Galois Theory

Daniel Fretwell

Contents

1 Introduction **1**

2 Fields recap **2**
2.1 Fields . . . 2
2.2 Field extensions . . . 3
2.3 Finite fields . . . 8

3 Galois groups **9**
3.1 Automorphisms . . . 9
3.2 The Galois group . . . 10

4 Properties of the Galois group **11**
4.1 A Galois group action . . . 11

5 Examples **13**
5.1 Quadratic extensions . . . 13
5.2 Multiquadratic extensions . . . 14
5.3 Cyclotomic extensions . . . 15

6 Normal and Separable extensions **16**
6.1 Normality . . . 17
6.2 Separability . . . 17
6.3 Putting together the pieces . . . 18
6.4 Extensions of finite fields . . . 18

7 The main theorem of Galois theory **19**
7.1 From subgroups to intermediate fields - Fixed fields . . . 20
7.2 From intermediate fields to subgroups . . . 20
7.3 The main theorem of Galois theory . . . 21
7.4 Returning to finite fields . . . 22

8 An example using the main theorem **23**

9 Solving polynomials via radicals **24**
9.1 Solvability by Radicals . . . 27

1 Introduction

Galois theory lies somewhere in the intersection of the theory of fields and the theory of groups. In fact it connects the two in ways which you will not have seen before. Evariste Galois is now a very famous mathematician, not just because he was able to create the theory that these notes explain but also for the fact that he was able to use it to answer some very important questions. There is a lot of conjecture in how

his life was ended at the age of 17 in a duel. According to sources it could it have been over many things, including romance and things related to his imprisonment...

Putting this aside let's discuss briefly what Galois achieved and consequently what we will achieve in these notes. Around the time when Galois lived, mathematicians were mainly interested in solving polynomials. Most people should know how to solve quadratic equations via a number of methods. Generally a formula exists; if we are solving $ax^2 + bx + c = 0$, where $a, b, c \in \mathbb{C}$ and a is non-zero, then the solutions will look like:

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

There are a number of things to note from this formula...things you may not have realised before:

- The solutions depend only on the coefficients a, b, c. If these were to lie in a subfield F of $\mathbb{C}$ then the solutions of the quadratic will be defined in the field $F(\sqrt{b^2 - 4ac})$. This "splitting field" may or may not be F depending on whether $b^2 - 4ac$ is the square of an element of F. If it is then the roots of the quadratic will lie in F. This is essentially what you are checking when you look to see whether $b^2 - 4ac \geq 0$ or not.
- The quantity $b^2 - 4ac$ bears some importance here but where did it actually come from? We will see that it relates directly to the roots of the quadratic.
- This formula only involves the field operations with a square root thrown in.
- The "plus or minus" part seems to give us some kind of symmetry to the roots.

We may ask whether higher degree polynomials have similar solutions. Can we always find a formula for the roots of an nth degree polynomial that only involves the coefficients and radicals? (A radical is just a posh term for square roots, cube roots, quartic roots, ...)

Back in Galois' day mathematicians had managed to solve this for cubics and quartics. In other words there IS a cubic/quartic formula that gives the roots of a general cubic/quartic in terms of simple arithmetic and radicals. However, noone could find a "quintic formula" for 5th degree polynomials. Galois' clever inventions earned him the fame of solving this problem and giving a negative answer.

His idea was a nice one, find a way to assign each polynomial a finite group (called the Galois group) that somehow measures the symmetry of the roots of the polynomial (just like the symmetry we noticed above). Then being able to solve the polynomial using the operations described above translates into a nice property of the finite group (the property of being a solvable group). Galois did all of this before the invention of group theory and before fields were rigorously defined...at the age of 17! In some sense he is the creator of groups.

For an important example, here is a quintic equation $x^5 - x + 1 = 0$. It will turn out that the polynomial $x^5 - x + 1$ will have Galois group isomorphic to S_5. But this group is NOT solvable...hence the polynomial CANNOT be solved using radicals!

In modern mathematical language we instead assign each field extension a Galois group. Nothing is lost here since we still recover Galois' work by defining the Galois group of a polynomial to be the Galois group of the splitting field extension of the polynomial.

These notes are not meant to be incredibly formal, in fact a number of proofs have been omitted. The book by Stewart contains much more material, including proofs of everything. The notes are meant to encapsulate some of the beauty of field theory and Galois theory. The intuitions are the main focus here.

2 Fields recap

2.1 Fields

Since we are going to be working with fields quite a lot we should recap the main ideas. A field is simply a nice place where we can add/subtract/multiply/divide (except by 0) and not have to worry too much about things behaving nicely. Here is the formal definition:

Definition 2.1.1. A *field* is a set K such that $(K,+)$ is an abelian group and $(K\backslash\{0\},\times)$ is an abelian group.

Example 2.1.2. These are fields (p is a prime):

$$\mathbb{Z}/p\mathbb{Z} \qquad \mathbb{Q} \qquad \mathbb{C} \qquad \mathbb{Q}(\sqrt{2}) = \{a+b\sqrt{2} \mid a,b \in \mathbb{Q}\} \qquad \mathbb{C}(t) = \{\text{Laurent series in t with complex coeffs}\}.$$

These aren't:

$$\mathbb{Z}/4\mathbb{Z} \qquad \mathbb{Z} \qquad \mathbb{Q}[t] = \{\text{polynomials in t with rational coeffs}\}.$$

Every field has a smallest subfield. It is either $\mathbb{Q}$ or $\mathbb{Z}/p\mathbb{Z}$ for some prime p. Which is the case depends on whether $p.1 = 1+1+...+1 = 0$ for some prime p. If such a prime exists then we say that the field has characteristic p, otherwise we say that the field has characteristic 0.

As usual with "sub objects" a subfield is a field lying inside another field with the same operations. However when dealing with fields we like to move outwards too. This gives us the notion of field extension.

2.2 Field extensions

Definition 2.2.1. Let K be a field. A *field extension* L/K is given by another field L containing K.

The point of referencing the smaller field K is because we don't want to "forget" where L came from, so to speak. We will see why in a short while when we define the degree of a field extension (here the extension $\mathbb{C}/\mathbb{R}$ will turn out to be "finite" but the extension $\mathbb{C}/\mathbb{Q}$ will be "infinite"). For now it is enough to say that field extensions will be the natural objects we want to assign groups to. NOTE: The notation L/K is nothing to do with quotients.

We have the following proposition:

Proposition 2.2.2. *Given any field extension L/K we have that L is a K-vector space. A special case of this is when we take $L = K$, so that every field is a vector space over itself.*

Proof. The vector space axioms are special versions of the field axioms (just restrict multiplication in L to multiplication of elements of L by elements of K to get the required scalar multiplication properties). □

Why do we care about this proposition? Well we know quite a lot of good stuff about vector spaces, for example we know things about bases. We are going to use what we know to study fields. To start with, we know that the number of elements in a basis for a vector space is invariant over all bases (the so called *dimension* of a vector space). This motivates the following:

Definition 2.2.3. The *degree* of a field extension L/K is the dimension of L as a K-vector space. It is denoted $[L:K]$ (with the convention that $[L:K] = \infty$ when L is infinite dimensional as a K-vector space).

The following will turn out to be a nice property of "towers" of fields.

Lemma 2.2.4. *Given two extensions M/L and L/K then we have that $[M:K] = [M:L][L:K]$ (whenever the numbers are finite).*

Proof. Let $[M:L] = n$ and $[L:K] = m$. Then we have a basis $\{\alpha_1, \alpha_2, ..., \alpha_n\}$ for M as an L-vector space and a basis $\{\beta_1, \beta_2, ..., \beta_m\}$ for L as a K-vector space. It can easily be checked that $\{\alpha_i\beta_j \mid 1 \leq i \leq n, 1 \leq j \leq m\}$ is a basis for M as a K-vector space. Thus $[M:K] = nm = [M:L][L:K]$. □

Before seeing some examples we should first find ways to create field extensions and maybe see how to find the degree. The best way to create extensions is by adding elements to fields we already know about. We do this when we construct the complex numbers from the real numbers, we start with $\mathbb{R}$ and throw in the element i to get all complex numbers.

Definition 2.2.5. Let K be a field and X be a set (not necessarily containing elements of K). The *field generated by K and X* is the smallest field containing K and X, denoted $K(X)$. We say that this field is formed by *adjoining X to K*.

How might we describe this field explicitly? Well we can try and split our set up into parts and hopefully adjoin the sets bit by bit. We are allowed to do this by the following lemma:

Lemma 2.2.6. *For any field K and any set $X = X_1 \cup X_2$ we have that $K(X) = K(X_1)(X_2)$.*

Proof. We know that $K(X_1)(X_2)$ is the smallest field containing $K(X_1)$ and X_2. But $K(X_1)$ is the smallest field containing K and X_1. It follows that $K(X_1)(X_2)$ is the smallest field containing K and X. But by definition this is $K(X)$. □

For the rest of our work we will only be considering the case where X is a finite set. By the above lemma it is sufficient to describe fields that are obtained by adjoining only one element. These are simple extensions.

Definition 2.2.7. A *simple extension* of a field K is an extension of the form $K(\{\alpha\})/K$, i.e. a field extension that you get by adjoining a single element. We conventionally miss out the set notation and write $K(\alpha)$ instead of $K(\{\alpha\})$.

It is quite easy to classify simple extensions, and even to find their degrees. Let's see some examples.

Example 2.2.8. I claim that:

$$\mathbb{Q}(\sqrt{3}) = \{a + b\sqrt{3} \,|\, a, b \in \mathbb{Q}\} = \mathrm{Span}_{\mathbb{Q}}(1, \sqrt{3}),$$

so that $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$, giving a basis $\{1, \sqrt{3}\}$ for $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$.

Ok so by definition the field $\mathbb{Q}(\sqrt{3})$ contains $\mathbb{Q}$ and $\sqrt{3}$. Now any field containing $\mathbb{Q}$ and $\sqrt{3}$ is forced to contain all numbers of the form $a + b\sqrt{3}$, for $a, b \in \mathbb{Q}$ to guarantee closure of addition and multiplication. We didn't have to consider any higher power of $\sqrt{3}$ in order to get closure since $\sqrt{3}^2 \in \mathbb{Q}$, so that the higher powers only give us numbers we already have considered!

So we see that:

$$\mathbb{Q}(\sqrt{3}) \supseteq \{a + b\sqrt{3} \,|\, a, b \in \mathbb{Q}\}.$$

But this set of numbers is actually a field itself, containing $\mathbb{Q}$ and $\sqrt{3}$ (check this). Thus we have equality, since $\mathbb{Q}(\sqrt{3})$ is defined to be the smallest such field. The fact that $\sqrt{3}$ is irrational tells us that $1, \sqrt{3}$ are linearly independent over $\mathbb{Q}$ and so this completes the basis claim.

Example 2.2.9. In a similar vein I claim that:

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2 \,|\, a, b, c \in \mathbb{Q}\} = \mathrm{Span}_{\mathbb{Q}}(1, \sqrt[3]{2}, (\sqrt[3]{2})^2),$$

so that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, giving a basis $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\}$ for $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. The argument is exactly the same but this emphasises the general case more. Note that to guarantee closure this time we have to consider upto the 2nd power of $\sqrt[3]{2}$ and had to go no further because $(\sqrt[3]{2})^3 \in \mathbb{Q}$, so that higher powers again give us numbers we already considered.

Example 2.2.10. We can now find more complicated fields such as $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ by writing as $\mathbb{Q}(\sqrt{3})(\sqrt{2})$. It turns out, by the usual arguments, that $\{1, \sqrt{2}\}$ is a basis for $\mathbb{Q}(\sqrt{3})(\sqrt{2})$ over $\mathbb{Q}(\sqrt{3})$, so that

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

We also know that $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2$ with basis $\{1, \sqrt{3}\}$.

By the tower of fields argument we can now see that:

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

and that a basis over $\mathbb{Q}$ is given by $\{1 \times 1, 1 \times \sqrt{3}, \sqrt{2} \times 1, \sqrt{2} \times \sqrt{3}\} = \{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ so that $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \,|\, a, b, c, d \in \mathbb{Q}\}$.

How might we describe $K(\alpha)$ in general? Well the key lies in these three examples. We know that $\mathrm{Span}_K(1, \alpha, \alpha^2, \alpha^3, ...)$ must be contained in $K(\alpha)$ since we require closure (as we found in the examples).

A few questions present themselves:

- Is there a point beyond which the powers of α become redundant in this span? We found that this was the case in the examples. This seems intuitively the same as whether α satisfies some polynomial over K (since if α satisfies some polynomial of degree n over K then we can rearrange, writing α^n and all higher powers of α as a span of $1, \alpha, \alpha^2, ..., \alpha^{n-1}$).
- Is $\text{Span}_K(1, \alpha, \alpha^2, \alpha^3, ...)$ necessarily a field? It was in our examples.

Before stating the formal result answering these questions we make a definition.

Definition 2.2.11. Let L/K be a field extension. An element $\alpha \in L$ is *algebraic* over K if $f(\alpha) = 0$ for some polynomial f with coefficients in K. If this is not true then we say that α is *transcendental* over K. The extension L/K is called *algebraic* if every $\alpha \in L$ is algebraic over K.

This definition will hopefully help us to decide what power of α we need to go up to in order to write $K(\alpha)$ as a span of powers of α. If α is algebraic over K then as discussed earlier, the degree of such a polynomial f over K with α as a root tells us a point at which the α powers become redundant in the span. What we need is a polynomial that is in some sense minimal with respect to having α as a root.

Lemma 2.2.12. *Let $\alpha \in L$ be algebraic over K. Then there exists a unique monic irreducible polynomial f over K such that $f(\alpha) = 0$.*

Proof. The fact that α is algebraic over K tells us that there is at least one polynomial g, defined over K, such that $g(\alpha) = 0$. Now we may use the degree as a measure of "minimality". Construct the set F of all minimal degree polynomials over K having α as a root. This is a well defined set due to the well ordering principle along with the fact that the set is non-empty (it contains g).

Now take any two polynomials $h_1, h_2 \in F$. I claim that $h_1 = kh_2$ for some constant $k \in K$. This follows easily from the fact that $K[x]$ is a Euclidean domain with respect to the degree map.

Thus $h_1(x) = k(x)h_2(x) + r(x)$ for some $k(x), r(x) \in K[x]$ with $\deg(r) < \deg(h_2)$. But h_1, h_2 have the same degree so that $k(x)$ has to be constant, by comparison of degrees. Substituting $x = \alpha$ gives $r(\alpha) = 0$, so by minimality of the elements of F, we must also have that r is the zero polynomial. Hence $h_1 = kh_2$ for some $k \in K$.

It is now a simple matter to finish the proof since there must exist a unique **monic** polynomial $f \in F$. This polynomial must be irreducible over K by minimality of the degree of f. To see this note that if $f(x) = p(x)q(x)$ for non-constant polynomials p, q over K then $0 = f(\alpha) = p(\alpha)q(\alpha)$ as a product in K. Then by the fact that K is an integral domain we conclude that one of p, q has alpha as a root, contradicting the minimality of the degree of f. □

You might have noticed in the above that the middle chunk of work is basically a special case of the theorem that Euclidean domains are principal ideal domains. Indeed the set E of polynomials with α as a root is an ideal of $K[x]$. This ring is a Euclidean domain, so E must be a principal ideal. The elements of F are the possible generators for the ideal E and in particular f is the unique monic generator for E. However, these notes are written without assuming the theory of ideals.

Definition 2.2.13. The unique polynomial described above is called the *minimal polynomial* of α over K.

Example 2.2.14. The number $\sqrt{3}$ has minimal polynomial $x^2 - 3$ over $\mathbb{Q}$. This is easy to prove since no linear polynomial with rational coefficients can have $\sqrt{3}$ as a root, otherwise $\sqrt{3}$ would be rational. Thus no smaller degree polynomial can have $\sqrt{3}$ as a root. It should be noticed that if we work over the field $\mathbb{Q}(\sqrt{3})$ then the minimal polynomial now becomes $x - \sqrt{3}$, our field is now "big enough" to find a smaller degree polynomial with $\sqrt{3}$ as a root.

The number $\sqrt[3]{2}$ has minimal polynomial $x^3 - 2$ over $\mathbb{Q}$. This is harder to prove using brute force but we shall now see a better way to show this.

It seems the problem in proving that a given polynomial IS the minimal polynomial rests in proving irreducibility. When working over $\mathbb{Q}$ we have nice tests for this. We do not prove the following results here but there are many places to look for them. They are not difficult to prove.

Lemma 2.2.15. *(Gauss' Lemma) Let f be a polynomial with integer coefficients. We have that f is irreducible over $\mathbb{Z}$ if and only if it is irreducible over $\mathbb{Q}$.*

So one way of Gauss' Lemma tells us the non-obvious fact that extending from $\mathbb{Z}$ to $\mathbb{Q}$ can create no further factorisation of polynomials with integer coefficients. The converse is obvious.

But how can we tell irreducibility over $\mathbb{Z}$? Well this turns out to be easier by brute force, since now the coefficients in any supposed factorisation can be assumed to be integers.

Example 2.2.16. (continued) We claimed that x^3-2 was irreducible over $\mathbb{Q}$. By Gauss' Lemma it is enough to show that it is irreducible over $\mathbb{Z}$. Suppose we have a factorisation $(x^3-2) \equiv (ax+b)(cx^2+dx+e)$ for $a,b,c,d,e \in \mathbb{Z}$. Equating x^3 coefficients we see that $ac=1$. The only integer solutions are $a=c=1$ or $a=c=-1$. We may assume the first without loss of generality. Equating constant coefficients we see that $be=-2$. Again the only integer solutions are $b=\pm 1, e=\mp 2$ or $b=\pm 2, e=\mp 1$. It is easily checked that in either case there is no possible value for d that completes the factorisation. Hence the polynomial is irreducible.

This method is better but we can improve.

Lemma 2.2.17. *(Eisenstein's criterion) Let $f(x) = a_n x^n + \ldots + a_1 x + a_0$ be a polynomial with integer coefficients. Suppose that there exists a prime number p such that:*

- *p does not divide a_n,*
- *p divides all of $a_0, a_1, a_2, ..., a_{n-1}$,*
- *p^2 does not divide a_0,*

then f is irreducible over $\mathbb{Z}$, and hence over $\mathbb{Q}$ (by Gauss' Lemma).

Example 2.2.18. (returned...yet again) It is now trivial to see why x^3-2 is irreducible over $\mathbb{Q}$. This is just Eisenstein's criterion with $p=2$.

Sometimes we have to be clever before using Eisenstein and shift.

Example 2.2.19. Let p be a prime and consider the polynomial $f(x) = x^{p-1} + x^{p-2} + \ldots + x + 1$. I claim that this polynomial is irreducible over $\mathbb{Q}$.

To see this note that (for $x \neq 1$) we may write:

$$x^{p-1} + x^{p-2} + \ldots + x + 1 \equiv \frac{x^p - 1}{x - 1}.$$

(get this either using geometric progression, by knowledge of pth roots of unity or by knowledge of factorisations).

Now let us substitute $x = y + 1$. This is a linear change of variables so will not change the state of irreducibility (check this). Our new polynomial is:

$$\frac{(y+1)^p - 1}{y} = y^{p-1} + \binom{p}{p-1} y^{p-2} + \ldots + \binom{p}{2} y + p.$$

But then we may use Eisenstein's criterion with prime p (check this). This example will be important later.

Let's now return to our job of describing simple extensions. As we noticed in our examples we hope that we can describe a simple basis for $K(\alpha)/K$ whenever α is algebraic over K. This is true and we can say more once we know the degree of the minimal polynomial of α over K.

Theorem 2.2.20. *Let $K(\alpha)/K$ be a field extension, where α is algebraic over K. If the minimal polynomial f of α has degree n then a basis for the extension is given by $\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$ so that $K(\alpha) = Span_K\{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$.*

Proof. As noted in examples we must have that $\text{Span}_K(1, \alpha, \alpha^2, \ldots, \alpha^{n-1}) \subseteq K(\alpha)$. Also, α^{n-1} is not in $\text{Span}_K(1, \alpha, \alpha^2, \ldots, \alpha^{n-2})$ since otherwise we could rearrange and find a polynomial of degree $n-1$ or less with α as a root, contradicting minimality of n as the degree of the minimal polynomial.

It only remains to prove that $\text{Span}_K(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ is a field, then it must be $K(\alpha)$ by definition. But most of this is trivial to check, the only problem is in finding the multiplicative inverse.

Take $\beta \in \text{Span}_K(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$. Then $\beta = k_0 + k_1\alpha + \ldots ...k_{n-1}\alpha^{n-1}$. Consider the polynomial $g(x) = k_0 + k_1 x + \ldots + k_{n-1}x^{n-1}$. Then $f(x)$ and $g(x)$ are coprime in $K[x]$ (since f is irreducible). Thus we can find polynomials $s(x), t(x) \in K[x]$ such that:

$$s(x)f(x) + t(x)g(x) \equiv r$$

for some constant $r \in K$ (this is the same as Euclid's algorithm in number theory). After multiplying through by r^{-1} we may assume that $r = 1$.

But now if we let $x = \alpha$:

$$s(\alpha)f(\alpha) + t(\alpha)g(\alpha) = 1,$$

$$t(\alpha)g(\alpha) = 1.$$

Now since $\beta = g(\alpha)$ we see that $\beta^{-1} = t(\alpha) \in \text{Span}_K(1, \alpha, \alpha^2, \ldots, \alpha^{n-1})$ (since $t(\alpha)$ is some polynomial in α and so can be reduced into something in this span, using the minimal polynomial). We are done. □

Example 2.2.21. Consider the extension $\mathbb{R}(i)/\mathbb{R}$. The minimal polynomial of i over $\mathbb{R}$ is $x^2 + 1$ (since i is not real so doesn't satisfy a linear equation over $\mathbb{R}$). This polynomial has degree 2 so the above theorem now tells us that:

$$\mathbb{R}(i) = \text{Span}_{\mathbb{R}}(1, i) = \{a + bi \,|\, a, b \in \mathbb{R}\} = \mathbb{C}.$$

This makes precise the notion of constructing the complex numbers from $\mathbb{R}$ by "inventing i".

Example 2.2.22. (Cyclotomic extensions) Let ζ be a primitive pth root of unity (in this case a pth root of unity that isn't 1). Now $x^p - 1$ is satisfied by ζ but since $\zeta \neq 1$ we have that:

$$\frac{\zeta^p - 1}{\zeta - 1} = \zeta^{p-1} + \zeta^{p-2} + \ldots + \zeta + 1 = 0$$

so that ζ is a root of the polynomial $x^{p-1} + x^{p-2} + \ldots + x + 1$. However, we proved earlier that this polynomial is irreducible over $\mathbb{Q}$. It is of degree $p - 1$ so we have that:

$$\mathbb{Q}(\zeta) = \text{Span}_{\mathbb{Q}}(1, \zeta, \zeta^2, \ldots, \zeta^{p-2}) = \{a_0 + a_1\zeta + a_2\zeta^2 + \ldots + a_{p-2}\zeta^{p-2} \,|\, a_0, a_1, a_2, \ldots, a_{p-2} \in \mathbb{Q}\}.$$

The degree of the extension is $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$. Adjoining a root of unity is often a nice thing to do to solve problems. Such fields are called cyclotomic fields and appear all over number theory, algebra and geometry.

What happens when α is not algebraic over K? Well in this case there is no such polynomial relationship and so we have to consider all such spans of powers of α. However we no longer have an f to "measure by", i.e. we cannot use Euclid's algorithm to get the $s(x), t(x)$ because there is no f. So we see that the span is no longer a field. However we may make its field of fractions:

Theorem 2.2.23. *Let $K(\alpha)/K$ be a field extension with α transcendental over K. Then the degree is infinite and:*

$$K(\alpha) = \left\{ \frac{p(\alpha)}{q(\alpha)} \,|\, p(x), q(x) \in K[x] \right\}.$$

Proof. Omitted □

Corollary 2.2.24. *Every finite extension of the form $K(\alpha)/K$ is algebraic.*

Do not be fooled into thinking the converse of the above is true. There are infinite degree extensions that are algebraic.

Before moving on we make one other construction that starts with the polynomial and constructs a corresponding field. We know that every polynomial over any subfield K of $\mathbb{C}$ factorises completely into linear terms over $\mathbb{C}$. We adjoin the roots of such a polynomial to K to get a nice field.

Definition 2.2.25. Let f be a polynomial over $K \subseteq \mathbb{C}$ with set of roots $R \subset \mathbb{C}$. The *splitting field* of f over K is the field $K(R)$. In other words the smallest field over which f factorises into linear terms.

Example 2.2.26. The splitting field of x^2+1 over $\mathbb{R}$ is the field $\mathbb{R}(i,-i) = \mathbb{C}$. Considered as a polynomial over $\mathbb{Q}$ the splitting field is $\mathbb{Q}(i,-i) = \{a+bi \,|\, a,b \in \mathbb{Q}\} \neq \mathbb{C}$.

In this example one of the two roots was redundant in making the splitting field, once we had adjoined i we didn't need to adjoin $-i$ since we had already counted it. This does not always happen!

Example 2.2.27. The polynomial x^3-2 has three roots in $\mathbb{C}$. These are $\sqrt[3]{2}, \zeta\sqrt[3]{2}, \zeta^2\sqrt[3]{2}$, where ζ is a primitive cube root of unity. We see that it is not enough to adjoin $\sqrt[3]{2}$ and get the field $\mathbb{Q}(\sqrt[3]{2})$, we must adjoin all three roots, they each contribute something. This behaviour will be something we have to study in detail later.

When we have studied Galois groups of field extensions the notion of splitting field will allow us to define the Galois groups of polynomials as mentioned in the introduction.

2.3 Finite fields

A finite field is exactly what it sounds like. We already know of the finite fields $\mathbb{Z}/p\mathbb{Z}$ for primes p but are there any more? The following will give us the lot.

Proposition 2.3.1. *Let p be a prime number. Then for every integer $n \geq 1$ there exists a field $\mathbb{F}_{p^n}$ of size p^n. Further every finite field is isomorphic to one of these.*

Proof. Let F be a finite field. The characteristic of F cannot be 0 since F is finite. It must be some prime p. Thus it has a smallest subfield isomorphic to $\mathbb{Z}/p\mathbb{Z}$. As proved earlier, it now follows that F is a vector space over $\mathbb{Z}/p\mathbb{Z}$ of finite dimension (again since F is finite).

Suppose the dimension is n and choose a basis $\{\alpha_1, \alpha_2, \ldots, \alpha_n\}$. Now we know that:

$$F = \{f_1\alpha_1 + f_2\alpha_2 + \ldots + f_n\alpha_n \,|\, f_1, f_2, \ldots, f_n \in \mathbb{Z}/p\mathbb{Z}\} = \mathrm{Span}_{\mathbb{Z}/p\mathbb{Z}}(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

This set clearly has p^n elements, since there are p choices for each f_i. Thus F has p^n elements.

Now to prove that there exists such a subfield for each p and each n. But we can construct such a field $\mathbb{F}_{p^n}$ by considering the splitting field of $x^{p^n} - x$ over $\mathbb{Z}/p\mathbb{Z}$, since this polynomial has no repeated roots mod p (use the derivative test).

Finally we show uniqueness. We show that every $x \in F$ must satisfy $x^{p^n} = x$, so that F is isomorphic to $\mathbb{F}_{p^n}$ (by the uniqueness of the splitting field upto isomorphism).

Clearly $x = 0$ satisfies $x^{p^n} = x$. Now by the definition of a field we have that $\mathbb{F}\backslash\{0\}$ is a group (of order $p^n - 1$) under multiplication. So by a corollary of Lagrange's theorem we must have that $x^{p^n-1} = 1$ for all non-zero $x \in F$. Multiplying both sides by x we see that $x^{p^n} - x = 0$ for all $x \in F$. Thus F is isomorphic to the splitting field of $x^{p^n} - x$ over $\mathbb{Z}/p\mathbb{Z}$. (No smaller degree polynomial can have all $x \in F$ as a root since we are working over a field so every polynomial f over has at most $\deg(f)$ roots). Thus $F \cong \mathbb{F}_{p^n}$. □

Finite fields will return later when we consider Galois groups of their extensions.

3 Galois groups

We are now ready to start Galois theory. In this course we will only deal with the Galois theory of finite degree extensions. There is a Galois theory for infinite algebraic extensions but it is very complicated and involves certain topological groups called profinite groups.

We start by looking at some of the extensions that we have worked with in the previous chapter. Consider the extension $\mathbb{C}/\mathbb{R}$. We already saw that we can describe $\mathbb{C}$ as $\mathbb{R}(i)$. There appears to be certain "symmetries" to this field, defined by the choice of generator. For example, we could have chosen the generator $-i$ instead and nothing would change. On the other hand we could have chosen the generator $23 + 3873i$ but this one does not seem to have the same aesthetic beauty as $-i$. One good thing about choosing $-i$ instead of i is that any element of $\mathbb{C}$ has the same real part for both. In some sense this choice of generator respects the extension $\mathbb{C}/\mathbb{R}$ as well as just the big field $\mathbb{C}$. It is as if the map sending i to $-i$ is a kind of "symmetry" of the field extension; it is a map from the big field to itself, respecting the operations and fixing elements in the small field. Once extended to the whole of $\mathbb{C}$ this map is of course complex conjugation.

In this chapter we are going to make precise this notion of symmetry of fields by defining the automorphisms of a field. The Galois group will then be a certain subgroup of these automorphisms that in some sense represent symmetries of the extension as a whole. We will see how the Galois group acts on roots of polynomials, giving us a way to find the Galois group given knowledge of generators for the field extension.

3.1 Automorphisms

Before defining automorphisms we should define homomorphisms of fields. This is going to be similar to defining homomorphisms of groups in that they will be maps that preserve the structure of the field, i.e. the operations.

Definition 3.1.1. Let L, L' be fields. A map:

$$\phi : L \longrightarrow L'$$

is a *field homomorphism* if:

- ϕ is a homomorphism $L \longrightarrow L'$, as additive groups.
- ϕ is a homomorphism $L\backslash\{0\} \longrightarrow L'\backslash\{0\}$, as multiplicative groups.

A surjective field homomorphism is a *field epimorphism*. An injective field homomorphism is a *field monomorphism* and a bijective field homomorphism is a *field isomorphism*. An *automorphism* of L is an isomorphism $L \longrightarrow L$.

Example 3.1.2. The complex conjugation map $\mathbb{Q}(i) \longrightarrow \mathbb{C}$ is a field monomorphism but not an isomorphism. If we instead consider it as a map $\mathbb{Q}(i) \longrightarrow \mathbb{Q}(i)$ then we get an automorphism. We will be interested in this way of producing automorphisms in a moment.

Example 3.1.3. Let ζ be a primitive cube root of unity. The map $\mathbb{Q}(\sqrt[3]{2}) \longrightarrow \mathbb{Q}(\zeta\sqrt[3]{2})$ that replaces all $\sqrt[3]{2}$'s with $\zeta\sqrt[3]{2}$ is a field isomorphism but notice that it is not an automorphism ($\mathbb{Q}(\sqrt[3]{2}) \neq \mathbb{Q}(\zeta\sqrt[3]{2})$ since the LHS consists of real numbers but the RHS contains imaginary things). Later we will see how this example explains why we have to distinguish between isomorphisms and automorphisms. This will show that the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not a *normal* extension.

Now we start to consider the set of all automorphisms of a field L as a whole.

Definition 3.1.4. The *automorphism group* of a field L is the set of all automorphisms of L. We denote it by $\mathrm{Aut}(L)$.

Lemma 3.1.5. *The set Aut(L) is really a group under composition of maps.*

Proof. First we prove closure. Take $\tau, \sigma \in \mathrm{Aut}(L)$. Then the composition $\tau\sigma$ is certainly a map $L \longrightarrow L$. It is left as an exercise to show that it satisfies the axioms of an automorphism. Associativity is automatic since composition of maps is always associative and the identity automorphism (id: $L \longrightarrow L$ defined by $x \longmapsto x$) is the identity element. The inverse of τ (which exists) is also an automorphism of L (check). □

3.2 The Galois group

As mentioned earlier, we want to make a group that somehow exhibits the symmetry of a field extension. We have recreated all of what was discussed earlier except the fixing of the smaller field. This is what we now throw in to construct the Galois group.

Definition 3.2.1. Given a field extension L/K the *Galois group* of L/K is the subgroup of $\mathrm{Aut}(L)$ consisting of automorphisms that fix elements of K, i.e. automorphisms that restrict to give the identity map $K \longrightarrow K$. We denote the Galois group by $\mathrm{Gal}(L/K)$ and refer to its elements as K-*automorphisms* of L.

It is clear that this is a group and is left to the reader as an exercise (note that it only remains to check the conditions on fixing K). We will try and find a few Galois groups by ad-hoc methods now. However, once we do these we will see a few tricks that we can use in general.

Example 3.2.2. Consider the extension $\mathbb{C}/\mathbb{R}$ again. Recall that we may take i as a generator here. Take any $\sigma \in \mathrm{Gal}(\mathbb{C}/\mathbb{R})$. Then, using the properties of automorphisms:

$$\sigma(a+ib) = \sigma(a) + \sigma(ib) = a + b\sigma(i)$$

so that we determine the map σ once we figure out what $\sigma(i)$ is.

Now i satisfies $i^2 + 1 = 0$. Applying σ to both sides and again using the properties of automorphisms tells us that:

$$\sigma(i) = \pm i.$$

The possibility $\sigma(i) = i$ gives us the identity map:

$$\mathrm{id} : \mathbb{C} \longrightarrow \mathbb{C}$$

$$a + ib \longmapsto a + ib.$$

The possibility $\sigma(i) = -i$ gives us the complex conjugate map:

$$\mathrm{conj} : \mathbb{C} \longrightarrow \mathbb{C}$$

$$a + ib \longmapsto a - ib.$$

Both of these maps are actually automorphisms of $\mathbb{C}$ (check this) and they both fix real numbers. Hence $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{\mathrm{id}, \mathrm{conj}\} \cong \mathbb{Z}/2\mathbb{Z}$, the cyclic group of order 2. This is reflected in the fact that doing the complex conjugate twice gives the identity map. Notice that $|\mathrm{Gal}(\mathbb{C}/\mathbb{R})| = [\mathbb{C} : \mathbb{R}]$. Could this be a coincidence?

Example 3.2.3. Consider the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ and take σ in the Galois group. Then similar to last time:

$$\sigma(a + b\sqrt[3]{2} + c(\sqrt[3]{2})^2) = a + b\sigma(\sqrt[3]{2}) + c(\sigma(\sqrt[3]{2}))^2$$

so that this time we only need to figure out what $\sigma(\sqrt[3]{2})$ is.

The element $\sqrt[3]{2}$ satisfies $(\sqrt[3]{2})^3 - 2 = 0$. Applying σ as before gives three possibilities:

$$\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$$

$$\sigma(\sqrt[3]{2}) = \zeta\sqrt[3]{2}$$

$$\sigma(\sqrt[3]{2}) = \zeta^2\sqrt[3]{2}.$$

However, as noted in a previous example, the last two possibilities will not create automorphisms of $\mathbb{Q}(\sqrt[3]{2})$ (they make isomorphisms with other fields). The first possibility leads to the identity automorphism. Hence $\mathrm{Gal}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\mathrm{id}\}$ is trivial. Here the Galois group does not have the same size as the degree of the extension.

4 Properties of the Galois group

We need to generalize the ideas in the previous two examples. How might we do this? Well, as said earlier, we will only consider extensions of finite degree. In fact to begin with we will consider simple extensions $K(\alpha)/K$ since then we will be able to build up in steps the theory for any extension of finite degree.

Here are the main points we need to think about, based on the examples:

- Given an element σ of the Galois group, which basis elements is it enough to exaluate σ on to completely describe σ? For finite degree simple extensions $K(\alpha)/K$ we can see that finding $\sigma(\alpha)$ is enough (recall here that a basis consists of powers of α). Notice the similarities with linear maps on vector spaces, to describe a linear map it is enough to evaluate it on basis elements. Here though we have multiplication to contend with too so that it is often enough to evaluate on a subset of the vector space basis and then build the rest multiplicatively (for example with the basis $\{1, \sqrt{2}, \sqrt{3}, \sqrt{6}\}$ for $\mathbb{Q}(\sqrt{2}, \sqrt{3})$ as a $\mathbb{Q}$-vector space we would only need to know $\sigma(\sqrt{2})$ and $\sigma(\sqrt{3})$ and then we could find $\sigma(\sqrt{6})$ by multiplying the two together since $\sqrt{6} = \sqrt{2}\sqrt{3}$).
- How do we find the possible values for $\sigma(\alpha)$? Can we use the fact that α is algebraic over K? We will use the minimal polynomial of α over K to find the possibilities for $\sigma(\alpha)$, as in the examples.
- Which possibilities for $\sigma(\alpha)$ will actually give automorphisms? Will different $\sigma(\alpha)$'s give the same automorphism? These are more delicate matters as the examples show. In the first example all possibilities gave different automorphisms yet in the second some didnt give automorphisms at all. The notions of normal and separable extensions will tame these situations.
- Is the Galois group always finite? How many elements does it have, or if this is not possible to predict then can we find a bound for this?

Once we have tackled these points we will have an algorithm for finding the Galois group of any finite degree extension (given knowledge of the generator(s)). We start with the second point.

4.1 A Galois group action

In the previous examples we found that for a generator α, we were able to use a certain polynomial having α as a root in order to find out the possibilities for $\sigma(\alpha)$. In this subsection we make this explicit by making a group action of the Galois group on certain roots of polynomials defined over K. Applying this to the minimal polynomial of α over K we will see that the action is quite special in that it is transitive on such roots (explained soon).

To make this formal we have the following result:

Theorem 4.1.1. *Let L/K be a finite extension and let f be a polynomial with coefficients in K. The group $Gal(L/K)$ acts on the roots of f that lie in L.*

Proof. Choose any $\sigma \in \mathrm{Gal}(L/K)$ and a root α of f lying in L. We must show that $\sigma(\alpha)$ is also a root of f (it must lie in L automatically because σ maps $L \longrightarrow L$). This tells us that the group action is well defined.

Suppose that f has the form:

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0,$$

where each $a_i \in K$. Then the fact that α is a root of f tells us that:

$$f(\alpha) = a_n \alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1 \alpha + a_0 = 0.$$

Now apply σ to see that:

$$\sigma(a_n \alpha^n + a_{n-1}\alpha^{n-1} + \ldots + a_1 \alpha + a_0) = \sigma(0) = 0.$$

However, using the fact that σ is a K-automorphism of L (so consequently fixes the a_i terms and behaves nicely with respect to addition and multiplication), we see that the LHS is the same as:

$$a_n(\sigma(\alpha))^n + a_{n-1}(\sigma(\alpha))^{n-1} + \ldots + a_1(\sigma(\alpha)) + a_0 = f(\sigma(\alpha)),$$

so that $\sigma(\alpha)$ is another root of f.

The group action axioms are trivial to check and are left as an exercise. □

Note that this is not just a result about the generator of a field extension, it is a general result about ANY polynomial over K. No matter which such polynomial you choose the Galois group has an action on its L-valued roots. Different polynomials give different actions and each one tells us a small piece of info about both the group itself and the set of roots (just as with any action). This is what will be helpful when we define the Galois group of a polynomial.

As discussed earlier, we know that for simple extensions $K(\alpha)/K$ we need only find $\sigma(\alpha)$ in order to completely define σ as a map on $K(\alpha)$. By the above theorem we can use ANY polynomial over K which has α as a root in order to find the possibilities for $\sigma(\alpha)\ldots$ they will just be the other roots of this polynomial that lie in $K(\alpha)$. But how will we know which of these possibilities for $\sigma(\alpha)$ actually give us automorphisms?

The key to this is to use the minimal polynomial of α over K. The action here will turn out to be very special.

Definition 4.1.2. Let G be a group acting on a set X. The action is *transitive* if given any two $x, y \in X$, there exists $g \in G$ such that $g.x = y$. Alternatively there is only one orbit under the action.

Example 4.1.3. Let the group D_4 of symmetries of the square act on the corners of a square. This action is transitive since any corner can be sent to any corner via rotations. However, if instead we only allowed the two rotations e and r_2 (rotation about 180 degrees) then the action is not transitive since no corner can be sent to an adjacent one.

Example 4.1.4. Let the group S_n of permutations on n objects act on the set $X = \{1, 2, 3, \ldots, n\}$ in the usual way. This action is transitive since the transposition (ij) will send number i to number j.

The next theorem sets the ball rolling towards our goal of finding the possibilities for the elements of the Galois group. If we use an irreducible polynomial over K then the action of the Galois group described above turns out to be transitive (on the roots lying in L). First we need an important (but technical) lemma, which will be stated without proof. It will be found in any good Galois theory book.

Lemma 4.1.5. *Let $K \subseteq M \subseteq L$ be a tower of fields and take $\alpha, \beta \in L$ sharing the same minimal polynomial over K. Given a K-monomorphism $\tau : M \longmapsto L$ there exists a K-automorphism $\sigma : L \longmapsto L$ with $\sigma|_M = \tau$ and $\sigma(\alpha) = \beta$.*

Now we are ready to prove transitivity of the action.

Theorem 4.1.6. *Let L/K be a finite extension and suppose that f is an irreducible polynomial over K. Then Gal(L/K) acts transitively on the set of distinct roots of f lying in L.*

Proof. Suppose $\alpha, \beta \in L$ are two distinct roots of f. We show that there exists $\sigma \in \text{Gal}(L/K)$ such that $\sigma(\alpha) = \beta$.

First note that we have an isomorphism $K(\alpha) \cong K(\beta)$, induced by the map $\alpha \mapsto \beta$, i.e. the map:

$$\sum_{i=0}^{n} a_i \alpha^i \longmapsto \sum_{i=1}^{n} a_i \beta^i.$$

This map clearly fixes elements of K.

Extend the above map into a K-monomorphism $K(\alpha) \mapsto L$ (we can do this because $\beta \in L$ so $K(\beta) \subseteq L$). Finally use the above lemma to extend this map to a K-automorphism $\sigma : L \mapsto L$ (we can do this because $\alpha \in L$ so $K(\alpha) \subseteq L$). We are done now because we have constructed a K-automorphism of L which satisfies $\sigma(\alpha) = \beta$. □

Now we are in business because we may apply this to special irreducible polynomials...the minimal polynomials of the generators! Doing this gets us a neat corollary:

Corollary 4.1.7. *We have that $|Gal(L/K)| \leq [L : K]$ for any finite extension L/K. Further suppose that $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for linearly independent α_i's and that each α_i has minimal polynomial f_i over K (so that the f_i's are distinct). Then $|Gal(L/K)| = k_1 k_2 \ldots k_n$, where k_i is the number of (distinct) roots (lying in L) of the f_i over K.*

Proof. Let $\sigma \in$Gal(L/K). Since $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ is built from K and the n generators $\alpha_1, \alpha_2, \ldots, \alpha_n$ we need only find $\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_n)$ in order to fully describe σ as a map on L. Also the α_i are linearly independent so we need ALL $\sigma(\alpha_i)$ values in order to fully describe σ. Now each α_i is a root of the irreducible polynomial f_i so that $\sigma(\alpha_i)$ is another root of f_i.

However Gal(L/K) acts transitively on the distinct roots of f_i that lie in L. There are k_i of these, so $\sigma(\alpha_i)$ can take any one of k_i possible values. Since the α_i are independent we thus see that there are $k_1 k_2 \ldots k_n$ possible choices for the list $\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_n)$. Further every possible choice DOES occur by transitivity of the action on the f_i's.

Thus

$$|\text{Gal}(L/K)| = k_1 k_2 \ldots k_n \leq \deg(f_1)\deg(f_2)\ldots\deg(f_n) = [L : K].$$

□

We have certainly seen examples of equality in the above and this type of behaviour deserves a name:

Definition 4.1.8. A finite extension L/K is called a *Galois extension* if $|\text{Gal}(L/K)| = [L : K]$.

Galois extensions will come back in chapter 5. These extensions will have extremely nice properties in that their Galois subgroups will correspond to subfields of L containing K.

5 Examples

In this section we consider a few examples using the theory that we uncovered in the previous section. We will study certain classes of field extension and will find their Galois groups.

5.1 Quadratic extensions

A quadratic extension of a field K is a field L with $[L : K] = 2$.

Proposition 5.1.1. *Every quadratic extension of K is of the form $K(\alpha)$ for some $\alpha \notin K$ satisfying $\alpha^2 \in K$.*

Proof. The fact that $[L : K] = 2$ means that we have a basis of L/K of the form $\{1, \beta\}$ for some $\beta \in L \setminus K$. Now we must have that $K \subseteq K(\beta) \subseteq L$. Using tower of fields we have:

$$2 = [L : K] = [L : K(\beta)][K(\beta) : K].$$

The fact that $\beta \notin K$ now implies $[K(\beta) : K] = 2$ and $[L : K(\beta)] = 1$. From this we know that $L = K(\beta)$.

It remains to create a generator α that satisfies the details of the proposition. The fact that $[K(\beta) : K] = 2$ tells us that $\{1, \beta, \beta^2\}$ is linearly dependent over K (since a basis consists of two elements). So there exists $a, b, c \in K$ such that $a\beta^2 + b\beta + c = 0$. Completing the square gives $(\beta + \frac{b}{2a})^2 = \frac{b^2 - 4ac}{2a} \in K$.

Let $\alpha = \beta + \frac{b}{2a}$. Then $L = K(\beta) = K(\alpha)$ and $\alpha^2 \in K$. This completes the proof. □

Now we can describe the Galois group of any quadratic extension.

Theorem 5.1.2. *Every quadratic extension L/K has Galois group isomorphic to $\mathbb{Z}/2\mathbb{Z}$, the cyclic group of order 2.*

Proof. By the proposition we may write $L = K(\alpha)$ for some $\alpha \notin K$ and $\alpha^2 \in K$. Suppose that $\alpha^2 = k \in K$ then α is a root of the polynomial $x^2 - k$ over K. This polynomial is irreducible since $\alpha \notin K$ so that there is no linear polynomial over K having α as a root.

The roots of the polynomial $x^2 - k$ are $\pm\alpha$. So the Galois group has two elements defined by $\alpha \mapsto \alpha$ and $\alpha \mapsto -\alpha$. This follows from the transitivity of the action, there MUST exist a unique element of the Galois group sending α to each possible root.

These two maps are defined in full by:

$$\sigma_1 : a_0 + a_1\alpha \longmapsto a_0 + a_1\alpha,$$

$$\sigma_2 : a_0 + a_1\alpha \longmapsto a_0 - a_1\alpha.$$

The second of these is a generalised complex conjugation, the first is the identity map. Thus $\mathrm{Gal}(L/K) = \{\sigma_1, \sigma_2\} \cong \mathbb{Z}/2\mathbb{Z}$ since there is only one group of order 2 upto isomorphism. (Note that $\sigma_2^2 = \sigma_1$, hence σ_2 is the element of order 2 and σ_1 is the identity element. □

5.2 Multiquadratic extensions

Now that we have considered extensions formed by adjoining one square root we now think about adjoining more than one.

Definition 5.2.1. A multiquadratic extension is one of the form $K(\alpha_1, \alpha_2, \ldots, \alpha_n)/K$, where each $\alpha_i \notin K$ and $\alpha_i^2 \in K$.

In order to find the Galois group here we have to be more careful. The α_i's might not be linearly independent, a problem we didn't have to consider when we adjoined one single element. The next example will make this clear.

Example 5.2.2. Both the extensions $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2}, \sqrt{8})/\mathbb{Q}$ are multiquadratic. However, the second is the same as $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$ since $\sqrt{8} = 2\sqrt{2} \in \mathbb{Q}(\sqrt{2})$. The elements $\sqrt{2}, \sqrt{8}$ are NOT linearly independent over $\mathbb{Q}$.

We are ready to find the Galois group of a general multiquadratic extension.

Theorem 5.2.3. *Suppose that $K(\alpha_1, \alpha_2, \ldots, \alpha_n)/K$ is a multiquadratic extension with linearly independent α_i's. Then $|Gal(K(\alpha_1, \alpha_2, \ldots, \alpha_n)/K)| = 2^n$ with elements given by every possibility taken from the n maps $\alpha_i \mapsto \pm\alpha_i$. The Galois group is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^n$.*

Proof. Take $\sigma \in \mathrm{Gal}(K(\alpha_1, \alpha_2, \ldots, \alpha_n)/K)$. As usual, linear independence tells us that we need to find $\sigma(\alpha_i)$ for each i in order to fully describe σ. But a similar argument to the last section tells us that $\sigma(\alpha_i) = \pm\alpha_i$ for each i. Thus there are 2^n possibilities for the list $\sigma(\alpha_1), \sigma(\alpha_2), \ldots, \sigma(\alpha_n)$ and that each such map has order 2 in the group. This completes the proof. □

Example 5.2.4. Take the extension $\mathbb{Q}(\sqrt{2}, \sqrt{3})/\mathbb{Q}$ from earlier. The numbers $\sqrt{2}$ and $\sqrt{3}$ are linearly independent over $\mathbb{Q}$ (check this).

So by the theorem the elements of the Galois group are described by the four possibilities:

$$\begin{aligned}
\sigma_1 &: \sqrt{2} \mapsto \sqrt{2} \qquad \sqrt{3} \mapsto \sqrt{3} \\
\sigma_2 &: \sqrt{2} \mapsto \sqrt{2} \qquad \sqrt{3} \mapsto -\sqrt{3} \\
\sigma_3 &: \sqrt{2} \mapsto -\sqrt{2} \qquad \sqrt{3} \mapsto \sqrt{3} \\
\sigma_4 &: \sqrt{2} \mapsto -\sqrt{2} \qquad \sqrt{3} \mapsto -\sqrt{3}
\end{aligned}$$

Explicitly:

$$\begin{aligned}
\sigma_1 &: a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \longmapsto a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \\
\sigma_1 &: a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \longmapsto a + b\sqrt{2} - c\sqrt{3} - d\sqrt{6}
\end{aligned}$$

$$\sigma_1 : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \longmapsto a - b\sqrt{2} + c\sqrt{3} - d\sqrt{6}$$
$$\sigma_1 : a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \longmapsto a - b\sqrt{2} - c\sqrt{3} + d\sqrt{6}$$

Notice that each of these has order 2 and that $\sigma_2\sigma_3 = \sigma_4 = \sigma_3\sigma_2$. Hence the Galois group of this extension is $\langle \sigma_2, \sigma_3 \rangle \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

5.3 Cyclotomic extensions

Cyclotomic extensions are extensions formed by adjoining roots of unity. These extensions are extremely useful in many areas of maths, such as number theory, algebra and even geometry. Gauss used them to do many marvelous things, including to show that the regular p-gon can be constructed with ruler and compass if and only if $p = 2$ or p is a Fermat prime. One direction of this is easy to prove, the other not so easy. Some of these uses require the Galois theory of such extensions and will be explored in the exercise sheets.

Let p be a prime and let ζ be a primitive p-th root of unity. Recall from earlier that $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$, since the minimal polynomial of ζ over $\mathbb{Q}$ is $x^{p-1} + x^{p-2} + \ldots + x + 1$. Notice that the roots of this polynomial are $\zeta, \zeta^2, \zeta^3, \ldots, \zeta^{p-1}$. Luckily all of the roots lie in $\mathbb{Q}(\zeta)$.

Thus the Galois group has to act transitively on these elements. Our theorems about the Galois group now tell us that the possible $\mathbb{Q}$-automorphisms of $\mathbb{Q}(\zeta)$ are described by:

$$\sigma_i : \zeta \mapsto \zeta^i$$

for $i = 1, 2, \ldots, p - 1$. So the Galois group has $p - 1$ elements.

Notice that:

$$\sigma_i\sigma_j(\zeta) = \sigma_i(\zeta^j) = \sigma_i(\zeta)^j = \zeta^{ij} = \sigma_{ij}(\zeta)$$

so that $\sigma_i\sigma_j = \sigma_{ij}$. This shows that the group operation in $\mathrm{Gal}\mathbb{Q}(\zeta)/\mathbb{Q})$ behaves exactly like multiplication mod p.

Note also that the Galois group is abelian since:

$$\sigma_i\sigma_j(\zeta) = \zeta^{ij} = \zeta^{ji} = \sigma_j\sigma_i(\zeta).$$

To make all of this precise, we have the following:

Theorem 5.3.1. *Let p be prime and ζ be a primitive pth root of unity. Then $Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/p\mathbb{Z})^\times$, the multiplicative group of non-zero integers mod p.*

Proof. Most of this is done above. The isomorphism is given explicitly by:

$$\sigma_i \mapsto \bar{i}.$$

□

The isomorphism above is one of great importance in number theory. It is quite remarkable that a purely algebraic construction such as the Galois group has connections with something that is highly number theoretical in flavour, congruence mod p. In fact not far from this lies a proof of quadratic reciprocity. Historically this led number theorists to start looking at Galois groups for more general reciprocity laws, leading to an interesting branch of number theory called class field theory. Here we get an infinite number of reciprocity laws, one for each so called abelian extension of number fields (fields that are finite extensions of $\mathbb{Q}$ with abelian Galois groups). In the exercise sheets some of this will be investigated.

A famous result from class field theory is the following theorem, explaining the importance of cyclotomic extensions of $\mathbb{Q}$.

Theorem 5.3.2. *(Kronecker-Weber) Let $L/\mathbb{Q}$ be a finite extension with abelian Galois group. Then $L \subseteq \mathbb{Q}(\zeta)$ for some nth root of unity ζ.*

This is not easy to prove but gives a nice tool for working with abelian extensions of $\mathbb{Q}$. Class field theory gives similar results for extensions of other fields, similar to $\mathbb{Q}$. However, examples can demonstrate this.

Example 5.3.3. In the exercise sheets you will use Gauss sums to prove that the field $\mathbb{Q}(\sqrt{(-1)^{\frac{p-1}{2}}p})$ is contained in the cyclotomic field $\mathbb{Q}(\zeta)$ where ζ is a primitive pth root of unity. This demonstrates a specific case of the Kronecker-Weber theorem. In fact from here it is easy to see that all quadratic extensions of $\mathbb{Q}$ must lie inside a cyclotomic field (see exercise sheet). This inclusion of fields leads to the proof of quadratic reciprocity alluded to above (to see a connection note that $(-1)^{\frac{p-1}{2}} = \left(\frac{-1}{p}\right)$, a Legendre symbol). More will be investigated in the sheets.

What happens when we adjoin primitive nth roots of unity for other n? The general result is as follows:

Theorem 5.3.4. *Let ζ be a primitive nth root of unity for some integer n. Then $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n)$, where ϕ is the Euler phi function. Further:*

$$Gal(\mathbb{Q}(\zeta)/\mathbb{Q}) \cong (\mathbb{Z}/n\mathbb{Z})^\times$$

Proof. The primitive nth roots of unity are all of the form ζ^i for i coprime to n. It turns out that the minimal polynomial of ζ over $\mathbb{Q}$ is the nth cyclotomic polynomial:

$$\prod_{\substack{1\leq i\leq n \\ \text{hcf}(i,n)=1}} (x - \zeta^i).$$

Certainly ζ is a root of this polynomial but the fact that it has rational coefficients and is irreducible over $\mathbb{Q}$ is not so easy to prove and is omitted (see any Stewart's book on Galois theory for details).

Now it is clear that all primitive roots of unity lie in $\mathbb{Q}(\zeta)$ and they are all roots of the minimal polynomial. Thus the Galois group acts transitively on these, giving elements (for i coprime to n):

$$\sigma_i : \zeta \longmapsto \zeta^i.$$

As in the previous case, the map:

$$\sigma_i \longmapsto \bar{i}$$

gives the required isomorphism. □

It should be noted that we have only considered cyclotomic extensions of $\mathbb{Q}$ here. We can adjoin roots of unity to other fields but the results are not so simple anymore. Maybe the field you start with contains some roots of unity already? Maybe the minimal polynomial will now have smaller degree? (We used Eisenstein's criterion to prove irreducibility of the cyclotomic polynomial over $\mathbb{Q}$, but this doesn't tell us about irreducibility over other fields. Well there is a generalisation of Eisenstein to certain number fields but this is quite a bit more advanced.)

There are lots of nice results in general which let us study other cyclotomic extensions but we shall move on since we have done the cases which will interest us the most in these notes.

6 Normal and Separable extensions

Some of the results at the end of chapter 4 were found to be quite interesting and useful. However they werent quite as beautiful as we hoped they would be.

Two problems arose:

- We had to keep speaking of the "roots lying in L" since by definition elements of the Galois group can only act on things inside L. There were "missing roots" of polynomials, ones that belonged to some other field, so couldn't be acted on.
- We had to make sure to say that the Galois group acts transitively on the DISTINCT roots lying in L. Can an irreducible polynomial ever have repeated roots? It might seem counter-intuitive but yes it is possible. However, this kind of behaviour never happens in fields of characteristic 0.

Both of these problems somehow stopped the Galois group from being the biggest that it can be. The lack of enough roots in L meant that there wasn't enough places to send a given root and the possibility of repeated roots meant that even once the given root was sent to all others, the same automorphism might have been obtained twice!

In this section we define two conditions a field extension may have, normality and separability. These are created in order to abolish the behaviour mentioned in the two points above.

Once done we will be in a position to show exactly what we suspect ... that there are no more problems, meaning that a finite extension which is both normal and separable is a Galois extension (i.e. the Galois group is the biggest it can be, it has size $[L : K]$).

6.1 Normality

To tackle point 1 we need to consider only extensions where irreducible polynomials have no "missing roots". The following does this quite nicely.

Definition 6.1.1. A finite extension L/K is *normal* if any irreducible polynomial f over K having a single root in L actually has all of its roots in L, i.e. the polynomial factorises fully into linear terms.

As said earlier, this does NOT imply that the roots are distinct, just that all of them lie in L once you know that one of them does.

The use of the word normal will be apparent later. As can be imagined, the definition of normality is not easy to work with since we have to prove something about infinitely many polynomials. Fortunately normal extensions have a nicer description.

Theorem 6.1.2. *Let L/K be a finite extension. Then L/K is normal if and only if L is the splitting field for some polynomial over K.*

Proof. Omitted. See Stewart. □

One other property of normal extensions is going to be paramount later.

Lemma 6.1.3. *Let L/K be a finite normal extension. Then given any field M with $K \subseteq M \subseteq L$ we have that L/M is a normal extension.*

Proof. We know that L/K is normal so that L is the splitting field for some polynomial f over K. Now since $K \subseteq M$ we can consider f to be a polynomial over M too. By minimality of the splitting field, we must have that L is still the splitting field for f, even over M. Thus L/M is normal. □

6.2 Separability

Now that we have tackled point 1 we had better make a start with point 2. Now we are considering the possibility of repeated roots occuring.

Definition 6.2.1. A finite extension L/K is separable if every irreducible polynomial over K has only simple roots (in L) when factorised over its splitting field (so there are no repeated roots).

Luckily we know ways of telling whether polynomials over a field have repeated roots. The derivative test is perfect here:

Lemma 6.2.2. *Let f be a polynomial defined over a field K. Then f has repeated roots in its splitting field over K if and only if f and $\frac{df}{dx}$ share a common polynomial factor of degree greater than 1. (Note that the derivative is a purely algebraic thing here, it makes sense because we are in a field).*

Proof. Omitted. Left as an exercise. □

In fields of characteristic 0 we have no problems with repeated roots:

Theorem 6.2.3. *Any finite extension L/K where K has characteristic 0 is a separable extension.*

Proof. Let:

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots, a_1 x + a_0$$

be an irreducible polynomial over K. Suppose that f has a repeated root. Then f shares a common polynomial factor of degree greater than 1 with its derivative:

$$f'(x) = na_n x^{n-1} + a_{n-1}(n-1)x^{n-2} + \ldots + 2a_2 + a_1.$$

Since f is irreducible this common factor must be f itself. But f' has smaller degree than f so $f'(x) = 0$. We have no notion of integration here so now we have to just equate coefficients and gather information about f that way. Doing this tells us that $na_i = 0$ for all $i \geq 1$. But we are in an integral domain so that either $n = 0$ or $a_i = 0$. However, the first possibility cannot be the case since we are in a field of characteristic 0, hence $a_i = 0$ for all $i \geq 1$. Thus f is constant, giving us our contradiction. □

The problem arises when we get to fields of characteristic p. Since here multiplication by p gives 0, it might be that the derivative is 0 without the polynomial being constant! (remember the derivative of say x^p is px^{p-1}, which is 0 in fields of characteristic p.)

Lemma 6.2.4. *The only polynomials that have repeated roots in characteristic p are of the form:*

$$f(x) = k_0 + k_1 x^p + \ldots + k_n x^{np}.$$

Proof. Left as an exercise. Use the discussion above. □

Finally we link searable extensions that come from subfields.

Theorem 6.2.5. *Let L/K be a separable extension. Then for any field M with $K \subseteq M \subseteq L$ we have that L/M and M/K are both separable.*

Proof. It is obvious that M/K is separable since $M \subseteq L$ and no irreducible polynomia over Kl has repeated roots in L. Now consider $\alpha \in L$ and let f_K, f_M be the minimal polynomials of α over K, M respectively. Now we must have that $f_M | f_K$ (why?) and so f_M cannot have any repeated roots since f_K doesn't (since L/K is separable). □

6.3 Putting together the pieces

Imagine an extension L/K that is both separable and normal now. Given one generator α for the extension we know that its minimal polynomial f over K is irreducible and has one root in L (namely α itself). So normality tells us that all of the roots of f lie in L. Separability now tells us that none of these roots are repeated. Finally the transitivity of the Galois group action tells us that there are now exactly $\deg(f)$ possible places to send α under the action. Doing this for all generators we see that the Galois group has maximum order of $[L : K]$, so that the extension is Galois!

In essence we have proved (informally) one direction of:

Theorem 6.3.1. *A finite extension L/K is Galois if and only if it is normal and separable.*

Proof. Omitted. See Stewart. □

6.4 Extensions of finite fields

We are in the position to look at what happens with finite fields now. Here the Galois group is going to be well behaved in that it is cyclic. In fact we only need to study finite extensions of $\mathbb{F}_p$, since later the main theorem of Galois theory will connect this situation with any extension of finite fields.

First we notice the following:

Lemma 6.4.1. *Each finite extension of the form $\mathbb{F}_{p^n}/\mathbb{F}_p$ is a Galois extension.*

Proof. It is enough to prove normality and separability. Normality follows from the construction of $\mathbb{F}_{p^n}$ as the splitting field of the polynomial $x^{p^n} - x$ over $\mathbb{F}_p$. Separability follows from the fact that the derivative:

$$\frac{d}{dx}(x^{p^n} - x) = p^n x^{p^n - 1} - 1 \equiv -1$$

is constant in a field of characteristic p and so the polynomial $x^{p^n} - x$ has no repeated roots in $\mathbb{F}_{p^n}$. □

Now that we know that these extensions are Galois we see that $|\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)| = [\mathbb{F}_{p^n} : \mathbb{F}_p] = n$. How might we go about finding the elements of the Galois group?

Proposition 6.4.2. *Let $F = \mathbb{F}_{p^n}$ be a finite field of characteristic p. The map $x \mapsto x^p$ is an automorphism of F. In fact it fixes elements of $\mathbb{F}_p$ so that actually it belongs to $Gal(\mathbb{F}_{p^n}/\mathbb{F})$.*

Proof. Notice that the map fixes elements of $\mathbb{F}_p$ by Fermat's little theorem. The rest of the proof is left as an exercise since it remains to check the axioms. □

Definition 6.4.3. The above automorphism is called the *Frobenius automorphism*, denoted ϕ_p.

The Frobenius automorphism is quite important in algebraic geometry for studying points modulo p on curves. It also appears quite heavily in algebraic number theory when trying to generalise the Legendre symbol and making general reciprocity laws. We can quite simply prove that this Frobenius automorphism actually generates the Galois group of any finite extension of $\mathbb{F}_p$.

Theorem 6.4.4. *We have that $Gal(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \phi_p \rangle \cong \mathbb{Z}/n\mathbb{Z}$, a cyclic group of order n.*

Proof. First we prove that ϕ_p^n is the identity automorphism. This is simple enough:

$$\phi_p^n(x) = x^{p^n} = x$$

since every $x \in \mathbb{F}^{p^n}$ satisfies $x^{p^n} = x$.

Next we prove that no smaller power of ϕ_p can be the identity, meaning that ϕ_p has order n in the Galois group. Once we know this it follows that the group is cyclic (since we know that the Galois group has order n).

Suppose $\phi_p^m = id$ for some $1 \leq m < n$. Then for all $x \in \mathbb{F}_{p^n}$ we must have that:

$$\phi_p^m(x) = x^{p^m} = x,$$

hence all x would satisfy $x^{p^m} - x = 0$. However we are working over a field so that the polynomial $x^{p^m} - x$ can have at most p^m roots, giving a contradiction. □

The nice thing about cyclic groups is that we know what their subgroups look like. In fact if $\langle g \rangle$ is a cyclic group of order n then we have a unique subgroup of order d for each positive divisor d of n, this being $\langle g^{\frac{n}{d}} \rangle$. In the next section we will prove that knowing this is enough to describe all fields lying between $\mathbb{F}_p$ and $\mathbb{F}_{p^n}$.

7 The main theorem of Galois theory

This section is the most important in the whole course. Now that we have invented the Galois group and studied its properties we are able to give a taster of what the group can do. We pose the question; Given a finite extension L/K, how do we find all fields lying inbetween L and K?

Definition 7.0.5. Given a finite extension L/K, the fields M satisfying $K \subseteq M \subseteq L$ will be called *intermediate fields.*

Galois realised that the Galois group plays a part in answering the above question. Recall that the Galois group is intuitively the set of symmetries of a field extension so that subgroups of the Galois group might correspond to other field extensions with this subset of things as symmetries. This will turn out to be the case and we will find a way to create an intermediate field from a subgroup of the Galois group. We will also be able to go the other way and find a way to make a subgroup from an intermediate field.

However, this will not be a one-to-one correspondence in general. The big theorem is that for Galois extensions we do have a bijection. More things will be true but first we work towards defining the correspondence. We notice that by definition, everything in the Galois group fixes elements in K. Is it necessarily true that ONLY the elements of K get fixed?

Example 7.0.6. In the case of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ we saw that the Galois group was trivial, containing only the identity automorphism. Clearly this fixes everything in $\mathbb{Q}(\sqrt[3]{2})$, not just the elements of $\mathbb{Q}$!

It is no coincidence that this extension is not Galois (i.e. it is not normal). We will see soon that Galois extensions do have the property that K is exactly the set of elements that are fixed by the whole Galois group. For now let us consider what elements are fixed by a subgroup of the Galois group.

7.1 From subgroups to intermediate fields - Fixed fields

Lemma 7.1.1. *Let L/K be a finite extension and suppose that H is a subgroup of $Gal(L/K)$. Then the set $L^H = \{x \in L \mid \sigma(x) = x \text{ for all } \sigma \in H\}$ is a subfield of L, containing K.*

Proof. This is simply axiom checking and so is left as an exercise. Note that L^H contains K since by definition each $\sigma \in H$ fixes elements of K. □

Definition 7.1.2. The field L^H is called the *fixed field* of H.

Notice that for any finite extension L/K we have that $L^{\{id\}} = L$ and that $L^{\mathrm{Gal}(L/K)}$ contains K but might be strictly bigger (as in the case of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$). However, intuitively we might be led to believe that bigger subgroups have smaller fixed fields (since it is "harder" to be fixed by more things). This logic is true.

Lemma 7.1.3. *Let H_1, H_2 be two subgroups of $Gal(L/K)$. If $H_1 \subseteq H_2$ then $L^{H_2} \subseteq L^{H_1}$.*

Proof. Take $x \in L^{H_2}$, then $\sigma(x) = x$ for all $\sigma \in H_2$. But $H_1 \subseteq H_2$, so that automatically we have that $\sigma(x) = x$ for all $\sigma \in H_1$. Thus $x \in L^{H_1}$. □

7.2 From intermediate fields to subgroups

We now need to find a way to travel from intermediate fields to subgroups of the Galois group. This is quite easy, we simply take the Galois group with respect to the new field.

Lemma 7.2.1. *Given an intermediate field $K \subseteq M \subseteq L$, the group $Gal(L/M)$ is a subgroup of $Gal(L/K)$.*

Proof. We know that $\mathrm{Gal}(L/M)$ is a group by definition. It lies inside $\mathrm{Gal}(L/K)$ since anything fixing M must fix K (by the inclusion $K \subseteq M$). □

We will need to know how the galois groups with respect to intermediate fields behave. The following result connects them vis conjugation.

Lemma 7.2.2. *If L/K is a finite extension and M is an intermediate field then:*

$$Gal(L/\tau(M)) = \tau\, Gal(L/M)\tau^{-1}$$

for any $\tau \in Gal(L/K)$.

Proof. Take any $\gamma \in \mathrm{Gal}(L/M)$, then $\tau\gamma\tau^{-1}$ is certainly an automorphism of L since it is a composition of automorphisms of L. We check that this element fixes $\tau(M)$, since then we get the inclusion:

$$\tau\mathrm{Gal}(L/M)\tau^{-1} \subseteq \mathrm{Gal}(L/\tau(M)).$$

To check this we take $y \in \tau(M)$ so that $y = \tau(x)$ for some $x \in M$. Then:

$$\tau\gamma\tau^{-1}(y) = \tau\gamma\tau^{-1}(\tau(x)) = \tau\gamma(x) = \tau(x) = y,$$

(since γ fixes elements of M).

The reverse inclusion is similar and is left as an exercise (prove that $\tau^{-1}\mathrm{Gal}(L/\tau(M))\tau \subseteq \mathrm{Gal}(L/M)$). □

7.3 The main theorem of Galois theory

We are now in a position to produce a one to one correspondence between subgroups of the Galois group and intermediate fields (when the extension is Galois).

Theorem 7.3.1. *(The main correspondence of Galois theory) Let L/K be a finite Galois extension. Then the subgroups of $Gal(L/K)$ are in one to one correspondence with the intermediate fields $K \subseteq M \subseteq L$. This correspondence is order-reversing, so that big subgroups correspond to small degree extensions of K and vise versa.*

The details are as follows:

- *Given a subgroup H of the Galois group we associate to it the intermediate field L^H.*
- *Given an intermediate field M we associate to it the subgroup $Gal(L/M)$.*
- *We have that $[L : L^H] = |H|$ and so $[L^H : K] = \frac{|Gal(L/K)|}{|H|}$.*
- *The normal subgroups of the Galois group are in one to one correspondence with intermediate fields that give normal extensions of K. In this case we have that $Gal(L^H/K) \cong Gal(L/K)/H$. This is much stronger than the previous point about the order of this group.*

Proof. We have already considered the correspondence and have shown the order reversing properties, but have yet to prove that it is one to one. This will now be shown now. The proof of the third point is omitted but can be found in chapter 10 of Stewart. It is a technical proof based on linear independence of monomorphisms, a result of Dedekind. We will need to use part 3 in the rest of the proof.

Define two maps:

$$\phi : \{\text{intermediate fields}\} \longrightarrow \{\text{subgroups of the Galois group}\}$$

$$M \longmapsto \mathrm{Gal}(L/M)$$

and

$$\psi : \{\text{subgroups of the Galois group}\} \longrightarrow \{\text{intermediate fields}\}$$

$$H \longmapsto L^H.$$

Then in order to prove that we have a one-to-one correspondence it is enough to proving that ϕ and ψ are maps inverse to each other, i.e. that both maps are bijections.

First we start with an intermediate field M. Now L/K is normal and separable so from earlier L/M must be normal and separable. This means that L/M is Galois, telling us that $L^{\mathrm{Gal}(L/M)} = M$ (i.e. the whole Galois group fixes only the elements in the base field). This is the same as $\psi(\phi(M)) = M$, so that $\psi\phi$ is the identity map on the set of intermediate fields.

Now take any subgroup H of $\mathrm{Gal}(L/K)$. We know that $H \subseteq \mathrm{Gal}(L/L^H)$. We will prove equality, meaning that $\phi(\psi(H)) = H$, giving that $\phi\psi$ is the identity map on the set of subgroups of the Galois group.

Recall above that $L^{\mathrm{Gal}(L/M)} = M$ for any intermediate field M. Let $M = L^H$, so that $L^{\mathrm{Gal}(L/L^H)} = L^H$. From here it is easy since now:

$$|H| = [L : L^H] = [L : L^{\mathrm{Gal}(L/L^H)}] = |\mathrm{Gal}(L/L^H)|,$$

where the last equality also follows from $[L : L^H] = |H|$. Now piece together the facts. We have just found that H and $\mathrm{Gal}(L/L^H)$ are both finite groups, of the same order, with $H \subseteq \mathrm{Gal}(L/L^H)$. Thus $H = \mathrm{Gal}(L/L^H)$ and we are done.

All that remains now is to show that the two concepts of normality match up and to reveal the isomorphism mentioned in the fourth point.

To start, suppose that M is an intermediate field such that M/K is a normal extension. We prove that $\mathrm{Gal}(L/M)$ is a normal subgroup of $\mathrm{Gal}(L/K)$. Take any $\tau \in \mathrm{Gal}(L/K)$. Then the restriction $\tau|_M$ is a K-monomorphism $M \longrightarrow L$. But then we must have that $\tau|_M$ is a K-automorphism of M. This implies that $\tau(M) = M$ and not some other field isomorphic to M.

But now (from earlier):

$$\tau\mathrm{Gal}(L/M)\tau^{-1} = \mathrm{Gal}(L/\tau(M)) = \mathrm{Gal}(L/M),$$

as required.

To prove the converse suppose we have a normal subgroup H of $\mathrm{Gal}(L/K)$. Now we know that $H = \mathrm{Gal}(L/M)$ for some intermediate field M (by the correspondence). Now consider any K-monomorphism $\sigma : M \longrightarrow L$. Then as before we may extend to a K-automorphism τ of L, with $\tau|_M = \sigma$.

Now the normality of the subgroup tells us that:

$$\tau\mathrm{Gal}(L/M)\tau^{-1} = \mathrm{Gal}(L/M).$$

However the LHS is $\mathrm{Gal}(L/\tau(M))$, thus by the one to one nature of the correspondence we must have that $\tau(M) = M$ (no two different intermediate fields can give the same subgroup).

But now we are done since this fact tells us that $\sigma(M) = M$, meaning that σ is a K-automorphism of M, Thus M/K is normal.

As for the last claim, form a surjective group homomorphism via restriction:

$$\mathrm{Gal}(L/K) \longrightarrow \mathrm{Gal}(M/K)$$

$$\tau \longmapsto \tau|_M.$$

The kernel of this map is exactly the group $\mathrm{Gal}(L/M)$ and so the first isomorphism theorem tells us that:

$$\mathrm{Gal}(M/K) \cong \mathrm{Gal}(L/K)/\mathrm{Gal}(L/M) = \mathrm{Gal}(L/K)/H.$$

□

7.4 Returning to finite fields

Earlier we were able to study the Galois groups of finite extensions of $\mathbb{F}_p$. Now that we have the main theorem of Galois theory at our disposal, we may find the Galois groups of a general finite extension of finite fields.

Recall that if p is prime then we found that $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ was cyclic of order n, generated by the Frobenius automorphism ϕ_p. Also each of these extensions are Galois so by our newfound correspondence, the intermediate fields correspond to subgroups of $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$.

But the cyclic group $\langle g \rangle$ of order n has exactly one subgroup of order d for each $d|n$, the cyclic group generated by $g^{\frac{n}{d}}$. So the subgroups of the Galois group are of the form $H_d = \langle \phi_p^d \rangle$ for each divisor d of n. Note that $|H_d| = \frac{n}{d}$.

Again by the correspondence, the fixed field of H_d must have degree $\frac{n}{\frac{n}{d}} = d$ over $\mathbb{F}_p$. It must be a finite field here since it is a subfield of $\mathbb{F}_{p^n}$, thus it is $\mathbb{F}_{p^d}$ (by the uniqueness properties of finite fields). We could have checked this explicitly since if $x \in \mathbb{F}_{p^n}$ is fixed by ϕ_p^d then x satisfies $x^{p^d} = x$ and so $x \in \mathbb{F}_{p^d}$. Also every such element is fixed by H_d and so it must be the fixed field.

We have proved the following:

Theorem 7.4.1. *Let $\mathbb{F}_{p^n}/K$ be an extension of fields. Then $K = \mathbb{F}_{p^d}$ for some $d|n$. Also $Gal(\mathbb{F}_{p^n}/\mathbb{F}_{p^d}) \cong H_d$ and $Gal(\mathbb{F}_{p^d}/\mathbb{F}_p) \cong H_n/H_d$.*

This completely classifies all possible extensions of finite fields.

8 An example using the main theorem

To demonstrate the power of the main theorem of Galois theory we will consider a substantial example. More applications appear on the exercise sheets. In this section we will look at the Galois theory of the extension $\mathbb{Q}(\sqrt{2},\sqrt{3})/\mathbb{Q}$.

First we notice that this extension is automatically separable (we are in characteristic 0). Also the extension is normal since it $\mathbb{Q}(\sqrt{2},\sqrt{3})$ is the splitting field for the polynomial $x^4-5x^2+6 \equiv (x^2-2)(x^2-3)$ over $\mathbb{Q}$. Using the tower of fields argument we find that $[\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2},\sqrt{3}) : \mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 4$. Thus the Galois group has order 4 (since the extension is Galois).

Let's find the elements of the Galois group. The generator $\sqrt{2}$ has minimal polynomial x^2-2 over $\mathbb{Q}$, so that any element of the Galois group must send $\sqrt{2}$ to either of $\pm\sqrt{2}$. Similarly with $\sqrt{3}$. Thus the elements of the Galois group are:

$$\begin{aligned}
\sigma_1 &: \sqrt{2} \mapsto \sqrt{2} \qquad \sqrt{3} \mapsto \sqrt{3} \\
\sigma_2 &: \sqrt{2} \mapsto \sqrt{2} \qquad \sqrt{3} \mapsto -\sqrt{3} \\
\sigma_3 &: \sqrt{2} \mapsto -\sqrt{2} \qquad \sqrt{3} \mapsto \sqrt{3} \\
\sigma_4 &: \sqrt{2} \mapsto -\sqrt{2} \qquad \sqrt{3} \mapsto -\sqrt{3}.
\end{aligned}$$

A few basic calculations show that σ_1 is the identity and that every other element has order 2, so that the Galois group is isomorphic to the Klein four group. This is an abelian group, thus all subgroups are normal, so all intermediate fields must be normal extensions of $\mathbb{Q}$.

What are the subgroups? Well there are two obvious ones; $\{\sigma_1\}$ and the whole group. The first consists of only the identity and so has fixed field being the whole of $\mathbb{Q}(\sqrt{2},\sqrt{3})$. The second is the entire Galois group and so (by Galois extension properties) must have fixed field being the base field, i.e. $\mathbb{Q}$.

Lagrange tells us that every other subgroup has order 2, and so there are three possibilities:

$$\{\sigma_1,\sigma_2\},\{\sigma_1,\sigma_3\},\{\sigma_1,\sigma_4\}.$$

These are all subgroups. How do we find their fixed fields? Well we are forced to work them out by hand. However we do know that they will be quadratic extensions of $\mathbb{Q}$ by the general fact we observed earlier:

$$[L^H : K] = \frac{|\mathrm{Gal}(L/K)|}{|H|}.$$

Take the subgroup $\{\sigma_1,\sigma_2\}$. Now a general element of $\mathbb{Q}(\sqrt{2},\sqrt{3})$ is of the form $x = a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$. In order to be fixed by both σ_1 and σ_2 we must have the following:

$$\sigma_2(x) = x,$$

i.e.

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

Thus anything in the fixed field of this subgroup must have $c=d=0$ (note how we used linear independence subtly here).

So the fixed field here is contained in $\{a+b\sqrt{2} \,|\, a,b \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{2})$. A quick check reveals that actually we have equality here (since everything in $\mathbb{Q}(\sqrt{2})$ IS fixed by σ_1 and σ_2). Notice that $\mathbb{Q}(\sqrt{2})$ is the splitting field of x^2-2 over $\mathbb{Q}$ so that we did get a normal extension field of $\mathbb{Q}$ (as expected).

The other two fixed fields are found in the same way so the calculations are left as an exercise. We get $\mathbb{Q}(\sqrt{3})$ and $\mathbb{Q}(\sqrt{6})$. These are splitting fields for x^2-3 and x^2-6, again as expected.

Now the power of Galois theory tells us that there can be NO OTHER FIELD lying inbetween $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{2},\sqrt{3})$. If there were then we would be able to find another subgroup of the Galois group!

This demonstrates how much the Galois group can tell us about fields. Sometimes the Galois group can be very nicely behaved and can tell us about fields that we might not have known much about. For example studying the Galois group of the cyclotomic extension $\mathbb{Q}(\zeta)/\mathbb{Q}$ can give the existence of certain intermediate fields that might be hard to find explicitly. This is another key part to the proof of quadratic reciprocity mentioned earlier.

Another major use is in the constructibility of polygons. Using field theory it is not so hard to prove that for a prime p, the p-gon cannot be constructed using ruler and compasses unless $p = 2$ or p is a Fermat prime. This is simply the fact that if ζ is a primitive pth root of unity then $[\mathbb{Q}(\zeta) : \mathbb{Q}] = p - 1$ and so we would require $p - 1$ to be a power of 2 in order to not contradict the theorems of constructibility.

However, it is NOT so easy to prove using field theory that all Fermat prime p-gons ARE constructible using ruler and compass. It is not obvious that there exists a tower of fields $\mathbb{Q} \subseteq K_1 \subseteq K_2 \subseteq \dots K_m \subseteq \mathbb{Q}(\zeta)$, where each consecutive extension is quadratic. But using the correspondence of Galois theory we are provided with the existence of such fields (which is enough). The Galois group here is $(\mathbb{Z}/p\mathbb{Z})^\times$, which is known to be cyclic of order $p - 1$. When $p = 2^{2^n} + 1$ is a Fermat prime, this group has order 2^{2^n}. Thus the cyclic nature of the Galois group tells us that there is a unique subgroup of order 2^i for each $i \leq 2^n$. The corresponding (unique) fixed fields will have degree $2^{2^n - i}$ over $\mathbb{Q}$ and so these fields make the tower that we need!

Gauss was able to find the fields explicitly using what are known as Gaussian periods and so was able to actually provide the construction that would produce the p-gon. His method involved a clever use of finite fields with roots of unity but is beyond the scope of these notes.

9 Solving polynomials via radicals

As an end to the course we study how Galois theory was applied classically. When Galois invented his theories he did so in a much more primitive way than these notes have discussed. His findings and creations were purely original concepts when he first made them. He did not express the Galois group as an object attatched to field extensions (since this was a concept developed much later) but as an object attatched to a polynomial to measure symmetries of roots of polynomials. In this section we study how the solvability of polynomials by radicals is linked with a specific property of the Galois group...solvability.

First we describe in modern terms what the Galois group of a polynomial is.

Definition 9.0.2. Let K be a field and f be a polynomial with coefficients in K. The *Galois group* of f over K, denoted by $\mathrm{Gal}(f)$, is $\mathrm{Gal}(L/K)$ where L is the splitting field of f over K.

Example 9.0.3. The Galois group of $x^3 - 1$ over $\mathbb{Q}$ is $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$, where ζ is a primitive cube root of unity. We have already seen that this Galois group is isomorphic to $(\mathbb{Z}/3\mathbb{Z})^\times$. This is reflecting the fact that two of the roots of f, namely ζ and ζ^2 are in some sense connected to each other by symmetry, but the root 1 is not, it is in some sense a different kind of root.

Lemma 9.0.4. *Let f be a separable polynomial over K (assumed here to be field of characteristic 0). We have that $|Gal(f)| = [L : K]$, where L is the splitting field of f over K.*

Proof. By definition $\mathrm{Gal}(f) = \mathrm{Gal}(L/K)$. Now L is the splitting field for f over K, so L/K is normal. Separability is automatic by the characteristic assumption. Hence L/K is Galois, so that $|\mathrm{Gal}(f)| = |\mathrm{Gal}(L/K)| = [L : K]$. □

Recall that the Galois group of a finite extension acts transitively on the roots of irreducible polynomials over the base field. Now that we are reversing the process and starting with an irreducible polynomial, we will be able to place a condition on the corresponding Galois group reflecting the transitivity of the action.

Definition 9.0.5. A subgroup H of S_n is called *transitive* if it acts transitively on $\{1, 2, \dots, n\}$ (using the permutation action).

Now we can have the following lemma:

Lemma 9.0.6. *The Galois group of a polynomial of degree n is isomorphic to a subgroup of S_n. If f is irreducible then the Galois group is a transitive subgroup of S_n.*

Proof. This is a consequence of the fact that the Galois group will permute the roots of f. Also if f is irreducible then the action is transitive, meaning the group should be. □

The previous lemma cuts down the work in finding the Galois group of an irreducible polynomial since not every subgroup of S_n is transitive. In order words, to be the Galois group of an irreducible polynomial we have to have a subgroup that is big enough to act transitively on the roots. This is a big restriction. Also at first thought it seems that we have created a useless definition here. After all we want to study solvability of equations yet to find the Galois group we need to know the splitting field, meaning we have to know the roots. Actually we can tell a great deal about Galois groups of polynomials without having to know the roots!

Example 9.0.7. The only transitive subgroup of S_2 is S_2 itself. The other subgroup contains just the identity element, and so is not transitive. Thus every irreducible quadratic over K (of characteristic 0 say) must have Galois group isomorphic to S_2, i.e. contains a transposition.

This is really telling us that any irreducible quadratic ax^2+bx+c over a field K (of characteristic 0 say) has two different "conjugate" roots that lie in some quadratic extension of K.

You already knew this by the quadratic formula:

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

so that the roots of such a quadratic lie in $K(\sqrt{b^2-4ac})$ and have obvious symmetries.

The discriminant b^2-4ac of an arbitrary quadratic (not necessarily irreducible) tells us the nature of the roots. Recall that if b^2-4ac is the square of an element in K then both roots lie in K. Also if $b^2-4ac=0$ then these roots are equal. Both of these facts can be seen from the formula. However we need a way to tell these things without having to use a formula (since later we will show that there is no formula for degree 5 polynomials or higher).

This can be interpreted in terms of Galois theory as follows. Let the roots of the quadratic be r_1 and r_2 in the splitting field. We create the quantity $\Delta = (r_1-r_2)^2$. It is an exercise to show that Δ is actually equal to the standard discriminant b^2-4ac so that $\Delta \in K$. Clearly $\Delta = 0$ if and only if $r_1 = r_2$.

The question is what happens to $\sqrt{\Delta} = (r_1-r_2)$ under the Galois group action. We know that this element is a root of the (possibly reducible) polynomial $y^2-\Delta$ over K, thus $\sqrt{\Delta}$ can only be sent to $\pm\sqrt{\Delta}$ under the action of the Galois group. The quadratic we started with is not necessarily irreducible so we are not guaranteed that both possibilities can occur (transitivity only works for irreducible polynomials). The polynomial $y^2-\Delta$ is exactly the polynomial you get when "completing the square", after a change of variables.

Now if the Galois group of our quadratic is trivial then $\sqrt{\Delta}$ is fixed by the entire Galois group and so $\sqrt{\Delta} = (r_1-r_2) \in K$ (since K is the fixed field of the Galois group). This is equivalent to $b^2-4ac = (\sqrt{\Delta})^2$ being the square of an element of K. Using this and the fact that $r_1+r_2 = -b \in K$ (exercise), it follows that both $r_1, r_2 \in K$.

If the Galois group is isomorphic to the whole of S_2 then $\sigma(\sqrt{\Delta}) = -\sqrt{\Delta}$ for the nontrivial element and so we no longer have that $\sqrt{\Delta} \in K$, thus the roots do not lie in K anymore.

So the properties of the discriminant we knew before are really telling you things about the Galois group. We need to extend all of this in order to tackle higher degree polynomials. The Δ above was extremely helpful in classifying the possibilities for the roots. We will extend this to give a discriminant for higher degree polynomials.

Example 9.0.8. We will find the transitive subgroups of S_3. By Lagrange any subgroup has order $1, 2, 3$ or 6. Now the only subgroup of order 1 consists of just the identity, which is obviously not transitive. It is clear that no subgroup of order 2 can be transitive too, since each such subgroup contains just one non-identity element so cannot possibly send an element of $\{1,2,3\}$ to any other element of this set.

Clearly S_3 is transitive so it remains to consider subgroups of order 3. Any such subgroup has to be cyclic (it has prime order), generated by a 3-cycle. Notice that there are only two 3-cycles in S_3 so that actually both must be contained in order to have a subgroup of order 3 (the other non-identity elements have order 2 and so cannot be in this group, else Lagrange's theorem would be contradicted). This subgroup is $\{\mathrm{id}, (123), (132)\} \cong A_3$.

So every irreducible cubic over a field K (of characteristic 0) has to have Galois group isomorphic to either A_3 or S_3. In a similar vein to the previous example, the two possibilities for the Galois group stand for two different types of behaviour of the roots.

Now consider any cubic $ax^3 + bx^2 + cx + d$ over K and suppose the roots are r_1, r_2, r_3 in the splitting field. Invent the element $\Delta = ((r_1 - r_2)(r_1 - r_3)(r_2 - r_3))^2$. This is the *discriminant* of the cubic. Again, it is clear that $\Delta = 0$ if and only if two of r_1, r_2, r_3 are equal. It is possible, as with quadratics, to write Δ in terms of a polynomial in the coefficients of the cubic a, b, c, d, showing that $\Delta \in K$ (this gives a cubic version "$b^2c^2 - 4ac^2 - 4b^2d - 27a^2d^2 + 18abcd$" of the quadratic discriminant "$b^2 - 4ac$"). However, we need an argument that will extend to any degree polynomial.

We use Galois theory. Note that any permutation of r_1, r_2, r_3 will leave the value of Δ unchanged (try this). Thus no matter what the Galois group of the given cubic is, we know that the value of Δ is fixed by the entire group, hence Δ lies in the fixed field of the entire group, which is K. So $\Delta \in K$.

Again, we consider what happens to $\sqrt{\Delta} = (r_1 - r_2)(r_1 - r_3)(r_2 - r_3)$. Just like last time, elements of the Galois group can only send $\sqrt{\Delta}$ to $\pm\sqrt{\Delta}$. Assume that the cubic is irreducible for simplicity. Then the Galois group is either isomorphic to A_3 or S_3. Can we tell which is the correct one by using the action on $\sqrt{\Delta}$?

Well notice that performing any odd permutation on r_1, r_2, r_3 will change the sign of $\sqrt{\Delta}$, hence not fixing $\sqrt{\Delta}$. So if the Galois group is S_3 then $\sqrt{\Delta} \notin K$. Also $\sqrt{\Delta}$ is fixed by any even permutation of r_1, r_2, r_3. So if the Galois group is A_4 then $\sqrt{\Delta} \in K$. This gives us a simple criterion for finding the Galois group of an irreducible cubic. Of course knowing the Galois group tells you about the structure of the splitting field so this is quite an achievement. We have done this without even knowing the roots themselves!

Example 9.0.9. To demonstrate the power of our criterion let's find the Galois groups of a few cubics. We work over $\mathbb{Q}$ because there are easy ways to tell apart irreducible polynomials from others (such as Eisenstein's criterion).

Take the cubic $x^3 - 10x + 2$. This is irreducible over $\mathbb{Q}$ by Eisenstein with $p = 2$. Without a general cubic formula we have no hope of solving this cubic (although such a formula exists). However we find it's Galois group by seeing that $\sqrt{\Delta} = \sqrt{3892} \notin \mathbb{Q}$, so $\mathrm{Gal}(x^3 - 10x + 2) \cong S_3$.

The cubic $x^3 - 7x + 7$ is irreducible over $\mathbb{Q}$ by Eisenstein with $p = 7$. We have that $\sqrt{\Delta} = \sqrt{49} = 7 \in \mathbb{Q}$. So $\mathrm{Gal}(f) \cong A_3$.

The case of Galois groups of quartics is a little more complicated. There are other transitive groups besides S_4 and A_4 so we have to invent other objects besides Δ and use their fixing properties to classify Galois groups of irreducible quartics. See Stewart for more details.

One general result reveals itself.

Theorem 9.0.10. *Let p be prime and f be an irreducible polynomial of degree p over $\mathbb{Q}$. If f has exactly two nonreal roots in the splitting field then $Gal(f) \cong S_p$.*

Proof. The fundamental theorem of algebra and the irreducibility of f in characteristic 0 tells us that f has exactly p distinct roots in $\mathbb{C}$. Thus the splitting field L is a subfield of $\mathbb{C}$ of finite degree over $\mathbb{Q}$. The splitting field must strictly contain $\mathbb{R}$ since f has a complex root.

Firstly the Galois group (considered as a subgroup of S_p) must contain a transposition. This comes from the fact that $\mathrm{Gal}(L/\mathbb{R})$ is a subgroup of $\mathrm{Gal}(L/\mathbb{Q})$ and the fact that f has exactly two nonreal roots suggests that $\mathrm{Gal}(L/\mathbb{R}) \cong S_2$.

In order to construct the splitting field we adjoin roots of f to $\mathbb{Q}$. Since f is irreducible we must end up adjoining an element of degree p. Thus $[L : K]$ is divisible by p. But this means that p divides $|\mathrm{Gal}(L/K)| = [L : K]$. Recall Cauchy's theorem on finite groups, that if prime p divides the order of a group then the group contains an element of order p. Thus $\mathrm{Gal}(L/K)$ contains an element of order p in S_p, i.e. a p-cycle.

But S_p can be generated by one transposition and one p-cycle (exercise. Hint: show that you can generate all transpositions). Thus we are done. □

The following example will be important later when we prove that not all quintics can be solved by radicals.

Example 9.0.11. Consider the quintic $f(t) = t^5 - 6t + 3$. This polynomial is irreducible over $\mathbb{Q}$ by Eisenstein with $p = 3$. It also has exactly three real roots (use a bit of analysis; intermediate value theorem and Rolle's theorem). Thus the above theorem tells us that $\mathrm{Gal}(f) \cong S_5$. The fact that the Galois group is S_5 will be important later.

9.1 Solvability by Radicals

When we solve a quadratic over a field K (of characteristic 0) we find that the solutions come neatly packaged to us using the arithmetic of the field $K(\sqrt{b^2 - 4ac})$, this is exactly the splitting field. In other words we get the solutions once we extend K by adjoining the square root of some element of K. We don't just adjoin any old element, it has to be an element of K.

We are interested in solving higher degree polynomials too. When solving a polynomial like $x^7 - 2$ over $\mathbb{Q}$ we find that the solutions come to us once we extend K by adjoining $\sqrt[7]{2}$ and certain 7-th roots of unity (which are each a choice of $\sqrt[7]{-1}$).

In general we make the following definition:

Definition 9.1.1. Let f be a polynomial over K with splitting field L. Then f is *solvable by radicals* if there exists a tower of fields $K = K_0 \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_n$, with $L \subseteq K_n$ and $K_{i+1} = K_i(\alpha_i)$, where α_i is such that $\alpha_i^{n_i} \in K_i$ for some $n_i \in \mathbb{N}$.

This definition may look obscure and convoluted but it really does capture what goes on when we solve polynomials using radical operations. For example we may build the number $\sqrt{3 + \sqrt[3]{5}}$ from $\mathbb{Q}$ by constructing the tower of fields $\mathbb{Q} \subseteq \mathbb{Q}(\sqrt[3]{5}) \subseteq \mathbb{Q}(\sqrt[3]{5}, \sqrt{3 + \sqrt[3]{5}})$. Here $\alpha_1 = \sqrt[3]{5}, n_1 = 3, \alpha_2 = \sqrt{3 + \sqrt[3]{5}}, n_2 = 2$.

The way we are going to study solvability by radicals is to translate the definition into some property of the Galois group. Intuitively here is how we shall think of it. Everytime we make one extension in this "radical tower" we are adjoining an nth root of something, creating a normal extension. Now the Galois groups of such extensions are cyclic.

When we look at the Galois group of the polynomial it is enough to study $\mathrm{Gal}(K_n/K)$. Since the tower of fields exists and the extension K_n/K is Galois, the main correspondence of Galois theory will give us the existence of a chain of normal subgroups of $\mathrm{Gal}(K_n/K)$. Further the cyclic nature of individual extensions in the tower translates into the quotient of consecutive normal subgroups in this chain being cyclic.

Here is the property we are interested in:

Definition 9.1.2. A finite group G is *solvable* if there exists a chain of normal subgroups:

$$\{e\} = G_0 \lhd G_1 \lhd G_2 \lhd \ldots G_n = G$$

such that the quotient G_i/G_{i-1} is cyclic for each $i = 1, 2, \ldots, n$.

Note that in a chain of normal subgroups it doesn't necessarily follow that each group is a normal subgroup of EVERY group to the right, only the next one in the list.

Fortunately our intuitions are correct although difficult to prove rigorously. Galois' main result is the following:

Theorem 9.1.3. *A polynomial f over K (of characteristic 0) is solvable if and only if $Gal(f)$ is a solvable group.*

Proof. Omitted. See Stewart. □

We can use this theorem to prove that there exist polynomials which aren't solvable by radicals.

Corollary 9.1.4. *There exist quintic equations that are not solvable by radicals.*

Proof. Earlier we saw that the quintic $x^5 - 6x + 3$ over $\mathbb{Q}$ has Galois group isomorphic to S_5. However this group is not solvable since it can be checked that A_5 is the only proper normal subgroup of S_5 and this group is not cyclic. (We say that A_5 is a *simple* group, since it has no normal subgroups other than $\{e\}$ and itself.)

Thus this quintic is not solvable by radicals. □

Note that this corollary prevents the existence of a "general quintic equation", unlike the case with quadratics, cubics and quartics. However it does NOT mean that no quintic can be solved by radicals. There are quintics like $x^5 - 1$ that are solvable by radicals.

One good thing about the solvability criterion is that once you have a solvable Galois group you can work backwards, using knowledge of the normal subgroups in order to figure out what the "radical tower" looks like...eventually finding out what form the roots must take. Stewart does this for general polynomials upto degree 4 in his book, deriving formulae similar to the quadratic formula for cubics and quartics.