Algebra 145 Lecture Notes

Robert Kropholler

February 12, 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 $y^3 + (a_1 - \frac{a_2^2}{3})y + (\frac{2a_2^3}{27} - \frac{a_1a_2}{3} + a_0)$. Let $b = \left(a_1 - \frac{a_2^2}{3}\right)$ and $c = \left(\frac{2a_2^3}{27} - \frac{a_1a_2}{3} + a_0\right)$.

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 2.0.1. 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 2.0.2. 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 2.0.3. A ring K is a *field* if every non-zero elements has a multiplicative inverse.

Lemma 2.0.4. *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 2.0.5. *Let $\varphi \colon K \to L$ be a ring homomorphism between 2 fields K, L. Then φ is injective.*

Definition 2.0.6. 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 3.0.1. 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 3.0.2. *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 $\deg(r) < \deg(g)$.*

Proof. content... □

Corollary 3.0.3. *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 3.0.4. *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 3.0.5. *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 3.0.6. *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 4.0.1. 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 $Aut(R)$ of ring isomorphisms $R \to R$.

Lemma 4.0.2. *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 $g \in G$. □

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 4.1.1. 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 4.1.2. *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 5.0.1. 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 5.0.2. 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 5.0.3. 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 5.0.4. We say that a set is a *basis* if it is a linearly independent spanning set.

Lemma 5.0.5. *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 5.0.6. The *dimension* of a vector space is the size of any basis.

6 Field Extensions

Definition 6.0.1. A *field extension* L/K is an injection $\varphi\colon K \to L$. We denote such a field extension. We will often write $\begin{matrix} L \\ | \\ K \end{matrix}$

Definition 6.0.2. The *degree of the extension* L/K is written $[L : K]$, is the dimension of L as a K vector space.

Proposition 6.0.3. *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 6.0.4. 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 6.0.5. *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 6.0.6. We call the polynomial $m_a(x)$ the *minimal polynomial* for a.

Definition 6.0.7. 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 6.1.1. 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 6.1.2. *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 6.1.3. 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 6.1.4. *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 6.1.5. *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 6.2.1. 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 6.2.2. *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 6.2.3. *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 6.2.4. *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 6.2.5. *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 6.2.6. *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 7.0.1. 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 7.0.2. 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 7.0.3. *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. $\square$

8 Normal Extensions

Definition 8.0.1. 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.

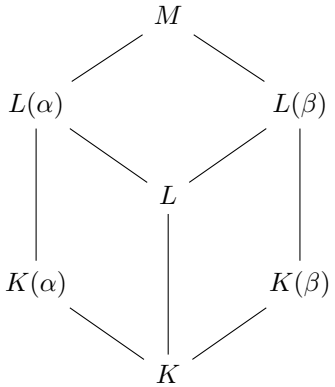
Non Example. The field $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not a normal extension. The polynomial $x^3 - 2$ has a root over this field but but since the other two roots of this polynomial are not real number we see that they are not elements of $\mathbb{Q}(\sqrt[3]{2})$ in which all elements are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

Theorem 8.0.2. *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

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

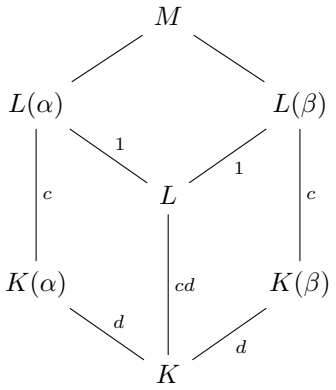
and deduce that $[L : K] = cd$.

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 9.0.1. 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 9.0.2. *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 9.0.3. *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 $\beta \in K(\gamma)$. □