Algebra 146 Lecture Notes

Robert Kropholler

May 1, 2019

1. Syllabus, solution to the cubic
2. Symmetric Polynomials
3. Symmetric Polynomials and a recap on vector spaces
4. Field Extensions and degrees, minimal polynomials, $K[x]$ is a principal ideal domain
5.

Contents

1 Solutions to Polynomial equations

This course will be interested in group actions on solution sets of polynomials. To begin with lets start by looking at a few polynomials.

Firstly, let us look at a linear polynomial $a_1x + a_0 = 0$ if one first divides by a_1 we can easily see that the solution to this is

$$x = \frac{-a_0}{a_1}$$

.

We should note that this did not require us to change the field we are working over since all we did was subtract and divide. Thus if the polynomial had rational coefficients, then the solution is also a rational number.

We should also note that we can always assume that the coefficient of x^n is 1 in a degree n polynomial without changing the solutions or changing the field.

We now look degree 2 polynomials. Since we can assume the coefficient of x^2 is 1 we are solving the equation $x^2 + a_1x + a_0 = 0$. We can solve this easily using the quadratic formula but lets go through the steps.

$$\begin{aligned} x^2 + a_1x + a_0 = (x + \frac{a_1}{2})^2 + (-\frac{a_1^2}{4} + a_0) = 0 \\ \Leftrightarrow (x + \frac{a_1}{2})^2 = \frac{a_1^2}{4} - a_0 \\ \Leftrightarrow x + \frac{a_1}{2} = \pm\sqrt{\frac{a_1^2}{4} - a_0} \\ \Leftrightarrow x = \frac{a_1 \pm \sqrt{a_1^2 - 4a_0}}{2} \end{aligned}$$

It is clear that this takes us outside the field that we originally started with. For instance the polynomial $x^2 - 2$ does not have rational solutions. One trick we should pick up on is that we can arrange the coefficient of x^{n-1} to be 0.

Let us try and solve the cubic now. We are looking at the polynomial $x^3 + a_2x^2 + a_1x + a_0$. Starting with the substitution $x = y - \frac{a_2}{3}$ we get the

polynomial $y^3 + (a_1 - \frac{a_2^2}{3})y + (\frac{2a_2^3}{27} - \frac{a_1 a_2}{3} + a_0)$. Let $b = \left(a_1 - \frac{a_2^2}{3}\right)$ and $c = \left(\frac{2a_2^3}{27} - \frac{a_1 a_2}{3} + a_0\right)$.

Thus we are solving the polynomial y^3+by+c. We then make the substitution $y = z - \frac{b}{3z}$, to arrive at the equation

$$z^3 - \frac{b^3}{27z^3} + c.$$

We can now multiply by z^3 and we are solving the polynomial

$$z^6 + cz^3 - \frac{b^3}{27}.$$

Which actually is a quadratic in z^3 and so we get solutions

$$z^3 = \frac{-c \pm \sqrt{c^2 + \frac{4b^3}{27}}}{2}.$$

Let $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ note that $\omega^3 = 1$.

We then get the solutions

$$z = \omega^i \left(\frac{-c \pm \sqrt{c^2 - \frac{4b^3}{27}}}{2}\right)$$

for $i = 1, 2, 3$.

We now have to substitute back to get a solution for x. After some work (skipped here!) we arrive at what is known as Cardano's formula for the three solutions.

$$y = \omega^i \sqrt[3]{-\frac{c}{2} + \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}} + \omega^{3-i} \sqrt[3]{-\frac{c}{2} - \sqrt{\frac{c^2}{4} + \frac{b^3}{27}}}.$$

$$x = -\frac{a_2}{3} + \omega^i \sqrt[3]{-\frac{\left(\frac{2a_2^3}{27} - \frac{a_1 a_2}{3} + a_0\right)}{2} + \sqrt{\frac{\left(\frac{2a_2^3}{27} - \frac{a_1 a_2}{3} + a_0\right)^2}{4} + \frac{\left(a_1 - \frac{a_2^2}{3}\right)^3}{27}}}$$

$$+ \omega^{3-i} \sqrt[3]{-\frac{\left(\frac{2a_2^3}{27} - \frac{a_1 a_2}{3} + a_0\right)}{2} - \sqrt{\frac{\left(\frac{2a_2^3}{27} - \frac{a_1 a_2}{3} + a_0\right)^2}{4} + \frac{\left(a_1 - \frac{a_2^2}{3}\right)^3}{27}}}.$$

And now you know why noone told you this formula!

The point of this exercise not being the actual algebra but the result in that we can solve a cubic using the operations $+, -, \times, \div, \sqrt[n]{}$. We should also note that the complexity of this process is rapidly ballooning. It is possible to do this for a quartic polynomial (we won't do that here for details see: Quartic Solution)

During the course we will see that this is in fact as far as one can go and that there is no solution to the quintic using the above operations.

2 Recap

Definition 2.1. A *commutative ring* is a set R with two binary operations $+, \times$ satisfying the following axioms.

- $(R, +)$ is an Abelian group.
- There is an identity 1 such that $1 \times r = r = r \times 1$ for all $r \in R$.
- $\times$ is commutative.
- $r \times (a + b) = (r \times a) + (r \times b)$ and $(a + b) \times r = (a \times r) + (b \times r)$.

We will be interested in two type of rings. The first is polynomial rings.

Definition 2.2. Let R be a ring. The *polynomial ring over* R is $R[x]$ is the set of polynomials in x with coefficients in R.

We define the polynomial ring in n variables inductively by $R[x_1, \ldots, x_n] = R[x_1, \ldots, x_{n-1}][x_n]$

The other type of rings we will be interested are fields.

Definition 2.3. A ring K is a *field* if every non-zero elements has a multiplicative inverse.

Lemma 2.4. *Let K be a field and $I \subset K$ be an ideal. Then $I = \{0\}$ or $I = K$.*

Proof. Suppose that $I \neq \{0\}$, then there is an element $r \in I$ such that $r \neq 0$. Then r has an inverse s so $rs = 1 \in I$. Thus $rsa = 1a = a \in I$ for all $a \in K$ and $I = K$. □

Remark 1. Every ring homomorphism will send the multiplicative identity to the multiplicative identity.

Corollary 2.5. *Let $\varphi \colon K \to L$ be a ring homomorphism between 2 fields K, L. Then φ is injective.*

Definition 2.6. Let K be a field. Then there is 1 homomorphism $\mathbb{Z} \to K$. Namely, $\varphi(1) = 1$. The *prime subfield of* K is the smallest subfield of K containing the image of φ.

The prime subfield is either $\mathbb{Z}/p\mathbb{Z}$ for some prime p or $\mathbb{Q}$. We define the *characteristic of* K is p if the prime subfield if $\mathbb{Z}/p\mathbb{Z}$ and 0 if the prime subfield is $\mathbb{Q}$.

3 Irreducibility Criteria

Definition 3.1. A polynomial f is *irreducible* if whenever $f = gh$, then either $\deg(g) = 0$ or $\deg(h) = 0$.

A polynomial f *divides* a polynomial g, written $f|g$, if there is a polynomial h such that $g = fh$.

A polynomial f is *prime* if whenever $f|gh$, then $f|g$ or $f|h$.

Recall that an ideal I is said to be prime, if whenever $ab \in I$, then $a \in I$ or $b \in I$. We can see from the above definition that a polynomial f is prime if and only if (f) is a prime ideal.

Proposition 3.2. *Let K be a field and $f, g \in K[x]$ with $\deg(g) \geqslant 1$. Then there are polynomial $q, r \in K[x]$ such that $f = gq + r$ and $\deg(r) < \deg(g)$.*

Corollary 3.3. *Let K be a field, $a \in K$. Then given a polynomial f we have that $f(a) = 0$ if and only if $x - a$ divides $f(x)$.*

We will be interested in polynomials over $\mathbb{Q}$. Since we can always multiply through by a common denominator we can equivalently study polynomials over $\mathbb{Z}$.

Theorem 3.4. *Let f be a polynomial in $\mathbb{Q}[x]$ with coefficients in $\mathbb{Z}$. Then f is irreducible over $\mathbb{Q}$ if and only if f is irreducible over $\mathbb{Z}$.*

Theorem 3.5. *Let $f(x) = a_n x^n + \cdots + a_1 x + a_0$. Suppose that p is a prime number and that $p|a_i$ for $0 < i < n$ and $p \nmid a_n$ and $p^2 \nmid a_0$. Then f is irreducible.*

Theorem 3.6. *Given a polynomial in $\mathbb{Z}[x]$ we can consider the reduction mod p for a prime p. This gives a polynomial $\bar{f} \in \mathbb{F}_p[x]$. Then if $\bar{f}$ is irreducible, then f is irreducible.*

There are other tricks we will see throughout the course.

4 Group Actions on Rings

Definition 4.1. A group G acts on a ring R if G acts on R and for each $g \in G$ the bijection ρ_g is a ring homomorphism.

This amounts to a group homomorphism from G to the group $\mathrm{Aut}(R)$ of ring isomorphisms $R \to R$.

Lemma 4.2. *Let G be a group acting on a ring R.*

1. *Let $R^G = \{r \in R \mid g \cdot r = r, \forall g \in G\}$. Then R^G is a subring of R.*
2. *If R is a field, then R^G is a subfield, which contains the prime subfield.*

Proof. We see that $\rho(g, r - s) = \rho(g, r) - \rho(g, s) = r - s$ for all $r, s \in R^G$ and all $g \in G$. Similarly $\rho(g, rs) = \rho(g, r)\rho(g, s) = rs$ for all $r, s \in R^G$ and all $g \in G$. $\square$

4.1 Symmetric Polynomials

Given a polynomial ring in n variables, $R[x_1, \ldots, x_n]$, there is an action of the symmetric group S_n given by $\rho(\sigma, r) = r$ for all $r \in R$ and $\rho(\sigma, x_i) = x_{\sigma(i)}$, then extend in the obvious way to all polynomials.

Definition 4.3. The *symmetric polynomials* are the polynomials in $R[x_1, \ldots, x_n]^{S_n}$.

There are certain obvious symmetric polynomials, namely the elementary symmetric polynomials s_i. There are n symmetric polynomials in $R[x_1, \ldots, x_n]^{S_n}$ which are as follows.

$$\begin{aligned}
s_1 &= x_1 + x_2 + \cdots + x_n \\
s_2 &= \sum_{i<j} x_i x_j \\
&\vdots \\
s_k &= \sum_{i_1<i_2<\cdots<i_k} x_{i_1} x_{i_2} \ldots x_{i_k} \\
&\vdots \\
s_n &= x_1 x_2 \ldots x_n.
\end{aligned}$$

These symmetric polynomials have come up before as the coefficients of a polynomials whose roots are $-x_i$, namely,

$$\prod_{i=1}^{n}(x + x_i) = x^n + s_1 x^{n-1} + \ldots s_k x^{n-k} + \cdots + s_n.$$

This means that if we are trying to find the roots α_i of a polynomial $f(x)$ we can see this as solving n equations which are the elementary symmetric polynomials in α_i being set equal to the coefficients.

We also have the following theorem, showing that understanding the elementary symmetric polynomials give a complete understanding of the symmetric polynomials.

Theorem 4.4. *The symmetric polynomials $R[x_1, \ldots, x_n]^{S_n}$ are generated by R and $s_1, \ldots, s_n$.*

Proof. We define an ordering on the monomials of $R[x_1, \ldots, x_n]$ by $x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n} < x_1^{b_1} x_2^{b_2} \ldots x_n^{b_n}$ if $a_1 < b_1$ or ($a_1 = b_1$ and $a_2 < b_2$) or ($a_1 = b_1$ and $a_2 = b_2$ and $a_3 < b_3$)....

Given a symmetric polynomial $f(x)$ consider the monomial $m(x)$ in $f(x)$ which is largest in the above ordering, this is of the form $x_1^{a_1} x_2^{a_2} \ldots x_n^{a_n}$. Notice that this is also the largest monomial in the symmetric polynomial $\rho(x) = s_1^{a_1 - a_2} s_2^{a_2 - a_3} \ldots s_n^{a_n}$. Let r be the coefficient of $m(x)$ in $f(x)$. Let $g(x) = f(x) - r\rho(x)$. This is symmetric since it is the sum of two symmetric polynomials.

Also every monomial in $g(x)$ is smaller than $m(x)$. We can then repeat this procedure with $g(x)$ and we will eventually arrive at the 0 polynomial. This completes the proof. □

Example. Consider the polynomial $x_1^2 + x_2^2 \in \mathbb{Z}[x_1, x_2]$. This is clearly symmetric so we can apply the above proof to write it in the symmetric polynomials $s_1 = x_1 + x_2$ and $s_2 = x_1 x_2$.

We see that x_1^2 is the largest monomial, so we will look at the symmetric polynomial $s_1^2 = (x_1 + x_2)^2 = x_1^2 + 2x_1x_2 + x_2^2$. Then $g(x) = f(x) - x_1^2 + 2x_1x_2 + x_2^2 = -2x_1x_2 = -2s_2$. Thus $x_1^2 + x_2^2 = s_1^2 - 2s_2$.

Example. Suppose that $x_1 + x_2 = 12$ and $x_1^2 + x_2^2 = 4$, then $x_1^k + x_2^k$ is an integer for all k.

We are given the equality $s_1 = 12$ and $s_1^2 - 2s_2 = 4$, from this we recover $s_2 = -70$. Now we can write any symmetric polynomial in terms of s_1 and s_2. Thus $x_1^k + x_2^k$ is an integer for all k.

5 Vector spaces

Definition 5.1. A *vector space over a field* K is a set V together with a binary operation $+ \colon V \times V \to V$ and a multiplication $\tau \colon K \times V \to V$ satisfying the following for all $v, w \in V$ and $a, b \in F$:

- $(V, +)$ is an Abelian group.
- $\tau(ab, v) = \tau(a, \tau(b, v))$.
- $\tau(a + b, v) = \tau(a, v) + \tau(b, v)$.
- $\tau(a, v + w) = \tau(a, v) + \tau(b, w)$.
- $\tau(1, v) = v$.

We usually drop τ and write av for $\tau(a, v)$.

This generalises the notion of vector space over the real numbers and we can work over any field. Every theorem you have learnt about vector spaces over the real numbers applies to vector spaces over an arbitrary field. For instance, we have the following definitions.

Definition 5.2. A set S is a *spanning set* for V if every element of V is a finite linear combination of elements of S. I.e. given an element of V there are elements of the field $a_1, \ldots, a_n$ and elements $s_1, \ldots, s_n$ of S such that $v = \sum_{i=1}^n a_i s_i$.

Definition 5.3. We say that a set S is linearly independent if whenever we have elements of $\{s_1, \ldots, s_n\}$ of the set S such that $\sum_{i=1}^n a_i s_i = 0$, then $a_i = 0$ for all i.

Definition 5.4. We say that a set is a *basis* if it is a linearly independent spanning set.

Lemma 5.5. *Suppose that S and T are bases of the vector space V, then there is a bijection $S \to T$.*

The proof of the above lemma is similar to the same as the case when the field is $\mathbb{R}$. You should have seen the finite dimensional version, the infinite dimensional version is similar.

Definition 5.6. The *dimension* of a vector space is the size of any basis.

6 Field Extensions

Definition 6.1. A *field extension* L/K is an injection $\varphi\colon K \to L$. We will sometimes write $\begin{matrix} L \\ | \\ K \end{matrix}$

Definition 6.2. The *degree of the extension* L/K is written $[L : K]$, is the dimension of L as a K vector space.

Proposition 6.3. *Let L/K and M/L be field extensions. Then $[M : K] = [M : L][L : K]$.*

Proof. We shall only be concerned with the case that $[M : L]$ and $[L : K]$ are finite. Let $l_1, \ldots, l_a$ be a basis for L/K and let $m_1, \ldots, m_b$ be a basis for M/L. Then $l_i k_j$ is a basis for M/K.

Let x be an element of M, then $x = y_1 m_1 + y_2 m_2 + \cdots + y_b m_b$. Where $y_j \in L$. Now each $y_j = z_{j,1} l_1 + \cdots + z_{j,a} l_a$. Thus $l_i k_j$ forms a spanning set for M/K.

We must now check that this set is linearly independent. Suppose that we have $y_{i,j}$ not all zero such that

$$\sum_{i=1}^{a} \sum_{j=1}^{b} y_{i,j} l_i m_j = 0.$$

Then factoring out the terms for each m_j we find that $\sum_{i=1}^{a} y_{i,j} l_i = 0$ for all j since the m_j are linearly independent. Also since the l_i are linearly independent we see that $\sum_{i=1}^{a} y_{i,j} l_i = 0$ implies that $y_{i,j} = 0$ for all i, j. □

Definition 6.4. We say that an element a in a field extension L/K is *algebraic* if $f(a) = 0$ for some $f(x) \in K[x]$. Otherwise, a is *transcendental*.

Proposition 6.5. *Given an algebraic element a of a field extension L/K. There is a unique monic irreducible polynomial $m_a(x) \in K[x]$ such that:*

- $m_a(a) = 0$
- *If* $f(x) \in K[x]$ *is such that* $f(a) = 0$*, then* $m_a(x)$ *divides* $f(x)$*.*

$m_a(x)$ *is called the* minimal polynomial for a*.*

Proof. We can replace any polynomial which a satisfies with a monic polynomial by dividing through by the coefficient of the highest power.

Let $m_a(x)$ be a monic polynomial which a satisfies such that $1 \leqslant \deg m_a(x)$ and for any polynomial $g(x)$ such that $g(a) = 0$ we have $\deg g(x) \geqslant \deg m_a(x)$. We will show that this polynomial is irreducible, unique and satisfies the division property above.

Irreducible: Suppose that $m_a(x)$ is not irreducible. Then $m_a(x) = h_1(x)h_2(x)$ where $1 \leqslant \deg h_i(x) < \deg m_a(x)$. Then $0 = m_a(a) = h_1(a)h_2(a)$. Thus we can assume that $h_1(a) = 0$, contradicting the minimal degree assumption.

Uniqueness: Suppose that $g(x)$ is another monic irreducible polynomial such that $g(a) = 0$. By the division algorithm we can write $g(x) = h(x)m_a(x) + r(x)$, where $\deg r(x) < \deg m_a(x)$ or $r = 0$. Evaluating at a we see that $0 = g(a) = h(a)m_a(a) + r(a) = 0 + r(a)$. Thus $r(a) = 0$ however by minimality of the degree of $m_a(x)$ we see that $r(x)$ is the zero polynomial. Thus $g(x) = h(x)m_a(x)$ but $g(x)$ is irreducible so $h(x)$ is a constant which much be 1 since both $g(x)$ and $m_a(x)$ are monic.

Division: Let $f(x)$ be any polynomial such that $f(a) = 0$. Then we have that $f(x) = h(x)m_a(x) + r(x)$ where once again $\deg r(x) < \deg m_a(x)$ or $r = 0$. Since $f(a) = 0$ we see that $r(a) = 0$ and by minimality of $\deg m_a(x)$ we have that $r(x) = 0$ and $f(x) = h(x)m_a(x)$, thus $m_a(x)$ divides $f(x)$. □

Definition 6.6. We call the polynomial $m_a(x)$ the *minimal polynomial* for a.

Definition 6.7. A field extension is *algebraic* if every element is algebraic. Otherwise, it is *transcendental*.

Note that every finite extension is algebraic, however the converse of this is not true. We will mostly be interested in finite algebraic extensions.

6.1 Ideals in $K[x]$

Definition 6.8. Let R be a ring and let I be an ideal. We say that I is *principal* if it is generated by 1 element.

We say that R is a *principal ideal domain* (PID) if every ideal is principal.

The easiest example of a principal ideal domain is $\mathbb{Z}$.

Lemma 6.9. *Let* K *be a field. Then* $K[x]$ *is a principal ideal domain.*

Proof. Let I be an ideal of $K[x]$. If $I = \{0\}$, then I is generated by 0.

Suppose that $I \neq \{0\}$. Let $f(x)$ be an element of I of minimal degree. Suppose that $g(x) \in I$. By the division algorithm we see that $g(x) = a(x)f(x) + b(x)$ where $\deg b(x) < \deg g(x)$ or $b = 0$. Since $g(x)$ and $a(x)f(x)$ are both in I we see that $b(x) \in I$, by minimality of the degree of $f(x)$ we see that $b = 0$. Thus $g(x) \in (f(x))$ and I is principal generated by $f(x)$. □

Definition 6.10. An ideal I of a ring R is *prime* if whenever $ab \in I$, then $a \in I$ or $b \in I$.

An ideal I of a ring R is *maximal* if whenever J is an ideal of R such that $I \subset J$, then $J = I$ or $J = R$.

We can reword both these conditions in terms of conditions on the corresponding quotients R/I. '

Theorem 6.11. *Let R be a ring and I and ideal. Then*

1. *I is prime if and only if R/I is an integral domain.*
2. *I is maximal if and only if R/I is a field.*

Proof. Prime ideals: Suppose that I is a prime ideal and $ab + I = 0 + I$ in R/I. Thus $ab \in I$ and since I is prime we see that either $a \in I$ or $b \in I$, so at least one of $a + I$ or $b + I$ equals $0 + I$.

Suppose that R/I is an integral domain and $ab \in I$. Then $(a + I)(b + I) = ab + I = 0 + I$. Since R/I is an integral domain we see that either $a + I = 0 + I$ or $b + I = 0 + I$. Thus $a \in I$ or $b \in I$ so I is a prime ideal.

Masimal ideals: Suppose that I is a maximal ideal. Let $a \notin I$ so $a + I \neq 0 + I$ consider the set $J = \{ar + b \mid r \in R, b \in I\}$. This is an ideal of R containing I. Since $a \in J$ we see that $J = R$. Thus there is an $r \in R$, $b \in I$ such that $ar + b = 1$. In R/I we have the equality $1 + I = (ar + b) + I = ar + I = (a + I)(r + I)$. Thus $a + I$ has a multiplicative inverse and R/I is a field.

Suppose that R/I is a field. Suppose that J is an ideal of R and $I \subsetneq J$. Let $b \in J \setminus I$, then $b + I \neq 0 + I$ so we have a multiplicative inverse $c + I$ such that $(b + I)(c + I) = bc + I = 1 + I$. Thus $1 - bc \in I \subset J$ so $1 - bc + bc = 1 \in J$ and $J = R$. Thus I is a maximal ideal. □

Theorem 6.12. *Let K be a field and $f(x) \in K[x]$. Then the following are equivalent:*

1. *$f(x)$ is irreducible.*
2. *$(f(x))$ is a prime ideal.*
3. *$(f(x))$ is a maximal ideal.*

Proof. 3) $\Rightarrow$ 2): since any field is an integral domain.

2) $\Rightarrow$ 1): Note that any polynomial in $(f(x))$ has degree $\geqslant \deg f(x)$. Suppose that $f(x)$ is reducible, then $f(x) = a(x)b(x)$ and $\deg a, \deg b < \deg f$ but since $(f(x))$ is a prime ideal at least one of $a(x)$ or $b(x)$ is in $(f(x))$ this contradicts our initial observation.

1) $\Rightarrow$ 3): Suppose that $f(x)$ is irreducible. Let J be an ideal of $K[x]$ such that $(f(x)) \subset J$. Then J is generated by one element $g(x)$. Thus we have that $f(x) = g(x)h(x)$ but since $f(x)$ is irreducible we see that $g(x)$ is a constant so $J = K[x]$ or $h(x)$ is a constant and so $g(x) \in (f(x))$ and $J = (f(x))$ thus $(f(x))$ is maximal. □

6.2 Simple Extensions

Definition 6.13. Let M/K be a field extension and let $a \in M$. The *simple extension* generated by a, denoted $K(a)$ is the smallest subfield of M containing both K and a. More generally for a subset S, $K(S)$ denotes the smallest subfield containing K and S.

Theorem 6.14. *Given a field K and a monic irreducible polynomial $m \in K[x]$, there exists a field extension M/K with the following properties:*

1. *$M = K(\alpha)$ for some element $\alpha \in M$.*
2. *The minimal polynomial for α is m.*
3. *$[M : K] = \deg m$*

Proof. For 1) since $m(x)$ is irreducible, we define M to be the field $K[x]/(m(x))$. Let $I = (m(x))$ and $\alpha = x + I \in M$. We will show that this has the desired properties.

Firstly $M = K(\alpha)$, since $K[x]$ is generated by K and x we see that M is generated by the image of K and the image of x. Thus we see that $M = K(\alpha)$.

One can check that if $f(x) \in K[x]$ is a polynomial, then $f(x+I) = f(x)+I$. Thus we see that since $m(x) \in I$ we see that $m(\alpha) = m(x) + I = I$ and that α satisfies m. Since it is irreducible and monic, it is the minal polynomial for α.

We will abuse notation and write k for the element $k + I$ for $k \in K$. This is allowable, since the K is a subfield of M. Let $n = \deg m$ and consider the set $B = \{1, \alpha, \alpha^2, \ldots, \alpha^{n-1}\}$. We will show that B is a basis. Firstly, we will show that it is linearly independent, suppose that we have an equation $k_0 + k_1\alpha + \cdots + k_{n-1}\alpha^{n-1} = 0$. This gives a polynomial equation which α satisfies with degree smaller than n so we reach a contradiction.

To show that the set B spans M, it suffices to show that we can write arbitrary powers of α as linear combinations of elements of B.

Let $m(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0$. Then $\alpha^n = -(a_{n-1}\alpha^{n-1} + \cdots + a_0)$. For higher powers we can reduce the highest power by writing $\alpha^k = \alpha^{k-n}\alpha^n$. Thus we can obtain any positive power.

To obtain negative powers note that $\dfrac{1}{\alpha} = \dfrac{-1}{a_0}(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1)$. Thus we can write any negative power in terms of positive powers and we are done. □

Theorem 6.15. *Given L/K and $\alpha \in L$ algebraic over K, the simple extension $K(\alpha)$ of K in L is isomorphic to the extension constructed above using the minimal polynomial m_α of α over K.*

Proof. Define a homomorphism $\varphi\colon K[x] \to L$ by $\varphi(k) = k$ and $\varphi(x) = \alpha$. The image of this homomorphism is the subfield generated by K and α which is $K(\alpha)$.

The kernel of this homomorphism is the set of polynomials which vanish on α. Each such polynomial is divisible by m_α. Thus we see that the ideal is exactly (m_α) and $K(\alpha) = K[x]\Big/(m_\alpha)$. □

Given two fields K, L and a homomorphism $i\colon K \to L$ there is a homomorphism $i\colon K[x] \to L[x]$, defined by sending the polynomial $i(a_n x^n + \cdots + a_1 x + a_0) = i(a_n)x^n + \cdots + i(a_1)x + i(a_0)$.

Theorem 6.16. *Let M/K be a field extension, where $\alpha \in M$ is algebraic over K with minimal polynomial m. Let $i\colon K \to L$ be a field homomorphism and $\beta \in L$. Then there is a homomorphism $j\colon K(\alpha) \to L$ with the following properties:*

$$j\big|_K = i$$
$$j(\alpha) = \beta$$

if and only if $i(m)(\beta) = 0$.

Proof. Suppose that there is a homomorphism satisfying the above conditions, then $0 = j(m(\alpha)) = i(m)(j(\alpha)) = i(m)(\beta)$. Thus we see that the condition is necessary.

To see that the condition is sufficient. We define a homomorphism $\varphi\colon K[x] \to L$ by $\varphi(k) = i(k)$ and $\varphi(x) = \beta$. We see that the kernel is exactly the polynomials $f(x)$ such that β satisfies $i(f)$. This means that the kernel is $(m(x))$ since this is a maximal ideal. Thus the first isomorphism theorem gives a homomorphism $K[x]\big/(m(x)) \to L$. □

Example. Let $K = \mathbb{Q}$ and let $M = \mathbb{R}$ and let $\alpha = \sqrt{2}$. Then there is a homomorphism $\varphi\colon \mathbb{Q}(\alpha) \to \mathbb{R}$ given by $\varphi|_{\mathbb{Q}} = \mathrm{id}$ and $\varphi(\alpha) = -\sqrt{2}$, since $(-\sqrt{2})^2 - 2 = 0$.

There is not a homomorphism $\psi\colon \mathbb{Q}(\alpha) \to \mathbb{Q}(i)$ given by $\psi|_{\mathbb{Q}} = \mathrm{id}$ and $\psi(\alpha) = i$ since i does not satisfy $x^2 - 2$.

Corollary 6.17. *Suppose we have a field extension M/K with $\alpha, \beta \in M$ both algebraic over K with the same minimal polynomial $m \in K[x]$. Then there is an isomorphism $j\colon K(\alpha) \to K(\beta)$ with $j\big|_K = \mathrm{id}$.*

Proof. This follows from the above theorem by setting $i = \mathrm{id}$ □

Corollary 6.18. *Suppose that the irreducible polynomial $m(x)$ has n roots in the field extension M/K. Suppose that α is one of these roots. Then there are exactly n homomorphisms $j\colon K(\alpha) \to M$. Such that $j|_K = \mathrm{id}$.*

7 Splitting Fields

Definition 7.1. A polynomial $f(x) \in K[x]$ *splits completely* over the field extension L/K if when considered as a polynomial in $L[x]$ it factors into a product of linear terms. i.e. $f(x) = a\prod_{i=1}^{n}(x - \alpha_i)$.

Equivalently, $f(x)$ splits completely over L if L contains all the roots of $f(x)$.

Example. The polynomial $x^2 - 2$ does not split completely over $\mathbb{Q}$ but it does over $\mathbb{R}$ or $\mathbb{C}$ or $\mathbb{Q}(\sqrt{2})$

Definition 7.2. We say that a field extension L/K is the *splitting field* of the polynomial $f(x) \in K[x]$ if $f(x)$ splits completely over L and does not split completely over any field extension M/K such that $M \subset L$.

Example. The splitting field of $x^2 - 2$ is $\mathbb{Q}(\sqrt{2})$. Since this polynomial splits completely in this field and for degree reasons there are no smaller fields.

Theorem 7.3. *Let $f(x)$ be a polynomial in $K[x]$.*

1. *There is a splitting field L/K for $f(x)$.*
2. *Given any two splitting fields $L/K, M/K$ there is an isomorphism $\varphi\colon L \to M$ such that $\varphi\big|_K = \mathrm{id}_K$.*

If one was working in the field $\mathbb{Q}$ the easiest way to find the splitting field would be to adjoin all the roots of the polynomial $f(x)$ i.e. the field $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$. In general we can do this by taking repeated simple extensions.

Proof. We will prove both statements by induction. Noting that both are true for degree 1 polynomials. In which case the splitting field is K.

For the first statement, the induction hypothesis is as follows. Assume that given a polynomial of degree $< n$ over a field L there exists a splitting field for $f(x)$ over L.

Suppose that $f(x)$ is degree n. Let $f_1(x)$ be an irreducible factor of $f(x)$. Consider the field $K(\alpha)$ where α is a root of $f_1(x)$. Over $K(\alpha)$ we see that $f(x) = (x - \alpha)^m g(x)$. Now the degree of $g(x)$ is $n - m$. Thus there is a field extension $L/K(\alpha)$ which is a splitting field for $g(x)$. Then $f(x)$ splits over L as well.

Take the smallest subfield of L over which $f(x)$ splits. This is the splitting field for $f(x)$.

The statement of part 2 is not obvious as we made some choices throughout.

The induction hypothesis for this one is suppose that $f(x)$ is a polynomial over a field K with degree $< n$ and suppose that $i\colon K \to K'$ is an isomorphism. Let $f'(x)$ be the corresponding polynomial over K'. let L/K be a splitting field for $f(x)$ and L'/K' be a splitting field for $f'(x)$. Then there is an isomorphism $j\colon L \to L'$ such that $j\big|_K = i$.

Let $g(x)$ be a polynomial of degree n over K and suppose that $i\colon K \to K'$ is an isomorphism. Let $g_1(x)$ be an irreducible component of $g(x)$, and $g_1'(x)$ the corresponding irreducible polynomial over K'. Consider the simple extensions $K(\alpha), K'(\beta)$ obtained by joining a root of $g_1(x)$ and $g_2(x)$ respectively. By uniqueness of simple extensions there is an isomorphism $K(\alpha) \to K'(\beta)$ extending i.

The splitting field $L/K(\alpha)$ of $g(x)/(x - \alpha)$ and $L'/K'(\beta)$ of $g'(x)/(x - \beta)$ are isomorphic by the induction hypothesis. This isomorphism extending i. We can also see that these are the splitting fields of $g(x)$ and $g'(x)$ over K and K' respectively. □

8 Normal Extensions

Definition 8.1. A field extension L/K is *normal* if any irreducible polynomial $f(x)$ with a root in L splits completely.

Example. The field extensions $\mathbb{Q}(\sqrt{2})/\mathbb{Q}, \mathbb{Q}(i)/\mathbb{Q}$ are both normal since if a quadratic has a root in a field, then it splits completely. In general extension of degree 2 are normal.

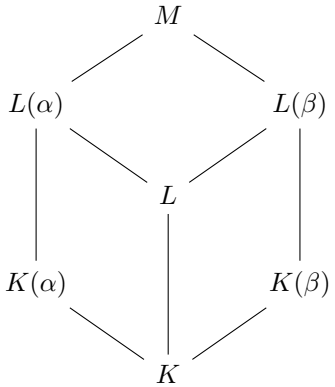
Non Example. The field $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not a normal extension. The polynomial $x^3 - 2$ has a root over this field but but since the other two roots of this polynomial are not real number we see that they are not elements of $\mathbb{Q}(\sqrt[3]{2})$ in which all elements are real numbers.

Theorem 8.2. *A field extension L/K of finite degree is normal if and only if it is the splitting field of some polynomial.*

Proof. Suppose that L/K has finite degree and is normal. We can then find a set of elements $\alpha_1, \ldots, \alpha_n$ such that $L = K(\alpha_1, \ldots, \alpha_n)$ Let $m_i(x)$ be the minimal polynomial of α_i. Let $f(x) = \prod_{i=1}^{n} mm_i(x)$. Since each of the irreducible polynomials $m_i(x)$ has a root in L and L is normal. We see that each $m_i(x)$ splits completely in L. Thus we see that $f(x)$ splits completely in L. Wince any field over which $f(x)$ splits completely must contain $\alpha_1, \ldots, \alpha_n$ we see that L is the splitting field for $f(x)$.

Suppose that L/K is the splitting field for the polynomial $f(x)$. Suppose that $g(x)$ is an irreducible polynomial with a root $\alpha \in L$. Let M be the splitting field of $g(x)$ and β be a root in M.

The fields $K, L, M, K(\alpha), K(\beta), L(\alpha), L(\beta)$ fit into the following diagram where a field above another field denotes a field extension.



We will calculate the degrees of the various extensions. Let $d = \deg g(x)$, thus we have $[K(\alpha) : K] = [K(\beta) : K] = d$.

Also since $L(\alpha)$ is the splitting field of $f(x)$ over $K(\alpha)$ and $L(\beta)$ is the splitting field of $f(x)$ over $L(\beta)$ we see that there is an isomorphism $L(\alpha) \to L(\beta)$ extending the isomorphism $K(\alpha) \to K(\beta)$. Thus $[L(\alpha) : K(\alpha)] = [L(\beta) : K(\alpha)] = c$

We see that $[L(\alpha) : L] = 1$ since $\alpha \in L$. Thus we get the following equality

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

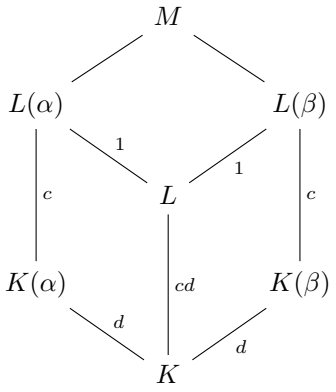
and deduce that $[L : K] = cd$.

We also have the equality

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

from which we deduce that $[L(\beta) : L] = 1$. Thus we see that $\beta \in L$ and the proof is complete.

We summarise these degrees in another diagram.



□

Normal extensions are going to be a key point of interest for us going forward.

9 Separable Extensions

Definition 9.1. An irreducible polynomial is *separable* if all its roots are distinct in any splitting field.

A polynomial is *separable* if all its irreducible components are separable.

An element $\alpha \in L/K$ is *separable* if its minimal polynomial is a separable polynomial.

An extension L/K is *separable* if every element in the extension is separable.

Most extension we will meet will be separable. It turns out that this property has many nice consequences. We start by giving an example of a non separable polynomial.

Non Example. Let $\mathbb{F}_3(t)$ be the field of functions of the form $\frac{f(x)}{g(x)}$ where f, g are polynomials with coefficients in $\mathbb{F}_3$. Consider the polynomial $f(x) = x^3 - t$. This polynomial is irreducible. Suppose that α is a root of this polynomial i.e. $\alpha^3 = t$. Then we can check that $f(x) = (x - \alpha)^3$ since we get $(x - \alpha)^3 = x^3 - 3\alpha x^2 + 3\alpha^2 x + \alpha^3 = x^3 - t$. Since $3a = 0$ for all elements of the ring.

This problem disappears over both finite fields and fields of characteristic 0. These are the fields we will be interested in for the remainder of the course.

Proposition 9.2. *Suppose that $f(x)$ is an irreducible monic polynomial in a field K of characteristic 0. Then $f(x)$ is separable.*

Thus every extension is separable in characteristic 0.

Proof. Let $f(x) = a_n x^n + \cdots + a_0$. Then $D(f) = na_n x^{n-1} + \cdots + a_1$. If $f(x)$ has a multiple root, then $f(x)$ and $D(f)$ have a common root, α. Since $f(x)$ is irreducible and monic we see that it is the minimal polynomial of α and thus if α is a root of $D(f)$ we must have $f(x)$ divide $D(f)$ but this cannot be the case for degree reasons unless $D(f) = 0$, this cannot be the case since $na_n \neq 0$. □

Theorem 9.3. *Suppose that L/K is a separable extension of finite degree. Then it is a simple extension.*

Proof. Since L/K is a finite extension it is generated by finitely many elements. So $L = K(\alpha_1, \ldots, \alpha_n)$. By induction it is enough to prove that $K(\alpha, \beta)$ is a simple extension.

We will prove the case of finite fields later when we completely classify finite fields. So for now suppose that K is infinite.

Let $f(x)$ be the minimal polynomial of α_1 and $g(x)$ be the minimal polynomial of β over K. Suppose that over the splitting field $M \supset L$ the roots of $f(x)$ are $\alpha = \alpha_1, \ldots, \alpha_a$ and the roots of $g(x)$ are $\beta = \beta_1, \ldots, \beta_b$. Since these polynomials are separable. These are distinct roots and $b = \deg g$ and $a = \deg f$.

Pick $c \in K$ such that $\alpha_i + c\beta_j$ are all different elements of M. This is possible since K is infinite and the ratios $\dfrac{\alpha_i - \alpha_{i'}}{\beta_1 j' - \beta_j}$ takes only finitely many values.

We claim that $\gamma = \alpha + c\beta$ is a generating element for $K(\alpha, \beta)$ i.e. $K(\gamma) = K(\alpha, \beta)$.

Let $h(x) = f(\gamma - cx)$. We can see that $h(x)$ has β as a root. We also see that no other β_j is a root of $h(x)$, since $h(\beta_j) = f(\gamma - c\beta_j) = f(\alpha + c(\beta - \beta_j))$ which is zero if and only if $\beta_j = \beta$.

Thus over the splitting M we can write the highest common factor of $g(x)$ and $h(x)$ as $H(x) = a(x)g(x) + b(x)h(x)$. In the splitting field of $h(x)g(x)$ we know that $g(x)$ and $h(x)$ split completely and $H(x)$ divides $g(x)$ we see that $H(x)$ splits completely. Since they only share one root we see that $H(x) = x - \beta$. Thus $\beta \in K(\gamma)$. □

10 Galois Extensions and Galois groups

From here forward we will only be considering finite degree extensions.

To each extension we can attach a group.

Definition 10.1. Let L/K be a field extension. The group $\mathrm{Aut}_K(L) = \{\varphi \colon L \to L \mid \varphi \text{ is an isomorphim and } \varphi(k) = k \text{ for all } k \in K\}$. This group is known as the *Galois group* of the extension L/K. It is sometimes denoted $G(L/K)$.

Let us look at some examples.

Example. Consider any irreducible polynomial $x^2 + bx + c$ over $\mathbb{Q}$. It is well known that this equation has two roots of the form $\dfrac{-b \pm \sqrt{b^2 - 4c}}{2}$. Let $d = b^2 - 4c$, then both these roots lie in the field $\mathbb{Q}(\sqrt{d}) = \{x + y\sqrt{d} \mid x, y \in \mathbb{Q}\}$.

We can now consider the group $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{d}))$. Notice that for any extension $\mathbb{Q}(\alpha)$ a homomorphism $f\colon \mathbb{Q}(\alpha) \to \mathbb{Q}(\alpha)$ is determined by $f\big|_{\mathbb{Q}}$ and $f(\alpha)$. We already are requiring that $f(q) = q$ for all $q \in \mathbb{Q}$. Thus we must find out what happens to $\sqrt{d}$.

Since $\alpha = \sqrt{d}$ is a root of the polynomial $x^2 - d$ we see that $f(\alpha)$ is also a root of $x^2 - d$. Thus we are restricted to $f(\alpha) = \alpha$ or $f(\alpha) = -\alpha$. It is easy to check that these both define homomorphisms. Thus $\mathrm{Aut}_{\mathbb{Q}}(\mathbb{Q}(\sqrt{d}))$ has two elements and there is only one group with 2 elements. Thus it is $\mathbb{Z}/2\mathbb{Z}$.

Example. Consider the field extension $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$. Once again we can see that isomorphism $f\colon \mathbb{Q}(\sqrt{2}, i) \to \mathbb{Q}(\sqrt{2}, i)$ is determined by $f(i)$ and $f(\sqrt{2})$. As before we see that $f(\sqrt{2})$ must be a root of $x^2 - 2$ giving two choice $\sqrt{2}, -\sqrt{2}$ and $f(i)$ must be a root of $x^2 + 1$ giving two choices $i, -i$.

We can use the proof of the tower law to get a basis for $\mathbb{Q}(\sqrt{2}, i)/\mathbb{Q}$ given by $\{1, \sqrt{2}, i, i\sqrt{2}\}$. Let us consider what happens to this basis given the four choices above we label the four possible homomorphisms $\sigma_1, \sigma_2, \sigma_3, \sigma_4$.

	1	i	$\sqrt{2}$	$i\sqrt{2}$
σ_1	1	i	$\sqrt{2}$	$i\sqrt{2}$
σ_2	1	i	$-\sqrt{2}$	$-i\sqrt{2}$
σ_3	1	$-i$	$\sqrt{2}$	$-i\sqrt{2}$
σ_4	1	$-i$	$-\sqrt{2}$	$i\sqrt{2}$

Thus these are 4 different automorphisms. We will see shortly that $|\mathrm{Aut}_K(L)| \leqslant [L : K]$, thus these give all the possible isomorphisms. We can all see that each squares to the identity, thus this group is $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Example. Let us consider the extension $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$. Once again we see that $f(\sqrt[3]{2})$ must be sent to a root of the polynomial $x^3 - 2$. However, there is only one root of this polynomial in the field $\mathbb{Q}(\sqrt[3]{2})$, namely, $\sqrt[3]{2}$ and we see that the only such isomorphism is the identity and the Galois group is the trivial group.

In this case we can see that failure of this group being larger is a lack of roots we shall shortly that we will ideally want our extensions to be normal.

Example. Let $K = \mathbb{F}_3(t)$ and L be the splitting field of $f(x) = x^3 - t \in K[x]$. As we have already seen the polynomial $f(x)$ has one root, α. Thus the extension L is generated by one element α. Any isomorphism must send α to α and we thus only have 1. Once again, the issue was the lack of roots. We will see that we will also want our extensions to be separable.

Definition 10.2. We say that an extension L/K is *Galois* if $|G(L/K)| = [L : K]$.

Let us begin by showing that this is as large as $G(L/K)$ can be. We do this by proving a more general fact.

Lemma 10.3. *Suppose that M/K is a field extension and that $i\colon K \to L$ is a homomorphism. Let $d = [M : K]$. Then there are exactly d homomorphisms $j\colon M \to L$ extending i if and only if M/K is separable and the minimal polynomial of α splits over L for every $\alpha \in M$.*

Otherwise there are less than d homomorphisms extending i.

Proof. We shall prove this by induction. The case where $[M : K] = 1$ being trivial as $M = K$.

Now suppose that either M/K is not a separable extension or there is an element α such that m_α does not split over L. In either case there are less roots of the polynomial m_α than $[K(\alpha) : K] = \deg(m_\alpha)$. Thus by the theorem on extending homomorphisms to simple extensions there are less than $[K(\alpha) : K]$ extensions of i to $K(\alpha)$ by induction for each of these there are at most $[M : K(\alpha)]$ extensions to M. Thus we get $< d$ extensions of i.

Suppose now that both conditions are satisfied. In this case we have exactly $[K(\alpha) : K]$ extensions of i to $K(\alpha)$ by the theorem on extending homomorphisms to simple extensions. Thus by induction for each one we have $[M : K(\alpha)]$ extensions to M.

Putting this together we have exactly $[M : K(\alpha)][K(\alpha) : K] = [M : K] = d$ extensions of i to M. □

Corollary 10.4. *$G(L/K) \leqslant [L : K]$ and we have equality if and only if L/K is a separable and normal extension.*

Proof. In the above theorem take $M = L$. Note that if L is a finite degree extension of K and we have a homomorphism $f\colon L \to L$ then it is surjective. To show this we take a basis $\{a_1, \ldots, a_n\}$. Since f is injective we see that $\{f(a_1), \ldots, f(a_n)\}$ is a linearly independent set thus we see that $[f(L) : K]$ is at least $n = [L : K]$ however it is also at most n. Thus we see that it is equal and f is surjective.

Thus we see from the above theorem that there are at most $[L : K]$ isomorphisms $f\colon L \to L$ such that $f(k) = k$ for all $k \in K$. We see that there are exactly $[L : K]$ isomorphisms if and only if L/K is separable and m_a splits for all $a \in L$, i.e. L is a normal extension. □

Corollary 10.5. *An extension is Galois if and only if it is separable and normal.*

An extension $L/\mathbb{Q}$ is Galois if and only if it L is the splitting field of some polynomial $f(x)$.

Recall that given a group H of isomorphisms of a field to itself we define the fixed subfield $L^H = \{x \in L \mid \sigma(x) = x \, \forall \sigma \in H\}$.

Theorem 10.6 (The Fundamental theorem of Galois theory)**.** *Let L/K be a Galois extension. Then*

1. *There is an inclusion reversing bijection from subgroups of $\mathrm{Aut}_K(L)$ and subfields M such that $K \subset M \subset L$.*

   Given by $H \mapsto L^H$ and $M \mapsto \mathrm{Aut}_M(L)$.

2. *Given a subfield M as above. Let $H = \mathrm{Aut}_M(L)$ then $[L : M] = |H|$ and $[M : K] = |{}^{G}/_{H}|$.*

3. *The extension M/K is normal if and only if $\mathrm{Aut}_M(L)$ is a normal subgroup of $\mathrm{Aut}_K(L)$.*

Before we begin the proof we require some lemmas about isomorphisms of field extensions.

Lemma 10.7. *Let $S = \{\varphi_1, \ldots, \varphi_n\}$ be a set of distinct isomorphisms of L. Then S is linearly independent, i.e. if $r_i \in L$ and $\sum_{i=1}^{n} r_i\varphi_i(\beta) = 0$ for all $\beta \in L$, then $r_i = 0$ for all i.*

Proof. Suppose that we have a relation $\sum_{i=1}^{n} r_i\varphi_i(\beta) = 0$ where some of the $r_i \neq 0$. We can reorder and look for the shortest such relation of the form $\sum_{i=1}^{k} r_i\varphi_i(\beta) = 0$ for all $\beta \in L$ such that all the $r_i \neq 0$.

Let $\alpha \in L$ be such that $\varphi_1(\alpha) \neq \varphi_2(\alpha)$. We now have the equality

$$\sum_{i=1}^{k} r_i\varphi_1(\alpha)\varphi_i(\beta) = 0. \tag{10.1}$$

We also have the equality

$$0 = \sum_{i=1}^{k} r_i\varphi_i(\alpha\beta) = \sum_{i=1}^{k} r_i\varphi_i(\alpha)\varphi_i(\beta). \tag{10.2}$$

We can now look at (10.2) − (10.1) to get the following

$$\sum_{i=1}^{k} r_i(\varphi_1(\alpha) - \varphi_i(\alpha))\varphi_i(\beta)$$

However, this gives us a shorter relation since some of the r_i are non-zero. □

Lemma 10.8. *Let H be a subgroup of $\mathrm{Aut}(L)$. Then $[L : L^H] = |H|$.*

Proof. Let $H = \{\sigma_1, \ldots, \sigma_n\}$. Let $[L : L^H] = m$ and L has a basis $\{\alpha_1, \ldots, \alpha_m\}$.

First assume for a contradiction that $m < n$. Consider the set of equations

$$\sum_{k=1}^{n} r_k\sigma_k(\alpha_i) = 0$$

in the variables r_k. There are n equations each in m variables. Since we have more equations than variables we have a non-zero solution. Thus there are r_k

not all zero such that $\sum_{k=1}^{n} r_k\sigma_k(\alpha_i) = 0$ for each i. Now let $\alpha \in L$ then there are $y_i \in L^H$ such that $\alpha = \sum_{i=1}^{m} y_i\alpha_i$. Thus we get the following:

$$\begin{aligned}\sum_{k=1}^{n} r_k\sigma_k(\alpha) &= \sum_{k=1}^{n} r_k\sigma_k(\sum_{i=1}^{m} y_i\alpha_i)\\ &= \sum_{k=1}^{n}\sum_{i=1}^{m} r_k\sigma_k(y_i\alpha_i)\\ &= \sum_{k=1}^{n}\sum_{i=1}^{m} r_k y_i\sigma_k(\alpha_i)\\ &= \sum_{i=1}^{m} y_i \sum_{k=1}^{n} r_k\sigma_k(\alpha_i)\\ &= \sum_{i=1}^{m} y_i(0) = 0\end{aligned}$$

This gives a contradiction to the previous lemma so $m \geqslant n$.

Now assume that $n < m$. Once again we have a sequence of equations in variables r_k this time one for each isomorphism.

$$\sum_{k=1}^{m} r_k\sigma_i(\alpha_k) = 0.$$

Once again by assumption there are more unknowns than equations so we once again have a non-zero solution. However since each of r_k are in L^H we see that the first equation becomes

$$\begin{aligned}0 &= \sum_{k=1}^{m} r_k\sigma_1(\alpha_k)\\ &= \sigma_1(\sum_{k=1}^{m} r_k\alpha_k).\end{aligned}$$

However, since σ_1 is injective we see that $\sum_{k=1}^{m} r_k\alpha_k = 0$ but α_k was a basis giving us the desired contradiction. So $n \geqslant m$ and we conclude that $n = m$. □

Corollary 10.9. *L/K is a Galois extension if and only if $L^{\mathrm{Aut}_K(L)} = K$.*

Corollary 10.10. *Suppose that G is a subgroup of $\mathrm{Aut}(L)$. Then L/L^G is a Galois extension with $\mathrm{Aut}_{L^G}(L) = G$.*

We are now ready to prove the fundamental theorem of Galois theory.

Proof. We first prove the correspondence.

Suppose that L/K is a Galois extension. We wish to show that there is a bijection given by $H \mapsto L^H$ and this has an inverse $M \mapsto \mathrm{Aut}_M(L)$ where $H < \mathrm{Aut}_K(L)$ and $K \subset M \subset L$. We will show that $L^{\mathrm{Aut}_M(L)} = M$ and $\mathrm{Aut}_{L^H}(L) = H$.

Suppose that M is a subfield of L containing K. Since L is a Galois extension, L is the splitting field of some polynomial in $K[x]$. We can also see that L is the splitting field of the same polynomial over $M[x]$. Thus L/M is a Galois extension so $|\mathrm{Aut}_M(L)| = [L : M]$.

We know wish to prove that $L^{\mathrm{Aut}_M(L)} = M$. Since each element of $\mathrm{Aut}_M(L)$ fixes M pointwise we see that $M \subset L^{\mathrm{Aut}_M(L)}$. We also know that $[L : L^{\mathrm{Aut}_M(L)}] = |\mathrm{Aut}_M(L)|$. Thus we see that $M = L^{\mathrm{Aut}_M(L)}$ for degree reasons.

Now suppose that H is a subgroup of $\mathrm{Aut}_K(L)$. We wish to show that $\mathrm{Aut}_{L^H}(L) = H$. This is exactly the statement of Corollary 10.10.

Now the second part comes from Lemma 10.8. We immediately see that if $H = \mathrm{Aut}_M(L)$ that $[L : M] = |H|$ and $[M : K] = \dfrac{[L : K]}{[L : M]} = \dfrac{|G|}{|H|} = |{}^{G}\!/_{H}|$.

Suppose that M/K is a normal extension and let $\alpha \in M$. Let $\sigma \in \mathrm{Aut}_K(L)$. Consider $\sigma(\alpha)$. Since elements of $\mathrm{Aut}_K(L)$ permute roots of irreducible polynomials we see that α and $\sigma(\alpha)$ satisfy the same irreducible polynomial. Thus since M is normal and $\alpha \in M$ we see that $\sigma(\alpha)$ is also in M. This gives us a homomorphism $\Phi\colon \mathrm{Aut}_K(L) \to \mathrm{Aut}_K(M)$ such that $\Phi(\sigma) = \sigma\big|_M$. The kernel of this homomorphism is exactly the elements of $\mathrm{Aut}_K(L)$ which fix M pointwise, which is $\mathrm{Aut}_M(L)$ and is a normal subgroup.

Suppose that $\mathrm{Aut}_M(L)$ is a normal subgroup, i.e. for all $\theta \in \mathrm{Aut}_M(L)$ and all $\sigma \in \mathrm{Aut}_K(L)$ we have that $\sigma^{-1}\theta\sigma = \theta' \in \mathrm{Aut}_M(L)$. Let α be in M a root of some irreducible polynomial $f(x)$. Then we know that $\sigma^{-1}(\theta(\sigma(\alpha))) = \theta'(\alpha)$, alternatively $\theta(\sigma(\alpha)) = \sigma(\theta'(\alpha))$. We know that $\theta'(\alpha) = \alpha$ so this equation reduces to $\theta(\sigma(\alpha)) = \sigma(\alpha)$ for all $\theta \in \mathrm{Aut}_M(L)$ and $\sigma \in \mathrm{Aut}_K(L)$. However this means that $\sigma(\alpha) \in M$ for all σ. Since $\mathrm{Aut}_K(L)$ acts transitively on roots of irreducible polynomials we see that the other roots of $f(x)$ are in M.

To conclude the proof of the theorem note that Φ from above is surjective since given a homomorphism $M \to M$ we can always extend to a homomorphism $L \to L$. □

For examples see that text book on the webpage as well as notes of Keith Conrad linked on the webpage.

11 Finite Fields

Definition 11.1. A *finite field* is a field with finitely many elements. We will denote the field with q elements $\mathbb{F}_q$.

We have already come across a finite field of order p. Namely, ${}^{\mathbb{Z}}\!/_{p\mathbb{Z}}$, which we will denote $\mathbb{F}_p$.

Theorem 11.2. *Let $\pi(x)$ be a monic irreducible polynomial in $\mathbb{F}_p[x]$. Then $F = \mathbb{F}_p[x]\Big/_{(\pi(x))}$ is a field of order p^n, where $n = \deg \pi(x)$.*

Proof. We can see that F is a field since $\pi(x)$ is a monic irreducible polynomial, thus $(\pi(x))$ is a maximal ideal of $\mathbb{F}_p[x]$.

We also know that F is a simple extension of $\mathbb{F}_p$ and thus the degree of this extension is the degree of $\pi(x)$. Thus $[F : \mathbb{F}_p] = \deg \pi(x) = n$. Thus F is a vector space of dimension n over $\mathbb{F}_p$ and has p^n elements. □

Example. $F = \mathbb{F}_2[x]/(x^3 + x + 1)$ is a field with 8 elements. We must check that $x^3 + x + 1$ is irreducible but we can see that it has no roots and since it is degree 3 this is sufficient.

Theorem 11.3. *Any finite field F has prime power order.*

Proof. Since there are only finitely many elements of a finite field, we see that the characteristic cannot be positive. Thus we see that there is an embedding of $\mathbb{F}_p$ into F. Thus $F/\mathbb{F}_p$ is a field extension. Since F is finite we see that this must be a finite degree extension. Suppose the extension is of degree n. Then $|F| = p^n$ since F is an n-dimensional vector space over $\mathbb{F}_p$. □

Lemma 11.4. *Let F be a finite field of order q. Then $F^\times$ is cyclic.*

Proof. Let m be the maximal order of any element of the group $F^\times$, so $m|q-1$. By the classification of abelian groups we see that any element of $F^\times$ has order dividing m. Thus the polynomial $x^m - 1$ has $q - 1$ solutions in F. However, this can only be the case if $m = q - 1$. Thus there is an element of order $q - 1$ and thus the group is cyclic. □

Theorem 11.5. *Every finite field is isomorphic to $\mathbb{F}_p[x]/(\pi(x))$ for some monic irreducible $\pi(x) \in \mathbb{F}_p[x]$.*

Proof. Let F be a finite field. By the previous theorem F is of order p^n for some n and some prime p. Since $F^\times$ is cyclic, we can pick a generator α of $F^\times$.

Since there is a fixed copy of $\mathbb{F}_p$ in F, coming from its characteristic. We can consider $\mathbb{F}_p(\alpha) \subset F$. Since every element of F is of the form α^k or 0, we can see that $\mathbb{F}_p(\alpha) = F$.

Let $\pi(x)$ be the minimal polynomial of α. Then by the definition of the simple extension $\mathbb{F}_p(\alpha)$ we see that $F = \mathbb{F}_p[x]/(\pi(x))$. □

Lemma 11.6. *Let F be a finite field of order p^n. Then F is the splitting field of $x^{p^n} - x \in FF_p[x]$.*

Proof. Since $F^\times$ is cyclic we can see that any non-zero element is a root of the polynomial $x^{p^n-1} - 1$. If we multiply by x we can see that every element is a root of the polynomial $x^{p^n} - x$. The polynomial $x^{p^n} - x$ since there are p^n roots of this polynomial in F we see that this polynomial must split completely. □

Theorem 11.7. *Given a prime p and a natural number n there is a field of order p^n.*

Proof. The field in question is the splitting field of $x^{p^n} - x$. □

Theorem 11.8. *Any two finite fields of the same size are isomorphic.*

Proof. Any such field is the splitting field of the polynomial $x^{p^n} - x$ and splitting fields are unique. □

This gives us a complete classification of finite fields. We have also justified our decision to write $\mathbb{F}_{p^n}$ for the field of order p^n since there is only one.

Theorem 11.9. *A subfield of $\mathbb{F}_{p^n}$ is of order p^d where $d|n$. Moreover, there is only one such subfield for each d.*

Proof. content... □

We have shown that $\mathbb{F}_{p^n}$ is the splitting field of $x^{p^n} - x$ over $\mathbb{F}_p$ and thus this is a Galois extension. Let us study its Galois group.

Theorem 11.10. $\mathrm{Aut}_{\mathbb{F}_p}(\mathbb{F}_{p^n})$ *is a cyclic group of order n. The generator of this group is the* Frobenius automorphism *given by $\alpha \mapsto \alpha^p$.*

Proof. content... □

12 Constructability and Origami

We have studied field extensions in a lot of abstraction and then used Galois theory to classify all finite fields.

We can also use Galois theory to answer some very classical geometric problems.

Given a set $P \subset \mathbb{R}^2$ we have the following two operations we can draw a line through the points (a_1, b_1) and (a_2, b_2). Namely the line given by the equation

$$y - b_1 = \frac{b_2 - b_1}{a_2 - a_1}(x - a_1).$$

Secondly, we can draw the circle with center a point (a_1, b_1) and a point on the circumference (a_2, b_2). Namely the circle with equation

$$(y - b_1)^2 + (x - a_1)^2 = \sqrt{(a_2 - a_1)^2 + (b_2 - b_1)^2}.$$

Given a set S of points in $\mathbb{R}^2$ we say that a point $p \in \mathbb{R}^2$ is *constructible from* S if it is in the intersection of either two lines, two circles or a circle or a line.

Figure

Definition 12.1. We say that a point is *constructible* if it is constructible in finitely many steps from $\{(0,0),(1,0)\}$. Let $\mathcal{C}$ denote the constructible numbers.

Examples. $(-1, 0)$ is constructible. $(0, 1)$ is constructible. $(1, 1)$ is constructible. $(\sqrt{2}, 0)$ is constructible. $(q, 0)$ is constructible for any $q \in \mathbb{Q}$.

Some basic constructions include.

- Midpoints of lines.
- Angle bisectors.
- Perpendicular bisectors.
- Parallel lines.

The Greeks asked 3 questions can be related to constructible numbers. These were:

1. Can you double the cube?
2. Can you trisect and angle?
3. Can you square the circle?

Each of these correspond to a question about whether or not a certain number is constructible. These are as follows:

1. Is $\sqrt[3]{2}$ constructible?
2. Given a constructible angle θ is $\cos(\theta/3)$ constructible?
3. Is $\sqrt{\pi}$ constructible?

Lemma 12.2 (Projection Lemma)**.** *$(a, b) \in \mathcal{C}$ if and only if $(a, 0) \in \mathcal{C}$ and $(b, 0) \in \mathcal{C}$.*

Proof. The proof is pictorial. First note that $(b, 0)$ is constructible if and only if $(0, b)$ is constructible. For one direction, we project to the respective axes.

Given $(a, 0)$ and $(0, b)$ we can draw the rectangle with 3 vertices $(a, 0), (0, b), (0, 0)$ the fourth vertex is the point (a, b). □

By considering the bijection $(a, b) \mapsto a + bi$ we can consider $S \subset \mathbb{R}^2$ as a subset of $\mathbb{C}$. From here on we will always consider the constructible numbers as a subset of $\mathbb{C}$.

Lemma 12.3. *The distance between any two constructible points is a constructible number.*

Proof. Figure □

Theorem 12.4. *The constructible numbers form a field.*

Proof. We have to prove that the set is closed under addition, multiplication and has inverses and identities.

It is clear that $0, 1$ are constructible so the identities are constructible.

By the projection lemma it is enough to do these for real numbers. For this we just need to be able to construct the lengths $a + b, ab, \dfrac{a}{b}$.

We can do this fairly easily with the following figures. □

This is a field extension of $\mathbb{Q}$. Let us study the subfields which are finite extensions of $\mathbb{Q}$.

Theorem 12.5. *Let S be a finite set of constructible numbers and suppose that α is constructible over S. Then α satisfies a quadratic equation in $\mathbb{Q}(S)[x]$.*

Proof. Suppose that α is constructible over S, then α is either the intersection of two lines, a circle and a line or two circles.

To solve the intersection of two lines we just have to solve a linear equation over $\mathbb{Q}(S)$, i.e. setting the equations of the lines equal to each other.

To find the intersection of the circle and a line we replace y in the equation of the circle $(y-a)^2+(x-b)^2=r^2$ by $y=mx+c$ where $y=mx+c$ is the equation of the line. This gives us a quadratic equation.

For the intersection of two circles, if we take the defining equation for one circle away from the other we obtain an equation for the line between their points of intersection. This reduces us to the previous case. □

Theorem 12.6. *Suppose that α satisfies a quadratic equation over $\mathbb{Q}(S)$. Then α is constructible.*

Proof. To prove this we must show that given a constructible number we can obtain its square roots. Since the square root of $a+bi$ can be described in terms of the square roots of a and b. We will just show how to take square roots of real numbers. This proof is contained in the figure below. □

,

Theorem 12.7. *Let α be a constructible number. Then $[\mathbb{Q}(\alpha):\mathbb{Q}]=2^k$ for some $k\in\mathbb{N}$.*

Proposition 12.8. *We cannot perform any the following constructions with a ruler and compass:*

1. *Doubling the cube,*
2. *Trisecting an angle,*
3. *Squaring the circle.*

Proof.

1. We have already seen that $[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}]=3$ and we know that $3\neq 2^k$. Thus $\sqrt[3]{2}$ is not constructible.
2. Given an angle θ trisecting is equivalent to constructing $\cos(\frac{\theta}{3})$.

   Thus, we use the triple angle formula $\cos(3\alpha)=\cos^3(\alpha)-3\cos(\alpha)$. This question only really makes sense for angles that are constructible. Since $\frac{\pi}{3}$ is constructible we will put $\alpha=\frac{\pi}{3}$ to get a polynomial satisfied by $\cos(\frac{\pi}{9})$. Namely, $f(x)=2x^3-6x-1$. This polynomial is irreducible by the rational roots test and thus $[\mathbb{Q}(\cos(\frac{\pi}{9})):\mathbb{Q}]=3$ and we cannot trisect the angle.

3. To square the circle we would require $\sqrt{\pi}$ to satisfy a polynomial of degree 2^k for some k. However $\sqrt{\pi}$ does not satisfy a polynomial of any degree. The proof of this fact is beyond the scope of this course. For more information look into the Lindemann-Weierstrass Theorem.

□

13 Radical Extensions

Definition 13.1. We say that a field extension L/K is *radical* if there are elements $v_1, \ldots, v_n$ such that:

- $L = K(v_1, \ldots, v_n)$ and
- $v_1^{m_1} \in K$ and $v_i^{m_i} \in K(v_1, \ldots, v_{i-1})$ for each $i \in \{2, \ldots, n\}$.

If an element α is an element of a radical extension, then we say that α is *expressable by radicals.*

A polynomial $f(x)$ is *solvable by radicals* if there is a radical extension L/K in which $f(x)$ splits.

These notions formalise what it means to solve $f(x)$ by the operations $+, -, \times, \div$ and $\sqrt[n]{}$.

Example. The polynomial $x^4 - 4x^2 + 2 \in \mathbb{Q}[x]$ is solvable by radicals.

The roots of this polynomial are $\pm\sqrt{2 \pm \sqrt{2}}$. Thus we see that the polynomial splits over $L = \mathbb{Q}(\sqrt{2+\sqrt{2}}, \sqrt{2-\sqrt{2}})$. As written it does not satisfy the properties of a radical extension. Note that $(\sqrt{2+\sqrt{2}})^2 - 2 = \sqrt{2} \in L$. Thus $L = \mathbb{Q}(\sqrt{2}, \sqrt{2+\sqrt{2}}, \sqrt{2-\sqrt{2}})$ and this satisfies the definition of being radical with $v_1 = \sqrt{2}, v_2 = \sqrt{2+\sqrt{2}}, v_3 = \sqrt{2-\sqrt{2}}$.

Theorem 13.2. *Let L be the splitting field of $x^m - 1$ over K, where the characteristic of K is 0. Then $\mathrm{Aut}_K(L)$ is Abelian.*

Proof. Since the characteristic of K is 0, we see that $x^m - 1$ has m distinct roots and they forms a subgroup of $C = \langle \zeta_m \rangle$ generated by a primitive m-th root. Every element of $\mathrm{Aut}_K(L)$ defines an isomorphism of C to itself. This means $\mathrm{Aut}_K(L) \leqslant \mathrm{Aut}(C)$ and $\mathrm{Aut}(C) = \left(\mathbb{Z}/m\mathbb{Z}\right)^\times$ which is an Abelian group. □

Theorem 13.3. *Let K be a field of characteristic 0, which contains all m-th roots of unity (i.e. $x^m - 1$ splits over K). Let $a \in K$. Let L be the splitting field of $x^m - a$ over K. Then $\mathrm{Aut}_K(L)$ is a cyclic of order dividing m.*

Proof. If u is a root of $x^m - a$, then all the other roots are of the form $\zeta_m^i u$ for some $i \in \{1, \ldots, m-1\}$. Any $\varphi \in \mathrm{Aut}_K(L)$ is determined by its value on u and $\varphi(u) = \zeta_m^i u$ for some i.

This defines a homomorphism $\mathrm{Aut}_K(L) \to \mathbb{Z}/m\mathbb{Z}$. Given by taking φ to i such that $\varphi(u) = \zeta_m^i u$. Since each element of $\mathrm{Aut}_K(L)$ is determined by $\varphi(u)$ we see that this is injective. Thus $\mathrm{Aut}_K(L)$ is isomorphic to a subgroup of a cyclic group and is thus cyclic. □

Definition 13.4. We say that L/K is a *cyclic extension* if $\mathrm{Aut}_K(L)$ is a cyclic group.

Theorem 13.5. *Suppose K is a field of characteristic 0 containing all the m-th roots of unity. Let L/K be a cyclic extension of degree m. Then $L = K(\sqrt[m]{a})$ for some $a \in K$ and $m \in \mathbb{N}$.*

Proof. Let σ be a generator of $\mathrm{Aut}_K(L)$. Let ζ_m be a primitive m-th root of unity. Let $b \in L$ and define

$$\Phi(b) = b + \zeta_m\sigma(b) + \zeta_m^2\sigma^2(b) + \cdots + \zeta_m^{m-1}\sigma^{m-1}(b) = \sum_{i=0}^{m-1} \zeta_m^i\sigma^i(b).$$

Note that $\sigma(\Phi(b)) = \zeta_m^{-1}\Phi(b)$. Thus $\sigma(\Phi(b)^m) = \zeta_m^{-m}\Phi(b)^m = \Phi(b)^m$ so $\Phi(b)$ is in K.

Since the automorphisms $\mathrm{id}, \sigma, \sigma^2, \ldots, \sigma^{m-1}$ are linearly independent. We see that there is a $\alpha \in L$ such that $\Phi(\alpha) \neq 0$. Also $\sigma^i(\Phi(\alpha)) = \zeta_m^i(\Phi(\alpha))$ so σ^i does not fix $\Phi(\alpha)$ for any $i < m$. So $\Phi(\alpha)$ does not lie in any proper subfield of L. So for degree reasons, $L = K(\Phi(\alpha))$. Also since $\Phi(\alpha)^m$ is fixed by σ and hence is in K. Letting $a = \Phi(\alpha)^m$ we see that $L = K(\sqrt[m]{a})$. □

Theorem 13.6. *Let K be a field of characteristic 0. Let E be a radical extension of K. Then there is an extension L of E which is a normal radical extension of K.*

Proof. Let $E = K(v_1, \ldots, v_n)$. Let $f_i(x) \in K[x]$ be the minimal polynomial for v_i. Let $f(x)$ be the product of the f_i. Let L be the splitting field of $f(x)$. This is a normal extension and clearly contains E, thus we are left to show that it is a radical extension.

Let $\mathrm{Aut}_K(L) = \{\theta_1, \ldots, \theta_m\}$. Since Galois groups act transitively on the roots of irreducible polynomials we say that for any root α of $f(x)$ there is i, j such that $\alpha = \theta_j(v_i)$. Thus,

$$L = K(v_1, \ldots, v_n, \theta_1(v_1), \ldots, \theta_1(v_n), \ldots, \theta_m(v_n)).$$

Since $\theta_j(v_i)^{m_i} = \theta_j(v_i^{m_i}) \in \theta_j(K(v_1, \ldots, v_{i-1})) = K(\theta(v_1, \ldots, \theta_j(v_{i-1})))$. This shows that the radical property is satisfied. □

13.1 Solvable groups

Definition 13.7. A group G is said to be solvable if there is a sequence of subgroups $N_i \leqslant G$ such that:

1. $G = N_0 \geqslant N_1 \geqslant \cdots \geqslant N_m = \{e\}$.
2. $N_i \lhd N_{i-1}$
3. $N_i \big/ N_{i+1}$ is Abelian.

Examples. Abelian groups are solvable, dihedral groups are solvable.

Non-abelian simple groups are not simple.

For finite groups we can change the definition so that the third point says cyclic instead of Abelian.

Theorem 13.8. *Let $f(x)$ be a polynomial over a field K of characteristic 0. Let F be the splitting field of $f(x)$. Then $f(x)$ is solvable by radicals if and only if $\mathrm{Aut}_K(F)$ is solvable.*

Proof. First assume that $f(x)$ is solvable by radicals. Then there is a radical extension E which contains a splitting field F for $f(x)$. By Theorem 13.6 we can find a normal radical extension $L = K(v_1, \ldots, v_n)$ also containing F. Let $L_{i-1} = K(v_1, \ldots, v_{i-1})$ and m_i the integer such that $v_i^{m_i} \in L_{i-1}$. Let m be the least common multiple of the m_i. Let ζ_m be a primitive m-th root of unity. Define $\widehat{K} = K(\zeta_m), \widehat{L_i} = L_i(\zeta_m)$ and $\widehat{L} = L(\zeta_m)$.

Note that $\widehat{L}$ is a normal radical extension of $\widehat{K}$ and $\widehat{K}$ contains all of the m-th roots of unity. Note also the $\widehat{L}/K$ is a normal extension. Thus $\mathrm{Aut}_K(F)$ is a quotient of $\mathrm{Aut}_K(\widehat{L})$. Thus if $\mathrm{Aut}_K(\widehat{L})$ is solvable so is $\mathrm{Aut}_K(F)$. Thus we must prove that $\mathrm{Aut}_K(\widehat{L})$ is solvable.

To prove that $\mathrm{Aut}_K(\widehat{L})$ is solvable. Let $N = \mathrm{Aut}_{\widehat{K}}(\widehat{L})$ and $N_i = \mathrm{Aut}_{\widehat{L}}(\widehat{L_i})$. We obtain the following diagram of fields and the corresponding diagram of subgroup of $\mathrm{Aut}_K(\widehat{L})$.

$$
\begin{array}{ccc}
\widehat{L} & \longrightarrow & \{e\} = N_n \\
\big| & & \\
\widehat{L_1} & \longrightarrow & N_1 \\
\big| & & \\
\vdots & & \\
\big| & & \\
\widehat{L_i} & \longrightarrow & N_i \\
\big| & & \\
\widehat{L_{i-1}} & \longrightarrow & N_{i-1} \\
\big| & & \\
\vdots & & \\
\big| & & \\
\widehat{K} & \longrightarrow & N \\
\big| & & \\
K & \longrightarrow & \mathrm{Aut}_K(\widehat{L})
\end{array}
$$

Note that $\widehat{L_i}$ is the splitting field of $x^{m_i} - a$ over $\widehat{F_{i-1}}$. So $N_i \lhd N_{i-1}$ and so we see that $\mathrm{Aut}_{\widehat{L_{i-1}}}(\widehat{L_i}) \cong {}^{N_{i-1}}\big/_{N_i}$ also by Theorem 13.3 we have that ${}^{N_{i-1}}\big/_{N_i}$ is cyclic. By the same reasoning ${}^{N}\big/_{N_1}$ is cyclic.

Similarly $N \lhd G$ and by Theorem 13.2 we see that ${}^{G}\big/_{N}$ is Abelian. Thus $\mathrm{Aut}_K(\widehat{L})$ is solvable and we have proved the first direction of the theorem.

Now suppose that $G = \mathrm{Aut}_K(F)$ is solvable. Now let $\hat{F} = F(\zeta_m)$ and $\hat{K} = K(\zeta_m)$, where $m = |G|$.

Let $\varphi \in \mathrm{Aut}_{\widehat{K}}(\hat{F})$ and $a \in F$. Then $\varphi(a)$ is also a root of the minimal polynomial of a over K so is also in F. Thus $\varphi\big|_F \in \mathrm{Aut}_K(F)$ and so $\hat{G} = \mathrm{Aut}_{\widehat{K}}(\hat{F}) \leqslant \mathrm{Aut}_K(F)$ and so is also solvable.

Thus we get a sequence of subgroups $\{e\} = N_m \lhd \cdots \lhd N_1 \lhd N_0 = \hat{G}$ such that $N_i \leqslant N_{i-1}$ and ${}^{N_i}\big/_{N_{i-1}}$ is cyclic. Now we get an ascending sequence of field extensions $\hat{K} = F_m \subset F_{m-1} \subset \cdots \subset F_1 \subset F_0 = \hat{F}$ with $N_i = \mathrm{Aut}_{\hat{K}}(F_i)$ and $\mathrm{Aut}_{F_i}(F_{i-1}) = {}^{N_{i-1}}\big/_{N_i}$.

Thus each extension is a cyclic extension and so by Theorem 13.5 we see that F_i is a radical extensionof F_{i-1} and so $\hat{F}$ is a radical extension. Thus $f(x)$ is solvable by radicals. □

13.2 Unsolvability of the quintic

Lemma 13.9. *A_5 is a simple group.*

Proof. This was proved in abstract algebra I. □

Since A_5 is not abelian we see that it is also not solvable, since it has no abelian quotients.

Proposition 13.10. *S_5 is not solvable.*

Proof. If S_5 were solvable, then so would any subgroup of S_5 and we would conclude that A_5 is solvable. □

Lemma 13.11. *S_5 is generated by any 5-cycle and any transposition.*

Proof. This is an exercise in conjugating permutations. □

Example. The polynomial $f(x) = x^5 - 6x + 3 \in \mathbb{Q}[x]$ is not solvable by radicals.

Proof. Let L be the splitting field of $f(x)$ we will show that $\mathrm{Aut}_{\mathbb{Q}}(L)$ is S_5 which is not solvable. Thus $f(x)$ is not solvable by radicals.

The polynomial $f(x)$ is irreducible by Eisenstein's criterion and thus $[L : \mathbb{Q}]$ is divisible by 5. Since $\mathrm{Aut}_{\mathbb{Q}}(L) \leqslant S_5$ and 5 divides $|\mathrm{Aut}_{\mathbb{Q}}(L)|$ we see that $\mathrm{Aut}_{\mathbb{Q}}(L)$ has an element of order 5 and so contains a 5-cycle, since these are the only elements of order 5 in S_5.

Note that $f(-2) = 17, f(0) = 3, f(1) = -2, f(2) = 23$, thus the intermediate value theorem tells us that $f(x)$ has at least 3 real roots. If $f(x)$ had more real

roots, then the derivative would have at least 3 real roots. However $x^4 - 6$ only has 2 real roots. Thus $f(x)$ has 3 real roots and 2 complex roots.

Since $L/\mathbb{Q}$ is a Galois extension we can see that complex conjugation is an automorphism fixing $\mathbb{Q}$. As a permutation in S_5 this switches exactly 2 elements and thus we get a transposition. Thus by Lemma 13.11 we see that $\mathrm{Aut}_{\mathbb{Q}}(L) = S_5$ and thus $f(x)$ is not solvable by radicals. □

This theorem was originally proved by Abel in the 1800's. For many years previous mathematicians had been searching for an equation to solve the quintic. This shows that there are no formulae that just contain $+, -, \times, \div$ and $\sqrt[n]{}$. It is however a remarkable theorem that is we let $\sqrt[a]{x}$ be a function giving the roots of $x^5 - x - a$, then the quintic can be solved in terms of $+, -, \times, \div$, $\sqrt[n]{}$ and $\sqrt[a]{}$.

14 The Fundamental Theorem of Algebra

Throughout the course we have regularly made use of the fundamental theorem of algebra.

Theorem 14.1 (The fundamental theorem of algebra)**.** *Let $f(x) \in \mathbb{R}[x]$ be a polynomial. Then there exists $\alpha \in \mathbb{C}$ such that $f(\alpha) = 0$.*

There are many proofs of this theorem coming from different areas of mathematics. We will provide a very algebraic proof which uses Sylow theory, a very important tool in finite group theory.

14.1 Sylow Theory

When looking at finite groups one of the first theorems proved is Lagrange's theorem.

Theorem 14.2 (Lagrange's Theorem)**.** *Let G be a finite group and $H \leqslant G$. Then $|H|$ divides $|G|$.*

In general there is no converse to Lagrange's theorem. In particular A_4 has no subgroup of order 6.

However we have some particular partial converses.

Theorem 14.3 (Cauchy's Theorem)**.** *Let G be a finite group and let p be a prime number such that p divides $|G|$. Then there is $g \in G$ such that $o(g) = p$, i.e. there is a subgroup of G of size p.*

Sylow theory is one particular generalisation of this theorem.

Namely, Sylow proved the following.

Theorem 14.4. *Suppose that G is a finite group and p is a prime number. Assume that $|G| = p^k m$ where $\gcd(m, p) = 1$. Then*

1. *There is a subgroup H of G such that $|H| = p^k$.*

2. *If H, K are two subgroups of size p^k, then there is a $g \in G$ such that $g^{-1}Hg = K$.*

3. *Let* $\mathrm{Syl}_p = \{H \leqslant G \mid |H| = p^k\}$. *Let* $n_p = |\mathrm{Syl}_p|$. *Then* $n_p \equiv 1 \mod p$ *and* n_p *divides* m.

Definition 14.5. Let G be as in the above theorem and H a subgroup of order p^k. Then we call H a *Sylow p-subgroup.*

Proof. To prove 1) we will show that there is a subgroup of order p^i for each $i \leqslant k$. Note that for $i = 1$ this is Cauchy's theorem.

Suppose that we have a subgroup H of size p^i for $i < k$. Then H acts on the set G/H by $\rho(h, gH) = hgH$ (Note: G/H need not be a group since H may not be a normal subgroup.) Since orbits of a group action partition the set, we see that $|G/H| = \sum |\mathcal{O}(x)|$.

The orbit stabiliser theorem also tells us that $|\mathcal{O}(x)| = p^j$ for some j. We also see that in the case that $j = 0$, then x is fixed by all of H. Thus reducing mod p we arrive at the equation $|G/H| \equiv \mathrm{Fix}(H) \mod p$. Let us examine what it means for gH to be in $\mathrm{Fix}(H)$.

$$\begin{aligned} hgH = gH \forall h \in H &\Leftrightarrow g^{-1}hgH = H \forall h \in H \\ &\Leftrightarrow g^{-1}hg \in H \forall h \in H \\ &\Leftrightarrow g^{-1}Hg = H. \end{aligned}$$

Thus we arrive at the set $N(H) = \{g \in G \mid g^{-1}Hg\}$. This is the normaliser of H and is a subgroup of G containing H. It is in fact the largest subgroup of G which contains H as a normal subgroup. Thus $\mathrm{Fix}(H) = N(H)/H$, the latter is a group.

Since we have the equality $|G/H| \equiv |N(H)/H| \mod p$ but since $|H| = p^i$ for $i < k$ we have that the left hand side is divisible by p. Thus $N(H)/H$ is a group with size divisible by p, thus there is a subgroup K of order p by Cauchy's theorem.

Thus we can take the preimage of K under the natural homomorphism $N(H) \to N(H)/H$ to get a subgroup of $N(H)$ of order p^{i+1}. Repeating in this fashion we get the desired result.

For part 2) suppose that H and K are both subgroups of size p^k. Consider the action of K on G/H then as above we get that $|G/H| \equiv |\mathrm{Fix}(K)| \mod p$. The left hand side is m and thus is not 0 modulo p. Thus the right hand side is non-empty. Thus we find a coset gH such that $kgH = gH$ for all $k \in K$. Thus $g^{-1}kg \in H$ for all $k \in K$ and we see that $g^{-1}Kg \subset H$ but these sets have the same size so they are in fact equal.

For 3) we will first prove that $n_p \equiv 1 \mod p$. Let $P \in \mathrm{Syl}_p$ and consider the action of P on Syl_p by conjugation. Once again we arrive at the fact that $n_p \equiv |\mathrm{Fix}(P)| \mod p$. Let us now examine $\mathrm{Fix}(P)$. This is the set of Sylow p subgroups Q such that $h^{-1}Qh = Q$ for all $h \in P$, (note that P is in this set).

I.e. P is a subgroup of $N(Q)$. However since $N(Q)$ is a subgroup of G we see that P and Q are Sylow p subgroups of $N(Q)$ and thus by 2) are conjugate. However Q is a normal subgroup of $N(Q)$ so $Q = P$. Thus $\mathrm{Fix}(P) = \{P\}$ and $n_p \equiv 1 \mod p$.

For the second half of 3), we look at the action of G on Syl_p by conjugation. By 2) there is one orbit of Sylow p subgroups, we can now use the orbit stabiliser theorem to see that $n_p = |{}^{G}\!/_{Stab(P)}|$ also the stabiliser of P is $N(P)$ which contains P and is a subgroup of G, thus $|{}^{G}\!/_{Stab(P)}|$ divides m. □

Proposition 14.6. *Let n_p be as above. Suppose that $n_p = 1$. Then the unique Sylow p subgroup H is normal.*

Proof. Let $g \in G$ we know that $g^{-1}Hg$ is a subgroup of G of order p^k. Thus since $n_p = 1$ we have that $g^{-1}Hg = H$. □

Proposition 14.7. *Let p, q be distinct primes. Let P be a Sylow p subgroup and Q be a Sylow q subgroup. Then*

1. *If $P \cap Q = \{e\}$.*
2. *If $n_p = 1$ and $n_q = 1$, then every element of P commutes with every element of Q.*

Proof. For 1) suppose that $h \in P \cap Q$. Then $o(h)$ divides p^k and also divides q^l and we must have $o(h) = 1$. Thus $h = e$.

For 2) let $g \in P$ and $h \in Q$, we wish to show that $gh = hg$, this is the same as showing $ghg^{-1}h^{-1} = e$. We can bracket $ghg^{-1}h^{-1}$ in two ways, firstly if we bracket it as $(ghg^{-1})h^{-1}$ we see that since Q is normal $ghg^{-1} \in Q$ and $h^{-1} \in Q$ so $ghg^{-1}h^{-1} \in Q$. Also if we write it as $g(hg^{-1}h^{-1})$ we see that since P is normal $hg^{-1}h^{-1} \in P$ and $g \in P$ so $ghg^{-1}h^{-1} \in P$ so $ghg^{-1}h^{-1} \in P \cap Q = \{e\}$. □

Proposition 14.8. *Let G be a group of order 15. Then G is Abelian.*

Proof. Let H be a Sylow 5 subgroup. Then $|H| = 5$ so $H \cong {}^{\mathbb{Z}}\!/_{5\mathbb{Z}}$ similarly any Sylow 3 subgroup K is isomorphic to ${}^{\mathbb{Z}}\!/_{3\mathbb{Z}}$. Since $n_p \equiv 1 \mod p$ and $n_p \div m$ we see that $n_5 = 1$ and $n_3 = 1$. Thus we have H, K are unique Sylow subgroups and are normal. We can now look at the subgroup HK. Since $H \cap K = \{e\}$ we see that $|HK| = 15$ and so $HK = G$, since H and K are Abelian and every element of H commutes with every element of K we see that G is Abelian. □

In the above proof we really just required that $n_5 = 1$ and $n_3 = 1$. To prove this we really just needed that $5 > 3$ and $5 \not\equiv 1 \mod 3$. Thus we can prove the following theorem.

Theorem 14.9. *Let G be a group of size pq where p and q are distinct primes. Suppose that $q > p$ and $q \not\equiv 1 \mod p$. Then G is Abelian.*

Proof. The proof follows the outline given above replacing 5 with q and 3 with p. □

We also know that groups of order p^2 are Abelian. This leaves us with the case that $|G| = pq$ and $q \equiv 1 \mod p$. In this case we cannot prove that the group is Abelian since S_3 satisfies this property and is not an Abelian group. However we can prove the following,

Theorem 14.10. *Let G be a group of order pq, where p and q are primes, then G is solvable.*

Proof. If $p = q$, then G is Abelian. Now suppose p, q are distinct primes we can assume that $p > q$. Since $p > q$ we see that $n_p = 1$, thus there is a normal Sylow p subgroup H. Since $|H| = p$ we see that H is a cyclic group of order p. Also G/H is of size q and so is also cyclic since q is a prime. Thus, we see that G is solvable. □

We can use this idea to prove that lots of groups are solvable and was very helpful in the classification of finite simple groups.

Theorem 14.11. *Let G be a group and $N \lhd G$. Suppose that N and G/N are solvable. Then G is solvable.*

14.2 Proof of the fundamental theorem of algebra

Before we prove the fundamental theorem we need one more group theory fact.

Theorem 14.12. *Let G be a group of order p^k, then G has a normal subgroup of size p.*

Proof. If G is Abelian, then we can just apply Cauchy's theorem.

Suppose that G is not Abelian, then we know that $Z(G) = \{h \in G \mid gh = hg \, \forall g \in G\} \neq \{e\}$. Thus $|Z(G)| = p^a$ for some $a \geqslant 1$. Thus $Z(G)$ has a subgroup of order p and we can see that any subgroup of $Z(G)$ is normal completing the proof. □

Corollary 14.13. *Every group of order p^k has a quotient of size p.*

Proof. If we repeatedly quotient by normal subgroups of order p we will arrive at the desired quotient. □

Theorem 14.14 (Fundamental Theorem of Algebra)**.** *Let $f(x) \in \mathbb{R}[x]$. Then there is a complex number α such that $f(\alpha) = 0$. In fact, $f(x)$ splits completely over $\mathbb{C}$.*