Introduction

Quadratics (Babylonians):

$$X^2 + bX = c = (X + \frac{1}{2}b)^2 + c - \frac{b^2}{4}$$

$$= (X - x_1)(X - x_2) \implies x_1 x_2 = c, x_1 + x_2 = -b$$

$$x_1 = \frac{1}{2}\left[(x_1 + x_2) + (x_1 - x_2)\right] = \frac{1}{2}\left[-b + \sqrt{b^2 - 4c}\right]$$

Cubics (Italy, 16th Century):

$$X^3 + aX^2 + bX + c = (X - x_1)(X - x_2)(X - x_3)$$

$$\implies x_1 + x_2 + x_3 = -a, x_1 x_2 + x_1 x_3 + x_2 x_3 = b, x_1 x_2 x_3 = -c$$

WLOG $X \to X - a/3$ and $a = 0$

$$x_1 = \frac{1}{3}\left[(x_1 + x_2 + x_3) + \underbrace{(x_1 + \omega x_2 + \omega^2 x_3)}_{=u} + \underbrace{(x_1 + \omega^2 x_2 + \omega x_3)}_{=v}\right]$$

where $\omega = e^{2\pi i/3}$ so $\omega^2 + \omega + 1 = 0$. Cyclic permutation of x_1, x_2, x_3 gives $u \to \omega u \to \omega^2 u$ and $v \to \omega v \to \omega^2 v$ which implies u^3 and v^3 are invariant under cyclic permutations of the roots.

Also $u \leftrightarrow v$ under $x_2 \leftrightarrow x_3$. So $u^3 + v^3$, $u^3 v^3$ are invariant under permutations of roots.

In fact,
$$u^3 + v^3 = 27 x_1 x_2 x_3 = -27c$$
$$u^3 v^3 = -27b^2$$

So u^3, v^3 are roots of $Y^2 + 27cY - 27b^2$. This gives a formula for x_1 (Cardano's formula).

Can follow a similar method for quartics - auxilliary cubic equation. Unfortunately it doesn't work for quintics - the reason being <u>group theory</u>.

1   Polynomials

In this course, all rings are commutative and non-zero. Let R be a ring, then $R[X]$ denotes the ring of polynomials $\sum_{i=0}^{n} a_i X^i$, $a_i \in R$. A polynomial $f \in R[X]$ determines a function $R \to R$, $r \mapsto f(r)$.

The polynomial is not in general determined by this function, e.g let $R = \mathbb{Z}/p\mathbb{Z}$ (p prime). Then for all $a \in R$, $a^p = a$ so the polynomials X^p and X represent the same function.

In the case when $R = K$ (a field), $K[X]$ is a <u>Euclidean domain</u>. The "division algorithm" says that if $f, g \in K[X]$, $g \neq 0$ then there exists unique $q, r \in K[X]$ such that $f = gq + r$ and $\deg r < \deg g$ (define $\deg(0) = -\infty$).

In particular, if $g = X - a$ is linear then $f = (X - a)q + f(a)$ ("remainder theorem"). So $K[X]$ is also a PID and a UFD - every polynomial is a product of irreducible polynomials, and there are GCD's, computable via Euclids algorithm in the usual way.

Proposition 1.1. *If K is a field, $0 \neq f \in K[X]$, then f has at most $\deg f$ roots in K.*

Proof. If f has no roots then we are done. Otherwise, suppose $f(a) = 0$ for $a \in K$. Then
$$f = (X - a)g$$
for some $g \in K[X]$ and $\deg g = \deg f - 1$. If $b \in K$ is a root of f then either $b = a$ or $g(b) = 0$ so the number of roots of f is at most one more than the number of roots of g. Now done by induction. $\square$

2 Symmetric polynomials

Let R be a ring, consider $R[X_1, \ldots, X_n]$ for $n \geq 1$.

Definition. A polynomial $f \in R[X_1, \ldots, X_n]$ is *symmetric* if for every $\sigma \in S_n$, $f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = f$.

The set of symmetric polynomials is a <u>subring</u> of $R[X_1, \ldots, X_n]$.

Example. $X_1 + \ldots + X_n$, or more generally, $p_k = X_1^k + \ldots + X_n^k = \sum_{i=1}^n X_i^k$.

Alternative definition: if $f \in R[X_1, \ldots, X_n]$, define $f\sigma = f(X_{\sigma(1)}, \ldots, X_{\sigma(n)})$. This is an action (on the right) of S_n on $R[X_1, \ldots, X_n]$. A polynomial f is symmetric if and only if it is fixed by this action.

Definition. *The elementary symmetric polynomials* are
$$s_r(X_1, \ldots, X_n) = \sum_{1 \leq i_1 < \ldots < i_r \leq n} X_{i_1} X_{i_2} \ldots X_{i_r}$$

Example. When $n = 3$ we have
$$s_1 = X_1 + X_2 + X_3$$
$$s_2 = X_1 X_2 + X_1 X_3 + X_2 X_3$$
$$s_3 = X_1 X_2 X_3$$

Theorem 2.1.

(i) *Every symmetric polynomial over R can be expressed as a polynomial in $\{s_r : 1 \leq r \leq n\}$, with coefficients in R.*

(ii) *There are no non-trivial relations between $s_1, \ldots, s_n$.*

Remark:

(a) Consider the ring homomorphism

$$\theta : R[Y_1, \ldots, Y_n] \to R[X_1, \ldots, X_n], \ Y_r \mapsto s_r$$

then (i) says the image of θ is the set of symmetric polynomials. (ii) says that θ is injective.

(b) Equivalent definition of the s_r's is

$$\prod_{i=1}^{n}(T + X_i) = T^n + s_1 T^{n-1} + \ldots + s_{n-1}T + s_n$$

If we need to specify the number of variables, write $s_{r,n}$ instead of s_r.

Proof. Terminology:

- A *monomial* is some $X_I = X_1^{i_1} \ldots X_n^{i_n}$ for $I \in \mathbb{N}^n = \{0, 1, 2, \ldots\}^n$. Its (total) degree is $\sum_\alpha i_\alpha$.

- A *term* is some cX_I, for $0 \neq c \in R$. So a polynomial is uniquely a sum of terms.

- *Total degree* of f is the maximum degree over its terms

Lexicographical ordering on monomials X_I: write $X_I > X_J$ if either $i_1 > j_1$ or, for some $1 \leq r < n$, $i_1 = j_1, \ldots, i_r = j_r$ and $i_{r+1} > j_{r+1}$.

This is a total ordering: for each pair $I \neq J$, exactly one of $X_I > X_J$ or $X_J > X_I$ holds.

First we prove (ii):

Let d be the total degree of some symmetric polynomial f, and let X_I be the largest (in lexicographical order) monomial which occurs in f, with coefficient $c \in R$. As f is symmetric, we must have $i_1 \geq i_2 \geq \ldots \geq i_n$ (otherwise we could exchange variables to get a larger monomial).

So

$$X_I = X_1^{i_1 - i_2} (X_1 X_2)^{i_2 - i_3} \ldots (X_1, \ldots X_n)^{i_n}$$

consider

$$g = s_1^{i_1 - i_2} s_2^{i_2 - i_3} \ldots s_{n-1}^{i_{n-1} - i_n} s_n^{i_n}$$

the leading monomial (i.e largest in lexicographical order) of g is X_I, and g is symmetric. So $f - cg$ is symmetric of total degree $\leq d$, and its leading monomial term is smaller (lexicographical) than X_I. As the set of monomials of degree at most d is finite, this process terminates.

To prove (ii): induct on n. Suppose we have $G \in R[Y_1, \ldots, Y_n]$ with $G(s_{n,1}, \ldots, s_{n,n}) = 0$. We want to show $G = 0$. If $n = 1$, this is trivial ($s_{1,1} = X_1$). If $G = Y_n^k H$, with $Y_n \nmid H$, then $s_{n,n}^k H(s_{n,1}, \ldots, s_{n,n}) = 0$. As $s_{n,n} = X_1 \ldots X_n$, $s_{n,n}$ is not a zero divisor in $R[X_1, \ldots, X_n]$ so $H(s_{n,1}, \ldots, s_{n,n}) = 0$.

So we may assume G is not divisible by Y_n. Replace X_n by 0. Then

$$s_{n,r}(X_1, \ldots, X_{n-1}, 0) = \begin{cases} s_{n-1,r}(X_1, \ldots, X_{n-1}) & \text{if } r < n \\ 0 & \text{if } r = n \end{cases}$$

and so $G(s_{n-1,1}, \ldots, s_{n-1,n-1}, 0) = 0$. So by induction, $G(Y_1, \ldots, Y_{n-1}, 0) = 0$, i.e $Y_n \mid G$, a contradiction.

$\square$

Example. $f = \sum_{i \neq j} X_i^2 X_j$ for $n \geq 3$. The leading term is $X_1^2 X_2 = X_1(X_1 X_2)$. Then compute

$$s_1 s_2 = \sum_i \sum_{j<k} X_i X_j X_k = \sum_{i \neq j} X_i^2 X_j + 3 \sum_{i<j<k} X_i X_j X_k$$

so $f = s_1 s_2 - 3s_3$.

Computing say $\sum X_i^5$ by hand is tedious. But there are alternative formulae.

Recall $p_k = \sum_{i=1}^n X_i^k$ for $k \geq 1$.

Theorem 2.2 (Newton's formulae). *Let $n \geq 1$. Then for all $k \geq 1$*

$$p_k - s_1 p_{k-1} + \ldots + (-1)^{k-1} s_{k-1} p_1 + (-1)^k k s_k = 0$$

by convention, $s_0 = 1$, and $s_r = 0$ if $r > n$.

Proof. We may assume $R = \mathbb{Z}$ (or $\mathbb{R}$). Generating function

$$F(T) = \prod_{i=1}^n (1 - X_i T) = \sum_{r=0}^n (-1)^r s_r T^r$$

Take logarithmic derivative with respect to T:

$$\frac{F'(T)}{F(T)} = \sum_{i=1}^n \frac{-X_i}{1 - X_i T} = -\frac{1}{T} \sum_{i=1}^n \sum_{r=1}^\infty X_i^r T^r = -\frac{1}{T} \sum_{r=1}^\infty p_r T^r$$

So

$$-TF'(T) = s_1 T - 2s_2 T^2 + \ldots + (-1)^{n-1} n s_n T^n$$

$$= F(T) \sum_{r=1}^\infty p_r T^r = (s_0 - s_1 T + \ldots + (-1)^n s_n T^n)(p_1 T + p_2 T^2 + \ldots)$$

comparing coefficients of T^k gives the result. $\square$

Definition. The *discriminant polynomial* is

$$D(X_1, \ldots, X_n) = \Delta(X_1, \ldots, X_n)^2$$

where $\Delta = \prod_{i<j}(X_i - X_j)$. (Recall from IA Groups that applying $\sigma \in S_n$ to Δ multiplies Δ by $\mathrm{sgn}(\sigma)$, so D is symmetric.)

So $D(X_1, \ldots, X_n) = d(s_1, \ldots, s_n)$ for some polynomial d ($\mathbb{Z}$-coefficients). For example, when $n = 2$, $D = (X_1 - X_2)^2 = s_1^2 - 4s_2$.

Definition. Let $f = T^n + \sum_{i=0}^{n-1} a_{n-i} T^i \in R[T]$. Its *discriminant* is $\mathrm{Disc}(f) = d(-a_1, a_2, -a_3, \ldots, (-1)^n a_n) \in R$.

Observe that if $f = \prod_{i=1}^n (T - x_i)$, $x_i \in R$, then $a_r = (-1)^r s_r(x_1, \ldots, x_n)$, so

$$\mathrm{Disc}(f) = \prod_{i<j}(x_i - x_j)^2 = D(x_1, \ldots, x_n)$$

If moreover $R = K$ is a field, then $\mathrm{Disc}(f) = 0$ iff f has a repeated root (i.e $x_i = x_j$ for some $i \neq j$). E.g when $n = 2$, $\mathrm{Disc}(T^2 + bT + c) = b^2 - 4c$.

3   Fields

Recall:

Definition. A *field* is a ring K (commutative with a 1) in which every non-zero element has a multiplicative inverse. The set of non-zero elements of K is a group under multiplication, written $K^\times$ or K^*, called the *multiplicative group of* K.

Definition. The *characteristic of a field* K is the least positive integer p (if it exists) such that $p \cdot 1_K = 0_K$, or is said to be 0 if no such p exists.

Example. $\mathbb{Q}$ has characteristic 0 and $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ has characteristic p (p prime).

The characteristic $\mathrm{char}(K)$ of K is either 0 or a prime. Inside K, there is a smaller subfield, called the *prime subfield* of K. It is either isomorphic to $\mathbb{Q}$ (if characteristic is 0), or to $\mathbb{F}_p$ (if $\mathrm{char}(K) = p$).

Proposition 3.1. *Let $\varphi : K \to L$ be a homomorphism of fields. Then φ is an injection.*

Proof. $\varphi(1_K) = 1_L \neq 0$, so $\mathrm{Ker}(\varphi) \subsetneq K$ is a proper ideal of K, so $\mathrm{Ker}(\varphi) = (0)$ $\qquad\qquad\square$

Definition. Let $K \subseteq L$ be fields (where the field operations on K are the same as those on L). We say K is a *subfield of* L, and L is *an extension of* K, denoted L/K.

Remarks:

(i) The notation L/K has nothing to do with the quotient (some write $L \mid K$)

(ii) It is useful to be more general - if $i : K \to L$ is a homomorphism of fields, then Proposition 3.1 says that K is isomorphic to its image $i(K) \subseteq L$. In this situation, also say L is an extension of K.

Example. Some extensions include

- $\mathbb{C}/\mathbb{R}$

- $\mathbb{R}/\mathbb{Q}$

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

Definition. $K \subseteq L$, $x \in L$. Define $K[x] = \{p(x) : p \in K[T]\}$ (a subring of L). Define $K(x) = \{\frac{p(x)}{q(x)} : p, q \in K[T], q(x) \neq 0\}$ (a subfield of L) "K adjoin x". For $x_1, \ldots, x_n \in L$, define

$$K(x_1, \ldots, x_n) = \left\{ \frac{p(x_1, \ldots, x_n)}{q(x_1, \ldots, x_n)} : p, q \in K[T_1, \ldots, T_n], q(x_1, \ldots, x_n) \neq 0 \right\}$$

(Easy to check $K(x_1, \ldots, x_{n-1})(x_n) = K(x_1, \ldots, x_n)$). Likewise $K[x_1, \ldots, x_n]$ is defined analagously.

Definition. Suppose L/K is a field extension. Then L is naturally a vector space over its subfield K (forget multiplication by elements of L). We can ask if it is a finite-dimensional vector space, if so we say that L/K is a *finite extension* and write $[L : K] = \dim_K(L)$ for the dimension. The dimension is called the *degree of the extension L over K*. If the dimension is infinite write $[L : K] = \infty$.

$\dim_K$ denotes the dimension as a K-vector space. Of course L has dimension 1 over itself. As a K-vector space, $L \cong K^{[L:K]}$.

Example.

(i) $\mathbb{C}/\mathbb{R}$, $[\mathbb{C} : \mathbb{R}] = 2$

(ii) For any field K, $K(X) = $ field of rational functions in $X = $ field of fractions of polynomial ring $K[X] = \{\frac{p}{q} : p, q \in K[X], q \neq 0\}$. Then $[K(X) : K] = \infty$ since $1, X, X^2, \dots$ are linearly independent.

(iii) $\mathbb{R}/\mathbb{Q}$, $[\mathbb{R} : \mathbb{Q}] = \infty$. This follows from countability - every finite dimensional vector space over $\mathbb{Q}$ is countable.

This course is largely about properties (and symmetries) of <u>finite</u> extensions of fields.

Definition. We say an extension L/K is *quadratic* (*cubic,...*) if $[L : K] = 2(, 3, \dots)$

Proposition 3.2. *Suppose K is a <u>finite</u> field (necessarily of characteristic $p > 0$). Then $|K|$ is a power of p.*

Proof. Certainly $K/\mathbb{F}_p$ is finite, so $K \cong (\mathbb{F}_p)^n$ (as a vector space), where $n = [K : \mathbb{F}_p]$, so $|K| = p^n$. $\qquad\square$

Later on we will see that every prime power $q = p^n$ admits a field $\mathbb{F}_q$ with q elements.

Here is a simple but powerful fact:

Theorem 3.3 ("Tower Law")**.** *Suppose M/L and L/K are field extensions. Then M/K is a finite extension if and only if both M/L and L/K are finite. If so, then $[M : K] = [M : L][L : K]$.*

In fact, a slightly more general statement holds:

Theorem 3.4. *Let L/K be an extension, V an L-vector space. Then $\dim_K(V) = [L : K]\dim_L(V)$ (and obvious conclusions if any quantities are infinite).*

Example. If $V = \mathbb{C}^n$ then $V \cong \mathbb{R}^{2n}$.

Proof. Let $\dim_L(V) = d < \infty$. Then $V \cong L \oplus \ldots \oplus L = L^d$ as an L-vector space, so also as a K-vector space. If $[L : K] = n < \infty$, then $L \cong K^n$ as a K-vector space, so

$$V \cong \underbrace{K^n \oplus \ldots \oplus K^n}_{d \text{ times}} = K^{nd}$$

so $\dim_K(V) = [L : K]\dim_L(V)$. If V is finite-dimensional over K, then a K-basis for V certainly spans V over L. So if $\dim_L(V) = \infty$ then $\dim_K(V) = \infty$. Likewise, if $[L : K] = \infty$ and $V \neq \{0\}$, then V has an infinite linearly independent subset, so $\dim_K(V) = \infty$. $\qquad\square$

Another important fact:

Proposition 3.5.

(i) *Let K be a field, $G \subseteq K^\times$ a <u>finite</u> subgroup. Then G is cyclic*

(ii) *If K is finite, then $K^\times$ is cyclic*

Proof. We prove (i) ((ii) follows immediately): (recall from IB GRM) we can write

$$G \cong \frac{\mathbb{Z}}{m_1\mathbb{Z}} \oplus \ldots \oplus \frac{\mathbb{Z}}{m_k\mathbb{Z}}$$

where $1 < m_1 \mid m_2 \mid \ldots \mid m_k = m$. So for all $x \in G$, $x^m = 1$. As K is a field, the polynomial $T^m - 1$ has at most m roots. So $|G| < m$. Hence $k = 1$ and G is cyclic.

$\qquad\square$

Remark: Let $K = F = \mathbb{Z}/p\mathbb{Z}$. The above says there exists $a \in \{1, \ldots, p-1\}$ such that $\mathbb{Z}/pZ = \{0\} \cup \{a, a^2, \ldots, a^{p-1}\}$. a is called a primitive root modulo p.

Proposition 3.6. *Let R be a ring, p a prime such that $p \cdot 1_R = 0_R$ (e.g R a field of characteristic p). Then the map*

$$\varphi_p : R \to R, \ \varphi_p(x) = x^p$$

is a homomorphism from R to itself (called the Frobenius endomorphism of R).

Proof. Have to show:

- $\varphi_p(1) = 1$

- $\varphi_p(xy) = \varphi_p(x)\varphi_p(y)$

- $\varphi_p(x + y) = \varphi_p(x) + \varphi_p(y)$

The first two are obvious. For the last one,

$$\varphi_p(x + y) = x^p + \sum_{i=1}^{p-1} \underbrace{\binom{p}{i}}_{\equiv 0 \pmod{p}} x^i y^{p-i} + y^p$$

$$= \varphi_p(x) + \varphi_p(y)$$

$\square$

Example. This gives another proof of Fermat's Little Theorem: $x^p \equiv x \pmod{p}$ (induction on x: $(x+1)^p = x^p + 1$).

4 Algebraic elements and extensions

Definition. Have L/K an extension, $x \in L$. We say x is *algebraic over K* if there exists a non-zero polynomial $f \in K[T]$ such that $f(x) = 0$. Otherwise we say x is *transcendental over K*.

Suppose $f \in K[T]$; evaluation $f(x) \in L$. This gives a map $\mathrm{ev}_x : K[T] \to L$, $f \mapsto f(x)$. This is obviously a homomorphism of rings.

$I = \mathrm{Ker}(\mathrm{ev}_x) \subseteq K[T]$ is an ideal (the set of polynomials which vanish at x). As $\mathrm{Im}(\mathrm{ev}_x)$ is a subring of L, it is an integral domain. So I is a <u>prime</u> ideal. Two possibilities:

(i) $I = \{0\}$. Then the only f with $f(x) = 0$ is $f = 0$. Hence x is transcendental over K.

(ii) $I \neq \{0\}$. As $K[T]$ is a PID, there exists a unique monic irreducible $g \in K[T]$ such that $I = (g)$. So $f(x) = 0$ if and only if f is a multiple of g. So x is algebraic over K; we call g the *minimal polynomial* of x over K. written $m_{x,K}$. It is the unique monic irreducible polynomial such that x is a root (and the monic polynomial of least degree with this property). [Depends on K as well as x]

Example.

- $x \in K$, $m_{x,K} = T - x$

- p prime, $d \geq 1$. Then $T^d - p \in \mathbb{Q}[T]$ is irreducible (Eisenstein's criterion) so it is the minimal polynomial of $\sqrt[d]{p} = x \in \mathbb{R}$ over $\mathbb{Q}$.

- $z = e^{2\pi i/p}$ (p prime) is a root of $T^p - 1$ and of $\frac{T^p - 1}{T - 1} = g(T) = T^{p-1} + \ldots + T + 1 \in \mathbb{Q}[T]$. As

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

  which is irreducible by Eisenstein, so g is irreducible and g is the minimal polynomial of z over $\mathbb{Q}$.

Definition. The *degree of x over K* (x algebraic over K) is the degree of $m_{x,K}$, written $\deg_K(x)$ or $\deg(x/K)$.

Ring/field characterisation of algebraicity:

Proposition 4.1. *Let L/K be a field extension, $x \in L$. The following are equivalent*

(i) *x is algebraic over K*

(ii) *$[K(x) : K] < \infty$*

(iii) *$\dim_K K[x] < \infty$*

(iv) *$K[x] = K(x)$*

(v) *$K[x]$ is a field*

If these hold, then $\deg_K(x) = [K(x) : K]$.

Note: recall $K[x] = \{p(x)\}$, $K(x) = \left\{ \frac{p(x)}{q(x)} | q(x) \neq 0, p, q \in K[T] \right\}$.

Proof. (ii) $\iff$ (iii), (iv) $\iff$ (v) are obvious.

Show (iii) $\Rightarrow$ (v),(iv) and (ii): let $0 \neq y = g(x) \in K[x]$. Consider $K[x] \to K[x]$, $z \mapsto yz$. It is a K-linear transformation, injective as $y \neq 0$, and since $\dim_K K[x] < \infty$, it is a bijection. So there exists z such that $yz = 1$. So $K[x]$ is a field, equal to $K(x)$ and $[K(x) : K] < \infty$.

Show (v)$\Rightarrow$(i): wlog $x \neq 0$, then $x^{-1} = a_0 + a_1 x + \ldots + a_n x^n \in K[x]$. Then $a_n x^{n-1} + \ldots + a_0 x - 1 = 0$, so x is algebraic over K.

Show (i)$\Rightarrow$(iii) and degree formula: The image of $\mathrm{ev}_x : K[T] \to L$ is $K[x] \subseteq L$. x is algebraic over K so the kernel of this map is $(m_{x,K})$, which is a maximal ideal ($m_{x,K}$ is irreducible). Applying the first isomorphism theorem gives

$\underbrace{K[T]/(m_{x,K})}_{\text{field}} \cong K[x]$. $m_{x,K}$ is monic of degree $d = \deg_K(x)$. So $K[T]/(m_{x,K})$ has basis $1, T, \ldots, T^{d-1}$. So $\dim_K K[x] = d < \infty$. Furthermore $\deg_K(x) = [K(x) : K] = d$. $\qquad\square$

Corollary 4.2.

   (i) *$x_1, \ldots, x_n$ are algebraic over K if and only if $L = K(x_1, \ldots, x_n)$ is a finite extension over K. If so, every element of L is algebraic in K*

   (ii) *If x, y are algebraic over K, then so are $x \pm y$, xy and $1/x$ (if $x \neq 0$).*

   (iii) *Let L/K any extension. Then $\{x \in L : x \text{ algebraic over } K\}$ is a subfield of L*

Proof.

   (i) If x_n is algebraic over K, it's certainly algebraic over $K(x_1, \ldots, x_{n-1})$, so $[L : K(x_1, \ldots, x_{n-1})]$. So by induction on n and the Tower Law, $[L : K] < \infty$. Convsersely, if $[L : K] < \infty$, then the subfield $K(y)$ is finite over K for all $y \in L$, so y is algebraic over K by Proposition 4.1.

   (ii) $x + y, xy, \frac{1}{x} \in K(x, y)$. So algebraic by (i).

   (iii) Trivial from (ii).

$\qquad\square$

Example. $z = e^{2\pi i/p}$, p prime. z has degree $p - 1$. Let $x = 2\cos 2\pi/p = z + z^{-1} \in \mathbb{Q}(z)$. So x is algebraic over $\mathbb{Q}$. Note $\mathbb{Q}(z) \supseteq \mathbb{Q}(x) \supseteq \mathbb{Q}$, $z^2 - xz + 1 = 0$. Hence the degree of z over $\mathbb{Q}(x)$ is at most 2. We have $[\mathbb{Q}(z) : \mathbb{Q}] = p - 1$ so $[\mathbb{Q}(z) : \mathbb{Q}(x)] = 2$ or 1. But $z \notin \mathbb{Q}(x) \subseteq \mathbb{R}$. So $[\mathbb{Q}(z) : \mathbb{Q}(x)] = 2$ and by the tower law $\deg_\mathbb{Q}(x) = \frac{p-1}{2}$.

We have
$$z^{\frac{p-1}{2}} + z^{\frac{p-3}{2}} + \ldots + z^{-\frac{p-1}{2}} = 0$$

$z + z^{-1} = x$. So can express this polynomial as a polynomial in $z + z^{-1} = x$ of degree $\frac{p-1}{2}$.

Example. Let $x = \sqrt{m} + \sqrt{n}$, $m, n \in \mathbb{Z}$ such that m, n, mn are not squares. We have
$$(x - \sqrt{m})^2 = n = x^2 - 2\sqrt{m}x + m$$

So $[\mathbb{Q}(x) : \mathbb{Q}(\sqrt{m})] \leq 2$, since the above is a quadratic with coefficients in $\mathbb{Q}(\sqrt{m})$. In the exact same way we have $[\mathbb{Q}(x) : \mathbb{Q}(\sqrt{n})] \leq 2$. The quadratic also implies $\sqrt{m} \in \mathbb{Q}(x)$. So by the tower law either $[\mathbb{Q}(x) : \mathbb{Q}] = 4$ or $[\mathbb{Q}(x) : \mathbb{Q}] = 2$ and $\mathbb{Q}(x) = \mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{n})$ (since m, n not squares, $[\mathbb{Q}(\sqrt{m}) : \mathbb{Q}] = 2$).

$\mathbb{Q}(\sqrt{m}) = \mathbb{Q}(\sqrt{n})$ implies $\sqrt{m} = a + b\sqrt{n}$, $a, b \in \mathbb{Q}$. This implies $m = a^2 + b^2 n + 2ab\sqrt{n}$. $b = 0$ implies $m = a^2$ and $a = 0$ implies $mn = b^2 n^2$, a contradiction. So $\deg_\mathbb{Q}(x) = 4$.

Definition. An extension L/K is *algebraic* if every $x \in L$ is algebraic over K.

Proposition 4.3.

 (i) *Finite extensions are algebraic*

 (ii) *$K(x)$ is algebraic over K if and only if x is algebraic over K*

 (iii) *Let $M/L/K$ be a series of extensions. Then M/K is algebraic if and only if both M/L and L/K are algebraic*

Proof.

 (i) If $[L : K] < \infty$ then $\forall x \in L$, $[K(x) : K] < \infty$, so x is algebraic over K.

 (ii) ($\Rightarrow$) is by definition, ($\Leftarrow$) follows from (i).

 (iii) Assume M/K is algebraic. Then for all $x \in M$, x is algebraic over K, so certainly x is algebraic over L. So M/L is algebraic. Since $L \subseteq M$, L/K must be algebraic as M/K is.

 The other direction follows from the below Lemma.

$\square$

Lemma 4.4. *Let $M/L/K$ be a series of extensions, where L/K is algebraic. Let $x \in M$. Suppose x is algebraic over L. Then x is algebraic over K.*

Proof. There exists $f = T^n + a_{n-1}T^n + \ldots + a_0 \in L[T]$ with $f \neq 0$ and $f(x) = 0$. Let $L_0 = K(a_0, \ldots, a_{n-1})$, then as each $a_i \in L$ is algebraic over K, by Corollary 4.2, $[L_0 : K]$ is finite. As $f \in L_0[T]$, x is algebraic over L_0. So $[L_0(x) : L_0] < \infty$, so $[L_0(x) : K] < \infty$ by the tower law, and so $[K(x) : K] < \infty$ and x is algebraic over K. $\qquad\square$

Example. Let $K = \mathbb{Q}$, $L = \{x \in \mathbb{C} : x \text{ is algebraic over } \mathbb{Q}\} = \overline{\mathbb{Q}}$. This is a field by Corollary 4.2. Obviously $L/\mathbb{Q}$ is algebraic, but the extension is <u>not</u> finite. Indeed, for all $n \geq 1$, $\sqrt[n]{2} \in L$ and $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$ (as $T^n - 2$ is irreducible over $\mathbb{Q}$). So as this holds for any n, L can't be finite. We'll see other fields like $\overline{\mathbb{Q}}$ later on (algebraically closed fields).

5   Algebraic numbers in $\mathbb{R}$ and $\mathbb{C}$

Traditionally, $x \in \mathbb{C}$ is said to be *algebraic* if it's algebraic over $\mathbb{Q}$, and otherwise said to be *transcendental*. $\overline{\mathbb{Q}}$ is a subfield of $\mathbb{C}$. It is a proper subfield since $\mathbb{Q}[T]$ is countable, and each polynomial has countably (finitely) many roots, so there are countably many elements of $\overline{\mathbb{Q}}$.

However $\mathbb{C}$ is uncountable. So there are "lots" of transcendental numbers. This argument is non-constructive - it is harder to write a transcendental number explicitly, or to show some given number is transcendental.

Liouville showed that $\sum_{n \geq 1} \frac{1}{10^{n!}}$ is transcendental ("algebraic numbers can't be very well approximated by rationals").

Hermite, Lindermann showed that e and π are transcendental.

In the 20th Century: <u>Gelfond-Schneider Theorem</u>: if x, y are algebraic $(x \neq 1)$, then x^y is algebraic if and only if y is rational. For example, this implies $\sqrt{2}^{\sqrt{3}}$ is transcendental. Also $e^\pi = (-1)^{-i/2}$ is transcendental.

Ruler & compass constructions

We have 3 basic geometric operations (in plane geometry).

(A) Given $P_1, P_2, Q_1, Q_2 \in \mathbb{R}^2$ with $P_i \neq Q_i$, we can construct (with a ruler) the point of intersection of the lines P_1Q_1, P_2Q_2 (assuming they intersect properly).
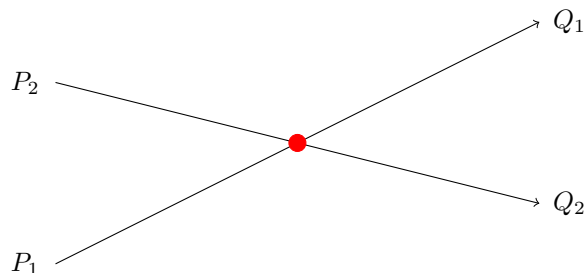
(B) Given P_1, P_2, Q_1, Q_2 with $P_i \neq Q_i$, we can construct the intersection points of the circles with centres P_i passing through Q_i.

(C) Can intersect lines with circles.

Definition. We say $(x, y) \in \mathbb{R}^2$ is *constructable from*

$$\{(x_1, y_1), \ldots, (x_n, y_n)\}$$

if it can be obtained by a finite sequence of constructions of type A,B,C, each involving only the starting points $\{(x_i, y_i) : 1 \leq i \leq n\}$ and any produced in a previous step.

Definition. We say $x \in \mathbb{R}$ is *constructable* if $(x, 0)$ is constructable from $\{(0, 0), (1, 0)\}$.

Note: every $x \in \mathbb{Q}$ is constructable, and so is $\sqrt{2}$.

Definition. Let $K \subseteq \mathbb{R}$ be a subfield. We say K is *constructable* if there exists some $n \geq 0$ and some sequence of fields $\mathbb{Q} = F_0 \subseteq F_1 \subseteq \ldots \subseteq F_n \subseteq \mathbb{R}$ and $a_i \in F_i$ (for $1 \leq i \leq n$) such that

(i) $K \subseteq F_n$

(ii) $F_i = F_{i-1}(a_i)$

(iii) $a_i^2 \in F_{i-1}$

Note: (ii) and (iii) imply that $[F_i : F_{i-1}] \leq 2$. So by the tower law, $K/\mathbb{Q}$ is finite and $[K : \mathbb{Q}]$ is a power of 2.

Theorem 5.1. *If $x \in \mathbb{R}$ is constructable, then $K = \mathbb{Q}(x)$ is constructable.*

Corollary 5.2. *If $x \in \mathbb{R}$ is constructable, then x is algebraic over $\mathbb{Q}$ and $\deg_{\mathbb{Q}}(x)$ is a power of 2 (follows from the above note and the theorem).*

Proof of Theorem 5.1. Induction on $k \geq 1$: we prove that if $(x, y) \in \mathbb{R}^2$ can be constructed with k R&C (Ruler & Compass) constructions, then $\mathbb{Q}(x, y)$ is a constructable extension of $\mathbb{Q}$.

So assume we have
$$\mathbb{Q} = F_0 \subseteq \ldots \subseteq F_n$$

satisfying (ii),(iii) and such that the coordinates of all points obtained after $(k-1)$ constructions lie in F_n.

Elementary analytic geometry tells us that in (A) the intersection point has coordinates which are rational functions of the coordinates of the points $\{P_i, Q_i\}$ with rational coefficients.

So if the kth construction is of type (A), then $x, y \in F_n$. For constructions (B) and (C), the coordinates of the two intersections can be written as $a \pm b\sqrt{e}$, $c \pm d\sqrt{e}$, where a, e are rational functions of the coordinates of $\{P_i, Q_i\}$. So for the two newly constructed points $x, y \in F_n(\sqrt{e})$, which is a constructable extension of $\mathbb{Q}$. $\qquad\square$

Remark: it is not hard to show that the converse is true, i.e if $\mathbb{Q}(x)/\mathbb{Q}$ is constructable then x is constructable.

Examples of classical problems:

1. "Squaring the circle" - construct a square whose area is that of a given circle, i.e have to construct $\sqrt{\pi}$. But since π is transcendental, it (and therefore $\sqrt{\pi}$) is not constructable.

2. "Duplicating the cube" - Construct a cube with volume twice that of a given cube, i.e construct $\sqrt[3]{2}$. But $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ is not a power of two, so $\mathbb{Q}(\sqrt[3]{2})$ (and so $\sqrt[3]{2}$) is not constructable.

3. "Trisect the angle" - say we are trying to trisect $2\pi/3$, which is certainly constructable. So if we can trisect $2\pi/3$, we can construct the angle $2\pi/9$, i.e the real numbers $\cos(2\pi/9), \sin(2\pi/9)$ are constructable. By the formula
$$\cos 3\theta = 4\cos^3 \theta - 3\cos \theta$$
we note $\cos(2\pi/9)$ is a root of $8X^3 - 6X + 1$, and $2\cos(2\pi/9) - 2$ is a root of $X^3 + 6X^2 + 9X + 3$ which is irreducible over $\mathbb{Q}$ by Eisenstein's criterion. So $\deg_{\mathbb{Q}}(\cos(2\pi/9)) = 3$ (not a power of two) so not constructable.

Later in the course we will see the following theorem

Theorem (Gauss). *A regular n-gon is constructable if and only if n is the product of a power of 2 and distinct primes of the form $2^{2^k} + 1$ ("Fermat primes").*

6 Splitting fields

Problem: we have a field K, $f \in K[T]$ - find an extension L/K (preferably as small as possible) such that f factors in $L[T]$ as a product of linear polynomials.

Example. Let $K = \mathbb{Q}$. By the Fundamental Theorem of Algebra, we can factor any monic $f \in \mathbb{Q}[T]$ as
$$f = \prod_{i=1}^{n}(T - x_i), \ x_i \in \mathbb{C}$$

(Later we will give another proof of the FTA.) So the "best" L would be $\mathbb{Q}(x_1, \ldots, x_n)$, a finite extension of $\mathbb{Q}$.

Example. Let $K = \mathbb{F}_p$. Let f be irreducible of degree $d > 1$. How to find L?

First step: find an extension in which f has at least one root.

Key construction: suppose $f \in K[T]$ is (monic and) irreducible. Let $L_f = K[T]/(f)$. As f is irreducible, (f) is maximal and so L_f is a field. By construction, if $x = T \pmod{(f)} \in L_f$ (the coset $T + (f)$), then $f(x) = 0$. Hence L_f/K

is a field extension in which f has a root.

Questions:

- Is L_f unique?
- What about the remaining roots?

Theorem 6.1. *Let $f \in K[T]$ be irreducible and monic. Let $L_f = K[T]/(f)$, $t \in L_f$ the residue class $T + (f)$. Then L_f/K is a finite extension of fields, $[L_f : k] = \deg(f)$ and f is the minimal polynomial of t over K.*

Proof. See previous example. □

So we have an extension of K in which f has a root. To what extent is this unique?

Also recall that if x is algebraic over K, then $K(x) \cong K[T]/(m_{x,K})$, where $m_{x,K}$ is the minimal polynomial of x over K.

Definition. Suppose K is a field, L/K and M/K extensions of K. A K-*homomorphism* from L to M is a field homomorphism $\sigma : L \to M$ such that $\sigma|_K = \mathrm{id}_K$. We also sometimes call this a K-*embedding*, since σ is an injection.

Theorem 6.2. *Let $f \in K[T]$ be irreducible, L/K be an arbitrary extension. Then*

(i) *If $x \in L$ is a root of f, then there exists a unique K-homomorphism $\sigma : L_f \to L$ sending $T + (f)$ to x.*

(ii) *Every K-homomorphism $L_f \to L$ arises as in (i). So there is a bijection between*

$$\{K\text{-}homomorphisms\ L_f \xrightarrow{\sigma} L\} \leftrightarrow \{roots\ of\ f\ in\ L\}$$

In particular, there are at most $\deg(f)$ such σ.

Proof. Note

$$
\begin{aligned}
f(x) = 0 \iff & \ \mathrm{ev}_x(f) = 0 \\
\iff & \ \mathrm{Ker}(\mathrm{ev}_x) = (f) \\
\iff & \ \mathrm{ev}_x \text{ comes from a homomorphism } \sigma : K[T]/(f) \to L \\
& \ \text{which is the identity on } K
\end{aligned}
$$

where $\mathrm{ev}_x : K[T] \to L$ is the homomorphism $g \mapsto g(x)$. □

Corollary 6.3. *If $L = K(x)$ for x algebraic over K, then there exists a unique isomorphism $\sigma : L_f \to K(x)$ such that $\sigma(t) = x$, with $f = m_{x,K}$.*

Proof. Take $L = K(x)$ in the above Theorem. □

Definition. Let x, y be algebraic over K. We say x, y are K-*conjugate* if they have the same minimal polynomial.

Then by the last corollary, both $K(x)$ and $K(y)$ are isomorphic to L_f (where f is their common minimal polynomial).

Corollary 6.4. *x, y are K-conjugate if and only if there exists a K-isomorphism $\sigma : K(x) \to K(y)$ with $\sigma(x) = y$.*

Proof. ($\Rightarrow$) follows by corollary 6.3.

($\Leftarrow$) follows since for all g in $K[T]$ we have $\sigma(g(x)) = g(\sigma(x)) = g(y)$ so x, y have the same minimal polynomial. $\square$

Moral: "the roots of an irreducible polynomial are algebraically indistinguishable".

It is useful (for inductive arguments) to have a generalisation of Theorem 6.2.

Definition. Let L/K, L'/K' be field extensions. Let $\sigma : K \to K'$ be a homomorphism of fields. If $\tau : L \to L'$ is a homomorphism such that $\tau(x) = \sigma(x)$ whenever $x \in K$, we say τ is a *σ-homomorphism* from L to L'. We also say τ *extends σ* or that σ is *the restriction of τ* to K. We write $\sigma = \tau|_K$.

From this definition we have the following variant of Theorem 6.2:

Theorem 6.5. *Let $f \in K[T]$ be irreducible, and $\sigma : K \to L$ be any homomorphism of fields. Let σf be the polynomial given by applying σ to the coefficients of f. Then*

   (i) If $x \in L$ is a root of σf, there exists a unique σ-homomorphism $\tau : L_f \to L$ such that $\tau(t) = \tau(T + (f)) = x$

   (ii) Every σ-homomorphism $L_f \to L$ is of the form arising from (i), so we have a bijection

$$\{\sigma\text{-homomorphisms } L_f \to L\} \leftrightarrow \{\text{roots of } \sigma f \text{ in } L\}$$

Example. σ might not be the "obvious" homomorphism. Indeed take $K = \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{R}$, and take $L = \mathbb{C}$. There is a homomorphism $\sigma : K \to L$ given by $x + y\sqrt{2} \mapsto x - y\sqrt{2}$. Now take $f = T^2 - (1 + \sqrt{2})$. The map $L_f \xrightarrow{\tau} \mathbb{C}$ must take $t = T + (f)$ to $\pm\sqrt{1 - \sqrt{2}} = \pm i\sqrt{\sqrt{2} - 1} \in \mathbb{C}$.

If instead we took σ to be the inclusion τ takes t to $\pm\sqrt{\sqrt{2} + 1}$.

What about all roots?

Definition. Let $f \in K[T]$ be a non-zero polynomial (not necessarily irreducible). An extension L/K is a *splitting field* for f over K if

   (i) f splits into linear factors in $L[T]$.

   (ii) $L = K(x_1, \ldots, x_n)$ where $\{x_1, \ldots, x_n\}$ are the roots of f in L.

Remark: (ii) says that f doesn't split into linear factors over any field L' with $K \subseteq L' \subsetneq L$. Furthermore, any splitting field is necessarily finite since the $\{x_1, \ldots, x_n\}$ are algebraic.

Theorem 6.6. *Every non-zero polynomial in $K[T]$ has a splitting field.*

Proof. Induction on $\deg(f)$ (for all K). If $\deg(f) = 0$ or 1, then K is a splitting field. So assume that for all fields K' and all polynomials of degree less than $\deg(f)$, there is a splitting field.

Consider g, an irreducible factor of f. Consider $K' = L_g = K[T]/(g)$. Let $x_1 = T + (g)$. Then $g(x_1) = 0$, so $f(x_1) = 0$ and $f = (T - x_1)f_1$, for some $f_1 \in K'[T]$ and $\deg(f_1) < \deg(f)$. So by induction there is a splitting field L for f_1 over K'. Let $x_2, \ldots, x_n \in L$ be the roots of f_1 in L. Then f splits into linear factors in L, with roots $x_2, \ldots, x_n$, and $L = K'(x_2, \ldots, x_n) = K(x_1, \ldots, x_n)$. So L is a splitting field for f over K. $\qquad\square$

Theorem 6.7 ("Splitting fields are unique"). *Let $f \in K[T]$ be non-zero, let L/K be a splitting field for f. Let $\sigma : K \to M$ be an extension such that $\sigma f \in M[T]$ splits [into linear factors] in $M[T]$. Then*

(i) *σ can be extended to a homomorphism $\tau : L \to M$.*

(ii) *If M is a splitting field for σf over $\sigma(K)$, then any τ as in (i) is an isomorphism. In particular, any two splitting fields for f are K-isomorphic.*

Remarks:

- It is not obvious without this theorem that two splitting fields have the same degree, because of the choices we had in the construction.

- Typically there will be more than one τ.

Proof.

(i) Induction on $n = [L : K]$. If $n = 1$ then $L = K$ and we are done.

   Let $x \in L \setminus K$ be a root of an irreducible factor $g \in K[T]$ of f, with $\deg(g) > 1$. Let $y \in M$ be a root of $\sigma g \in M[T]$ (since σf splits in M this exists). Theorem 6.4 implies there exists $\sigma_1 : K(x) \to M$ such that $\sigma_1(x) = y$ and σ_1 extends σ.

   Now $[L : K(x)] < [L : K]$ and L is certainly a splitting field for f over $K(x)$ and $\sigma_1 f = \sigma f$ splits in M. So by induction we can extend σ_1 to a homomorphism $\tau : L \to M$.

(ii) Assume M is a splitting field for σf over $\sigma(K)$. Let τ be as in (i) and $\{x_i\}$ the roots of f in L. Then the roots of σf in M are just $\{\tau(x_i)\}$. Since M is a splitting field, $M = \sigma K(\tau(x_1), \ldots, \tau(x_n)) = \tau(L)$. So τ is an isomorphism. If $K \subseteq M$ and σ is the inclusion, τ is a K-isomorphism from L to M.

$\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad$ $\square$

Example.

(i) $f = T^3 - 2 \in \mathbb{Q}[T]$. In $\mathbb{C}$, $f = (T - \sqrt[3]{2})(T - \omega\sqrt[3]{2})(T - \omega^2\sqrt[3]{2})$ where $\omega = \exp(2\pi i/3)$. So a splitting field for f over $\mathbb{Q}$ is $L = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2})$. Then $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ and $\mathbb{Q}(\sqrt[3]{2}) \subseteq \mathbb{R}$, but $\omega \notin \mathbb{R}$, $\omega^2 + \omega + 1 = 0$, so $[L : \mathbb{Q}(\sqrt[3]{2})] = 2$ and $[L : \mathbb{Q}] = 6$.

(ii) $f = \frac{T^5 - 1}{T - 1} = T^4 + T^3 + T^2 + T + 1 \in \mathbb{Q}[T]$. Let $z = \exp(2\pi i/5)$. Then $f = \prod_{1 \le a \le 4}(T - z^a)$. So $\mathbb{Q}(z)$ is already a splitting field over $\mathbb{Q}$ and $[\mathbb{Q}(z) : \mathbb{Q}] = 4$.

(iii) $f = T^3 - 2 \in \mathbb{F}_7[T]$. This is irreducible since 2 is not a cube modulo 7. Consider the field $L = \mathbb{F}_7[X]/(X^3 - 2) = \mathbb{F}_7(x)$. Then $x^3 = 2$. Now $2^3 = 1 = 4^3$ in $\mathbb{F}_7$. So $(2x)^3 = (4x)^3 = 2$ and so $f = (T - x)(T - 2x)(T - 4x) \in L[T]$

7   Normal extensions

Philosophy: pass from polynomials to fields generated by their roots.

Here we will see an "intrinsic" characterisation of splitting fields.

Definition. An extension L/K is said to be *normal* if L/K is algebraic and for every $x \in L$, $m_{x,K}$ splits into linear factors over L.

Note: this condition is equivalent to: for every $x \in L$, L contains a splitting field for $m_{x,K}$. Or again, for every $f \in K[T]$ irreducible, if f has a root in L, then it splits over L.

Theorem 7.1 ("Splitting fields are normal"). *Let L/K be a finite extension. Then L is normal over K if and only if L is the splitting field for some $f \in K[T]$ (not necessarily irreducible).*

Proof. Suppose L/K is normal, and write $L = K(x_1, \ldots, x_n)$. Then $m_{x_i,K}$ splits in L, and L is generated by the roots of $f = \prod_i m_{x_i,K}$. So L is a splitting field for f.

Conversely, if L is the splitting field for $f \in K[T]$. Let $x \in L$, $m_{x,K} = g$ its minimal polynomial - we want to show g splits in f. Let M be a splitting field for g over L, and $y \in M$ some root of g. We want to show $y \in L$. Since L is a splitting field for f over K, L is a splitting field for f over $K(x)$, and $L(y)$ is a splitting field for f over $K(y)$.

Now there exists a K-isomorphism between $K(x)$ and $K(y)$ as x, y are both roots of the same irreducible polynomial $g \in K[T]$. So $[L : K(x)] = [L(y) : K(y)]$ by uniqueness of splitting fields. Hence multiply both sides by $[K(x) : K] = [K(y) : K] = \deg(g)$, and use the tower law to see $[L : K] = [L(y) : K] = [L(y) : L][L : K]$. So $L(y) = L$, i.e $y \in L$. $\qquad\square$

There is a "field-theoretic" version of a splitting field:

Corollary 7.2 ("Normal closure"). *Let L/K be a finite extension. Then there exists a finite extension M/L such that*

(i) *M/K is normal*

(ii) *If $L \subseteq M' \subseteq M$ and M'/K is normal, then $M' = M$*

Moreover, any two such extensions M are L-isomorphic.

Proof. Say $L = K(x_1, \ldots, x_k)$. Let $f = \prod_i m_{x_i, K}$. Let M be a splitting field for f over L. Then as the x_i's are roots of f, M is also a splitting field for f over K. So M/K is normal. Let M' be as in (ii); then as $x_i \in M'$, $m_{x_i, K}$ splits in M' (as M'/K is normal). So $M' = M$.

For uniqueness: any M satisfying (i) must contain a splitting field for f, and by the above, (ii) implies that M is a splitting field for f. So uniqueness follows from uniqueness of splitting fields. $\qquad\square$

8 Seperability

Over $\mathbb{C}$, we can tell if f has multiple zeros by looking at its derivative. Over arbitrary fields, turns out the same is true if we replace the analytic notion of differentiation with an algebraic one.

Definition. The *(formal) derivative* of a polynomial $f = \sum_{0 \leq i \leq d} a_i T^i \in K[T]$ is $f' = \sum_{1 \leq i \leq d} i a_i T^{i-1}$.

It is easy to check that $(f + g)' = f' + g'$, $(fg)' = f'g + fg'$ and $(f^n)' = nf'f^{n-1}$.

Example. Let K be a field of characteristic $p > 0$. Then if $f = T^p + a_0$, $f' = pT^{p-1} + 0 = 0$. So it is possible to have a non-constant polynomial with zero derivative.

Proposition 8.1. *Let $f \in K[T]$, L/K an extension and $x \in L$ a root of f. Then x is a simple root if and only if $f'(x) \neq 0$.*

Proof. Write $f = (T - x)g \in L[T]$. Then $f' = g + (T - x)g'$ so $f'(x) = g(x)$ and $g(x)$ is non-zero if and only if $(T - x) \nmid g$, i.e x is a simple root of f. $\qquad\square$

Definition. We say $f \in K[T]$ is *seperable* if it splits into distinct linear factors in a splitting field (i.e has $\deg(f)$ distinct roots).

Corollary 8.2. *f is seperable if and only if $\gcd(f, f') = 1$.*

Note: we take $\gcd(f, g)$ to be the unique monic h such that $(h) = (f, g)$. Then $h = af + bg$ for some a, b which can be computed by Euclids algorithm. Observe that $\gcd(f, g)$ is the same in $K[T]$ or $L[T]$ for any $K \subseteq L$, since Euclids algorithm gives the same result.

Proof of Corollary. Replacing K by a splitting field for f, we may assume f has all its roots in K. Now f is seperable if and only if f, f' have no common root, which holds if and only if $\gcd(f, f') = 1$. $\square$

Example. $\mathrm{char}(K) = p > 0$, $f = T^p - b$, $b \in K$. Then $f' = 0$ so $\gcd(f, f') = f \neq 1$. So f is inseperable. Let L be any extension of K containing some $a \in L$ such that $a^p = b$. Then $f = (T - a)^p = T^p + (-a)^p = T^p - b$. So f has only one root in a splitting field. In fact, if b isn't a pth power in K, then f is irreducible (Exercise).

Theorem 8.3.

 (i) *Let $f \in K[T]$ be irreducible. Then f is seperable if and only if $f' \neq 0$.*

 (ii) *If $\mathrm{char}(K) = 0$ then every irreducible polynomial in $K[T]$ is seperable.*

 (iii) *If $\mathrm{char}(K) = p > 0$ then an irreducible $f \in K[T]$ is inseperable if and only if $f = g(T^p)$ for some $g \in K[T]$.*

Proof.

 (i) Assume wlog that f is monic. Then as f is irreducible, $\gcd(f, f') = f$ or 1. But $\deg(f) > \deg(f')$ so $\gcd(f, f') \neq f$ unless $f' = 0$, and converse is obvious.

 (ii) Write $f = \sum_{0 \leq i \leq d} a_i T^i$, $f' = \sum_{1 \leq i \leq d} i a_i T^{i-1}$. So $f' = 0$ if and only if $i a_i = 0$ for all $1 \leq i \leq d$, so $a_i = 0$ for all $1 \leq i \leq d$ (since characteristic 0). Hence f is constant, and not irreducible.

 (iii) As above get $i a_i = 0$ for all $1 \leq i \leq d$, and $a_i = 0$ for all i not divisible by p. Thus $f = g(T^p)$ where $g = \sum_i a_{pi} T^i$.

                                                                            $\square$

Now we go from polynomials to fields:

Definition. Let L/K be an extension. Say $x \in L$ is *seperable over K* if x is algebraic over K and $m_{x,K}$ is seperable. Say L/K is *seperable over K* if x is seperable over K for all $x \in L$.

Theorem 8.4. *Let x be algebraic over K, and L/K any extension in which $m_{x,K}$ splits. Then x is seperable over K if and only if there are exactly $\deg_K(x)$ K-homomorphisms from $K(x) \to L$.*

Proof. Recall (from 6.2) that the number of such homomorphisms is the number of roots of $m_{x,K}$ in L. This is equal to $\deg_K(x)$ if and only if $m_{x,K}$ splits. $\square$

Notation: write $\mathrm{Hom}_K(L, M) = \{K\text{-homomorphisms } L \to M\}$ (not to be confused with linear maps $L \to M$).

Theorem 8.5 ("Counting embeddings"). *Let $L = K(x_1, \ldots, x_k)$ be a finite extension of K, and M/K any extension. Then $|\mathrm{Hom}_K(L, M)| \leq [L : K]$ with equality if and only if*

(i) *For all i, $m_{x_i, K}$ splits into linear factors over M*

(ii) *All the x_i are seperable over K*

Remarks:

1. (i) and (ii) are the same as saying $m_{x_i, K}$ splits into distinct linear factors in M

2. Obvious variant: take any homomorphism $\sigma : K \to M$ and the condition becomes that the number of σ-homomorphisms is bounded by $[L : K]$ with equality if and only if for all i, $\sigma m_{x_i, K}$ splits over M

Proof. Induction on k. If $k = 0$ we're done. For $k \geq 1$ take $K_1 = K(x_1)$, $\deg_{K_1}(x_1) = d = [K_1 : K]$. Then $|\mathrm{Hom}_K(K_1, M)| = e = |\{\text{roots of } m_{x_1, K} \text{ in } M\}| \leq d$. Let $\sigma : K_1 \to M$ be a K-homomorphism. Apply induction to L/K_1. So there exist at most $[L : K_1]$ extensions of σ to a homomorphism $L \to M$. So $|\mathrm{Hom}_K(L, M)| \leq e[L : K_1] \leq d[L : K_1] = [L : K]$.

If equality holds, then $e = d$, i.e $M_{x_1, K}$ has d distinct roots in M. But we could have taken any other x_i instead of x_1 in the above, to get (i) and (ii).

Conversely, assume (i) and (ii) hold. Then by the previous theorem $|\mathrm{Hom}_K(K_1, M)| = d$ and (i), (ii) still hold over K_1. So by induction on k, each $\sigma : K_1 \to M$ has $[L : K_1]$ extensions to $L \to M$, so $|\mathrm{Hom}_K(L, M)| = [L : K]$. $\qquad\square$

Theorem 8.6 ("Seperably generated implies seperable"). *Let $L = K(x_1, \ldots, x_k)$ be a finite extension of K. Then L/K is seperable over K if and only if x_i is seperable over K for all i.*

Proof. If L/K is seperable, all the x_i are seperable by definition. So assume all the x_i are seperable over K, and let M be a normal closure (splitting field of $\prod_i m_{x_i, K}$ over L). Then in the previous theorem, both (i) and (ii) are satisfied so $|\mathrm{Hom}_K(L, M)| = [L : K]$. But if $x \in L$, then $L = (x, x_1, \ldots, x_k)$ as well. So by the previous theorem again, x is seperable. $\qquad\square$

Corollary 8.7. *Let $x, y \in L$, L/K an extension of K. If x, y are seperable over K, so are $x + y$, xy and $1/x$ (if $x \neq 0$).*

Proof. Apply previous theorem to $K(x, y)$. So $\{x \in L : x \text{ seperable over } K\}$ forms a subfield of L. $\qquad\square$

Theorem 8.8 ("Primitive element theorem for seperable extensions"). *Let K be an infinite field, and $L = K(x_1, \ldots, x_k)$ a finite extension where $x_1, \ldots, x_k$ are seperable. Then there exists $x \in L$ such that $L = K(x)$ (by the previous, x is also seperable over K).*

Proof. It is enough to consider the case $k = 2$, $L = K(x, y)$ with x, y seperable over K. Let $n = [L : K]$ and let M be a normal closure for L/K. Then there exist n distinct K-homomorphisms $\sigma_i : L \to M$. Let $a \in K$ and consider $z = x + ay$. We will choose a such that $L = K(z)$.

As $L = K(x, y)$, $\sigma_i(x) = \sigma_j(x)$ and $\sigma_i(y)$ and $\sigma_j(y)$ occurs iff $\sigma_i = \sigma_j$, i.e $i = j$. Consider $\sigma_i(z) = \sigma_i(x) + a\sigma_i(y)$. If $\sigma_i(x) = \sigma_j(x)$ then $[\sigma_i(x) - \sigma_j(x)] - a[\sigma_i(y) - \sigma_j(y)] = 0$ and if $i \neq j$, at least one of these brackets is non-zero, so there exists at most one $a \in K$ for which it holds. So there is at most one a for which $\sigma_i(z) = \sigma_j(z)$. Since K is infinite, there exists a such that $\sigma_i(z)$ is distinct for all $1 \leq i \leq n$. But then $\deg_K(z) = n$, so $L = K(z)$. $\qquad\square$

For finite fields, the result is much easier:

Theorem 8.9. *If L/K is an extension of finite fields, then $L = K(x)$ for some $x \in K$.*

Proof. The multiplicative group $L^\times$ is cyclic. Let x be a generator of this group. Then $L = K(x)$. $\qquad\square$

9 Galois Theory

Automorphisms of fields: $\sigma : L \to L$ is an *automorphism* of the field L if it is a bijective homomorphism.

The set of automorphisms of L forms a group under composition of functions and is denoted $\mathrm{Aut}(L)$ (the "automorphism group of L").

If $S \subseteq \mathrm{Aut}(L)$, is a subset, let $L^S = \{x \in L : \forall \sigma \in S, \ \sigma(x) = x\}$. This is a subfield of L (since each σ is a homomorphism) and is called the *fixed field* of S.

E.g $L = \mathbb{C}$, $\sigma = $ complex conjugation. Then $L^{\{\sigma\}} = \mathbb{R}$. Let L/K be an extension. Define $\mathrm{Aut}(L/K) = \{K\text{-automorphisms of } L\} = \{\sigma \in \mathrm{Aut}(L) : \sigma(x) = x \ \forall x \in K\}$ (a subgroupf of $\mathrm{Aut}(L)$). Then $\sigma \in \mathrm{Aut}(L/K)$ if and only if $K \subseteq L^{\{\sigma\}}$.

Theorem 9.1. *Let L/K be finite. Then $|Aut(L, K)| \leq [L : K]$.*

Proof. Take $M = L$ in Theorem 8.5. Then $\mathrm{Hom}_K(L, M) = \mathrm{Aut}(L/K)$. $\qquad\square$

Fact: If $K = \mathbb{Q}$ or $\mathbb{F}_p$ then $\text{Aut}(K) = \{1\}$ ($\sigma(1_K) = 1_K$ implies $\sigma(m1_K) = m\sigma(1_K)$ for all $m \in \mathbb{Z}$). So for any L, $\text{Aut}(L) = \text{Aut}(L/K)$ where K is the prime subfield (copy of $\mathbb{Q}$ or $\mathbb{F}_p$).

There is a notion of when L/K has "many" symmetries.

Definition. An extension L/K is said to be *Galois* if it is algebraic and $L^{\text{Aut}(L/K)} = K$, i.e automorphisms detect when an element of L is in K.

Examples:

1. $\mathbb{C}/\mathbb{R}$ is Galois (e.g complex conjugation fixes only elements of $\mathbb{R}$). Likewise $\mathbb{Q}(i)/\mathbb{Q}$ is Galois.

2. $K/\mathbb{F}_p$ a finite extension. Then K is a finite field. The Frobenius automorphism $\varphi_p : K \to K$, $x \mapsto x^p$ has $K^{\{\varphi_p\}} = \{x \in K : x \text{ root } of T^p - T\}$. $T^p - T$ has at most p roots and everything in $\mathbb{F}_p$ is a root so $K^{\{\varphi_p\}} = \mathbb{F}_p$, i.e $K/\mathbb{F}_p$ is Galois.

Definition. If L/K is Galois, write $\text{Gal}(L/K) = \text{Aut}(L/K)$, the Galois group of L/K.

Theorem 9.2 (Classification of finite Galois extensions)**.** *Let L/K be a finite extension, $G = Aut(L/K)$. The following are equivalent*

(i) *L/K is Galois (i.e $L^G = K$)*

(ii) *L/K is normal and seperable*

(iii) *L is the splitting field of a seperable polynomial*

(iv) *$|Aut(L/K)| = [L : K]$.*

If so then the minimal polynomial of $x \in L$ is $m_{x,K} = \prod_{i=1}^{r}(T - x_i)$, where $\{x_1, \ldots, x_r\} = \{\sigma(x) : \sigma \in G\}$ is the orbit of G on x (the x_i are distinct)

Proof. First we show (i)⇒(ii) and the last part. Let $x \in L$, $\{x_1, \ldots, x_r\}$ be the orbit of G on x, $f = \prod(T - x_i)$. Then $f(x) = 0$. As G permutes $\{x_i\}$, $f \in L^G[T] = K[T]$, so $m_{x,K} \mid f$. Also since $m_{x,K}(\sigma(x)) = \sigma(m_{x,K}(x)) = 0$, every x_i is a root of $m_{x,K}$. So $f = m_{x,K}$ and x is seperable over K, and $m_{x,K}$ splits in L, so L/K is normal and seperable.

Now we show (ii)⇒(iii). By Theorem 7.1, L is a splitting field for some $f \in K[T]$. Write $f = \prod q_i^{e_i}$, where q_i are irreducible and $e_i \geq 1$. Since L/K is seperable, q_i are seperable, so $g = \prod q_i$ is seperable amd L is also a splitting field for g.

Now we show (iii)⇒(iv). Write $L = K(x_1, \ldots, x_k)$, the splitting field of some seperable f with roots x_i. Take $M = L$ and apply Theorem 8.5 as since $m_{x_i,K} \mid f$, the conditions for equality hold. Hence $|\text{Hom}_K(L, M)| = [L : K]$

Finally we show (iv)$\Rightarrow$(i). Suppose $|G| = [L : K]$. Then $G \subseteq \text{Aut}(L/L^G) \subseteq$ $\text{Aut}(L/K)$ so in fact $G = \text{Aut}(L/L^G)$, and $[L : K] = |G| \leq [L : L^G]$. As $L^G \supseteq K$, this implies that $L^G = K$ by the tower law. $\qquad\square$

Corollary 9.3. *Let L/K be a finite Galois extension. Then $L = K(x)$ for some x seperable over K of degree $[L : K]$.*

Proof. By (ii) in the previous theorem, L/K is seperable. So by the Primitive Element Theorem, $L = K(x)$ and the result follows. $\qquad\square$

Theorem 9.4 ("The Galois correspondence")**.** *Let L/K be a finite Galois extension, $G = \text{Gal}(L/K)$.*

(a) *Let $F \subseteq L$ be a subfield with $F \supseteq K$. Then L/F is a Galois extension, $\text{Gal}(L/F) \subseteq \text{Gal}(L/K)$. The map $F \mapsto \text{Gal}(L/K)$ is a bijection between $\{F \text{ field} : K \subseteq F \subseteq L\}$ and $\{\text{subgroups } H \text{ of } G\}$ whose inverse is the map taking H to the fixed field L^H. This bijection is inclusion-reversing and if $F = L^H$, $[F : K] = (G : H)$ (where $(G : H)$ denotes the index of the subgroup).*

Proof.

(a) Let $x \in L$. Then $m_{x,F}$ divides $m_{x,K}$ in $F[T]$. As $m_{x,K}$ splits into distinct linear factors in L, so does $m_{x,F}$. Hence L/F is normal and seperable, hence is Galois. By definition $\text{Gal}(L/F) \subseteq G$.

To check we have a bijection, with claimed inverse, note $F \mapsto H = \text{Gal}(L/F) \mapsto L^H$. But $L^{\text{Gal}(L/F)} = F$ as L/F is Galois, i.e $L^H = F$. Also $H \mapsto L^H \mapsto \text{Gal}(L/L^H)$. It is enough to show $[L : L^H] \leq |H|$ since certainly $H \subseteq \text{Gal}(L/L^H)$ and $|\text{Gal}(L/L^H)| \leq [L : L^H]$. By Corollary 9.3, $L = L^H(x)$ for some x, and $f = \prod_{\sigma \in H}(T - \sigma(x)) \in L^H[T]$, with x a root. So $[L : L^H] = \deg_{L^H}(x) \leq \deg(f) = |H|$. So we have a bijection.

If $F \subseteq F'$, then $\text{Gal}(L/F') \subseteq \text{Gal}(L/F)$, so the bijection is inclusion-reversing. Finally if $F = L^H$ then

$$[F : K] = \frac{[L : K]}{[L : F]} = \frac{|\text{Gal}(L/K)|}{|\text{Gal}(L/F)|} = \frac{|G|}{|H|} = (G : H)$$

$\qquad\square$