

## Introduction

Quadratics (Babylonians):

$$\begin{aligned} X^2 + bX + c &= (X + \frac{1}{2}b)^2 + c - \frac{b^2}{4} \\ &= (X - x_1)(X - x_2) \implies x_1x_2 = c, x_1 + x_2 = -b \\ x_1 &= \frac{1}{2} [(x_1 + x_2) + (x_1 - x_2)] = \frac{1}{2} [-b + \sqrt{b^2 - 4c}] \end{aligned}$$

Cubics (Italy, 16th Century):

$$\begin{aligned} X^3 + aX^2 + bX + c &= (X - x_1)(X - x_2)(X - x_3) \\ \implies x_1 + x_2 + x_3 &= -a, x_1x_2 + x_1x_3 + x_2x_3 = b, x_1x_2x_3 = -c \end{aligned}$$

WLOG  $X \rightarrow X - a/3$  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  $u \rightarrow \omega u \rightarrow \omega^2 u$  and  $v \rightarrow \omega v \rightarrow \omega^2 v$  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  $u^3 + v^3, u^3v^3$  are invariant under permutations of roots.

In fact,

$$\begin{aligned} u^3 + v^3 &= 27x_1x_2x_3 = -27c \\ u^3v^3 &= -27b^2 \end{aligned}$$

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 group theory.

## 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  $R \rightarrow R$ ,  $r \mapsto f(r)$ .

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 Euclidean domain. 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 Euclid’s 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  $R[X_1, \dots, X_n]$  for  $n \geq 1$ .

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

The set of symmetric polynomials is a subring of  $R[X_1, \dots, X_n]$ .

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

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

**Definition.** The *elementary symmetric polynomials* are

$$s_r(X_1, \dots, X_n) = \sum_{1 \leq i_1 < \dots < i_r \leq n} X_{i_1} X_{i_2} \dots X_{i_r}$$

**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  $s_1, \dots, s_n$ .*

**Remark:**

(a) Consider the ring homomorphism

$$\theta : R[Y_1, \dots, Y_n] \rightarrow R[X_1, \dots, X_n], \quad Y_r \mapsto s_r$$

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

(b) Equivalent definition of the  $s_r$ 's is

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

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

*Proof.* Terminology:

- A *monomial* is some  $X_I = X_1^{i_1} \dots X_n^{i_n}$  for  $I \in \mathbb{N}^n = \{0, 1, 2, \dots\}^n$ . 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  $1 \leq r < n$ ,  $i_1 = j_1, \dots, i_r = j_r$  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 (i):

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  $i_1 \geq i_2 \geq \dots \geq i_n$  (otherwise we could exchange variables to get a larger monomial).

So

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

consider

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

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  $G \in R[Y_1, \dots, Y_n]$  with  $G(s_{n,1}, \dots, s_{n,n}) = 0$ . 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  $s_{n,n}^k H(s_{n,1}, \dots, s_{n,n}) = 0$ . As  $s_{n,n} = X_1 \dots X_n$ ,  $s_{n,n}$  is not a zero divisor in  $R[X_1, \dots, X_n]$  so  $H(s_{n,1}, \dots, s_{n,n}) = 0$ .

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

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

and so  $G(s_{n-1,1}, \dots, s_{n-1,n-1}, 0) = 0$ . So by induction,  $G(Y_1, \dots, Y_{n-1}, 0) = 0$ , 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  $f = s_1 s_2 - 3 s_3$ .

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  $k \geq 1$*

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

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

$$\begin{aligned} -TF'(T) &= s_1 T - 2s_2 T^2 + \dots + (-1)^{n-1} n s_n T^n \\ &= F(T) \sum_{r=1}^{\infty} p_r T^r = (s_0 - s_1 T + \dots + (-1)^n s_n T^n) (p_1 T + p_2 T^2 + \dots) \end{aligned}$$

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

**Definition.** The *discriminant polynomial* is

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

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

So  $D(X_1, \dots, X_n) = d(s_1, \dots, s_n)$  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  $\text{Disc}(f) = d(-a_1, a_2, -a_3, \dots, (-1)^n a_n) \in R$ .

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

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

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

### 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  $\text{char}(K)$  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  $\text{char}(K) = p$ ).

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

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

**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  $i : K \rightarrow L$  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  $x_1, \dots, x_n \in L$ , define

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

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

**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 finite extensions of fields.

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

**Proposition 3.2.** Suppose  $K$  is a finite 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  $|K| = p^n$ .  $\square$

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  $V \cong L \oplus \dots \oplus L = L^d$  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

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

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  $\dim_K(V) = \infty$ .  $\square$

Another important fact:

**Proposition 3.5.**

- (i) Let  $K$  be a field,  $G \subseteq K^\times$  a finite 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

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

where  $1 < m_1 \mid m_2 \mid \dots \mid m_k = m$ . 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.  $\square$

**Remark:** Let  $K = F = \mathbb{Z}/p\mathbb{Z}$ . The above says there exists  $a \in \{1, \dots, p-1\}$  such that  $\mathbb{Z}/p\mathbb{Z} = \{0\} \cup \{a, a^2, \dots, a^{p-1}\}$ .  $a$  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*

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

*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,

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

□

**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  $\text{ev}_x : K[T] \rightarrow L$ ,  $f \mapsto f(x)$ . This is obviously a homomorphism of rings.

$I = \text{Ker}(\text{ev}_x) \subseteq K[T]$  is an ideal (the set of polynomials which vanish at  $x$ ). As  $\text{Im}(\text{ev}_x)$  is a subring of  $L$ , it is an integral domain. So  $I$  is a prime 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  $K$ . 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  $\frac{T^p - 1}{T - 1} = g(T) = T^{p-1} + \dots + T + 1 \in \mathbb{Q}[T]$ . As

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

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

*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  $K[x] \rightarrow K[x]$ ,  $z \mapsto yz$ . 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  $x^{-1} = a_0 + a_1x + \dots + a_nx^n \in K[x]$ . Then  $a_nx^{n-1} + \dots + a_0x - 1 = 0$ , so  $x$  is algebraic over  $K$ .

Show (i)  $\Rightarrow$  (iii) and degree formula: The image of  $\text{ev}_x : K[T] \rightarrow L$  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  $1, T, \dots, T^{d-1}$ . So  $\dim_K K[x] = d < \infty$ . Furthermore  $\deg_K(x) = [K(x) : K] = d$ .  $\square$

**Corollary 4.2.**

- (i)  $x_1, \dots, x_n$  are algebraic over  $K$  if and only if  $L = K(x_1, \dots, x_n)$  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  $K(x_1, \dots, x_{n-1})$ , so  $[L : K(x_1, \dots, x_{n-1})] < \infty$ . So by induction on  $n$  and the Tower Law,  $[L : K] < \infty$ . Conversely, 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).

$\square$

**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

$$z^{\frac{p-1}{2}} + z^{\frac{p-3}{2}} + \dots + z^{-\frac{p-1}{2}} = 0$$

$z + z^{-1} = x$ . 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  $m = a^2 + b^2n + 2ab\sqrt{n}$ .  $b = 0$  implies  $m = a^2$  and  $a = 0$  implies  $mn = b^2n^2$ , 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.

□

**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  $f = T^n + a_{n-1}T^{n-1} + \dots + a_0 \in L[T]$  with  $f \neq 0$  and  $f(x) = 0$ . Let  $L_0 = K(a_0, \dots, a_{n-1})$ , 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  $K$ .  $\square$

**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 not 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”).

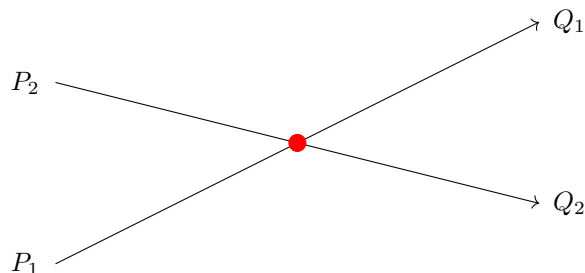
Hermite, Lindermann showed that  $e$  and  $\pi$  are transcendental.

In the 20th Century: Gelfond-Schneider Theorem: 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*

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

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  $\mathbb{Q} = F_0 \subseteq F_1 \subseteq \dots \subseteq F_n \subseteq \mathbb{R}$  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

$$\mathbb{Q} = F_0 \subseteq \dots \subseteq F_n$$

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  $k$ th 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  $\mathbb{Q}$ .  $\square$



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

**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  $\pi$  is transcendental, it (and therefore  $\sqrt{\pi}$ ) is not constructible.
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 constructible.
3. “Trisect the angle” - say we are trying to trisect  $2\pi/3$ , which is certainly constructible. 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 constructible. 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 constructible.

Later in the course we will see the following theorem

**Theorem (Gauss).** *A regular  $n$ -gon is constructible 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

$$f = \prod_{i=1}^n (T - x_i), \quad x_i \in \mathbb{C}$$

(Later we will give another proof of the FTA.) So the “best”  $L$  would be  $\mathbb{Q}(x_1, \dots, x_n)$ , 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.  $\square$

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  $\sigma : L \rightarrow M$  such that  $\sigma|_K = \text{id}_K$ . We also sometimes call this a  $K$ -embedding, since  $\sigma$  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  $\sigma : L_f \rightarrow L$  sending  $T + (f)$  to  $x$ .*
- (ii) *Every  $K$ -homomorphism  $L_f \rightarrow L$  arises as in (i). So there is a bijection between*

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

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

*Proof.* Note

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

where  $\text{ev}_x : K[T] \rightarrow L$  is the homomorphism  $g \mapsto g(x)$ .  $\square$

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

*Proof.* Take  $L = K(x)$  in the above Theorem.  $\square$

**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  $\sigma : K(x) \rightarrow K(y)$  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  $\sigma : K \rightarrow K'$  be a homomorphism of fields. If  $\tau : L \rightarrow L'$  is a homomorphism such that  $\tau(x) = \sigma(x)$  whenever  $x \in K$ , we say  $\tau$  is a  $\sigma$ -homomorphism from  $L$  to  $L'$ . We also say  $\tau$  extends  $\sigma$  or that  $\sigma$  is the restriction of  $\tau$  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  $\sigma : K \rightarrow L$  be any homomorphism of fields. Let  $\sigma f$  be the polynomial given by applying  $\sigma$  to the coefficients of  $f$ . Then

- (i) If  $x \in L$  is a root of  $\sigma f$ , there exists a unique  $\sigma$ -homomorphism  $\tau : L_f \rightarrow L$  such that  $\tau(t) = \tau(T + (f)) = x$
- (ii) Every  $\sigma$ -homomorphism  $L_f \rightarrow L$  is of the form arising from (i), so we have a bijection

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

**Example.**  $\sigma$  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  $\sigma : K \rightarrow L$  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  $\sigma$  to be the inclusion  $\tau$  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)  $L = K(x_1, \dots, x_n)$  where  $\{x_1, \dots, x_n\}$  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  $\{x_1, \dots, x_n\}$  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  $x_2, \dots, x_n \in L$  be the roots of  $f_1$  in  $L$ . Then  $f$  splits into linear factors in  $L$ , with roots  $x_2, \dots, x_n$ , and  $L = K'(x_2, \dots, x_n) = K(x_1, \dots, x_n)$ . So  $L$  is a splitting field for  $f$  over  $K$ .  $\square$

**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  $\sigma : K \rightarrow M$  be an extension such that  $\sigma f \in M[T]$  splits [into linear factors] in  $M[T]$ . Then*

- (i)  $\sigma$  can be extended to a homomorphism  $\tau : L \rightarrow M$ .
- (ii) If  $M$  is a splitting field for  $\sigma f$  over  $\sigma(K)$ , then any  $\tau$  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  $\tau$ .

*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  $\sigma f$  splits in  $M$  this exists). Theorem 6.4 implies there exists  $\sigma_1 : K(x) \rightarrow M$  such that  $\sigma_1(x) = y$  and  $\sigma_1$  extends  $\sigma$ .

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  $\sigma_1$  to a homomorphism  $\tau : L \rightarrow M$ .

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

□

**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  $f = \prod_{1 \leq a \leq 4} (T - z^a)$ . 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  $L = K(x_1, \dots, x_n)$ . 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  $L$ . 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  $y \in L$ .  $\square$

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  $L = K(x_1, \dots, x_k)$ . 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.  $\square$

## 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  $(f^n)' = n f' f^{n-1}$ .

**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  $f$ .  $\square$

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

**Corollary 8.2.**  *$f$  is separable 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 separable if and only if  $f, f'$  have no common root, which holds if and only if  $\gcd(f, f') = 1$ .  $\square$

**Example.**  $\text{char}(K) = p > 0$ ,  $f = T^p - b$ ,  $b \in K$ . Then  $f' = 0$  so  $\gcd(f, f') = f \neq 1$ . So  $f$  is inseparable. 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  $p$ th power in  $K$ , then  $f$  is irreducible (Exercise).

**Theorem 8.3.**

- (i) Let  $f \in K[T]$  be irreducible. Then  $f$  is separable if and only if  $f' \neq 0$ .
- (ii) If  $\text{char}(K) = 0$  then every irreducible polynomial in  $K[T]$  is separable.
- (iii) If  $\text{char}(K) = p > 0$  then an irreducible  $f \in K[T]$  is inseparable 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 *separable over  $K$*  if  $x$  is algebraic over  $K$  and  $m_{x,K}$  is separable. Say  $L/K$  is *separable over  $K$*  if  $x$  is separable 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 separable over  $K$  if and only if there are exactly  $\deg_K(x)$   $K$ -homomorphisms from  $K(x) \rightarrow L$ .

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

**Theorem 8.5** (“Counting embeddings”). *Let  $L = K(x_1, \dots, x_k)$  be a finite extension of  $K$ , and  $M/K$  any extension. Then  $|\text{Hom}_K(L, M)| \leq [L : K]$  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 separable 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  $\sigma : K \rightarrow M$  and the condition becomes that the number of  $\sigma$ -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  $|\text{Hom}_K(K_1, M)| = e = |\{\text{roots of } m_{x_1, K} \text{ in } M\}| \leq d$ . Let  $\sigma : K_1 \rightarrow M$  be a  $K$ -homomorphism. Apply induction to  $L/K_1$ . So there exist at most  $[L : K_1]$  extensions of  $\sigma$  to a homomorphism  $L \rightarrow M$ . So  $|\text{Hom}_K(L, M)| \leq e[L : K_1] \leq d[L : K_1] = [L : K]$ .

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  $|\text{Hom}_K(K_1, M)| = d$  and (i), (ii) still hold over  $K_1$ . So by induction on  $k$ , each  $\sigma : K_1 \rightarrow M$  has  $[L : K_1]$  extensions to  $L \rightarrow M$ , so  $|\text{Hom}_K(L, M)| = [L : K]$ .  $\square$

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

*Proof.* If  $L/K$  is separable, all the  $x_i$  are separable by definition. So assume all the  $x_i$  are separable 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  $|\text{Hom}_K(L, M)| = [L : K]$ . But if  $x \in L$ , then  $L = (x, x_1, \dots, x_k)$  as well. So by the previous theorem again,  $x$  is separable.  $\square$

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

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

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

*Proof.* It is enough to consider the case  $k = 2$ ,  $L = K(x, y)$  with  $x, y$  separable over  $K$ . Let  $n = [L : K]$  and let  $M$  be a normal closure for  $L/K$ . Then there exist  $n$  distinct  $K$ -homomorphisms  $\sigma_i : L \rightarrow M$ . 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  $\sigma_i(y) = \sigma_j(y)$  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  $L = K(z)$ .  $\square$

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  $L = K(x)$ .  $\square$

## 9 Galois Theory

Automorphisms of fields:  $\sigma : L \rightarrow L$  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  $\text{Aut}(L)$  (the “automorphism group of  $L$ ”).

If  $S \subseteq \text{Aut}(L)$ , is a subset, let  $L^S = \{x \in L : \forall \sigma \in S, \sigma(x) = x\}$ . This is a subfield of  $L$  (since each  $\sigma$  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  $\text{Aut}(L/K) = \{K\text{-automorphisms of } L\} = \{\sigma \in \text{Aut}(L) : \sigma(x) = x \forall x \in K\}$  (a subgroup of  $\text{Aut}(L)$ ). Then  $\sigma \in \text{Aut}(L/K)$  if and only if  $K \subseteq L^{\{\sigma\}}$ .

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

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

**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  $\varphi_p : K \rightarrow K$ ,  $x \mapsto x^p$  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,  $G = \text{Aut}(L/K)$ . The following are equivalent*

- (i)  $L/K$  is Galois (i.e  $L^G = K$ )
- (ii)  $L/K$  is normal and separable
- (iii)  $L$  is the splitting field of a separable polynomial
- (iv)  $|\text{Aut}(L/K)| = [L : K]$ .

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

*Proof.* First we show (i) $\Rightarrow$ (ii) and the last part. Let  $x \in L$ ,  $\{x_1, \dots, x_r\}$  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 separable over  $K$ , and  $m_{x,K}$  splits in  $L$ , so  $L/K$  is normal and separable.

Now we show (ii) $\Rightarrow$ (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 separable,  $q_i$  are separable, so  $g = \prod q_i$  is separable and  $L$  is also a splitting field for  $g$ .

Now we show (iii) $\Rightarrow$ (iv). Write  $L = K(x_1, \dots, x_k)$ , the splitting field of some separable  $f$  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.  $\square$

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

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

**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  $F \mapsto \text{Gal}(L/F)$  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).*

(b) *Let  $\sigma \in G$ ,  $H \subseteq G$  a subgroup,  $F = L^H$ . Then  $\sigma H \sigma^{-1}$  corresponds to  $\sigma F$ .*

(c) *The following are equivalent (for a subgroup  $H \subseteq G$ )*

- (i)  $L^H/K$  is Galois
- (ii)  $L^H/K$  is normal
- (iii) For all  $\sigma \in G$ ,  $\sigma(L^H) = L^H$
- (iv)  $H$  is a normal subgroup of  $G$

*If so,  $\text{Gal}(L^H/K) \cong G/H$ .*

*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 separable, 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

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

- (b) Under (a),  $\sigma H \sigma^{-1}$  corresponds to  $L^{\sigma H \sigma^{-1}} = \{x \in L : \sigma \tau \sigma^{-1} = x, \forall \tau \in H\}$  and  $\sigma \tau \sigma^{-1} = x$  if and only if  $\tau \sigma^{-1}(x) = \sigma^{-1}(x)$ , i.e.  $\tau(y) = y$  where  $x = \sigma(y)$ . So  $x \in L^{\sigma H \sigma^{-1}}$  if and only if  $x = \sigma(y)$  for  $y \in L^H$ , i.e.  $L^{\sigma H \sigma^{-1}} = \sigma F$ .
- (c)  $L/K$  is separable, so  $L^H/K$  is separable, so (i) is equivalent to (ii). Let  $F = L^H$ . Let  $F = L^H$ ,  $x \in F$ . Then  $\{\text{roots of } m_{x,K}\}$  is the orbit of  $x$  under  $G$ . So  $m_{x,K}$  splits in  $F$  if and only if  $\forall \sigma \in G, \sigma(x) \in F$ . As this must hold for all  $x \in F$ ,  $F$  is normal if and only if  $\sigma F \subseteq F$ . As  $[\sigma F : K] = [F : K]$  ( $K$ -isomorphic extensions), this means  $\sigma F = F$ . By (b), this is equivalent to:  $\forall \sigma \in G, \sigma H \sigma^{-1} = H$ , i.e.  $H$  is a normal subgroup of  $G$ .

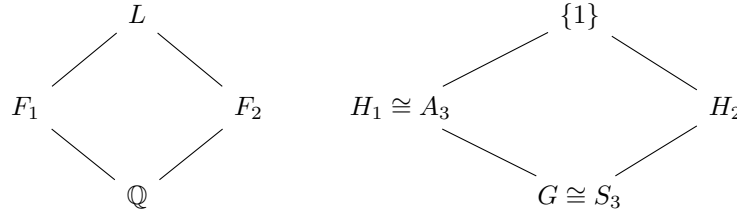
Last part: since  $\forall \sigma \in G, \sigma F = F$ , we have a homomorphism  $G \rightarrow \text{Gal}(F/K)$  given by restricting  $\sigma \in G$  to  $F$ . This homomorphism has kernel  $H$  (since  $F = L^H$ ). So  $G/H \rightarrow \text{Gal}(F/K)$  is an isomorphism.

□

**Example.**  $K = \mathbb{Q}$ ,  $L = \mathbb{Q}(\sqrt[3]{2}, \omega) \subseteq \mathbb{C}$  where  $\omega = \exp(2\pi i/3)$ . Then  $L$  is a splitting field for  $T^3 - 2$  and  $[L : \mathbb{Q}] = 6$ . So  $L/K$  is the splitting field of a separable polynomial, hence is Galois, and if  $G = \text{Gal}(L/K)$  then  $|G| = 6$ . Obvious subfields of  $L$ :  $F_1 = \mathbb{Q}(\omega)$ ,  $F_2 = \mathbb{Q}(\sqrt[3]{2})$ . Then  $[F_1 : \mathbb{Q}] = 2$  and  $[F_2 : \mathbb{Q}] = 3$ .

$G$  must be isomorphic to either cyclic groups of order 6, or  $S_3$ .  $F_2/\mathbb{Q}$  isn't normal, as  $\omega\sqrt[3]{2} \notin F_2$ . So  $H_2 = \text{Gal}(L/F_2)$  isn't a normal subgroup of  $G$ . So  $G$  is non-abelian and  $G \cong S_3$ , and  $H_2 \cong \{(12), e\}$ ,  $H_1$  must be  $\cong A_3$ . The other subgroups are  $\{(13), e\}$  and  $\{(23), e\}$  which are the conjugates of  $H_2$ . So the corresponding subfields are  $\{\sigma F_2 : \sigma \in G\}$ , which are  $\mathbb{Q}(\omega\sqrt[3]{2})$ ,  $\mathbb{Q}(\omega^2\sqrt[3]{2})$  (conjugates of  $\sigma(\sqrt[3]{2})$  are the roots of the minimal polynomial). So this describes all  $F$  with  $\mathbb{Q} \subseteq F \subseteq L$ .

In fact, we could have seen at once that  $G \cong S_3$ :  $f \in K[T]$  separable polynomial,  $x_1, \dots, x_n$  roots in splitting field  $L$ .  $G = \text{Gal}(L/K)$  permutes  $\{x_i\}$  as  $f(\sigma x_i) = \sigma f(x_i) = 0$  and if  $\sigma(x_1) = x_i$  for all  $i$ , then since  $L = K(x_1, \dots, x_n)$ ,  $\sigma = \text{id}$ . This gives a homomorphism  $G \rightarrow S_n$  which is injective (where  $n = \deg f$ ).



**Definition.** The subgroup  $\text{Gal}(f/K) \subseteq S_n$  given by the image of  $G$  is the Galois group of  $f$  over  $K$ . Note that  $[L : K] = |\text{Gal}(L/K)| = |\text{Gal}(f/K)|$  so divides  $n!$ .

There exist several methods for determining  $\text{Gal}(f/K)$ .

**Proposition 9.5.** A polynomial  $f$  is irreducible if and only if  $\text{Gal}(f/K)$  is transitive (recall that a subgroup  $G \subseteq S_n$  is transitive if  $\forall i, j \in \{1, \dots, n\}$ , there exists  $\sigma \in G$  with  $\sigma(i) = j$ , i.e. there is only one orbit).

*Proof.* Let  $x$  be a root of  $f$  in a splitting field  $L$ . Then its orbit under  $G = \text{Gal}(f/K)$  is the set of roots of  $m_{x,K}$  (by 9.2). As  $m_{x,K} \mid f$ , have  $m_{x,K} = f$  if and only if  $f$  is irreducible. And  $m_{x,K} = f$  if and only if every root of  $f$  is in the orbit of  $x$ , i.e. iff  $G$  acts transitively on the roots of  $f$ .  $\square$

**Remark:** if  $G \subseteq S_n$  is transitive, then by the orbit-stabiliser theorem,  $n \mid |G|$ .

Recall (from section 2) the discriminant: if  $f \in K[T]$  is monic,  $f = \prod_{1 \leq i \leq n} (T - x_i)$  in  $L$  (splitting field) then  $\text{Disc}(f) = \Delta^2 \in K$  where  $\Delta = \prod_{1 \leq i < j \leq n} (x_i - x_j)$ .  $\text{Disc}(f) \neq 0$  if and only if  $f$  is separable.

**Proposition 9.6.** Assume  $\text{char}(K) \neq 2$ . The fixed field of  $G \cap A_n$  is  $K(\Delta)$ . In particular,  $\text{Gal}(f/K) \subseteq A_n$  if and only if  $\text{Disc}(f)$  is a square in  $K$ .

*Proof.* If  $\pi \in S_n$ , the sign of  $\pi$  is an element of  $\{\pm 1\}$ , and

$$\prod_{1 \leq i \leq j \leq n} (T_{\pi(i)} - T_{\pi(j)}) = \text{sgn}(\pi) \prod_{1 \leq i \leq j \leq n} (T_i - T_j)$$

So if  $\sigma \in G$ , then  $\sigma(\Delta) = \text{sgn}(\sigma)\Delta$ . Since  $\text{char}(K) \neq 2$ ,  $-1 \neq 1$  so as  $\Delta \neq 0$ , this implies  $\Delta \in K$  if and only if  $G \subseteq A_n$  and  $\Delta$  lies in the fixed field  $F$  of  $G \cap A_n$ . As

$$[F : K] = (G : G \cap A_n) = \begin{cases} 1 & \text{if } G \subseteq A_n \\ 2 & \text{otherwise} \end{cases}$$

we have  $F = K(\Delta)$ .  $\square$

**Example.** Let  $f = T^3 + aT + b$ , say  $f = \prod_{i=1}^3 (T - x_i)$ ,  $x_3 = -x_1 - x_2$  and

$$\begin{aligned} a &= x_1x_2 - (x_1 + x_2)^2 \\ b &= x_1x_2(x_1 + x_2) \end{aligned}$$

So (plugging in)  $\text{Disc}(f) = -4a^3 - 27b^2$ . So  $\text{Gal}(f/K) \subseteq A_3$  if and only if  $-4a^3 - 27b^2$  is a square in  $K$ . Suppose  $a = -21$ ,  $b = -7$ . Then  $f \in \mathbb{Q}[T]$  is irreducible. We have  $\text{Disc}(f) = 4 \cdot 21^3 - 27 \cdot 7^2 = (27 \cdot 7)^2$ . So  $\text{Gal}(f/\mathbb{Q}) \subseteq A_3$ . As  $f$  is irreducible, the Galois group is transitive, so  $\text{Gal}(f/\mathbb{Q}) = A_3$ . Thus this method computes the Galois group of any cubic polynomial (when  $\text{char}(K) \neq 2, 3$ ).

## 10 Finite fields

Let  $p$  be prime, and write  $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ . We aim to describe all finite fields of characteristic  $p$  (i.e all finite extensions  $F$  of  $\mathbb{F}_p$ ), and their Galois theory. Recall:

- $|F| = p^n$ , where  $n = [F : \mathbb{F}_p]$ .
- $F^\times$  is cyclic of order  $p^n - 1$ .
- $\varphi_p : F \rightarrow F$ ,  $x \mapsto x^p$  is an automorphism of  $F$ .

**Theorem 10.1.** *Let  $n \geq 1$ . Then there exists a field with  $q = p^n$  elements. Any such field is a splitting field of the polynomial  $T^q - T$  over  $\mathbb{F}_p$ . In particular, any two finite fields of the same order are isomorphic.*

*Proof.* Let  $F$  be a field with  $q = p^n$  elements. Then if  $x \in F^\times$ ,  $x^{q-1} = 1$ . So for all  $x \in F$ ,  $x^q = x$ . So  $f = T^q - T = \prod_{x \in F} (T - x)$  splits into linear factors in  $F$ , and not in any proper subfield of  $F$ . So  $F$  is a splitting field for  $f$  over  $\mathbb{F}_p$ . So by uniqueness of splitting fields,  $F$  is unique up to isomorphism.

To show the existence of such an  $F$ , given  $n$ , let  $L/\mathbb{F}_p$  be a splitting field of  $f = T^q - T$  where  $q = p^n$ . Let  $F \subseteq L$  be the fixed field of  $\varphi_p^n : x \mapsto x^q$ . So  $F$  is the set of roots of  $f$  in  $L$ . So  $|F| = q$  (and  $F = L$ ).  $\square$



**Notation:** write  $\mathbb{F}_q$  for any finite field with  $q$  elements (by the above theorem, any two such fields are isomorphic, although there is no canonical isomorphism).

**Theorem 10.2.**  $\mathbb{F}_{p^n}/\mathbb{F}_p$  is Galois with Galois group cyclic of order  $n$ , generated by  $\varphi_p$ .

*Proof.*  $T^{p^n} - T = \prod_{x \in \mathbb{F}_{p^n}} (T - x)$  is separable, so  $\mathbb{F}_{p^n}$  is Galois over  $\mathbb{F}_p$  (as the splitting field of a separable polynomial). Let  $G \subseteq \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$  be the subgroup generated by  $\varphi_p$ . Then  $\mathbb{F}_{p^n}^G = \{x : x^p = x\} = \mathbb{F}_p$ . So by the Galois correspondence  $G = \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ .  $\square$

**Theorem 10.3.**  $\mathbb{F}_{p^n}$  has a unique subfield of order  $p^m$  for each  $m \mid n$ , and no others. If  $m \mid n$  then  $\mathbb{F}_{p^m} \subseteq \mathbb{F}_{p^n}$  is the fixed field of  $\varphi_p^m$ .

*Proof.*  $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) \cong \mathbb{Z}/n\mathbb{Z}$ . The subgroups of  $\mathbb{Z}/n\mathbb{Z}$  are the  $m\mathbb{Z}/n\mathbb{Z}$  for  $m \mid n$ ,  $m \geq 1$ . So by Galois correspondence, the subfields of  $\mathbb{F}_{p^n}$  are the fixed fields of these subgroups, i.e. of the subgroups  $\langle \varphi_p^n \rangle$ , which have degree equal to the indices  $(\mathbb{Z}/n\mathbb{Z} : m\mathbb{Z}/n\mathbb{Z}) = m$ .  $\square$

**Remark:** if  $m \mid n$ , then  $\text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) = \langle \varphi_p^m \rangle$ .

**Theorem 10.4.** Let  $f \in \mathbb{F}_p[T]$  be separable of degree  $n \geq 1$ , whose irreducible factors have degrees  $n_1, \dots, n_r$ ,  $\sum n_i = n$ . Then  $\text{Gal}(f/\mathbb{F}_p) \subseteq S_n$  is cyclic, generated by an element of cycle type  $(n_1, \dots, n_r)$ . In particular,  $|\text{Gal}(f/\mathbb{F}_p)|$  is equal to the lowest common multiple of  $\{n_i\}$ .

*Proof.* Let  $L$  be a splitting field for  $f$  over  $\mathbb{F}_p$ , with roots  $x_1, \dots, x_n \in L$ . Then  $\text{Gal}(L/\mathbb{F}_p)$  is cyclic, generated by  $\varphi_p$ . As the irreducible factors of  $f$  are the minimal polynomials of the  $x_i$ 's, and the set of roots of the minimal polynomial of  $x_i$  is the orbit of  $\varphi_p$  on  $x_i$ , the cycle type of  $\varphi_p$  is  $(n_1, \dots, n_r)$ . The order of any such permutation is then  $\text{lcm}(n_1, \dots, n_r)$ .  $\square$

**Theorem 10.5** (“Reduction mod  $p$ ”). Let  $f \in \mathbb{Z}[T]$  be a monic, separable polynomial,  $p$  prime,  $n = \deg(f) \geq 1$ . Suppose the reduction  $\bar{f} \in \mathbb{F}_p[T]$  is also separable. Then  $\text{Gal}(\bar{f}/\mathbb{F}_p) \subseteq \text{Gal}(f/\mathbb{Q})$ , as subgroups of  $S_n$ .

**Corollary 10.6.** With the same assumptions as in the above theorem, suppose that  $\bar{f} = g_1 \dots g_r$  where  $g_i \in \mathbb{F}_p[T]$  are irreducible of degree  $n_i$ . Then  $\text{Gal}(f/\mathbb{Q})$  contains an element of cycle type  $(n_1, \dots, n_r)$ .

*Proof.* Combine the previous two theorems. □

**Example.**  $f = T^4 - 3T + 1$

- $p = 2$ :  $f = T^4 + T + 1 \pmod{2}$  is irreducible (no roots and not divisible by  $T^2 + T^1$  the only reducible quadratic)
- $p = 5$ :  $f = (T + 1)(T^3 - T^2 + T + 1) \pmod{5}$  where the latter factor is irreducible

So by the Corollary,  $\text{Gal}(f/\mathbb{Q})$  contains a 4-cycle and a 3-cycle. So  $12 \mid |G|$ , so  $G$  is either  $S_4$  or  $A_4$ . As 4-cycles are odd,  $G$  must be  $S_4$ .

**Remark:** if  $\bar{f}$  is separable, then  $\text{Disc}(\bar{f}) \neq 0$ , so  $p \nmid \text{Disc}(f)$  and  $f$  is separable. If  $f$  is separable, then  $\bar{f}$  is separable for all but the finite set of primes  $p$  which divide  $\text{Disc}(f)$ .

**Remark:** the identification of  $\text{Gal}(f/\mathbb{Q})$  with a subgroup of  $S_n$  depends on fixing an ordering of the roots. Taking a different ordering corresponds to conjugation of the Galois group  $\text{Gal}(f/\mathbb{Q})$  in  $S_n$ . So  $\text{Gal}(\bar{f}/\mathbb{F}_p) \subseteq \text{Gal}(f/\mathbb{Q})$  really means that  $\text{Gal}(\bar{f}/\mathbb{F}_p)$  is conjugate to a subgroup of  $\text{Gal}(f/\mathbb{Q})$ .

The following proof is **\*non-examinable\***:

*Proof of Theorem 10.5.* Let  $L = \mathbb{Q}(x_1, \dots, x_n)$  be a splitting field of  $f = \prod (T - x_i)$ , with degree  $N = [L : \mathbb{Q}]$ . Consider  $R = \mathbb{Z}[x_1, \dots, x_n]$ . As  $f(x_i) = 0$ ,  $f$  monic, so every element of  $R$  is a  $\mathbb{Z}$ -linear combination of  $x_1^{a_1} \dots x_n^{a_n}$ ,  $0 \leq a_i < n$ . So  $R$  is finitely generated as an abelian group. As  $R \subseteq L \cong \mathbb{Q}^N$ , we must have  $R \cong \mathbb{Z}^M$  for  $M \leq N$ . Then  $\bar{R} = R/pR$  has  $p^M$  elements. Let  $\bar{P}$  be a maximal ideal of  $\bar{R}$ , corresponding to an ideal  $P$  of  $R$  containing  $pR$ . Then  $F = R/P \cong \bar{R}/\bar{P}$  is a finite field with  $p^d$  elements say.

$F = \mathbb{F}_p(\bar{x}_1, \dots, \bar{x}_n)$  where  $\bar{x}_i = x_i + P \in F$  and  $\bar{f} = \prod (T - \bar{x}_i)$ . As  $\bar{f}$  is separable, the  $\bar{x}_i$  are distinct and  $F$  is a splitting field for  $\bar{f}$ .  $G = \text{Gal}(f/\mathbb{Q})$  takes  $R$  to itself (permutes  $x_i$ 's). Let  $H \subseteq G$  be the stabiliser of  $P$ , i.e.  $\{\sigma \in G : \sigma P = P\}$ . Then  $H$  acts on  $R/P = F$ , permuting the  $\bar{x}_i$ 's in the same way as it permutes the  $x_i$ 's. So we have an injective homomorphism  $H \rightarrow \text{Gal}(F/\mathbb{F}_p)$ .

Now we just need to show this is an isomorphism. Let  $\{P_1 = P, P_2, \dots, P_r\}$  be the orbit of  $P$  under  $G$ . The  $P_i$  are all maximal ideals,  $R/P_i \cong R/P$  has  $p^d$  elements. As  $P_i$  are maximal,  $P_i + P_j = R$  if  $i \neq j$ . So by the Chinese Remainder

Theorem,  $R/(P_1 \cap \dots \cap P_r) \cong R/P_1 \times \dots \times R/P_r$ . As  $p \in P_i$ ,  $pR \subseteq P_1 \cap \dots \cap P_r$ , so

$$p^N \geq p^M = |R/pR| \geq |R/(P_1 \cap \dots \cap P_r)| = \prod_{i=1}^r |R/P_i| = p^{rd}$$

Orbit-Stabiliser Theorem implies  $r = (G : H) = |G|/|H| = N/|H|$  and as  $H \rightarrow \text{Gal}(F/\mathbb{F}_p)$  is an injection,  $H \leq d$  with equality if and only if the injection is an isomorphism. So  $N = rd$ , so combined with previous inequality,  $N = rd$  so  $H \cong \text{Gal}(\bar{f}/\mathbb{F}_p)$ .  $\square$

**Remark:** if  $\text{Gal}(f/\mathbb{Q})$  contains an element of cycle type  $(n_1, \dots, n_r)$  then it is a (hard) fact that there exist infinitely primes  $p$  such that  $\bar{f}$  factors into irreducibles with degrees  $n_1, \dots, n_r$  ("Cebotarev density theorem" - generalisation of Dirichlet's theorem on primes in arithmetic progression).

## 11 Cyclotomic extensions

We will look at polynomials of the form  $T^n - 1$  (later  $T^n - a$ ).

**Lemma 11.1.** *Let  $C$  be a cyclic group of order  $n > 1$  (written multiplicatively). If  $a \in \mathbb{Z}$ ,  $(a, n) = 1$ , then the map  $[a] : C \rightarrow C$ ,  $[a](g) = g^a$  is an automorphism of  $C$ , and  $(\mathbb{Z}/n\mathbb{Z})^\times \rightarrow \text{Aut}(C)$ ,  $a \mapsto [a]$  is an isomorphism.*

*Proof.* Clearly  $[a]$  is a homomorphism, and since  $(a, n) = 1$ , it is an automorphism as there exists  $b$  with  $ab \equiv 1 \pmod{n}$ . So have injective map  $(\mathbb{Z}/n\mathbb{Z})^\times \rightarrow \text{Aut}(C)$  with  $a \mapsto [a]$  which is obviously a homomorphism. If  $\varphi \in \text{Aut}(C)$  and  $g$  is a generator of  $C$ , then  $\varphi(g) = g^a$  for some  $a \in (\mathbb{Z}/n\mathbb{Z})^\times$ , so  $\varphi = [a]$ . So we have an isomorphism.  $\square$

Let  $K$  be a field,  $n \geq 1$ . Define  $\mu_n(K) = \{x \in K : x^n = 1\}$ , the group of  $n$ th roots of unity in  $K$ . The group  $\mu_n(K)$  is finite, hence cyclic (Proposition 3.5), hence of order dividing  $n$ . Say  $\zeta \in \mu_n(K)$  is a primitive  $n$ th root of 1 if  $\zeta$  has order  $n$  in  $K^\times$ .

Such a  $\zeta$  exists if and only if  $\mu_n(K)$  has  $n$  elements, in which case  $\zeta$  is a generator. In particular,  $f = T^n - 1$  has  $n$  distinct roots, so is separable.

In general,  $f = T^n - 1$  is separable if and only if  $(f, f') = 1$ , and since  $f' = nT^{n-1}$ , this holds iff  $n1_K \neq 0$ .

Until the end of this section we assume  $\text{char}(K) > 0$  or  $\text{char}(K) = p > 0$  and  $p \nmid n$ , i.e  $T^n - 1$  is separable.

Let  $L/K$  be a splitting field for  $f = T^n - 1$ , and  $G = \text{Gal}(L/K)$  (since  $f$  is separable, this is Galois). Then  $|\mu_n(L)| = n$  and there exists a primitive  $n$ th root of 1,  $\zeta = \zeta_n \in L$ .  $L/K$  is called a *cyclotomic extension*.

**Proposition 11.2.**

- (i)  $L = K(\zeta)$
- (ii) There exists an injective homomorphism  $\chi = \chi_n : G \rightarrow (\mathbb{Z}/n\mathbb{Z})^\times$  such that if  $\chi(\sigma) = a \pmod{n}$ , then  $\sigma(\zeta) = \zeta^a$ . In particular,  $G$  is abelian.
- (iii)  $\chi$  is an isomorphism if and only if  $G$  acts transitively on the set of primitive roots of unity in  $L$  ( $\chi$  is called the cyclotomic character).

*Proof.*

- (i)  $\mu_n(L) = \langle \zeta \rangle$  so the roots of  $T^n - 1$  are the powers of  $\zeta$ , so  $L = K(\zeta)$ .
- (ii) Consider the action of  $G$  on  $L$ . It permutes  $\mu_n(L)$  and if  $\zeta, \zeta' \in \mu_n(L)$ ,  $\sigma \in G$ , then  $\sigma(\zeta\zeta') = \sigma(\zeta)\sigma(\zeta')$ . So  $\sigma$  acts as an automorphism of  $\mu_n(L)$ , and  $\sigma(\zeta_n) = \zeta_n$  if and only if  $\sigma = \text{id}$  (as  $L = K(\zeta_n)$ ). So we have an injective homomorphism  $G \rightarrow \text{Aut}(\mu_n(L))$  and  $\text{Aut}(\mu_n(L)) \cong (\mathbb{Z}/n\mathbb{Z})^\times$  by lemma 11.1.
- (iii)  $\zeta_n^a$  is primitive if and only if  $(a, n) = 1$ . So the set of primitive  $n$ th roots of 1 is  $\{\zeta_n^a : a \in (\mathbb{Z}/n\mathbb{Z})^\times\}$ , which by (ii) is the orbit of  $\zeta$  under  $G$ . So  $\chi$  is surjective iff there is one orbit.

□

**Example:**  $K = \mathbb{Q}$ , can take  $L = \mathbb{Q}(e^{2\pi i/n})$ . What is the minimal polynomial of  $e^{2\pi i/n}$ ?

**Definition.** ( $K$  satisfying earlier hypothesis) The  $n$ th cyclotomic polynomial is

$$\Phi_n(T) = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^\times} (T - \zeta_n^a)$$

which has roots precisely the set of primitive  $n$ th roots of 1 in the splitting field  $L$  of  $T^n - 1$ . As  $G$  permutes the primitive  $n$ th roots of 1 in  $L$ ,  $\Phi_n \in L^G[T] = K[T]$ . Also  $\chi$  is surjective if and only if  $\Phi_n \in K[T]$  is irreducible.

$\Phi_n$  doesn't really depend on  $K$ . In fact,  $x \in L$  satisfies  $x^n = 1$  if and only if  $x$  is a primitive  $d$ th root of unity for some (unique)  $d \mid n$ . So  $T^n - 1 = \prod_{d \mid n} \Phi_d$ .

So  $\Phi_n = (T^n - 1) / \prod_{\substack{d \mid n \\ d \neq n}} \Phi_d$ , giving an inductive definition of  $\Phi_n$ , and showing that  $\Phi_n$  is the image of in  $K[T]$  of a polynomial in  $\mathbb{Z}[T]$  which doesn't depend on  $K$ . e.g.  $\Phi_p = (T^p - 1)/(T - 1) = T^{p-1} + \dots + T + 1$ .  $\Phi_1 = T - 1$  and  $\Phi_{p^n} = (T^{p^n} - 1)/(T^{p^{n-1}} - 1) = \Phi_p(T^{p^{n-1}})$ .

Have  $\deg(\Phi_n) = |(\mathbb{Z}/n\mathbb{Z})^\times| = \varphi(n)$ , where  $\varphi$  is the Euler  $\varphi$ -function.

We have 2 special cases

**Theorem 11.3** ("Irreducibility of cyclotomic polynomials"). *Let  $K = \mathbb{Q}$ . Then  $\chi_n$  is an isomorphism for  $n > 1$ . In particular,  $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n)$ , and  $\Phi_n$  is irreducible over  $\mathbb{Q}$ .*

*Proof.* By 11.2, all of these statements are equivalent. So it suffices to show  $\Phi_n$  is irreducible over  $\mathbb{Q}$ . If  $n$  is prime (or a prime power) can prove this using Eisenstein, but this doesn't work for general  $n$ .

$\chi_n$  is an isomorphism if for all primes  $p$  with  $(p, n) = 1$ , the class of  $p \in (\mathbb{Z}/n\mathbb{Z})^\times$  lies in the image of  $\chi$  (factor  $a$  with  $(a, n) = 1$  as a product of primes).

Let  $f$  be the minimal polynomial of  $\zeta$  over  $\mathbb{Q}$ . Let  $g$  be the minimal polynomial of  $\zeta^p$  over  $\mathbb{Q}$ . If  $f = g$  then  $\zeta^p$  lies in the orbit of  $G$  on  $\zeta$ , i.e.  $p$  lies in the image of  $\chi$ , so we're done.

If  $f \neq g$ , then  $(f, g) = 1$  and  $f, g \mid T^n - 1$ , so  $fg \mid T^n - 1$ . As  $\zeta$  is a root of  $g(T^p)$ ,  $f \mid g(T^p)$ . Reduce modulo  $p$  to get  $\bar{f} \in \mathbb{F}_p[T]$  and  $\bar{f} \mid \overline{g(T^p)} = [\bar{g}(T)]^p$  (as we're in characteristic  $p$ ) and as both  $\bar{f}$  and  $\bar{g}$  divide  $T^n - 1 \in \mathbb{F}_p[T]$ , which is separable (as  $p \nmid n$ ), which implies  $\bar{f} \mid \bar{g}$ , hence  $\bar{f}^2 \mid \bar{f}\bar{g} \mid T^n - 1$ , contradicting separability of  $T^n - 1$ .  $\square$

So the minimal polynomial of  $e^{2\pi i/n}$  over  $\mathbb{Q}$  is  $\Phi_n(T)$ .

Now we look at  $K = \mathbb{F}_p$ .

**Proposition 11.4.**  $K = \mathbb{F}_p$ ,  $(n, p) = 1$ . Then

- (i)  $\chi_n : G \rightarrow \langle p \rangle \subseteq (\mathbb{Z}/n\mathbb{Z})^\times$  is an isomorphism. Also  $\chi_n(\varphi_p) = p \pmod{n}$
- (ii)  $[L : K] = r$ , the order of  $p$  modulo  $n$ .
- (iii)  $\varphi_p$  has cycle type  $(r, \dots, r)$  as a permutation of the roots of  $\Phi_n$  (the primitive  $n$ th roots of unity in  $L$ )

[Recall  $\varphi_p \in G$  is  $x \mapsto x^p$  (Frobenius map), and  $\varphi_p$  generates  $G$ ]

*Proof.*  $\varphi_p(\zeta) = \zeta^p$  and  $L = K(\zeta)$  so  $\chi_n(\varphi_p) = p$ , hence  $\chi_n(G) = \langle p \rangle$  and  $[L : K] = |G| = |\langle p \rangle|$  which is the order of  $p$  modulo  $n$ .

If  $(a, n) = 1$ ,  $\varphi_p^k(\zeta^a) = \zeta^a \iff \varphi_p^k(\zeta) = \zeta \iff r \mid k$ . So the orbits of  $\varphi_p$  on  $\{\zeta^a : (a, n) = 1\}$  (the set of roots of  $\Phi_n$ ) all have length  $r$ .  $\square$

**Remarks:**

1. This ‘almost’ gives another proof of the irreducibility of  $\Phi_n$  over  $\mathbb{Q}$ . By the theorem about reduction mod  $p$ ,  $\text{Gal}(\Phi_n/\mathbb{Q}) \supseteq \text{Gal}(\Phi_n/\mathbb{F}_p)$  as subgroups (up to conjugacy) of the symmetric group  $S_{\varphi(n)}$ . It is not hard to show that  $\chi_n(\text{Gal}(\Phi_n/\mathbb{Q})) \supseteq \chi_n(\text{Gal}(\Phi_n/\mathbb{F}_p)) = \langle p \rangle$ . So letting  $p \nmid n$  vary, we have  $\text{Gal}(\Phi_n/\mathbb{Q}) = (\mathbb{Z}/n\mathbb{Z})^\times$ .
2. (iii) implies that the factorisation of  $\Phi_n$  over  $\mathbb{F}_p$  is a product of irreducibles of degree  $r$ , which depends only on  $p \pmod{n}$ . For a general polynomial  $f \in \mathbb{Z}[T]$ , the factorisation of  $f$  modulo  $p$  doesn’t follow any obvious pattern. Trying to answer this question is part of the “Langlands Programme”; the case when there is a pattern is a (congruence) pattern is when  $\text{Gal}(f/\mathbb{Q})$  is abelian, (“Class Field Theory”).

## Application 1

Quadratic reciprocity. Recall: for  $p$  odd prime,  $a \in \mathbb{Z}$ ,  $(a, p) = 1$ , Legendre symbol

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{if } a \text{ is a square mod } p \\ -1 & \text{if not} \end{cases}$$

Euler’s formula:  $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$ . Let  $q \neq p$  another odd prime, let  $n = q$  in the above so  $L = K(\zeta_q)$ , splitting field for  $f = T^q - 1 = (T - 1)\Phi_q$ . So on the roots of  $f$  in  $L$ , Frobenius map  $\varphi_p$  has cycle type  $(1, r, \dots, r)$ . and there are  $(q - 1)/r$   $r$ -cycles. So its sign is  $\text{sgn}(\varphi_p) = (-1)^{(r-1)(q-1)/r} = (-1)^{(q-1)/r}$  ( $q$  is odd). Also  $2 \mid \frac{q-1}{r} \iff r \mid \frac{q-1}{2} \iff p^{\frac{q-1}{2}} \equiv 1 \pmod{q}$  (as  $r$  is the order of  $p \pmod{q}$ ). So  $\text{sgn}(\varphi_p) = \left(\frac{p}{q}\right)$  by Euler’s formula.

As  $G = \langle \varphi_p \rangle$ ,  $\text{sgn}(\varphi_p) = 1 \iff G \subseteq A_q$ . This holds iff  $\text{Disc}(f)$  is a square in  $\mathbb{F}_p$ .

**Lemma 11.5.** *Let  $f = \prod (T - x_i)$  over any field. Then  $\text{Disc}(f) = (-1)^{d(d-1)/2} \prod f'(x_i)$ ,  $d = \deg(f)$ .*

*Proof.* Example Sheet 3. □

Continuing with the previous,  $f = T^q - 1 = \prod_{a=0}^{q-1} (T - \zeta_q^a)$ ,  $f' = qT^{q-1}$ . So

$$\text{Disc}(f) = (-1)^{q(q-1)/2} \prod_{a=0}^{q-1} q\zeta_q^{a(q-1)} = (-1)^{(q-1)/2} q^q \zeta_q^{(q-1)q(q-1)/2} = (-1)^{\frac{q-1}{2}} q^q$$

So

$$\left(\frac{p}{q}\right) = \left(\frac{\text{Disc}(f)}{p}\right) = \left(\frac{(-1)^{(q-1)/2} q}{p}\right) = \left(\frac{q}{p}\right) (-1)^{(p-1)(q-1)/4}$$

Since  $q$  is odd and  $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ . So we have obtained the quadratic reciprocity law.

## Application 2

Construction of regular polygons. Ruler-and-compass construction of regular  $n$ -gon,  $n \geq 3$  is equivalent to constructing the real number  $\cos(2\pi/n)$ .

**Theorem 11.6** (Gauss). *A regular  $n$ -gon is constructable iff  $n$  is a power of 2 times a product of distinct primes, each of which are of the form  $2^{2^k} + 1$ .*

**Remark:** when is  $2^{2^k} + 1 = F_k$  (Fermat numbers) prime?  $F_1 = 5$ ,  $F_2 = 17$ ,  $F_3 = 257$ ,  $F_4 = 65537$  are all prime. Fermat conjectured that all  $F_k$  are prime. However, we have the following result of Euler

**Theorem 11.7** (Euler, 1732).  $F_5 = 641 \times 6700417$ .

Since then, many  $F_k$ 's are known to be composite, none have been seen to be prime for  $k \geq 5$ .

**Lemma 11.8.** *If  $m$  is a positive integer such that  $2^m + 1$  is prime, then  $m$  is a power of 2.*

*Proof.*  $2^{qr} + 1 = (2^r + 1)(2^{q(r-1)} - 2^{q(r-2)} + \dots + 1)$  if  $q$  is odd.  $\square$

*Proof of Theorem 11.6.* Recall  $x \in \mathbb{R}$  is constructible if and only if there exists a sequence of fields  $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \dots \subseteq K_m \ni x$  and  $[K_{i+1} : K_i] = 2$  for all  $0 \leq i \leq m-1$ . In particular, a necessary condition is that  $\deg_{\mathbb{Q}}(x)$  is a power of 2.

In our case,  $x = \cos(2\pi/n) = \frac{1}{2}(\zeta_n + \zeta_n^{-1})$ ,  $\zeta_n = e^{2\pi i/n}$  so  $\zeta_n^2 - 2x\zeta_n + 1 = 0$ . Also  $x \in \mathbb{R}$ ,  $\zeta_n \notin \mathbb{R}$  ( $n \geq 3$ ) so  $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(x)] = 2$ . So if  $x$  is constructible,  $[\mathbb{Q}(\zeta_n) : \mathbb{Q}]$  is a power of 2. But  $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) = \prod_i p_i^{e_i-1}(p_i - 1)$ , where  $n = \prod_{i=1}^r p_i^{e_i}$ . So this is a power of 2 if and only if for all odd  $p_i$ ,  $e_i = 1$  and  $p_i - 1$  is a power of 2. By the above lemma,  $\varphi(n)$  is a power of 2 if and only if it is of the required form.

Now we show the other direction. Suppose  $\varphi(n) = 2^m$ . Then  $\mathbb{Q}(\zeta_n)/\mathbb{Q}$  is Galois, with Galois group  $G \cong (\mathbb{Z}/n\mathbb{Z})^\times$ ,  $|G| = 2^m$ .

Observe that there exist subgroups  $G = H_0 \supseteq H_1 \supseteq \dots \supseteq H_m = \{1\}$  such that  $[H_i : H_{i+1}] = 2$  for all  $0 \leq i \leq m-1$ . Indeed since  $2 \mid |G|$  (assuming  $G \neq \{1\}$ ), there exists  $\sigma \in G$  of order 2 (Cauchy's theorem). Hence take  $H_{m-1} = \langle \sigma \rangle$ , and repeat on  $G/H_{m-1}$  and continue to construct all the  $H_i$ 's. Then  $K_i = \mathbb{Q}(\zeta_n)^{H_i}$  satisfy  $[K_{i+1} : K_i] = (H_i : H_{i+1}) = 2$ .  $\square$

## 12 Kummer extensions

We consider extensions of the form  $L = K(x)$ ,  $x^n = a \in K$  (not necessarily  $a = 1$ ). These extensions are not necessarily Galois, e.g.  $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ .

First we prove a result of independent interest:

**Theorem 12.1** (Linear independence of field embeddings). *Let  $K, L$  be fields,  $\sigma_1, \dots, \sigma_n : K \rightarrow L$  distinct field homomorphisms,  $n \geq 1$ . Then if  $y_1, \dots, y_n \in L$  are such that for all  $x \in K$ ,  $y_1\sigma_1(x) + \dots + y_n\sigma_n(x) = 0$  then  $y_1 = \dots = y_n = 0$ . i.e.  $\sigma_1, \dots, \sigma_n$  are  $L$ -linearly independent elements of the set of functions  $K \rightarrow L$ , which is an  $L$ -vector space.*

This is a special case ( $G = K^\times$ ) of

**Theorem 12.2** (Linear independence of characters). *Let  $G$  be a group,  $L$  a field, and  $\sigma_1, \dots, \sigma_n : G \rightarrow L^\times$  distinct group homomorphisms. Then  $\sigma_1, \dots, \sigma_n$  are linearly independent over  $L$ .*

*Proof.* Induction on  $n$ : if  $n = 1$  the result is obvious. Suppose  $n > 1$ ,  $y_1, \dots, y_n \in L$  such that for all  $g \in G$

$$y_1\sigma_1(g) + \dots + y_n\sigma_n(g) = 0 \quad (*)$$



Then there exists  $h \in G$  such that  $\sigma_1(h) \neq \sigma_n(h)$  (since the  $\sigma_i$  are distinct). As the  $\sigma_i$  are homomorphisms, putting  $hg$  into (\*), we get

$$y_1\sigma_1(h)\sigma_1(g) + \dots + y_n\sigma_n(h)\sigma_n(g) = 0$$

Multiplying (\*) by  $\sigma_n(h)$  and subtracting from the above

$$y'_1\sigma_1(g) + \dots + y'_{n-1}\sigma_{n-1}(g) = 0$$

where  $y'_i = y_i(\sigma_i(h) - \sigma_n(h))$ . Hence by induction  $y'_i = 0$  for all  $i$ , and since  $\sigma_1(h) \neq \sigma_n(h)$ ,  $y_1 = 0$ . Now (\*) becomes a linear dependence between  $\sigma_2, \dots, \sigma_n$ , hence  $y_2 = y_3 = \dots = y_n = 0$  by induction.  $\square$

Assume that  $n > 1$ ,  $n1_K \neq 0$ .

**Theorem 12.3.** *Assume that  $K$  contains a primitive  $n$ th root of 1,  $\zeta = \zeta_n$ . Suppose  $L/K$  is an extension with  $L = K(x)$  and  $x^n = a \in K^\times$ . Then*

- (i)  *$L/K$  is a splitting field for  $f = T^n - a$ , and is Galois with cyclic Galois group.*
- (ii)  *$[L : K]$  is the least  $m \geq 1$  such that  $x^m \in K$ .*

*Proof.*

- (i) As  $\mu_n(K) = \{\zeta_n^i : 0 \leq i < n\}$ , has  $n$  elements, the polynomial  $f$  has  $n$  distinct roots  $\{\zeta^i x\}$  in  $L$ , so  $L/K$  is a splitting field for the separable polynomial  $f$ , thus is Galois. Let  $\sigma \in \text{Gal}(L/K) = G$ . Then  $f(\sigma(x)) = 0$ , so  $\sigma(x) = \zeta^i x$  for some  $i$ , which is unique mod  $n$ . Define

$$\Theta : G \rightarrow \mu_n(K) = \{\zeta^i\} \cong \mathbb{Z}/n\mathbb{Z}$$

by  $\Theta(\sigma) = \frac{\sigma(x)}{x}$  (which must be equal to some  $\zeta^i$ ). We claim this is a homomorphism: let  $\sigma, \tau \in G$ , then because  $\zeta \in K$ ,  $\tau(\Theta(\sigma)) = \Theta(\sigma)$ , so

$$\Theta(\tau\sigma) = \frac{\tau\sigma(x)}{x} = \tau\left(\frac{\sigma(x)}{x}\right) \cdot \frac{\tau(x)}{x} = \tau(\Theta(\sigma)) \cdot \Theta(\tau) = \Theta(\sigma)\Theta(\tau)$$

So  $\Theta$  is a homomorphism, and injective since  $\Theta(\sigma) = 1$  if and only if  $\sigma(x) = x$ , i.e  $\sigma = \text{id}$ . So  $G$  is isomorphic to a subgroup of a cyclic group, thus is cyclic.

- (ii) If  $m > 1$ , since  $L/K$  is Galois,  $x^m \in K$  if and only if for all  $\sigma \in G$ ,  $\sigma(x^m) = x^m$ . This is the same as: for all  $\sigma \in G$ ,  $\Theta(\sigma)^m = 1$ , i.e  $|G| = [L : K] \mid m$  (since  $G$  is cyclic).  $\square$

**Corollary 12.4.** Assume  $K$  contains a primitive  $n$ th root of unity, let  $a \in K^\times$ . Then  $f = T^n - a$  is irreducible in  $K[T]$  iff  $a$  is not a  $d$ th power in  $K$ , for any  $1 \neq d \mid n$ .

*Proof.* Let  $L = K(x)$  for  $x^n = a$ . Then minimal polynomial of  $x$  divides  $f$ , so  $f$  is irreducible if and only if  $G = [L : K] = n$ .

Suppose  $n = md$ ,  $d \neq 1$ . Then  $a$  is a  $d$ th power in  $K$  if and only if  $x^m \in K$  (as  $\zeta_n \in K$ ), which by the previous theorem holds iff  $|G| \mid m$ .  $\square$

**Remark:** this doesn't hold in general if  $\zeta_n \notin K$ . For example, take  $K = \mathbb{Q}$ ,  $T^4 + 4$ .

**Terminology:** extensions of the form  $L = K(\sqrt[n]{a})$ , where  $\zeta_n \in K$ , are called *Kummer extensions*.

**Example.**  $n = 2$ ,  $\text{char}(K) \neq 2$ ,  $\zeta_2 = -1 \in K$ .  $K(\sqrt{a})/K$  is quadratic if  $a \notin (K^\times)^2$ . Conversely (Example sheet 1), every quadratic  $L/K$  is  $L = K(\sqrt{a})$  for some  $a$ .

For general  $n$ :

**Theorem 12.5.** Suppose  $K$  contains a primitive  $n$ th root of unity, where  $n > 1$ . Let  $L/K$  be a Galois extension, with  $\text{Gal}(L/K)$  cyclic of order  $n$ . Then  $L = K(\sqrt[n]{a})$  for some  $a \in K$ .

*Proof.* Let  $G = \text{Gal}(L/K) = \{\sigma^i : 0 \leq i < n\}$ . For  $y \in L$ , let

$$x = R(y) = y + \zeta^{-1}\sigma(y) + \dots + \zeta^{-(n-1)}\sigma^{n-1}(y) = \sum_{j=0}^{n-1} \zeta^{-j}\sigma^j(y)$$

(Lagrange resolvent). Then  $\sigma(x) = \zeta x$  (since  $\sigma^n = \text{id}$ ). Hence  $\sigma(x^n) = x^n$ , i.e.  $x^n \in K$ . By Theorem 12.1 (linear independence of field homomorphisms), there exists  $y$  such that  $x = R(y) \neq 0$ . As  $\sigma^i(x) = \zeta^i x$ , the  $\sigma^i(x)$  are distinct. Hence  $\deg_K(x) = n$  and so  $L = K(x)$ .  $\square$

**Example:** suppose  $L/\mathbb{Q}$  has degree 3 and is Galois. Then as  $\zeta_3 \notin \mathbb{Q}$ , this isn't a Kummer extension.

## 13 Trace and norm

Let  $L/K$  be an extension of degree  $n$  (so  $L$  is a  $n$ -dimensional  $K$ -vector space). Let  $x \in L$ . The map  $u_x : L \rightarrow L$ ,  $y \mapsto xy$  is obviously  $K$ -linear (since it's  $L$ -linear). So it has characteristic polynomial, determinant and trace.

**Definition.** The *trace* and *norm* of  $x$  (relative to  $L/K$ ) are  $\text{Tr}_{L/K}(x) = \text{tr}(U_x)$ ,  $N_{L/K}(x) = \det U_x$  (sometimes write  $\text{tr}_K$ ,  $\det_K$  if it's important to know  $K$ ). The *characteristic polynomial* of  $x$  is  $f_{x,L/K}(T) = \det(T \text{id} - u_x)$ .

Explicitly, let  $(e_i)_{i=1,\dots,n}$  be a basis for  $L/K$ . Then there exists a unique matrix  $A = (a_{ij})$  such that  $xe_i = \sum_j a_{ji}e_j$ . Then  $\text{Tr}_{L/K}(x) = \text{tr}(A)$  etc.

**Example.** Consider  $\mathbb{Q}(\sqrt{d})/\mathbb{Q}$ , a quadratic extension, basis  $\{1, \sqrt{d}\}$  ( $d$  not a square in  $\mathbb{Q}$ ). Let  $x = a + b\sqrt{d}$ . Then  $A = \begin{pmatrix} a & bd \\ b & a \end{pmatrix}$  as  $x \cdot 1 = a \cdot 1 + b\sqrt{d}$  and  $x\sqrt{d} = bd \cdot 1 + a\sqrt{d}$ . So  $\text{Tr}_{L/K}(x) = 2a$ ,  $N_{L/K}(x) = a^2 - b^2d$ .

**Example.**  $\mathbb{C}/\mathbb{R}$ , basis  $\{1, i\}$ . Then matrix of  $u_{x+iy}$  is  $\begin{pmatrix} x & -y \\ y & x \end{pmatrix}$  (usual representation of complex numbers by  $2 \times 2$  real matrices - Cauchy-Riemann).

**Lemma 13.1.** Let  $x, y \in L$ ,  $a \in K$ ,  $n = [L : K]$ . Then

- (i)  $\text{Tr}_{L/K}(x + y) = \text{Tr}_{L/K}(x) + \text{Tr}_{L/K}(y)$  and  $N_{L/K}(xy) = N_{L/K}(x)N_{L/K}(y)$
- (ii)  $N_{L/K}(x) = 0$  if and only if  $x = 0$ .
- (iii)  $\text{Tr}_{L/K}(1) = n$ ,  $N_{L/K}(1) = 1$
- (iv)  $\text{Tr}_{L/K}(ax) = a \text{Tr}_{L/K}(x)$ ,  $N_{L/K}(ax) = a^n N_{L/K}(x)$

So  $\text{Tr}_{L/K}$  is  $K$ -linear,  $N_{L/K} : L^\times \rightarrow K^\times$  is a homomorphism.

*Proof.* Trivial. □

**Theorem 13.2.** *Let  $M/L/K$  be finite extensions. Then for all  $x \in M$ ,  $\text{Tr}_{L/K}(\text{Tr}_{M/L}(x)) = \text{Tr}_{M/K}(x)$  and  $N_{L/K}(N_{M/L}(x)) = N_{M/K}(x)$ .*

*Proof.* We only prove this for the trace, as this is all we'll use. Let  $x \in M$ . Choose bases  $u_1, \dots, u_m$  for  $M/L$  and  $v_1, \dots, v_n$  for  $L/K$ . Let  $(a_{ij})$  be the matrix of  $u_{x, M/L}$  with entries in  $L$ . Then  $\text{Tr}_{M/L}(x) = \sum_{i=1}^m a_{ii}$ . For each  $(i, j)$  let the matrix of  $U_{a_{ij}, L/K}$  be  $A_{ij}$  (entries in  $K$ ). Then  $\text{Tr}_{L/K}(\text{Tr}_{M/L}(x)) = \sum_{i=1}^m \text{Tr}_{L/K}(a_{ii}) = \sum_{i=1}^m \text{tr}(A_{ii})$ .

Now we consider the basis  $u_1 v_1, \dots, u_1 v_n, \dots, u_m v_m$  for  $M/K$ . Then the matrix of  $u_{x, M/K}$  is the block matrix

$$\begin{pmatrix} A_{11} & A_{12} & \dots & & \\ A_{21} & A_{22} & \dots & & \\ \vdots & \vdots & \ddots & & \\ & & & A_{nn} & \end{pmatrix}$$

so  $\text{Tr}_{M/K}(x) = \sum_{1 \leq i \leq n} \text{tr}(A_{ii})$ .  $\square$

**Proposition 13.3.** *Suppose  $L = K(x)$ , and let  $f = T^n + c_{n-1}T^{n-1} + \dots + c_0 \in K[T]$  be the minimal polynomial of  $x/K$ . Then  $f_{x, L/K} = f$  and  $\text{Tr}_{L/K}(x) = -c_{n-1}$ ,  $N_{L/K}(x) = (-1)^n c_0$ .*

*Proof.* It is enough to prove the first statement since the other properties are immediate from basic linear algebra. In terms of the basis  $1, x, \dots, x^{n-1}$  for  $L/K$ , the matrix of  $u_x$  is

$$\begin{pmatrix} 0 & 0 & \dots & 0 & -c_0 \\ 1 & 0 & \dots & 0 & -c_1 \\ 0 & 1 & \dots & 0 & -c_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \dots & 1 & -c_{n-1} \end{pmatrix}$$

Since  $u_x(x^i) = x^{i+1}$  for all  $0 \leq i \leq n-2$  and  $u_x(x^{n-1}) = x^n = -\sum_j c_j x^j$ . This matrix has characteristic polynomial  $f$ .  $\square$

**Corollary 13.4.** *Assume  $\text{char}(K) = p > 0$ ,  $L = K(x)$ , where  $x \notin K$ ,  $x^p \in K$ . Then for all  $y \in L$ ,  $\text{Tr}_{L/K}(y) = 0$  and  $N_{L/K}(y) = y^p$ .*

*Proof.* Recall that  $[L : K] = p$  (Example sheet 2, Q7). If  $y \in K$ , then  $\text{Tr}_{L/K}(y) = py = 0$  and  $N_{L/K}(y) = y^p$ . Otherwise since  $[L : K]$  is prime,  $L = K(y)$ , and if  $y = \sum a_i x^i$  for  $a_i \in K$ , then  $y^p = \sum a_i^p (x^p)^i \in K$ . So the minimal polynomial of  $y$  is  $T^p - y^p$ . So done by 13.3.  $\square$

**Proposition 13.5.** *Let  $L/K$  be a finite separable extension of degree  $n$ . Let  $\sigma_1, \dots, \sigma_n : L \rightarrow M$  be the distinct  $K$ -homomorphisms into a normal closure  $M$  for  $L/K$ . Then  $\text{Tr}_{L/K}(x) = \sum_{i=1}^n \sigma_i(x)$ ,  $N_{L/K}(x) = \prod_{i=1}^n \sigma_i(x)$ , and  $f_{x, L/K} = \prod_{i=1}^n (T - \sigma_i(x))$ .*

**Remark:** if  $L/K$  is a finite Galois extension, then  $\text{Tr}_{L/K}(x) = \sum_{\sigma \in G} \sigma(x)$  etc.

*Proof.* Again it is enough to show that  $f_{x,L/K}$  is of that form. Let  $(e_i)$  be a basis for  $L/K$ , and let  $P = (\sigma_i(e_j))_{ij} \in \text{Mat}_{n \times n}(M)$ . Recall that the  $\sigma_i$  are linearly independent (12.1), so there doesn't exist any  $y_1, \dots, y_n \in M$  such that  $\sum_i u_i \sigma_i(e_j) = 0$  for all  $j$ . So  $P$  is non-singular.

Let  $A = (a_{ij})$  be a matrix of  $u_x$ . Then  $xe_j = \sum_r a_{rj} e_r$  hence

$$\sigma_i(x)\sigma_i(e_j) = \sum_r \sigma_i(e_r)a_{rj} \quad (*)$$

for all  $i, j$ . So if  $S$  is the diagonal matrix with  $(i, i)$  entry  $\sigma_i(x)$ , then  $(*)$  says that  $SP = PA$ , so  $S = PAP^{-1}$  as  $P$  was invertible. Therefore  $S, A$  are conjugates and have the same characteristic polynomial.  $S$  has characteristic polynomial  $\prod_{i=1}^n (T - \sigma_i(x))$  and  $A$  has characteristic polynomial  $f_{x,L/K}$ .  $\square$

For the next theorem, note first that since  $\text{Tr}_{L/K} : L \rightarrow K$  is  $K$ -linear, it is either surjective or the zero map.

**Theorem 13.6.** *Let  $L/K$  be a finite extension. Then  $L/K$  is separable if and only if  $\text{Tr}_{L/K}$  is surjective.*

**Remark:** if  $\text{char}(K) = 0$ , it is obvious that  $\text{Tr}_{L/K}(1) = n \neq 0$  so result is easy in this case.

*Proof.* Suppose  $L/K$  is separable and  $\{\sigma_1, \dots, \sigma_n\} = \text{Hom}_K(L, M)$  for a normal closure  $M$  of  $L/K$ . Then  $\text{Tr}_{L/K}(x) = \sum \sigma_i(x)$ . By linear independence of the  $\sigma_i$ , there exists  $x$  such that  $\text{Tr}_{L/K}(x) \neq 0$ . Hence  $\text{Tr}_{L/K}$  is surjective.

Conversely, suppose  $L/K$  is inseparable, then there exists  $x \in L$  such that  $K(x) \supsetneq K(x^p)$  (Example sheet 2, Q7). By Corollary 13.4,  $\text{Tr}_{K(x)/K(x^p)} = 0$ , so by 13.2,  $\text{Tr}_{M/K} = 0$ .  $\square$

**Example.** Finite fields  $\mathbb{F}_{q^n}/\mathbb{F}_q$  ( $q = p^n$ ) - this is separable, so there exists  $x \in \mathbb{F}_{q^n}$  such that  $\text{Tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x) = 1$  (exercise: prove this directly using the fact that the multiplicative group is cyclic).

**Remark:** can use this criterion (13.6) to give another proof that if  $M/L$  and  $L/K$  are separable, then so is  $M/K$ .

## 14 Algebraic closure

**Definition.** A field  $K$  is *algebraically closed* if every non-constant polynomial in  $K[T]$  splits into linear factors over  $K$ . Equivalently, the only irreducibles in  $K[T]$  are the linear polynomials.

**Example.**  $\mathbb{C}$  is algebraically closed (FTA).

**Proposition 14.1.** *The following conditions on a field  $K$  are equivalent*

1.  $K$  is algebraically closed
2. if  $L/K$  is an extension, and  $x \in L$  is algebraic over  $K$ , then  $x \in K$
3. if  $L/K$  is algebraic, then  $L = K$

*Proof.* We first show (i) implies (ii): let  $L, x$  be as in (ii). Let  $f$  be the minimal polynomial of  $x/K$ . Then  $f$  is linear, so  $x \in K$ .

Now show (ii) implies (iii): by definition of algebraic, all  $x \in L$  are algebraic over  $K$ , so  $x \in K$ .

Now show (iii) implies (i): let  $f \in K[T]$  be irreducible,  $L = K[T]/(f)$ , which is algebraic over  $K$ . Then (iii) implies  $L = K$  so  $f$  is linear.  $\square$

**Proposition 14.2.** *Let  $L/K$  be algebraic, and suppose that every irreducible polynomial  $f \in K[T]$  splits into linear factors in  $L[T]$ . Then  $L$  is algebraically closed (such a field is called an algebraic closure of  $K$ ).*

*Proof.* Let  $M/L$  be an extension,  $x \in M$  algebraic over  $L$  (so by 4.4)  $x$  is algebraic over  $K$ ; by hypothesis  $m_{x,K} \in K[T]$  splits into linear factors over  $L$ . So  $x \in L$  hence by (ii) in the previous proposition,  $L$  is algebraically closed.  $\square$

**Corollary 14.3.** *The field  $\overline{\mathbb{Q}} \subseteq \mathbb{C}$  of all algebraic numbers is algebraically closed (and is an algebraic closure of  $\mathbb{Q}$ ).*

*Proof.* We apply 14.2 to  $\overline{\mathbb{Q}}/\mathbb{Q}$ ; this extension is algebraic and if  $f \in \mathbb{Q}[T]$  is irreducible, then by the FTA,  $f = \prod (T - x_i) \in C[T]$ , and  $x_i \in \overline{\mathbb{Q}}$  (by definition of  $\overline{\mathbb{Q}}$ ). So the hypotheses of 14.2 hold.  $\square$

By proposition 14.2, an algebraic closure of  $K$  is the same as an algebraic extension of  $K$  which is algebraically closed. The main results are:

- every field has an algebraic closure
- it is unique up to isomorphism

The main difficulty in proving these are set-theoretic. “Morally” we are trying to find “a splitting field for all polynomials over  $K$ ”.

Special case:  $K$  countable - then  $K[T]$  is also countable. Enumerate the monic irreducibles  $\{f_i : i \geq 1\}$  in  $K[T]$ . Let  $L_0 = K$ , and for each  $i \geq 1$ , let  $L_i$  be a splitting field for  $f_i$  over  $L_{i-1}$  [it is possible to do this without the axiom of choice]. We may assume that  $L_{i-1} \subseteq L_i$  is a subfield (if  $\sigma : L_{i-1} \rightarrow L_i$  is an extension, replace  $L_i$  with  $L_{i-1} \cup (L_i \setminus \sigma(L_{i-1}))$ ). Let  $L = \bigcup_{i \geq 0} L_i$ . Then every  $f_i$  splits in  $L[T]$  so  $L$  is an algebraic closure of  $K$ .

**Example.**  $\mathbb{F}_p$  has an algebraic closure.

For general (uncountable) fields, we need some set-theoretic “trick”.

**Lemma** (Zorn’s Lemma). Let  $S$  be a non-empty partially ordered set. Suppose that every chain in  $S$  has an upper bound in  $S$ . Then  $S$  has a maximal element.

**Definition.** A binary relation  $\leq$  on a set  $S$  is a *partial order* if  $\forall x, y, z \in S$

- (i)  $x \leq x$
- (ii)  $x \leq y$  and  $y \leq z \implies x \leq z$
- (iii)  $x \leq y$  and  $y \leq x \implies x = y$

$(S, \leq)$  is a *partially ordered set* or *poset*. It is *totally ordered* if moreover

- (iv)  $\forall x, y \in S$ , either  $x \leq y$  or  $y \leq x$

**Definition.** A *chain* in a poset  $(S, \leq)$  is a subset  $T \subseteq S$  which under  $\leq$  is totally ordered. An *upper bound* for  $T \subseteq S$  is an element  $z \in S$  such that  $\forall x \in T, x \leq z$ . An element  $y \in S$  is *maximal* if  $\forall x \in S, y \leq x \implies y = x$ .

If  $S$  is totally ordered, it is easy to see it has at most one maximal element.

**Example.** Let  $V$  be a vector space (over a field  $K$ ). Then  $V$  has a basis.

Indeed if  $V = \{0\}$  this is trivial. Otherwise let  $S = \{X \subseteq V : X \text{ linearly independent}\}$ . Define a partial order on  $S$  by inclusion:  $X \leq X'$  if  $X \subseteq X'$ .  $S$  is non-empty so let  $T \subseteq S$  be a chain and define  $Y = \bigcup_{X \in T} X$ . We need to check  $Y \in S$ . It is enough to check any finite subset  $\{y_1, \dots, y_k\}$  of  $Y$  is linearly independent, say  $y_i \in X_i$  for  $X_i \in T$ . Since  $T$  is a chain, we may assume  $X_1 \subseteq X_2 \subseteq \dots \subseteq X_k$  and therefore  $\{y_1, \dots, y_k\} \subseteq X_k$  and thus are linearly independent.

**Proposition 14.4.** *Let  $L/K$  be an algebraic extension and  $M$  an algebraically closed field,  $\sigma : K \rightarrow M$  a homomorphism. Then there exists  $\bar{\sigma} : L \rightarrow M$  extending  $\sigma$ .*

*Proof.* If  $L = K(x)$ ,  $x$  algebraic over  $K$  with minimal polynomial  $f = m_{x,K}$ , then  $\sigma f \in M[T]$  splits into linear factors. So there exists  $\bar{\sigma} : K(x) \rightarrow M$  extending  $\sigma$  (in fact there is one homomorphism for each root of  $\sigma f$  in  $M$ ).

Now we prove it for general  $L$ . Assume  $K \subseteq L$  is a subfield (if not consider image of  $K$  in the extension). Let

$$S = \{(F, \tau) : K \subseteq F \subseteq L, \tau : F \rightarrow M \text{ a homomorphism with } \tau|_K = \sigma\}$$

Write  $(F, \tau) \leq (F', \tau')$  if  $F \subseteq F'$  and  $\tau'|_F = \tau$ . Then  $(S, \leq)$  is a poset,  $(K, \sigma) \in S$  so  $S \neq \emptyset$ . Consider a chain  $T = \{(F_i, \tau_i)\}_{i \in I} \subseteq S$  ( $I$  some index set). Let  $F' = \bigcup_{i \in I} F_i$ , since  $T$  is a chain,  $\forall i, j$  either  $F_i \subseteq F_j$  or  $F_j \subseteq F_i$ . So if  $x \in F_i$ ,  $y \in F_j$ , then (assuming  $F_i \subseteq F_j$ )  $xy, x + y \in F_j \subseteq F'$ , so  $F'$  is a field. Define  $\tau' : F' \rightarrow M$  by  $\tau'(x) = \tau_i(x)$  for  $x \in F_i$ . Since  $F_i \subseteq F_j$  implies  $\tau_j|_{F_i} = \tau_i$ , and  $T$  is a chain,  $\tau'$  is well defined. So  $(F', \tau') \in S$  and it is an upper bound for  $T$ .

So by Zorn's lemma,  $S$  has a maximal element  $(F, \tau)$ . We claim that  $F = L$ . If  $x \in L$ , then by the above applied to  $F(x)/F \xrightarrow{\tau} M$ , can extend  $\tau$  to some  $\bar{\tau} : F(x) \rightarrow M$ . Then  $(F(x), \bar{\tau}) \in S$  and  $(F, \tau) \leq (F(x), \bar{\tau})$ . So by maximality  $F(x) = F$ , i.e  $x \in F$ .  $\square$

The proof of existence of algebraic closure will use the following.

**Theorem 14.5** (“Maximal ideal theorem”). *Let  $R$  be a non-zero ring (with a 1 and commutative). Then  $R$  has a maximal ideal.*

*Proof.* Let  $S = \{\text{proper ideals } I \subsetneq R\}$ , partially ordered by inclusion. A maximal ideal is then just a maximal element of  $S$ . Let  $\emptyset \neq T \subseteq S$  be a chain. Then  $J := \bigcup_{I \in T} I$  is an ideal (easy to check). As  $1 \notin I$ , for all  $I \in S$ ,  $1 \notin J$ . So  $J$  is a proper ideal and is clearly an upper bound for  $T$ . Now apply Zorn's lemma.  $\square$

**Theorem 14.6.** *Let  $K$  be a field. Then  $K$  has an algebraic closure  $\bar{K}$ . If  $\sigma : K \xrightarrow{\sim} K'$  is an isomorphism and  $\bar{K}, \bar{K}'$  are algebraic closures of  $K$  and  $K'$  respectively, then there exists an isomorphism  $\bar{\sigma} : \bar{K} \xrightarrow{\sim} \bar{K}'$  extending  $\sigma$  (so algebraic closure is unique up to isomorphism).*

*Proof.* First we prove existence. Let  $P = \{\text{monic irreducibles in } K[T]\}$ . We construct  $K_1$  such that every  $f \in P$  has a root in  $K_1$ . We first find a ring in which every  $f \in P$  has a root. Let  $R = K[\{T_f\}_{f \in P}]$  (i.e the finite  $K$ -linear combinations of monomials  $T_{f_1}^{m_1} \dots T_{f_k}^{m_k}$ ,  $f_i \in P$ ). Let  $I$  be the ideal generated by  $\{f(T_f) : f \in P\}$ . In  $R/I$ ,  $T_f + I$  is a root of  $f$ . We check  $I \neq R$ : if  $I = R$ , then  $1 \in I$  so for some finite subset  $Q \subseteq P$ , there exist  $r_f \in R$  (with  $f \in Q$ ) with  $1 = \sum_{f \in Q} r_f f(T_f)$ . Enlarging  $Q$  if necessary, we may assume each  $r_f$  is a



polynomial in  $\{T_g : g \in Q\}$ .

Let  $L/K$  be a splitting field for  $\prod_{f \in Q} f \in K[T]$ , and for each  $f \in Q$  take some  $a_f$  which is a root of  $f$ . Consider  $\varphi : R \rightarrow L$ ,  $\varphi|_K = \text{id}$ ,  $\varphi(T_f) = a_f$  if  $f \in Q$  and  $\varphi(T_f) = 0$  if  $f \notin Q$ . Then  $1 = \varphi(1) = \sum_{f \in Q} \varphi(r_f f(T_f)) = \sum_{f \in Q} \varphi(r_f) f(a_f) = 0$ , a contradiction.

Now apply the maximal ideal theorem to  $R/I$  to get a maximal ideal  $\bar{J}$ , or equivalently there exists a maximal ideal  $J \subseteq R$  containing  $I$  (ideals of  $R/I$  biject with ideals of  $R$  containing  $I$ ). Let  $K_1 = R/J$ , a field; let  $x_f = T_f + J \in K_1$ . Then  $K_1/K$  is generated by  $\{x_f\}$ ,  $f(x_f) = 0$ . So  $K_1/K$  is an algebraic extension of  $K$  in which every polynomial has a root. Apply the same procedure to  $K_1$ ,  $P_1 = \{\text{monic irreducibles in } K_1[T]\}$  to get  $K_2$ , and so on. Obtain  $K \subseteq K_1 \subseteq K_2 \subseteq \dots$  such that if  $f \in K_n[T]$  is irreducible, it has a root in  $K_{n+1}$ .

So if  $f \in K[T]$  is non constant, then  $f = (T - x_1)f_1 \in K_1[T]$  then  $f_1 = (T - x_2)f_2 \in K_2[T]$  so  $f$  factorises into linear factors in  $K_{\deg f}[T]$ . Therefore  $\bar{K} = \bigcup_n K_n$  is an algebraic closure of  $K$ .

Now we show uniqueness. Let  $K \subseteq \bar{K}$ ,  $K' \subseteq \bar{K}'$  be algebraic closures,  $\sigma : K \xrightarrow{\sim} K'$ . Then by 14.4,  $\sigma$  extends to a homomorphism  $\bar{\sigma} : \bar{K} \rightarrow \bar{K}'$  (as  $\bar{K}/K$  is algebraic and  $\bar{K}'$  is algebraically closed). But  $K' \subseteq \sigma(\bar{K}) \subseteq \bar{K}'$ , so  $\bar{K}'/\sigma(\bar{K})$  is algebraic. As  $\bar{K}$  is algebraically closed, so is  $\sigma(\bar{K})$ . So  $\bar{K}' = \sigma(\bar{K})$  (14.1 (iii)).  $\square$

## 15 Cubics & quartics

Let  $f \in K[T]$  be a monic cubic which is separable. Then  $G := \text{Gal}(f/K) \leq S_3$  acting on the roots  $x_1, x_2, x_3$  in a splitting field  $L$ .

If  $f$  is reducible,  $f$  is the product of linear factors in  $K$  so  $G = \{e\}$ . If  $f$  is the product of a linear and a quadratic polynomial then  $G = S_2$ .

If  $f$  is irreducible (assuming  $\text{char}(K) \notin \{2, 3\}$ ) then  $G = S_3$  or  $A_3$ ; and  $G = A_3$  iff  $\Delta^2 = \text{Disc}(f) \in (K^\times)^2$ .

$$\begin{array}{ccc}
 L = K(x_1, x_2, x_3) & & \{e\} \\
 \left| \begin{array}{c} 3 \text{ if } f \text{ irred, } 1 \text{ otherwise} \end{array} \right. & & \left| \right. \\
 K(\Delta) = L^{G \cap A_3} & & G \cap A_3 \\
 \left| \begin{array}{c} 2 \text{ if } \Delta^2 \in (K^\times)^2, 1 \text{ otherwise} \end{array} \right. & & \left| \right. \\
 K & & G
 \end{array}$$

Let  $K_1 = K(\Delta)$ . Then  $K_1 = L$  if  $f$  is reducible. If  $f$  is irreducible, then  $L/K_1$  is Galois with Galois group  $\mathbb{Z}/3\mathbb{Z}$ . If  $\omega \in K_1$  is a primitive 3rd root of unity, then  $L = K_1(y)$  for some  $y$  with  $y^3 \in K$  (Kummer extension). If not, let  $L(\omega)$  be the splitting field of  $f(T^3 - 1)$  over  $K$ . Then  $L(\omega)/K_1(\omega)$  is Galois, with Galois group  $\mathbb{Z}/3\mathbb{Z}$ . So  $L(\omega) = K_1(\omega, y)$  with  $y^3 \in K_1(\omega)$ . So the  $x_i$  lie in a field obtained by adjoining successive square and cube roots to  $K$  ( $\omega = \frac{-1+\sqrt{-3}}{2}$ ). This is effectively Cardano's solution.

Explicitly, assume wlog that  $f(T) = T^3 + bT + c$ . Then  $\Delta^2 = -4b^3 - 27c^2$ . There are two cases:

- $b = 0$ , then roots of  $f$  are  $\omega^j \sqrt[3]{-c}$ , so take  $y$  to be any of these
- $b \neq 0$ , then  $y$  a Lagrange resolvent: if the roots of  $f$  in  $L$  are  $x_1, x_2, x_3$ , take  $y = x_1 + \omega^2 x_2 + \omega x_3$  and  $y' = x_1 + \omega x_2 + \omega^2 x_3$ . Then  $y = (1 - \omega)(x_1 - \omega x_2)$  since  $x_1 + x_2 + x_3 = 0$ . Then  $L(\omega) = K(\Delta, \omega, y)$  if and only if  $y \neq 0$  (by proof of structure of Kummer extensions).  $yy' = -3b$  (direct computation) so  $y \neq 0$ , also  $y + y' = y + y' + (x_1 + x_2 + x_3) = 3x_1$  and  $y^3 = \frac{1}{2}(-3\sqrt{-3}\Delta + 27c)$  (direct computation again), so  $x_1 = y - \frac{3b}{y}$ .

Now let  $f \in K[T]$  be a monic, separable quartic,  $\text{char}(K) \notin \{2, 3\}$ .  $\text{Gal}(f/K) \subseteq S_4$ . Consider the action of  $S_4$  on the partitions

$$(12 \mid 34), (13 \mid 24), (14 \mid 23) \text{ of } \{1, 2, 3, 4\}$$

So this gives a homomorphism  $S_4 \rightarrow S_3$  which has kernel  $V = \{e, (12)(34), (13)(24), (14)(23)\}$  (Klein's 4-groups). So the homomorphism is surjective. Take a splitting field  $L$  for  $f$ , roots  $x_1, \dots, x_4$ . Assume  $x_1 + \dots + x_4 = 0$ , i.e.  $f = T^4 + aT^2 + bT + c$ .

$$\begin{array}{ccc} L & & \{e\} \\ \downarrow & & \downarrow \\ M = L^{G \cap V} & & G \cap V \\ \downarrow & & \downarrow \\ K & & G \end{array}$$

As  $V \trianglelefteq S_4$ ,  $G \cap V \trianglelefteq G$  and  $\text{Gal}(M/K) = G/G \cap V \rightarrow S_4/V \cong S_3$ . So we should be able to write  $M$  as the splitting field of a cubic.

Let  $y_{12} = x_1 + x_2 = -(x_3 + x_4) = -y_{34}$ ,  $y_{13} = x_1 + x_3 = -y_{24}$ ,  $y_{14} = x_1 + x_4 = -y_{23}$ . Note that each element in  $G \cap V$  maps  $y_{12}$  to  $y_{12}$  or  $y_{32} = -y_{12}$  and similarly for  $y_{13}$  etc. So  $y_{12}^2, y_{13}^2, y_{14}^2$  are fixed under  $V \cap G$ . If  $y_{12}^2 = y_{13}^2$ , either  $y_{12} = y_{13}$  implying  $x_2 = x_3$ , or  $y_{12} = -y_{13}$  implying  $2x_1 + x_2 + x_3 = x_1 - x_4 = 0$ , both of which are impossible ( $f$  separable).

So  $\{y_{ij}^2\}$  are the roots of a separable cubic  $g \in K[T]$ , the *resolvent cubic*. Now  $M = L^{G \cap V}$  is the splitting field of  $g$ . Note  $x_1 = \frac{1}{2}(y_{12} + y_{13} + y_{14})$ ; likewise for  $x_2$  etc. Hence  $L = M(y_{12}, y_{13}, y_{14})$ . So compute

$$g = (T - y_{12}^2)(T - y_{13}^2)(T - y_{14}^2) = T^3 + 2aT^2 + (a^2 - 4c)T - b^2$$

In particular,  $y_{12}y_{13}y_{14} = b$ , so  $L = M(y_{12}, y_{13})$ ,  $y_{12}^2, y_{13}^2 \in M$ . So we have found a way to solve  $f = 0$  by first solving the resolvent equation  $g = 0$  and then taking (at most two) square roots.

## 16 Solubility by radicals

Suppose  $f \in K[T]$  monic,  $\text{char}(K) = 0$ . What does it mean to have a “formula” for roots of  $f$ ?

**Definition.** An irreducible polynomial  $f \in K[T]$  is *soluble by radicals over  $K$*  if there exist a sequence of fields  $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_m$  with  $x \in K_m$  a root of  $f$  and  $K_i = K_{i-1}(y_i)$  where  $y_i^{d_i} \in K_{i-1}$  ( $d_i \geq 1$ ).

We can adjoin “extra” roots if we want. Then we see that  $f$  is soluble by radicals over  $K$  if there exist  $d \geq 1$  and  $K = K_0 \subseteq K_1 \subseteq \dots \subseteq K_m$  such that

- $f$  has a root  $x \in K_m$
- $K_1 = K(\zeta_d)$ ,  $\zeta_d$  primitive  $d$ th root of unity
- For  $i \geq 1$ ,  $K_i = K_{i-1}(y_i)$  where  $a_i = y_i^d \in K_{i-1}$ .

Call this condition (R).

Note that  $K_1/K_0$  is Galois, with abelian Galois group. For  $i \geq 1$ ,  $K_i/K_{i-1}$  is Galois, with group  $\subseteq \mathbb{Z}/d\mathbb{Z}$  (Kummer extension).

To get all the roots of  $f$ , look at a normal closure  $M$  of  $K_m$ . This contains a splitting field for  $f$  over  $K$  (contains one root and  $f$  is irreducible).

To determine  $M$ , let  $K'_i \subseteq M$  be the normal closure of  $K_i$  (so  $K'_1 = K_1 = K(\zeta_d)$ ).

**Proposition 16.1.**  $K'_i = K'_{i-1}(\{ \sqrt[d]{\sigma(a_i)} : \sigma \in \text{Gal}(K'_{i-1}/K) \})$

*Proof.* Let  $\sigma \in \text{Gal}(K'_{i-1}/K)$ , then there exists  $\bar{\sigma} \in \text{Gal}(K'_i/K)$  such that  $\bar{\sigma}|_{K'_{i-1}} = \sigma$ ,  $K'_i \ni \bar{\sigma}(y_i)$  as  $K'_i/K$  is Galois and  $\bar{\sigma}(y_i)^d = \sigma(y_i^d) = \sigma(a_i)$ . So  $\text{RHS} \subseteq K'_i$ .

Now it is enough to show that the RHS is normal. But the RHS is a splitting field over  $K'_{i-1}$  of  $\prod_{\sigma} (T^d - \sigma(a_i)) = g_i \in K[T]$ .

If  $K'_{i-1}$  is a splitting field of some  $h_{i-1}$  over  $K$ , then the RHS is the splitting field of  $g_i h_{i-1}$  over  $K$ , so is normal.  $\square$

**Proposition 16.2.**  $\text{Gal}(K'_i/K'_{i-1})$  is abelian.

*Proof (variant on Theorem 12.3).* Let  $A = \text{Gal}(K'_i/K'_{i-1})$ . For all  $\tau \in A$ ,  $\sigma \in \text{Gal}(K'_{i-1}/K)$ ,  $\tau(\sqrt[d]{\sigma(a_i)}) = \zeta_d^{m_\sigma} \sqrt[d]{\sigma(a_i)}$ ,  $m_\sigma \in \mathbb{Z}/d\mathbb{Z}$ . Then  $\tau \mapsto (m_\sigma)_{\sigma \in \text{Gal}(K'_{i-1}/K)} \in (\mathbb{Z}/d\mathbb{Z})^r$ ,  $r = |\text{Gal}(K'_{i-1}/K)|$  is an injective homomorphism  $A \rightarrow \mathbb{Z}/d\mathbb{Z}$  (for details review 12.3).

Set  $i = 1$  so  $K'_1 = K_1 = K(\zeta_d)$  so the Galois group  $\subseteq (\mathbb{Z}/d\mathbb{Z})^\times$ .  $\square$

$$\begin{array}{ccc}
 M = K'_m & & \{e\} \\
 | & & | \\
 K'_{m-1} & & N_{m-1} \\
 | & & | \\
 \vdots & & \vdots \\
 | & & | \\
 K = K_0 & & N_0 = G = \text{Gal}(M/K)
 \end{array}$$

**Definition.** A finite group  $G$  is soluble (or solvable) if there exist a chain of normal subgroups. i.e there exist  $N_i \trianglelefteq G$  such that  $G = N_0 \supseteq N_1 \supseteq \dots \supseteq N_m = \{e\}$  such that  $N_i/N_{i+1}$  is abelian for all  $i$ .

**Example.** (Simplest non-abelian soluble group)  $\{e\} \trianglelefteq A_3 \trianglelefteq S_3$ ,  $S_3/A_3 \cong \mathbb{Z}/2\mathbb{Z}$ ,  $A_3 \cong \mathbb{Z}/3\mathbb{Z}$ .

$S_4 \supseteq A_4 \supseteq V = (\mathbb{Z}/2\mathbb{Z})^2 \supseteq \{e\}$ , both  $V \trianglelefteq S_4$  and  $A_4 \trianglelefteq S_4$ ,  $S_4/A_4 \cong \mathbb{Z}/2\mathbb{Z}$ ,  $A_4/V \cong \mathbb{Z}/3\mathbb{Z}$ .

If  $G = \text{Gal}(M/K)$  as above, then  $N_i/N_{i+1} = \text{Gal}(K'_i/K'_{i-1})$  is abelian by 16.2. Hence  $G$  is soluble.

**Theorem 16.3** (Abel-Ruffini). If  $f \in K[T]$  is soluble by radicals over  $K$ , then  $\text{Gal}(f/K)$  is soluble.

*Proof.*  $\text{Gal}(f/K) = \text{Gal}(L/K) \cong \text{Gal}(M/K)/\text{Gal}(M/L)$ . As  $\text{Gal}(M/K)$  is soluble, result follows from the below lemma.  $\square$

**Lemma 16.4.** Every subgroup and quotient of a soluble group is soluble.

*Proof.*  $\{e\} \trianglelefteq N_m \dots \trianglelefteq N_1 \trianglelefteq N_0 = G$ ,  $N_i/N_{i+1}$  abelian,  $H \subseteq G$  subgroup. Then  $H \cap N_i \trianglelefteq G$  and  $(H \cap N_i)/(H \cap N_{i+1}) \rightarrow N_i/N_{i+1}$  is injective. So  $(H \cap N_i)/(H \cap N_{i+1})$  abelian and  $H$  is soluble.

Suppose  $\pi : G \rightarrow \bar{G} = G/H$ ,  $H$  normal subgroup of  $G$ . Then  $\pi(N_i) \trianglelefteq \bar{G}$ , and  $N_i/N_{i+1} \rightarrow \pi(N_i)/\pi(N_{i+1})$  is surjective.  $\square$

**Proposition 16.5.** *If  $n \geq 5$ , then  $S_n$  and  $A_n$  are not soluble.*

*Proof.*  $A_5 \subseteq A_n \subseteq S_n$ , so it suffices to prove (by 16.4) that  $A_5$  is not soluble. But  $A_5$  is not abelian and it is simple, so is not soluble.  $\square$

**Corollary 16.6.** *If  $\deg(f) = n \geq 5$  and  $\text{Gal}(f/K) \supseteq A_n$  (i.e equals  $A_n$  or  $S_n$ ), then  $f$  is not soluble by radicals.*

*Proof.* Combine the previous.  $\square$

**Remark:** it is easy to show the converse of 16.3.

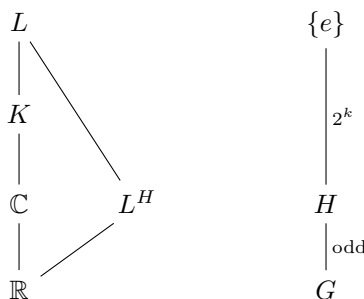
## 17 $\mathbb{C}$ is algebraically closed

What we'll use:

- (i) Every polynomial of odd degree over  $\mathbb{R}$  has a root (intermediate value theorem)
- (ii) Every quadratic over  $\mathbb{C}$  splits into linear factors (can take square roots)
- (iii) Every finite group  $G$  has a subgroup  $H$  such that  $(G : H)$  is odd and  $H = 2^k$  for some  $k$  (Sylow theorem  $p = 2$ )
- (iv) If  $G$  is a  $p$ -group then  $G$  has a subgroup of index  $p$  (since  $G$  has non-trivial centre)

*Proof.* Let  $K/\mathbb{C}$  be a finite extension. Let  $L \supseteq K$  be a normal closure over  $\mathbb{R}$ , so  $G = \text{Gal}(L/\mathbb{R})$ . We'll show  $L = \mathbb{C}$ .

Let  $H \leq G$  be a Sylow 2-subgroup. Then  $[L^H : \mathbb{R}] = (G : H)$  which is odd. So if  $x \in L^H$ , by (i)  $x \in \mathbb{R}$ , i.e  $L^H = \mathbb{R}$  so  $G = H$  is a 2-group. Let  $G \supseteq G_1 = \text{Gal}(L/\mathbb{C})$  and  $G_2 \subseteq G_1$  a subgroup of index 2 (exists by (iv)). Then  $[L^{G_2} : \mathbb{C}] = (G_1 : G_2) = 2$  contradicting (ii).



So  $G$  has no subgroup of index 2, i.e  $G_1 = \{e\}$  so  $L = \mathbb{C}$ .  $\square$

## 18 Artin's Theorem

**Theorem 18.1** (Artin's theorem on invariants). *Let  $L$  be a field,  $G \leq \text{Aut}(L)$  a finite subgroup,  $L^G = \{x \in L : \sigma(x) = x \forall \sigma \in G\}$  a subfield of  $L$ . Then  $[L : L^G] = |G|$ . In particular,  $L/L^G$  is finite, so is Galois with Galois group  $G$ .*

**Remark:** compare this with theorem 9.2: no  $K$  is involved in this one.

*Proof.* If we know  $L/L^G$  is finite, then we can apply theorem 9.2 to see  $[L : L^G] = |G|$ . Let  $K = L^G$ , and take  $x \in L$ . Then if  $\{\sigma_1(x), \dots, \sigma_r(x)\}$  is the orbit of  $G$  on  $x$ ,  $x$  is a root of the polynomial  $f = \prod_{i=1}^r (T - \sigma_i(x)) \in L^G[T] = K[T]$ . So  $x$  is algebraic and separable over  $K$ , and  $\deg_K(x) = r \leq |G|$ . Choose  $y \in L$  with  $\deg_K(y)$  maximal.

Now we claim that  $L = K(y)$  (so is finite over  $K$ ). If not, there exists  $x \in L \setminus K(y)$ . By the above,  $x$  and  $y$  are both algebraic and separable over  $K$ . So the primitive element theorem implies there exists  $z \in L$  such that  $K(z) = K(x, y) \supsetneq K(y)$ . So  $\deg_K(z) > \deg_K(y)$ , a contradiction.  $\square$

**Remark:** some approaches to Galois theory use this as a starting point.

**Example.** Let  $k$  be a field,  $L = k(X_1, \dots, X_n)$  the field of fractions of the polynomial ring  $k[X_1, \dots, X_n]$ . Let  $G = S_n$ , permuting the  $X_i$ . Then  $G \subseteq \text{Aut}(L)$ . Recall that  $k[X_1, \dots, X_n]^G = k[s_1, \dots, s_n]$  where  $s_1, \dots, s_n$  are the elementary symmetric polynomials. So  $k(s_1, \dots, s_n) \subseteq L^G$ .

**Theorem 18.2.**  $L^G = k(s_1, \dots, s_n)$  in the above example.

*Proof.* Let  $\frac{f}{g} \in L^G$ ,  $f, g \in k[X_1, \dots, X_n] := R$ . So for all  $\sigma \in G$ ,  $\frac{f}{g} = \frac{\sigma(f)}{\sigma(g)}$ .  $R$  is a UFD by Gauss' lemma, and the units in  $R$  are  $k^\times$ . So  $\sigma(f) = c_\sigma f$ ,  $\sigma(g) = c_\sigma g$  for some  $c_\sigma \in k^\times$ . As  $G$  is finite of order  $N = n!$ ,  $f = \sigma^N f = c_\sigma^N f$ , so  $c_\sigma^N = 1$ . But then  $fg^{N-1}$  or  $g^N$  are both in  $R^G = k[s_1, \dots, s_n]$ . So  $\frac{f}{g} = \frac{fg^{N-1}}{g^N} \in k(s_1, \dots, s_n)$ .  $\square$

Now let  $L = k(X_1, \dots, X_n)$ ,  $K = k(s_1, \dots, s_n) = L^G$  (with  $G = S_n$ ).  $L/K$  is a finite Galois extension with Galois group  $S_n$  by Artin's Theorem.

Let  $f = T^n - s_1 T^{n-1} + \dots + (-1)^n s_n \in K[T]$ . Then in  $L$ ,  $f = \prod (T - X_i)$  (by the definition of the elementary symmetric polynomials). So  $L/K$  is a splitting field for  $f$ . So  $\text{Gal}(f/K) = S_n$ , i.e. "the general polynomial of degree  $n$  has Galois group  $S_n$ ".

It is not hard to use this to find some Galois extension with Galois group  $G$  for every  $G$  (see Example sheet 4 Q11).

This is one of a number of theorems in "Invariant Theory". Take a ring  $R$ , group  $G \subseteq \text{Aut}(R)$ : what can we say about  $R^G$ ? When  $R = k[X_1, \dots, X_n]$ ,  $G \subseteq S_n$ ,

knowing  $R^G$  can help to compute Galois groups. For example, if  $G = A_n$

$$k[X_1, \dots, X_n]^{A_n} = k[s_1, \dots, s_n, \Delta]$$

(where  $\Delta = \prod_{i < j} (X_i - X_j)$  is the discriminant and when the characteristic is not 2)

**Example.**  $k[X_1, X_2]$ ,  $G = \{1, \sigma\}$ ,  $\sigma : X_1 \mapsto -X_2, X_2 \mapsto -X_1$  ( $\text{char}(k) \neq 2$ ). Then  $R^G = k[X_1^2, X_2^2, X_1 X_2] \cong k[Y_1, Y_2, Y_3]/(Y_1 Y_2 - Y_3^2)$ . Geometrically:  $\{Y_1 Y_2 = Y_3^2\} \subseteq \mathbb{R}^3$  is a double-cone.

If you fix  $K$  and  $G$ , it is not always the case that there exists a Galois extension  $L/K$  with  $\text{Gal}(L/K) = G$  (for example if  $K$  is algebraically closed,  $L = K$  so  $G = \{e\}$ ; or if  $K = \mathbb{F}_p$ ,  $G$  is always cyclic).

**Unsolved problem** (“Inverse Galois Problem”): is every finite  $G$  the Galois group of some  $L/\mathbb{Q}$ ? (See the extra Example sheet to see every abelian group is.)

Famous theorem by Shafarevich: every finite soluble group is a Galois group over  $\mathbb{Q}$ .

It is known for most finite simple groups. E.g the “monster group” is a Galois group over  $\mathbb{Q}$ .

A possibly better question: understand  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$  (then the inverse Galois problem is equivalent to saying every finite group is a quotient of this). What are the representations of  $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ ? This has connections with the Langlands program.