GALOIS THEORY

NICK GILL

These notes are for use in the first half of the Masters course on Galois Theory, Bristol, 2009. The treatment is based on notes by Andrey Lazarev and Trevor Woolley (both Bristol) and Rick McFeat (Western Australia). Two texts for the course are recommended - see the bibliography. The official book for this course is [Gar86]; the secondary book, [Ste03], is more informal in tone.

Most of the exercises in the following set of notes are very easy. So make sure you do them! Some proofs are not included, but citations are provided. You should regard these as hard exercises - try and prove them yourself. If repeated attempts don't yield success, then refer to the relevant text.

The website for (my part of) the course is:

`http://www.maths.bris.ac.uk/∼manpg/teaching.html`

1. Motivation

Galois theory started with... wait for it... a man called Evariste Galois. It straddles, and informs, several areas of mathematics, most notably group theory and number theory. The beauty of Galois theory, and its importance in many areas of pure mathematics, will hopefully become very obvious as the course proceeds.

1.1. **Some history.** Right from its first conception, Galois theory provided answers to some of the most long-standing questions in mathematics.

1.1.1. *Solutions to polynomial equations.* We all learn at school how to solve the quadratic equation,

$$ax^2 + bx + c = 0,$$

where x is a variable and a, b, c are fixed real or complex numbers. Our method is to *complete the square* and then solve for x; this yields the well-known quadratic formula:

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

This stuff aint new: the Babylonians could solve quadratic equations using algebraic methods in 1600BC. Some time later the Greeks came up with geometric methods that did the job. Indian mathematicians also knew the answer to this a very long time ago.

Cubic equations proved much harder. Take the polynomial equation,

$$a_nx^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0 = 0.$$

Now, we can reduce the problem of solving this equation to that of solving a *monic polynomial*:

$$x^n + a_{n-1}x^{n-1} + \cdots + a_2x^2 + a_1x + a_0 = 0.$$

(Exercise) In the cubic case it is easy to show that this general monic case can be reduced to the situation

$$x^3 + a_1 x + a_0 = 0.$$

(Exercise) A bunch of renaissance mathematicians in Bologna came up with a general solution to this last equation. There was a vast amount of intrigue and murkiness over who deserved the credit for this discovery. Niccolo "Tartaglia" Fontana demonstrated his methods in public around 1535.

For the equation $x^3 + px = q$, we have the solution

$$x = \sqrt[3]{\frac{q}{2} + \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}} + \sqrt[3]{\frac{q}{2} - \sqrt{\frac{p^3}{27} + \frac{q^2}{4}}}.$$

Notice that the expression for this general solution depends on the coefficients via a finite number of operations involving $+, -, \times, \div$ and extraction of roots, $\sqrt[n]{}$. We refer to such an expression as a *radical* expression. This will be a very important concept in what follows.

Quartic equations were solved around the same time. Ludovico Ferrari came up with a method for solving the quartic by reducing it to a cubic. The method also expressed the solutions of a quartic as a radical expression.

Quintic equations were the natural next equation to be solved.... But nobody could do it. Various big names - Euler, Lagrange - proved results related to this question, some of which made people start to think that perhaps no such equation existed.

In 1824, Abel proved that there is no general formula for the equation

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

using $+, -, \times, \div$, and $\sqrt[n]{}$. In other words the quintic is *insoluble by radicals.*

So now, supposing we have a particular quintic equation, how do we know if it can be solved by radicals? Abel was working on this question in the years after 1824. Unfortunately tuberculosis brought an end to his mathematical research and, indeed, his life in 1829, at the age of 26.

Our man Evariste Galois appeared on the scene around now. He had a whole heap of trouble with the mathematical establishment, with various political groups, and - most fatal of all - with the ladies. It would seem likely that it was an affair of the heart that led to his accepting a challenge to a duel one day in 1832. And so, at the age of 20, he died.

The day before this duel Galois wrote to his friend Auguste Chevalier outlining his mathematical discoveries; hoping that Chevalier could make these discoveries known. Perhaps the most significant of these discoveries can be summed up in the statement that *an equation is soluble by radicals provided its group is soluble.* What this mysterious sentence really means will be the subject of a large part of ths course.

We won't dwell on the historical events surrounding the lives of both Galois, and Abel. Suffice to say that they are both fascinating figures, and you could do worse than look them up on wikipedia.

1.1.2. *Construction problems.* We should also briefly mention an application of Galois theory that was of great historical importance.

Suppose that one is given two instruments - a ruler (an unmarked straight edge), and a compass.

Now suppose I draw an angle, α, from two straight lines. You probably know from highschool that, using only a ruler and compass, it is possible to draw the angle $\frac{\alpha}{2}$. In other words, I can *bisect the angle*.

The Greeks loved this sort of game, and could do many nice constructions of the same ilk. But there were some constructions that they couldn't do:

- *duplication of the cube*: given a cube C, construct a cube D of twice the volume;
- *trisection of the angle*;
- *quadrature of the circle*: given a circle C, construct a square S of the same area.

It turns out that all of these problems are impossible, for reasons that Galois theory makes clear.

There is a related problem that I should mention. We would like to draw a regular polygon using only a ruler and compass. It turns out that some regular polygons (e.g. a pentagon) are easy to construct with ruler and compass; others are not. This led to the question: Is it possible to construct all regular polygons with ruler and compass?

Carl Friedrich Gauss in 1796 showed that a regular n-sided polygon can be constructed with ruler and compass if the odd prime factors of n are distinct Fermat primes. Gauss conjectured that this condition was also necessary, but he offered no proof of this fact, which was proven by Pierre Wantzel in 1837... using Galois theory.

1.2. The "group of an equation".

Before we get to some proper mathematics, I want to have an (arm-waving) look at that mysterious sentence from earlier, "an equation is soluble by radicals provided its group is soluble". Specifically, I have this question: *what is the "group of an equation"?*

We proceed by example Consider the polynomial equation

$$x^4 - 2 = 0,$$

with integer coefficients. We have four solutions:

$$\alpha = \sqrt[4]{2}, \beta = i\sqrt[4]{2}, \gamma = -\sqrt[4]{2}, \delta = -i\sqrt[4]{2}.$$

Note that two of these solutions are not real. Now let us list some equations that these four roots satisfy:

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

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

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

which are all still valid. Likewise we could permute the variables as follows

$$\alpha \mapsto \beta \mapsto \gamma \mapsto \delta.$$

You can check that the equations above remain valid. So, does any such permutation work? For any such equation? The answer is "no": try, for instance, swapping β and γ, and you find that the first of the equations above becomes false.

The set of permutations of the set $\{\alpha, \beta, \gamma, \delta\}$ that preserve the validity of all polynomial equations (with coefficients in $\mathbb{Q}$) in these variables is called the *Galois group* of the equation $x^4 = 2$. This group is the symmetric group of the square (which makes sense if you look at the location of α, β, γ, and δ in the Complex plane. It is also known as D_8, the dihedral group of order 8.

In fact this Galois group can be defined more generally. Take the equation

$$x^2 + 1 = 0$$

which has roots $\alpha = i$, and $\beta = -i$. Now the conjugation map

$$\bar{\ } : \mathbb{C} \to \mathbb{C}, \ z \mapsto \bar{z},$$

acts as a permutation on the set of roots $\{\alpha, \beta\}$. It's not hard to prove that this permutation preserves the validity of all polynomial equations in α and β with real coefficients.

But now the conjugation map is, of course, a map of the whole field. This phenomenon is general: those permutations relating to the equation $x^4 - 2$ that we discussed above can be extended to yield maps $\mathbb{C} \to \mathbb{C}$. So, the Galois group is a set of maps between fields.

We're going to need to move from arm-waving to mathematics. Let's highlight some issues:

- What is the relation between $\mathbb{R}$ and $\mathbb{C}$ for the equation $x^2 + 1$? Or between $\mathbb{Q}$ and $\mathbb{C}$ for the equation $x^4 - 2$? More generally, what is a *field extension*?
- What about other fields?
- What do we mean by a "root of a polynomial", when there is no root in that field?

2. Some algebra

We assume a number of basic facts about the integers $\mathbb{Z}$, which I will not review here. Students should be familiar with unique factorization, the division algorithm, Euler's theorem, the Euclidean algorithm to find the highest common factor of two integers, and the Chinese remainder theorem.

2.1. A review of rings.

Definition 1. *A* **commutative ring with** 1 *is a set R equipped with two binary operations $+$ and $\cdot$ such that*

- *$(R, +)$ is an abelian group;*
- *$\cdot$ is associative and commutative;*
- *distributivity holds: for all $a, b, c \in R$*

$$(a + b) \cdot c = (a \cdot c) + (b \cdot c), \ \text{and}$$
$$a \cdot (b + c) = (a \cdot b) + (a \cdot c).$$

- *there exists an element $1 \in R$ such that $a1 = 1a = a$ for all $a \in R$.*

We will write ab for $a \cdot b$, and label the additive identity by 0. There are more general definitions of rings, but we will not need them. Thus whenever we refer to a **ring** we mean a commutative ring with 1.

Definition 2. *We say that a set R is an* **integral domain** *if it is a ring such that*

- *If $ab = 0$ for $a, b \in R$, then either $a = 0$ or $b = 0$.*

A set R is a **field** *if it is a ring such that*

- *$F\backslash\{0\}$ is an abelian group under $\cdot$.*

Note that then 1 is the identity of $F\backslash\{0\}$; what is more we often write F^* for $F\backslash\{0\}$.

We recall the definitions of *subring*, *subfield*, and *ideal.* If a ring R has an ideal I, then we can form the *quotient ring* R/I.

Definition 3. *Let R and S be two rings. A homomorphism ϕ between R and S is a map $R \to S$ such that, for all $a, b \in R$,*

$$\phi(a+b) = \phi(a) + \phi(b), \text{ and}$$
$$\phi(ab) = \phi(a)\phi(b).$$

We have the consequent definitions of *epimorphism, monomorphism* and *isomorphism.* In addition, if we take $R = S$, then a homomorphism ϕ is called an *endomorphism*, while an isomorphism ϕ is called an *automorphism.*

Obviously all of the above definitions apply if R is not just a ring, but a field. *Field automorphisms* will be central objects in this course. (See the earlier arm-waving!)

Exercise 2.1. *A field is an integral domain.*

Exercise 2.2. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ *are fields;* $\mathbb{Z}$ *is an integral domain.*

Exercise 2.3. *Let $R = \mathbb{Z}$, and consider the ideal $I = nZ = \{nz \mid z \in \mathbb{Z}\}$. Then R/I is the ring $\mathbb{Z}/n\mathbb{Z}$, the ring of integers modulo n. We can think of elements of $\mathbb{Z}/n\mathbb{Z}$ as being elements in the set*

$$\{0, 1, \dots, n-1\},$$

with the ring operations being defined by

$$ab = ab \pmod{n}, \quad a + b = (a+b) \pmod{n}.$$

Then $\mathbb{Z}_{\mathbb{Z}}/n\mathbb{Z}$ is a field if and only if n is a prime number. For n prime we write $\mathbb{F}_n$ for $\mathbb{Z}/n\mathbb{Z}$.

Exercise 2.4. *Let $F = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$. Then F is a field.*

Exercise 2.5. *Let $\phi : R \to S$ be a ring homomorphism. Then $\ker(\phi)$ is an ideal of R, $\mathrm{im}(S)$ is a subring of S, and, moreover,*

$$R/\ker(\phi) \cong \mathrm{im}(S).$$

2.2. **The characteristic.**

Definition 4. *Let K be a field. The* **prime subfield** *of K is the intersection of all subfields of K.*

Note that the prime subfield must contain the elements 0 and 1.

Theorem 2.6. stewart [Ste03, p.3] *Every prime subfield is isomorphic to $\mathbb{Q}$ or to the field $\mathbb{F}_p$, for p some prime.*

If K has prime subfield isomorphic to $\mathbb{Q}$, then we say K *has characteristic* 0. If K has prime subfield isomorphic to $\mathbb{F}_p$, then we say that K *has characteristic p.*

Exercise 2.7. *If K is a subfield of L, then K and L have the same characteristic.*

If n is an integer, and k and element of the field K, then we write nk to mean

$$\underbrace{k + \cdots + k}_{n} = (\underbrace{1 + \cdots + 1}_{n})k.$$

Exercise 2.8. *If K is a non-zero element of the field K, and if n is an integer such that $nk = 0$, then n is a multiple of the characteristic of K.*

2.3. Fields of fractions.

Definition 5. *A* **field of fractions** *for a ring R is a field K containing a subring R' isomorphic to R, such that every element of K can be expressed in the form $\frac{r}{s}$ for $r, s \in R'$, where $s \neq 0$.*

Note that this definition generalizes the relationship of the field $\mathbb{Q}$ to the ring $\mathbb{Z}$. Just as in that example, one shouldn't assume that an element has a unique expression $\frac{r}{s}$ (for instance $\frac{1}{2} = \frac{2}{4}$ in $\mathbb{Q}$).

Theorem 2.9. [Ste03, p.5] *Every integral domain possesses a field of fractions.*

3. Polynomials

Definition 6. *Let R be a ring. A* **polynomial over R in the indeterminate** *t is an expression*

$$a_n t^n + a_{n-1} t^{n-1} + \cdots + a_1 t + a_0, \tag{3.1}$$

in which $n \in \mathbb{Z}^+$, and $a_0, \ldots, a_n \in R$. The quantity a_i is called the **coefficient of** *t^i; note that if $a_i = 0$ then we often omit it.*

If $i > n$, then we sometimes like to think that a_i exists, and is equal to 0. This allows us to write polynomials as $\sum a_i t^i$ where the sum is considered overal all integers $i \geq 0$.

Given two polynomials $\sum a_i t^i$ and $\sum b_i t^i$, we define

$$\sum a_i t^i + \sum b_i t^i = \sum (a_i + b_i) t^i, \text{ and}$$
$$\sum a_i t^i \cdot \sum b_i t^i = \sum c_i t^i,$$

where $c_j = \sum_{h+i=j} a_h b_i$. The set of all polynomials over R in indeterminate t is a ring, $R[t]$, the *ring of polynomials over R in the indeterminant t.*

Exercise 3.1. *Let $R = \mathbb{Z}$. Define $f = 3t + 1$, $g = 4t^3 + 2t - 7l$ calculate $f + g$, and fg.*

Now take $f \in R[t]$, $f \neq 0$; it can be written in the form (3.1), with $a_n \neq 0$. Then we say that f has *degree* n, write $\deg f = n$. We call a_n the *leading coefficient* of f; if $a_n = 1$, then we call f *monic.* (If $f = 0$ then, by convention, we say that $\deg f = -\infty$.)

Note that there is a natural ring monomorphism

$$R \to R[t], \lambda \mapsto 0t + \lambda.$$

This embeds R into $R[t]$ and the image of R is just the set of *constant polynomials.*

Lemma 3.2. *Let R be an integral domain. Then $R[t]$ is an integral domain.*

Proof. Take $f, g \in R[t]$ non-zero. Then they have nonzero leading coefficients, call these a and b. The product fg in $R[t]$ has leading coefficient ab. Since R is an integral domain we know that $ab \neq 0$; we conclude therefore that $fg \neq 0$, as required. ☐

3.1. **The Euclidean algorithm.** Throughout this section K is a field. In this section we establish a number of facts about $K[t]$ that mirror properties of $\mathbb{Z}$ with which we are (hopefully!) already familiar. We start with a simple observation:

e: degree **Exercise 3.3.** *If R is an integral domain and $f, g \in R[t]$, then*

$$\begin{aligned} \deg(f+g) &\leq \max\{\deg f, \deg g\}; \\ \deg(fg) &= \deg f + \deg g. \end{aligned}$$

(Why the inequality in the first line?)

Proposition 3.4. *(Division algorithm) Let f and g be polynomials over a field K, and suppose that f is non-zero. Then there exist unique polynomials q and r over K such that*

$$g = qf + r$$

and $\deg r < \deg f$.

Proof. We start by showing that q and r exist; we proceed by induction on $\deg g$. If $\deg g < \deg f$ then $g = 0f + g$, and we are done. If $\deg f = 0$ then $f = j \in K$ and we may take $q = k/j$ and $r = 0$. So assume that $0 < \deg f \leq \deg g$.

Thus, we take $m \leq n$, and

$$\begin{aligned} f &= a_m t^m + \cdots + a_0, \\ g &= b_n t^n + \cdots + b_0, \end{aligned}$$

where $a_m \neq 0 \neq b_n$. Let

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

Then $\deg g_1 < \deg g$ since leading terms cancel. Thus, by the inductive hypothesis,

$$g_1 = q_1 f + r_1,$$

with $\deg r_1 < \deg f$. But then

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

and, since $\deg r_1 < \deg f$, we have the desired representation.

We must now prove uniquess. Suppose that

$$g = fq_1 + r_1 = fq_2 + r_2, \text{ where } \deg r_1, \deg r_2 < \deg f.$$

Then

$$f(q_1 - q_2) = r_2 - r_1.$$

Now we use Ex. e: degree 3.3. If $q_1 \neq q_2$, then the left-hand side of this equation is a non-zero polynomial with degree at least $\deg f$. The right-hand side has degree strictly less than $\deg f$, thus we have a contradiction.

We conclude that $q_1 = q_2$ and, therefore, that $r_1 = r_2$. Thus q and r are unique. ☐

p: pid **Proposition 3.5.** *If K is a field then $K[t]$ is a principal ideal domain.*

Proof. Let I be a non-trivial ideal of $K[t]$; we need to prove that $I = (f) = \{fg \mid g \in K[t]\}$ for some $f \in K[t]$. Let f be a non-zero polynomial of minimal degree in I. If $g \in J$ then the Division Algorithm implies that there exists $q, r \in K[t]$ such that $g = qf + r$ with $\deg(r) < \deg(f)$. Now $r = q - gj \in J$ and, since f is of minimal degree, we conclude that $r = 0$. In other words $f \mid g$ and $g \in (f)$. Thus $I \subseteq (f)$; since $(f) \subseteq I$ we conclude that $I = (f)$ as required. □

Take $f, g \in K[t]$. We say that f *divides* g and write $f \mid g$, when there exists $h \in K[t]$ such that $g = fh$. If f does not divide g then we write $f \nmid g$.

Definition 7. *A polynomial $d \in K[t]$ is a* **highest common factor (h.c.f)** *of f and g if $d \mid f$ and $d \mid g$ and further, whenever $e \mid f$ and $e \mid g$ we have $e \mid d$. We often write (f, g) for a highest common factor of f and g. If 1 is a highest common factor of f and g then we call f and g* **relatively prime**.

Exercise 3.6. *Take $d, e, f, g \in K[t]$. If d is an h.c.f. of f and g, and $k \in K^*$, then kd is also a h.c.f. of f and g.*

If d and e are two h.c.f.'s of f and g, then there exists $k \in K^*$ such that $e = kd$.

The polynomial d is a common factor of f and g of largest degree if and only if d is a h.c.f. of f and g.

Theorem 3.7. (Euclidean algorithm for polynomials) *Let $f, g \in K[t]$. Write $r_{-1} = g, r_0 = f$ and define q_i and r_i for $i \geq 1$ via the relation*

e: descent

$$r_{i-2} = q_i r_{i-1} + r_i, \tag{3.2}$$

in which $\deg r_i < \deg r_{i-1}$. Then, for some non-negative integer I, one has $r_I = 0$ and then a highest common factor of f and g is r_{I-1}.

Proof. Clearly the algorithm is well-defined: the sequence $(\deg r_i)i \geq 0$ is decreasing and bounded below by zero; thus the algorithm terminates with an integer I such that $r_I = 0$.

Next we prove that r_{I-1} divides both f and g by examining equation (3.2) for different values of i. Setting $i = I$, we observe that, since $r_I = 0$, r_{I-1} divides r_{I-2}. Setting $i = I - 1$, this in turn implies that r_{I-1} divides r_{I-3}. Continuing in this way we find that r_{I-1} divides $r_0 = g$ and $r_{-1} = f$.

Now suppose that $e \mid f$ and $\mid g$. Then (3.2) implies that e divides $r_1, r_2, \ldots, r_{I-1}$. Thus r_{I-1} is an h.c.f of f and g. □

This result is sometimes expressed in the literature as: $K[t]$ *is a Euclidean Domain.* Let us work through an example: we find a highest common factor of $g = t^5 - 3t + 2$ and $f = t^2 - 2t + 1$ in $\mathbb{Q}[t]$:

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

Thus $2t - 2$ is a h.c.f. of f and g in $\mathbb{Q}[t]$. In fact $t - 1$ is also a h.c.f. of f and g.

Exercise 3.8. *Take f and g in the example but consider them as polyomials in $\mathbb{F}_2[t]$. Now find a h.c.f.*

t: ab **Theorem 3.9.** *Let d be a h.c.f of f and g in $K[t]$. Then there exist polynomials $a, b \in K[t]$ such that*

$$d = af + bg.$$

Proof. We apply the Euclidean algorithm in reverse: as before write $r_{-1} = g, r_0 = f$ and define q_i and r_i for $i \geq 1$ via the relation

e: descent2
$$r_{i-2} = q_i r_{i-1} + r_i, \tag{3.3}$$

in which $\deg r_i < \deg r_{i-1}$. Let I be the smallest non-negative integer such that $r_I = 0$; then r_{I-1} is a highest common factor of f and g. Since h.c.f's are unique up to constant factors we may assume that $d = r_{I-1}$.

Now by (3.3) with $i = 1$, r_1 is a linear combination of r_{-1} and r_0. Indeed for $i > 1$, r_i is a linear combination of r_{i-1} and r_{i-2}. Thus, by induction, every r_i is a linear combination of r_{-1} and r_0.

In particular this is true for $i = I - 1$. Thus there are polynomials $a, b \in K[t]$ such that

$$r_{I-1} = af + bg.$$

□

Note that, for given f and g, this proof gives a method for calculating a and b.

3.2. Factorization of polynomials.

Throughout this section R is a ring, K a field.

Definition 8. *An* **irreducible polynomial** *in $R[t]$ is a non-constant polynomial which cannot be written as a prodcut of two polynomials of smaller degree. A polynomial which is not irreducible is* **reducible**.

Note that all polynomials of degree 0 are reducible, while those of degree 1 are irreducible. Beware: some texts define degree 0 polynomials to be irreducible.

The irreducible polynomials in $R[x]$ are analogous to the prime numbers in $\mathbb{Z}$. This should become clear as we prove various prime-number type properties...

Exercise 3.10. *Is the polynomial $f = t^2 - 2 \in \mathbb{Q}[t]$ reducible? Is the polynomial $f = t^2 - 2 \in \mathbb{R}[t]$ reducible?*

l: divisible **Lemma 3.11.** *Suppose that $f, g, h \in K[t]$ and that f is irreducible. If $f \mid gh$ then either $f \mid g$ or $f \mid h$.*

Proof. Suppose that $f \nmid g$. A h.c.f. of f and g divides f which is irreducible. Thus such an h.c.f. must equal λ for some $\lambda \in K^*$. But then there exist $a, b \in K[t]$ such that

$$\lambda = af + bg.$$

Then

$$h = \lambda^{-1}(af + bg)h = (\lambda^{-1}ah)f + \lambda^{-1}b(gh).$$

Now, since f divides gh, we conclude that f divides the term on the right-hand side of the equation. Thus $f \mid h$. □

t: uft **Theorem 3.12.** (Unique factorization theorem) *If $f \in K[t]$, and $\deg f \geq 1$, then f can be written as a product of irreducible polynomials in $K[t]$, and this factorization is unique apart from the order of the irreducible factors and the presence of constant factors.*

Proof. Any polynomial $f \in K[t]$ can be written as a product of irreducible polynomials. For, if it is not irreducible, it is a product of polynomials of positive degree, and so the conclusion follows by induction.

Now we need to prove that this product is unique up to ordering and constant factors. Suppose that $f = g_1 \cdots g_r = h_1 \cdots h_s$, with each of g_i, h_j irreducible. Lem. l: divisible 3.11 implies that $g_1 \mid h_1$ for some $1 \leq i \leq s$. Without loss of generality assume that $g_1 = h_1$, so $g_1 = \lambda_1 g_1$ for some $\lambda_1 \in K^*$. Then

$$\begin{aligned} (\lambda_1 g_1) h_2 \cdots h_s &= g_1 \cdots g_r \\ \Longrightarrow g_1(\lambda_1 h_2 \cdots h_s - g_2 \cdots g_r) &= 0. \end{aligned}$$

Since $K[t]$ is an integral domain we conclude that

$$g_2 \cdots g_r = (\lambda_1 h_2) h_3 \cdots h_s.$$

An inductive argument implies that we can choose an ordering such that $h_i = \lambda_i g_i$ for $1 \leq i \leq r$. We then obtain

$$h_{r+1} \cdots h_s = \lambda,$$

a constant. Thus $r = s$, and our factorization is unique up to constant factors. $\square$

This result is sometimes expressed in the literature as: *$K[t]$ is a Unique Factorization Domain (UFD).* This is a broader class of objects than the Euclidean domains mentioned earlier.

Corollary 3.13. *If $f \in K[t]$ is monic, and $\deg f \geq 1$, then f can be written as a product of irreducible monic polynomials in $K[t]$, and this factorization is unique apart from the order of the irreducible factors.*

Exercise 3.14. *Prove this corollary!*

3.3. **Zeros of polynomials.**

Definition 9. *Let R be a ring, $f \in R[t]$. We say that $\alpha \in R$ is a* **zero** *or a* **root** *of $f \in R[t]$ if $f(\alpha) = 0$.*

l: root **Lemma 3.15.** *Let K be a field and suppose that $\alpha \in K$ and $f \in K[t]$. Then $f(\alpha) = 0$ if and only if $(t - \alpha) \mid f$.*

Proof. Suppose, first of all, that $(t - \alpha) \mid f$; then $f = (t - \alpha)g$ for some $g \in K[t]$. But then $f(\alpha) = (\alpha - \alpha)g(\alpha) = 0$.

On the other hand suppose that $f(\alpha) = 0$. By the division algorithm there exist $a, r \in K[t]$ such that $f = q(t - \alpha) + r$ where $\deg r < 1$, i.e. $r = \lambda$ for some $\lambda \in K$. Then

$$0 = f(\alpha) = q(\alpha)(t - \alpha) + \lambda = \lambda.$$

Thus $f = q(t - \alpha$ and $(t - \alpha) \mid f$. $\square$

Note that this lemma, along with Thm. t: uft 3.12 implies the following crucial fact: if $f \in K[t]$ has degree n, then f has at most n roots.

Note too that we will often be concerned with the question of when a given polynomial f is irreducible; Lem. l: root 3.15 gives us one useful test. We will discuss other such tests later.

Exercise 3.16. *Show that the polynomial $f(t) = t^3 + t + 2$ is irreducible in $\mathbb{F}_3[t]$.*

4. Field extensions

We begin with a construction that will be very important throughout the rest of the course. Take a polynomial $f \in K[t]$, where K is some field. Consider the quotient ring $K[t]/(f)$ (by (f) we mean the ideal $\{fg \mid g \in K[t]\}$).

l: irred **Lemma 4.1.** *If f is irreducible then $K[t]/(f)$ is a field.*

Proof. We need to check the field axioms. The only one that presents a serious challenge is to show that every non-zero element of $K[t]/(f)$ has an inverse.

Take $g \in K[t]$. Then g is in a non-zero residue class of $K[t]/(f)$ if and only if f does not divide into g. But now, since f is irreducible, this implies that any highest common factor of f and g will be a constant.

Then Theorem t: ab 3.9 implies that there exist polynomials a and b such that

$$d = af + gb,$$

where d is a constant. Then

$$\begin{aligned} 1 &= (d^{-1}a)f + (d^{-1}b)g \\ \implies (d^{-1}a)f &= 1 \pmod{f}. \end{aligned}$$

□

What does $K[t]/(f)$ look like? Assume that f is irreducible of degree d. The Division Algorithm implies that every residue class in $K[t]/(f)$ contains **precisely one** polynomial of degree at most $d-1$. Thus the set of residues is in 1-1 correspondece with the set

$$\{a_0 + a_1 t + \cdots + a_{d-1}t^{d-1} \mid a_i \in K\}.$$

Exercise 4.2. *Prove that, as an additive group, $K[t]/(f)$ is isomorphic to K^d.*

Note that the set of special residue classes which contain the constant polynomials a_0 (for some $a_0 \in K$) form a field isomorphic to K. In other words the field K lies inside the field $K[t]/(f)$. This motivates our next definition.

Definition 10. *A* **field extension** *of a field K is a triple (i, K, L) where L is a field, and i is a ring monomorphism of K into L. We identify the image $i(K)$ with K, and think of K lying inside L; we then denote the field extension $L : K$, or L/K (omitting mention of i).*

Some examples:

- The field extension $\mathbb{C} : \mathbb{R}$ is formally given by

$$i : \mathbb{R} \to \mathbb{C},\ x \mapsto x + 0i.$$

- Likewise with $\mathbb{C} : \mathbb{Q}$, or $\mathbb{R} : \mathbb{Q}$.
- The construction we considered above yielded a field extension $K[t]/(f) : K$.

4.1. **Degree.**

Theorem 4.3. *Let $L : K$ be a field extension. Under the operations*

$$L \times L \to L, (l_1, l_2) \mapsto l_1 + l_2, \text{ and}$$
$$K \times L \to L, (k.l) \mapsto kl,$$

L forms a vector space over K.

The first operation is *vector addition*, the second *scalar multiplication.* So in this vector space the scalars are elements of K, the vectors are elements of L.

Proof. Check that the axioms for a vector space are satisfied by $L : K$. ☐

So in all the examples of field extensions that we gave earlier, we were also listing vector spaces!

Definition 11. *The* **degree of an extension** *$L : K$ is the dimension of L as a vector space over K. We write $[L : K]$ for the degree of $L : K$. We call the extension* **finite** *if $[L : K] < \infty$, and* **infinite** *if $[L : K] = \infty$.*

Exercise 4.4. *Calculate the degree of the extensions that were listed above. The only (slightly) hard one is the degree of the extension $K[t]/(f)$.*

Theorem 4.5. *Suppose that $M : L$ and $L : K$ are field extensions. Then $M : K$ is a field extension, and*

$$[M : K] = [M : L][L : K]. \tag{4.1}$$

Proof. That $M : K$ is a field extension is immediate (compose the inclusion maps given by $M : L$ and $L : K$). We need to prove the identity (4.1).

Suppose first that the RHS is finite. Thus $[M : L] = m \in \mathbb{Z}^+$ and $[L : K] = n \in \mathbb{Z}^+$. Let $\{e_1, \dots, e_m\}$ be a basis for M over L, and let $\{f_1, \dots, f_n\}$ be a basis for L over K. We claim that the lm elements $e_i f_j, 1 \leq i \leq m, 1 \leq j \leq n$, form a basis for M over K. This claim implies immediately that

$$[M : K] = lm = [L : K][K : M],$$

as required.

We prove first that

$$M \subseteq \text{span}\{e_i f_j \mid 1 \leq i \leq m, 1 \leq j \leq n\}.$$

Let z be an element of M. Then, since $\{e_1, \dots, e_m\}$ is a basis for M over L,

$$z = a_1 e_1 + \cdots + a_m e_m,$$

for elements $a_1, \dots, a_m$ in L. Now, since $\{f_1, \dots, f_n\}$ is a basis for L over K, we have for each $i = 1, \dots, m$,

$$a_i = b_{i1} f_1 + \cdots + b_{in} f_n,$$

for elements $b_i 1, \dots, b_i n$ in K. This implies that

$$z = \sum_{i=1}^{m} \sum_{j=1}^{n} b_{ij} e_i f_j,$$

as required.

Next we prove linear independence. Suppose that

$$\sum_{i=1}^{m}\sum_{j=1}^{n} c_{ij}e_i f_j = 0$$

for some elements $c_{ij}, 1 \leq i \leq m, 1 \leq j \leq n$. This implies that

$$\left(\sum_{i=1}^{m} c_{i1}e_i\right) f_1 + \cdots + \left(\sum_{i=1}^{m} c_{in}e_i\right) f_n = 0.$$

Since $\{f_1, \dots, f_n\}$ is a basis for L over K this implies that $\sum_{i=1}^{m} c_{ij}e_i$ for each $j = 1, \dots, n$. But now, since $\{e_1, \dots, e_m\}$ is a basis for M over L, this implies that c_ij for all i, j. Linear independence is proved.

Suppose next that the RHS is not finite; we need to show that the LHS is not finite. Suppose that, instead, $[M : K] = n < \infty$. Then we can find a basis $\{g_1, \dots, g_l\}$ for M over K. But $\{g_1, \dots, g_n\}$ spans M over K, so it certainly spans M over L. Thus $[M : L] < \infty$. Moreveor L is a K-linear subspace of M so $[L : K] < \infty$. Then $[M : L][L : K] < \infty$ which is a contradiction, as required. ☐

Definition 12. *A sequence $K_n : K_{n-1}, K_{n-1} : K_{n-2}, \dots, K_1 : K_0$ is called a* **tower** *of field extensions, and we write it as $K_n : K_{n-1} : \cdots : K_1 : K_0$.*

Exercise 4.6. *Generalize the previous theorem to towers of arbitrary length. Thus, for a tower, $K_n : k_{n-1} : \cdots : K_1 : K_0$, prove that*

$$[K_n : k_{n-1} : \cdots : K_1 : K_0] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_1 : K_0].$$

Exercise 4.7. *Suppose that $L : K$ is a field extension with $[L : K]$ prime. Then there exists no subfield M of L containing K other than K itself.*

4.2. **Simple extensions.**

Definition 13. *Suppose that $L : K$ is a field extension and $A \subset L$. Write $K(A)$ for the intersection of all subfields of L that contain K and A. We call $K(A)$ the extension of K* **generated by** *A. If $A = \{a_1, \dots, a_n\}$ then write $K(a_1, \dots, a_n)$ for $K(A)$. We call $L : K$ a* **simple extension** *if $L = K(\alpha)$ for some $\alpha \in L$; we say L is* **finitely generated over** *K if $L = K(A)$ for a finite set A.*

Note that $K(A)$ is a field, in fact the smallest subfield of L containing both K and A. Some examples:

- $\mathbb{C} = \mathbb{R}(i)$, a simple extension.
- The set $\{a+b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ which we encountered earlier is a simple field extension of $\mathbb{Q}$; it is $\mathbb{Q}(\sqrt{2})$.
- $\mathbb{C} : \mathbb{Q}$ is not simple (since any simple extension of a countable field is countable).
- The field extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ is simple even though it does not appear to be! To see this, define $\alpha = \sqrt{2} + \sqrt{3}$. Then

$$\alpha^2 = 5 + 2\sqrt{6},$$

and, in particular, $\sqrt{6} = \frac{1}{2}(\alpha^2 - 5) \in \mathbb{Q}(\alpha)$. This implies that

$$(\sqrt{6} - 2)\alpha = \sqrt{2} \in \mathbb{Q}(\alpha);$$
$$(3 - \sqrt{6})\alpha = \sqrt{3} \in \mathbb{Q}(\alpha).$$

Thus $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$; in other words $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\alpha)$, a simple extension of $\mathbb{Q}$.

- It is useful to imagine what a field extension looks like in general. Consider the previous example, $\mathbb{Q}(\sqrt{2}, \sqrt{3})$. Observe that this must contain the set

$$S = \{ a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q} \}.$$

If we can prove that S is a field then, by definition, $S = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. In fact, proving this is easy; an immediate consequence is that $[\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}] = 4$.

You might also like to consider the example $\mathbb{Q}(\sqrt[3]{2})$. Can you find a "natural" basis for this extension? What is its degree? We will give a result later that answers this sort of question for general field extensions $K(A)$.

4.3. **Algebraic extensions.**

Definition 14. *Suppose that $L : K$ is a field extension, and that $\alpha \in L$. If there is a polynomial $f = a_n t^n + \cdots a_1 t + a_0 \in K[t]$ for which $f(\alpha) = 0$, then we say that α is* **algebraic** *over K. If no such polynomial exists, then we say that α is* **transcendental** *over K.*

Observe that, since L is a vector space over K, the element α is algebraic if the set $\{1, \alpha, \ldots, \alpha^n\}$ is linearly independent for some natural number n. Conversely α is transcendental if $\{1, \alpha, \ldots, \alpha^n\}$ is linearly independent for each $n \in \mathbb{N}$.

It is a fact (not easily proved) that π, e and $2^{\sqrt{2}}$ are transcendental over $\mathbb{Q}$. In fact the set of transcendental elements in $\mathbb{R}$ has measure 1. (When applied to real numbers, the adjective *transcendental* is always relative to $\mathbb{Q}$ unless otherwise stated.)

Definition 15. *Suppose that $L : K$ is a field extension and $\alpha \in L$. We define the* **evaluation map***,*

$$E_\alpha : K[t] \to L,\ f \mapsto f(\alpha).$$

Observe that E_α is a ring homomorphism. What is more

- α is transcendental if and only if $\ker(E_\alpha) = \{0\}$;
- α is algebraic if and only if $\ker(E_\alpha) \neq \{0\}$.

Since $K[t]$ is a principal ideal domain we know that $\ker(E_\alpha) = (f)$, for some polynomial f. If α is algebraic, then f is non-zero; in fact we may take f to be monic, and this defines f uniquely (see the proof of Prop. p: pid 3.5.)

Definition 16. *The* **minimal polynomial** *of the element $\alpha \in L$ from a field extension $L : K$ is the monic polynomial m_α such that* $\ker(E_\alpha) = (m_\alpha)$.

The next theorem connects the two primary constructions of field extensions that we have seen: $K[t]/(f)$ for irreducible f, and $K(\alpha)$. First of all we need to formally define what it means for two field extensions to be the same.

d: field extension

Definition 17. *Let (i_1, K_1, L_1) and (i_2, K_2, L_2) be two field extensions. An* **isomorphism of field extensions** *is a pair (λ, μ) of field isomorphism $\lambda : K_1 \to K_2$, $\mu : L_1 \to L_2$ such that the following diagram commutes:*

$$\begin{tikzcd} K_1 \arrow[r, "i_1"] \arrow[d, "f"'] & L_1 \arrow[d, "g"] \\ K_2 \arrow[r, "i_2"'] & L_2. \end{tikzcd}$$

Of course, most of the time we do not think of field extensions in terms of monomorphisms; instead we identify $i_j(K_j)$ and K_j, so that K_j is just a *subfield* of L_j $(j = 1, 2)$. In this formulation, an isomorphism of field extensions is a field isomorphism $\mu : L_1 \to L_2$ such that

$$\mu\, |_{K_1} = K_2.$$

t: cd

Theorem 4.8. *Suppose that $L : K$ is a field extension, and that $\alpha \in L$ is algebraic. Then*

(a) *the minimal polynomial m_α of α is irreducible in $K[t]$;*
(b) *the image $E_\alpha(K[t])$ of the polynomial ring $K[t]$ is the subfield $K(\alpha)$ of L;*
(c) *the evaluation map E_α factorizes as $i\tilde{E}_\alpha q$ in the following way:*

$$\begin{tikzcd} K[t] \arrow[r, "E_\alpha"] \arrow[d, "q"'] & L \\ K[t]/(m_\alpha) \arrow[r, "\tilde{E}_\alpha"'] & K(\alpha). \arrow[u, "i"'] \end{tikzcd}$$

Here q is the quotient map, i is the inclusion map, and $\tilde{E}_\alpha$ is an isomorphism of field extensions.

Proof. (a) Suppose that $m_\alpha = fg$. Then applying the evaluation map we obtain

$$0 = E_\alpha(m_\alpha) = E_\alpha(f)E_\alpha(g) = f(\alpha)g(\alpha).$$

Then, without loss of generality, $f(\alpha) = 0$. Thus $f \in (m_\alpha)$ and so $m_\alpha \mid f$. In particular $\deg(m_\alpha) = \deg(f)$, and m_α is irreducible.

(b) The field $E_\alpha(K[t])$ is a subfield of L. Furthermore $E_\alpha(k) = k$ for $k \in k$, and $E_\alpha(t) = \alpha$. Thus $K \cup \{\alpha\} \subseteq \mathrm{im}(E_\alpha)$ and so $K(\alpha) \subseteq \mathrm{im}(E_\alpha)$. On the other hand it is obvious that $\mathrm{im}(E_\alpha) \subseteq K(\alpha)$, so we are done.

(c) Since m_α is irreducible, Lem. l: irred 4.1 implies that $K[t]/(m_\alpha)$ is a field. The ring isomorphism theorem implies that one has the following factorization:

$$\begin{tikzcd} K[t] \arrow[r, "E_\alpha"] \arrow[d, "q"'] & L \\ K[t]/\ker(E_\alpha) \arrow[r, "\cong"'] & \mathrm{im}(E_\alpha), \arrow[u, "i"'] \end{tikzcd}$$

which yields the result.

□

Recall that, given an irreducible polynomial $f \in K[t]$, we have a good understanding of what the field $K[t]/(f)$ looks like: its elements are in 1-1 correspondence with polynomials in t of degree strictly smaller than f. This information can now be used to understand the structure of field extensions of form $K(A)$, especially $K(\alpha)$: in particular, observe that the ring homomorphism $E_\alpha : K[t] \to L$ maps t to α. Following the proof above, we conclude that, if $\deg(m_\alpha) = n$, the elements of the field $K(\alpha)$ are in 1-1 correspondence with the set

$$\{a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0 \mid a_0, \ldots, a_{n-1} \in K\}.$$

For instance, recall the example of a field

$$F = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

We have already seen that $F = \mathbb{Q}(\sqrt{2})$. One can easily check that, for $\alpha = \sqrt{2}$, the minimal polynomial over $\mathbb{Q}$ is $m_\alpha = t^2 - 2$. Thus $F \cong \mathbb{Q}[t]/(t^2 - 2)$ and we also have a 1-1 correspondence between F and the set

$$\{a + bt \mid a, b \in \mathbb{Q}\}.$$

These different representations of the same field have their advantages, mostly when it comes to multiplying elements.

t: algebraic

Theorem 4.9. *Suppose that $L : K$ is a field extension, and that $\alpha \in L$. Then α is algebraic over K if and only if $[K(\alpha) : K] < \infty$, in which case $[K(\alpha) : K] = \deg(m_\alpha)$.*

Proof. Suppose that $[K(\alpha) : K] = n < \infty$. Now $K(\alpha)$ is a vector space over K of dimension n and so the elements $1, \alpha, \alpha^2, \ldots, \alpha^n$ are linearly independent in $K(\alpha) : K$. Thus, for some $k_0, \ldots, k_n \in K$ not all zero, we have

$$k_n\alpha^n + \cdots k_1\alpha + k_0 = 0.$$

Then the polynomial $k_nt^n + \cdots k_1t + k_0 \in \ker(E_\alpha)$. Thus $\ker(E_\alpha) \neq \{0\}$, and so α is algebraic over K.

Now for the converse: suppose that α is algebraic over K, and m_α is its minimal polynomial. Let $n = \deg(m_\alpha)$ and suppose that $1, \alpha, \ldots, \alpha^{n-1}$ are linearly dependent over K. Then there exist $k_0, \ldots, k_{n-1} \in K$, not all zero, satisfying

$$k_{n-1}\alpha^{n-1} + \cdots + k_1\alpha + k_0 = 0.$$

This implies that $\deg(m_\alpha) < n$ which is a contradiction. We conclude that $1, \alpha, \ldots, \alpha^{n-1}$ are linearly independent over K.

The result follows if we can show that the set $\{1, \alpha, \ldots, \alpha^{n-1}\}$ spans $K(\alpha)$, since this set will then be a basis of $K(\alpha)$. So take $\beta \in K(\alpha)$ and observe that $\beta = E_\alpha(f)$ for some $f \in K[t]$. We can write $f = m_\alpha q + r$ where $\deg r < n$. Then

$$\beta = E_\alpha(f) = E_\alpha(m_\alpha)E_\alpha(q) + E_\alpha(r) = E_\alpha(r).$$

Thus if $r = k_{n-1}t^{n-1} + \cdots + k_1t + k_0$, then

$$\beta = k_{n-1}\alpha^{n-1} + \cdots + k_1\alpha + k_0 \in \text{span}\{1, \alpha, \ldots, \alpha^{n-1}\}$$

as required. $\square$

Definition 18. *For $L : K$ a field extension define the set L^{alg} to be those elements of L which are algebraic over K.*

Theorem 4.10. *If $L : K$ is a field extension then L^{alg} is a subfield of L.*

Proof. We need to check that $(L^{alg}, +)$ and $(L^{alg}\backslash\{0\}, \cdot)$ are abelian groups. Since they are sets inside larger abelian groups we just need to check closure under composition and inversion in each case.

Suppose that α and β are algebraic over K. Then $m_\beta \in K[t] \subseteq K(\alpha)[t]$. Thus β is algebraic over $K(\alpha)$. Then Thm. t: algebraic 4.9 implies that

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

But then

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

Now observe that $K(\alpha+\beta)$, $K(-\alpha)$, and $K(\alpha\beta)$ are all subfields of $K(\alpha, \beta)$. Furthermore, if $\alpha \neq 0$, then $K(\alpha^{-1})$ is a subfield of $K(\alpha, \beta)$. Thus they are all finite extensions of K, and so $\alpha + \beta$, $-\alpha$, $\alpha\beta$, and α^{-1} are all algebraic as required. ☐

Definition 19. *A field extension $L : K$* **is algebraic** *if every element of L is algebraic over K. i.e. $L = L^{alg}$.*

Theorem 4.11. *Suppose that $L : K$ is a field extension. The following are equivalent:*

(a) *$[L : K] < \infty$;*
(b) *$L : K$ is algebraic, and L is finitely generated over K;*
(c) *L is finitely generated over K*

Proof. First we prove (a) $\implies$ (b). Suppose that $[L : K] = s < \infty$. If $\alpha \in L$, then

$$[K(\alpha) : K] \leq [L : K] < \infty,$$

so α is algebraic over K. Thus $L : K$ is algebraic. Moreover if $\{\gamma_1, \dots, \gamma_s\}$ is a basis for L over K, then $L = K(\gamma_1, \dots, \gamma_s)$, and L is finitely generated over K.

(b) $\implies$ (c) is trivial. So now prove (c) $\implies$ (a). Suppose that $L = K(\alpha_1, \dots, \alpha_n)$. Define

$$K_0 = K,\, K_1 = K_0(\alpha_1), K_1 = K_2(\alpha_2), \dots, K_n = K_{n-1}(\alpha_n) = L.$$

Then $[K_j : K_{j-1}]$ is finite for $1 \leq j \leq n$, since α_j is algebraic in each case. Thus

$$[L : K] = [K_n : K_{n-1}] \cdots [K_2 : K_1][K_1 : K_0] < \infty,$$

as required. ☐

Let $L : K$ be a field extension, $\alpha \in L$. We have a number of equivalent statements:

(a) α is algebraic;
(b) $f(\alpha) = 0$ for some non-zero $f \in K[t]$;
(c) $\ker(E_\alpha) \neq \{0\}$;
(d) α has a well-defined non-zero minimal polynomial;
(e) $K(\alpha) : K$ is algebraic.

Of course one has a load of similar statements if one starts instead with α *is transcendental.*

Exercise 4.12. *Suppose that $M : L$ and $L : K$ are algebraic extension. Then $M : K$ is algebraic.*

We have proved a lot of results about algebraic extensions, and almost entirely neglected transcendental extensions. However that's because, when the extension is simple, there is only one transcendental extension. So everything's (kind of) easy!

Exercise 4.13. *Every simple transcendental extension $K(\alpha) : K$ is isomorphic to the extension $K(t) : K$ of rational expressions in an indeterminate t over K. The isomorphism can be chosen to carry t into α.*

5. Ruler and compass constructions

This section can be thought of as a bit of a diversion from the main mathematical train of thought. But the results we discuss here are not only beautiful, they are also historically very important. Some of the problems we solve in this section were open for upwards of 2000 years.

Here is the set-up: Assume two points P_0 and P_1 are given in $\mathbb{R}^2$. By rescaling and rotation, there is no loss of generality in supposing these points to be $P_0 = (0, 0)$ and $P_1 = (1, 0)$. We can then make the following definition:

Definition 20. *A point $P \in \mathbb{R}^2$ is* **constructible** *if there exists a sequence of points $P_0, P_1, \dots, P_n = P$ with the following property. Write $A_j = \{P_0, \dots, P_j\}$ for $2 \leq j \leq n$. The for each j with $2 \leq j \leq n$, the point P_j is one of:*

(a) *the intersection of two distinct lines, each joining two points in A_{j-1};*
(b) *the intersection of a line L and a circle C where*
  - *L joins two points in A_{j-1};*
  - *the centre of C is a point of A_{j-1} and the radius of C is equal to the distance between two points of A_{j-1};*

(c) *the intersection of two circles with distinct centres in A_{j-1}, and so that both radii are equal to the respective distances of two pairs of points of A_{j-1}.*

Now let us see how this relates to Galois theory:

Theorem 5.1. *If $P = (x, y)$ is a constructible point, then the field extension $\mathbb{Q}(x, y) : \mathbb{Q}$ is finite and satisfies $[\mathbb{Q}(x, y) : \mathbb{Q}] = 2^r$ for some natural number r.*

Proof. Since P is constructible, there exists a finite sequence, $P_0, P_1, \dots, P_n = P$ generated in the process describe above. For $j = 0, \dots, n$, write $P_j = (x_j, y_j)$ and

$$K_j = \mathbb{Q}(x_0, y_0, x_1, y_1, \dots, x_j, y_j).$$

Observe that $K_j = K_{j-1}(x_j, y_j)$. We make the following claim:

Claim: For $j = 2, \dots, n$, $[K_j : K_{j-1}] \in \{1, 2\}$.

Proof that the claim implies the theorem: Observe that $\mathbb{Q}(x, y)$ is a subfield of K_n. The claim implies that

$$[K_n : \mathbb{Q}] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_1 : K_0] = 2^s,$$

for some natural number s. (Note that $K_0 = \mathbb{Q}$.) Thus $[\mathbb{Q}(x, y) : \mathbb{Q}] = 2^r$ for some natural number r, as required.

Proof of claim: The point P_j can be constructed in one of three different ways; we need to check that the claim holds for each of these methods.

- $P = L_1 \cap L_2$ for two lines L_1 and L_2. Since L_i connects two points in K_{j-1} we conclude (check!) that the equation for L_i has form $\lambda_i x + \mu_i y + \nu_i = 0$ for some $\lambda_i, \mu_i, \nu_i \in K_j$, $i = 1, 2$.

  Now the intersection of two such lines is a point with coordinates in K_j (check!), and so $[K_{j+1} : K_j] = 1$ in this case.
- $P = C \cap L$ for a circle C and line L. Now C has centre (a_1, b_1) and radius equal to the distance between the points (a_2, b_2) and (a_3, b_3); then the equation for C is
$$(x - a_1)^2 + (y - b_1)^2 = (a_3 - a_2)^2 + (b_3 - b_2)^2.$$
  Since the three points (a_i, b_i), $i = 1, 2, 3$, are in A_j we conclude that C has equation
$$x^2 + y^2 + \lambda x + \mu y + \nu = 0$$
  for some $\lambda, \mu, \nu \in K_{j-1}$. Now, as we have seen, L has equation
$$\rho x + \sigma y + \tau = 0$$
  for some $\rho, \sigma, \tau \in K_{j-1}$. Substitution yields an equation
$$x^2 + \alpha x + \beta = 0$$
  for some $\alpha, \beta = 0$. If the quadratic on the LHS of this equation is reducible then x lies in K_{j-1} (it is a solution to a linear equation) and $[K_j : K_{j-1}] = 1$. If it is irreducible then $[K_j : K_{j-1}] = 2$ and we are done.
- $P = C_1 \cap C_2$ for two circles C_1 and C_2. Then, just as in the previous case, for $i = 1, 2$, we have equations
$$x^2 + y^2 + \lambda_i x + \mu_i y + \nu_i = 0.$$
  By elimination these intersect at the common solution of the equations
$$x^2 + y^2 + \lambda_1 x + \mu_1 y + \nu_1 = 0;$$
$$(\lambda_2 - \lambda_1)x + (\mu_2 - \mu_1)y + (\nu_2 - \nu_1) = 0.$$
  The second equation defines a line with coefficients in K_{j-1}. Hence we are back in case (2) where, as we have seen, the claim holds.

$\square$

We are now in a position to prove a number of "impossibility" theorems. Each of the next three results relates to a problem that was open for 2000 odd years! We begin with an exercise.

Exercise 5.2. *Call a line "constructible" if it joins two constructible points. Suppose that two constructible lines, L_1 and L_2, intersect at angle θ. Let Q be a constructible point, and M a constructible line through Q. Then a line N can be constructed that intersects M at Q, forming the angle θ.*

t: trisect

Theorem 5.3. *There are angles which cannot be trisected, such as $\frac{\pi}{3}$.*

Proof. Let $\theta = \frac{\pi}{9}$. Suppose that $\frac{\pi}{3}$ can be trisected, then (by the exercise) there is a construcible point P other than $(0, 0)$ on the line L defined by,
$$y = (\tan\theta)x.$$

Now we can intersect L with the circle C of radius 1 and centre $(0,0)$, thereby constructing the point $(\cos\theta, \sin\theta)$. Now there exists a natural number r such that

$$2^r = [\mathbb{Q}(\cos\theta, \sin\theta) : \mathbb{Q}] = [\mathbb{Q}(\cos\theta, \sin\theta) : \mathbb{Q}(\cos\theta)][\mathbb{Q}(\cos\theta) : \mathbb{Q}].$$

Thus, in particular, $[\mathbb{Q}(\cos\theta) : \mathbb{Q}] = 2^s$ for some natural number s.

But now observe that

$$\begin{aligned} &\cos(3\theta) = 4(\cos\theta)^3 - 3\cos\theta \\ \Longrightarrow\ &(2\cos\theta)^3 - 2(2\cos\theta) = 2\cos(3\theta) = 2\cos(\frac{\pi}{3}) = 1. \end{aligned}$$

Thus $z = 2\cos\theta$ satisfies $z^3 - 3z - 1$. **Claim**: the polynomial $t^3 - 3t - 1$ is irreducible.

Proof that claim implies theorem. The claim implies that

$$[\mathbb{Q}(\cos\theta) : \mathbb{Q}] = [\mathbb{Q}(2\cos\theta) : \mathbb{Q}] = 3.$$

Thus, in particular, $[\mathbb{Q}(\cos\theta) : \mathbb{Q}]$ does not divide 2^s for $s > 1$ and we are done.

Proof of claim: If the polynomial $t^3 - 3t - 1$ is reducible, then it has a rational zero. Let $z = \frac{p}{q}$ be such a solution, expressed in lowest terms. Then $p^3 - 3q^2p - q^3 = 0 \implies p \mid q^3$, which implies that $p \mid q^3$. This implies that $p = 1$. Then we have $q \mid p^3$, and so $q = 1$. Thus $z = 1$; but 1 is not a zero of the given polynomial so we have a contradiction as required. □

Note that this result is a proof that the angle $\frac{\pi}{3}$ cannot be trisected. On the other hand the angle π **can** be trisected!

Exercise 5.4. *Describe the procedure for trisecting π with ruler and compass.*

Theorem 5.5. *The cube cannot be duplicated by ruler and compass.*

Proof. "Duplicating the cube" means constructing a cube Q of volume 2. Suppose that we can do this: then Q has side length $\sqrt[3]{2}$, and so we are able to construct the point $P = (\sqrt[3]{2}, 0)$. Now $\sqrt[3]{2}$ is a root of the polynomial $f = t^3 - 2$. **Claim**: f is irreducible.

Proof that claim implies theorem: Since f is irreducible, $[\mathbb{Q}(\sqrt[3]{2} : \mathbb{Q}] = 3$. Since 3 does not divide 2^s for any natural number s we conclude that P is not constructible.

Proof of claim: As before it is enough to show that f has no rational roots. It is easy enough to verify that $\sqrt[3]{2}$ is not rational, and we are done. □

Theorem 5.6. *We cannot "square the circle" using a ruler and compass.*

Proof. "Squaring the circle" means drawing a square of area equal to π. Suppose we can do this; then we are able to construct two points of distance $\sqrt{\pi}$ apart; this in turn means that we can construct the point $(\sqrt{\pi}, 0)$. This implies that $[Q(\sqrt{\pi}) : \mathbb{Q}] = 2^s$ for some natural number s. Since $\mathbb{Q}(\pi)$ is a subfield of $\mathbb{Q}(\sqrt{\pi})$ we conclude that $[\mathbb{Q}(\pi) : \mathbb{Q}] = 2^r$ for some natural number r.

But now π is transcendental (Lindemann, 1882) and we have a contradiction. □

Tthere is nothing particularly special about the rules of construction corresponding to a ruler and compass. Given any set of rules for constructing points, one can (try to) prove results similar to those above. For instance one can study constructibility problems corresponding to origami-type procedures, or to cord-and-nail procedures.

6. Some results on irreducibility

The previous section highlighted how important it is to know when a given polynomial $f \in R[t]$ is irreducible. In this section we outline a number of results that tell us when a polynomial is irreducible in $\mathbb{Z}[t]$. In fact analogues of (most of) these results can be proved in much greater generality.

Definition 21. *The* **content** *of a polynomial $f = a_n t^n + \cdots a_1 t + a_0 \in \mathbb{Z}[t]$ is defined to be the greatest common divisor of the coefficients: $(a_n, \dots, a_1, a_0)$. If the content of f is equal to 1 then these coefficients are* **relatively prime** *and we call f primitive.*

l: prim **Lemma 6.1.** *If f and g are primitive elements of $\mathbb{Z}[t]$, then so is fg.*

Proof. Write

$$f = f_n t^n + \cdots + f_1 t + f_0;$$
$$g = g_n t^n + \cdots + g_1 t + g_0.$$

Let d be the content of fg, and suppose that $d > 1$. Let p be a prime dividing d. Since f and g are primitive we know that p does divides neither every f_i nor every g_i. Let j (resp. k) be the minimum value such that p does not divide f_j (resp. g_k).

Let c_{j+k} be the coefficient of t^{j+k} in fg. Then

$$c_{j+k} = \sum_{l+m=j+k} = \sum_{l<j} f_l g_{j+k-l} + \sum_{m<k} f_{j+k-m} g_l + f_j g_k.$$

Now p divides the left hand side. On the right hand side, p divides all terms except for the last. This is a contradiction. □

Theorem 6.2. (Gauss' Lemma) *Let $f \in \mathbb{Z}[t]$. Then f is irreducible in $\mathbb{Z}[t]$ if and only if f is irreducible in $\mathbb{Q}[t]$.*

Proof. Suppose that f is irreducible in $\mathbb{Z}[t]$, and $f = gh$ with $g, h \in \mathbb{Q}[t]$. We need to show that $\deg g = \deg f$ or $\deg h = \deg f$. We can assume that f is primitive, since $\frac{1}{d} f = (\frac{1}{d} g)h$ where d is the content of f.

Let d_g (resp. d_h) be the lowest common multiple of the set of denominators in coefficients of g (resp. h). Then $d_g g$ and $d_h h$ are both elements of $\mathbb{Z}[t]$. Now let n_g (resp. n_h) be the content of $d_g g$ (resp. $d_h h$). Set $\lambda_g = \frac{n_g}{d_g}$ and $\lambda_h = \frac{n_h}{d_h}$. Then $\lambda_g g$ and $\lambda_h h$ are primitive elements of $\mathbb{Z}[t]$.

Now observe that

$$\lambda_g \lambda_h f = (\lambda_g g)(\lambda_h h).$$

The RHS is a product of polynomials in $\mathbb{Z}[t]$. Since f is primitive in $\mathbb{Z}[t]$ we conclude that l: prim
$\lambda_g \lambda_h \in \mathbb{Z}$. Furthermore the RHS is a product of primitive polynomials and so Lem. 6.1 implies that $\lambda_g \lambda_h = \pm 1$. Thus we obtain that

$$\pm f = (\lambda_g g)(\lambda_h h).$$

Since f is irreducible in $\mathbb{Z}[t]$, we conclude that either $\deg g = \deg f$ or $\deg h = \deg f$, as required. □

Exercise 6.3. *Formulate and prove the two previous results for any unique factorization domain, R. (Instead of $\mathbb{Q}$, one needs to use the field of fractions for R.)*

We need some notation for the next result. For $f \in \mathbb{Z}[t]$ and $m \in \mathbb{Z}^+$, we write $[f]_m$ for the image of f under the canonical map $\mathbb{Z}[t] \to \mathbb{Z}/m\mathbb{Z}[t]$ (where we reduce every coefficient modulo m).

Theorem 6.4. (Localization principle) *Suppose that $f, g, h \in \mathbb{Z}[t]$. If $f = gh$ then, for all $m \in \mathbb{Z}^+$,*

$$[f]_m = [g]_m[h]_m.$$

Furthemore if m does not divide the leading coefficient of f, then $[f]_m$ irreducible implies that f is irreducible.

Proof. That $[f]_m = [g]_m[h]_m$ is trivial. Now suppose that $f = gh$ where $\deg g, \deg h < \deg f$, and that m does not divide the leading coefficient of f. Then $\deg[g]_m \deg[h]_m < \deg[f]_m$, and the second part follows. □

Corollary 6.5. (Eisenstein's criterion) *Suppose that*

$$f = f_n t^n + \cdots + f_1 t + f_0$$

is a polynomial in $\mathbb{Z}[t]$. suppose that p is a prime such that $p | f_i$ for $i = 0, \ldots, n-1$, $p \not| f_n$, and $p^2 \not| f_0$. Then f is irreducible in $\mathbb{Z}[t]$.

Proof. Suppose f is reducible of degree n, and localize at p:

$$\begin{aligned} f = gh &\implies [f]_p = [g]_p[h]_p \\ &\implies x^n = [g]_p[h]_p. \end{aligned}$$

Now the final equation is in $\mathbb{Z}/p\mathbb{Z}[t]$, which is a unique factorization domain. It follows that $[g]_p = t^r$ and $[h]_p = t^{n-r}$ where r is some positive integer. Then p must divide all non-leading coefficients of g and h; in particular p divides the constant term in both g and h. But this implies that p^2 divides f_0, which is a contradiction. □

Exercise 6.6. *Formulate and prove Eisenstein's criterion for an arbitrary integral domain R. Note that in this case one must be careful to choose p to be a* **prime** *element, rather than an* **irreducible** *element of R. In arbitrary integral domains, these two concepts are distinct.*

We should note an important variation in definitions: Garlling garling [Gar86], and others, require a polynomial in $\mathbb{Z}[t]$ to have content equal to 1 if it is to be irreducible. This makes some sense: since $\mathbb{Z}$ is not a field, not all polynomials will be divisible by a constant polynomial other than ± 1. However we will not use this definition of irreducibility in this course.

7. Splitting fields

We return to the main stream of the course. We want to examine field extensions, and their connection to the factorization of polynomials. If we have a polynomial $f \in \mathbb{Z}[t]$, then we know that there exists a field extension - $\mathbb{C}$ - within which f factorizes into linear factors. But is this true for a general field K?

Definition 22. *Take $f \in K[t]$ of degree n, with $L : K$ a field extension. We say that f* **splits** *over L if one has*

$$f(t) = \lambda(t - \alpha_1) \cdots (t - \alpha_n),$$

for some $\lambda \in K$, and $\alpha_1, \dots, \alpha_n \in L$.

We say, furthermore, that $L : K$ is a **splitting field extension for f over K** *(or simply that L is a* **splitting field** *for f) if*

(a) *f splits over L, and*
(b) *there exists no proper subfield M of L containing L such that f splits over M.*

Observe that if f splits over some field L_0, then a splitting field for f must exist.

Exercise 7.1. *Let $f = t^2 + 1$. Show that $\mathbb{C}$ is a splitting field for f over $\mathbb{R}$, but is not a splitting field for f over $\mathbb{Q}$.*

Theorem 7.2. *Suppose that $L : K$ is a field extension, and that $f \in K[t]$. Suppose that f splits over L as*

$$f(t) = \lambda(t - \alpha_1) \cdots (t - \alpha_n).$$

Then $K(\alpha_1, \dots, \alpha_n)$ is a splitting field for f over K.

Proof. It is plain that f splits over $K(\alpha_1, \dots, \alpha_n)$. Suppose now that M is a field with $K \subseteq M \subseteq K(\alpha_1, \dots, \alpha_n)$, and that f splits over M. Then

$$f = \mu(t - \beta_1) \cdots (t - \beta_n),$$

for some $\mu \in K$ and $\beta_1, \dots, \beta_n \in M$. Now $L[t]$ is a unique factorization domain; thus, by reordering, we have $\beta_i = \alpha_i$ for $i = 1, dots, n$. Thus $\alpha_1, \dots, \alpha_n \in M$ and so $K(\alpha_1, \dots, \alpha_n) \subseteq M$. We are done. $\square$

Corollary 7.3. *If $L : K$ is a splitting field extension for $f \in K[t]$, then $L : K$ is an algebraic extension.*

The problem with the previous result is that we had to assume that K lay inside a field L over which the polynomial f split. But how do we know that such a field L exists for arbitrary K and f? We need an "intrinsic" construction of a splitting field...

t: intrinsic **Theorem 7.4.** *Suppose that $f \in K[t]$ is irreducible of degree n. Then there is a simple algebraic extension $K(\alpha) : K$ such that $[K(\alpha) : K] = n$ and $f(\alpha) = 0$.*

This result is very much reminiscent of Thm. t: cd 4.8. Crucially, though, in this instance we don't require the existence of an ambient field L.

Proof. Let $\phi : K \to K[t]$ be the canonical monomorphism embedding K in $K[t]$ as the constant polynomials. Write $L = K[t]/(f)$, and let $q : K[t] \to L$ be the induced quotient map. Since f is irreducible, Lem. l: irred 4.1 implies that L is a field.

Let $i = q\phi$; then i is a monomorphism of K into L so that (i, K, L) is a field extension. Write $\alpha = q(t) = t + (f)$. Since t generates $K[t]$ over K, we know that $L = K(\alpha)$. Furthermore, since q is a ring homomorphism,

$$f(\alpha) = f(q(t)) = q(f) = q(0 + (f)) = 0.$$

Thus α is algebraic over K. Furthermore, since f is irreducible and $f(\alpha) = 0$, we know that f is a scalar multiple of the minimal polynomial m_α of α over K. Then $[L : K] = \deg m_\alpha = n$, as required. $\square$

Theorem 7.5. *Suppose that $f \in K[t]$. Then there exists a splitting field extension $L : K$ for f with $[L : K] \leq n!$.*

Proof. We prove this by induction on the degree of f. If $\deg f \leq 1$, then the conclusion is trivial. So suppose that $\deg f > 1$.

Suppose that f is irreducible over K. By Thm. `t: intrinsic` 7.4, there exists a simple algebraic extension $K(\alpha) : K$ with $[K(\alpha) : K] = n$, and such that

$$f(t) = (t - \alpha)g(t),$$

with $g \in K(\alpha)[t]$, and $\deg g = n - 1$. By the inductive hypothesis, there exists a splitting field for f, say $L : K(\alpha)$, with $[L : K(\alpha)] \leq (n-1)!$. Write

$$g = \lambda(t - \beta_1) \cdots (t - \beta_{n-1}),$$

where $\lambda \in K(\alpha)$ is the leading coefficient of g. But then

$$f = \lambda(t - \alpha)(t - \beta_1) \cdots (t - \beta_{n-1}),$$

and so λ is the leading coefficient of f and lies in K. Thus f splits over L. Then $L = K(\alpha, \beta_1, \dots, \beta_{n-1})$ is a splitting field extension of f over K. What is more

$$[L : K] = [L : K(\alpha)][K(\alpha) : K] \leq (n-1)!n = n!.$$

Suppose that f is not irreducible over K. Write $f = gh$ with $\deg g = k$, $\deg h = l$, $\deg f = k + l$, and both k and l at least 1. By the inductive hypothesis, there is a splitting field extension $L : K$ for g with $[L : K] \leq k!$. Thus we may write

$$g = \lambda(t - \alpha_1) \cdots (t - \alpha_k),$$

with $\lambda \in K$ and $\alpha_1, \dots, \alpha_k \in L$; then $L = K(\alpha_1, \dots, \alpha_k)$.

Now we consider h as an element of $L[t]$. By the inductive hypothesis, there is a splitting field $M : L$ for h with $[M : L] \leq l!$, and we can write

$$h = \mu(t - \beta_1) \cdots (t - \beta_l),$$

where $\mu \in L$ and $\beta_1, \dots, \beta_l \in M$. Clearly then

$$f = gh = \lambda\mu(t - \alpha_1) \cdots (t - \alpha_k)(t - \beta_1) \cdots (t - \beta_l),$$

where the leading coefficient of f, namely $\lambda\mu$, must lie in K. Then

$$M = L(\beta_1, \dots, \beta_l) = K(\alpha_1, \dots, \alpha_k, \beta_1, \dots, \beta_l),$$

so $M : K$ is a splitting field extension for f over K. Moreover by the tower law

$$[M : K] = [M : L][L : K] \leq l!k! \leq (l + k)! = n!.$$

□

The implications of this theorem are significant: we now know that every polynomial $f \in K[t]$ splits over some field. Up to this point we have started many of our results by assuming that $L : K$ is a field extension, and α is a root of f in L; in other words, we had to assume that a field extension existed in which f had a root. Now we know that a field extension exists containing **all** roots of f.

The question now is: what do these field extensions look like? Can f have more than one splitting field? We work towards an answer to these questions; first we have to examine simple extensions.

t: unique simple **Theorem 7.6.** *Suppose that $K(\alpha) : K$ is a simple field extension. Suppose that α is algebraic over K with minimal polynomial m_α. Suppose also that $i : K \to L$ is a field monomorphism, and that $\beta \in L$. Then there exists a monomorphism $j : K(\alpha) \to L$ with $j(\alpha) = \beta$ and $j|_K = i$ if and only if $i(m_\alpha)(\beta) = 0$.*

Moreover, if $i(m_\alpha)(\beta) = 0$, then the associated monomorphism j is unique.

Note that $j|_K = i$ means that *the restriction of j to K is equal to i*. In this case we say that j **extends** i. Note too that, by $i(m_\alpha)$ we mean the polynomial in $K'[t]$ which is obtained by applying i to each of the coefficients of m_α.

Proof. ($\Longrightarrow$) Suppose that a monomorphism j exists with the stated properties. Then

$$i(m_\alpha)(\beta) = j(m_\alpha)(\beta) = j(m_\alpha)(j(\alpha)) = j(m_\alpha(\alpha) = j(0) = 0.$$

($\Longleftarrow$) This is a long proof involving a big commutative diagram; drawing the diagram is beyond my latex skills, so I'm omitting this. Please see garling [Gar86, Thm. 7.4].

For uniqueness, suppose that j and j' are both monomorphisms of $K(\alpha)$ with the required propoerties. Then the set

$$F = \{\gamma \in K(\alpha) : j(\gamma) = j'(\gamma)\}$$

forms a subfield of $K(\alpha)$. (Check!) Moeover it is clear that $K \cup \{\alpha\} \subseteq F$. Thus $K(\alpha) \subseteq F \subseteq K(\alpha)$; thus $F = K(\alpha)$ and $j = j'$ as required. $\square$

When we use this theorem we will tend to identify K and $i(K)$; in other words, we think of K as being a subfield of L. Bear this in mind, when trying to understand the corollaries that follow.

c: same minimal **Corollary 7.7.** *Suppose that $K(\alpha) : K$ and $K'(\alpha') : K'$ are simple field extensions. Suppose also that α is algebraic over K and α' is algebraic over K', and that $i : K \to K'$ is an isomorphism. Then there exists an isomorphism $j : K(\alpha) \to K'(\alpha')$ such that $j(\alpha) = \alpha'$ and $j|_K = i$ if and only if $i(m_\alpha) = m_{\alpha'}$.*

Note that the conclusion of the corollary could alternatively be stated as, $i(m_\alpha) = m_{\alpha'}$ if and only if there exists an isomorphism $j : K(\alpha) \to K'(\alpha')$ such that the following diagram commutes:

$$\begin{array}{ccc} K(\alpha) & \xrightarrow{j} & K'(\alpha') \\ \uparrow & & \uparrow \\ K & \xrightarrow[i]{} & K', \end{array}$$

where the vertical arrows correspond to the natural inclusion maps. In other words,

$$i(m_\alpha) = m_{\alpha'}$$

if and only if $K(\alpha) : K$ is isomorphic to $K'(\alpha') : K'$ as a field extension (see Def. d: field extensi 17).

Proof of Corollary. We use Thm. t: unique simple 7.6, with $L = K'(\alpha')$. Then we have a monomorphism $j : K(\alpha) \to K'(\alpha')$ satisfying $j(\alpha) = \alpha'$ and $j|_K = i$ if and only if $i(m_\alpha)(\alpha') = 0$.

Note first that, if j exists, then it is an isomorphism since the image of j contains both K' and α'. It is sufficient to prove that

$$i(m_\alpha)(\alpha') = 0 \Longleftrightarrow i(m_\alpha) = m'_\alpha.$$

The ($\Longleftarrow$) part of this statement is immediate, since every element is a root of its minimal polynomial. So suppose that $i(m_\alpha)(\alpha') = 0$. One can check that, since i is an isomorphism of fields, $i(m_\alpha)$ is monic and irreducible over K'; this implies that $i(m_\alpha) = m_{\alpha'}$ as required.

The uniqueness of j follows immediately from Thm. t: unique simple 7.6. $\square$

Corollary 7.8. *Suppose that $K(\alpha) : K$ is a simple field extension, and that α is algebraic over K. Suppose also that $i : K \to L$ is a monomorphism, and that $i(m_\alpha)$ has r distinct roots in L. Then there are exactly r distinct monomorphisms $j : K(\alpha) \to L$ with $j|_K = i$.*

Proof. This is immediate from Thm. t: unique simple 7.6, and uniqueness. $\square$

We can now turn our attention to splitting fields. The next result (essentially) proves that splitting fields are unique; this will be spelt out in the corollary.

t: unique splitting

Theorem 7.9. *Suppose that $\Sigma : K$ is a splitting field extension for $f \in K[t]$, and that $i : K \to L$ is a field monomorphism. Then there is a monomorphism $j : \Sigma \to L$ with $j|_K = i$ if and only if $i(f)$ splits over L.*

Proof. ($\Longrightarrow$) Since f splits over Σ, we can write

$$f = \lambda(t - \alpha_1) \cdots (t - \alpha_n),$$

for some $\lambda \in K$ and $\alpha_1, \dots, \alpha_n \in \Sigma$. But $j : \Sigma \to L$ is a monomorphism with $j|_K = i$ and so

$$i(f) = j(f) = j(\lambda)(t - j(\alpha_1) \cdots (t - \alpha_n) = i(\lambda)(t - j(\alpha_1) \cdots (t - \alpha_n).$$

Then, since $i(\lambda) \in L$ and $j(\alpha_i) \in L$ for $i = 1, \dots, n$, we conclude that $i(f)$ splits over L.

($\Longleftarrow$) We use induction on $n = \deg f$. When $n = 1$, the result is clear since $\Sigma = K$ in this case, and we set $j = i$.

So now suppose that the conclusion holds for $n - 1$, and take $f \in K[t]$ of degree n such that $i(f)$ splits over L. Since f splits over Σ we may write

$$f = \lambda(t - \alpha_1) \cdots (t - \alpha_n),$$

with $\alpha_i \in \Sigma$ for $1 \leq i \leq n$, and $\lambda \in K$. Observe that α_1 is algebraic over K; call its minimal polynomial m, an irreducible polynomial over K. Then there is a polynomial $g \in K[t]$ such that $f = gm$. By reordering the roots of f if necessary we may suppose that m splits over Σ:

$$m = (t - \alpha_1) \cdots (t - \alpha_r),$$

where $r \leq n$.

Now, since i is a monomorphism, we know that

$$i(f) = i(mg) = i(m)i(g).$$

Since $i(f)$ splits over L we know that

$$i(m)i(g) = i(f) = \mu(t - \beta_1) \cdots (t - \beta_n),$$

where $\mu, \beta_1, \dots, \beta_n \in L$. Thus $i(m)$ splits over L and, since $K[t]$ is a unique factorization domain, we can reorder the β_i, so that $i(\alpha_i) = \beta_i$, $i = 1, \dots, r$, and

$$i(m) = (t - \beta_1) \cdots (t - \beta_r).$$

Observe that $K(\alpha_1) : K$ is a simple extension with minimal polynomial m_1 such that $i(m_1)(\beta_1) = 0$. Thm. t: unique simple 7.6 implies that there exists a unique monomorphism $j_1 : K(\alpha_1) \to L$ with $j_1(\alpha_1) = \beta_1$ and $j_1|_K = i$.

We have the following commutative diagram:

$$\begin{array}{ccc}
\Sigma & & L \\
\uparrow & & \uparrow \\
K(\alpha_1) & \xrightarrow{j_1} & i(K)(\beta_1) \\
\uparrow & & \uparrow \\
K & \xrightarrow[i]{} & i(K),
\end{array}$$

where the vertical arrows correspond to inclusion maps. Now consider f as a polynomial in $K(\alpha_1)[t]$. We have $f = (t - \alpha_1)h$ for some $h \in K(\alpha_1)[t]$ of degree $n-1$. Clearly h splits over Σ:

$$h = \lambda(t - \alpha_2) \cdots (t - \alpha_n).$$

Since $\Sigma = K(\alpha_1)(\alpha_2, \ldots, \alpha_n)$ we find that Σ is a splitting field for h over $K(\alpha - 1)$.

We can now imply induction to deduce the existence of a monomorphism $j : \Sigma \to L$ with $j|_{K(\alpha_1)} = j_1$. Since $j_1|_K = i$ we conclude that $j|_K = i$ as required. $\square$

c: iso exists

Corollary 7.10. *Suppose that $i : K \to K'$ is an isomorphism, and that $f \in K[t]$. Suppose also that $\Sigma : K$ is a splitting field extension for f, and that $\Sigma' : K'$ is a splitting field extension for $i(f)$. Then there exists an isomorphism $j : \Sigma \to \Sigma'$ such that $j|_K = i$.*

Note that we are effectively proving that the following diagram commutes:

$$\begin{array}{ccc}
\Sigma & \xrightarrow{j} & \Sigma' \\
\uparrow & & \uparrow \\
K & \xrightarrow[i]{} & K',
\end{array}$$

where the vertical arrows correspond to the natural inclusion maps. If we take $K = K'$ and i the identity, then uniqueness of splitting fields is explicit.

Proof of Corollary. Since $K' \subseteq \Sigma'$ and $i : K \to K'$ is an isomorphism we may view the map $i : K \to \Sigma'$ as a monomorphism. Clearly $i(f)$ splits over Σ' and so, by Thm. t: unique s 7.9 there exists a monomorphism $j : \Sigma \to \Sigma'$ with $j|_K = i$.

Now $j(\Sigma)$ is a subfield of Σ', and it is clear that $j(f) = i(f)$ splits over $j(\Sigma)$. Thus $j(\Sigma)$ is a splitting field for f inside Σ'. Since Σ' is, by definition, a minimal field over which f splits, we conclude that $j(\Sigma) = \Sigma$ and j is an isomorphism as required. $\square$

Our final corollary to Thm. t: unique simple 7.6 sets the scene for the (long-awaited) definition of the Galois group. This corollary gives sufficient conditions existence of an automorphism of a splitting field. These automorphism will be central objects in what follows.

c: aut exist

Corollary 7.11. *Let $f \in K[t]$ be irreducible, and take $\Sigma : K$ a splitting field extension for f. Then whenever α and β are roots of f in Σ, there exists an automorphism $\sigma : \Sigma \to \Sigma$ such that*

(a) *$\sigma(\alpha) = \beta$, and*
(b) *σ fixes K, i.e. $\sigma(k) = k$, for all $k \in K$.*

Proof. Clearly λf is the minimal polynomial for α and β for some $\lambda \in K$. Cor. c: same min 7.7 implies that there exists an isomorphism $j : K(\alpha) \to K(\beta)$ with $j(\alpha) = \beta$ and $j|_K = id$, the identity.

Now apply Cor. c: iso exists 7.10 with j in place of i. Since $\Sigma : K(\alpha)$ is a splitting field extension for f over $K(\alpha)$ and $\Sigma : K(\beta)$ is likewise a splitting field extension for $f = j(f)$ over $K(\beta)$, then there exists an isomorphism $\sigma : \Sigma \to \Sigma$ such that $\sigma|_{K(\alpha)} = j$. But this implies that $\sigma|_K = j|_K = id$, and condition (b) holds. Furthermore

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

and condition (a) holds as required. $\square$

8. A first look at the Galois group

The final corollary of the previous section directs our attention towards what will be our central objects of interest: automorphisms of field extensions.

Definition 23. *Let $L : K$ be a field extension. Define*

$$\Gamma(L : K) = \{\, \sigma \in AutL \mid \sigma(k) = k, \forall k \in K \,\}.$$

When $L : K$ is a splitting field extension for f over K, then write $\Gamma(L : K) = \Gamma_K(f)$, the **Galois group of f over K**.

Note that $\Gamma(L : K)$ is a group; the group operation is composition of functions. Let us look at some examples where $f \in \mathbb{Q}[t]$.; in particular we will use Cor. c: aut exist 7.11 to deduce the existence of elements of $\Gamma_{\mathbb{Q}} f$.

- Let $f = t^2 + 1 \in \mathbb{Q}[t]$. Clearly $\mathbb{Q}(i)$ is a splitting field extension for f over Q. Now f has two roots: i and $-i$. Then Cor. c: aut exist 7.11 tells us that there exists an automorphism σ that satisfies $\sigma(i) = -i$ and $\sigma(k) = k$ for all $k \in \mathbb{Q}$. Thus σ has form
$$\sigma : \mathbb{Q}(i) \to \mathbb{Q}(i),\; a + bi \mapsto a - bi.$$
This is just complex conjugation.
- Take $f = t^2 + 3t + 3 \in \mathbb{Q}[t]$. This is irreducible over $\mathbb{Q}$ by Eisenstein's criterion. Now f has three distinct roots $\alpha_1, \alpha_2, \alpha_3$. We know that there exist elements in $\Gamma_K(f)$ mapping α_i to α_j for any $i, j = 1, 2, 3; i \neq j$. We should be careful not to conclude that we therefore have six non-trivial elements in $\Gamma_K(f)$ because one automorphism could satisfy more than one of the given conditions.

To get a better handle on the structure of $\Gamma_K(f)$ we need to recall some basic group theory.

8.1. **A review of some group theory.** This review will be exceedingly brief. Please see [Ros94, §4] for more details, and examples. Throughout what follows G is a group, Ω a set.

Definition 24. *An* **action** *of G on Ω is a map*

$$G \times \Omega \to \Omega, (g, \omega) \mapsto g\omega$$

satisfying:

(a) $1\omega = \omega$*, for all* $\omega \in \Omega$*;*
(b) $(gh)\omega = g(h(\omega))$ *for all* $g, h \in G$ *and* $\omega \in \Omega$*.*

Note that when we say that G **acts on** Ω, we should really specify the particular map $G \times \Omega \to \Omega$ that we are talking about. In practice we don't tend to do this, as the context makes things clear. For the rest of this subsection we suppose that G acts on Ω.

Intuitively we think of each element of G as being a permutation of the set Ω. So we "apply" $g \in G$ to the set Ω, and all the elements swap around. In fact this intuition can be made rigorous:

Lemma 8.1. *The action of G on Ω induces a natural homomorphism*

$$\phi : G \to Sym(\Omega), g \mapsto \phi_g,$$

where $\phi_g : \Omega \to \Omega$ *is defined by* $\phi_g(\omega) = g\omega$*.*

Note that we write $Sym(\Omega)$ for the group of permutations on Ω. The proof of the lemma is easy; consider it an exercise. In fact the presence of the homomorphism ϕ can be taken as an alternative definition for an action; see [Ros94] for more details.

Definition 25. *The* **kernel** *of the action of G on Ω is defined to be the set*

$$\ker = \{\, g \in G \mid g\omega = \omega \text{ for all } \omega \in \Omega \,\}.$$

If $\ker = \{1\}$ *then we say that the action of G on Ω is* **faithful**.

Note that ker is also the kernel of the group homomorphism ϕ that we defined above. This implies in particular that the kernel of the action is a normal subgroup of G.

Definition 26. *The action of G on Ω is* **transitive** *if for all* $\alpha, \beta \in \Omega$*, there exists* $g \in G$ *such that* $g\alpha = \beta$*.*

Exercise 8.2. *Take* $\alpha \in \Omega$*. Then G acts transitively if and only if, for all* $\beta \in \Omega$*, there exists* $g \in G$ *such that* $g\alpha = \beta$*.*

Lemma 8.3. *If G acts transitively on Ω, and Ω is finite of order n, then n divides $|G|$.*

Proof. This is a consequence of the Orbit-Stabilizer theorem. See [Ros94] for details. □

Be warned: it will be very useful to have a good understanding of group actions in what follows. If you need more of a reminder than what has already been given, then a couple of hours in the presence of Rose [Ros94] is strongly recommended. A final piece of notation: when Ω is finite of order n we write S_n for $Sym(\Omega)$.

8.2. **Early results on the Galois group.** Let K be a field, $f \in K[t]$ of degree n, and Σ a splitting field for f over K. Let $\Omega = \{\alpha_1, \dots, \alpha_n\}$, the set of roots of f in Σ.

Lemma 8.4. *If $\sigma \in \Gamma_K(f)$ then for all $i \in \{1, \dots, n\}$, there exists $j \in \{1, \dots, n\}$ such that $\sigma(\alpha_i) = \alpha_j$.*

Proof. We will prove this directly. Note, though, that an alternative proof can be written down which uses Cor. 7.7.

We need to show that $\sigma(\alpha_i)$ is a root of f. Write

$$f = a_n t^n + \cdots + a_1 t + a_0,$$

where $a_i \in K$. Then

$$\begin{aligned}
& a_n(\alpha_i)^n + \cdots + a_1\alpha_i + a_0 = 0 \\
\Longrightarrow\ & \sigma(a_n(\alpha_i)^n + \cdots + a_1\alpha_i + a_0) = \sigma(0) \\
\Longrightarrow\ & \sigma(a_n)(\sigma(\alpha_i))^n + \cdots + \sigma(a_1)\sigma(\alpha_i) + \sigma(a_0) = 0 \\
\Longrightarrow\ & a_n(\sigma(\alpha_i)^n + \cdots + a_1(\sigma(\alpha_i)) + a_0 = 0,
\end{aligned}$$

as required. □

l: action **Lemma 8.5.** $\Gamma_K(f)$ *acts on* Ω.

Proof. The previous lemma implies that we have a map

$$G \times \Sigma \to \Sigma,\ (\sigma, \alpha_i) \mapsto \sigma(\alpha_i).$$

If $\sigma = 1$ then clearly $1(\alpha_i) = \alpha_i$ for all $i = 1, \dots, n$. In addition, since the group operation is composition of functions we have that

$$(\sigma_1\sigma_2)(\alpha_i) = \sigma_1(\sigma_2(\alpha_i))$$

for all $i = 1, \dots, n$. Thus the two axioms are satisfied and we are done. □

l: faithful **Lemma 8.6.** $\Gamma_K(f)$ *acts faithfully on* Ω.

Proof. Suppose that σ lies in the kernel of the action. Recall that $\Sigma = K(\alpha_1, \dots, \alpha_n)$. Then σ fixes all elements of K and also satisfies $\sigma(\alpha_i) = \alpha_i$ for $i = 1, \dots, n$. Thus σ fixes all elements of Σ; in other words $\sigma = 1$ as required. □

l: transitive **Lemma 8.7.** *Suppose that f is irreducible over K. Then $\Gamma_K(f)$ acts transitively on Ω.*

Proof. Since f is irreducible, there exists $\lambda \in K$ such that λf is the minimal polynomial for all elements in Ω. Then the result follows from Cor. 7.11. □

e: transitive **Exercise 8.8.** *Note that if f is not irreducible, then the lemma just stated does not hold. Prove a result that connects the orbit decomposition of the action of $\Gamma_K(f)$ on Ω to the set of irreducible factors of f.*

The series of lemmas that we have just proved give us some very strong information about the possible structure of $\Gamma_K(f)$. Lem. 8.5 tells us that $\Gamma_K(f)$ acts on Ω, the set of roots of f. Thus we have a natural homomorphism $\phi : \Gamma_K(f) \to S_n$; now Lem. 8.6 implies that ϕ is in fact a monomorphism. In other words $\Gamma_K(f)$ is isomorphic to a subgroup of S_n (we write $\Gamma_K(f) \lesssim S_n$). In particular this means that $|\Gamma_K(f)|$ divides $n!$ (and we have

an upper bound on $|\Gamma_K(f)|$). On the other hand if f is irreducible, then Lem. 8.7 implies 1: transitive
that n divides $|\Gamma_K(f)|$ (and we have a lower bound on $|\Gamma_K(f)|$).

Let us look at our earlier examples again:

- If $f = t^2 + 1 \in \mathbb{Q}[t]$, then we know that $\Gamma_K(f) \lesssim S_2$. Since $|S_2| = 2$ and we saw earlier that $\Gamma_K(f)$ contains a non-trivial element σ we conclude that $\Gamma_K(f) = \{1, \sigma\}$.
- If $f = t^3 + 3t + 3 \in \mathbb{Q}[t]$ then we know that $\Gamma_K(f) \lesssim S_3$. Since f is irreducible we know that 3 divides $|\Gamma_K(f)|$. Now S_3 has precisely two subgroups of order divisible by 3; namely A_3 and S_3 (where A_3 is the alternating group on three letters). Thus $\Gamma_K(f)$ must be isomorphic to one of these.

Exercise 8.9.

- *Let $f \in K[t]$ be of degree 2. Then $\Gamma_K(f)$ has order 1 or 2. Give conditions under which $\Gamma_K(f)$ has order 2.*
- *Can you determine whether $\Gamma_K(f)$ is A_3 or S_3 in the last example? (Hard!)*

Let us look at a few more difficult examples.

- Take $f = t^4 - 2 \in \mathbb{Q}[t]$; observe that f is irreducible by Eisenstein's criterion. Write $\alpha = \sqrt[4]{2}$; then
$$f = (t-\alpha)(t+\alpha)(t-\alpha i)(t+\alpha i).$$
Let Σ be a splitting field for f; clearly $\Sigma \subseteq \mathbb{Q}(\alpha, i)$. Furthermore Σ contains αi and α so Σ contains i; thus $\mathbb{Q}(\alpha, i) = \Sigma$.

  We want to calculate the degree of $\Sigma : \mathbb{Q}$. The minimal polynomial of i over $\mathbb{Q}$ is $t^2 + 1$ so $[\mathbb{Q}(i) : \mathbb{Q}] = 2$. On the other hand the minimal polynomial for α over $\mathbb{Q}$ is $t^4 - 2$; this polynomial is irreducible over $\mathbb{Q}(i)$, so we use the tower law:
$$[\Sigma : \mathbb{Q}] = [\mathbb{Q}(\alpha, i)\mathbb{Q}] = [\mathbb{Q}(\alpha, i), \mathbb{Q}(i)][\mathbb{Q}(i) : \mathbb{Q}] = 4 \times 2 = 8.$$
Alternatively we could have used the fact that $t^2 + 1$ is irreducible over $\mathbb{Q}(\alpha)$.

  The following diagram displays the inclusion maps corresponding to the situation, with the degree of each extension labelled in each case.
$$\begin{tikzcd}
 & \mathbb{C} & \\
 & \mathbb{Q}(\alpha, i) \arrow[u] & \\
\mathbb{Q}(i) \arrow[ur, "4"] & & \mathbb{Q}(\alpha) \arrow[ul, "2"'] \\
 & \mathbb{Q} \arrow[ul, "2"] \arrow[ur, "4"'] \arrow[uu, dotted, dash, "8"'] &
\end{tikzcd}$$
  Now the Galois group $\Gamma_{\mathbb{Q}}(f)$ is a transitive subgroup of S_4, hence is isomorphic to C_4, E_4, D_8, or S_4.
- Let us look next at $f = t^6 - 1$ in $\mathbb{Q}[t]$. Observe that
$$f = (t-1)(t+1)(t^2 - t + 1)(t^2 + t + 1);$$

in particular it is not irreducible! Let ω be a root of t^2+t+1 in $\mathbb{C}$. Then

$$f = (t-1)(t+1)(t+\omega)(t+\omega^2)(t-\omega)(t-\omega^2).$$

Thus $\mathbb{Q}(\omega):\mathbb{Q}$ is a splitting field for f over $\mathbb{Q}$, and $[\mathbb{Q}(\omega):\mathbb{Q}]=2$.

Now is $|\Gamma_{\mathbb{Q}}(f)|$ equal to 1 or 2? Refer to Cor. 7.11 which tells us that if two roots of f have the same minimal polynomial, then there is an automorphism of Σ mapping one root onto the other. In this instance ω and ω^2 have minimal polynomial t^2+t+1, while $-\omega$ and $-\omega^2$ have minimal polynomial t^2-t+1. Thus there must exist an automorphism $\sigma \in \Gamma_Q(f)$ satisfying

$$\sigma(\pm\omega) = \pm\omega^2,\ \sigma(\pm\omega^2) = (\pm\omega).$$

Thus $\Gamma_Q(f) = \{1,\sigma\}$ and we have a complete description of σ.

Note that this example should give you an idea of how to generalize Lem. 8.7 (see Ex. 8.8).

Exercise 8.10. *Calculate the splitting field for* t^6+1.

- Take $f = t^p - 7 \in \mathbb{Q}[t]$ where p is a prime number; then f is irreducible by Eisenstein. Write $\sqrt[p]{7}$ for the unique positive root of 7; this is a root of f. We calculate Σ, the splitting field for f.

  If α is any other root of f, then $(\alpha/\sqrt[p]{7})^p = \alpha^p/7 = 1$. Thus $\alpha = \sqrt[p]{7}\omega$ where ω is a p-th root of 1. The set of p-th roots of 1 is a cyclic group of order p that we shall call U_p (Exercise!). Thus

$$\begin{aligned} t^p - 1 &= (t-1)(t^{p-1}+\cdots+t+1) \\ &= (t-1)(t-\omega)(t-\omega^2)\cdots(t-\omega^{p-1}), \end{aligned}$$

  for some ω to be a **primitive** p-th root of 1, that is a generator of U_p. Thus $\mathbb{Q}(\omega):\mathbb{Q}$ is a splitting field extension for t^p-1.

  Now observe that

$$f = (t-\sqrt[p]{7})(t-\omega\sqrt[p]{7})(t-\omega^2\sqrt[p]{7})\cdots(t-\omega^{p-1}\sqrt[p]{7}),$$

  thus Σ, the splitting field for f is contained in $\mathbb{Q}(\sqrt[p]{7},\omega)$. It is clear that Σ also contains $\sqrt[p]{7}$ and ω, thus we conclude that $\Sigma = \mathbb{Q}(\sqrt[p]{7},\omega)$.

  Now ω is a root of the polynomial $t^{p-1}+\cdots+t+1$, which is irreducible (Exercise!). We conclude that $[\mathbb{Q}(\omega:\mathbb{Q}] = p-1$. In addition $[\mathbb{Q}(\sqrt[p]{7}):\mathbb{Q}] = p$, since f is the minimal polynomial for $\sqrt[p]{7}$. We conclude that $p(p-1)$ divides $[\Sigma:\mathbb{Q}]$.

  But now the minimal polynomial, m, of $\sqrt[p]{7}$ over $\mathbb{Q}(\omega)$ divides t^p-7 in $\mathbb{Q}(\omega)[t]$ and so

$$\deg m = [\mathbb{Q}(\omega,\sqrt[p]{7}):\mathbb{Q}(\omega)] \le p.$$

Thus $[\Sigma : \mathbb{Q}] \leq p(p-1)$ and $p(p-1)$ divides $[\Sigma : \mathbb{Q}]$. We conclude that $[\Sigma : \mathbb{Q}] = p(p-1)$. The diagram illustrates the set-up:

$$\begin{tikzcd}
& \mathbb{Q}(\omega, \sqrt[p]{7}) & \\
\mathbb{Q}(\sqrt[p]{7}) \arrow[ur, "p-1"] & & \mathbb{Q}(\omega) \arrow[ul, "p"'] \\
& \mathbb{Q} \arrow[ul, "p"] \arrow[ur, "p-1"'] \arrow[uu, dotted, "p(p-1)"'] &
\end{tikzcd}$$

8.3. **A note about "algebraic closure".** Before we move onto other matters, we should make mention of the notion of *algebraic closure*. We are familiar with the fundamental theorem of algebra which states that any polynomial in $\mathbb{C}[t]$ factorizes into linear factors. In the language of this course, this is equivalent to saying that $\mathbb{C}$ is a splitting field for any $f \in \mathbb{C}[t]$. A field with this property is called **algebraically closed**.

It turns out that any field K lies inside a bigger field L which is algebraic over K and is algebraically closed. Such a field L is called the **algebraic closure** of K; not only does L always exist, but $L : K$ is unique. This fact deals with all our earlier concerns about whether a polynomial f in $K[t]$ will necessarily have a root. We dealt with these concerns by constructing a splitting field for f; an alternative method would have been to prove this result about algebraic closure.

There is one major drawback to this alternative method: in order to prove the uniqueness of the algebraic closure one must use **Zorn's lemma**. This lemma is logically equivalent to the **Axiom of Choice**. The Axiom of Choice is an "optional" axiom when we do mathematics. That is to say, one can do mathematics with or without it - the consistency of one's mathematical system is not affected either way. However, because the Axiom of Choice (and hence Zorn's lemma) is optional in this way, people prefer to do mathematics without it, where possible.

A full description of Zorn's Lemma, and the concept of algebraic closure can be found in [Gar86, SS2,8]. We will not use these concepts in this course.

9. Normal extensions

As usual K is a field.

Definition 27. *An extension $L : K$ is* **normal** *if it is algebraic, and whever f is an irreducible polynomial in $K[t]$, then either*

(a) *f splits over L, or*
(b) *f has no roots in L.*

Definition 28. *Let $S \subseteq K[t]$. An extension L of K is a* splitting field extension for *S if*

(a) *every polynomial f in S splits over L, and*
(b) *if M is a field such that $K \subseteq M \subseteq L$, and every polynomial in S splits over M, then $M = L$.*

This definition of a splitting field extension is a generalization of the concept of splitting field that we have already encountered. In fact if S is finite, the two concepts coincide: in this case put $g = \prod_{f \in S} f$. Then $g \in K[t]$ and a splitting field for g over K is the same as a splitting field for S over K. Thus our definition is new only when S is infinite.

t: splitting normal

Theorem 9.1. *An extension $L : K$ is normal if and only if $L : K$ is a splitting field extension for some subset S of $K[t]$.*

Proof. ($\Longrightarrow$) Suppose that $L : K$ is normal. Then $L : K$ is algebraic, and we may take $S = \{m_\alpha : \alpha \in L\}$ with m_α the minimal polynomial over K of α in L. By normality, each polynomial in S splits over L.

Now suppose that $K \subseteq M \subseteq L$ and every polynomial in S splits over M. Take $\beta \in L \backslash M$; then m_β is irreducible over K and does not split over M. But $m_\beta \in S$ so S does not split over M; a contradiction. We conclude that no such β exists; in other words $L = M$ as required.

($\Longleftarrow$) Suppose that $L : K$ is a splitting field extension for $S \subseteq K[t]$. Let

$$A = \{\alpha \in L \mid f(\alpha) = 0 \text{ for some } f \in S\}.$$

Clearly $K(A) \subseteq L$. What is more every element of S splits over $K(A)$, by definition. Thus, by the definition of a splitting field extension $L \subseteq K(A)$. We conclude that $K(A) = L$. Note, in particular, that $L : K$ is an algebraic extension.

Take m to be an irreducible polynomial in $K[t]$. We want to prove that if m has a root in L, then m splits; thus, there is no loss of generality in assuming that m is monic. Let β be a root of m in L; we have $m = m_\beta$. Our first job is to reduce this to a question of finite extensions.

Since $\beta \in K(A)$ we know that $\beta \in K(\alpha_1, \dots, \alpha_n)$ for some $\alpha_1, \dots, \alpha_n \in A$. What is more there exist $f_1, \dots, f_n \in S$ such that α_i is a root of f_i for $1 \leq i \leq n$. Now each f_i splits over L; let R be the set of roots of $g = f_1 \cdots f_n$. Then $K(R) : K$ is a splitting field extension for f and $\beta \in K(R)$.

Let us view m as an element of $K(R)[t]$ and build a splitting field extension $H : K(R)$ for m. Let γ be another root of m in H. We will be finished if we can show that $\gamma \in K(R)$.

We have the following commutative diagram; all arrows correspond to inclusions:

$$\begin{tikzcd}
 & H & \\
K(R) \arrow[ur] & & K(R,\gamma) \arrow[ul] \\
K(\beta) \arrow[u] & & K(\gamma) \arrow[u] \\
 & K \arrow[ul, "\deg m"] \arrow[ur, "\deg m"'] &
\end{tikzcd}$$

Note that m is the minimal polynomial of both β and γ over K so

$$[K(\beta) : K] = [K(\gamma) : K] = \deg m,$$

just as we have labelled in our diagram.

Now by Cor. 7.7 there exists an isomorphism $\tau : K(\beta) \to K(\gamma)$ such that $\tau(\beta) = \tau$ and τ fixes K. Since τ fixes K we conclude that $\tau(g) = g$.

Next observe that $K(R) : K(\beta)$ is a splitting field extension for g over $K(\beta)$, and $K(R, \gamma) : K(\gamma)$ is a splitting field extension for $\tau(g) = g$ over $K(\gamma)$. Thus, by Cor. 7.11, there is an isomorphism $\sigma : K(R) \to K(R, \gamma)$ such that $\sigma|_{K(\beta)} = \tau$. This means that

$$[K(R) : K(\beta)] = [K(R, \gamma) : K(\gamma)]$$

and, by the tower law,

$$\begin{aligned} &= [K(R) : K(\beta)][K(\beta) : K] \\ &= [K(R, \gamma) : K(\gamma)][K(\gamma) : K] \\ &= [K(R, \gamma) : K]. \end{aligned}$$

Since $K(R) \subseteq K(R, \gamma)$, we conclude that $K(R) = K(R, \gamma)$ and $\gamma \in K(R)$ as required. □

Corollary 9.2. *A finite extension $L : K$ is normal if and only if $L : K$ is a splitting field extension for some polynomial $g \in K[t]$.*

Proof. The implication ($\Longleftarrow$) is trivial. We prove ($\Longrightarrow$): suppose that $L : K$ is finite and normal. Let $\alpha_1, \ldots, \alpha_n$ be a basis for $L : K$, and write $g = m_{\alpha_1} m_{\alpha_2} \cdots m_{\alpha_n}$. Then $L : K$ is a splitting field extension for g. □

Definition 29. *Suppose that $L : K$ is algebraic. We say that an extension $F : L$ is a* **normal closure** *for $L : K$ if*

(a) *$F : K$ is normal;*
(b) *when $F : M : L$ is a tower of field extension, and $M : K$ is normal, then $M = F$.*

Corollary 9.3. *If $L : K$ is finite, then there exists a finite normal closure $F : L$.*

Proof. Let $\alpha_1, \ldots, \alpha_n$ be a basis for L over K, and put $g = m_{\alpha_1} \cdots m_{\alpha_n}$. Let $F : L$ be a splitting field extension for g over L. Then $F : K$ is a splitting field extension for g over K, and by Thm. 9.1, it is normal.

Now suppose that $F : M : L$ is a tower of field extensions and $M : K$ is normal. For each i with $1 \leq i \leq n$, one has $\alpha_i \in L \subseteq M$ and $m_{\alpha_i}(\alpha_i) = 0$; thus, by normality, each polynomial m_{α_i} splits over M. But then M is a splitting field extension for g over K, so that $M = F$. Thus $F : L$ is a normal closure. □

Corollary 9.4. *Suppose that $L : K$ is normal, and that M is a field with $K \subseteq M \subseteq L$. Then $L : M$ is normal.*

Proof. Since $L : K$ is normal, Thm. 9.1 implies that there exists $S \subseteq K[t]$ such that $L : K$ is a splitting field extension for S. But S can be thought of as a subset of $M[t]$, and $L : M$ is a splitting field extension for S. Thus Thm. 9.1 implies that $L : M$ is normal. □

We need to be careful in our application of this final corollary. It is quite possible to have the following situation.

$$\begin{tikzcd}
L & \\
& M \arrow[ul, "\triangleleft"'] \\
K \arrow[uu, "\triangleleft"] \arrow[ur, "\ntriangleleft"'] &
\end{tikzcd}$$

All arrows denote inclusion; the symbol $\triangleleft$ is used to denote a normal extension. An example of this situation is given by the following situation. Let ω be a primitive cubic root of unity. Observe that $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ is a splitting field extension for $t^3 - 2 \in \mathbb{Q}[t]$; thus, in particular, it is a normal extension. However when we analyse its subfields we get the following set-up (with arrows denoting inclusion as usual):

$$\begin{tikzcd}
& \mathbb{Q}(\sqrt[3]{2}, \omega) & \\
\mathbb{Q}(\sqrt[3]{2}) \arrow[ur, "\triangleleft"] & & \mathbb{Q}(\omega) \arrow[ul, "\triangleleft"'] \\
& \mathbb{Q} \arrow[ul, "\ntriangleleft"] \arrow[uu, "\triangleleft"] \arrow[ur, "\triangleleft"'] &
\end{tikzcd}$$

If we draw the diagram for a normal extension $L : K$, then extensions $L : M$ will be normal (the top layer) but extensions $M : K$ may not be (the bottom layer). Precisely when this bottom layer is normal is explained in the following result (in the finite case).

Theorem 9.5. *Suppose that $L : K$ is a finite normal extension, and that M is an intermediate field ($K \subseteq M \subseteq L$). Then the following are equivalent:*

(a) *the field extension $M : K$ is normal;*
(b) *if $\sigma : L \to L$ is an automorphism that fixes K, then $\sigma(M) \subseteq (M)$;*
(c) *if $\sigma : L \to L$ is an automorphism that fixes K then $\sigma(M) = M$.*

Proof. (a)$\Longrightarrow$(b). Suppose that $M : K$ is normal and $\sigma : L \to L$ is an automorphism that fixes K. Take $\alpha \in M$, and write m_α for the minimal polynomial of α over K. Observe that $\sigma(\alpha)$ is a root of m_α and, clearly, $\sigma(\alpha) \in \sigma(M)$. But m_α splits over M by normality, thus $\sigma(\alpha) \in M$ for all $\alpha \in M$. We conclude that $\sigma(M) \subseteq M$.

(b)$\Longrightarrow$(c). Since σ is an automorphism of L it is, in particular, bijetive. Thus $[\sigma(M) : K] = [M : K]$ and so if $\sigma(M) \subseteq M$, then $\sigma(M) = M$.

(c)$\Longrightarrow$(a). Suppose that whenever $\sigma : L \to L$ is an automorphism that fixes K, then $\sigma(M) = M$. Now $L : K$ is normal and finite; hence Cor. c: finite normal 9.2 implies that $L : K$ is the splitting field extension for some polynomial $g \in K[t]$.

Take $\alpha \in M$ and let m_α be the minimal polynomial of α over K. Since $L : K$ is normal, and $m_\alpha(\alpha) = 0$ we find that m_α splits over L. Let β be any root of m_α in L; it is sufficient to prove that β lies in M.

By Thm. 7.6 implies that there exists a monomorphism $j : K(\alpha) \to K(\beta)$ with $j|_K$ equal to the identity on K and $j(\alpha) = \beta$. Since $j(g) = g$ we know that $L : K(\alpha)$ and $L : K(\beta)$ are both splitting field extension for $g = j(g)$. Then Cor. 7.10 implies that there is an isomorphism $\sigma : L \to L$ with $\sigma|_{K(\alpha)} = j$ and so $\sigma|_K = \mathrm{id}_K$. Now $\sigma(M) = M$ implies that $\beta = \sigma(\alpha) \in M$ as required. $\square$

References

garling [Gar86] D. J. H. Garling, *A course in Galois theory*, Cambridge University Press, Cambridge, 1986.

rose [Ros94] John S. Rose, *A course on group theory*, Dover Publications Inc., New York, 1994, Reprint of the 1978 original [Dover, New York; MR0498810 (58 #16847)].

stewart [Ste03] Ian Stewart, *Galois theory*, third ed., Chapman and Hall Ltd., London, 2003.