MA3D5 Galois Theory

Samir Siksek

CHAPTER 1

Introduction

1. Very Brief Orientation

You all know the quadratic formula. Is there a formula for 'solving' cubic equations? This depends on what we mean by 'solving'. Centuries ago when such questions were popular, mathematicians wanted a formula for the solutions that involved only the operations addition, subtraction, multiplication, division and extraction of n-th roots; this is called *solubility by radicals*. The answer is yes for cubic polynomials. The formula is long, but here is an example: the equation

$$x^3 + 3x + 2 = 0$$

has the three solutions

$$\begin{aligned} &\sqrt[3]{-1+\sqrt{2}} + \sqrt[3]{-1-\sqrt{2}}, \\ &\zeta\sqrt[3]{-1+\sqrt{2}} + \zeta^2\sqrt[3]{-1-\sqrt{2}}, \\ &\zeta^2\sqrt[3]{-1+\sqrt{2}} + \zeta\sqrt[3]{-1-\sqrt{2}}, \end{aligned} \tag{1}$$

where $\zeta = \exp(2\pi i/3)$ is a primitive cube root of unity.

The answer is again yes for quartic equations, but no in general for quintic and higher degree equations. For example, the equation

$$x^5 - 6x + 3 = 0$$

is not solvable by radicals.

Galois Theory gives us a machine to answer such questions. Given a polynomial f (with coefficients in $\mathbb{Q}$), Galois Theory gives a field, called the **splitting field** of f which is the smallest field containing all the roots of f. Associated to this **splitting field** is a **Galois group** G, which is a finite group. Galois Theory translates the question: 'is $f = 0$ soluble in radicals?' to the question 'is G a soluble group?', and group theory gives us a way of answering this.

2. Books and Lecture Notes

Derek Holt's lecture notes for this module are great though somewhat concise. The material in my notes is mostly close to Derek's, but the presentation is more detailed.

You might find the following books helpful:

- Ian Stewart, *Galois Theory*.
- D. J. H. Garling, *A Course in Galois Theory*.

There are pleny of online lecture notes, and some of these might suit you, so just google. Here are some that appear to be particularly good.

- Miles Reid, *MA3D5 Galois Theory*. These are Miles' lecture notes from when he taught the module.
- Andrew Baker, *An Introduction to Galois Theory*.
- Keith Conrad has many expository course handouts on various topics in Galois Theory. You might find it helpful to look here if you're stuck on something:
  `http://www.math.uconn.edu/~kconrad/blurbs/`

It's important to realise that the material is pretty standard. So you can't go wrong in picking a book or set of lecture notes to dip in to. What you should be looking for is the book or notes with the presentation that suits your taste!

3. Thanks!

Many thanks to Saul Schleimer and Adam Thomas for suggesting corrections to previous versions of these lecture notes.

CHAPTER 2

Algebra II Revision

You should go through your first and second year algebra lecture notes and revise rings, ideals, the first isomorphism theorem and fields. Here we go quickly through some basic facts.

1. Tests For Irreducibility

THEOREM 1 (Gauss's Lemma). *Let $f \in \mathbb{Z}[x]$ be primitive (i.e. the gcd of all the coefficients is 1). Then f is irreducible in $\mathbb{Q}[x]$ if and only if it is irreducible in $\mathbb{Z}[x]$.*

THEOREM 2 (Eisenstein's Criterion). *Let p be a prime. Let $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ satisfy*

- $p \nmid a_n$;
- $p \mid a_i$ *for* $i = 0, 1, \ldots, n-1$;
- $p^2 \nmid a_0$.

Then f is irreducible in $\mathbb{Q}[x]$.

2. Rings

DEFINITION. Let R be a ring (alway commutative with 1). An ideal I of R is a subset that satisfies the following:

- $0 \in I$,
- if $u, v \in I$ then $u - v \in I$,
- if $x \in R$ and $u \in I$ then $xu \in I$.

Most ideals we will meet in Galois Theory will be principal ideals. Let $w \in R$. The **principal ideal of R generated by w** is

$$(w) = wR = \{wa : a \in R\}.$$

More generally if $w_1, \ldots, w_n \in R$ then the **ideal of R generated by $w_1, \ldots, w_n$** is

$$(w_1, \ldots, w_n) = w_1 R + \cdots + w_n R = \{w_1 a_1 + \cdots + w_n a_n : a_1, \ldots, a_n \in R\}.$$

EXAMPLE 3. In $\mathbb{Z}$, the principal ideal $(2) = 2\mathbb{Z} = \{2a : a \in \mathbb{Z}\}$ is just the even integers.

EXAMPLE 4. Usually we will consider ideals in $K[x]$ where K is a field. The ring $K[x]$ is a principal ideal domain. In fact

$$(f_1, \ldots, f_n) = (f)$$

where $f = \gcd(f_1, \ldots, f_n)$.

DEFINITION. Let R be a ring, I an ideal and $r \in R$. We define the **coset**

$$r + I = \{r + a : a \in I\}.$$

and the **quotient** $R/I = \{r + I : r \in R\}$ to be the set of all cosets of I.

EXERCISE 5.

$$r + I = s + I \iff r - s \in I.$$

PROPOSITION 6. *Let R be a ring and I an ideal. The quotient R/I is a ring with*

- *addition defined by $(r + I) + (s + I) = (r + s) + I$;*
- *multiplication defined by $(r + I)(s + I) = rs + I$;*
- *$0 + I$ is the additive identity;*
- *$1 + I$ is the multiplicative identity.*

PROOF. Either work it out for yourself or revise your Algebra II notes. The main point is to check that the operations are well defined and for this you'll need Exercise 5. □

THEOREM 7 (The First Isomorphism Theorem). *Let $\phi : R \to S$ be a homomorphism of rings. Then*

(1) $\mathrm{Ker}(\phi)$ *is an ideal of R;*
(2) $\mathrm{Im}(\phi)$ *is a subring of S;*
(3) *the map $\hat{\phi} : R/\mathrm{Ker}(\phi) \to \mathrm{Im}(\phi)$ defined by $\hat{\phi}(r + \mathrm{Ker}(\phi)) = \phi(r)$ is a well-defined isomorphism.*

EXAMPLE 8. Define $\phi : \mathbb{R}[x] \to \mathbb{C}$ by $\phi(f) = f(i)$ (the elements of $\mathbb{R}[x]$ are polynomials, and to find the image of a polynomial f just substitute i in it). You can easily check that ϕ is a homomorphism.

Let's show that ϕ is surjective. Let $\alpha \in \mathbb{C}$. We can write $\alpha = a + bi$ where $a, b \in \mathbb{Q}$. Now $\phi(a + bx) = a + bi = \alpha$. So ϕ is surjective.

What's the kernel? Suppose $f \in \mathrm{Ker}(\phi)$. Then $f(i) = 0$. We can write $f = a_n x^n + \cdots + a_0$ where $a_j \in \mathbb{R}$. Thus

$$a_n i^n + a_{n-1} i^{n-1} + \cdots + a_0 = 0.$$

Taking complex conjugates of both sides we have

$$\overline{a_n}\,\overline{i}^n + \overline{a_{n-1}}\,\overline{i}^{n-1} + \cdots + \overline{a_0} = 0.$$

But $\overline{a_j} = a_j$ and $\overline{i} = -i$ so

$$a_n(-i)^n + a_{n-1}(-i)^{n-1} + \cdots + a_0 = 0.$$

In otherwords, $-i$ is a root of f, just as i is a root of f. Hence $x^2 + 1 = (x - i)(x + i)$ is a factor of f. Conversely every multiple of $x^2 + 1$ is in the kernel. So $\mathrm{Ker}(\phi) = (x^2 + 1)$ (the principal ideal generated by $x^2 + 1$). The First Isomorphism Theorem tells us that $\mathbb{R}[x]/(x^2 + 1) \cong \mathbb{C}$ where the isomorphism is given by $f(x) + (x^2 + 1) \mapsto f(i)$.

3. Maximal Ideals

DEFINITION. Let R be a ring. An ideal $I \neq R$ is **maximal** if the only ideals containing it are I and R.

LEMMA 9. *Let K be a field and let $f \in K[x]$ be a non-constant polynomial. Then (f) is a maximal ideal if and only if f is irreducible.*

PROOF. Suppose f is irreducible. Let $I = (f)$; this is an ideal of $K[x]$. Suppose J contains I but is not equal to it. Then there is some $g \in J$ such that $g \notin (f)$. Hence $f \nmid g$. As f is irreducible, the polynomials f and g are coprime. By Euclid's algorithm, there are polynomials h_1, $h_2 \in K[x]$ such that

$$h_1 f + h_2 g = 1.$$

As f, $g \in J$, we have $1 \in J$ so $J = K[x]$.

We leave the converse as an exercise. □

EXAMPLE 10. Let $f = x^2 + 1 \in \mathbb{R}[x]$. The polynomial f is irreducible in $\mathbb{R}[x]$ and so $(f) = \{hf : h \in \mathbb{R}[x]\}$ is maximal.

Now think of f as a polynomial in $\mathbb{C}[x]$. Then $f = (x-i)(x+i)$ and so is not irreducible in $\mathbb{C}[x]$. Consider the ideal $(f) = \{hf : h \in \mathbb{C}[x]\}$. Let

$$J = (x-i) = \{(x-i)h : h \in \mathbb{C}[x]\}.$$

As $(x-i) \mid (x^2+1)$ we have $x^2+1 \in J$. So $(f) \subset J$. Is $J = (f)$? No, for example, every polynomial $g \in (f)$ is a multiple of x^2+1. However the polynomial $x-i \in J$ is not a multiple of x^2+1 and so does not belong to (f). Therefore $J \neq (f)$. Moreover, every element of J is a multiple of $x-i$ and so $1 \notin J$. Hence $J \neq R[x]$. This shows that (f) is not maximal in $\mathbb{C}[x]$.

PROPOSITION 11. *Let R be a ring and $I \neq R$ an ideal. Then R/I is a field if and only if I is maximal.*

PROOF. Either work it out for yourself or revise your Algebra II notes. □

EXAMPLE 12. In Example 8 we saw that $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$, so $\mathbb{R}[x]/(x^2+1)$ is a field, and hence by Proposition 11, the principal ideal (x^2+1) is maximal. We see that this is consistent with Lemma 9 as x^2+1 is irreducible in $\mathbb{R}[x]$.

In $\mathbb{C}[x]$ the polynomial x^2+1 factors as $(x-i)(x+i)$. Hence it is not maximal and the quotient $\mathbb{C}[x]/(x^2+1)$ is not a field. Write $I = (x^2+1)$. The computation

$$((x-i)+I)((x+i)+I) = (x^2+1)+I = 0$$

shows that the ring $\mathbb{C}[x]/(x^2+1)$ contains zero divisors and so is not a field.

CHAPTER 3

Fields and Field Extensions

1. Fields

LEMMA 13. *Let K be a field. Every ideal of K is either 0 or K.*

PROOF. Let $I \subseteq K$ be a non-zero ideal, and let $a \in I$ be a non-zero element. Thus there is some $a^{-1} \in K$ so that $a^{-1}a = 1$. Hence $1 = a^{-1}a \in I$, so $I = K$. □

LEMMA 14. *Let $\phi : K \to L$ be a homomorphism of fields. Then ϕ is injective.*

PROOF. It is sufficient to prove that $\mathrm{Ker}(\phi) = 0$. But $\mathrm{Ker}(\phi)$ is an ideal of K. By Lemma 13, we have $\mathrm{Ker}(\phi) = 0$ or $\mathrm{Ker}(\phi) = K$, so suppose the latter. Then $\phi(1) = 0 \neq 1$ so ϕ is not a homomorphism, giving a contradiction. □

2. Field Extensions

DEFINITION. A **field extension** L/K is a homomorphism $\iota : K \to L$. We think of K as being a **subfield** of L, with the inclusion defined by ι.

EXAMPLE 15. $\mathbb{R}/\mathbb{Q}$ is a field extension. Here the homomorphism $\mathbb{Q} \to \mathbb{R}$ is the obvious inclusion map $a \mapsto a$. Likewise $\mathbb{C}/\mathbb{R}$ and $\mathbb{C}/\mathbb{Q}$ are field extensions.

EXAMPLE 16. Let K be a field. Recall that $K[x]$ is the ring of polynomials in variable x with coefficients in K, and that $K(x)$ is its **field of fractions**, so that elements of $K(x)$ are of the form f/g where $f, g \in K[x]$ and g is not the zero polynomial. Then $K(x)/K$ is a field extension. The field $K(x)$ is called the **field of rational functions over K in variable x**.

3. Field Characteristic

DEFINITION. Let K be a field. We say that K **has characteristic** 0 if for all positive integers n, $n \neq 0$ when viewed as an element of K. In other words, in K,

$$\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} \neq 0,$$

where 1 is the multiplicative identity of K.

Let m be a positive integer. We say that K **has characteristic** m if m is the least positive integer n such that $n = 0$ in K.

EXAMPLE 17. Observe that in $\mathbb{F}_2$, $2 = 0$. So $\mathbb{F}_2$ has characteristic 2.
The fields $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ have characteristic 0.

THEOREM 18. *Let K have characteristic $m > 0$. Then m is a prime.*

PROOF. Suppose that m is composite. Then we can write $m = m_1 m_2$ where m_1, m_2 are integers satisfying $1 < m_i < m$. Now in K, $m_1 m_2 = m = 0$, so $m_1 = 0$ in K or $m_2 = 0$ in K. This contradicts the minimality in the definition of the characteristic m. □

EXAMPLE 19. Let p be a prime. The field $\mathbb{F}_p$ has characteristic p.

THEOREM 20. *Let K be a field. Then K contains either $\mathbb{Q}$, or it contains $\mathbb{F}_p$ for some prime p. More precisely,*

(i) *$\mathbb{Q}$ is a subfield of K if and only if K has characteristic 0;*
(ii) *$\mathbb{F}_p$ is a subfield of K if and only if K has characteristic p.*

PROOF. Easy exercise. □

DEFINITION. Let K be a field. If K contains $\mathbb{Q}$ then we call $\mathbb{Q}$ the **prime subfield** of K. Otherwise K contains $\mathbb{F}_p$ for some prime p and we call this the **prime subfield** of K.

4. Field Generation

DEFINITION. Let K be a field and S be a non-empty subset of K. We define the the **subfield of K generated by S** to be the intersection of all the subfields of K which contain S.

EXAMPLE 21. Let us compute the subfield of $\mathbb{R}$ generated by $\{1\}$. Let L be a subfield of $\mathbb{R}$. From the field axioms we know that $1 \in L$. As fields are closed under addition, subtraction, multiplication and division, we know that L contains

$$\frac{\pm(1+1+1+\cdots+1)}{1+\cdots+1};$$

in other words every subfield L of $\mathbb{R}$ contains $\mathbb{Q}$.

But $\mathbb{Q}$ is a subfield of $\mathbb{R}$ containing $\{1\}$. Thus the intersection of all subfields containing $\{1\}$ is $\mathbb{Q}$. Thus the subfield generated by $\{1\}$ is $\mathbb{Q}$ (take another look at the definition).

EXAMPLE 22. Let $S = \{i\} \subset \mathbb{C}$. We will compute the subfield of $\mathbb{C}$ generated by S. Let L be a subfield containing S. This must contain 1 (as it is a subfield of $\mathbb{C}$) and so contain $\mathbb{Q}$. Thus L contains the set $\mathbb{Q} \cup \{i\}$. This set is not a field. For example, $1, i \in \mathbb{Q} \cup \{i\}$ but $1 + i \notin \mathbb{Q} \cup \{i\}$.

Let $a, b \in \mathbb{Q}$. Then $a, b \in L$ and $i \in L$. Hence $a + bi \in L$. It is now clear that L contains the Gaussian field

$$\mathbb{Q}(i) = \{a + bi : a, b \in \mathbb{Q}\}.$$

But the Gaussian field is a subfield of $\mathbb{C}$ containing S. Thus $\mathbb{Q}(i)$ is the subfield of $\mathbb{C}$ generated by S.

LEMMA 23. *Let K be a field and S a subset such that $S \neq \emptyset$, $S \neq \{0\}$. Let K' be a subfield of K. The following are equivalent:*

(a) *K' is generated by S;*
(b) *K' is the smallest subfield of K containing S;*
(c) *K' is the set of all elements of K that can be obtained from elements of S by a finite sequence of field operations.*

PROOF. Easy exercise. □

DEFINITION. Let L/K be an extension and $A \subset L$. We write $K(A)$ for the subfield of L generated by $K \cup A$, and call this **the field obtained by adjoining** A **to** K.

If $A = \{a_1, \ldots, a_n\}$ then we write $K(a_1, \ldots, a_n)$ for $K(A)$.

EXAMPLE 24. Note that $\mathbb{R}(i) = \mathbb{C}$.

EXAMPLE 25. We will show later that

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

and

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 : a, b, c \in \mathbb{Q}\}.$$

DEFINITION. We say that an extension L/K is **simple** if we can write $L = K(\alpha)$ for some $\alpha \in L$.

EXAMPLE 26. Let $L = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Is $L/\mathbb{Q}$ a simple extension? This means, is there $\alpha \in L$ so that $L = \mathbb{Q}(\alpha)$? We will see that the answer is yes. Specifically, take

$$\alpha = \sqrt{2} + \sqrt{3}.$$

Clearly $\alpha \in L$. Let $M = \mathbb{Q}(\alpha)$. Thus $M \subseteq L$. We want to show that $M = L$. It is enough to show that $\sqrt{2}$ and $\sqrt{3} \in M$. Note

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

So $\sqrt{6} = \frac{1}{2}(\alpha^2 - 5) \in \mathbb{Q}(\alpha) = M$. Hence

$$\alpha\sqrt{6} = \sqrt{2}\sqrt{6} + \sqrt{3}\sqrt{6} = 2\sqrt{3} + 3\sqrt{2} \in M.$$

We have $\alpha = \sqrt{2} + \sqrt{3} \in M$ and $\beta = 3\sqrt{2} + 2\sqrt{3} \in M$. So any linear combination of these with coefficients in $\mathbb{Q}$ will be in M. e.g.

$$\sqrt{2} = \beta - 2\alpha \in M, \qquad \sqrt{3} = 3\alpha - \beta \in M.$$

It follows that $L = M = \mathbb{Q}(\alpha)$ and so $L/\mathbb{Q}$ is a simple extension.

5. Adjoining Roots

Let K be a subfield of $\mathbb{C}$ and let $f \in K[x]$ be a non-constant polynomial with degree n. We know by the Fundamental Theorem of Algebra that f has n roots $\alpha_1, \ldots, \alpha_n$ (counting multiplicities) in $\mathbb{C}$. Taking α to be any of these roots, we can form the extension $K(\alpha)$ which does contain a root of f.

Now if K is an arbitrary field (not necessarily contained in $\mathbb{C}$) and $f \in K[x]$ is a non-constant polynomial, can we find a field extension L/K that contains a root of f? For example, if $K = \mathbb{C}(t)$ (where t is an indeterminant) and $f = x^7 + tx + 1 \in K[x]$, is there an extension L/K that contains a root of f? In this section we answer these questions affirmatively.

PROPOSITION 27 (Adjoining Roots of Irreducible Polynomials). *Let K be a field and let $f \in K[x]$ be an irreducible polynomial. Let $L := K[x]/(f)$. Then*

(I) *L is a field;*
(II) *the map $K \to L$ given by $a \mapsto a + (f)$ is a field extension;*
(III) *the element $x + (f) \in L$ is a root of f;*
(IV) *$L = K(\alpha)$ where $\alpha = x + (f)$.*

PROOF. By Lemma 9, the ideal (f) is maximal. Hence $L = K[x]/(f)$ is a field. This proves (I). Write $I = (f)$. The field operations on L are given by $(g_1 + I) + (g_2 + I) = (g_1 + g_2) + I$ and $(g_1 + I)(g_2 + I) = g_1 g_2 + I$. Hence the map $K \to L$ given by $a \mapsto a + (f)$ is a homomorphism. Therefore it is injective by Lemma 14, and so L/K is a field extension giving (II).

Now write $f = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_0$ with $a_i \in K$. Then

$$f(x+I) = (a_n + I)(x+I)^n + \cdots + (a_0 + I) = (a_n x^n + \cdots + a_0) + I = f + I = 0 + I$$

since $f \in I$. In other words, $f(x+I)$ is the zero element of L and so $x+I \in L$ is a root of f. This proves (III).

To prove (IV), we want to show that every element of L can be written in terms of elements of K and $\alpha = x + I$ using field operations. Any element of $L = K[x]/I$ has the form $g + I$ where $g = b_m x^m + \cdots + b_0 \in K[x]$. So

$$\begin{aligned} g + I &= b_m x^m + \cdots + b_0 + I \\ &= (b_m + I)(x + I)^m + \cdots + (b_0 + I) \\ &= (b_m + I)\alpha^m + \cdots + (b_0 + I) \in K(\alpha). \end{aligned}$$

This completes the proof. □

EXAMPLE 28. Proposition 27 seems quite abstract. Let's see an example to make it more concrete. Let $K = \mathbb{Q}$ and $f = x^2 - 5 \in \mathbb{Q}[x]$. This is an irreducible polynomial. Let $I = (x^2 - 5)$. Then $(x^2 - 5) + I = 0$. So $x^2 + I = 5 + I$. Now let $L = \mathbb{Q}[x]/I$. We regard $\mathbb{Q}$ as a subfield of L by the identification $a \mapsto a + I$. Thus the element $5 + I$ in L is the same as 5 in $\mathbb{Q}$. Now note that $x^2 + I = 5 + I$ can be rewritten as $(x + I)^2 = (5 + I)$, so in L

we have an element $\alpha = x + I$ which is a square-root of 5, and so a root of $x^2 - 5$.

6. Splitting Fields

DEFINITION. Let K be a field, and $f \in K[x]$ be of degree n. Let M be some extension of K such that

$$f = a(x - \alpha_1) \cdots (x - \alpha_n)$$

with the $\alpha_i \in M$. We call $K(\alpha_1, \ldots, \alpha_n)$ the **splitting field** of f over K. The splitting field is the smallest field (inside M) over which f splits as a product of linear factors.

The way we have defined the splitting field of f over K leaves two issues:

- Is there an extension M/K such that f splits completely into linear factors over M?
- Despite calling it **the** splitting field, it appears to depend on M.

These two issues are dealt with below in Theorem 32.

EXAMPLE 29. Let $f = x^4 - 3x^3 + 2x^2$. We can factor $f = x^2(x-1)(x-2)$. Hence the splitting field for f over $\mathbb{Q}$ is $\mathbb{Q}(0,1,2) = \mathbb{Q}$.

EXAMPLE 30. Let $f = x^2 - 2$. The splitting field for f over $\mathbb{Q}$ is $\mathbb{Q}(\sqrt{2}, -\sqrt{2}) = \mathbb{Q}(\sqrt{2})$.

The roots of $g = (x^2+1)(x^2+2x+2)$ are i, $-i$, $1+i$, $1-i$. Thus the splitting field of g over $\mathbb{Q}$ is $\mathbb{Q}(i, -i, 1+i, 1-i) = \mathbb{Q}(i)$.

EXAMPLE 31. Let $f = x^4 - 2$. The roots of f are $\pm\sqrt[4]{2}$, $\pm i\sqrt[4]{2}$. Thus the splitting field of f over $\mathbb{Q}$ is

$$\mathbb{Q}(\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}) = \mathbb{Q}(\sqrt[4]{2}, i).$$

THEOREM 32 (Existence and Uniqueness of Splitting Fields). *Let K be a field and $f \in K[x]$ a polynomial. Then a splitting field L/K for f exists. Moreover, if L_1/K and L_2/K are splitting fields for f then there is a field isomophism $\iota : L_1 \to L_2$ that satisfies $\iota(a) = a$ for all $a \in K$.*

PROOF. The existence proof is easy by induction on f. If f has degree 1 then $f = a(x - \alpha)$ where a and $\alpha \in K$, so the splitting field is $K(\alpha) = K$.

For the inductive step, let f have degree $n \geq 2$. Suppose first that f is irreducible in $K[x]$. By Proposition 27 there is a field $L_1 = K(\alpha_1)$ where α_1 is a root of f in L_1. Thus $f = (x - \alpha_1)g$ where g is a polynomial in $L_1[x]$ of degree $n-1$. Applying the inductive hypothesis, there is an extension L/L_1 which is a splitting field for g. This means that

$$L = L_1(\alpha_2, \ldots, \alpha_n)$$

where

$$g = a(x - \alpha_2) \cdots (x - \alpha_n).$$

Thus

$$f = a(x-\alpha_1)(x-\alpha_2)\cdots(x-\alpha_n)$$

and

$$L = L_1(\alpha_2,\ldots,\alpha_n) = K(\alpha_1)(\alpha_2,\ldots,\alpha_n) = K(\alpha_1,\ldots,\alpha_n).$$

It follows that L/K is a splitting field for $f \in K[x]$.

If f is reducible then we can write $f = gh$ where $g,\ h \in K[x]$ have degree strictly less than n. Thus by the inductive hypothesis there is a splitting field L_1/K for g:

$$L_1 = K(\alpha_1,\ldots,\alpha_{n_1}), \qquad g = a(x-\alpha_1)\cdots(x-\alpha_{n_1}).$$

We regard h as a polynomial with coefficients in $L_1 \supseteq K$. Then h has a splitting field L/L_1:

$$L = L_1(\beta_1,\ldots,\beta_{n_2}), \qquad h = b(x-\beta_1)\cdots(x-\beta_{n_2}).$$

Then

$$f = gh = ab(x-\alpha_1)\cdots(x-\alpha_{n_1})(x-\beta_1)\cdots(x-\beta_{n_2}),$$

and

$$L = L_1(\beta_1,\ldots,\beta_{n_2}) = K(\alpha_1,\ldots,\alpha_{n_1},\beta_1,\ldots,\beta_{n_2}).$$

The extension L/K is therefore a splitting field for f. This completes the existence proof.

The uniqueness part follows from Proposition 86 which will be proved in due course. So we won't worry about that now. □

7. The Degree of An Extension

THEOREM 33. *Let L/K be a field extension. Then L is a vector space over K.*

PROOF. Convince yourself that the vector space axioms are satisfied. □

EXAMPLE 34.

$$\mathbb{C} = \{a+bi \,:\, a,\ b \in \mathbb{R}\}.$$

Thus every element α of $\mathbb{C}$ can be written uniquely in the form $a\cdot 1 + b\cdot i$ where $a,\ b \in \mathbb{R}$. It follows that $1,\ i$ is a basis for $\mathbb{C}$ as a vector space over $\mathbb{R}$.

DEFINITION. Let L/K be a field extension. We define the **degree** of L/K (written as $[L:K]$) to be the dimension of L as a vector space over K. We say that the extension L/K is **finite** if the degree $[L:K]$ is finite (therefore L is a finite-dimensional K-vector space). Otherwise we say that L/K is **infinite**.

EXAMPLE 35. From the previous example, $[\mathbb{C}:\mathbb{R}] = 2$ and so $\mathbb{C}/\mathbb{R}$ is a finite extension.

EXAMPLE 36. Let K be a field and x a variable. We shall argue by contradiction that $K(x)/K$ is an infinite extension. So suppose $[K(x):K]=n$. Consider $1, x, \ldots, x^n$. This is a sequence of $n+1$ elements of $K(x)$. Therefore they must be linearly dependent over K. It follows that there are $a_0, a_1, \ldots, a_n \in K$, not all zero, such that

$$a_0 + a_1 x + \cdots + a_n x^n = 0.$$

Note that this equality is taking place in $K(x)$. But as both sides belong to $K[x]$, it takes place in $K[x]$. This means that $a_0 = a_1 = \cdots = a_n = 0$, contradicting the fact that not all the a_i are zero. It follows that $K(x)/K$ is infinite.

LEMMA 37. *Let K be a finite field. Then its prime subfield is $\mathbb{F}_p$ for some prime p and moreover $\#K = p^n$ where $n = [K:\mathbb{F}_p]$.*

PROOF. As K is finite, K cannot contain $\mathbb{Q}$. By Theorem 20 its prime subfield is $\mathbb{F}_p$ for some prime p. Let $n = [K:\mathbb{F}_p]$. Then K is an n-dimensional vector space over $\mathbb{F}_p$. Let $x_1, \ldots, x_n$ be a basis for $K/\mathbb{F}_p$. Then every element $x \in K$ can be written uniquely as

$$x = a_1 x_1 + a_2 x_2 + \cdots + a_n x_n$$

with $a_i \in \mathbb{F}_p$. Clearly the number of elements $x \in K$ is p^n. □

We see that we can't have a finite field of cardinality 6, 10, 12, 15, 18,....

8. Algebraics and Transcendentals

DEFINITION. Let L/K be a field extension. Let $\alpha \in L$. We say that α is **algebraic** over K if there is a non-zero polynomial $f \in K[x]$ such that $f(\alpha) = 0$. We say that α is **transcendental** over K if it is not algebraic.

The extension L/K is called an **algebraic extension** if every element $\alpha \in L$ is algebraic over K. Otherwise it is called a **transcendental extension**.

EXAMPLE 38. Every complex number is algebraic over $\mathbb{R}$. To see this let $\alpha = a + bi$ where $a, b \in \mathbb{R}$. Observe that $(\alpha - a)^2 = -b^2$. So α is a root of the polynomial

$$f = (x-a)^2 + b^2.$$

The polynomial f is non-zero (it's actually monic) and belongs to $\mathbb{R}[x]$, so α is algebraic over $\mathbb{R}$.

Thus $\mathbb{C}/\mathbb{R}$ is an algebraic extension.

EXAMPLE 39. Let K be a field, and let $K(x)$ be the field of rational functions in variable x over K. The extension $K(x)/K$ is not algebraic. Convince yourself that x is not algebraic over K. It follows that $K(x)/K$ is a simple transcendental extension.

DEFINITION. A number $\alpha \in \mathbb{C}$ is called an **algebraic number** if it is algebraic over $\mathbb{Q}$. This is the same as saying that it is the root of a polynomial with rational coefficients. A number $\alpha \in \mathbb{C}$ is called a **transcendental number** if it is transcendental over $\mathbb{Q}$.

EXAMPLE 40. $\sqrt{2}$ is an algebraic number, as it is a root of x^2-2 which has rational coefficients.

π is a transcendental number. The proof is long-winded, but only uses basic calculus. If you're interested, google it. So $\mathbb{R}/\mathbb{Q}$ is a transcendental extension, as $\mathbb{R}$ contains an element π that is transcendental over $\mathbb{Q}$. Note that $\mathbb{R}$ contains some algebraic elements too, such as $\sqrt{2}$.

EXAMPLE 41. We shall see later that algebraic numbers form a field. For now let $\theta \in \mathbb{C}$ be a root of the irreducible polynomial x^3-2x^2+x+1. We will show that θ^2 is algebraic. Since

$$\theta^3+\theta = 2\theta^2-1$$

squaring both sides we get

$$\theta^6+2\theta^4+\theta^2 = 4\theta^4-4\theta^2+1.$$

Thus

$$\theta^6-2\theta^4+5\theta^2-1=0.$$

It follows that θ^2 is a root of $f=x^3-2x^2+5x-1$, so it is algebraic. How about $\phi=\theta^2-1$? This is a root of

$$g(x)=f(x+1)\in\mathbb{Q}[x]$$

so it is algebraic. What about ϕ/θ? Or $\theta\sqrt{2}$? Or ... It's not trivial to construct polynomials in $\mathbb{Q}[x]$ that have these numbers as roots. One of the things we will do, by studying degrees and the tower law, is to show that such numbers are algebraic without having to construct the polynomials.

THEOREM 42. *If L/K is a finite extension, then it is algebraic.*

PROOF. Suppose L/K is finite of degree $[L:K]=n$. We want to show that every $\alpha\in L$ is algebraic over K. Suppose $\alpha\in L$. Then $1,\alpha,\dots,\alpha^n$ are $n+1$ elements in L which is an n-dimensional vector space over K. It follows that these elements are linearly dependent, so there are $a_0,a_1,\dots,a_n\in K$, not all zero, such that

$$a_0\cdot 1+a_1\cdot\alpha+\cdots+a_n\cdot\alpha^n=0.$$

Let $f(x)=a_0+a_1x+\cdots+a_nx^n$. This is a non-zero element of $K[x]$, and $f(\alpha)=0$. Hence α is algebraic as required. □

EXAMPLE 43. The converse of Theorem 42 is false. We will see conterexamples in due course. One such counterexample is the field extension

$$\mathbb{Q}(\sqrt{2},\sqrt{3},\sqrt{5},\dots)/\mathbb{Q}.$$

The notation means the smallest extension of $\mathbb{Q}$ that contains the square-roots of the prime numbers. This is an example of an algebraic extension that has infinite degree.

9. Minimal Polynomial

DEFINITION. Let L/K be a field extension, and suppose $\alpha \in L$ is algebraic over K. We define the **minimal polynomial** of α over K to be the monic polynomial $m \in K[x]$ of smallest degree such that $m(\alpha) = 0$.

LEMMA 44. *Let L/K be a field extension.*

(i) *If $\alpha \in L$ is algebraic over K then the minimal polynomial exists and is unique.*
(ii) *Moreover, the minimal polynomial m over α is the unique monic irreducible polynomial $m \in K[x]$ satisfying $m(\alpha) = 0$.*
(iii) *If $f \in K[x]$ satisfies $f(\alpha) = 0$ then $m \mid f$.*

Warning: We want m to be irreducible in $K[x]$, not in $L[x]$. In $L[x]$, the polynomial m has the factor $x - \alpha$.

PROOF. As α is algebraic over K, there is certainly a monic polynomial $m \in K[x]$ such that $m(\alpha) = 0$. We want to show that if m is chosen to have minimal degree then m is unique. So suppose that m_1, $m_2 \in K[x]$ are monic and satisfy $m_1(\alpha) = m_2(\alpha) = 0$, and have minimal degree n among polynomials with this property. We want to show that $m_1 = m_2$. Suppose they are not equal. Write

$$m_1 = x^n + a_{n-1}x^{n-1} + \cdots + a_0, \qquad m_2 = x^n + b_{n-1}x^{n-1} + \cdots + b_0$$

where a_i, $b_i \in K$. Then $f = m_1 - m_2$ has degree $< n$, and is non-zero as $m_1 \neq m_2$. Let $c \in K\backslash 0$ be the leading coefficient of f, and let $g = c^{-1}f$. Then g is monic, of degree $< n$ and $g(\alpha) = 0$ as $m_1(\alpha) = m_2(\alpha) = 0$. This contradicts the minimality of n, proving uniqueness.

Let us prove (ii), i.e. irreducibility of the minimal polynomial. Suppose $m \in K[x]$ is monic and satisfies $m(\alpha) = 0$, but that m is reducible in $K[x]$. Then $m = f_1 f_2$ where both f_1, $f_2 \in K[x]$ are monic and with stricly smaller degrees. Then $f_1(\alpha)f_2(\alpha) = f(\alpha) = 0$. Thus $f_1(\alpha) = 0$ or $f_2(\alpha) = 0$, and we contradict the fact that the degree of f is minimal.

For (iii), suppose $f \in K[x]$ and $f(\alpha) = 0$. Then, by the Division Algorithm,

$$f = qm + r$$

where q, $r \in K[x]$ and $\deg(r) < \deg(m)$. But $f(\alpha) = 0$, $m(\alpha) = 0$ so $r(\alpha) = 0$. If r is not the zero polynomial, then by dividing by its leading coefficient we can make it monic, and we have a contradiction. So $r = 0$. Hence $m \mid f$. □

10. Conjugates

DEFINITION. Let K be a field and α be algebraic over K. Let $m \in K[x]$ be the minimal polynomial of α over K. The K-conjugates of α are the roots of m in any splitting field.

EXAMPLE 45. The minimal polynomial of $\sqrt{-2}$ over $\mathbb{Q}$ is x^2+2. So the $\mathbb{Q}$-conjugates of $\sqrt{-2}$ are $\sqrt{-2}$ and $-\sqrt{-2}$.

Let $K = \mathbb{Q}(\sqrt[4]{-2})$. Then $\sqrt{-2} \in K$. So the minimal polynomial of $\sqrt{-2}$ over K is $x - \sqrt{-2}$. The only K-conjugate of $\sqrt{-2}$ is $\sqrt{-2}$.

EXAMPLE 46. The $\mathbb{Q}$-conjugates of $\sqrt[3]{2}$ are $\sqrt[3]{2}, \zeta\sqrt[3]{2}$ and $\zeta^2\sqrt[3]{2}$ where ζ is a primitive cube root of 1.

EXAMPLE 47. Let ζ be a primitive p-th root of unity, where p is a prime. Then ζ is a root of $x^p - 1$. The polynomial $x^p - 1$ is reducible over $\mathbb{Q}$,

$$x^p - 1 = (x-1)(x^{p-1} + x^{p-2} + \cdots + 1).$$

Thus $x^p - 1$ is not the minimal polynomial of ζ. Now ζ must be a root of the second factor $x^{p-1} + x^{p-2} + \cdots + 1$. We know from Algebra II that this polynomial is irreducible over $\mathbb{Q}$. Thus it is the minimal polynomial for ζ. The roots of $x^p - 1$ are $1, \zeta, \ldots, \zeta^{p-1}$. Therefore the roots of $x^{p-1} + x^{p-2} + \cdots + 1$ are $\zeta, \ldots, \zeta^{p-1}$. Hence the $\mathbb{Q}$-conjugates of ζ are $\zeta, \ldots, \zeta^{p-1}$.

EXAMPLE 48. Recall from Algebra 2 that in $\mathbb{F}_p[x, y]$,

$$(x+y)^p = x^p + y^p. \tag{2}$$

Why? Actually by the binomial theorem,

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

But it is easy to convince yourself that $p \mid \binom{p}{k}$ for $1 \le k \le p-1$, giving (2).

Let p be an odd prime. Let $K = \mathbb{F}_p(t)$ where t is a variable over $\mathbb{F}_p$. Let $f = x^p - t \in K[x]$. This is an irreducible polynomial—if you don't know how to prove this, ask the TAs during the support class! Now observe that

$$(x - \sqrt[p]{t})^p = x^p - t = f$$

by (2). It follows that the splitting field of f is $L = K(\sqrt[p]{t})$ and the only K-conjugate of $\sqrt[p]{t}$ is $\sqrt[p]{t}$.

11. Simple Extensions Again

PROPOSITION 49. *Let α be algebraic over K with minimal polynomial $m \in K[x]$. Let (m) be the principal ideal in $K[x]$ generated by m. Then the map*

$$\hat{\phi} : K[x]/(m) \to K(\alpha), \qquad \hat{\phi}(f + (m)) = f(\alpha)$$

is an isomorphism.

PROOF. You should compare this to the proof of Proposition 27.

Let $\phi : K[x] \to K(\alpha)$ be given by $\phi(f) = f(\alpha)$. This is clearly a ring homomorphism. We will use the First Isomorphism Theorem. Observe that $f \in \mathrm{Ker}(\phi)$ iff $f(\alpha) = 0$ iff $m \mid f$. Therefore $\mathrm{Ker}(\phi) = (m)$ (the principal ideal generated by m). As m is irreducible, the ideal (m) is maximal (Lemma 9) and so $K[x]/(m)$ is a field (Proposition 11). By the First Isomorphism Theorem, the map

$$\hat{\phi} : K[x]/(m) \to \mathrm{Im}(\phi), \qquad \hat{\phi}(f + (m)) = \phi(f) = f(\alpha)$$

is a well-defined isomorphism. It remains to show that $\mathrm{Im}(\phi) = K(\alpha)$. As $K[x]/(m)$ is a field, its isomorphic image $\mathrm{Im}(\phi)$ is also a field. But $\mathrm{Im}(\phi) \supseteq K$ since for every $a \in K$, we have $\phi(a) = a$, and also $\phi(x) = \alpha$ so $\alpha \in \mathrm{Im}(\phi)$. Hence $K \cup \{\alpha\}$ is contained in the field $\mathrm{Im}(\phi) \subseteq K(\alpha)$. So $\mathrm{Im}(\phi) = K(\alpha)$. □

THEOREM 50. *Let L/K be a field extension and let $\alpha \in L$ be algebraic over K. Suppose that the minimal polynomial m of α over K has degree d. Then*

(i) $K(\alpha) = \{a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1} : a_0, \ldots, a_{d-1} \in K\}$.
(ii) *A basis for $K(\alpha)$ over K is $1, \alpha, \ldots, \alpha^{d-1}$. In particular, $[K(\alpha) : K] = d$.*

PROOF. By Proposition 49, every element of $K(\alpha)$ has the form $f(\alpha)$ where $f \in K[x]$. By the division algorithm $f = qm + r$ where $q, r \in K[x]$ with $0 \le \deg(r) \le d - 1$. We can write $r = a_0 + a_1 x + \cdots + a_{d-1}x^{d-1}$ with $a_i \in K$. Thus every element of $K(\alpha)$ has the form

$$\begin{aligned} f(\alpha) &= q(\alpha)m(\alpha) + r(\alpha) \\ &= r(\alpha) \qquad \text{as } m(\alpha) = 0 \\ &= a_0 + a_1\alpha + \cdots + a_{d-1}\alpha^{d-1}. \end{aligned}$$

This proves (i).

For (ii) it is clear that every element of $K(\alpha)$ is a linear combination of $1, \alpha, \ldots, \alpha^{d-1}$ over K. We must show that this set is linearly independent. Suppose there are $b_0, \ldots, b_{d-1} \in K$ such that $b_0 + b_1\alpha + \cdots + b_{d-1}\alpha^{d-1} = 0$. Let $g = b_0 + b_1 x + \cdots + b_{d-1}x^{d-1}$. Then $g \in K[x]$ satisfies $g(\alpha) = 0$ and $\deg(g) \le d - 1 < \deg(m)$. As m is the minimal polynomial, this is only possible if g is the zero polynomial, so $b_0 = b_1 = \cdots = b_{d-1} = 0$ proving linear independence. □

EXAMPLE 51. We continue Example 25. Observe that $x^2 - 2$ is the minimal polynomial for $\sqrt{2}$ over $\mathbb{Q}$ (it's monic, $\sqrt{2}$ is a root, and it's irreducible by Eisenstein's Criterion). Thus by Theorem 50, $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \deg(x^2 - 2) = 2$ and

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}.$$

Likewise $x^3 - 2$ is the minimal polynomial for $\sqrt[3]{2}$ over $\mathbb{Q}$. Thus $[\mathbb{Q}(\sqrt[3]{2} : \mathbb{Q}] = 3$ and

$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{2}^2 \ : \ a, b, c \in \mathbb{Q}\}.$$

CHAPTER 4

The Tower Law

THEOREM 52. *Let $K \subseteq L \subseteq M$ be field extensions of finite degree (or we could write $M/L/K$). Let $\ell_1, \ell_2, \ldots, \ell_r$ be a basis for L/K and $m_1, \ldots, m_s$ be a basis for M/L. Then*

$$\{\ell_i m_j : i = 1, \ldots, r,\ j = 1, \ldots, s\} \tag{3}$$

is a basis for M/K. Moreover,

$$[M : K] = [M : L] \cdot [L : K]. \tag{4}$$

PROOF. Observe that

$$[L : K] = r < \infty \qquad [M : L] = s < \infty.$$

Suppose for the moment that (3) is a basis for M/K as claimed in the statement of the theorem. Then $[M : K] = rs = [M : L] \cdot [L : K]$ proving (4). Thus all we need to do is prove that (3) is indeed a basis for M/K.

Let us show first that (3) is linearly independent over K. Thus suppose $a_{ij} \in K$ such that

$$\sum_{j=1}^{s} \sum_{i=1}^{r} a_{ij} \ell_i m_j = 0.$$

We can rewrite this as

$$\sum_{j=1}^{s} (\sum_{i=1}^{r} a_{ij} \ell_i) m_j.$$

Let $b_j = \sum_{i=1}^{r} a_{ij} \ell_i$ for $j = 1, \ldots, s$. Since $a_{ij} \in K \subseteq L$ and $\ell_i \in L$ we see that $b_j \in L$. But

$$\sum_{j=1}^{s} b_j m_j = 0.$$

As $m_1, \ldots, m_s$ is a basis for M/L we have

$$b_1 = b_2 = \cdots = b_s = 0.$$

But

$$b_j = \sum_{i=1}^{r} a_{ij} \ell_i = 0, \qquad j = 1, \ldots, s.$$

As $\ell_1, \ldots, \ell_r$ is a basis for L/K and $a_{ij} \in K$ we have $a_{ij} = 0$ for $j = 1, \ldots, s$ and $i = 1, \ldots, r$. This proves that (3) is linearly independent.

Now we show (3) spans M as a vector space over K. Let $m \in M$. As $m_1, \ldots, m_s$ is a basis for M/L, we can write

$$m = b_1 m_1 + \cdots + b_s m_s$$

for some $b_1, \ldots, b_s \in L$. Moreover, as $\ell_1, \ldots, \ell_r$ is a basis for L/K we can express each of the bs as a linear combination of the ℓs with coefficients in K:

$$b_j = a_{1j}\ell_1 + \cdots + a_{rj}\ell_r, \qquad j = 1, \ldots, s;$$

here $a_{ij} \in K$. Thus

$$m = \sum_{j=1}^{s} b_j m_j = \sum_{j=1}^{s} (a_{1j}\ell_1 + \cdots + a_{rj}\ell_r) m_j = \sum_{j=1}^{s} \sum_{i=1}^{r} a_{ij}\ell_i m_j .$$

We've shown that any $m \in M$ can be written as linear combination of $\ell_i m_j$ with coefficients in K. This completes the proof. □

1. Extended Example $\mathbb{Q}(\sqrt{5}, \sqrt{6})$

We shall evaluate $[\mathbb{Q}(\sqrt{5}, \sqrt{6}) : \mathbb{Q}]$. Write $L = \mathbb{Q}(\sqrt{5})$, $M = \mathbb{Q}(\sqrt{5}, \sqrt{6}) = L(\sqrt{6})$. By the tower law,

$$[M : \mathbb{Q}] = [L : \mathbb{Q}][M : L] .$$

The polynomial $x^2 - 5$ is monic, irreducible over $\mathbb{Q}$ and has $\sqrt{5}$ as a root. Therefore it is the minimal polynomial for $\sqrt{5}$ over $\mathbb{Q}$. By Theorem 50, we have 1, $\sqrt{5}$ is a $\mathbb{Q}$-basis for L over $\mathbb{Q}$. In particular, $[L : \mathbb{Q}] = 2$. We want to compute $[M : L]$. As $M = L(\sqrt{6})$, we need a minimal polynomial for $\sqrt{6}$ over L. Now $\sqrt{6}$ is a root of $x^2 - 6$. We want to know if $x^2 - 6$ is irreducible over $L = \mathbb{Q}(\sqrt{5})$. Suppose it isn't. Then, as it is quadratic, its roots must be contained in L. So $\sqrt{6} = a + b\sqrt{5}$ for some $a, b \in \mathbb{Q}$. Squaring both sides, and rearranging, we get

$$(a^2 + 5b^2 - 6) + 2ab\sqrt{5} = 0.$$

As 1, $\sqrt{5}$ are linearly independent over $\mathbb{Q}$,

$$a^2 + 5b^2 - 6 = 2ab = 0.$$

Thus either $a = 0$, $b = \sqrt{\frac{6}{5}}$ or $b = 0$, $a = \sqrt{6}$, in either case contradicting a, $b \in \mathbb{Q}$. Hence $\sqrt{6} \notin L$, and $x^2 - 6$ is irreducible over L. It follows that $x^2 - 6$ is the minimal polynomial for $\sqrt{6}$ over L. Hence $[M : L] = 2$ and so by the tower law, $[M : \mathbb{Q}] = 2 \times 2 = 4$.

We can also write a $\mathbb{Q}$-basis for $M = \mathbb{Q}(\sqrt{5}, \sqrt{6})$ over $\mathbb{Q}$. By the above 1, $\sqrt{5}$ is a basis for L over $\mathbb{Q}$. Also, as $x^2 - 6$ is the minimal polynomial for $\sqrt{6}$ over L, we have (Theorem 50) that 1, $\sqrt{6}$ is a basis for $L(\sqrt{6}) = M$ over L. The tower law (Theorem 52) tells us

$$1,\ \sqrt{5},\ \sqrt{6},\ \sqrt{30}$$

is a basis for M over $\mathbb{Q}$.

We'll go a little further with the example, and in fact show that $M = \mathbb{Q}(\sqrt{5} + \sqrt{6})$ (thus M is a simple extension of $\mathbb{Q}$). Let $\alpha = \sqrt{5} + \sqrt{6}$. Since $\alpha \in M$ it follows that $\mathbb{Q}(\alpha) \subseteq M$. To show $M = \mathbb{Q}(\alpha)$ it is enough to show

that $\mathbb{Q}(\alpha) \supseteq M$. For this it is enough to show that $\sqrt{5} \in \mathbb{Q}(\alpha)$ and $\sqrt{6} \in \mathbb{Q}(\alpha)$. Note that

$$(\alpha - \sqrt{5})^2 = 6,$$

which gives

$$\alpha^2 + 5 - 2\sqrt{5}\alpha = 6. \tag{5}$$

Rearranging

$$\sqrt{5} = \frac{\alpha^2 - 1}{2} \in \mathbb{Q}(\alpha).$$

Similarly $\sqrt{6} \in \mathbb{Q}(\alpha)$ as required. Hence $M = \mathbb{Q}(\alpha)$.

Finally, we will write down a minimal polynomial m for α over $\mathbb{Q}$. Since $M/\mathbb{Q}$ has degree 4, we know from (iii) that we are looking for a monic polynomial of degree 4. Rearranging (5) we have $\alpha^2 - 1 = 2\sqrt{5}\alpha$. Squaring both sides and rearranging, we see that α is the root of

$$f = x^4 - 22x^2 + 1.$$

Do we have to check if f is irreducible? Normally we do, but not here. Observe that $m \mid f$ (as $f(\alpha) = 0$) and they both have degree 4. So $m = f$.

2. Another Extended Example

In this example we will compute the degree of the splitting field of $f = x^3 - 5$ over $\mathbb{Q}$. The splitting field of f over $\mathbb{Q}$ is the field we obtain by adjoining to $\mathbb{Q}$ all the roots of f. The three roots of f are

$$\theta_1 = \sqrt[3]{5}, \qquad \theta_2 = \zeta\sqrt[3]{5}, \qquad \theta_3 = \zeta^2\sqrt[3]{5},$$

where ζ is a primitive cube root of 1. The splitting field is therefore $\mathbb{Q}(\theta_1, \theta_2, \theta_3)$.

Let

$$K = \mathbb{Q}(\theta_1), \qquad L = K(\theta_2) = \mathbb{Q}(\theta_1, \theta_2), \qquad M = L(\theta_3) = \mathbb{Q}(\theta_1, \theta_2, \theta_3).$$

By the tower law

$$[M : \mathbb{Q}] = [K : \mathbb{Q}][L : K][M : L].$$

As $x^3 - 5$ is irreducible over $\mathbb{Q}$, we have $[K : \mathbb{Q}] = 3$. To calculate $[L : K]$ we need to know the degree of the minimal polynomial of θ_2 over K. Note that θ_2 is a root of $f = x^3 - 5$. However, f is not the minimal polynomial of θ_2 over K. Indeed, as $\sqrt[3]{5} \in K$, we have

$$f = (x - \sqrt[3]{5}) \cdot g$$

where $g \in K[x]$ is monic and quadratic. Thus θ_2 is a root of g. Is g reducible over K? As g is quadratic, if it is reducible over K it would mean that $\theta_2 \in K$. However, $\theta_2 = \zeta\sqrt[3]{5} \notin \mathbb{R}$ and $K = \mathbb{Q}(\sqrt[3]{5}) \subset \mathbb{R}$. Therefore $\theta_2 \notin K$, and so g is irreducible over K. It follows that g is the minimal polynomial of θ_2 over K. Hence $[L : K] = 2$.

Finally, we want $[M : L]$. Now, θ_3 is also a root of g. As g is quadratic and has one root in L (specifically θ_2) its other root must be in L. Thus

$\theta_3 \in L$, and so $M = L(\theta_3) = L$, and hence $[M : L] = 1$. Hence $[M : \mathbb{Q}] = 3 \times 2 \times 1 = 6$.

3. Field of Algebraic Numbers

LEMMA 53. *Let L/K be a field extension. Let $\alpha, \beta \in L$ be algebraic over K. Then $\alpha \pm \beta$, $\alpha \cdot \beta$ and α/β are algebraic over K (the last one provided $\beta \neq 0$ of course).*

PROOF. Observe that $\alpha \pm \beta$, $\alpha \cdot \beta$, α/β all belong to $K(\alpha, \beta)$. By Theorem 42 we only have to prove that $K(\alpha, \beta)/K$ is a finite extension. By the tower law

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

where $L = K(\alpha)$. Let m_α and $m_\beta \in K[x]$ be the minimal polynomials of α and β over K. We know that $[L : K] = \deg(m_\alpha)$ is finite. Note that $K \subset L$ so $m_\beta \in L(x)$ and $m_\beta(\beta) = 0$. Thus β is algebraic over L. We do not know if m_β is the minimal polynomial of β over L, since we do not know it is irreducible over L. Let $m'_\beta \in L(x)$ be the minimal polynomial for β over L. Then $m'_\beta \mid m_\beta$. So

$$[L(\beta) : L] = \deg(m'_\beta) \leq \deg(m_\beta) < \infty.$$

By the tower law we know that $[K(\alpha, \beta) : K]$ is finite, so $K(\alpha, \beta)$ is algebraic over K. □

EXAMPLE 54. Let

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

By the above lemma it is easy to check that $\overline{\mathbb{Q}}$ is a field. It is called the **field of algebraic numbers**, and also the **algebraic closure of** $\mathbb{Q}$.

EXERCISE 55. Show that $\overline{\mathbb{Q}}/\mathbb{Q}$ is an infinite algebraic extension.

CHAPTER 5

Normal Extensions

DEFINITION. Let L/K be an algebraic extension. We say that L/K is **normal**, if for every irreducible polynomial $f \in K[x]$, if f has a root in L then it splits completely into linear factors in $L[x]$ (so all its roots will belong to L).

An equivalent formulation of this definition is the following: L/K is **normal** if for all $\alpha \in L$, the minimal polynomial $m_\alpha \in K[x]$ has all its roots in L.

EXAMPLE 56. Let $d \in \mathbb{Q}$ be a non-square. We shall show that $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is normal. Every $\alpha \in \mathbb{Q}(\sqrt{d})$ can be written as $\alpha = a + b\sqrt{d}$ with $a, b \in \mathbb{Q}$. Thus α is a root of the polynomial $f = (x-a)^2 - db^2 \in \mathbb{Q}[x]$. The minimal polynomial $m_\alpha \in \mathbb{Q}[x]$ must divide f. However both roots of f belong to $\mathbb{Q}(\sqrt{d})$; these are $\alpha = a + b\sqrt{d}$ and $a - b\sqrt{d}$. So all roots of m_α belong to $\mathbb{Q}(\sqrt{d})$. Thus $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ is normal.

EXAMPLE 57. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not normal. The polynomial $x^3 - 2$ is irreducible over $\mathbb{Q}$ but has exactly one root in $\mathbb{Q}(\sqrt[3]{2})$ and two other roots not in $\mathbb{Q}(\sqrt[3]{2})$ since they are not real. Likewise $K = \mathbb{Q}(\sqrt{2}, \sqrt[3]{2})$ is not normal for the same reason.

EXAMPLE 58. Let $L = \mathbb{Q}(i, \sqrt[3]{2})$. We will show that $L/\mathbb{Q}$ is not normal. This is a little harder than the previous example as $L \not\subset \mathbb{R}$ and so we can't use the same argument. Suppose $L/\mathbb{Q}$ is normal. As $x^3 - 2$ is irreducible over $\mathbb{Q}$ and has a root $\sqrt[3]{2} \in L$, the other two roots $\zeta\sqrt[3]{2}$ and $\zeta^2\sqrt[3]{2}$ belong to L. In particular, $\zeta = \zeta\sqrt[3]{2}/\sqrt[3]{2} \in L$. Let $M = \mathbb{Q}(\sqrt[3]{2})$. Then $[M : \mathbb{Q}] = 3$, and as $i \notin M \subset \mathbb{R}$ and i is a root of $x^2 + 1 \in M[x]$ we have $[L : M] = 2$. Thus $\zeta = a + bi$ where $a, b \in M$. But $\zeta = \exp(2\pi i/3) = -1/2 + \sqrt{3}i/2$. Comparing real and imaginary parts we have $b = \sqrt{3}/2$. Thus $\sqrt{3} \in M$. This is impossible as $[M : \mathbb{Q}] = 3$ and $[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = 2 \nmid 3$. It follows that $L/\mathbb{Q}$ is not normal and so not Galois.

THEOREM 59. *Let L/K be a finite normal extension. Then L is the splitting field of some polynomial $f \in K[x]$.*

PROOF. Let $\alpha_1, \ldots, \alpha_n$ be a K-basis for L and $m_i \in K[x]$ be the minimal polynomial of α_i. Let $f = m_1 m_2 \cdots m_n \in K[x]$. Let M be the splitting field of f. As the extension L/K is normal, every root of m_i belongs to L and so every root of f belongs to L thus $M \subseteq L$. However, since M contains $\alpha_1, \ldots, \alpha_n$ we have $L \subseteq M$. Thus $L = M$ is the splitting field of f. □

The converse of this theorem is also true, but much harder, and will be proved later.

CHAPTER 6

Separability

DEFINITION. A polynomial $f \in K[x]$ is **separable over** K if it does not have repeated roots in its splitting field, otherwise we say it is **inseparable over** K.

EXAMPLE 60. The polynomial $(x-1)(x^2+1) \in \mathbb{Q}[x]$ has distinct roots 1, i, $-i$ in its splitting field $\mathbb{Q}(i)$. Therefore it is separable over $\mathbb{Q}$. The polynomial $f = (x-1)(x^2+1)^2 \in \mathbb{Q}[x]$ has repeated roots i, $-i$ in its splitting field so is inseparable.

EXAMPLE 61. Now let p be a prime, $K = \mathbb{F}_p(t)$ and $g = x^p - t \in K[x]$. We saw in Examples 48 and 77 before that g is irreducible over K (and therefore squarefree as an element of $K[x]$), that its splitting field is $K(\sqrt[p]{t})$ and that $g = (x - \sqrt[p]{t})^p$. Hence the irreducible polynomial g has precisely one root $\sqrt[p]{t}$ repeated p times. It follows that g is inseparable over K.

DEFINITION. Let L/K be an algebraic extension. We say that $\alpha \in L$ is **separable** over K if its minimal polynomial is separable. We say that L/K is a **separable extension** if every $\alpha \in L$ is separable over K.

EXAMPLE 62. We continue Example 61 Let $K = \mathbb{F}_p(t)$ and $L = K(\sqrt[p]{t})$. Then $\sqrt[p]{t}$ has minimal polynomial $x^p - t$ over K, which is inseparable. Hence $\sqrt[p]{t}$ is inseparable over K, and so L/K is an inseparable extension.

EXAMPLE 63. In this example we shall show that $\mathbb{C}/\mathbb{R}$ is a separable extension. Let $\alpha \in \mathbb{C}$, and suppose that it is inseparable over $\mathbb{R}$. Let $m \in \mathbb{R}[x]$ be the minimal polynomial of α. Then m has repeated roots in $\mathbb{C}$. As $[\mathbb{C} : \mathbb{R}] = 2$, we see that $\deg(m) = 1$ or 2. If $\deg(m) = 1$ then m has no repeated roots. So $\deg(m) = 2$. It follows that α must have multiplicity 2 as a root of m, and there are no other roots. As m is monic,

$$m = (x-\alpha)^2 = x^2 - 2\alpha x + \alpha^2.$$

But $m \in \mathbb{R}[x]$. So $-2\alpha = a \in \mathbb{R}$. Hence $\alpha = -a/2 \in \mathbb{R}$. It follows that m is reducible in $\mathbb{R}[x]$ giving a contradiction. Hence $\mathbb{C}/\mathbb{R}$ is separable.

Now let L/K be any extension of degree 2. If you look carefully at the above proof, you will find that most of it continues to hold with $\mathbb{R}$ replaced by K and $\mathbb{C}$ replaced by L. The only place where things might go wrong is when we arrive at $-2\alpha = a \in K$ and we want to deduce that $\alpha = -a/2 \in K$. Can we divide by 2? If the characteristic of K is not 2 then we can, and the proof works, and we deduce that L/K is separable. If

the characteristic of K is 2, then $2 = 0$ in K and so we can't divide by 2. The proof fails, and we can't deduce separability of L/K. For example, if $K = \mathbb{F}_2(t)$ and $L = K(\sqrt{t})$, then L/K is a degree 2 inseparable extension.

DEFINITION. Let K be a field. Let $f = a_n x^n + \cdots + a_0 \in K[x]$. Define the **formal derivative of** f to be

$$Df = na_n x^{n-1} + \cdots + 2a_2 x + a_1 \in K[x].$$

EXAMPLE 64. It is important to note that the formal derivative of a non-contant polynomial can be zero if you're working over fields of positive characteristic. For example, if p is a prime then $D(x^p+1) = px^{p-1} = 0$ in $\mathbb{F}_p[x]$.

LEMMA 65. *Let $f, g \in K[x]$ and $a \in K$. Then*

(a) $D(f+g) = Df + Dg$,
(b) $D(af) = aDf$,
(c) $D(fg) = fDg + gDf$.

PROOF. These are easy consequences of the definition. □

LEMMA 66. *Suppose L/K is a field extension, and $f, g \in K[x]$. Then*

$$\gcd(f,g) = 1 \text{ in } K[x] \iff \gcd(f,g) = 1 \text{ in } L[x].$$

PROOF. This follows from Euclid's algorithm, which computes the GCD without asking whether the coefficients of the polynomials are in K or L! □

LEMMA 67. *Let $f \in K[x]$ and L be its splitting field. Then f has repeated roots in L if and only if* $\gcd(f, Df) \neq 1$.

PROOF. Suppose f has a repeated root $\alpha \in L$. Then $f = (x-\alpha)^2 g$ where $g \in L[x]$. Note

$$D(f) = 2(x-\alpha)g + (x-\alpha)^2 Dg.$$

In particular $x - \alpha$ divides both f and Df and so $\gcd(f, Df) \neq 1$.

Now suppose $\gcd(f, Df) \neq 1$. Then f, Df have a common root in L. There is no loss of generality in assuming that f is monic. We can write

$$f = (x-\alpha_1)\cdots(x-\alpha_n), \qquad \alpha_i \in L.$$

By reordering the α_i we may suppose that α_1 is the common root of f and Df. Now, by the product rule

$$Df = (x-\alpha_2)\cdots(x-\alpha_n) + (x-\alpha_1)(x-\alpha_3)\cdots(x-\alpha_n) + \cdots.$$

All the summands are divisible by $x - \alpha_1$ except the first one. So

$$0 = Df(\alpha_1) = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3)\cdots(\alpha_1 - \alpha_n).$$

It follows that $\alpha_1 = \alpha_i$ for some $i > 1$, so f has repeated roots. □

LEMMA 68. *Let K has characteristic* 0. *Let $f \in K[x]$ be an irreducible polynomial. Then f is separable.*

PROOF. We may by scaling suppose that f is monic. Suppose f is inseparable. Then f has a repeated root in its splitting field. By Lemma 67 we have $\gcd(f, Df) \neq 1$. Let $g = \gcd(f, Df)$. But $g \in K[x]$, and $g \mid f$. As f is irreducible and $g \neq 1$ we have $g = f$. Hence $\gcd(f, Df) = f$. So $f \mid Df$. But $\deg(Df) < \deg(f)$, so $Df = 0$. Now write

$$f = x^n + a_{n-1}x^{n-1} + \cdots + a_0.$$

Then

$$Df = nx^{n-1} + \cdots.$$

As the characteristic of K is 0, we have $n \neq 0$ in K and so $Df \neq 0$ giving a contradiction. □

LEMMA 69. *Suppose that K has characteristic 0. Let L/K be an algebraic extension. Then L/K is a separable extension.*

PROOF. Let $\alpha \in L$ and let m be its minimal polynomial over K. By Lemma 68 we know that m is separable. Therefore L/K is separable. □

EXAMPLE 70. Observe that we've only seen one example of an inseparable extension: $K(\sqrt[p]{t})/K$ where p is a prime and $K = \mathbb{F}_p(t)$ (Example 62). Note that the characteristic of K is p so this doesn't contradict the lemma.

CHAPTER 7

Automorphism Groups

1. Field Automorphisms

DEFINITION. Let L be a field. An **automorphism** of L is an isomorphism σ from L to itself. Let L/K be a field extension. An **automorphism** of L/K (also called a K**-automorphism of** L) is an automorphism σ of L that satisfies $\sigma(a) = a$ for all $a \in K$.

EXAMPLE 71. In this example we shall compute the automorphisms of $\mathbb{C}/\mathbb{R}$. Let σ be such an automorphism. Every $\alpha \in \mathbb{C}$ can be written as $\alpha = a + bi$ where $a, b \in \mathbb{R}$. Hence

$$\sigma(\alpha) = \sigma(a + bi) = \sigma(a) + \sigma(b)\sigma(i) = a + b\sigma(i)$$

as $a, b \in \mathbb{R}$. Thus to know σ all we need to know is $\sigma(i)$. Now

$$\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$$

as $-1 \in \mathbb{R}$. Thus $\sigma(i) = \pm i$. If $\sigma(i) = i$, then $\sigma(\alpha) = \alpha$ for all $\alpha \in \mathbb{C}$, so σ is the identity map $\mathbb{C} \to \mathbb{C}$. If $\sigma(i) = -i$, then $\sigma(\alpha) = \overline{\alpha}$, so σ is complex conjugation $\mathbb{C} \to \mathbb{C}$. Thus there are precisely two $\mathbb{R}$-automorphisms of $\mathbb{C}$.

EXAMPLE 72. We shall compute all automorphisms of $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. A $\mathbb{Q}$-basis for $\mathbb{Q}(\sqrt[3]{2})$ is 1, $\sqrt[3]{2}$, $\sqrt[3]{2}^2$ (why?). Thus every $\alpha \in \mathbb{Q}(\sqrt[3]{2})$ can be expressed uniquely as

$$\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{2}^2$$

where $a, b, c \in \mathbb{Q}$. Let σ be a $\mathbb{Q}$-automorphism of $\mathbb{Q}(\sqrt[3]{2})$. Thus $\sigma(a) = a$, $\sigma(b) = b$, $\sigma(c) = c$, and so

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

Thus α is determined by $\sigma\left(\sqrt[3]{2}\right)$. However,

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

Thus

$$\sigma\left(\sqrt[3]{2}\right) = \sqrt[3]{2}, \qquad \zeta\sqrt[3]{2}, \text{or} \qquad \zeta^2\sqrt[3]{2},$$

where ζ is a primitive cube root of unity. But σ is an automorphism from $\mathbb{Q}(\sqrt[3]{2})$ to itself, and thus $\sigma\left(\sqrt[3]{2}\right) \in \mathbb{Q}(\sqrt[3]{2})$. However, $\mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$, and $\zeta\sqrt[3]{2} \notin \mathbb{R}$, $\zeta^2\sqrt[3]{2} \notin \mathbb{R}$. Hence $\sigma\left(\sqrt[3]{2}\right) = \sqrt[3]{2}$. So $\sigma(\alpha) = \alpha$ for all $\alpha \in \mathbb{Q}(\sqrt[3]{2})$. It follows that the only automorphism of $\mathbb{Q}(\sqrt[3]{2})$ is the identity $1 : \mathbb{Q}(\sqrt[3]{2}) \to \mathbb{Q}(\sqrt[3]{2})$.

LEMMA 73. *Let L/K be a field extension. Let $\alpha \in L$ be algebraic and $f \in K[x]$ satisfy $f(\alpha) = 0$. Let $\sigma \in \mathrm{Aut}(L/K)$. Then $f(\sigma(\alpha)) = 0$. In particular, $\sigma(\alpha)$ is a K-conjugate of α.*

PROOF. Let $f = a_0 + a_1 x + \cdots + a_n x^n$ with $a_i \in K$. Then $\sigma(f(\alpha)) = \sigma(0) = 0$. However,

$$\begin{aligned} 0 = \sigma(f(\alpha)) &= \sigma(a_0 + a_1\alpha + \cdots + a_n\alpha^n) \\ &= \sigma(a_0) + \sigma(a_1)\sigma(\alpha) + \cdots + \sigma(a_n)\sigma(\alpha)^n \qquad \text{as } \sigma \text{ is an isomorphism} \\ &= a_0 + a_1\sigma(\alpha) + \cdots + a_n\sigma(\alpha)^n \qquad \text{as } \sigma \text{ is a } K\text{-automorphism} \\ &= f(\sigma(\alpha)). \end{aligned}$$

Now suppose let $f = m \in K[x]$ be the minimal polynomial of α. Then $\sigma(\alpha)$ is a root of m and therefore one of the K-conjugates of α. □

THEOREM 74. *Let L/K be an extension. Let $\mathrm{Aut}(L/K)$ be the set of K-automorphisms of L. Then $\mathrm{Aut}(L/K)$ is a group with respect to composition of maps. Moreover, if L/K is finite, then $\mathrm{Aut}(L/K)$ is finite.*

We call $\mathrm{Aut}(L/K)$ the **automorphism group of** L/K.

EXAMPLE 75. In Example 71 we saw that

$$\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{1, \tau\}$$

where $1 : \mathbb{C} \to \mathbb{C}$ is the identity map, and $\tau : \mathbb{C} \to \mathbb{C}$ is complex conjugation. If $\alpha \in \mathbb{C}$, then

$$\tau^2(\alpha) = \tau(\tau(\alpha)) = \overline{\overline{\alpha}} = \alpha,$$

so $\tau^2 = 1$ (the identity map). It is clear that $\mathrm{Aut}(\mathbb{C}/\mathbb{R})$ is cyclic of order 2.

EXAMPLE 76. From Example 72

$$\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{1\}$$

which is the trivial group.

PROOF OF THEOREM 74. Let L/K be an extension. The proof that $\mathrm{Aut}(L/K)$ is a group under composition is an easy exercise.

Suppose L/K is finite. We want to show that $\mathrm{Aut}(L/K)$ is finite. Let $\sigma \in \mathrm{Aut}(L/K)$ and let $\alpha \in L$. Let $[L : K] = n$. Then L has a K-basis $\alpha_1, \ldots, \alpha_n$. Every $\alpha \in L$ can be written uniquely as a linear combination

$$\alpha = a_1\alpha_1 + \cdots + a_n\alpha_n$$

with $a_i \in K$. Then

$$\sigma(\alpha) = a_1\sigma(\alpha_1) + \cdots + a_n\sigma(\alpha_n)$$

as σ is a K-automorphism. It follows that σ is determined by the values of $\sigma(\alpha_1), \ldots, \sigma(\alpha_n)$. As L/K is finite, it is algebraic. By Lemma 73, $\sigma(\alpha_i)$ is K-conjugate of α_i. Each α_i has finitely many K-conjugates (as they're all roots of the minimal polynomial of α_i). So the possibilities for each $\sigma(\alpha_i)$ is finite. Thus the number of possibilities for σ is finite. Hence $\mathrm{Aut}(L/K)$ is finite. □

EXAMPLE 77. This example is a continuation of Example 48. In that example we let p be an odd prime, $K = \mathbb{F}_p(t)$ where t is an indeterminate of $\mathbb{F}_p$ (i.e. a variable), and let $L = K(\sqrt[p]{t})$. We found that the minimal polynomial of $\sqrt[p]{t}$ is

$$x^p - t = (x - \sqrt[p]{t})^p.$$

Thus the only K-conjugate of $\sqrt[p]{t}$ is itself. In this example, $[L : K] = p$. However, $\mathrm{Aut}(L/K) = 1$. Why? Because an automorphism σ of L/K is determined by $\sigma(\sqrt[p]{t})$. This has to be a K-conjugate of $\sqrt[p]{t}$. Thus $\sigma(\sqrt[p]{t}) = \sqrt[p]{t}$), so $\mathrm{Aut}(L/K) = 1$.

2. The Frobenius Automorphism for Finite Fields

Recall by Lemma 37, a finite field K has cardinality p^n for some prime p, and prime subfield $\mathbb{F}_p$.

LEMMA 78. *Let K be a finite field having $q = p^n$ elements where p is prime. Then $\alpha^q = \alpha$ for all α in K.*

PROOF. Let K be a field with q elements. Then K^* is a group with order $q-1$. Hence every $\alpha \in K^*$ satisfies $\alpha^{q-1} = 1$, and so $\alpha^q = \alpha$. But 0 also satisfies $\alpha^q = \alpha$, so all α in K satisfy it. □

LEMMA 79. *Let K be a field of size p^n. Let $\phi : K \to K$ be given by $\phi(\alpha) = \alpha^p$. Then ϕ is an automorphism of $K/\mathbb{F}_p$. Moreover, it has order n in* $\mathrm{Aut}(K/\mathbb{F}_p)$.

We call ϕ the **Frobenius automorphism**.

PROOF. Note that $\phi(\alpha\beta) = \phi(\alpha)\phi(\beta)$ and $\phi(\alpha^{-1}) = \phi(\alpha)^{-1}$. Moreover, since K has characteristic p,

$$(\alpha + \beta)^p = \alpha^p + \beta^p,$$

thus $\phi(\alpha+\beta) = \phi(\alpha)+\phi(\beta)$. Hence ϕ is a field homomorphism. By Lemma 14, the map ϕ is injective. As K is finite, it must be surjective as well so ϕ is an isomorphism. Since $\#\mathbb{F}_p = p$, it follows from Lemma 78 that $\alpha^p = \alpha$ for all $\alpha \in \mathbb{F}_p$. Thus $\phi(\alpha) = \alpha$. This completes the proof that ϕ is an automorphism of $K/\mathbb{F}_p$.

We now want to show that ϕ has order n. Write $q = p^n$. For $\alpha \in K$ note that $\phi^n(\alpha) = \alpha^q$. By Lemma 78, we have $\phi^n(\alpha) = \alpha$ for all $\alpha \in K$. Thus $\phi^n = 1$ in $\mathrm{Aut}(K/\mathbb{F}_p)$. Suppose ϕ has order m. Then $m \mid n$. Moreover, every α in K satisfies $\alpha^{p^m} = \phi^m(\alpha) = \alpha$. Thus every $\alpha \in K$ is a root of the polynomial $f = X^{p^m} - X$. The number of distinct elements of K is p^n, and the number of distinct roots of f is $\leq \deg(f) = p^m$. Thus $n \leq m$. But $m \mid n$ so $n = m$ is the order of ϕ. □

3. Linear Independence of Automorphisms

LEMMA 80. *Let $\sigma_1, \ldots, \sigma_m$ be distinct automorphisms of a field L. Then $\sigma_1, \ldots, \sigma_m$ are linearly independent over L: if $a_1, \ldots, a_m \in L$ satisfy*

$$a_1\sigma_1(x) + \cdots + a_m\sigma_m(x) = 0 \text{ for all } x \in L$$

then $a_1 = a_2 = \cdots = a_m = 0$.

PROOF. The proof is by induction on m. Suppose $m = 1$. Then $a_1\sigma_1(x) = 0$ for all $x \in L$. As σ_1 is an automorphism, $\sigma_1(1) = 1$. Letting $x = 1$ we have $a_1 = 0$, which proves the statement for $m = 1$.

Suppose now that the statement is true for $m = k \geq 1$. Suppose that $a_1, \ldots, a_{k+1} \in L$ such that

$$a_1\sigma_1(x) + \cdots + a_{k+1}\sigma_{k+1}(x) = 0 \quad \text{for all } x \in L. \tag{6}$$

We may assume that all $a_i \neq 0$ (otherwise we can apply the inductive hypothesis). Now the σ_i are distinct. So there is some $\alpha \in L$ such that $\sigma_1(\alpha) \neq \sigma_{k+1}(\alpha)$. Replacing x by αx in (6) we have

$$a_1\sigma_1(\alpha)\sigma_1(x) + \cdots + a_{k+1}\sigma_{k+1}(\alpha)\sigma_{k+1}(x) = 0 \quad \text{for all } x \in L. \tag{7}$$

Multiplying (6) by $\sigma_1(\alpha)$ and subtracting from (7) we have

$$a_2(\sigma_2(\alpha) - \sigma_1(\alpha))\sigma_2(x) + \cdots + a_{k+1}(\sigma_{k+1}(\alpha) - \sigma_1(\alpha))\sigma_{k+1}(x) = 0$$

for all $x \in L$. Now we have only k automorphisms, so by the inductive hypothesis

$$a_2(\sigma_2(\alpha) - \sigma_1(\alpha)) = \cdots = a_{k+1}(\sigma_{k+1}(\alpha) - \sigma_1(\alpha)) = 0.$$

This gives a contradiction as $a_{k+1} \neq 0$ and $\sigma_{k+1}(\alpha) \neq \sigma_1(\alpha)$. □

The following theorem improves on Theorem 74.

THEOREM 81. *Let L/K be a finite extension. Then*

$$\#\mathrm{Aut}(L/K) \leq [L : K].$$

PROOF. Let $\sigma_1, \ldots, \sigma_m$ be the distinct K-automorphisms of L. Let $\alpha_1, \ldots, \alpha_n$ be a K-basis for L. Then $m = \#\mathrm{Aut}(L/K)$, and $n = [L : K]$. We want to show that $m \leq n$. Suppose $m > n$. We will contradict Lemma 80 by showing the existence of $y_1, \ldots, y_m \in L$, not all zero, such that

$$y_1\sigma_1(x) + \cdots + y_m\sigma_m(x) = 0, \quad \text{for all } x \in L. \tag{8}$$

Consider the following system of equations

$$y_1\sigma_1(\alpha_1) + y_2\sigma_2(\alpha_1) + \cdots + y_m\sigma_m(\alpha_1) = 0 \tag{9}$$

$$y_1\sigma_1(\alpha_2) + y_2\sigma_2(\alpha_2) + \cdots + y_m\sigma_m(\alpha_2) = 0 \tag{10}$$

$$\vdots \qquad \vdots$$

$$y_1\sigma_1(\alpha_n) + y_2\sigma_2(\alpha_n) + \cdots + y_m\sigma_m(\alpha_n) = 0 \tag{11}$$

This is a homogeneous system of n linear equations in m unknowns with coefficients in L. As $m > n$ there is a non-trivial solution $y_1, y_2, \ldots, y_m \in L$ (of course non-trivial means that not all y_i are zero). Now let $y_1, y_2, \ldots, y_m \in L$ be this non-trivial solution. Let $x \in L$. As $\alpha_1, \ldots, \alpha_n$ is a K-basis for L, there are $a_1, \ldots, a_n \in K$ such that

$$x = a_1\alpha_1 + \cdots + a_n\alpha_n.$$

As the σ_i are K-automorphisms of L we have,

$$\sigma_i(x) = a_1\sigma_i(\alpha_1) + \cdots + a_n\sigma_i(\alpha_n).$$

Now multiplying (9) by a_1, (10) by a_2, ..., (11) by a_n and adding we deduce (8), giving us a contradiction. □

4. Building-Up Automorphism Groups I

LEMMA 82. *Let α, β be algebraic over K having the same minimal polynomial $m \in K[x]$. Then there is an isomorphism*

$$\sigma : K(\alpha) \to K(\beta)$$

that satisfies $\sigma(\alpha) = \beta$, and $\sigma(a) = a$ for all $a \in K$.

PROOF. We apply Proposition 49. Thus we have isomorphisms

$$\phi_1 : K[x]/(m) \to K(\alpha), \qquad \phi_1(f + (m)) = f(\alpha),$$

and

$$\phi_2 : K[x]/(m) \to K(\beta), \qquad \phi_2(f + (m)) = f(\beta).$$

Let $\sigma = \phi_2 \circ \phi_1^{-1} : K(\alpha) \to K(\beta)$. Now $\phi_1(x + (m)) = \alpha$, $\phi_2(x + (m)) = \beta$. So $\sigma(\alpha) = \beta$. Also, if $a \in K$, let $f = a \in K[x]$, then $\phi_1(a + (m)) = a$ and $\phi_2(a + (m)) = a$, so $\sigma(a) = a$. □

EXAMPLE 83. Let $L = \mathbb{Q}(\sqrt{7})$. Then $\sqrt{7}$ and $-\sqrt{7}$ have the same minimal polynomial over $\mathbb{Q}$, which is $x^2 - 7$. Hence by Lemma 82 we have an isomorphism $\sigma : \mathbb{Q}(\sqrt{7}) \to \mathbb{Q}(\sqrt{7})$ that satisfies $\sigma(\sqrt{7}) = -\sqrt{7}$ and $\sigma(a) = a$ for $a \in \mathbb{Q}$. It follows that σ is a $\mathbb{Q}$-automorphism of L, and it is given by

$$\sigma(a + b\sqrt{7}) = a - b\sqrt{7}, \qquad a, b \in \mathbb{Q}.$$

Thus we have found two elements of $\mathrm{Aut}(L/\mathbb{Q})$ which are 1 (the identity) and σ. But by Theorem 81, we know that $\#\mathrm{Aut}(L/\mathbb{Q}) \leq [L : \mathbb{Q}] = 2$ so we have found all elements of $\mathrm{Aut}(L/\mathbb{Q})$:

$$\mathrm{Aut}(L/\mathbb{Q}) = \{1, \sigma\}$$

which is cyclic of order 2.

EXAMPLE 84. Let p, q be distinct primes and $L = \mathbb{Q}(\sqrt{p}, \sqrt{q})$. We will write down some automorphisms of L. Suppose σ is a $\mathbb{Q}$-automorphism

of L. Then σ is determined by $\sigma(\sqrt{p})$ and $\sigma(\sqrt{q})$, which must be conjugates of $\sqrt{p}$, $\sqrt{q}$. There are four possibilities:

$$\begin{cases}\sigma_1(\sqrt{p})=\sqrt{p},\\ \sigma_1(\sqrt{q})=\sqrt{q},\end{cases}\quad\begin{cases}\sigma_2(\sqrt{p})=-\sqrt{p},\\ \sigma_2(\sqrt{q})=\sqrt{q},\end{cases}\quad\begin{cases}\sigma_3(\sqrt{p})=\sqrt{p},\\ \sigma_3(\sqrt{q})=-\sqrt{q},\end{cases}\quad\begin{cases}\sigma_4(\sqrt{p})=-\sqrt{p},\\ \sigma_4(\sqrt{q})=-\sqrt{q}.\end{cases}$$

Do all these give us $\mathbb{Q}$-automorphisms of L? In the homework you saw that $L/\mathbb{Q}$ has degree 4 with basis 1, $\sqrt{p}$, $\sqrt{q}$, $\sqrt{pq}$. For example, if $\sigma=\sigma_2$ then

$$\sigma(a+b\sqrt{p}+c\sqrt{q}+d\sqrt{pq})=a-b\sqrt{p}+c\sqrt{q}-d\sqrt{pq},\qquad a,b,c,d\in\mathbb{Q}.$$

You can probably check by brute force that $\sigma: L\to L$ is an isomorphism. Here we shall see a slicker way.

In the homework you checked that $\sqrt{p}$ has minimal polynomial x^2-p over $K=\mathbb{Q}(\sqrt{q})$. Hence there is a K-automorphism σ of L that satisfies $\sigma(\sqrt{p})=-\sqrt{p}$. Note that $\sigma(\sqrt{q})=\sqrt{q}$ as $\sqrt{q}\in K$. Thus $\sigma=\sigma_2$ is an automorphism of L/K. As it fixes every element of K and $K\supset\mathbb{Q}$ it fixes every element of $\mathbb{Q}$, and $\sigma_2\in\mathrm{Aut}(L/\mathbb{Q})$. By symmetry, $\sigma_3\in\mathrm{Aut}(L/\mathbb{Q})$. What about σ_4? Actually, $\sigma_4=\sigma_2\sigma_3$ so it is an automorphism. Hence $\mathrm{Aut}(L/\mathbb{Q})=\{1,\sigma_2,\sigma_3,\sigma_4\}$. This is isomorphic to $C_2\times C_2$.

5. Building-Up Automorphism Groups II

We now prove a generalization of Lemma 82. Let $\phi: K_1\to K_2$ be a homomorphism of fields. We also denote by $\phi: K_1[x]\to K_2[x]$ the map $\phi(a_nx^n+\cdots+a_0)=\phi(a_n)x^n+\cdots+\phi(a_0)$. It is an easy exercise to show that $\phi: K_1[x]\to K_2[x]$ is a homomorphism of rings, and that if $\phi: K_1\to K_2$ is an isomorphism, then so is $\phi: K_1[x]\to K_2[x]$.

LEMMA 85. *Let $\phi: K_1\to K_2$ be an isomorphism of fields. Let α be algebraic over K_1 with minimal polynomial $m\in K_1[x]$, and suppose β is algebraic over K_2 with minimal polynomial $\phi(m)$. Then there is a field isomorphism $\psi: K_1(\alpha)\to K_2(\beta)$ such that $\psi(\alpha)=\beta$ and $\psi(a)=\phi(a)$ for all $a\in K_1$.*

PROOF. As α is algebraic over K_1, every element of $K_1(\alpha)$ can be written as a polynomial in α with coefficients in K_1. Define $\psi: K_1(\alpha)\to K_2(\beta)$ by

$$\psi(f(\alpha))=\phi(f)(\beta),\qquad f\in K_1[x].$$

We first check that ψ is well-defined. Suppose that f, $g\in K_1[x]$ satisfying $f(\alpha)=g(\alpha)$. As m is the minimal polynomial of α, we have $m\mid(f-g)$ and so $\phi(m)\mid(\phi(f)-\phi(g))$. As β is a root of $\phi(m)$ we have $\phi(f)(\beta)=\phi(g)(\beta)$. So ψ is well-defined. It is easy to see that ψ is a homomorphism satisfying $\psi(\alpha)=\beta$ and $\psi(a)=\phi(a)$ for all $a\in K$. As with any homomorphism of fields, ψ must be injective. The surjectivity is easy to check from the definition and the fact that $\phi: K_1\to K_2$ is an isomomorphism. □

PROPOSITION 86. *Let $\phi : K_1 \to K_2$ be an isomorphism of fields. Let $f_1 \in K_1[x]$ and $f_2 = \phi(f_1) \in K_2[x]$. Let L_1, L_2 be the splitting fields of f_1, f_2 respectively. Then there is a field isomorphism $\psi : L_1 \to L_2$ with $\psi(a) = \phi(a)$ for all $a \in K_1$.*

PROOF. We shall use induction on $n = \deg(f_1) = \deg(f_2)$. If $n = 1$, then $L_1 = K_1$, $L_2 = K_2$, and we let $\psi = \phi$.

Suppose now that $n \geq 2$. Let g be an irreducible factor of f_1. Since $\phi : K_1[x] \to K_2[x]$ is an isomorphism, $\phi(g)$ is an irreducible factor of f_2. We may write

$$L_1 = K_1(\alpha_1, \ldots, \alpha_n), \qquad L_2 = K_2(\beta_1, \ldots, \beta_n)$$

where the α_i are roots of f_1 and the β_i are the roots of f_2. By reordering, we may assume that α_1 is a root of g and β_1 is a root of $\phi(g)$. By the previous lemma, there is an isomorphism $\phi' : K_1(\alpha_1) \to K_2(\beta_1)$ such that $\phi'(\alpha_1) = \beta_1$ and $\phi'(a) = \phi(a)$ for all $a \in K_1$.

As α_1 is a root of f_1 we can write $f_1 = (x - \alpha_1)h_1$ where $h_1 \in K_1(\alpha_1)[x]$. Similarly $f_2 = (x - \beta_1)h_2$ where $h_2 \in K_2(\beta_1)[x]$. Now

$$(x - \beta_1)h_2 = \phi'(f_1) = \phi'((x - \alpha_1)h_1) = (x - \beta_1)\phi'(h_1)$$

so $\phi'(h_1) = h_2$. Moreover, L_1, L_2 are respectively splitting fields for h_1, h_2 over $K_1(\alpha_1)$, $K_2(\beta_1)$. It follows by the inductive hypothesis that there is an isomorphism $\psi : L_1 \to L_2$ such that $\psi(a) = \phi'(a)$ for all $a \in K_1(\alpha_1)$. Hence if $a \in K_1$, then $\psi(a) = \phi'(a) = \phi(a)$, as required. □

COROLLARY 87. *Let $f \in K[x]$, and let g be an irreducible factor of f. Let L be the splitting field of f, and let $\alpha, \beta \in L$ be two roots of g. Then there is a $\psi \in \mathrm{Aut}(L/K)$ such that $\psi(\alpha) = \beta$.*

PROOF. As g is irreducible, it is the minimal polynomial of α, β. By Lemma 82, there is an isomorphism $\phi : K(\alpha) \to K(\beta)$ such that $\phi(\alpha) = \beta$ and $\phi(a) = a$ for all $a \in K$.

Now L is the splitting field of f over $K(\alpha)$ and over $K(\beta)$. Moreover, $\phi(f) = f$. Applying Proposition 86, we have that there is an isomorphism $\psi : L \to L$ such that $\psi(a) = \phi(a)$ for all $a \in K(\alpha)$. Hence $\psi(a) = \phi(a) = a$ for all $a \in K$. It follows that $\psi \in \mathrm{Aut}(L/K)$. Moreover, $\psi(\alpha) = \phi(\alpha) = \beta$. □

6. The Automorphism Group of a Cyclotomic Field

Let p be a prime and let $\zeta = \exp(2\pi i/p)$. We know that ζ is a p-th root of unity, and hence algebraic. The field $\mathbb{Q}(\zeta)$ is called the p-th cyclotomic field. In this example we will compute $\mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q})$.

Recall that the p-th roots of unity are $1, \zeta, \zeta^2, \ldots, \zeta^{p-1}$. These are the root of $x^p - 1$. This factors over $\mathbb{Q}$ into

$$x^p - 1 = (x - 1)(x^{p-1} + x^{p-2} + \cdots + 1).$$

The second factor $f = x^{p-1} + x^{p-2} + \cdots + 1$ is irreducible (see the section on Eisenstein's criterion in your Algebra II notes). Its roots are $\zeta, \ldots, \zeta^{p-1}$.

Thus $[\mathbb{Q}(\zeta):\mathbb{Q}] = \deg(f) = p-1$. Moreover, the splitting field of f is

$$\mathbb{Q}(\zeta,\dots,\zeta^{p-1}) = \mathbb{Q}(\zeta).$$

Now from Corollary 87 (applied to $f = g$) we have that for any $1 \le a \le p-1$, there is an automorphism $\sigma_a \in \mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q})$ such that $\sigma_a(\zeta) = \zeta^a$. This gives $p-1$ distinct elements $\sigma_1,\dots,\sigma_{p-1}$ of $\mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q})$. From Theorem 81 we know that $\#\mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q}) \le p-1$. Thus $\#\mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q}) = p-1$ and

$$\mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \{\sigma_1,\dots,\sigma_{p-1}\}.$$

The above lists the elements of $\mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q})$ but doesn't tell us much about the group structure. What is $\sigma_a\sigma_b$? Note that

$$(\sigma_a\sigma_b)(\zeta) = \sigma_a(\sigma_b(\zeta)) = \sigma_a(\zeta^b) = \sigma_a(\zeta)^b = \zeta^{ab}.$$

Notice that the exponents only matter modulo p as ζ has order p. Hence if $1 \le c \le p-1$ and $c \equiv ab \pmod{p}$, then $\sigma_a\sigma_b = \sigma_c$. It follows that we have an isomorphism,

$$\phi : (\mathbb{Z}/p\mathbb{Z})^* \to \mathrm{Aut}(\mathbb{Q}(\zeta)/\mathbb{Q}), \qquad \phi(\overline{a}) = \sigma_a.$$

CHAPTER 8

Fixed Fields

1. Fixed Fields

DEFINITION. Let L/K be a field extension and H a subgroup of $\mathrm{Aut}(L/K)$. Let

$$L^H = \{\alpha \in L : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}.$$

LEMMA 88. *Let L/K be a field extension and H a subgroup of* $\mathrm{Aut}(L/K)$. *Then L^H is a subfield of L containing K.*

L^H is called the **fixed field** of H.

PROOF. Suppose $a \in K$ and $\sigma \in H$. As H is contained in $\mathrm{Aut}(L/K)$, σ is a K-automorphism and so $\sigma(a) = a$. Hence $a \in L^H$. It follows that $K \subseteq L^H$. In particular, L^H contains 0, 1. To show that L^H is a subfield of L we must show that it is closed under field operations.

Suppose α, $\beta \in L^H$. By definition, for any $\sigma \in H$, we have $\sigma(\alpha) = \alpha$, $\sigma(\beta) = \beta$. As any such σ is contained in $\mathrm{Aut}(L/K)$ and therefore an isomorphism of fields, $\sigma(\alpha+\beta) = \sigma(\alpha) + \sigma(\beta) = \alpha + \beta$. Hence $\alpha + \beta \in L^H$. It follows that L^H is closed under addition and similarly it is closed under the other field operations. Therefore L^H is a subfield of L. □

EXAMPLE 89. This is a continuation of Example 83. We let $L = \mathbb{Q}(\sqrt{7})$, and found that

$$\mathrm{Aut}(L/\mathbb{Q}) = \{1, \sigma\}$$

where

$$\sigma(a + b\sqrt{7}) = a - b\sqrt{7}, \qquad a, b \in \mathbb{Q}.$$

Let's calculate $L^{\mathrm{Aut}(L/\mathbb{Q})}$. Let $\alpha \in L$. Then $\alpha \in L^{\mathrm{Aut}(L/\mathbb{Q})}$ if and only if $1(\alpha) = \alpha$ and $\sigma(\alpha) = \alpha$. Writing $\alpha = a + b\sqrt{7}$ with a, $b \in \mathbb{Q}$ we see that $\alpha \in L^{\mathrm{Aut}(L/\mathbb{Q})}$ if and only if $b = 0$, so $L^{\mathrm{Aut}(L/\mathbb{Q})} = \mathbb{Q}$.

EXAMPLE 90. This is a continuation of Example 84, where p, q are distinct primes and $L = \mathbb{Q}(\sqrt{p}, \sqrt{q})$. We found that $\mathrm{Aut}(L/\mathbb{Q}) = \{1, \sigma_2, \sigma_3, \sigma_4\}$, which is isomorphic to $C_2 \times C_2$.

Let $H = \{1, \sigma_4\} = \langle \sigma_4 \rangle$. This is a subgroup of $\mathrm{Aut}(L/\mathbb{Q})$ of order 2. Let's work out L^H. Every $\alpha \in L$ can be written uniquely as

$$\alpha = a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq}, \qquad a, b, c, d \in \mathbb{Q}.$$

Now $\alpha \in L^H$ if and only if $1(\alpha) = \alpha$ and $\sigma_4(\alpha) = \alpha$. The condition $1(\alpha) = \alpha$ always holds. The condition $\sigma_4(\alpha) = \alpha$ gives

$$a - b\sqrt{p} - c\sqrt{q} + d\sqrt{pq} = a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq}$$

and therefore,

$$2b\sqrt{p}+2c\sqrt{q}=0.$$

Since $\sqrt{p}$ and $\sqrt{q}$ are linearly independent over $\mathbb{Q}$ we conclude that $2b=2c=0$ and so $b=c=0$. Hence

$$L^H=\{a+d\sqrt{pq}\,:\,a,d\in\mathbb{Q}\}=\mathbb{Q}(\sqrt{pq}).$$

2. Fixed Fields II

LEMMA 91. *Let A be a matrix, and let B be obtained from A by permuting its rows. Then A and B have the same kernel.*

PROOF. Think about it. □

Let n be a positive integer. Let

$$\mathbf{x}=\begin{pmatrix}x_1\\x_2\\\vdots\\x_n\end{pmatrix}\in L^n$$

and $\sigma\in\mathrm{Aut}(L)$. We will write

$$\sigma(\mathbf{x})=\begin{pmatrix}\sigma(x_1)\\\sigma(x_2)\\\vdots\\\sigma(x_n).\end{pmatrix}.$$

LEMMA 92. *Let L be a field and H a subgroup of $\mathrm{Aut}(L)$. Write $F=L^H$. Let V be a non-trivial L-subspace of L^n. Suppose for every $\sigma\in H$ and every $\mathbf{x}\in V$ we have $\sigma(\mathbf{x})\in V$ (we say that V is **stable** under H). Then V contains a non-zero vector $\mathbf{y}$ that belongs to F^n.*

PROOF. As V is non-trivial it contains a non-zero vector $\mathbf{x}$. We choose $\mathbf{x}$ so that it has the least possible number of non-zero entries. By permuting the coordinate vectors we may suppose that

$$\mathbf{x}=\begin{pmatrix}x_1\\x_2\\\vdots\\x_r\\0\\\vdots\\0\end{pmatrix}$$

where $x_1,\dots,x_r \in L$ are non-zero and r is minimal. Now let $\mathbf{y} = (1/x_r)\mathbf{x}$. As $\mathbf{x} \in V$ and V is an L-subspace, we have $\mathbf{y} \in V$. We can write

$$\mathbf{y} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_{r-1} \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}.$$

We claim that $\sigma(\mathbf{y}) = \mathbf{y}$ for all $\sigma \in H$. Suppose otherwise. Thus there is a $\sigma \in H$ such that $\sigma(\mathbf{y}) \neq \mathbf{y}$. As V is stable under H, we have $\sigma(\mathbf{y}) \in V$. Let $\mathbf{z} = \sigma(\mathbf{y}) - \mathbf{y}$. This is an element of V, it is non-zero as $\sigma(\mathbf{y}) \neq \mathbf{y}$, and

$$\mathbf{z} = \begin{pmatrix} \sigma(y_1) - y_1 \\ \sigma(y_2) - y_2 \\ \vdots \\ \sigma(y_{r-1}) - y_{r-1} \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix},$$

which contradicts the minimality of r. This proves our claim: $\sigma(\mathbf{y}) = \mathbf{y}$ for all $\sigma \in H$. Thus $\sigma(y_i) = y_i$ for all $\sigma \in H$ and so $y_i \in L^H = F$. Hence $\mathbf{y} \in F^n$ as required. □

Theorem 81 says that if L/K is a finite extension, then $\#\mathrm{Aut}(L/K) \leq [L:K]$. Here we prove an inequality that is in the opposite direction.

LEMMA 93. *Let L be a field and let H be a finite subgroup of its automorphism group* $\mathrm{Aut}(L)$. *Let $F = L^H$. Then*

$$[L:F] \leq \#H.$$

In particular $[L:F]$ is finite.

PROOF. Let $m = \#H$ and write $H = \{\sigma_1,\dots,\sigma_m\}$. Recall the familiar fact that $\sigma\sigma_1,\dots,\sigma\sigma_m$ is a permutation of $\sigma_1,\dots,\sigma_m$ for any $\sigma \in H$. Let $\alpha_1,\dots,\alpha_n$ be a F-linearly independent subset of L. Consider the $m \times n$ matrix

$$A = \begin{pmatrix} \sigma_1(\alpha_1) & \sigma_1(\alpha_2) & \cdots & \sigma_1(\alpha_n) \\ \sigma_2(\alpha_1) & \sigma_2(\alpha_2) & \cdots & \sigma_2(\alpha_n) \\ \vdots & \vdots & & \vdots \\ \sigma_m(\alpha_1) & \sigma_m(\alpha_2) & \cdots & \sigma_m(\alpha_n) \end{pmatrix}$$

Note that $\sigma(A)$ is a matrix obtained from A by permuting the rows for any $\sigma \in H$. By Lemma 91, $\sigma(A)$ has the same kernel at A. We write $V = \ker(A)$.

This is a subspace of L^n. Suppose $\mathbf{x} \in V$. Then $A\mathbf{x} = \mathbf{0}$ and so $\sigma(A)\sigma(\mathbf{x}) = \mathbf{0}$. It follows that

$$\sigma(\mathbf{x}) \in \ker(\sigma(A)) = \ker(A) = V.$$

Thus V is stable under H. Suppose first that V is non-trivial. By Lemma 92 there is some non-zero $\mathbf{y} \in \ker(A)$ such that $\mathbf{y} \in F^n$. Write

$$\mathbf{y} = \begin{pmatrix} y_1 \\ y_2 \\ \vdots \\ y_n \end{pmatrix}$$

with $y_i \in F$. From the first row of the relation $A\mathbf{y} = \mathbf{0}$ we have

$$y_1\sigma_1(\alpha_1) + y_2\sigma_1(\alpha_2) + \cdots + y_n\sigma_1(\alpha_n) = 0.$$

As $y_i \in F = L^H$ we can write this as

$$\sigma_1(y_1\alpha_1 + y_2\alpha_2 + \cdots + y_n\alpha_n) = 0.$$

As σ_1 is an isomorphism,

$$y_1\alpha_1 + y_2\alpha_2 + \cdots + y_n\alpha_n = 0.$$

As $\alpha_1, \ldots, \alpha_n$ is linearly independent over F we have $y_1, \ldots, y_n = 0$, contradicting the fact that $\mathbf{y} \neq \mathbf{0}$. We conclude that $V = \ker(A) = 0$. The Rank-Nullity Theorem tells us that

$$\operatorname{rank}(A) + \operatorname{nul}(A) = n.$$

The $\operatorname{rank}(A)$ is the maximal number of linearly independent rows, so $\operatorname{rank}(A) \leq m$ and the nullity $\operatorname{nul}(A)$ is the dimension of the kernel, so $\operatorname{nul}(A) = 0$. Hence

$$n = \operatorname{rank}(A) \leq m = \#H.$$

Thus $[L : F] \leq \#H$ as required. □

THEOREM 94. *Let L be a field and let H be a finite subgroup of its automorphism group* $\operatorname{Aut}(L)$. *Let $F = L^H$. Then*

$$[L : F] = \#H.$$

PROOF. We know from Lemma 93 that L/F is finite and $[L : F] \leq \#H$. By definition of F, every element of H is an automorphism of L/F (i.e. it fixes every element of F). Hence H is a subgroup of $\operatorname{Aut}(L/F)$. By Theorem 81,

$$\#\operatorname{Aut}(L/F) \leq [L : F].$$

In particular,

$$\#H \leq [L : F].$$

It follows that $[L : F] = \#H$. □

EXAMPLE 95. This a continuation of Examples 84 and 90. There $L = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ where p, q are distinct primes. We found that

$$\mathrm{Aut}(L/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$$

where

$$\begin{cases} \sigma_1(\sqrt{p}) = \sqrt{p}, \\ \sigma_1(\sqrt{q}) = \sqrt{q}, \end{cases} \quad \begin{cases} \sigma_2(\sqrt{p}) = -\sqrt{p}, \\ \sigma_2(\sqrt{q}) = \sqrt{q}, \end{cases} \quad \begin{cases} \sigma_3(\sqrt{p}) = \sqrt{p}, \\ \sigma_3(\sqrt{q}) = -\sqrt{q}, \end{cases} \quad \begin{cases} \sigma_4(\sqrt{p}) = -\sqrt{p}, \\ \sigma_4(\sqrt{q}) = -\sqrt{q}. \end{cases}$$

Moreover, $\sigma_1 = 1$, $\sigma_2^2 = \sigma_3^2 = 1$ and $\sigma_2\sigma_3 = \sigma_3\sigma_2 = \sigma_4$. Hence $\mathrm{Aut}(L/\mathbb{Q}) \cong C_2 \times C_2$.

In the homework you wrote down the subgroups of $\mathrm{Aut}(L/\mathbb{Q})$ and computed their fixed fields. It's worthwhile to look at this again, and check that the computations are consistent with Theorem 94.

The subgroups of $\mathrm{Aut}(L/\mathbb{Q})$ are

$$H_1 = \{1\}, \qquad H_2 = \{1, \sigma_2\}, \quad H_3 = \{1, \sigma_3\}, \quad H_4 = \{1, \sigma_4\}, \quad H_5 = \mathrm{Aut}(L/\mathbb{Q}).$$

Every element $\alpha \in L$ can be written uniquely as

$$\alpha = a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq}$$

with $a, b, c, d \in \mathbb{Q}$. Now,

$$1(\alpha) = a + b\sqrt{p} + c\sqrt{q} + d\sqrt{pq} \tag{12}$$

$$\sigma_2(\alpha) = a - b\sqrt{p} + c\sqrt{q} - d\sqrt{pq} \tag{13}$$

$$\sigma_3(\alpha) = a + b\sqrt{p} - c\sqrt{q} - d\sqrt{pq} \tag{14}$$

$$\sigma_4(\alpha) = a - b\sqrt{p} - c\sqrt{q} + d\sqrt{pq}. \tag{15}$$

Recall, for a subgroup H of $\mathrm{Aut}(L/\mathbb{Q})$,

$$L^H = \{\alpha \in L : \sigma(\alpha) = \alpha \text{ for all } \sigma \in H\}.$$

Hence

$$L^{H_1} = L.$$

This is indeed trivially consistent with Theorem 94: $\#H_1 = 1 = [L : L^{H_1}]$.

To compute L^{H_2}, we want to know when $\alpha \in L^{H_2}$. For this we want $1(\alpha) = \alpha$ and $\sigma_2(\alpha) = \alpha$. For this we need, $b = d = 0$. So

$$L^{H_2} = \{a + c\sqrt{q} : a, c \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{q}).$$

As a check, $\#H_2 = 2 = [L : \mathbb{Q}(\sqrt{q})]$. Similarly,

$$L^{H_3} = \{a + b\sqrt{p} : a, b \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{p}), \qquad \#H_3 = 2 = [L : \mathbb{Q}(\sqrt{p})].$$

For $\alpha \in L^{H_4}$ we need $b = c = 0$, so

$$L^{H_4} = \{a + d\sqrt{pq} : a, d \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{pq}), \qquad \#H_4 = 2 = [L : \mathbb{Q}(\sqrt{pq})].$$

Finally we want to know when $\alpha \in L^{H_5}$. For this we want $1(\alpha) = \alpha$, $\sigma_2(\alpha) = \alpha$, $\sigma_3(\alpha) = \alpha$, $\sigma_4(\alpha) = \alpha$. We find that $b = c = d = 0$. Thus

$$L^{H_5} = \{a : a \in \mathbb{Q}\} = \mathbb{Q}.$$

Again we check that $\#H_5 = 4 = [L : \mathbb{Q}]$.

CHAPTER 9

Galois Extensions and Galois Groups

1. Galois Extensions

DEFINITION. Let L/K be an algebraic extension. We say that L/K **is a Galois extension** if

$$L^{\mathrm{Aut}(L/K)} = K.$$

EXAMPLE 96. Let $L = \mathbb{Q}(\sqrt{2})$. Then $\mathrm{Aut}(L/\mathbb{Q}) = \{1, \sigma\}$ where $\sigma(\sqrt{2}) = -\sqrt{2}$ and an easy calculation shows that $L^{\mathrm{Aut}(L/\mathbb{Q})} = \mathbb{Q}$. Thus $L/\mathbb{Q}$ is a Galois extension.

EXAMPLE 97. Let $L = \mathbb{Q}(\sqrt[3]{2})$. From Examples 72 and 76 we know that $\mathrm{Aut}(L/\mathbb{Q}) = \{1\}$, thus $L^{\mathrm{Aut}(L/\mathbb{Q})} = L \neq \mathbb{Q}$. Hence $L/\mathbb{Q}$ is a non-Galois extension.

We shall see later that the problem here is that we have adjoined one root of the irreducible polynomial $x^3 - 2 \in \mathbb{Q}[x]$ but not the others.

EXAMPLE 98. Let p be a prime, $K = \mathbb{F}_p(t)$ and $L = K(\sqrt[p]{t})$. In Example 77 we saw that $\mathrm{Aut}(L/K) = \{1\}$ and so $L^{\mathrm{Aut}(L/K)} = L$. Hence L/K is a non-Galois extension.

Recall that in Example 62 we showed that L/K is inseparable. We shall see later that inseparability of L/K is what prevents it from being a Galois extension.

EXAMPLE 99. Let $L = \mathbb{Q}(\sqrt{p}, \sqrt{q})$ where p, q are distinct primes. In Example 95 we saw that

$$L^{\mathrm{Aut}(L/\mathbb{Q})} = \mathbb{Q}.$$

Thus $L/\mathbb{Q}$ is Galois.

LEMMA 100. *Let L/K be a finite Galois extension. Then*

$$\#\mathrm{Aut}(L/K) = [L : K].$$

PROOF. Let $H = \mathrm{Aut}(L/K)$. As L/K is finite, we know from Theorem 81 that $\#H \leq [L : K]$ and so H is indeed finite. We now apply Theorem 94. This says that $[L : L^H] = \#H$. As L/K is Galois, $L^H = K$ and $[L : K] = \#H = \#\mathrm{Aut}(L/K)$ as required. □

2. Criteria for Galois Extensions

THEOREM 101. *Let L/K be a finite extension. The following are equivalent.*

(a) *L/K is Galois.*

(b) *L is the splitting field of a separable polynomial $f \in K[x]$.*
(c) *L/K is separable and normal.*

PROOF. (b) $\implies$ (a) For this we will use induction on $[L:K]$. If $[L:K] = 1$ then $L = K$ and so L/K is definitely Galois. Suppose $[L:K] > 1$, and that L is a splitting field of $f \in K[x]$ which is separable. If f splits completely into linear factors over K then $L = K$, so we may suppose that f has some irreducible factor $g \in K[x]$ of degree $n \geq 2$. The irreducible factor g must be separable. Let $\alpha_1, \ldots, \alpha_n$ be the roots of g which must be distinct. Now $K \subset K(\alpha_1) \subseteq L$ with $[K(\alpha_1):K] = n \geq 2$ so

$$[L:K(\alpha_1)] = \frac{[L:K]}{n} < [L:K].$$

Moreover, L is the splitting field of f over $K(\alpha_1)$. Hence by the inductive hypothesis $L/K(\alpha_1)$ is Galois.

We want to show that L/K is Galois. Let

$$G = \mathrm{Aut}(L/K), \qquad H = \mathrm{Aut}(L/K(\alpha_1)).$$

It is easy to see that H is a subgroup of G. Moreover, as $L/K(\alpha_1)$ is Galois, $L^H = K(\alpha_1)$. Hence $L^G \subseteq L^H = K(\alpha_1)$. We want to show that $L^G = K$. Let $\theta \in L^G$. As $\theta \in K(\alpha_1)$ we can write $\theta = a_0 + a_1\alpha_1 + \cdots + a_{n-1}\alpha_1^{n-1}$, with $a_i \in K$.

By Corollary 87, for each i there is a K-automorphism $\sigma_i : L \to L$ such that $\sigma_i(\alpha_1) = \alpha_i$. As $\theta \in L^G$ we have $\sigma_i(\theta) = \theta$ so

$$\theta = \sigma_i(\theta) = \sigma_i(a_0 + \cdots + a_{n-1}\alpha_1^{n-1}) = a_0 + \cdots + a_{n-1}\alpha_i^{n-1}.$$

Hence the polynomial $a_{n-1}x^{n-1} + \cdots + a_0 - \theta$ of degree $\leq n-1$ has the distinct $\alpha_1, \ldots, \alpha_n$ among its roots. It must be the zero polynomial, so $\theta = a_0 \in K$.

(a) $\implies$ (c) Suppose L/K is Galois, and let $\alpha \in L$. We want to show that the minimal polynomial of α has all its roots in L (so L/K is normal) and that these roots are distinct (so L/K is separable). Let $[L:K] = n$. Then $\#\mathrm{Aut}(L/K) = n$, as L/K is Galois. Let $\mathrm{Aut}(L/K) = \{\sigma_1, \ldots, \sigma_n\}$. Let $\{\alpha_1, \ldots, \alpha_s\}$ be the set $\{\sigma_1(\alpha), \ldots, \sigma_n(\alpha)\} \subset L$ after removing repetitions. Let

$$p = (x - \alpha_1) \cdots (x - \alpha_s).$$

Then the σ_i permute the α_i, and so $\sigma_i(p) = p$. It follows that the coefficients of p belong to $L^{\mathrm{Aut}(L/K)} = K$. Thus $p \in K[x]$. But $p(\alpha) = 0$, so the minimal polynomial of α divides p. Hence the roots of the minimal polynomial of α are distinct and belong to L as required.

(c) $\implies$ (b) As L/K is finite, $L = K(\alpha_1, \ldots, \alpha_n)$, where $\alpha_i \in L$. Let m_i be the minimal polynomial of α_i over K. As L/K is normal, all the roots of m_i belong to L, and as L/K is separable, the m_i have distinct roots. Let $f = m_1 \ldots m_n$. Then L/K is the splitting field of f. Moreover f is separable as all its irreducible factors have distinct roots. □

3. Finite Fields

THEOREM 102. *Let p be a prime. Then for each $n \geq 1$, there is an extension $K/\mathbb{F}_p$ of degree n (and thus $\#K = p^n$). Moreover,*

(i) *K is the splitting field of $x^{p^n} - x \in \mathbb{F}_p[x]$;*
(ii) *K is unique up to isomorphism;*
(iii) *$K/\mathbb{F}_p$ is a Galois extension whose automorphism group is cyclic of order n, generated by the Frobenius automorphism.*

PROOF. Let $f = x^{p^n} - x \in \mathbb{F}_p[x]$, and let K be the splitting field of f. Now $Df = p^n x^{p^n-1} - 1 = -1$ and so $\gcd(f, Df) = 1$. It follows that f does not have repeated roots and so is a separable polynomial. By Theorem 101, $K/\mathbb{F}_p$ is a Galois extension. Let $\phi : K \to K$ be the Frobenius automorphism (see Section 2). Consider the set of roots

$$R = \{\alpha \in K : f(\alpha) = 0\}.$$

As f splits completely in K and has distincts roots, $\#R = \deg(f) = p^n$. The relation $f(\alpha) = 0$ can be rewritten as $\alpha^{p^n} = \alpha$ or equivalently $\phi^n(\alpha) = \alpha$. Thus $R = K^{\langle \phi^n \rangle}$ (the subfield fixed by ϕ^n). In particular R is a subfield of K and f splits completely in R. It follows that R is the splitting field of f and so $R = K$. Hence $\#K = p^n$. By Lemma 37 we have $n = [K : \mathbb{F}_p]$. As $K/\mathbb{F}_p$ is Galois, $\#\mathrm{Aut}(K/\mathbb{F}_p) = [K : \mathbb{F}_p] = n$. Recall (Lemma 79) that the Frobenius automorphism $\phi \in \mathrm{Aut}(K/\mathbb{F}_p)$ has order n. Thus ϕ is a cyclic generator of $\mathrm{Aut}(K/\mathbb{F}_p)$. We have now proved (i) and (iii).

To prove (ii), suppose K' is another field with p^n elements. By Lemma 78 every $\alpha \in K'$ is a root of $f = x^{p^n} - x$. So K' is contained in a splitting field K'' for f. Now any two splitting fields are isomorphic, so $K \cong K''$. But $K' \subseteq K''$ and $\#K' = p^n = \#K = \#K'$. Thus $K' = K'' \cong K$. □

4. Computing Galois Groups

DEFINITION. Let L/K be a Galois extension. We call $\mathrm{Aut}(L/K)$ the **Galois Group** of L/K.

Suppose L/K is a finite Galois extension. By Theorem 101 we can write $L = K(\alpha_1, \ldots, \alpha_n)$ where $\alpha_1, \ldots, \alpha_n$ are the roots of a separable polynomial $f \in K[x]$. The Galois Group $\mathrm{Aut}(L/K)$ is determined by its action on $\alpha_1, \ldots, \alpha_n$. Moreover, since elements of $\mathrm{Aut}(L/K)$ send elements of L to their K-conjugates, they permute $\alpha_1, \ldots, \alpha_n$. Thus we can think of $\mathrm{Aut}(L/\mathbb{Q})$ as a subgroup of S_n. By computing the Galois group of a Galois extension, we mean identifying the subgroup of S_n. This of course depends on the choice of f and the choice of ordering of roots $\alpha_1, \ldots, \alpha_n$.

EXAMPLE 103. Let $L = \mathbb{Q}(\sqrt{2})$. The extension $L/\mathbb{Q}$ is the splitting field of $f = x^2 - 2 \in \mathbb{Q}[x]$ which has distinct roots. Without doing any calculations, we know from Theorem 101 that $L/\mathbb{Q}$ is Galois.

The roots of f are $\alpha_1 = \sqrt{2}$, $\alpha_2 = -\sqrt{2}$. Then $\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})$ will be identified as a subgroup of S_2. But as the extension is Galois we know

from Lemma 100 that $\#\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q}) = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$. The only subgroup of S_2 that has order 2 is S_2 itself. Therefore, the Galois group is isomorphic to $S_2 = \{1, (1,2)\}$. Note that with this identification $(1,2)$ swaps $\sqrt{2}$ and $-\sqrt{2}$. Therefore it sends $a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$ to $a - b\sqrt{2}$.

EXAMPLE 104. Let p, q be distinct primes, and let $L = \mathbb{Q}(\sqrt{p}, \sqrt{q})$. We had to work quite hard (Examples 84, 90, 95, 99) to show that $L/\mathbb{Q}$ is Galois and determine $\mathrm{Aut}(L/\mathbb{Q})$. Let $f = (x^2 - p)(x^2 - q) \in \mathbb{Q}[x]$. This polynomial is separable as it has distinct roots. Its splitting field is

$$\mathbb{Q}(\sqrt{p}, -\sqrt{p}, \sqrt{q}, -\sqrt{q}) = L.$$

By Theorem 101 we know that $L/\mathbb{Q}$ is Galois without needing any further calculations.

Letting

$$\alpha_1 = \sqrt{p}, \quad \alpha_2 = -\sqrt{p}, \quad \alpha_3 = \sqrt{q}, \quad \alpha_4 = -\sqrt{q}.$$

We will identify $\mathrm{Aut}(L/\mathbb{Q})$ as a subgroup of S_4. We can actually use our earlier computations. Recall that

$$\mathrm{Aut}(L/\mathbb{Q}) = \{\sigma_1, \sigma_2, \sigma_3, \sigma_4\}$$

where

$$\begin{cases} \sigma_1(\sqrt{p}) = \sqrt{p}, \\ \sigma_1(\sqrt{q}) = \sqrt{q}, \end{cases} \quad \begin{cases} \sigma_2(\sqrt{p}) = -\sqrt{p}, \\ \sigma_2(\sqrt{q}) = \sqrt{q}, \end{cases} \quad \begin{cases} \sigma_3(\sqrt{p}) = \sqrt{p}, \\ \sigma_3(\sqrt{q}) = -\sqrt{q}, \end{cases} \quad \begin{cases} \sigma_4(\sqrt{p}) = -\sqrt{p}, \\ \sigma_4(\sqrt{q}) = -\sqrt{q}. \end{cases}$$

Note that σ_2 swaps α_1, α_2 and keeps α_3, α_4 fixed. Thus $\sigma_2 = (1,2)$ as an element of S_4. Similarly $\sigma_1 = 1$, $\sigma_3 = (3,4)$ and $\sigma_4 = (1,2)(3,4)$. Thus

$$\mathrm{Aut}(L/\mathbb{Q}) = \{1,\ (1,2),\ (3,4),\ (1,2)(3,4)\},$$

as a subgroup of S_4.

Computing $\mathrm{Aut}(L/\mathbb{Q})$ involved some hard work, so it's fair to ask if we can simplify the computation. Let's start again and see if we can simplify the computation just from the knowledge that $L/\mathbb{Q}$ is Galois of degree 4, and that it is the splitting field of f. Recall that $\mathrm{Aut}(L/\mathbb{Q})$ sends a root of f to one of its conjugates. Now $\sqrt{p}, -\sqrt{p}$ are conjugates and $\sqrt{q}, -\sqrt{q}$ are conjugates. Thus the elements of S_4 in $\mathrm{Aut}(L/\mathbb{Q})$ are only allowed to swap α_1, α_2 and they're only allowed to swap α_3, α_4. So as a subgroup of S_4, $\mathrm{Aut}(L/\mathbb{Q})$ is contained in

$$\{1,\ (1,2),\ (3,4),\ (1,2)(3,4)\}. \tag{16}$$

But the extension is Galois and so by Lemma 100 we have $\#\mathrm{Aut}(L/\mathbb{Q}) = [L : \mathbb{Q}] = 4$. The only subgroup of (16) of size 4 is the whole of (16). So

$$\mathrm{Aut}(L/\mathbb{Q}) = \{1,\ (1,2),\ (3,4),\ (1,2)(3,4)\}.$$

You will notice that this is much simpler than the computation we did before.

EXAMPLE 105. We saw before (Examples 72, 76, 97) that $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois. Let $f = x^3 - 2 \in \mathbb{Q}[x]$. This polynomial is separable as it has distinct roots:

$$\alpha_1 = \sqrt[3]{2}, \qquad \alpha_2 = \zeta\sqrt[3]{2}, \qquad \alpha_3 = \zeta^2\sqrt[3]{2},$$

where $\zeta = \exp(2\pi i/3)$. The splitting field of f is

$$L = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3) = \mathbb{Q}(\sqrt[3]{2}, \zeta).$$

By Theorem 101, the extension $L/\mathbb{Q}$ is Galois. Let us identify $\mathrm{Aut}(L/\mathbb{Q})$ as a subgroup of S_3. It will be easy for you to check (using the Tower Law) that $[L : \mathbb{Q}] = 6$ (c.f. Section 2). As $\#S_3 = 6$, we see that $\mathrm{Aut}(L/\mathbb{Q})$ is the whole of S_3.

Identifying $\mathrm{Aut}(L/\mathbb{Q})$ with S_3 tells us how it acts on $\alpha_1, \alpha_2, \alpha_3$. It is important to know how to use this to deduce how $\mathrm{Aut}(L/\mathbb{Q})$ acts on other elements of L. For example, take $\sigma = (1,3,2)$. Then

$$\sigma(\alpha_1) = \alpha_3, \qquad \sigma(\alpha_3) = \alpha_2, \qquad \sigma(\alpha_2) = \alpha_1.$$

Now $\zeta \in L$. What is $\sigma(\zeta)$? Observe that $\zeta = \alpha_2/\alpha_1$. So

$$\sigma(\zeta) = \frac{\sigma(\alpha_2)}{\sigma(\alpha_1)} = \frac{\alpha_1}{\alpha_3} = \frac{1}{\zeta^2} = \zeta^{-2} = \zeta.$$

Let's try $\tau = (1,2)$:

$$\tau(\zeta) = \frac{\tau(\alpha_2)}{\tau(\alpha_1)} = \frac{\alpha_1}{\alpha_2} = \frac{1}{\zeta} = \zeta^2.$$

CHAPTER 10

The Fundamental Theorem of Galois Theory

Let L/K be a Galois extension with Galois group $G = \mathrm{Aut}(L/K)$. Let $\mathscr{H}$ be the set of subgroups of G. Let $\mathscr{F}$ be the set of fields F such that $K \subseteq F \subseteq L$ (the intermediate fields for L/K). We shall define the following maps:

$$* : \mathscr{F} \to \mathscr{H}, \qquad F \mapsto F^* = \mathrm{Aut}(L/F),$$
$$\dagger : \mathscr{H} \to \mathscr{F}, \qquad H \mapsto H^\dagger = L^H.$$

The maps $*$ and $\dagger$ are together known as the **Galois correspondence**.

THEOREM 106 (Fundamental Theorem of Galois Theory). *Let L/K be a finite Galois extension, with Galois group $G = \mathrm{Aut}(L/K)$.*

(i) *The maps $*$ and $\dagger$ are mutual inverses*

$$F^{*\dagger} = F, \qquad H^{\dagger *} = H,$$

and hence are bijections between $\mathscr{F}$ and $\mathscr{H}$.

(ii) *The bijections $*$ and $\dagger$ are inclusion reversing:*

$$F_1 \subseteq F_2 \implies F_1^* \supseteq F_2^*, \qquad H_1 \subseteq H_2 \implies H_1^\dagger \supseteq H_2^\dagger.$$

(iii) *L/F is Galois for all $F \in \mathscr{F}$. Moreover,*

$$[L : F] = \#F^*, \qquad [F : K] = \frac{\#G}{\#F^*}.$$

(iv) *Let $F \in \mathscr{F}$. Then*

$$F/K \text{ is Galois} \iff F^* \trianglelefteq G \iff \sigma(F) = F \text{ for all } \sigma \in G. \tag{17}$$

In this case $\mathrm{Aut}(F/K) \cong G/F^*$.

PROOF. Recall by Theorem 101 that a finite extension is Galois if and only it is the splitting field of a separable polynomial. Since L/K is finite and Galois, L is the splitting field of a separable polynomial $f \in K[x]$. If $F \in \mathscr{F}$ then $K \subseteq F \subseteq L$ so $f \in F[x]$, and L is also the splitting field of f over F. Hence L/F is Galois. This proves the first part of (iii).

Now as L/F is Galois, by Lemma 100 we have $[L : F] = \#\mathrm{Aut}(L/F) = \#F^*$. This proves the second part of (iii). For the third part of (iii) we will apply the Tower Law to $L/F/K$

$$[F : K] = \frac{[L : K]}{[L : F]} = \frac{\#G}{\#F^*}.$$

Here we've used the fact that since L/K is Galois, then $[L : K] = \#\mathrm{Aut}(L/K) = G$ (Lemma 100 again). This completes the proof of (iii).

For (i), note that

$$F^{*\dagger} = \mathrm{Aut}(L/F)^{\dagger} = L^{\mathrm{Aut}(L/F)} = F$$

where the first two equalities use the definitions, and the last one uses the fact that L/F is Galois. This proves the first part of (i). For the second part,

$$H^{\dagger *} = \left(L^H\right)^* = \mathrm{Aut}(L/L^H).$$

This group contains H. But L/L^H is Galois by part (i) so $\#\mathrm{Aut}(L/L^H) = [L : L^H]$. By Theorem 94, $[L : L^H] = \#H$. Hence $\#\mathrm{Aut}(L/L^H) = \#H$. Hence $\mathrm{Aut}(L/L^H)$ is a group that contains H and has the same number of elements. So $\mathrm{Aut}(L/L^H) = H$. I.e. $H^{\dagger *} = H$. This finishes the proof of (i).

Part (ii) is a very easy exercise from the definitions.

All that remains is (iv). For this we need some lemmas. □

LEMMA 107. *In the notation of the Fundamental Theorem, for all $\sigma \in G$, and for all $F \in \mathscr{F}$,*

$$\sigma(F)^* = \sigma F^* \sigma^{-1}.$$

PROOF. Recall the definition $F^* = \mathrm{Aut}(L/F)$. This is the set of elements $\tau \in G$ that fix every element of F. Now

$$\begin{aligned}
\tau \in \sigma(F)^* &\iff \tau\beta = \beta \text{ for all } \beta \in \sigma(F) \\
&\iff \tau\sigma\alpha = \sigma\alpha \text{ for all } \alpha \in F \\
&\iff \sigma^{-1}\tau\sigma\alpha = \alpha \text{ for all } \alpha \in F \\
&\iff \sigma^{-1}\tau\sigma \in F^* \\
&\iff \tau \in \sigma F^* \sigma^{-1}.
\end{aligned}$$

Thus $\sigma(F)^* = \sigma F^* \sigma^{-1}$. □

LEMMA 108. *In the notation of the Fundamental Theorem, F/K is Galois if and only if $\sigma(F) = F$ for all $\sigma \in G$.*

PROOF. Suppose F/K is Galois. Then F is the splitting field of some separable $f \in K[x]$. Write $F = K(\alpha_1, \ldots, \alpha_n)$ where the α_i are the roots of f. Let $\sigma \in G = \mathrm{Aut}(L/K)$. Then, since $f \in K[x]$, $f(\sigma(\alpha_i)) = \sigma(f(\alpha_i)) = \sigma(0) = 0$. Hence $\sigma(\alpha_i) = \alpha_j$ for some j. Therefore, σ fixes every element of K and permutes the α_i. As $F = K(\alpha_1, \ldots, \alpha_n)$, we have $\sigma(F) = F$.

Conversely, suppose $\sigma(F) = F$ for all $\sigma \in G$. Let $\alpha_1, \ldots, \alpha_n$ be a basis for F/K. Let $\beta_1, \ldots, \beta_m$ be the distinct elements of the set

$$\{\sigma(\alpha_i) : i = 1, \ldots, n, \sigma \in G\}.$$

Then $\beta_j \in F$ as $\sigma(F) = F$. Also the β_j contain the α_i among them (as $1 \in G$). Thus $F = K(\beta_1, \ldots, \beta_m)$. Let

$$p = (x - \beta_1) \cdots (x - \beta_m).$$

This polynomial has distinct roots and is therefore separable. Moreover, $\sigma(p) = p$ for all $\sigma \in G$ (as the σ permute the β_j). It follows that the coefficients of p belong to $L^G = K$ (as L/K is Galois and $G = \mathrm{Aut}(L/K)$). Hence $p \in K[x]$. We see that F is the splitting field of a separable polynomial $\in K[x]$ and so F/K is Galois. □

COMPLETING THE PROOF OF THE FUNDAMENTAL THEOREM. It remains to prove part (iv) of the fundamental theorem. We know by Lemma 108 that F/K is Galois if and only if $\sigma(F) = F$ for all $\sigma \in G$. We want to show that this is equivalent to F^* being a normal subgroup of G. Recall that a subgroup H of G is **normal** (written $H \trianglelefteq G$) if $\sigma H \sigma^{-1} = H$ for all $\sigma \in G$. We know by Lemma 107, that $F^* \trianglelefteq G$ if and only if $\sigma(F)^* = F^*$ for all $\sigma \in G$. As $* : \mathscr{F} \to \mathscr{H}$ is a bijection (part (ii) of the Fundamental Theorem), this is equivalent to $\sigma(F) = F$ for all $\sigma \in G$. We have now established the equivalences in (17). Assume that these hold. Define

$$\phi : G \to \mathrm{Aut}(F/K)$$

by $\phi(\sigma) = \sigma|_F$ for $\sigma \in G$. Note that if $\sigma \in G$ then $\sigma(F) = F$ and so $\sigma|_F$ does define an isomorphism $F \to F$. The kernel of ϕ is those $\sigma \in G$ that fix every element of F. Thus $\ker(\phi) = F^*$. By the First Isomorphism Theorem we have an induced isomorphism

$$\hat{\phi} : G/F^* \to \mathrm{Im}(\phi).$$

To complete the proof we want to show that ϕ is surjective. But

$$\#\mathrm{Im}(\phi) = \#(G/F^*) = \frac{\#G}{\#F^*} = [F : K] = \#\mathrm{Aut}(F/K)$$

where in the third equality we used part (iii) of the Fundamental Theorem, and in the final equality we used the assumption that F/K is Galois. As $\mathrm{Im}(\phi)$ is a subgroup of $\mathrm{Aut}(F/K)$ we see that $\mathrm{Im}(\phi) = \mathrm{Aut}(F/K)$ so ϕ is surjective. □

1. Example/a worked out exam question

Let $f = x^3 - 5 \in \mathbb{Q}[x]$ and order its roots as $\theta_1 = \sqrt[3]{5}$, $\theta_2 = \zeta\sqrt[3]{5}$, $\theta_3 = \zeta^2\sqrt[3]{5}$ where $\zeta = \exp(2\pi i/3)$. Let L be the splitting field of $f = x^3 - 5 \in \mathbb{Q}[x]$.

(i) Show that $L/\mathbb{Q}$ is Galois, with Galois group S_3.
(ii) With the help of the Fundamental Theorem of Galois Theory, explain how many intermediate fields $\mathbb{Q} \subseteq K \subseteq L$ there are.
(iii) Calculate the intermediate fields

$$\{1, (1,2)\}^\dagger, \qquad \{1, (1,2,3), (1,3,2)\}^\dagger.$$

(iv) Compute $\mathbb{Q}(\sqrt{-3})^*$ as a subgroup of S_3.

Answer.

(i) The polynomial f is separable as the roots θ_1, θ_2, θ_3 are distinct (or we can say that f is separable as $f \in \mathbb{Q}[x]$ and $\mathbb{Q}$ has characteristic 0). As L is the splitting field of a separable polynomial we know that it is Galois.

As f is irreducible, $[\mathbb{Q}(\theta_1):\mathbb{Q}] = 3$. Now $L = \mathbb{Q}(\theta_1, \zeta)$ and ζ is a root of $x^2 + x + 1$. Moreover, $\zeta \notin \mathbb{Q}(\theta_1)$ as $\zeta \notin \mathbb{R}$. Hence $[L:\mathbb{Q}(\theta_1)] = 2$. By the tower law $[L:\mathbb{Q}] = 6$.

Finally, as $L/\mathbb{Q}$ is Galois, $\#\mathrm{Aut}(L/\mathbb{Q}) = [L:\mathbb{Q}] = 6$. Since $\mathrm{Aut}(L/\mathbb{Q})$ is a subgroup of S_3 and $\#S_3 = 6$ we have $\mathrm{Aut}(L/\mathbb{Q}) = S_3$.

(ii) By the Fundamental Theorem of Galois Theory, there is a bijection between the intermediate fields $\mathbb{Q} \subseteq K \subseteq L$ and the subgroups of the Galois group $\mathrm{Aut}(L/\mathbb{Q}) = S_3$.

S_3 has exactly six subgroups:

$$\{1\}, \quad S_3, \quad A_3 = \langle (1,2,3) \rangle, \quad \langle (1,2) \rangle, \quad \langle (1,3) \rangle, \quad \langle (2,3) \rangle.$$

Thus there are exactly six intermediate fields.

(iii) By the Fundamental Theorem of Galois Theory, $[H^\dagger:\mathbb{Q}] = \#S_3/\#H = 6/\#H$.

Let

$$H_1 = \{1, (1,2)\}, \qquad H_2 = \{1, (1,2,3), (1,3,2)\}.$$

Then $[H_1^\dagger:\mathbb{Q}] = 3$ and $[H_2^\dagger:\mathbb{Q}] = 2$.

Note that $(1,2)\theta_3 = \theta_3$. Thus $\mathbb{Q}(\theta_3) \subseteq H_1^\dagger$. As $[\mathbb{Q}(\theta_3):\mathbb{Q}] = 3$ we have $H_1^\dagger = \mathbb{Q}(\theta_3)$.

Also

$$(1,2,3)(\zeta) = (1,2,3)(\theta_2/\theta_1) = \theta_3/\theta_2 = \zeta.$$

Thus $\mathbb{Q}(\zeta) \subseteq \langle (1,2,3) \rangle^\dagger = H_2^\dagger$. But ζ is the root of the irreducible $x^2 + x + 1$, so $[\mathbb{Q}(\zeta):\mathbb{Q}] = 2$. Hence $H_2^\dagger = \mathbb{Q}(\zeta)$.

(iv) Note $\zeta = (-1 + \sqrt{-3})/2$, so $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta)$. As $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta) = H_2^\dagger$, we have $\mathbb{Q}(\sqrt{-3})^* = H_2^{\dagger *} = H_2$.

There is another way of doing this last bit if we didn't spot that $\mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta)$. Note that $\#\mathbb{Q}(\sqrt{-3})^* = 6/[\mathbb{Q}(\sqrt{-3}):\mathbb{Q}] = 3$. The only subgroup of S_3 of order 3 is $A_3 = H_2$. Thus $\mathbb{Q}(\sqrt{-3})^* = H_2$.

CHAPTER 11

Solubility by Radicals

DEFINITION. A field extension M/K is called **radical** if there is a chain of subfields

$$K = M_0 \subseteq M_1 \subseteq M_2 \subseteq \cdots \subseteq M_n = M$$

such that $M_i = M_{i-1}(\alpha_i)$ with $\alpha_i^{n_i} \in M_{i-1}$ for some integer $n_i > 0$.

EXAMPLE 109. Let

$$M = \mathbb{Q}\left(\zeta, \sqrt{2}, \sqrt[3]{-1+\sqrt{2}}, \sqrt[3]{-1-\sqrt{2}}\right),$$

where ζ is a primitive cube root of 1. Then $M/\mathbb{Q}$ is a radical extension. Indeed, let

$$\alpha_1 = \zeta, \qquad \alpha_2 = \sqrt{2}, \qquad \alpha_3 = \sqrt[3]{-1+\sqrt{2}}, \qquad \alpha_4 = \sqrt[3]{-1-\sqrt{2}},$$

and let

$$M_0 = \mathbb{Q}, \quad M_1 = \mathbb{Q}(\alpha_1), \quad M_2 = \mathbb{Q}(\alpha_1, \alpha_2), \quad M_3 = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3), \quad M_4 = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \alpha_4) = M,$$

and observe that $\alpha_1^3 \in M_0$, $\alpha_2^2 \in M_1$, $\alpha_3^3 \in M_2$, $\alpha_4^3 \in M_3$.

EXERCISE 110. If M/K is a radical extension then it is finite.

EXERCISE 111. Let L/K be a non-trivial radical extension. Show that there is some prime p and an $\alpha \in L$ such that $\alpha \notin K$ but $\alpha^p \in K$.

DEFINITION. Let $f \in K[x]$. We say f is **soluble by radicals** if and only if the splitting field L is contained in a field M which is a radical extension of K.

Note that we do not insist on the splitting field itself being a radical extension, merely that it is contained in a radical extension.

EXAMPLE 112. Let K be a field of characteristic 0. Let $f \in K[x]$ be a quadratic polynomial. We know from the quadratic formula that the splitting field of f is $K(\sqrt{\Delta})$ where Δ is the discriminant of f. Thus f is soluble by radicals.

In fact, it is known by Cardano's formulae (which we won't go through) that cubic and quartic polynomials are soluble in radicals.

The main theorem in this subject is the following.

THEOREM 113. *Assume that K has characteristic 0. Let $f \in K[x]$ be irreducible and let L be its splitting field. Then f is soluble by radicals if and only if* $\mathrm{Aut}(L/K)$ *is soluble.*

We will not prove the theorem completely, but only the $\Longrightarrow$ direction.

To understand the theorem we should define what it means for a group to be soluble.

1. Soluble Groups

DEFINITION. Let G be a group. A **subnormal series** for G is a chain of subgroups

$$1 = G_0 \subseteq G_1 \subseteq G_2 \subseteq \cdots \subseteq G_n = G$$

such that G_i is a normal subgroup of G_{i+1} for $0 \leq i \leq n-1$.

If moreover each G_i is a normal subgroup of G then we say call the chain of subgroups a normal series. We shall not need normal series.

DEFINITION. A group is called **soluble** if it has a subnormal series as above where every quotient G_{i+1}/G_i is abelian.

EXAMPLE 114. Every abelian group G is soluble, with subnormal series $1 \subseteq G$.

EXAMPLE 115. S_3 is soluble with subnormal series $1 \subset A_3 \subset S_3$. Observe that $A_3/1 \cong A_3 \cong C_3$ and $S_3/A_3 \cong C_2$ are both abelian.

EXAMPLE 116. D_4 (the group of symmetries of the square) is soluble. Let $R \subset D_4$ be the subgroup consisting of the four rotations in D_4. Then $1 \subset R \subset D_4$ is a subnormal series with $R/1 \cong R \cong C_4$ and $D_4/R \cong C_2$ are both abelian.

EXAMPLE 117. S_4 is soluble with subnormal series

$$1 \subset V_4 \subset A_4 \subset S_4, \qquad (V_4 = \{1, (1,2)(3,4), (1,3)(2,4), (1,4)(2,3)\}),$$

with quotients $V_4 \cong C_2 \times C_2$, $A_4/V_4 \cong C_3$, $S_4/A_4 \cong C_2$, which are all abelian.

EXAMPLE 118. A_5 and S_5 are not soluble, as we shall see in due course.

DEFINITION. Let $g, h \in G$. The **commutator** of g, h, denoted by $[g,h]$, is $[g,h] = g^{-1}h^{-1}gh$.

LEMMA 119. *Let G be a group and N a normal subgroup. Then G/N is abelian if and only if $[g,h] \in N$ for all $g, h \in G$.*

PROOF. Note that G/N is abelian if and only if $gN \cdot hN = hN \cdot gN$ or equivalently $ghN = hgN$ for all $g,\ h \in G$. This is equivalent to $[g,h] = (hg)^{-1}gh \in N$. □

PROPOSITION 120.
(i) *Subgroups of soluble groups are soluble.*
(ii) *If $\phi : G \to H$ is a homomorphism and G is soluble then* $\mathrm{Im}(\phi)$ *is soluble.*
(iii) *Quotient groups of soluble groups are soluble (i.e. if N is a normal subgroup of G and G is soluble then G/N is soluble).*
(iv) *If N is a normal subgroup of G and both N and G/N are soluble then G is soluble.*

PROOF. Let's prove (i). Let H be a subgroup of G and suppose G is soluble with subnormal series $1 \subseteq G_0 \subseteq \cdots \subseteq G_n = G$ with abelian quotients G_{i+1}/G_i. Let $H_i = G_i \cap H$. We will show that $1 \subseteq H_0 \subseteq \cdots \subseteq H_n = H$ is a subnormal series with abelian quotients H_{i+1}/H_i, which tells us that H is soluble. First we show that H_i is normal in H_{i+1}. Let $h \in H_{i+1}$. Then

$$h^{-1}H_i h = h^{-1}(G_i \cap H)h = (h^{-1}G_i h) \cap (h^{-1}Hh).$$

But $h \in H_{i+1} \subset G_{i+1}$ and G_i is normal in G_{i+1} so $h^{-1}G_i h = G_i$. Also, $h \in H_{i+1} \subseteq H$, so $h^{-1}Hh = H$. Hence

$$h^{-1}H_i h = G_i \cap H = H_i.$$

Hence H_i is a normal subgroup of H_{i+1} and so $1 \subseteq H_1 \cdots \subseteq H_n = H$ is a subnormal series of H. Also if $g, h \in H_{i+1}$, then $g, h \in G_{i+1}$ and so $[g,h] \in G_i$ by Lemma 119 as G_{i+1}/G_i is abelian. But $g, h \in H$, so $[g,h] \in H$ so $[g,h] \in G_i \cap H = H_i$. Again by Lemma 119, the quotient H_{i+1}/H_i is abelian. This proves (i).

The remaining parts are similar exercises proved using Lemma 119. □

2. More on Radical Extensions

LEMMA 121. *If M/L and L/K are radical extensions then M/K is a radical extension.*

PROOF. This is obvious from the definition. □

PROPOSITION 122. *Let $K \subset \mathbb{C}$. Suppose that L/K is a radical extension. Then there is a field M containing L such that M/K is both Galois and radical.*

PROOF. By assumption, there is a sequence $K = L_0 \subseteq \cdots \subseteq L_n = L$ such that $L_i = L_{i-1}(\alpha_i)$ with $\alpha_i^{r_i} \in L_{i-1}$ for some positive integer r_i. Let m_i be the minimal polynomial of α_i over K, and let $f = m_1 m_2 \cdots m_n$. As $K \subset \mathbb{C}$, it has characteristic 0. By Lemma 68, the irreducible polynomials m_i are separable, so f is separable. Let M be the splitting field of f over K. By Theorem 101, the extension M/K is Galois. Moreover, M contains the α_i and K, so M contains L.

It remains to show that M/K is radical. We do this by induction on n. If $n = 0$, then $K = L = M$, and so M/K is trivially radical. Suppose $n > 0$. Let $F = K(\beta_1, \ldots, \beta_k)$ where the β_j are the roots of $m_1 m_2 \cdots m_{n-1}$. Note that α_i is a root of m_i and so belongs to F for $i \leq n-1$. So L_{n-1} is contained in F, and F is the splitting field of $m_1 m_2 \cdots m_{n-1}$ over K. By the inductive hypothesis F/K is radical and Galois. To show that M/K is radical, it is enough to show that M/F is radical by Lemma 121.

Let $\gamma_1, \ldots, \gamma_s$ be the roots of m_n. As α_n is a root of m_n we can suppose that $\gamma_1 = \alpha_n$. Note that $M = F(\gamma_1, \ldots, \gamma_s)$. As M/K is Galois, and the γ_i

share the same minimal polynomial of K (hence conjugate), there is $\sigma_i \in \mathrm{Aut}(M/K)$ such that $\sigma_i(\gamma_1) = \gamma_i$. Hence

$$\sigma_i(\alpha_n^{r_n}) = \sigma_i(\gamma_1^{r_n}) = \gamma_i^{r_n}.$$

But $\alpha_n^{r_n} \in L_{n-1} \subseteq F$. As the intermediate extension F/K is Galois, we know from the Fundamental Theorem of Galois Theorem that $\sigma_i(F) = F$. Hence

$$\gamma_i^{r_n} = \sigma_i(\alpha_n^{r_n}) = \alpha_n^{r_n} \in F.$$

It follows that $M = F(\gamma_1, \ldots, \gamma_s)$ is a radical extension of F, as required. □

3. Galois Groups of Radical Galois Extensions are Soluble

It is convenient to work inside $\mathbb{C}$.

LEMMA 123. *Let K be a subfield of $\mathbb{C}$. Let $\zeta = \exp(2\pi i/p)$ with p prime. Then $K(\zeta)/K$ is Galois and $\mathrm{Aut}(K(\zeta)/K)$ is abelian.*

PROOF. The minimal polynomial of ζ divides $x^p - 1$ which is a separable polynomial, and all its roots are powers of ζ. Thus $K(\zeta)/K$ is a separable normal extension and hence Galois. An element $\sigma \in \mathrm{Aut}(K(\zeta)/K)$ is determined by $\sigma(\zeta)$ which must be of the form ζ^a for some a. Write σ_a for this element. Then

$$\sigma_a\sigma_b(\zeta) = \zeta^{a+b} = \sigma_b\sigma_a(\zeta).$$

Hence $\sigma_a\sigma_b = \sigma_b\sigma_a$ as required. □

LEMMA 124. *Let K be a subfield of $\mathbb{C}$ such that $\zeta = \exp(2\pi i/p) \in K$ where p is prime. Let $\alpha \in K$. Then $K(\sqrt[p]{\alpha})/K$ is Galois and $\mathrm{Aut}(K(\sqrt[p]{\alpha})/K)$ abelian.*

PROOF. This is similar to the above. The key difference is that an element σ of $\mathrm{Aut}(K(\sqrt[p]{\alpha})/K$ sends $\sqrt[p]{\alpha}$ to $\zeta^a \sqrt[p]{\alpha}$. Denote this element by σ_a. Note that as $\zeta \in K$, $\sigma_a(\zeta) = \zeta$. Thus

$$\sigma_a\sigma_b(\sqrt[p]{\alpha}) = \zeta^{a+b}\sqrt[p]{\alpha} = \sigma_b\sigma_a(\sqrt[p]{\alpha}).$$

Hence $\sigma_a\sigma_b = \sigma_b\sigma_a$ as required. □

LEMMA 125. *Let K be a subfield of $\mathbb{C}$ and $\alpha \in K$. Let $L = K(\sqrt[p]{\alpha}, \zeta)$ where p is prime and $\zeta = \exp(2\pi i/p)$. Then the extension L/K is Galois, and $\mathrm{Aut}(L/K)$ is soluble.*

PROOF. It's an easy exercise to show that L/K is Galois. For solubility, note that since $K(\zeta)/K$ is Galois (Lemma 123), by the Fundamental Theorem of Galois Theory, $\mathrm{Aut}(L/K(\zeta))$ is a normal subgroup of $\mathrm{Aut}(L/K)$. Thus we have a subnormal series

$$1 \subseteq \mathrm{Aut}(L/K(\zeta)) \subseteq \mathrm{Aut}(L/K).$$

The first quotient is $\mathrm{Aut}(L/K(\zeta))$ which is abelian by Lemma 124 and the second quotient is

$$\mathrm{Aut}(L/K)/\mathrm{Aut}(L/K(\zeta)) \cong \mathrm{Aut}(K(\zeta)/K)$$

which is abelian by Lemma 123. □

PROPOSITION 126. *If a field extension L/K is Galois and radical then* $\mathrm{Aut}(L/K)$ *is soluble.*

PROOF. We shall prove this by induction on $[L:K]$. If $[L:K]=1$ then $\mathrm{Aut}(L/K)=1$ is soluble. Suppose $[L:K]>1$.

By Exercise 111, as L/K is radical, there is $\alpha\in L$ such that $\alpha\notin K$ and $\alpha^p=\beta\in K$ for some prime p. The minimal polynomial m of α over K divides $x^p-\beta$. As $\alpha\notin K$, the minimal polynomial has degree ≥ 2. Now L/K is Galois and so there are at least two roots of $x^p-\beta$ in L. It follows that $\zeta=\exp(2\pi i/p)\in L$. Consider the chain of subfields

$$K\subseteq M\subseteq L,\qquad M=K(\zeta,\alpha).$$

By Lemma 125, M/K is Galois, and hence by the Fundamental Theorem of Galois Theory, $\mathrm{Aut}(L/M)$ is a normal subgroup of $\mathrm{Aut}(L/K)$, and

$$\mathrm{Aut}(L/K)/\mathrm{Aut}(L/M)\cong\mathrm{Aut}(M/K)$$

Clearly L/M is Galois and radical and $[L:M]<[L:K]$. By the inductive hypothesis $\mathrm{Aut}(L/M)$ is soluble. Moreover, by Lemma 125, $\mathrm{Aut}(M/K)$ is soluble. It follows from part (iv) of Proposition 120 that $\mathrm{Aut}(L/K)$ is soluble as required. □

COROLLARY 127. *Let $f\in K[x]$ where $K\subset\mathbb{C}$, and let L be the splitting field of f over K. If f is soluble in radicals then* $\mathrm{Aut}(L/K)$ *is soluble.*

PROOF. We know that L/K is Galois. By definition of soluble polynomial, $L\subseteq M$ with M/K a radical extension. From Proposition 122 we know that $M\subset M'$ where M'/K is radical and Galois. Now consider the tower $K\subseteq L\subseteq M'$. As L/K is Galois, we know from the Fundamental Theorem of Galois Theory that

$$\mathrm{Aut}(M'/K)/\mathrm{Aut}(M'/L)\cong\mathrm{Aut}(L/K).$$

Thus $\mathrm{Aut}(L/K)$ is a quotient of the soluble $\mathrm{Aut}(M'/K)$. By Part (iii) of Proposition 120, $\mathrm{Aut}(L/K)$ is soluble. □

4. A Quintic That is not Soluble in Radicals

LEMMA 128. *Let G be a group, and let α,β,γ be non-identity elements of G whose orders are finite and pairwise coprime. Suppose $\alpha\beta\gamma=1$. Then G is insoluble.*

PROOF. By contradiction. Suppose G is soluble, so that there is a subnormal series

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

with G_{i+1}/G_i abelian. Let u, v, w be the orders of α, β, γ. Let

$$a=\alpha G_{n-1},\qquad b=\beta G_{n-1},\qquad c=\gamma G_{n-1}.$$

Then $abc = 1$ and $a^u = b^v = c^w = 1$ in G/G_{n-1}. But as G/G_{n-1} is abelian, $(bc)^m = b^m c^m$. Thus

$$a^{vw} = (bc)^{-vw} = b^{-vw}c^{-vw} = 1.$$

Hence the order of a divides u and vw. As these are coprime, $a = 1$ in G/G_{n-1} and so $\alpha \in G_{n-1}$. Similarly $\beta, \gamma \in G_{n-1}$. Apply the argument recursively to deduce that $\alpha, \beta, \gamma \in G_0 = \{1\}$. This contradicts that these are non-identity elements. □

LEMMA 129. *A_n and S_n are insoluble for $n \geq 5$.*

PROOF. Apply Lemma 128 with $\alpha = (1,2,3,4,5)$, $\beta = (1,2)(3,4)$, $\gamma = (1,5,3)$. These are even permutations so contained in A_n and S_n for $n \geq 5$, satisfying $\alpha\beta\gamma = 1$ and have orders 5, 2, 3 which are pairwise coprime. □

LEMMA 130. *Let G be a subgroup of S_5 containing a transposition and a 5-cycle. Then $G = S_5$.*

PROOF. Let $\tau = (a,b)$ be a transposition in G, and let σ_0 be a 5-cycle in G. There is some power $\sigma = \sigma_0^k$ such that $\sigma(a) = b$. Thus $\sigma = (a,b,c,d,e)$ where a,b,c,d,e are the numbers $1,2,3,4,5$ in some order. Now as $\tau, \sigma \in G$, we have

$$(a,b,c,d,e)(a,b) = (a,c,d,e)$$

is an element of order 4 in G. Also

$$(a,c,d,e)^2(a,b) = (a,d)(b,c,e)$$

is an element of order 6 in G. But σ has order 5. Thus $\#G$ is divisible by $\mathrm{lcm}(4,6,5) = 60$. So $G = A_5$ or S_5. But G contains the transposition (a,b) so $G \neq A_5$ and hence $G = S_5$. □

THEOREM 131. *The polynomial $f = 2x^5 - 10x + 5$ has Galois group S_5 and hence is not soluble in radicals.*

PROOF. Note $f' = 10(x^4 - 1)$ vanishes at ± 1. Thus the graph of f has turning points at $(-1,13)$ and $(1,-3)$. A quick sketch convinces us that f has three real roots and hence two complex roots. Let $L/\mathbb{Q}$ be the splitting field of f. Let $\tau \in \mathrm{Aut}(L/\mathbb{Q})$ be the restriction of complex conjugation to $L \subset \mathbb{C}$. Then τ fixes the three real roots and swaps the two complex ones. Hence τ is a transposition as an element of S_5. Moreover, f is irreducible, so $5 \mid [L:\mathbb{Q}] = \#\mathrm{Aut}(L/\mathbb{Q})$. Then as a subgroup of S_5, $\mathrm{Aut}(L/\mathbb{Q})$ contains a 5-cycle. By Lemma 130, $\mathrm{Aut}(L/\mathbb{Q}) = S_5$ as required. □

CHAPTER 12

Ruler and Compass Constructions

By a ruler we mean an *unmarked* straight edge. Most of you have met ruler and compass constructions at GCSE, and will remember (or can google) how to bisect a line segment or an angle. We will be concerned with certain classical problems such as whether there are ruler and compass constructions to trisect angles or to square circles (explained later). First we start with an algebraic formulation of ruler and compass constructions.

DEFINITION. Let $\mathscr{P}$ be a finite set of points in $\mathbb{R}^2$. Consider the following two operations:

(a) **Operation 1 (ruler)**: Through any two points of $\mathscr{P}$ draw a straight line.

(b) **Operation 2 (compass)**: Draw a circle whose centre is a point $P \in \mathscr{P}$ and whose radius is equal to the distance between some pair of points $Q, R \in \mathscr{P}$.

A point of intersection of any two distinct lines or line and circle or circle and circle obtained using operations 1 and 2 is called **constructible in one step from** $\mathscr{P}$. A point $P \in \mathbb{R}^2$ is called **constructible** from the set $\mathscr{P}$ if there is a sequence

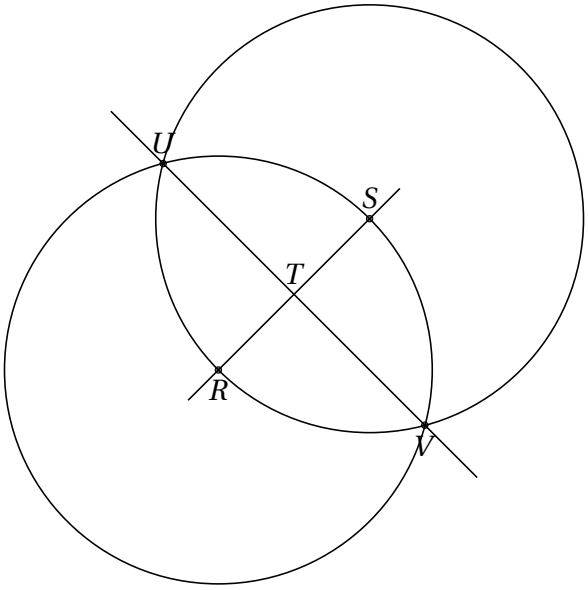
$$P_1, P_2, P_3, \ldots, P_n$$

with $P_n = P$ such that

- P_1 is constructible in one step from $\mathscr{P}$,
- P_2 is constructible in one step from $\mathscr{P} \cup \{P_1\}$,
- P_3 is constructible in one step from $\mathscr{P} \cup \{P_1, P_2\}$,
- $\vdots$
- P_n is constructible in one step from $\mathscr{P} \cup \{P_1, P_2, \ldots, P_{n-1}\}$.

EXAMPLE 132. Let $R, S \in \mathbb{R}^2$, with $R \neq S$. Let $\mathscr{P} = \{R, S\}$. We shall show that the mid-point $\frac{1}{2}(R+S)$ is constructible from $\mathscr{P}$ following the steps of the usual construction of the mid-point of a line segment. First draw a circle centred at R with radius $\|R-S\|$ (the distance between R and S) and another centred at S with the same radius. These intersect at points U, V (see the picture). The points U, V are constructible from $\mathscr{P}$ in one step. Now draw the line joining R, S and the line joining U, V and let T be their point of intersection (again see the picture). By definition, T is constructible in one step from $\mathscr{P} \cup \{U, V\}$, and so is constructible from $\mathscr{P}$. It remains to observe that $T = \frac{1}{2}(R+S)$. Now if you're pedantic you

can check this algebraically, or if you're sensible you can just say that it's geometrically obvious.



EXERCISE 133. Let A, B, C be three non-colinear points in $\mathbb{R}^2$. Show that there is a point $D \in \mathbb{R}^2$, constructible from $\mathscr{P} = \{A, B, C\}$, so that the angle $\angle ABD = \frac{1}{2}\angle ABC$. Thus "angles can be bisected using a ruler and compass construction".

1. Fields and Constructible Points

Let $\mathscr{P}$ be a finite set of points in $\mathbb{R}^2$. Write $\mathbb{Q}(\mathscr{P})$ for the subfield of $\mathbb{R}$ generated by the x and y-coordinates of the points in $\mathscr{P}$.

EXAMPLE 134. If $\mathscr{P} = \{(0,0),(1,1)\}$ then $\mathbb{Q}(\mathscr{P}) = \mathbb{Q}$. If $\mathscr{P} = \{(0,0),(1,1),(\sqrt{2},1)\}$ then $\mathbb{Q}(\mathscr{P}) = \mathbb{Q}(\sqrt{2})$.

LEMMA 135. *Let $\mathscr{P}$ be a finite set of points in $\mathbb{R}^2$, and write $K = \mathbb{Q}(\mathscr{P})$. Let $P = (u, v)$ be constructible in one step from $\mathscr{P}$. Then $[K(u,v) : K] = 1$ or 2.*

PROOF. The point P is formed as the intersection of a line and a line, or a line and a circle or a circle and a circle. We will show that these lines and circles have equations with coefficients in K. Let's look first at lines. A line is formed by joining two distinct points (α, β), $(\gamma, \delta) \in \mathscr{P}$. The equation of this line is

$$(\gamma - \alpha)(y - \beta) = (\delta - \beta)(x - \alpha).$$

This can be rearragned as an equation of the form $ax + by = c$ where $a = \delta - \beta \in K$, $b = \alpha - \gamma \in K$ and $c = \alpha(\delta - \beta) - \beta(\gamma - \alpha) \in K$.

Now we consider a circle as in operation 2. This is centred at a point $(\alpha, \beta) \in \mathscr{P}$ and has radius the distance $\|(\gamma, \delta) - (\epsilon, \phi)\|$ where (γ, δ), $(\epsilon, \phi) \in$

$\mathscr{P}$. The equation of the circle is then

$$(x-\alpha)^2+(y-\beta)^2=(\phi-\delta)^2+(\epsilon-\gamma)^2.$$

We can rearrange this as

$$x^2+y^2+ax+by+c=0$$

where a, b, c are polynomial expressions in $\alpha,\ldots,\phi$ with coefficients in $\mathbb{Q}$ and hence belong to K.

We return to $P=(u,v)$. Suppose P is the intersection of a non-parallel lines $ax+by=c$, $a'x+b'y=c'$ with a, b, c, a', b', $c'\in K$. We can write u, v in terms of these coefficients showing that they belong to K. Thus $[K(u,v):K]=1$.

Suppose that P is a point of intersection of the line $ax+by=c$ with the circle $x^2+y^2+a'x+b'y+c'=0$ where the coefficients belong to K. Consider the case where $a\neq 0$. Then $x=-(b/a)y+c/a$, and substituting into the equation of the circle we obtain a quadratic equation for y with coefficients in K. As v is a root of this equation, we have that $[K(v):K]=1$ or 2 depending on whether the equation is reducible or irreducible over K. Now $u=-(b/a)v+c/a\in K(v)$. Hence $K(u,v)=K(v)$ showing that $[K(u,v):K]=1$ or 2. The case $a=0$ is similar.

Finally suppose that P is a point of intersection of two circles

$$x^2+y^2+ax+by+c=0,\qquad x^2+y^2+a'x+b'y+c'=0,$$

where the coefficients are in K. Subtracting the equations we obtain

$$(a-a')x+(b-b')y+(c-c')=0$$

which is the equation of a line with coefficients in K. Thus P belongs to the intersection of a circle and a line with coefficients in K and we are reduced to the previous case. □

THEOREM 136. *Let $\mathscr{P}$ be a finite set of points in $\mathbb{R}^2$ and let $K=\mathbb{Q}(\mathscr{P})$. Let P be a point constructible from $\mathscr{P}$. Then $[K(P):K]=2^r$ for some $r\geq 0$.*

PROOF. By definition, there is a sequence of points

$$P_1,P_2,P_3,\ldots,P_n$$

with $P_n=P$ such that

- P_1 is constructible in one step from $\mathscr{P}$,
- P_2 is constructible in one step from $\mathscr{P}\cup\{P_1\}$,
- P_3 is constructible in one step from $\mathscr{P}\cup\{P_1,P_2\}$,
- $\vdots$
- P_n is constructible in one step from $\mathscr{P}\cup\{P_1,P_2,\ldots,P_{n-1}\}$.

By the above lemma,

$$[\mathbb{Q}(\mathscr{P}\cup\{P_1,\ldots,P_{m+1}\}):\mathbb{Q}(\mathscr{P}\cup\{P_1,\ldots,P_m\})]=1\text{ or }2$$

for $m = 0, 1, \ldots, n-1$. Hence by the tower law,

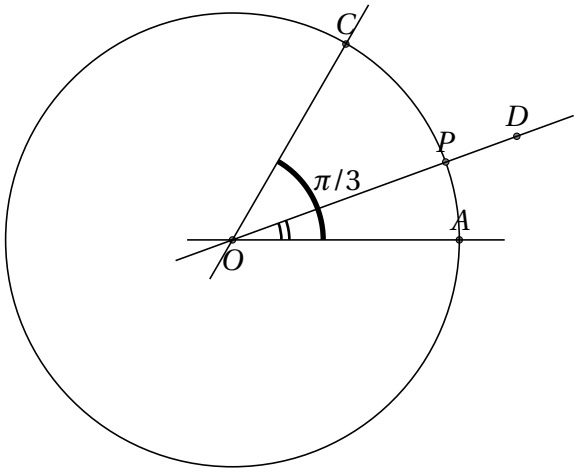
$$[\mathbb{Q}(\mathscr{P} \cup \{P_1, \ldots, P_n\}) : \mathbb{Q}(\mathscr{P})] = 2^k$$

for some $k \geq 0$. Now $K = \mathbb{Q}(\mathscr{P})$ and $K(P) = K(P_n) \subseteq \mathbb{Q}(\mathscr{P} \cup \{P_1, \ldots, P_n\})$. Thus $[K(P) : K]$ divides $[\mathbb{Q}(\mathscr{P} \cup \{P_1, \ldots, P_n\}) : \mathbb{Q}(\mathscr{P})] = 2^k$ (again by the tower law). This completes the proof. □

2. Impossibility of Trisecting Angles

THEOREM 137. *The angle $\pi/3$ cannot be trisected using ruler and compass constructions. More precisely, consider the points $A = (1,0)$, $O = (0,0)$, $C = (1/2, \sqrt{3}/2)$ (in which case $\angle AOC = \pi/3$), and let $\mathscr{P} = \{A, O, C\}$. Then there is no point D constructible from $\mathscr{P}$ such that $\angle AOD = \frac{1}{3}\angle AOC$.*

PROOF. The proof is by contradiction. Suppose that there is such a point D. Observe that $K = \mathbb{Q}(\mathscr{P}) = \mathbb{Q}(\sqrt{3})$. Let P be the point on the intersection of the line OD with the circle centred at O and passing through A (see picture).



Then P is also constructible from $\mathscr{P}$, and by Theorem 136, $[K(P) : K] = 2^r$ for some $r \geq 0$. Since $[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt{3}) : \mathbb{Q}]$ we see that $[K(P) : \mathbb{Q}] = 2^{r+1}$. Now $\mathbb{Q}(P)$ is contained in $K(P)$ and so $[\mathbb{Q}(P) : \mathbb{Q}]$ divides $[K(P) : \mathbb{Q}]$ and so equals 2^s for some $s \geq 0$.

Observe that $\angle AOP = \angle AOD = \frac{1}{3}\angle AOC = \pi/9$. As P is on the unit circle, $P = (\cos(\pi/9), \sin(\pi/9))$. Hence $\mathbb{Q}(P) = \mathbb{Q}(u, v)$ where $u = \cos(\pi/9)$ and $v = \sin(\pi/9)$. Thus $\mathbb{Q}(u)$ is a subfield of $\mathbb{Q}(P)$ and so $[\mathbb{Q}(u) : \mathbb{Q}] = 2^t$ for some $t \geq 0$.

Finally for the contradiction. For this we will use the triple angle formula

$$\cos(3\phi) = 4\cos^3(\phi) - 3\cos(\phi)$$

which is easy to prove using the formula for $\cos(A + B)$ and the double angle formulae. Letting $\phi = \pi/9$, we see that u is a root of $4x^3 - 3x = \cos(\pi/3) = 1/2$, and so is a root of $8x^3 - 6x - 1$. This polynomial is irreducible, thus $[\mathbb{Q}(u) : \mathbb{Q}] = 3$, giving a contradiction. □

3. The Impossibility of Squaring a Circle

THEOREM 138. *The circle cannot be squared using ruler and compass constructions. More precisely, let* $O = (0,0)$, $A = (1,0)$, $\mathscr{P} = \{O, A\}$. *Then there is no quadruple of points* P, Q, R, S *constructible from* $\mathscr{P}$ *and forming a square whose area equals the area of the circle centred at* O *and passing through* A.

PROOF. Again the proof is by contradiction. Observe that $\mathbb{Q}(\mathscr{P}) = \mathbb{Q}$. Let $L = \mathbb{Q}(P,Q)$. Then by Theorem 136, $[L : \mathbb{Q}] = 2^r$ for some $r \geq 0$ and in particular it is finite. However, writing $P = (a,b)$, $Q = (c,d)$, we have

$$\pi = \|P - Q\|^2 = (a-c)^2 + (b-d)^2 \in L.$$

Thus $\mathbb{Q}(\pi)/\mathbb{Q}$ is a finite extension. This contradicts the fact that π is transcendental. □

4. The Cube cannot be Doubled

EXERCISE 139. Show that the cube cannot be doubled by ruler and compass constructions in the following sense: let $O = (0,0)$, $A = (1,0)$. Show that it is impossible to construct from $\mathscr{P} = \{O, A\}$ points P, Q such that the cube with side PQ has volume twice the cube with side OA.