ defines the embedding $\rho : G(f) \to (\mathbb{Z}/n)^*$ of our Galois group into the multiplicative group of the ring $\mathbb{Z}/n$. In particular, $G(f)$ is commutative.*

Any field K of characteristic 0 contains the field of rational numbers $\mathbb{Q}$ (as a prime subfield), and our polynomial f has coefficients in $\mathbb{Q}$. Thus, the Galois group of f over K embeds into the similar group over $\mathbb{Q}$: $G(f)_K \overset{e}{\subset} G(f)_{\mathbb{Q}}$. And $\rho_K = \rho_{\mathbb{Q}} \circ e$. So, the image of ρ will be largest in the case of $\mathbb{Q}$. It appears, that in this case it coincides with the whole $(\mathbb{Z}/n)^*$.

Theorem 121. *The map $\rho_{\mathbb{Q}} : Gal(\mathbb{Q}(f)/\mathbb{Q}) \to (\mathbb{Z}/n)^*$ is an isomorphism.*

Proof. We will start with the following lemma:

Lemma 122. *Let $\varphi(t)$ be irreducible factor of $t^n - 1 \in \mathbb{Q}[t]$, and $\beta \in \mathbb{Q}(\varphi)$ be its root. Let p be prime relatively prime to n. Then β^p is also a root of φ.*

Proof. Let us choose $\varphi(t)$ monic. Then, by Gauss's lemma, $\varphi(t) \in \mathbb{Z}[t]$. We have: $t^n - 1 = \varphi(t)\psi(t)$, and again by Gauss's lamma, ψ also has integral coefficients. If β^p would not be a root of $\varphi(t)$, it would be one of $\psi(t)$ (since $(\beta^p)^n = 1$). In other words, β would be a root of $\psi(t^p)$. Since β is also a root of $\varphi(t)$, and $\varphi(t)$ is irreducible, this implies that $\psi(t^p)$ is divisible by $\varphi(t)$. Let $\psi(t^p) = \varphi(t)\theta(t)$, and again θ has integral coefficients. Consider the reduction modulo p: $\mathbb{Z}[t] \to \mathbb{Z}/p[t]$, $g \mapsto \overline{g}$. Then $(t^n - 1) = \overline{\varphi}(t)\overline{\psi}(t)$, and $\overline{\psi}(t^p) = \overline{\varphi}(t)\overline{\theta}(t)$. But now coefficients of our polynomials belong to $\mathbb{Z}/p$, and this ring has the property that $u^p = u$, for any $u \in \mathbb{Z}/p$. Since the map $Fr : \mathbb{Z}/p[t] \to \mathbb{Z}/p[t]$, $g \mapsto g^p$ is a ring homomorphism, we get: $\overline{\psi}(t^p) = (\overline{\psi}(t))^p$, and thus, $(\overline{\psi}(t))^p = \overline{\varphi}(t)\overline{\theta}(t)$. This shows that $\overline{\psi}(t)$ and $\overline{\varphi}(t)$ have common roots. But the polynomial $(t^n - 1) = \overline{\varphi}(t)\overline{\psi}(t)$ has no multiple roots since p and n are relatively prime. Contradiction. Hence, β^p is a root of $\varphi(t)$. □

Let now α be the root generating the multiplicative subgroup of roots of degree n of unity in $\mathbb{Q}(t^n - 1)$, and $\Phi_n(t)$ be the minimal polynomial of α, then, for arbitrary $k \in (\mathbb{Z}/n)^*$, k can be presented as a product $\prod_i p_i$ of primes relatively prime to n. It follows from Lemma 122 that α^k is also a root of $\Phi_n(t)$. Thus, we have an automorphism $\sigma_k : \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ sending α to α^k. This shows that the map ρ is surjective. □

And the above considerations also give us the description of the minimal polynomial $\Phi_n(t)$ for the primitive n-th root of 1.

Proposition 123.

$$\Phi_n(t) = \prod_{k \in (\mathbb{Z}/n)^*} (t - \alpha^k)$$

Proof. Since $\Phi_n(t)$ is irreducible, and α is simultaneously a root of $\Phi_n(t)$ and $t^n - 1$, the latter should be divisible by the former. In particular, all roots of Φ_n have multiplicity 1, and have the form α^r, for some $r \in \mathbb{Z}/n$. It follows from Lemma 122 that, for any $k \in (\mathbb{Z}/n)^*$, α^k is a root of $\Phi_n(t)$. On the other hand, if r is not relatively prime to n, then there exists $d < n$ such that α^r is a root of $t^d - 1$. So, if α^r would be a root of Φ_n, then Φ_n would divide $t^d - 1$, and α would also be a root of $t^d - 1$, which is not the case, since α is primitive (it has order n in the multiplicative group). Thus, the roots of Φ_n are exactly α^k, where $k \in (\mathbb{Z}/n)^*$, and we get the needed decomposition. □

This proposition shows that Φ_n does not depend on the choice of the primitive n-th root of unity, but only on n. We also get: $deg(\Phi_n(t)) = \#((\mathbb{Z}/n)^*) =: \varphi(n)$.

Lemma 124. (1) *If $(m,n)=1$, then $\varphi(n\cdot m)=\varphi(n)\cdot\varphi(m)$;*
(2) $\varphi(p^r)=p^{r-1}(p-1)$.

Proof. 1) If $(n,m)=1$, then by the Chinese remainder theorem, $\mathbb{Z}/nm\cong\mathbb{Z}/n\times\mathbb{Z}/m$. In particular, $(\mathbb{Z}/nm)^*\cong(\mathbb{Z}/n)^*\times(\mathbb{Z}/m)^*$, and thus, $\varphi(nm)=\varphi(n)\varphi(m)$.

2) Clearly, $k\in(\mathbb{Z}/p^r)^*$ if and only if $k\not\vdots p$, and there are $p^{r-1}(p-1)$ such elements. □

Corollary 125. *Let $n=\prod_i p_i^{k_i}$, where p_i are <u>different</u> primes. Then*

$$[\mathbb{Q}(\zeta_n):\mathbb{Q}]=\prod_i p_i^{k_i-1}(p_i-1)$$

(here ζ_n is the primitive n-th root of unity).

Proof. Indeed, $[\mathbb{Q}(\zeta_n):\mathbb{Q}]$ is the degree of $\Phi_n(t)$ - the minimal polynomial of ζ_n, and so is equal to $\varphi(n)=\prod_i p_i^{k_i-1}(p_i-1)$. □

Example 126. (1) $[\mathbb{Q}(\sqrt{1}):\mathbb{Q}]=\varphi(2)=1$;
(2) $[\mathbb{Q}(\sqrt[3]{1}):\mathbb{Q}]=\varphi(3)=2$;
(3) $[\mathbb{Q}(\sqrt[4]{1}):\mathbb{Q}]=\varphi(4)=2$;
(4) $[\mathbb{Q}(\sqrt[5]{1}):\mathbb{Q}]=\varphi(5)=4$;
(5) $[\mathbb{Q}(\sqrt[136]{1}):\mathbb{Q}]=\varphi(136)=\varphi(2^3)\varphi(17)=2^2(2-1)(17-1)=2^6$. *But we know even the Galois group of this extension: $Gal(\mathbb{Q}(\sqrt[136]{1})/\mathbb{Q})=(\mathbb{Z}/136)^*=(\mathbb{Z}/8)^*\times(\mathbb{Z}/17)^*=(\mathbb{Z}/2\times\mathbb{Z}/2)\times(\mathbb{Z}/16)$. Notice, that our Galois group is a 2-group. The consequence is that the regular 136-gon can be constructed with the help of ruler and compass. Actually, regular n-gon can be constructed if and only if $\varphi(n)=2^s$, so not many n-s will qualify.*

What are the polynomials $\Phi_n(t)$? The following statement permits to produce them inductively.

Proposition 127.

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

Proof. We know that $\Phi_d(t)=\prod_\beta(t-\beta)$, where β runs over all primitive roots of degree d of unity. In the same way, $(t^n-1)=\prod_\gamma(t-\gamma)$, where γ runs over **all** roots of degree n of unity. It remains to notice that

$$\cup_{d|n}\left\{\begin{array}{c}\text{prim. roots}\\ \text{of degree } d\end{array}\right\}=\left\{\begin{array}{c}\text{all roots}\\ \text{of degree } n\end{array}\right\}.$$

□

Thus, $\Phi_n(t)=\frac{(t^n-1)}{\prod\limits_{\substack{d|n\\ d<n}}\Phi_d(t)}$. The first few examples are:

Example 128. (1) $\Phi_1(t)=t-1$;
(2) $\Phi_2(t)=t+1$;
(3) $\Phi_3(t)=t^2+t+1$;
(4) $\Phi_4(t)=t^2+1$;
(5) $\Phi_5(t)=t^4+t^3+t^2+t+1$;
(6) $\Phi_6(t)=t^2-t+1$;
(7) $\Phi_p(t)=t^{p-1}+t^{p-2}+\ldots+t+1$, *for p-prime.*

19. Radical extensions

Consider polynomials of slightly more general form: t^n-c, where $c\in K$ is arbitrary element now. These are exactly the polynomials producing radical extensions. We will assume that $char(K)=0$. The polynomial t^n-c is still separable (like t^n-1), and so it has no multiple roots. If $\beta_1,\ldots,\beta_n$ are all roots of t^n-c in its splitting field, then $\alpha_1=1=\frac{\beta_1}{\beta_1},\alpha_2=\frac{\beta_2}{\beta_1},\ldots,\alpha_n=\frac{\beta_n}{\beta_1}$ are different roots of t^n-1. So, these are all roots of the latter polynomial. This shows that the splitting field of t^n-c contains one of t^n-1:

$K(t^n-c) \supset K(t^n-1) \supset K$. Thus the Galois group $Gal(K(t^n-c)/K(t^n-1))$ is a normal subgroup in $Gal(K(t^n-c)/K)$, and the quotient $Gal(K(t^n-c)/K)/Gal(K(t^n-c)/K(t^n-1))$ is $Gal(K(t^n-1)/K)$. To understand $Gal(K(t^n-c)/K)$, we need to describe $Gal(K(t^n-c)/K(t^n-1))$, since we already have an idea what the quotient is like.

Let us fix some root β of t^n-c, and some primitive root ω of t^n-1. Then all the roots of t^n-c can be described as $\{\beta\omega^r, r \in \mathbb{Z}/n\}$. Denote $L = K(t^n-1)$. Then $K(t^n-c) = L(t^n-c) = L(\beta)$ is a simple extension of L, and so any element $g \in Gal(L(t^n-c)/L)$ is determined by its action on β. But $g(\beta)$ should be again a root of t^n-c, so $g(\beta) = \beta\omega^{r(g)}$, where $r(g) \in \mathbb{Z}/n$ is uniquely defined element. We obtain injective map of sets: $r : Gal(L(t^n-c)/L) \to \mathbb{Z}/n$.

Proposition 129. *If L contains all roots of 1 of degree n, then we have an injective group homomorphism*

$$r : Gal(L(t^n-c)/L) \to \mathbb{Z}/n.$$

In particular, this Galois group is abelian.

Proof. Clearly, $r(Id) = 0 \in \mathbb{Z}/n$, while $(h \circ g)(\beta) = h(g(\beta)) = h(\beta\omega^{r(g)}) = h(\beta)\omega^{r(g)} = \beta\omega^{r(h)}\omega^{r(g)} = \beta\omega^{r(h)+r(g)}$ (we used the fact that h fixes L, and so acts identically on ω), and so r respects the operation. □

What subgroup inside $\mathbb{Z}/n$ we will get depends not only on L, but also on c. If $c = b^m$, where m is a divisor of n (that is, $n = m \cdot l$), then $(t^n-c) = \prod_{0 \le i < m}(t^l - \omega^{il}b)$. We can choose β to be the root of (t^l-b) (remember, it was arbitrary root of t^n-c). Then $L(t^n-c) = L(\beta) = L(t^l-b)$. Thus, decreasing n, if necessary, we can assume that c is not the d-th power for any divisors $d > 1$ of n. And in this case, we get the whole group $\mathbb{Z}/n$.

Proposition 130. *If L contains all roots of 1 of degree n, and c is not a p-th power in L, for any p - prime divisor of n, then $Gal(L(t^n-c)/L) = \mathbb{Z}/n$.*

Proof. We know that $Gal(L(t^n-c)/L) = \mathbb{Z}/d \subset \mathbb{Z}/n$, where $n \vdots d$. Consider the polynomial $\prod_{g \in Gal}(t - g(\beta))$. Since it is stable under $Gal(L(t^n-c)/L)$ it has coefficients in L. But if $g = i \in \mathbb{Z}/d$, then $g(\beta) = \beta\omega^{i\frac{n}{d}}$. In particular, the free term of our polynomial will be $\pm\beta^d$. Thus, $\beta^d \in L$. But $c = (\beta^d)^{\frac{n}{d}}$, so if $d < n$ we get a contradiction. □

Example 131. (1) $Gal(\mathbb{Q}(i, \sqrt[4]{2})/\mathbb{Q}(i)) = \mathbb{Z}/4$;
(2) $Gal(\mathbb{Q}(t^4-36)/\mathbb{Q}(i)) = \mathbb{Z}/2$;
(3) $Gal(\mathbb{Q}(t^3-81)/\mathbb{Q}(t^3-1)) = \mathbb{Z}/3$.

Since $Gal(K(t^n-c)/K)$ has a commutative normal subgroup $Gal(K(t^n-c)/K(t^n-1))$ with commutative quotient $Gal(K(t^n-1)/K)$, we observe that this group is soluble (we know it already from the fact that t^n-c is soluble in radicals, anyway, but the extract of arguments above was actually used in the proof of Theorem 100). Notice, however, that this group is **not** commutative, in general.

Example 132. (1) $Gal(\mathbb{Q}(t^3-2)/\mathbb{Q}) = S_3$;
(2) $Gal(\mathbb{Q}(t^4-2)/\mathbb{Q}) = D_8$.

20. Finite fields

We've encountered some fields with finitely many elements in this course. The first example of course was $\mathbf{Z}_p$, the integers modulo p, for p a prime, a field with p elements. In exercises we constructed other finite fields by adjoining roots of irreducible polynomials to these fields. For example we constructed fields of order $2, 4, 8$; and $3, 9$.

The first thing to note is that any finite field has order $q = p^n$ were p is prime and $n \ge 1$. Indeed, suppose F is a finite field. The prime subfield P of F cannot be isomorphic to $\mathbf{Q}$, so must be isomorphic to $\mathbf{Z}_p$ for some prime number p; we identify P with $\mathbf{Z}_p$. Now F must be a extension of $\mathbf{Z}_p$ of finite degree, say n. Then F is a vector space of dimension n over $\mathbf{Z}_p$. Choose a basis $x_1, \ldots, x_n$. Then every element of F is uniquely expressible as

$$\lambda_1 x_1 + \cdots + \lambda_n x_n$$

where $\lambda_i \in \mathbf{Z}_p$. Thus there are exactly p^n elements of F. Now the next obvious question: how many fields are there of a given order $q = p^n$.

Example 133. *Fields of order* 9. *These are extensions of degree* 2 *over* Z_3. *There are* 3 *monic irreducible quadratics over* $\mathbf{Z}_3$*:*

$$t^2+1, t^2+t-1, t^2-t-1.$$

If f *is any of these, then by Thm. 34 there is an extension* $\mathbf{Z}_3(\alpha) \supset \mathbf{Z}_3$ *such that* f *is the minimal polynomial of* α *over* $\mathbf{Z}_3$. *As* $\mathbf{Z}_3(\alpha)$ *is a vector space of dimension* 2 *over* $\mathbf{Z}_3$, *it has order* $3^2 = 9$.

It might appear that we have constructed 3 *non-isomorphic extensions, one for each irreducible quadratic, but they are actually all isomorphic. To see this, let* $\mathbf{Z}_3(\alpha) \supset \mathbf{Z}_3$ *be an extension were the minimal polynomial of* α *is* t^2+1. *Let* $\beta = \alpha + 1 \in \mathbf{Z}_3(\alpha)$. *Then* $\beta^2 = \alpha^2 + 2\alpha + 1 = 2\alpha = 1 - \beta$. *So* β *has minimal polynomial* t^2+t-1 *and* $\mathbf{Z}_3(\beta) = \mathbf{Z}_3(\alpha)$. *Likewise,* $\gamma = \alpha - 1$ *has minimal polynomial* t^2-t-1 *and* $\mathbf{Z}_3(\gamma) = \mathbf{Z}_3(\alpha)$.

Theorem 134. *Let* p *be a prime and* $q = p^n$ *a positive power of* p.

(a) *There exists a field* F *of order* q.
(b) *Any* 2 *such are isomorphic.*
(c) *The elements of* F *are zeroes of* $t^q - t$. *In particular* F *is a splitting field for* $t^q - t$ *over any subfield.*
(d) *The multiplicative group* $F^\times$ *of* F *is cyclic of order* $q-1$.
(e) F *is a Galois extension of its prime field with cyclic Galois group of order* n.
(f) F *contains a subfield of order* p^d *if and only if* d *divides* n, *and if so this subfield is unique.*
(g) *The irreducible factors of* $t^q - t$ *over* $\mathbf{Z}_p$ *are precisely the irreducible polynomials over* $\mathbf{Z}_p$ *with degree dividing* n.

Let's explore some of the consequences of this theorem.

A consequence of (d): The nonzero elements of a finite field can be written as powers of a suitably chosen one. For example in $\mathbf{Z}_{11}$, 2 works:

$$\mathbf{Z}_{11}^* = \{1, 2, 4, 8, 5, 10, 9, 7, 3, 6\}.$$

It is not well understood which nonzero elements of $\mathbf{Z}_p^*$ are generators.

Now there are two ways of listing the elements of Z_p^* :

$$Z_p^* = \{1, 2, \ldots, p-1\} = \{1, v, v^2, \ldots, \nu^{p-1}\}.$$

additively and multiplicatively. These interact in such a way as to satisfy the distributive law!

Let us experiment also with (g) in case $p = 2$:

$$t^2 - t = t(t-1).$$

$$t^4 - t = t(t-1)(t^2+t+1).$$

$$\begin{aligned} t^8 - t &= t(t-1)(t^6+t^5+t^4+t^3+t^2+t+1) \\ &= t(t-1)(t^3+t+1)(t^3+t^2+1). \end{aligned}$$

$$\begin{aligned} t^{16} - t &= t(t-1)(t^2+t+1)(t^4+t^3+t^2+t+1)(t^8-t^7+t^5-t^4+t^3-t+1) \\ &= t(t-1)(t^2+t+1)(t^4+t^3+t^2+t+1)(t^4+t^3+1)(t^4+t+1). \end{aligned}$$

Before tackling a proof of the theorem, let us introduce a useful tool in the study of a field K of positive characteristic p, the *Frobenius map* $\phi : K \to K$ defined by $\phi(x) = x^p$. This is an endomorphism of K. Indeed

$$\phi(xy) = (xy)^p = x^p y^p = \phi(x)\phi(y)$$

and

$$\phi(x+y) = (x+y)^p = x^p + \binom{p}{1}x^{p-1}y + \binom{p}{2}x^{p-2}y^2 + \cdots + y^p = x^p + y^p,$$

as all the binomial coefficients $\binom{p}{i}$ are divisible by p when $1 \le i \le p-1$. Note that if F is finite, then ϕ is actually an isomorphism.

We use this to prove part (a): the existence of a field of order $q = p^n$, where p is an arbitrary prime number and n an arbitrary positive integer. Let F be a splitting field for $f = t^q - t$ over $\mathbf{Z}_p$. Now $Df = -1$ is relatively prime to f, so by Lemma 64 f has q distinct zeroes in F. Call the set of zeroes R. Then $R = \{x \in F : \phi^n(x) = x\}$. Now ϕ^n is a monomorphism, so for all x and y in R we have $\phi^n(x + y) = \phi^n(x) + \phi^n(y) = x + y$ and $\phi^n(xy) = \phi^n(x)\phi^n(y) = xy$ and $\phi^n(x^{-1}) = \phi^n(x)^{-1} = x^{-1}$, $\phi(-x) = -x$. Hence R is actually a field. But f splits over R so $R = F$ and F is a field of order q.

Next, a proof of parts (b) and (c): Conversely let F be any field of order q. The multiplicative group $F^\times$ is a group of order $q - 1$, so if $x \in F^\times$, then $x^{q-1} = 1$, so $x^q - x = 0$. This is a group of order $q - 1$, so if $x \in F^\times$, then $x^{q-1} = 1$ so that $x^q - x = 0$. We also have $0^q - 0 = 0$, so the polynomial $x^q - x$ splits over F, and doesn't split over a smaller field, because *every* element of F is a zero. So F is a splitting field of $t^q - t$ over Z_q. By the uniqueness of splitting fields (Prop. 59), we conclude that there is at most 1 field of any given order $q = p^n$.

Proof of part (d): It suffices to prove the following: If K is an arbitrary field, and H is a finite subgroup of the multiplicative group of K, then H is cyclic.

By the structure theorem for finite abelian groups,

$$H \cong C_{r_1} \times C_{r_2} \times \cdots \times C_{r_t}$$

where $1 < r_1|r_2|\cdots|r_t$ and $m = r_1 \cdots r_t$. Now if $x \in H$ then $x^{r_t} = 1$ so every element of H is a zero of $x^{r_t} - 1$. Thus $t = 1$ and $H \cong C_{r_1}$ is cyclic.

Next a proof of part (e): By part (c) and its proof, F is a normal and separable extension of $\mathbf{Z}_p$, and is therefore Galois over $\mathbf{Z}_p$ by Thm. 73. A more direct way to see this, and to get the Galois group at the same time, is to use the Frobenius automorphism $\phi : F \to F$. Note that for all $x \in \mathbf{Z}_p$, $\phi(x) = x^p = x$, so ϕ is an element $Gal(F \supset \mathbf{Z}_p)$. As $F^\times$ is cyclic of order $p^n - 1$, we see that ϕ^i is a nonzero element of $Gal(F \supset P)$ for $i = 1, 2, \ldots, n - 1$ (by applying each to a generator of $F^\times$). Thus $F \supset \mathbf{Z}_p$ is Galois with Galois group cyclic of order n, generated by the Frobenius automorphism ϕ.

Proof of part (f): Let K be a subfield of F. Then K has order p^d for some d. Now F is a vector space over K so p^n must be a power of p^d. It follows that d divides n. On the other hand, if d is any integer and $d|n$, then $p^n - 1 = (p^d - 1)s$ where $s = p^{n-d} + p^{n-2d} + \cdots + p^d + 1$ and therefore $t^{p^n} - t$ is divisible by $t^{p^d} - t$ as

$$\begin{aligned} t^{p^n} - t &= t(t^{p^n-1} - 1) = t(t^{p^d-1} - 1)(t^{(p^d-1)(s-1)} + t^{(p^d-1)(s-2)} + \cdots + t^{p^d-1} + 1) \\ &= (t^{p^d} - t)(t^{(p^d-1)(s-1)} + t^{(p^d-1)(s-2)} + \cdots + t^{p^d-1} + 1). \end{aligned}$$

Therefore the set of zeros of $t^{p^d} - t$ in F is a subfield of F of order p^d, and this is the unique such subfield.

One can use the Galois correspondence to give an alternative proof of part (f). What are the subgroups of a cyclic group of order n generated by ϕ? We get one subgroup of order n/d for each divisor d of n, the cyclic subgroup generated by $\phi^{n/d}$. This is a subgroup of index d in $Gal(F \supset \mathbf{Z}_p)$ so the corresponding fixed field $\{x \in F : x^{p^d} = x\}$ is a subfield of F of degree d over $\mathbf{Z}_p$, i.e. of order p^d.

Finally we prove part (g): If f is an irreducible factor of $t^{p^n} - t$ over $\mathbf{Z}_p$, then if F is a field of order p^n it contains an element α with minimal polynomial f over $\mathbf{Z}_p$. Then $\mathbf{Z}_p(\alpha)$ is a subfield of F of order $p^{\delta f}$ and it follows by the determination of subfields above that δf divides n.

Conversely let f be an arbitrary irreducible polynomial over $\mathbf{Z}_p$ such that δf divides n. Then adjoining a zero of f to $\mathbf{Z}_p$ we get a field of order $p^{\delta f}$. By uniqueness this is isomorphic to a subfield of a field of order p^n. But f splits in this larger field, and every element of this larger field is a zero of $t^q - t$. It follows that f divides $t^q - t$.

21. Fundamental Theorem of Algebra.

A field K is called *algebraically closed* if every polynomial over K has a zero in K.

Theorem 135. *The complex field* $\mathbf{C}$ *is algebraically closed.*

The first rigorous proof of this theorem was given by Gauss in his PhD Thesis of 1799 (he actually proved that any polynomial over $\mathbf{R}$ has a zero in $\mathbf{C}$), but we use a later proof due to Legendre, filling some gaps using Galois Theory.

Flaws in pre-Gauss proofs: It was assumed that f had zeroes 'somewhere' and eventually shown that these zeroes are in $\mathbf{C}$. With Galois theory we know where somewhere is, namely a splitting field for f.

Definition 136. *An* ordered field *is a field K with a relation $\leq$ such that*

(1) *$k \leq k$ for all $k \in K$.*
(2) *$k \leq l$ and $l \leq m$ implies that $k \leq m$.*
(3) *$k \leq l$ and $l \leq k$ implies $k = l$.*
(4) *if $l, k \in L$, then either $l \leq k$ or $k \leq l$.*
(5) *if $k, l, m \in K$ and $k \leq l$ then $k + m \leq l + m$.*
(6) *if $k, l, m \in K$ and $k \leq l$ and $0 \leq m$ then $km \leq lm$.*

Conditions (1)-(4) give K a total ordering, and (5)-(7) describe how the field operations behave with respect to the ordering. The notions of $<$, $>$, *positive*, and *negative* are defined in the obvious ways.

The rationals $\mathbf{Q}$ and the reals $\mathbf{R}$ are examples of ordered fields, with their natural orderings. It is not possible to order the complex numbers to make it an ordered field.

Lemma 137. *Let K be an ordered field. Then for any $k \in K$, we have $k^2 \geq 0$, and the characteristic of K is 0.*

Proof. Suppose $k \geq 0$. Then by condition (6), $k^2 \geq k0 = 0$. If $k \leq 0$, then by condition (5) we have $0 = k + (-k) \leq -k$, so $k^2 = (-k)^2 \geq 0$. In particular $1 = 1^2 > 0$, so for any positive integer n, $1 + 1 + \cdots + 1 > 0$. Therefore K cannot have positive characteristic. □

Note that it is not possible to extend the natural ordering on $\mathbf{R}$ to $\mathbf{C}$ so that $\mathbf{C}$ is an ordered field, because $i^2 = -1$ is negative.

We will need the following properties of $\mathbf{R}$: it is an ordered field (with the natural ordering), every positive element is a square, and every polynomial over $\mathbf{R}$ of odd degree has a zero in $\mathbf{R}$.

Lemma 138. *Let K be a field of characteristic 0 with the following property: for some prime p every finite extension M of K with $M \neq K$ has degree $[M : K]$ divisible by p. Then every finite extension of K has degree a power of p.*

Proof. Let N be a finite extension of K. By using Lemma 71 we may assume that $N \supset K$ is normal. As K has char 0, it is also separable, hence Galois. Let G be Galois group, and P Sylow p-subgroup. The fixed field $P^\dagger$is an extension of K of degree equal to the index of P in G. This is not divisible by p, so by assumption we must have $P = G$, so $G = [N : K]$ is indeed a power of p. □

Theorem 139. *Let K be an ordered field in which every positive element is the square of some element and such that every odd-degree polynomial over K has a zero in K. Then $K(i)$ is algebraically closed, where $i^2 = -1$.*

Proof. First we note the K cannot have a finite, nontrivial extension of odd degree. If $[M : K] = r > 1$ is odd, then choosing any $\alpha \in M \backslash K$, the degree of the minimal polynomial of α over K divides r and is thus odd. This by our assumption on K has a zero in K, contradicting its irreducibility. So every finite extension of K has even degree, and thus by the Lemma above, every finite extension of K has degree a power of 2.

Let M be a nontrivial extension of $K(i)$ where $i^2 = -1$. By Lemma 71 we may assume that $M \supset K(i)$ is normal, and hence Galois. Its Galois group is a 2-group, and therefore by Prop. 94 has a subgroup of index 2. The fixed field of this subgroup is an extension N of $K(i)$ of degree 2. So we have $N = K(i)(\alpha)$, where the minimal polynomial of α has degree 2. We have seen (Example 98) that since the characteristic is not equal to 2, we may assume α is a square root of an element of $K(i)$, say $a + bi$.

But $a + bi$ has a square root in $K(i)$, namely, $\sqrt{\frac{a+\sqrt{a^2+b^2}}{2}} + \sqrt{\frac{-a+\sqrt{a^2+b^2}}{2}}i$, where we take the positive square root of $a^2 + b^2$, and the outside square roots are taken so that their product is $b/2$. It follows that $\alpha \in K$, so that $N = K(i)$, a contradiction.

So $K(i)$ has no finite extensions of degree > 1, Let f be an irreducible polynomial of $K(i)$, then a splitting field for f over $K(i)$ is a finite extension. Only possibility is that f has degree 1. So any polynomial over $K(i)$ factors into linear factors and hence has a zero in $K(i)$. □

22. Primitive elements

In all of examples that we considered any finite field extensions turned out to be generated by one element. Such an element, if it exists, is called *a primitive element*. We will now see that under mild restrictions primitive elements exist.

Theorem 140. *Let $L \supset K$ be a finite extension. An element $\alpha \in L$ for which $L = K(\alpha)$ exists if and only if there exist only finitely many intermediate fields $F : L \supset F \supset K$. If L is separable over K then such an element always exist.*

Proof. If K is finite than L is also finite and therefore the multiplicative group of L is generated by one element which is then primitive. So let us assume that K is infinite.

Suppose that there exists only finitely many fields intermediate between L and K. Let $\alpha, \beta \in L$. For $c \in K$ there exist only finitely many fields of the form $K(\alpha + c\beta)$. Therefore there are $c_1, c_2 \in K$, $c_1 \neq c_2$ and such that

$$K(\alpha + c_1\beta) = K(\alpha + c_2\beta).$$

Note that $\alpha + c_1\beta$ and $\alpha + c_2\beta$ belong to the same field, hence $(c_1 - c_2)\beta$ also belongs to this field and therefore β does so as well. Thus, α also belongs to the same field and it follows that $K(\alpha, \beta)$ is generated by one element (e.g. $\alpha + c_1\beta$). An obvious induction shows that any intermediate field generated by finitely many elements (in particular, L itself is generated by one element).

Conversely, suppose that $L = K(\alpha)$ for some α. Let $m(x)$ be the minimal polynomial of α over K. For any intermediate field F consider $m_F(x)$, the minimal polynomial of α *over* F. Clearly, m_F divides m. Since there are only finitely many (monic) divisors of m we obtain a map

$$F \mapsto m_F$$

from the set of intermediate fields into a finite set of polynomials. Let F_0 be the subfield in F generated by the coefficients of the polynomial m_F. Then m_F has coefficients in F_0 and it is irreducible over F_0 since it is even irreducible over F. Therefore the degree of α over F is the same as the degree of α over F_0. It follows that $F_0 = F$. We conclude that F is determined uniquely by m_F and therefore the above map is injective. This finishes the proof of the first statement of the theorem.

Now suppose that L is separable over K. Using induction, the general case is reduced to the one when $L = K(\alpha, \beta)$ where α, β are separable over K. Let $\sigma_1, \ldots, \sigma_n$ be different embeddings of K into the normal closure of L. By Theorem 72 $n = [L : K]$ (here we use the condition that $L \supset K$ is separable.)

Set

$$P(x) = \prod_{i \neq j} (\sigma_i(\alpha) + x\sigma_i(\beta) - \sigma_j(\alpha) - x\sigma_j(\beta)).$$

Clearly, $P(x)$ is a nonzero polynomial and therefore there exists an element $c \in K$ for which $P(c) \neq 0$. Then the elements $\sigma_i(\alpha + c\beta)$ are all different and therefore $K(\alpha + c\beta)$ has degree over K no less that n. However $n = [K(\alpha, \beta) : K]$ and therefore $K(\alpha, \beta) = K(c)$. □

Example 141. *Consider the extension $L = \mathbb{Q}(\sqrt{2}, \sqrt[3]{5}) \supset \mathbb{Q} = K$. The embeddings of L into its normal closure is simply the Galois group of the latter over K and its elements permutes the roots of $t^2 - 2$ (which are $\pm\sqrt{2}$) and the roots of $t^3 - 5$ (which are $\sqrt[3]{5}, \omega\sqrt[3]{5}, \omega^2\sqrt[3]{5}, \omega = \sqrt[3]{1}$). Consider the six elements $\pm\sqrt{2} + \omega^i\sqrt[3]{5}, i = 0, 1, 2$. Clearly, these elements are pairwise distinct and therefore by the above proof the element $\sqrt{2} + \sqrt[3]{5}$ is primitive.*

23. Symmetric polynomials

Let k be a field and consider the polynomial

$$F(X, t_1, t_2, \ldots, t_n) = (X - t_1)(X - t_2)\ldots(X - t_n) = X^n - s_1X^{n-1} + \ldots + (-1)^n s_n.$$

Thus, $s_1 = t_1 + t_2 + \ldots + t_n$ and $s_n = t_1t_2\ldots t_n$.

Let σ be a permutation of integers $1, 2, \ldots, n$. For $f \in k[t_1, \ldots, t_n]$ define $f^\sigma \in k[t_1, \ldots, t_n]$ by the formula

$$f^\sigma(t_1, \ldots, t_n) = f(t_{\sigma(1)}, \ldots, t_{\sigma(n)}).$$

This defines an action of S_n on $k[t_1, \dots, t_n]$. A polynomial f is called *symmetric* if $f^\sigma = f$. It is clear that the set of symmetric polynomials is a subring in $k[t_1, \dots, t_n]$ which contains k and elementary symmetric polynomials. The following theorem says, essentially, that this is all it contains.

Theorem 142. *A symmetric polynomial can be written as a polynomial expression in $s_1, s_2, \dots, s_n$.*

Proof. Introduce the *lexicographic order* on the set of monomials in $t_1, \dots, t_n$ (i.e. words $\mathbf{t^a} = \mathbf{t_1^{a_1} \dots t_n^{a_n}}$.) A letter t_i beats t_j if and only if $i > j$. Write every monomial in the form $t_1 \dots t_1 \cdot t_2 \dots t_2 \cdot \dots t_n \dots t_n$. A monomial A beats a monomial B iff the letter entering in A beats the corresponding letter in B the first time they differ.

Further, call the *leading term* of a polynomial $f = f(t_1, \dots, t_n)$ its highest term in lexicographic order. Let $t_1^{a_1} \dots t_n^{a_n}$ be the leading term of a symmetric polynomial f. Consider the polynomial $S = s_1^{b_1} \dots s_n^{b_n}$. It leading term is the product of leading terms of each factor, which is

$$t_1^{b_1+b_2+\dots+b_n} t_2^{b_2+b_3+\dots+b_n} \dots t_{n-1}^{b_{n-1}+b_n} t_n^{b_n}.$$

Then choose $b_n = a_n, b_{n-1} = a_{n-1} - b_n = a_{n-1} - a_n$ etc. Then f minus a suitable scalar multiple of S has leading term lower in the lexicographic order that that of f. Then apply induction to finish the proof. □

Remark 143. *It is possible to prove that the subring of symmetric polynomials in $k[t_1, \dots, t_n]$ is itself isomorphic to the polynomial ring in $s_1, s_2, \dots, s_n$, i.e. that there are no algebraic relations between the elementary symmetric polynomials, in other words they are* algebraically independent*. The notion of algebraic independence will be considered in some detail in the next section.*

24. Transcendental extensions

Technically speaking the notion of a transcendental extension of a field lies outside of Galois Theory (which is concerned with *algebraic* extensions). Nevertheless, this is an important notion and any course dealing with field theory would be incomplete without mentioning it. Here we will give a brief introduction into this subject.

Let $L \supset K$ be an extension of fields and let S be a subset of L. Consider the polynomial ring $K[X] := K[\{x_i\}], i \in S$ (in other words, the generators x_i are indexed by the elements in the set S. The map $x_i \mapsto i$ defines a ring homomorphism $K[X] \to L$. We say that the set S is *algebraically independent* if this map is injective. In other words S is algebraically independent if various monomials of the form $x_1^{i_1} \dots x_2^{i_n}, x_i \in S$ are linearly independent over k. If S is not algebraically independent we say that it is *algebraically dependent.*

The extension $L \supset K$ is called *purely transcendental* if L contains an algebraically independent set S and $L = K(S)$. For example, if S consists of one element x then we arrive at the notion of a simple transcendental extension $K(x) \supset K$ discussed in Section 3.

Let S be an algebraically independent subset of L which is maximal with respect to inclusion among all algebraically independent subsets of K. Then S is called a *transcendence basis* of L over K. The cardinality of L is called the *transcendence degree* of L over k; as we will see shortly it does not depend on the choice of a transcendence basis.

Remark 144. *The existence of a transcendence basis follows from a general result in set theory called 'Zorn's lemma'. We don't intend to discuss it here, but note that the existence of a basis in a general (infinite dimensional) vector space over a field also relies on this result. In many respects the notions of algebraic (in)dependence and transcendence basis are similar to the notions of linear independence and linear basis.*

Note that if S is a transcendence basis of L over K then L is algebraic over $K(S)$.

Theorem 145. *Any two transcendence bases of an extension $L \supset K$ have the same cardinality. Moreover, if $S \subset L$ is an algebraically independent then there exists a transcendence basis B of L such that $S \subset B$.*

Proof. We will prove that if there exists one *finite* transcendence basis $\{x_1, \dots, x_m\}$ then any other transcendence basis must contain m elements. For this it suffice to prove that if $w_1, \dots, w_n \in L$ are algebraically independent then $n \leq m$ (why?).

Now, since $x_1, \dots x_m$ is a transcendence basis there exists a nonzero polynomial f_1 of $m+1$ variables with coefficients in K such that $f_1(w_1, x_1, \dots, x_m) = 0$. Moreover, w_1 enters non-trivially in f_1 (otherwise $x_1, \dots, x_m$ would be algebraically dependent) and some x_i enters non-trivially in f_1 (otherwise w_1 would

be algebraic). Assume without loss of generality that $i = 1$ or otherwise renumber the variables $x_1, \ldots, x_m$ appropriately. Thus, x_1 is algebraic over $K(w_1, x_2, x_3, \ldots, x_m)$.

Assume by induction that after a suitable renumbering of $x_2, \ldots, x_m$ we can find $w_1, \ldots, w_r$ with $r < n$ such that L is algebraic over $K(w_1, \ldots, w_r, x_{r+1}, \ldots, x_m)$. Note that the base of induction $r = 1$ has just been proved.

Then there exists a nonzero polynomial f of $m + 1$ variables with coefficients in K for which

$$f(w_{r+1}, w_1, \ldots, w_r, x_{r+1}, \ldots, x_m) = 0$$

and w_{r+1} enters into f non-trivially. Since w_i's are algebraically independent we see that a certain element x_j also enters non-trivially in f; after a suitable renumbering we can assume that $j = r+1$. Therefore x_{r+1} is algebraic over $K(w_1, \ldots, w_{r+1}, x_r, \ldots, x_m)$ and it follows that L is algebraic over $K(w_1, \ldots, w_{r+1}, x_r, \ldots, x_m)$. Repeating this procedure we find that if $n \geq m$ then L is algebraic over $K(w_1, \ldots, w_m)$. Therefore $n \geq m$ implies $n = m$ as required.

We proved that the transcendence degree is either finite and equal to the cardinality of any transcendence basis or it is infinite and then any transcendence basis is infinite. The statement about the cardinality in the infinite case is left for you as an exercise as well as the statement that any algebraically independent set could be completed to a transcendence basis.

□