Galois Theory

Prof. A.J. Scholl

Michaelmas 2005

LaTeXed by Sebastian Pancratz

These notes are based on a course of lectures given by Prof. A.J. Scholl in Part II of the Mathematical Tripos at the University of Cambridge in the academic year 2005–2006.

These notes have not been checked by Prof. A.J. Scholl and should not be regarded as official notes for the course. In particular, the responsibility for any errors is mine — please email Sebastian Pancratz (`sfp25`) with any comments or corrections.

Contents

Chapter 1

Polynomials

Let R be any commutative ring with an identity element 1. The ring of polynomials is

$$R[X] = \left\{ \sum_{i=0}^{n} a_i X^i \colon n \in \mathbb{N} \wedge a_1, \ldots, a_n \in R \right\}.$$

More generally, $R[X_1, \ldots, X_n]$ is the ring of polynomials in several variables. It is important to distinguish between a polynomial and the function that it might represent. If $f(X) = \sum_{i=0}^{n} a_i X^i \in R[X]$ then it determines a function $R \to R, b \mapsto \sum_{i=0}^{n} a_i b^i = f(b)$. The function $b \mapsto f(b)$ does *not* in general determine $f(X)$ uniquely, e.g. if $R = \mathbb{F}_p = \frac{\mathbb{Z}}{p\mathbb{Z}}$, $f(X) = X^p$, $g(X) = X$ then by Fermat's Little Theorem $f(b) = g(b)$ for all $b \in \mathbb{F}_p$ but $f \neq g$.

Here, we are mostly interested in the case $R = K$, a field. Recall that $K[X]$ is a Euclidean domain, so if $f, g \in K[X]$ with $g \neq 0$ then there exist unique $q, r \in K[X]$ such that

(i) $f = qg + r$;
(ii) $\deg r < \deg g$.

A particular case is when $g = X - a$ is linear, then we get $f(X) = (X - a)q(X) + f(a)$, since r is constant as $\deg r < 1 = \deg(X - a)$. This is known as the remainder theorem.

As a consequence, $K[X]$ is a unique factorisation domain (UFD) and a principal ideal domain (PID), so that greatest common divisors exist, and if $f, g \in K[X]$ then $\gcd(f, g) = pf + qg$ for some $p, q \in K[X]$.

Proposition 1.1. Let K be a field, $0 \neq f \in K[X]$. Then f has at most $\deg f$ roots in K.

Proof. If f has no roots, there is nothing to prove. Otherwise, let $c \in K$ be a root. So $f(X) = (X - c)q(X)$ by the division algorithm, and $\deg q = \deg f - 1$. So if b is any root of f, then $(b - c)q(b) = 0$, so $c = b$ or b is a root of q (as K is a field). So

$$\begin{aligned} |\{\text{roots of } f\}| &\leq 1 + |\{\text{roots of } q\}| \\ &\leq 1 + \deg q \\ &= \deg f \end{aligned}$$

by induction on the degree of f. □

Remark. Consider $X^2 - 1 \in R[X]$, $R = \mathbb{Z}/8\mathbb{Z}$. This has four roots $\pm 1, \pm 3$, so the assumption R a field is essential.

Lecture 1

Chapter 2

Symmetric Polynomials

For $n \geq 1$ let S_n denote the symmetry group of degree n, i.e. the permutations of $\{1, \ldots, n\}$.

Definition. Let R be a ring, $X_1, \ldots, X_n$ be indeterminates. A polynomial $f(X_1, \ldots, X_n) \in R[X_1, \ldots, X_n]$ is *symmetric* if

$$\forall \sigma \in S_n \quad f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = f(X_1, \ldots, X_n).$$

If f, g are symmetric, clearly so are $f + g$ and fg. Also constant polynomials are symmetric. So the set of symmetric polynomials is a subring of $R[X_1, \ldots, X_n]$ containing R.

Example. Power sums $p_r = X_1^r + \cdots + X_n^r$ for any $r \geq 0$.

Another way of expressing the definition is as follows. The group S_n acts on $R[X_1, \ldots, X_n]$ by $\sigma \colon f \mapsto f(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) = f^\sigma$, say. This is a group action, $(f^\sigma)^\tau = f^{\sigma\tau}$. The ring of symmetric polynomials is just the set of elements of $R[X_1, \ldots, X_n]$ fixed by S_n, called invariants.

Elementary Symmetric Polynomials

Consider

$$\begin{aligned}\prod_{i=1}^{n}(T + X_i) &= (T + X_1)(T + X_2) \cdots (T + X_n) \\ &= T^n + (X_1 + \cdots + X_n)T^{n-1} + \cdots + X_1 \cdots X_n\end{aligned}$$

Define $s_r = s_{r,n}$ to be the coefficient of T^{n-r}. So

$$s_r = \sum_{1 \leq i_1 < \cdots < i_r \leq n} X_{i_1} \cdots X_{i_r}.$$

For example, if $n = 3$ then $s_1 = X_1 + X_2 + X_3$, $s_2 = X_1X_2 + X_1X_3 + X_2X_3$, $s_3 = X_1X_2X_3$. We always have $s_{0,n} = 1$ and by convention $s_{r,n} = 0$ if $r > n$.

Theorem 2.1 (Newton, Main Theorem of Symmetric Functions). (i) Every symmetric polynomial in $R[X_1, \ldots, X_n]$ is a polynomial in $\{s_{r,n}\}_{r=0}^n$ with coefficients in R.

(ii) There are no non-trivial relations between the elementary symmetric polynomials.

The meaning of (ii) is the following. Consider the map

$$\vartheta\colon R[Y_1,\dots,Y_n] \to R[X_1,\dots,X_n], G(Y_1,\dots,Y_n) \mapsto G(s_1,\dots,s_n).$$

This clearly is a homomorphism. (ii) means that $\ker\vartheta = \{0\}$, so ϑ defines an isomorphism between $R[Y_1,\dots,Y_n]$ and the ring of symmetric polynomials in $X_1,\dots,X_n$.

Proof. (i) If $I = (i_1,\dots,i_n)$ with $i_k \geq 0$ for all $k = 1,\dots,n$, write $X_I = X_1^{i_1}\cdots X_n^{i_n}$. Any polynomial of this form is called a *monomial*. The polynomials in $R[X_1,\dots,X_n]$ are just R-linear combinations of monomials. The *degree* of X_I is $i_1+\cdots+i_n$. A polynomial is said to be *homogenous* if all the monomials occurring in it (i.e. with non-zero coefficients) have the same degree. If $f \in R[X_1,\dots,X_n]$, we can uniquely write $f = f_0+f_1+\cdots+f_d$ for some d where each f_k is either 0 or is homogeneous of degree k. Permuting $\{X_1,\dots,X_n\}$ does not change the degree of the monomials, so if f is symmetric, so are the homogeneous parts $f_0, f_1, \dots, f_d$. So to prove (i), we may assume without loss of generality that f is homogeneous of degree d, say.

Define an ordering on the set of all monomials $\{X_I\}$ as follows. We say $X_I > X_J$ if either $i_1 > j_1$ or if for some $p > 1$, $i_1 = j_1, \dots, i_{p-1} = j_{p-1}$ and $i_p > j_p$. (This is called the *lexicographical ordering*.) This is a total ordering on $\{X_I\}$, i.e. for a pair I, J exactly one of $X_I > X_J, X_I < X_J, X_I = X_J$ holds.

Suppose f is homogeneous of degree d and symmetric. Consider the monomial X_I occurring in f which is greatest for lexicographical ordering, and let $c \in R$ be its coefficient. We claim that $i_1 \geq i_2 \geq \cdots \geq i_n$; if not, say $i_p < i_{p+1}$, then if we interchange X_p and X_{p+1} then the new monomial $X_{I'}$ has exponents $I' = (i_1,\dots,i_{p-1},i_{p+1},i_p,i_{p+2},\dots)$, so $X_{I'} > X_I$. So

$$X_I = X_1^{i_1-i_2}(X_1X_2)^{i_2-i_3}\cdots(X_1\cdots X_{n-1})^{i_{n-1}-i_n}(X_1\cdots X_n)^{i_n}.$$

Let $g = s_1^{i_1-i_2}s_2^{i_2-i_3}\cdots s_{n-1}^{i_{n-1}-i_n}s_n^{i_n}$, which is symmetric, homogeneous of degree d and its leading term (highest monomial) is X_I (since the highest monomial in s_r is just $X_1X_2\cdots X_r$).

Consider $h = f - cg$. If h is non-zero, then h is homogeneous of degree d, symmetric, and its highest monomial is less than X_I. As the number of monomials of given degree is finite, repeating this process ultimately terminates and we have expressed f as a polynomial in $\{s_r\}$.

(ii) Suppose $G \in R[Y_1,\dots,Y_n]$ such that $G(s_{1,n},\dots,s_{n,n}) = 0$. We want to show by induction on n that $G = 0$. If $n = 1$, there is nothing to prove.

If Y_n^k divides G for some $k > 0$ then $H = G/Y_n^k$ is also a relation ($H(s_{1,n},\dots,s_{n,n}) = 0$). So dividing by powers of Y_n, we may assume $Y_n \nmid G$. Now substitute $X_n = 0$ to get

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

and $G(s_{1,n-1},\dots,s_{n-1,n-1},0) = 0$. By induction, this means $G(Y_1,\dots,Y_{n-1},0) = 0$, in other words, $Y_n \mid G$. So there are no non-zero relations. □

Lecture 2

Example. Consider $\sum_{i\neq j} X_i^2 X_j$. The highest monomial occurring is $X_1^2 X_2 = X_1(X_1X_2)$. We have

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

So $\sum_{i\neq j} X_i^2 X_j = s_1 s_2 - 3s_3$.

Considering similarly $\sum_i X_i^5$ leads to Newton's identities.

Theorem 2.2 (Newton's Formula)**.** Let $n \geq 1$. Let $p_k = X_1^k + \cdots + X_n^k$. Then for all $k \geq 1$,

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

Note that $k = p_0$ and by convention $s_r = 0$ if $r > n$.

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

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

Comparing coefficients of T^k gives the identity

$$(-1)^{k-1} k s_k = \sum_{r=0}^{k-1} (-1)^r s_r p_{k-r}$$ □

Discriminant

Consider

$$\begin{aligned} \Delta(X_1, \ldots, X_n) &= \prod_{i<j} (X_i - X_j) \\ \Delta(X_{\sigma(1)}, \ldots, X_{\sigma(n)}) &= \operatorname{sgn}(\sigma) \Delta(X_1, \ldots, X_n) \end{aligned}$$

for all $\sigma \in S_n$, so

$$\Delta^2(X_1, \ldots, X_n) = \prod_{i<j} (X_i - X_j)^2$$

$$= (-1)^{n(n-1)/2} \prod_{i \neq j} (X_i - X_j)$$

is a symmetric polynomial.

Example. Let $n = 2$. Then

$$\begin{aligned} \Delta^2(X_1, X_2) &= (X_1 - X_2)^2 = (X_1 + X_2)^2 - 4X_1X_2 \\ &= s_1^2 - 4s_2. \end{aligned}$$

Let

$$\begin{aligned} f(T) &= \prod_{i=1}^{n} (T - \alpha_i) \\ &= T^n - c_1 T^{n-1} + \cdots + (-1)^n c_n \end{aligned}$$

where $c_r = s_r(\alpha_1, \ldots, \alpha_n)$. Then the discrimant of f

$$\begin{aligned} \mathrm{Disc}(f) &= \Delta^2(\alpha_1, \ldots, \alpha_n) \\ &= \prod_{i<j} (\alpha_i - \alpha_j)^2 \end{aligned}$$

is a polynomial in $\{c_i\}$ and vanishes if and only if f has a repeated root.

Example. If $n = 2$, $f(T) = T^2 + bT + c$ then $\mathrm{Disc}(f) = b^2 - 4c$. (Note that $\mathrm{Disc}(f) = s_1^2 - 4s_2$ as above. But then $s_1(\alpha_1, \alpha_2) = \alpha_1 + \alpha_2 = b$ and $s_2(\alpha_1, \alpha_2) = \alpha_1\alpha_2 = c$.)

Chapter 3

Fields and Extensions

Recall that a *field* is a commutative ring with an identity element 1, $1 \neq 0$, in which every non-zero element is invertible.

If K is a field then one of the followings holds.

- For every $n \in \mathbb{Z}$, $n \neq 0$, $n.1_K \neq 0_K$ where

$$n.1_K = \begin{cases} 1_K + \cdots + 1_K & n > 0 \\ -(-n).1_K & n < 0 \end{cases}$$

  In this case, we say K has characteristic 0.
- There exists $n \in \mathbb{Z}$, $n \neq 0$, with $n.1_K = 0_K$, Then because K has no zero-divisors, there exists a unique prime p such that $p.1_K = 0_K$. We say K has characteristic p.

In each case, K has a minimal subfield, called the *prime subfield* of K.

- If $\operatorname{char} K = 0$, this is

$$\left\{ \frac{m.1_K}{n.1_K} \mid n \neq 0 \right\} \cong \mathbb{Q}$$

- If $\operatorname{char} K = p > 0$, this is

$$\{m.1_K \mid 0 \leq m \leq p-1\} \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$$

Definition. Let $K \subset L$ be fields with the field operations in K being the same as those in L. We say L is an *extension* of K, written L/K.

Example. $\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ are extensions. Let K be any field; then the field $K(X)$ of rational functions $\left\{ \frac{f}{g} \colon f, g \in K[X], g \neq 0 \right\}$ is an extension of K.

Actually, in practice we use something more general. If $i \colon K \to L$ is a homomorphism of fields (which is necessarily injective since K has no proper ideals other than $\{0\}$), then we will also say that L is an extension of K, and even identify K with its image in L.

Example. Let $\mathbb{C} = \{(x, y) \colon x, y \in \mathbb{R}\}$ with suitable $+, \times$, let $i = (0, 1)$. Then $\mathbb{R} \cong \{(x, 0) \colon x \in \mathbb{R}\}$.

Let L/K be a field extension. Addition and multiplication in L by elements of K turn L into a vector space over K.

Definition. If L is finite-dimensional as a vector space over K, we say that L/K is a *finite extension* and set $[L : K] = \dim_K L$, called the *degree* of L/K. If not, we say L/K is an *infinite extension* and write $[L : K] = \infty$.

So if $[L : K] = n \in \mathbb{N}$ then $L \cong K^n$ as a K-vector space.

Example. (i) $\mathbb{C}/\mathbb{R}$ is a finite extension of degree 2 since $\{1, i\}$ is a basis for $\mathbb{C}$ over $\mathbb{R}$.
(ii) For any K, $[K(X) : K] = \infty$ because $1, X, X^2, \ldots$ are linearly independent over K.
(iii) $\mathbb{R}/\mathbb{Q}$ is an infinite extension. (This is left as an exercise.)

Remark. An extension of degree 2, (3, etc.) is called a quadratic, (cubic, etc.) extension.

Theorem 3.1. Let K be a finite field of characteristic $p > 0$. Then $|K| = p^n$ for some $n \geq 1$ with $n = [K : \mathbb{F}_p]$.

Proof. Let $n = [K : \mathbb{F}_p] = \dim_{\mathbb{F}_p} K$. This is finite since K is finite. Then $K \cong \mathbb{F}_p^n$ as $\mathbb{F}_p$-vector spaces, so $|K| = p^n$. □

Theorem 3.2. Let L/K be a finite extension of degree n, and V a vector space over L. Then $\dim_K V = n \dim_L V$, and V is finite dimensional over K if and only if it is finite-dimensional over L.

Proof. Suppose $\dim_L V = d < \infty$, so $V \cong L^d = L \oplus \cdots \oplus L$ as an L-vector space, hence also as a K-vector space. So $V \cong L^d \cong K^{nd}$ as K-vector spaces, so $\dim_K V = nd < \infty$. Conversely, if $\dim_K V < \infty$ then any K-basis for V span V over L, so $\dim_L V < \infty$. □

Corollary 3.3 (Tower Law)**.** Let $M/L/K$ be extensions. Then M/K is finite if and only if both M/L and L/K are finite, and if so, $[M : K] = [M : L][L : K]$.

Proof. If L/K is not finite, then M/K is certainly not finite as $L \subset M$. So suppose L/K is finite. Then by Theorem 3.2, M/L is finite if and only if M/K is finite, and if so $[M : K] = [M : L][L : K]$. □

Proposition 3.4. Let F be a field. $F^* = F \setminus \{0\}$ is the multiplicative group of its non-zero elements. Let $G \subset F^*$ be a finite subgroup. Then G is cyclic.

As a special case, if F is a finite field then F^* is cyclic.

Proof. G is a finite abelian group, so $G = C_1 \times \cdots \times C_k$ say, where each C_i is a cyclic subgroup of G, $|C_i| = d_i$ with $1 \neq d_1 \mid d_2 \mid \cdots \mid d_k$ and $|G| = n = \prod_{i=1}^k d_i$. G is cyclic if and only if $k = 1$. But if $k > 1$ then $d_k < n$, and for every $x \in G$, $x^{d_k} = 1$. So the polynomial $X^{d_k} - 1$ has at least n roots in F, contradicting that F is a field (see Proposition 1.1). □

Proposition 3.5. Let R be a ring of characteristic p, a prime, i.e. $p.1_R = 0_R$. Then the map $\phi_p \colon R \to R$ given by $\phi_p(x) = x^p$ is a ring homomorphism called the *Frobenius endomorphism* of R.

Lecture 4

Proof. We have to prove that $\phi_p(1) = 1$, $\phi_p(xy) = \phi_p(x)\phi_p(y)$ and $\phi_p(x+y) = \phi_p(x) + \phi_p(y)$. Only the last one of these is non-trivial. We have

$$\begin{aligned}\phi_p(x+y) &= (x+y)^p \\ &= x^p + \sum_{r=1}^{p-1} \binom{p}{r} x^r y^{p-r} + y^p \\ &= x^p + y^p \\ &= \phi_p(x) + \phi_p(y)\end{aligned}$$

since, if $1 \leq r < p$, $\binom{p}{r} \equiv 0 \pmod{p}$. □

Example. Fermat's Little Theorem states that for prime p,

$$\forall a \in \mathbb{Z} \quad a^p \equiv a \pmod{p}$$

It can be proved by induction on a since $(a+1)^p \equiv a^p + 1$ by the above.

Chapter 4

Algebraic Elements and Extensions

Let L/K be an extension of fields, $x \in L$. We define

$$K[x] = \left\{ \sum_{i=0}^{n} a_i x^i \colon n \geq 0 \wedge a_1, \ldots, a_n \in K \right\} \subset L,$$
$$K(x) = \left\{ \frac{y}{z} \colon y, z \in K[x] \wedge z \neq 0 \right\} \subset L.$$

Clearly $K[x]$ is a subring of L, and $K(x)$ is a subfield of L. Moreover, $K[x]$ is the smallest subring of L containing K and x, and $K(x)$ is the smallest subfield of L containing K and x. We say $K[x]$, $K(x)$ are obtained by *adjoining x to K*.

Example. Consider $\mathbb{C}/\mathbb{Q}$. $\mathbb{Q}[i] = \{a + bi \colon a, b \in \mathbb{Q}\}$ is already a field, so $\mathbb{Q}[i] = \mathbb{Q}(i)$ since

$$(a + bi)^{-1} = \frac{a}{a^2 + b^2} - \frac{b}{a^2 + b^2} i$$

if $a + bi \neq 0$.

Definition. We say x is *algebraic over K* if there exists a non-constant polynomial $f(X) \in K[X]$ such that $f(x) = 0$. If not, we say that x is *transcendental over K*.

Suppose x is algebraic over K. Choose a monic polynomial $m(X) \in K[X]$ of least degree such that $m(x) = 0$. Then $m(X)$ is irreducible: if $m = fg$ with $\deg f, \deg g < \deg m$ then one of $f(x)$ or $g(x)$ would be 0. Also, if $f(X) \in K[X]$ with $f(x) = 0$, then $m \mid f$, since by the Euclidean division algorithm, we can write $f(X) = q(X)m(X) + g(X)$ with $\deg g < \deg m$ and then $g(x) = 0$, so $g(X)$ must be the zero polynomial. In particular, $m(X)$ is unique, it is called the *minimal polynomial*.

Another way of seeing this is the following. The map

$$\begin{aligned} \vartheta_x \colon K[X] &\to L \\ f(X) &\mapsto f(x) \end{aligned}$$

is clearly a homomorphism. Then x is algebraic over K if and only if $\ker(\vartheta_x) \neq \{0\}$. If so, then $\ker(\vartheta_x)$ is a non-zero prime ideal of $K[X]$ (prime as the image is embedded in a field), so $\ker(\vartheta_x) = (m)$ for some irreducible polynomial $m(X) \in K[X]$, which is unique if required to be monic. It is then the minimal polynomial. Note also that the image of ϑ_x is just $K[x] \subset L$.

Theorem 4.1. Let L/K be an 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 they hold, then $[K(x) : K]$ equals the degree of the minimal polynomial of x over K, called the *degree of x over K* $\deg_K(x)$.

Proof. The proof proceeds as follows.

$$\text{degree formula} \Longleftarrow \text{(i)} \Longleftarrow \text{(iv)} \Longleftrightarrow \text{(v)}$$
$$\Downarrow \quad \nearrow$$
$$\text{(iii)} \Longleftrightarrow \text{(ii)}$$

[(ii) $\Longrightarrow$ (iii), (iv) $\Longleftrightarrow$ (v).] These are obvious.

[(iii) $\Longrightarrow$ (iv) and (ii).] Let $0 \neq g(X) \in K[x]$. Then multiplication by $g(x)$ is an injective linear map $K[x] \to K[x]$, so as $\dim_K K[x] < \infty$, it is surjective, so it is invertible, hence (iv) and (v), and clearly (iii) and (iv) $\Longrightarrow$ (ii).

[(iv) $\Longrightarrow$ (i).] If $x \neq 0$, write $x^{-1} = a_0 + a_1 x + \cdots + a_{n-1}x^{n-1} \in K[x] = K(x)$, hence $a_{n-1}x^n + \cdots + a_1 x^2 + a_0 x - 1 = 0$, so x is algebraic over K.

[(i) $\Longrightarrow$ (iii), degree formula] It is enough to show that if x is algebraic of degree n with minimal polynomial $m(X)$, then $1, x, \ldots, x^{n-1}$ is a basis for $K[x]$ as a K-vector space.

But $\{x^i : i \geq 0\}$ spans $K[x]$ over K and the relation $m(X) = 0$ shows that x^r is a linear combination of $1, x, \ldots, x^{r-1}$ for $r \geq n$. So $\{1, x, \ldots, x^{n-1}\}$ spans $K[x]$, and by definition of the minimal polynomial, it is a linear independent set as well. □

Example. Note that the minimal polynomial depends on the field K. As an example, let $L = \mathbb{C}$, $x = \sqrt{i} = \frac{\sqrt{2}}{2}(1 + i)$, and consider $K = \mathbb{Q}$ or $K = \mathbb{Q}[i]$. Over $\mathbb{Q}$, the minimal polynomial is X^4+1, which is irreducible over $\mathbb{Q}$. But over $\mathbb{Q}[i]$, $X^4+1 = (X^2+i)(X^2-i)$, and the minimal polynomial is $X^2 - i$.

Corollary 4.2. (i) Let L/K be a field extension, $x_1, \ldots, x_n \in L$. Then $K(x_1, \ldots, x_n)/K$ is a finite extension if and only if $x_1, \ldots, x_n$ are algebraic over K.

(ii) If $x, y \in L$ are algebraic over K, then $x \pm y$, xy and, if $x \neq 0$, x^{-1} are also algebraic over K.

Proof. (i) If $[K(x_1, \ldots, x_n) : K] < \infty$ then for all $i = 1, \ldots, n$, $[K(x_i) : K] < \infty$, so by Theorem 4.1 x_i is algebraic over K. Conversely, if x_n is algebraic over K then it is certainly algebraic over $K(x_1, \ldots, x_{n-1})$, so $[K(x_1, \ldots, x_n) : K(x_1, \ldots, x_{n-1})] < \infty$. By the induction hypothesis, $[K(x_1, \ldots, x_{n-1}) : K] < \infty$, so by the tower law, $[K(x_1, \ldots, x_n) : K] < \infty$.

(ii) x, y are algebraic, so by (i) $[K(x, y) : K] < \infty$. If z is $x \pm y$, xy, or x^{-1} then $z \in K(x, y)$, so $[K(z) : K] < \infty$ and so z is algebraic over K. □

Lecture 5

If we are not using (i) to prove (ii), we have polynomials $f(X), g(X)$ such that $f(x) = 0$, $g(y) = 0$, so do we have $h(X)$ such that $h(x + y) = 0$?

Example. Let $K = \mathbb{Q}, m, n \in \mathbb{Z}$. Let $x = \sqrt{m}, y = \sqrt{n}, f(X) = X^2 - m, g(X) = X^2 - n$; $z = x + y = \sqrt{m} + \sqrt{n}$. Then $z^2 = m + 2\sqrt{mn} + n$, so $(z^2 - m - n)^2 = 4mn$. Therefore, there is a quartic polynomial satisfied by $x + y$.

But if x is a root of $X^3 + X + 3$, y a root of $X^4 + 2X^3 + 2$, then it is not easy to compute $f(X)$ such that $f(x + y) = 0$.

Example. Let $a, b \in K$, $\alpha = \sqrt{a}$, $\beta = \sqrt{b}$. We try to find a polynomial with root $\gamma = \alpha + \beta$.

$$\begin{aligned}\gamma^2 &= (\alpha + \beta)^2 = a + b + 2\alpha\beta \\ \gamma^4 &= (a + b)^2 + 4\alpha\beta(a + b) + 4\alpha^2\beta^2 \\ &= (a^2 + 6ab + b^2) + 4(a + b)\alpha\beta\end{aligned}$$

Eliminating $\alpha\beta$, we obtain

$$\gamma^4 - 2(a + b)\gamma^2 = -(a - b)^2$$

i.e., γ is a root of $f(X) = X^4 - 2(a + b)X^2 + (a - b)^2$.

In general, if $\deg_K \alpha = m$, $\deg_K \beta = n$, the monomials $\alpha^i\beta^j$, $0 \le i < m, 0 \le j < n$ span $K[\alpha, \beta]$. So given any $\gamma \in K[\alpha, \beta]$, there is a linear combination of these, and so there must be a linear relation between $1, \gamma, \gamma^2, \ldots, \gamma^{mn}$, and this is our relation of algebraic dependence, although it is not necessarily the minimal one.

So far, we have shown that $[K(\gamma) : K] \mid 4$. The following is left as an exercise. Let $K = \mathbb{Q}$ and suppose m, n, mn are all non-squares. Then $[\mathbb{Q}(\sqrt{m} + \sqrt{n}) : \mathbb{Q}] = 4$.

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

Proposition 4.3. (i) Any finite extension is algebraic.

(ii) $K(x)/K$ is algebraic if and only if x is algebraic over K, so if and only if $K(x)/K$ is finite.

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

Proof. (i) Suppose L/K is finite, $x \in L$. Then $K(x)/K$ is finite, so x is algebraic over K. This holds for all $x \in L$, so L/K is algebraic.

(ii) Suppose $K(x)/K$ is algebraic. Then x is algebraic over K, so $K(x)/K$ is finite and by (i) $K(x)/K$ is algebraic.

(iii) Suppose M/K is algebraic. So every $x \in M$ is algebraic over K, hence L/K is algebraic. Also $x \in M$ will be algebraic over $L \supset K$, so M/L is algebraic. The converse follows from the following lemma. □

Lemma 4.4. Let $M/L/K$ be extensions of fields. Suppose L/K is algebraic, let $x \in M$. Then x is algebraic over L if and only if x is algebraic over K.

Proof. One direction is immediate from the definition. Conversely, suppose x is algebraic over L, so $f(x) = 0$ for some $f(X) = X^d + a_1X^{d-1} + \cdots + a_d \in L[X]$. Let

$L_0 = K(a_1, \ldots, a_d)$; as L/K is algebraic, $a_1, \ldots, a_d$ are algebraic over K, so by Corollary 4.2 (i), L_0/K is a finite extension. As $f \in L_0[X]$, x is algebraic over L_0, hence $[L_0(x) : L_0] < \infty$. So by the tower law $[L_0(x) : K] < \infty$ and so $[K(x) : K] < \infty$, i.e. x is algebraic over K. □

Example. Let $\bar{\mathbb{Q}} = \{x \in \mathbb{C} : x \text{ is algebraic over } \mathbb{Q}\}$. Then by Corollary 4.2 (ii), if $x, y \in \bar{\mathbb{Q}}$ then $x \pm y, xy, x^{-1} \in \bar{\mathbb{Q}}$, hence $\bar{\mathbb{Q}}$ is a subfield of $\mathbb{C}$ and so $\bar{\mathbb{Q}}$ is an algebraic extension of $\mathbb{Q}$. $\bar{\mathbb{Q}}$ is not a finite extension of $\mathbb{Q}$, e.g. $\bar{\mathbb{Q}} \supset \mathbb{Q}(\sqrt[n]{2})$ and as $X^n - 2$ is irreducible over $\mathbb{Q}$, it is the minimal polynomial of $\sqrt[n]{2}$. So $[\mathbb{Q}(\sqrt[n]{2}) : \mathbb{Q}] = n$. As this holds for any $n \in \mathbb{N}$, $[\bar{\mathbb{Q}} : \mathbb{Q}] = \infty$.

Example. Let $L = \mathbb{Q}(\sqrt[3]{2}, \sqrt[4]{5})$. We claim that $[L : \mathbb{Q}] = 12$. Note $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ as $X^3 - 2$ is irreducible. By the tower law, $3 \mid [L : \mathbb{Q}]$. Also, $[\mathbb{Q}(\sqrt[4]{5}) : \mathbb{Q}] = 4$ as $X^4 - 5$ is irreducible, so $4 \mid [L : \mathbb{Q}]$. Hence $12 \mid [L : \mathbb{Q}]$.

Note $X^4 - 5$ is the minimal polynomial for $\sqrt[4]{5}$ over $\mathbb{Q}$, so some factor of it is a minimal polynomial for $\sqrt[4]{5}$ over $\mathbb{Q}(\sqrt[3]{2})$, i.e. $[L : \mathbb{Q}] \mid 12$.

Example. Let $\alpha = e^{2\pi i/p} + e^{-2\pi i/p}$, where p is an odd prime. We find $\deg_{\mathbb{Q}} \alpha$. Write $\omega = e^{2\pi i/p}$, so $\omega^p = 1$ and ω is a root of

$$\frac{X^p - 1}{X - 1} = 1 + X + \cdots + X^{p-1} = f(X)$$

Note $f(X)$ is irreducible over $\mathbb{Q}$. So $[\mathbb{Q}(\omega) : \mathbb{Q}] = p - 1$. Now $\alpha \in \mathbb{Q}(\omega)$, $\alpha = \omega + \omega^{-1}$. Hence $\mathbb{Q} \subset \mathbb{Q}(\alpha) \subset \mathbb{Q}(\omega)$, so the tower law implies $\deg_{\mathbb{Q}} \alpha \mid p - 1$.

We also have $\alpha\omega = \omega^2 + 1$, i.e. ω is a root of $X^2 - \alpha X + 1$ in $\mathbb{Q}(\alpha)[X]$ of degree 2. But $\omega \notin \mathbb{Q}(\alpha)$ as $\mathbb{Q}(\alpha) \subset \mathbb{R}$. So this polynomial is a polynomial for ω over $\mathbb{Q}(\alpha)$, i.e. $[\mathbb{Q}(\omega) : \mathbb{Q}(\alpha)] = 2$. The tower law gives $[\mathbb{Q}(\alpha) : \mathbb{Q}] = (p - 1)/2$.

Chapter 5

Algebraic and Transcendental Numbers in $\mathbb{R}$ and $\mathbb{C}$

Classically, $x \in \mathbb{R}$ or $x \in \mathbb{C}$ is *algebraic* if it is algebraic over $\mathbb{Q}$ and *transcendental* if it is transcendental over $\mathbb{Q}$.

In a certain sense, most numbers are transcendental. Suppose x is algebraic, so $f(x) = 0$ for some $f(X) = c_d X^d + c_{d-1} X^{d-1} + \cdots + c_0$ with $c_0, \ldots, c_d \in \mathbb{Z}$, $c_d > 0$, $\gcd(c_0, \ldots, c_d) = 1$ and $f(X)$ an irreducible polynomial. These conditions determine $f(X)$ uniquely. We can then define the *height* of x as

$$H(x) = d + |c_0| + \cdots + |c_d| \in \mathbb{N}$$

For given $C \in \mathbb{N}$, the set of polynomials $f(X)$ as above with $d + \sum_{i=0}^{d} |c_i| \leq C$ is finite, hence there exists only finitely many $x \in \bar{\mathbb{Q}}$ with $H(x) \leq C$. So $\bar{\mathbb{Q}}$ is countable and the set of transcendental numbers is uncountable.

Exhibiting transcendental numbers is non-trivial. We will see that

$$\sum_{n=1}^{\infty} \frac{1}{2^{2^{n^2}}}$$

is transcendental. Showing that a particular number, e.g. π, is transcendental is harder.

History

In the 19th century, it was proved by Hermite and Lindemann that e and π are transcendental. In the 20th century Gelfond and Schneider showed that x^y is transcendental if x, y are algebraic, $x \neq 0$ and $y \notin \mathbb{Q}$. In particular, $e^\pi = (-1)^{-i}$ is transcendental. Alan Baker (1967) showed that $x_1^{y_1} \cdots x_m^{y_m}$ is transcendental if x_i, y_i are algebraic, $x_i \neq 0$ and $1, y_1, \ldots, y_m$ are linearly independent over $\mathbb{Q}$. It is not known whether π^e is transcendental, though.

Example

Proposition 5.1. The number

$$x = \sum_{n=1}^{\infty} \frac{1}{2^{2^{n^2}}}$$

is transcendental.

Proof. Write $k(n) = 2^{n^2}$. Supopse $f(X) = \mathbb{Z}[X]$ is a polynomial of degree $d > 0$ such that $f(x) = 0$. We will obtain a contradiction. Let $x_n = \sum_{m=1}^{n} \frac{1}{2^{k(m)}}$. Then

$$|x - x_n| = \sum_{m=n+1}^{\infty} \frac{1}{2^{k(m)}} \leq \sum_{j=0}^{\infty} \frac{1}{2^{k(n+1)+j}} = \frac{2}{2^{k(n+1)}}$$

Consider $f(x_n)$. For all but a finite number of values of n, $f(x_n) \neq 0$ since $f(X)$ is a polynomial. But $f(x_n)$ is rational, and as the denominator of x_n is $2^{k(n)}$, the denominator of $f(x_n)$ is at most $2^{dk(n)}$. Therefore, for all sufficiently large n, $|f(x_n)| \geq \frac{1}{2^{dk(n)}}$.

Since $f(x) = 0$, we can write $f(X) = (X - x)g(X)$, for some $g(X) \in \mathbb{R}[X]$, so

$$\begin{aligned} |g(x_n)| &= \frac{|f(x_n)|}{|x_n - x|} \\ &\geq \frac{1}{2^{dk(n)}} \frac{2^{k(n+1)}}{2} \\ &= 2^{k(n+1)-dk(n)-1} \end{aligned}$$

and

$$k(n+1) - dk(n) = 2^{(n+1)^2} - d2^{n^2} = 2^{n^2}(2^{2n+1} - d) \to \infty \text{ as } n \to \infty$$

i.e. $|g(x_n)| \to \infty$ as $n \to \infty$, contradicting

$$\lim_{n\to\infty} g(x_n) = g\left(\lim_{n\to\infty} x_n\right) = g(x) \neq \infty \qquad \square$$

Remark. From the proof, we see that this works for a wide range of functions $k(n)$. In fact, all we need is $k(n+1) - dk(n) \to \infty$ as $n \to \infty$, e.g. $k(n) = n!$ will also work as $(n+1)! - dn! = (n+1-d)n!$, so $\sum_{n=1}^{\infty} \frac{1}{2^{n!}}$ is transcendental too.

Ruler and Compass Constructions

In this section we consider the following three classical problems:

- trisecting the angle,
- duplicating the cube, and
- squaring the circle

using only a ruler, i.e. a straight edge, and a compass.

We first define the notion of a ruler and compass construction. Assume a finite set of points $(x_1, y_1), \ldots, (x_m, y_m) \in \mathbb{R}^2$ is given. The following constructions are permitted.

(A) From P_1, P_2, Q_1, Q_2 with $P_i \neq Q_i$ we can construct the point of intersection of lines P_1Q_1 and P_2Q_2, if they are not parallel.

(B) From P_1, P_2, Q_1, Q_2 with $P_i \neq Q_i$ we may construct the one or two points of intersection of the circles with centres P_i passing through Q_i, assuming they intersect and $P_1 \neq P_2$.

(C) From P_1, P_2, Q_1, Q_2 with $P_i \neq Q_i$ we can construct the one or two points of intersection of the line P_1Q_1 and the circle with centre P_2 passing through Q_2.

Remark. The construction (C) to construct the intersection of a line and a circle can be reduced to a sequence of constructions of the type (A) and (B). (This is left as an exercise.)

Lecture 6

Example. (i) We can draw a line perpendicular to a constructed line $\ell = QR$ and through a construced point P.
First consider the case $P \in \ell$. The following sequence of constructions yields the desired line.
(a) Construct $\mathrm{circ}(P, Q)$;
(b) construct $\mathrm{circ}(Q, Q')$;
(c) construct $\mathrm{circ}(Q', Q)$;
(d) construct the two points of intersection S, T of the previous two circles. The line ST is the desired line.
Now consider the case $p \notin \ell$. We construct the line as follows.
(a) Construct $\mathrm{circ}(P, Q)$, let Q' denote the intersection of ℓ and this circle;
(b) construct $\mathrm{circ}(Q, P)$;
(c) construct $\mathrm{circ}(Q', P)$; let S denote the intersection of the previous two circles. The line PS is the desired line.

(ii) Given a line ℓ, we can draw a line parallel two ℓ through a constructed point P.
(a) Construct the line perpendicular to ℓ through P, denote this by ℓ';
(b) construct the line perpendicular to ℓ' through P. This is the desired line.

(iii) We can mark off a given length defined by two points R, S on a constructed line $\ell = PQ$, starting at P.
(a) Construct the line parallel to ℓ through R, denote this by ℓ';
(b) construct $\mathrm{circ}(R, S)$, denote the intersection with ℓ' by T;
(c) construct the line PR;
(d) construct the line parallel to PR through T, let P' denote the intersection of this line with ℓ. Then the line segment PP' has the same length as the segment RS.

As a consequence of the constructions described above, we can set up cartesian coordinates given initial points $(0, 0), (0, 1)$.

Definition. We say that the point $(x, y) \in \mathbb{R}^2$ is *constructible from* $(x_1, y_1), \ldots, (x_m, y_m)$ if it can be obtained from them by a finite sequence of constructions of types (A) and (B). We say $x \in \mathbb{R}$ is *constructible* if $(x, 0)$ is constructible from $(0, 0)$ and $(1, 0)$.

Proposition 5.2. $P = (a, b) \in \mathbb{R}^2$ is constructible if and only if $a, b \in \mathbb{R}$ are constructible.

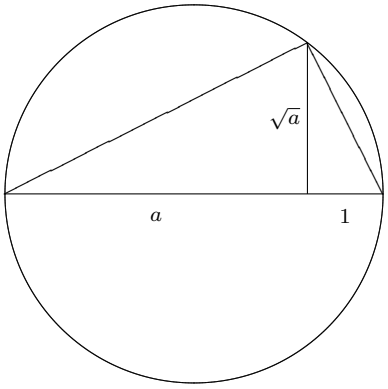
Proof. Given P, we get its coordinates by dropping perpendiculars to the axis. Conversely, given a, b, we first mark off the distance a along the x-axis and b along the y-axis. Next we construct the perpendicular to the x-axis through $(a, 0)$ and likewise the perpendicular to the y-axis through $(0, b)$. Their intersection is the desired point (a, b). □

Proposition 5.3. The set of constructible numbers forms a subfield of $\mathbb{R}$.

Proof. If a, b are constructible, we have to show that $a+b$, ab, $-a$ and $\frac{1}{a}$ are constructible. Note that $a + b$ and $-a$ are obvious from the third example given above. To show it is closed under multiplication and division, we construct similar right-angled triangles. Given one of the triangles and a side of the other, we construct the other triangle by drawing parallel lines. If r, s and r', s' are the lengths of the catheti, then similarity implies $\frac{r}{s} = \frac{r'}{s'}$. □

Proposition 5.4. If $a > 0$ is constructible then so is $\sqrt{a}$.

Proof. Draw a circle of radius $\frac{a+1}{2}$ as shown in the following figure.



Then the line segment perpendicular to the hypotenuse has length $\sqrt{a}$. □

Definition. Let K be a subfield of $\mathbb{R}$. We say K is *constructible* is there exists $n \geq 0$ and a chain of subfields of $\mathbb{R}$ such that

$$\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_n \subset \mathbb{R}$$

and elements $a_i \in F_i$, $1 \leq i \leq n$, such that

(i) $K \subset F_n$;
(ii) $F_i = F_{i-1}(a_i)$;
(iii) $a_i^2 \in F_{i-1}$.

Remark. Note that (ii) and (iii) imply that $[F_i : F_{i-1}] \in \{1, 2\}$. Conversely, if $[F_i : F_{i-1}] = 2$ then $F_i = F_{i-1}(\sqrt{b})$ for some $b \in F_i$, see Example Sheet 1.

So by the tower law, if K is constructible then $K/\mathbb{Q}$ is finite and $[K : \mathbb{Q}]$ is a power of 2.

Theorem 5.5. If $x \in \mathbb{R}$ is constructible, then $\mathbb{Q}(x)$ is constructible.

In fact, the converse is also true. It is sufficient to show that using ruler and compass, we can construct $x \pm y$, xy, $\frac{x}{y}$ and $\sqrt{x}$ from x, y.

Proof. We will prove by induction on k that if (x, y) can be constructed in at most k steps from $(0, 0), (0, 1)$ then $\mathbb{Q}(x, y)$ is constructible.

Assume there exists a sequence of fields $\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_n \subset \mathbb{R}$ satisfying (ii) and (iii) and such that the coordinates of all points obtained from $(0, 0), (0, 1)$ after k constructions lie in F_n.

Elementary coordinate geometry implies that in constructions of type (A), coordinates of the new point are rational expressions of the coordinates of the four starting points, with rational coefficients. So (x, y) is constructible in $k + 1$ steps and the last construction is of type (A), then already $x, y \in F_n$.

After constructions of type (B), the coordinates of the new point are of the form $x = a \pm b\sqrt{e}$, $y = c \pm d\sqrt{e}$, where a, b, c, d, e are rational functions of coordinates of the four starting points. So $x, y \in F_n(\sqrt{e})$.

By induction, the desired result follows. □

Lecture 6

Corollary 5.6. If $x \in \mathbb{R}$ is constructible then x is algebraic and its degree over $\mathbb{Q}$ is a power of 2.

We now return to the three classical problems mentioned earlier.

Duplicating the Cube

One would like to construct a cube whose volume is twice the volume of a given cube. This is equivalent to the constructibility of $\sqrt[3]{2}$. As $\deg_{\mathbb{Q}} \sqrt[3]{2} = 3$ is not a power of 2, this is impossible.

Squaring the Circle

This means constructing a square with area the same as the area of a circle of radius 1. This is equivalent to the constructibility of $\sqrt{\pi}$. As π is transcendental, so is $\sqrt{\pi}$ and hence it is not constructible.

Trisecting the Angle

To show this is impossible in general, it is enough to show one cannot trisect a particular constructed angle using ruler and compass. We will show this for the angle $2\pi/3$.

Since we can construct the angle $2\pi/3$ easily by an equilateral triangle, this is reduced to showing that the angle $2\pi/9$ can not be constructed, i.e., that the numbers $\cos 2\pi/9$, $\sin 2\pi/9$ are not constructible.

From $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$ we find that $\cos 2\pi/9$ is a root of $8X^3 - 6X + 1$ and $2(\cos 2\pi/9 - 1)$ is a root of $X^3 + 6X^2 + 9X + 3$, which is irreducible. Now $[\mathbb{Q}(\cos 2\pi/9) : \mathbb{Q}] = 3$ is not a power of 2, so the number is not constructible.

Proposition 5.7. A regular p-gon, where p is prime, is not constructible by ruler and compass if $p - 1$ is not a power of 2.

Proof. Constructing a regular p-gon is equivalent to constructing the angle $2\pi/p$, which is equivalent to constructing $\cos 2\pi/p$. But in an earlier example, we showed $\deg_{\mathbb{Q}} 2\pi/p = (p-1)/2$. □

Indeed, Gauss showed that a regular n-gon is constructible if and only if $n = 2^{\alpha} p_1 \cdots p_l$ for $p_1, \ldots, p_l$ distinct primes of the form $2^{2^k} + 1$.

Chapter 6

Splitting Fields

Basic Construction

Let $f(X) \in K[X]$ be an irreducible polynomial of degree d. Then there exists an extension L/K of degree d in which $f(X)$ has a root, constructed as follows. Consider the ideal $(f) \subset K[X]$ which is maximal since $f(X)$ is irreducible. Therefore,

$$L_f = K[X]/(f)$$

is a field, and the inclusion $K \subset K[X]$ gives a field homomorphism $K \hookrightarrow L_f$. Let $x = X + (f) \in L_f$. Then $f(x) = f(X) + (f) = 0$ in L_f. So x is a root of f in L_f. We say L_f is obtained from K by adjoining a root of f.

Recall that a field homomorphism is necessarily injective. We call a field homomorphism an *embedding* of fields.

Definition. (i) Let $L/K, M/K$ be extensions of fields. A homomorphism $L \to M$ which is the identity map on K is called a *K-homomorphism* or *K-embedding*.

(ii) Let L/K and L'/K' be extensions of fields. Suppose $\sigma\colon K \hookrightarrow K'$ is an embedding. A homomorphism $\sigma'\colon L \to L'$ such that

$$\forall x \in K \quad \sigma'(x) = \sigma(x)$$

is called a *σ-embedding* of L into L', or we say *σ' extends σ*, and that σ is the *restriction* of σ' to K, written $\sigma = \sigma'|_K$.

Theorem 6.1. Let L/K be an extension of fields, and $f(X) \in K[X]$ irreducible. Then

(i) If $x \in L$ is a root of $f(X)$, there exists a unique K-embedding

$$\sigma\colon L_f = K[X]/(f) \to L$$

sending $X + (f)$ to x.

(ii) Every K-embedding $L_f \hookrightarrow L$ arises in this way. In particular, the number of such σ equals the number of distinct roots of $f(X)$ in L, hence is at most $\deg f$.

Proof. By the First Isomorphism Theorem, to give a K-homomorphism $\sigma\colon L_f \to L$ is equivalent to giving a homomorphism of rings $\phi\colon K[X] \to L$ such that $\phi(a) = a$ for all

$a \in K$ and $\phi(f) = 0$, i.e. $\ker \phi = (f)$.

$$\begin{array}{ccc} L_f = K[X]/(f) & \xrightarrow{\sigma} & L \\ \pi \uparrow & \nearrow_{\phi=\sigma\pi} & \\ K[X] & & \end{array}$$

Such a ϕ is uniquely determined by $\phi(X)$ since

$$\phi\left(\sum a_i X^i\right) = \sum \phi(a_i)\phi(X)^i = \sum a_i \phi(X)^i$$

if $a_i \in K$, and the condition $\phi(f) = 0$ is equivalent to $f(\phi(X)) = 0$. So we have a bijection

$$\left\{\begin{array}{c}\phi\colon K[X] \to L \\ \text{s.t. } \phi(f) = 0\end{array}\right\} \xrightarrow{\sim} \left\{\begin{array}{c}\text{roots of} \\ f(X) \text{ in } L\end{array}\right\}$$

$$\phi \longmapsto \phi(X)$$

from which everything else follows. □

Corollary 6.2. If $L = K(x)$ is a finite extension of K and $f(X)$ is the minimal polynomial of x over K, then there exists a unique K-isomorphism $\sigma\colon L_f \xrightarrow{\sim} L$ sending $X + (f)$ to x.

Proof. By Theorem 6.1 (i), there exists a unique K-homomorphism σ. But as $[L_f : K] = [L : K] = \deg f$, σ is an isomorphism. □

Corollary 6.3. Let x, y be algebraic over K. Then x, y have the same minimal polynomial over K if and only if there exists a K-isomorphism $\sigma\colon K(x) \xrightarrow{\sim} K(y)$ sending x to y. (We say x, y are *K-conjugate* if they have the same minimal polynomial.)

Proof. If there exists such σ then

$$\{f(X) \in K[X]\colon f(x) = 0\} = \{f(X) \in K[X]\colon f(y) = 0\}$$

so they have the same minimal polynomial. Conversely, if $f(X)$ is the minimal polynomial of both x, y then

$$\begin{array}{ccccc} K(y) & \xleftarrow{\sim} & L_f = K[X]/(f) & \xrightarrow{\sim} & K(x) \\ y & \longleftarrow\!\shortmid & X + (f) & \longmapsto & x \end{array}$$

giving the required σ. □

Example. (i) $x = i$, $y = -i$ have minimal polynomial $X^2 + 1$ over $\mathbb{Q}$. By Corollary 6.3, there exists a unique isomorphism $\sigma\colon \mathbb{Q}(-i) \xrightarrow{\sim} \mathbb{Q}(i)$ such that $\sigma(i) = -i$. Here σ is complex conjugation.

(ii) Let $x = \sqrt[3]{2}$, $y = e^{2\pi i/3}\sqrt[3]{2}$. The minimal polynomial is $X^3 - 2$, so x, y are conjugate over $\mathbb{Q}$ and there exists an isomorphism $\mathbb{Q}(\sqrt[3]{2}) \xrightarrow{\sim} \mathbb{Q}(e^{2\pi i/3}\sqrt[3]{2})$ sending $\sqrt[3]{2}$ to $e^{2\pi i/3}\sqrt[3]{2}$.

The following theorem is a variant of Theorem 6.1.

Lecture 8

Theorem 6.4. Let $f(X) \in K[X]$ be irreducible, and $\sigma\colon K \to L$ be any embedding. Let $\sigma f \in L[X]$ be the polynomial obtained by applying σ to the coefficients of f.

(i) If $x \in L$ is a root of σf, there is a unique σ-embedding $\bar{\sigma}\colon L_f = K[X]/(f) \hookrightarrow L$ such that $\bar{\sigma}\colon X + (f) \mapsto x$.
(ii) Every σ-embedding $\bar{\sigma}\colon L_f \to L$ is obtained in this way. In particular, the number of such $\bar{\sigma}$ equals the number of distinct roots of σf in L.

Proof. This is analogous to the proof of Theorem 6.1. □

Definition. Let K be a field, $f(X) \in K[X]$. An extension L/K is a *splitting field* for $f(X)$ if

(i) $f(X)$ splits into linear factors in $L[X]$.
(ii) If $x_1, \ldots, x_n \in L$ are the roots of $f(X)$ in L then $L = K(x_1, \ldots, x_n)$.

Remark. (ii) is equivalent to saying that $f(X)$ does not split into linear factors over any smaller extension.

Example. Let $K = \mathbb{Q}$.

(i) If $f(X) = X^2 + 1$, then $f(X) = (X + i)(X - i)$, so $\mathbb{Q}(i)/\mathbb{Q}$ is a splitting field for $f(X)$. Note that $\mathbb{Q}(i)$ is obtained by adjoining just one root of $f(X)$.
(ii) If $f(X) = X^3 - 2$ then $L = \mathbb{Q}\left(\sqrt[3]{2}, e^{2\pi i/3}\right)$ is a splitting field for $f(X)$ over $\mathbb{Q}$. We have $[\mathbb{Q}(\sqrt[3]{2} : \mathbb{Q}] = 3$. As $\omega = e^{2\pi i/3} \notin \mathbb{Q}(\sqrt[3]{2}) \subset \mathbb{R}$ and $\omega^2 + \omega + 1 = 0$, we have $[L : \mathbb{Q}(\sqrt[3]{2})] = 2$. So $[L : \mathbb{Q}] = 6$. In particular, L is not obtained by adjoining just one root of $f(X)$ since that gives an extension of degree 3.
(iii) Let $f(X) = (X^5 - 1)/(X - 1) = X^4 + X^3 + X^2 + X + 1$. Then

$$f(Y + 1) = \frac{(Y + 1)^5 - 1}{Y} = Y^4 + 5Y^3 + 10Y^2 + 10Y + 5$$

is irreducible by Eisenstein's criterion. $\zeta = e^{2\pi i/5}$ is a root of $f(X)$, and the other roots of $f(X)$ in $\mathbb{C}$ are $\zeta^2, \zeta^3, \zeta^4$. So $L = \mathbb{Q}(\zeta)$ is a splitting field for $f(X)$ over $\mathbb{Q}$.

Theorem 6.5 (Existence of Splitting Fields)**.** Let $f(X) \in K[X]$. Then there exists a splitting field for $f(X)$ over K.

Proof. We prove this by induction, adjoining roots of $f(X)$ to K one by one.

Let $d \geq 1$ and assume that over *any* field, every polynomial of degree at most d has a splitting field. This is clearly true for $d = 1$. Let $\deg f = d + 1$, and let $g(X)$ be any irreducible factor of $f(X)$ with $\deg g \geq 1$. Let $K_1 = K[X]/(g)$, and $x_1 = X + (g) \in K_1$. Then $g(x_1) = 0$, so $f(x_1) = 0$, hence $f(X) = (X - x_1)f_1(X)$, say, with $\deg f_1 = d$, $f_1 \in K_1[X]$. By induction, $f_1(X)$ has a splitting field over K_1, call it $L = K_1(x_2, \ldots, x_n)$ where $x_2, \ldots, x_n$ are the roots of $f_1(X)$ in L. Then $f(X)$ also splits into linear factors in $L[X]$ and $L = K(x_1, x_2, \ldots, x_n)$, and $x_1, x_2, \ldots, x_n$ are the roots of $f(X)$ in L. So L is a splitting field for $f(X)$ over K. □

Remark. If $K \subset \mathbb{C}$ this just follows from the Fundamental Theorem of Algebra.

Theorem 6.6 (Uniqueness of Splitting Fields)**.** Let $f(X) \in K[X]$, let L/K be a splitting field for $f(X)$. Let $\sigma\colon K \hookrightarrow M$ be any embedding such that σf splits into linear factors in $M[X]$. Then the following hold.

(i) There exists at least one embedding $\bar{\sigma}\colon L \hookrightarrow M$ extending σ.
(ii) The number of $\bar{\sigma}$ as in (i) is at most $[L : K]$ with equality holding if $f(X)$ has no repeated roots in L, i.e., if it splits into distinct linear factors.
(iii) If M is a splitting field for σf over $\sigma(K)$, then any $\bar{\sigma}$ as in (i) is an isomorphism. In particular, any two splitting fields for $f(X)$ over K are isomorphic.

Proof. We proceed by induction on $n = [L : K]$. If $n = 1$ then $f(X)$ is a product of linear factors over K, and (i)–(iii) hold trivially. So assume $n > 1$, so $L \neq K$. Let $x_1, \ldots, x_m$ be the distinct roots of $f(X)$ in L; then at least one of them, say x_1, is not in K. Let $K_1 = K(x_1)$, $d = \deg_K(x_1) = [K_1 : K] > 1$. The minimal polynomial $g(X)$ of x_1 over K is an irreducible factor of $f(X)$, so if $f(X)$ has no repeated roots in L, neither does $g(X)$. By Theorem 6.4, $\sigma\colon K \hookrightarrow M$ extends to an embedding $\sigma_1\colon K_1 \hookrightarrow M$, and the number of such σ_1 is at most d, with equality if and only if $g(X)$ has no repeated roots. By induction, σ_1 extends to at least one and at most $[L : K_1]$ embeddings $\bar{\sigma}_1\colon L \hookrightarrow M$. This proves (i).

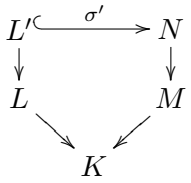
Since $[L : K_1][K_1 : K] = [L : K]$ we obtain the first part of (ii). If $f(X)$ has no repeated roots in L, then each σ_1 extends to $[L : K_1]$ embeddings $\bar{\sigma}$ by induction, giving $[L : K_1]d = [L : K]$ embeddings in all.

Finally, pick any $\bar{\sigma}\colon L \hookrightarrow M$ as in (i). Then the roots of σf in M are just $\{\sigma(x_i)\}$, so if M is a splitting field for σf over $\sigma(K)$, we have $M = \sigma(K)(\bar{\sigma}(x_1), \ldots, \bar{\sigma}(x_m)) = \bar{\sigma}(L)$, i.e., $\bar{\sigma}$ is an isomorphism. □

Corollary 6.7. Let K be a field and $L/K, M/K$ be finite extensions. Then there exists a finite extension N/M and a K-embedding $\sigma\colon L \hookrightarrow N$.

Loosely speaking, any two finite extensions of K are contained in a bigger one.

Proof. Let $L = K(x_1, \ldots, x_n)$ for some finite subset $\{x_1, \ldots, x_n\} \subset L$. Let $f(X) \in K[X]$ be the product of the minimal polynomials of $x_1, \ldots, x_n$. Let L' be a splitting field for $f(X)$ over L, and let N be a splitting field for $f(X)$ over M.



Then L' is also a splitting field for $f(X)$ over K since $L = K(x_1, \ldots, x_n)$, where $x_1, \ldots, x_n$ are among the roots of $f(X)$. As $f(X)$ splits into linear factors in $N[X]$, by Theorem 6.6, there exists a K-embedding $\sigma'\colon L' \hookrightarrow N$. Comparing with the inclusion $L \hookrightarrow L'$ gives σ. □

Remark. The field L' constructed in the proof is called the *normal closure* of L/K.

Chapter 7

Separability

Over $\mathbb{R}$, or $\mathbb{C}$, a polynomial $f(X)$ has a repeated roots at $X = a$ if and only if $f(a) = f'(a) = 0$. The same is true over *any* field if we replace calculus by algebra.

Definition. Let R be a ring, $f(X) \in R[X]$ be a polynomial, $f(X) = \sum_{i=0}^{d} a_i X^i$. Its *formal derivative* is the polynomial $f'(X) = \sum_{i=0}^{d} i a_i X^{i-1}$.

Exercise 1. Check that $(f+g)' = f' + g'$, $(fg)' = fg' + f'g$, $(f^n)' = nf'f^{n-1}$.

Proposition 7.1. Let $f(X) \in K[X]$, L/K an extension of fields, $x \in L$ a root of $f(X)$. Then x is a *simple root* of $f(X)$, i.e. $(X-x)^2 \nmid f(X)$, if and only if $f'(x) \neq 0$.

Proof. Write $f(X) = (X-x)g(X)$ where $g(X) \in L[X]$. Then x is a simple root of $f(X)$ if and only if $g(x) \neq 0$. But $f'(X) = g(X) + (X-x)g'(X)$, so $f'(x) = g(x)$. □

Example. Let K be a field of characteristic $p > 0$. Let $b \in K$, and assume that b is *not* a pth power in K.

Consider $f(X) = X^p - b \in K[X]$, let L/K be a splitting field for $f(X)$, and let $a \in L$ be a root of $f(X)$ in L. Note $f'(X) = pX^{p-1} = 0$, so $X = a$ is a multiple root. In fact, since $a^p = b$, in $L[X]$ we have $f(X) = X^p - a^p = (X-a)^p$, so $X = a$ is the only root of $f(X)$. Finally, $f(X)$ is irreducible over K. If not, write $f(X) = g(X)h(X)$ with $g(X), h(X) \in K[X]$ monic and then in $L[X]$, $g(X) = (X-a)^m$ for some $0 < m < p$, so $g(X) = X^m - maX^{m-1} + \cdots \in K[X]$. Hence $ma \in K$, so since $m \not\equiv 0 \pmod{p}$, this implies $a \in K$, i.e. b is a pth power. Contradiction.

Example. As an example of a pair (K, b), take $K = \mathbb{F}_p(X)$ and $b = X$.

Definition. A polynomial $f(X)$ is *separable* if it splits into distinct linear factors over a splitting field. If not, we say $f(X)$ is *inseparable*.

Corollary 7.2. $f(X)$ is separable if and only if $\gcd(f(X), f'(X)) = 1$.

Proof. $f(X)$ is separable if and only if $f(X), f'(X)$ have no common zeros. □

Remark. If $f, g \in K[X]$, $\gcd(f, f')$ is the same computed in $K[X]$ or in $L[X]$ for any extension L/K. This follows from Euclid's algorithm for greatest common divisors.

Theorem 7.3. (i) Let $f \in K[X]$ be irreducible. Then f is separable if and only if $f' \neq 0$, i.e. not the zero polynomial.
(ii) If $\operatorname{char} K = 0$ then every irreducible $f \in K[X]$ is separable.

(iii) If $\operatorname{char} K = p > 0$ then an irreducible $f \in K[X]$ is inseparable if and only if $f(X) = g(X^p)$ for some neccessarily irreducible $g \in K[X]$.

Proof. (i) We may assume f is monic. Then as $\gcd(f, f') \mid f$, $\gcd(f, f') \in \{1, f\}$. If $f' = 0$ then $\gcd(f, f') = f$, so f is inseparable. If $f' \neq 0$ then $\gcd(f, f') \mid f'$, so $\deg \gcd(f, f') \leq \deg f' < \deg f$, hence $\gcd(f, f') = 1$, i.e. f is separable.

(ii),(iii) Let $f(X) = \sum_{i=0}^{d} a_i X^i$. Then $f' = 0$ if and only if $ia_i = 0$ for all $1 \leq i \leq d$. If $\operatorname{char} K = 0$ this holds if and only if $a_i = 0$ for all $i \geq 1$, i.e. f is constant. If $\operatorname{char} K = p > 0$ this holds if and only if $a_i = 0$ whenever $p \nmid i$, i.e. $f(X) = g(X^p)$ where $g(X) = \sum_{0 \leq j \leq d/p} a_{pj} X^i$. □

Definition. (i) Let x be algebraic over K. We say x is *separable* over K if its minimal polynomial is separable.

(ii) If L/K is an algebraic extension, then L/K is said to be *separable* if every $x \in L$ is separable over K.

Remark. If $x \in K$ then x is separable over K as the minimal polynomial is $X - x$. Also, if $\operatorname{char} K = 0$ then any algebraic x is separable over K by Theorem 7.3 (ii), so every algebraic extension of fields of characteristic 0 is separable.

The following is an immediate consequence of the definition and Theorem 6.1.

Proposition 7.4. Suppose x is algebraic over K, has minimal polynomial $f \in K[X]$, and L is any extension over which f splits into linear factors. Then x is separable over K if and only if there are exactly $\deg f$ K-embeddings $K(x) \hookrightarrow L$.

Theorem 7.5 (Primitive Element Theorem)**.** Let $L = K(x_1, \ldots, x_r, y)$ be a finite extension of K. Assume that each x_i is separable over K, and that K is infinite. Then there exists $c_1, \ldots, c_r \in K$ such that $L = K(z)$ where $z = y + c_1 x_1 + \cdots + c_r x_r$.

Proof. By induction on r, it suffices to consider the case $r = 1$. So assume $L = K(x, y)$, x separable over K, y algebraic over K. Let f, g be the minimal polynomials of x, y, and let M/L be a splitting field for fg. Let $x = x_1, x_2, \ldots, x_m$ be the distinct roots of g in M. (So as x is separable, $f(X) = \prod_{i=1}^{n}(X - x_i)$.) There is only a finite number of $c \in K$ for which two of the mn numbers $y_j + cx_i$ are equal. As K is infinite, we may then choose c such that no two of them are equal, and let $z = y + ck$. Consider the polynomials $f(X) \in K[X]$, $g(z - cX) \in K(z)[X]$. They both have x as a root, since $z - cx = y$. We claim that they have no other common root.

Roots of f are x_i, so if they do have a root in common $z - cx_i = y_j$ for some j, i.e. $y_j + cx_i = z = y_1 + cx_1$, which forces $i = 1$, i.e. $x_i = x$, by choice of c.

So the greatest common divisor of $f(X)$ and $g(z - cX)$ is $X - x$ as f is separable. But since $f(X), g(z - cX) \in K(z)[X]$, their greatest common divisor is in $K(z)[X]$, so $x \in K(z)$. So $y = z - cx \in K(z)$, i.e. $K(z) = L$. □

Corollary 7.6. If L/K is finite and separable, then $L = K(x)$ for some $x \in L$. We say L/K is a simple extension.

Proof. If K is infinite then $L = K(x_1, \ldots, x_r)$ with $x_1, \ldots, x_r$ separable over K, hence the result follows by Theorem 7.5. If K is finite, then so is L. The group L^* is cyclic, let x be a generator. Then certainly $L = K(x)$. □

Chapter 8

Algebraic Closure

Definition. A field K is said to be *algebraically closed* if every non-constant polynomial $f \in K[X]$ splits into linear factors in $K[X]$.

Example. $\mathbb{C}$ is algebraically closed. We will see later that $\bar{Q}$ is algebraically closed. As an exercise, show that no finite field is algebraically closed.

Proposition 8.1. The following are equivalent.

(i) K is algebraically closed.
(ii) If L/K is any extension and $x \in L$ is algebraic over K then $x \in K$.
(iii) If L/K is algebraic then $L = K$.

Proof. [(i) $\implies$ (ii)] Suppose x is algebraic over K. Then the minimal polynomial of x splits into linear factors over K, so is linear, i.e. $x \in K$.

[(iii) $\implies$ (i)] Let $f \in K[X]$, let L be a splitting field for f over K. Then if (iii) holds, $L = K$, so f splits already in $K[X]$.

[(ii) $\implies$ (iii)] If L/K is algebraic, then by (ii) every $x \in L$ is an element of K, i.e. $L = K$. □

Proposition 8.2. Let L/K be an algebraic extension such that every irreducible polynomial in $K[X]$ splits into linear factors over L. Then L is algebraically closed. We say L is an *algebraic closure* of K.

Proof. Let L'/L be an algebraic extension. It is sufficient to prove that $L' = L$. Let $x \in L'$. Then as L'/L and L/K are algebraic, x is algebraic over K. Let $f \in K[X]$ be its minimal polynomial. By hypothesis, f splits into linear factors in $L[X]$, so $x \in L$. Hence $L = L'$. □

Apply this with $K = \mathbb{Q}$, $L = \bar{\mathbb{Q}}$ to see that $\bar{\mathbb{Q}}$ is algebraically closed.

Proposition 8.3. Let L/K be an algebraic extension, and let $\sigma\colon K \hookrightarrow M$ be an embedding of K into an algebraically closed field. Then σ can be extended to an embedding $\bar{\sigma}\colon L \hookrightarrow M$.

Proof. Suppose that $L = K(x)$, and let f be the minimal polynomial of x over K. Let $y \in M$ be a root of $\sigma f \in M[X]$. Then we know that σ extends to a unique embedding $K(x) \hookrightarrow M$ such that $x \mapsto y$.

We can move from finite to infinite extensions using Zorn's lemma.

Definition. A *partially ordered set* S is a non-empty set with a relation $\leq$ such that

- $\forall x \in S\ x \leq x$;
- $\forall x, y \in S\ x \leq y \wedge y \leq x \implies x = y$;
- $\forall x, y, z \in S\ x \leq y \wedge y \leq z \implies x \leq z$.

Definition. A *chain* in a partially ordered set S is a subset $T \subset S$ which is *totally ordered* by $\leq$, i.e.

$$\forall x, y \in T \quad x \leq y \vee y \leq x.$$

Zorn's lemma tells us when S has a *maximal element*, i.e. $z \in S$ such that if $z \leq x$ then $z = x$. If every chain $T \subset S$ has an *upper bound*, i.e. there exists $z \in S$ such that for all $x \in T$ we have $x \leq z$, then S has maximal elements.

As a consequence, every ring R has a maximal ideal.

Proof of Proposition 8.3 continued. Let L/K be an arbitrary algebraic extension. Let $S = \{(L_1, \sigma_1)\}$ where $K \subset L_1 \subset L$ and $\sigma_1 \colon L_1 \to M$ is a σ-embedding. Define $(L_1, \sigma_1) \leq (L_2, \sigma_2)$ if $L_1 \subset L_2$ and $\sigma_2|_{L_1} = \sigma_1$, i.e. $\sigma_2(x) = \sigma_1(x)$ for all $x \in L_1$. This is a partial order on S.

Let $\{(L_i, \sigma_i) \colon i \in I\}$ be a chain in S, where I is some index set. Let $L' = \bigcup_{i \in I} L_i$ which is a field: if $x \in L_i$, $y \in L_j$ then without loss of generality $L_i \subset L_j$, so $x, y \in L_j$, hence $x \pm y, \frac{x}{y}, xy \in L_j$ as well. Define $\sigma' \colon L' \hookrightarrow M$ as follows: $\sigma'(x) = \sigma_i(x)$ for any $i \in I$ such that $x \in L_i$. (If $x \in L_i$ and $x \in L_j$ then without loss of generality $L_i \subset L_j$ and $\sigma_j|_{L_i} = \sigma_i$, so $\sigma_i(x) = \sigma_j(x)$.) Then for all $i \in I$, $(L_i, \sigma_i) \subset (L', \sigma')$.

So $(L', \sigma') \in S$ is an upper bound for the chain, so by Zorn's lemma, S has maximal elements.

Let (L', σ') be a maximal element. If $(L' \subsetneq L$, then there exists $x \in L \setminus L'$ algebraic over L'. By the first part, $\sigma' \colon L' \hookrightarrow M$ extends to an embedding $\sigma'' \colon L'(x) \hookrightarrow M$, i.e. $(L', \sigma') \leq (L'(x), \sigma'')$ and $L' \neq L'(x)$, contradicting the maximality of (L', σ'). So $L' = L$ and $\bar{\sigma} = \sigma'$ is the desired embedding. $\square$

Theorem 8.4. Let K be a field. Then K has an algebraic closure, $\bar{K}$ say. Moreover, if $\sigma \colon K \xrightarrow{\sim} K'$ and $\bar{K}'$ is an algebraic closure of K', then there exists a σ-isomorphism $\bar{\sigma} \colon \bar{K} \xrightarrow{\sim} \bar{K}'$.

Recall that to say $\bar{K}$ is an algebraic closure means that $\bar{K}$ is an algebraic extension of K and $\bar{K}$ is algebraically closed.

Proof. The idea is to construct a "splitting field" for all irreducible polynomials in $K[X]$.

If K is countable then $K[X] = \{f_1, f_2, \dots\}$ is also countable. We could then inductively define a sequence of extensions $K = K_0 \subset K_1 \subset \cdots$ by letting K_n be the splitting field of f_n over K_{n-1}. Then setting $\bar{K} = \bigcup_{n \in \mathbb{N}} K_n$, every polynomial in $K[X]$ splits in $\bar{K}$, hence by Proposition 8.2, $\bar{K}$ is an algebraic closure of K.

We now consider the general case. For each irreducible polynomial $f \in K[X]$, let M_f be a splitting field for f over K. Write $M_f = K(x_{f,1}, \dots, x_{f,d(f)})$ where $\{x_{f,i}\}_{i=1}^{d(f)}$ are the roots of f in M_f. Hence $M_f \cong R_f / I_f$ where $R_f = K[X_{f,1}, \dots, X_{f,d(f)}]$ and I_f is the kernel of the map $R_f \to M_f, X_{f,i} \mapsto x_{f,i}$.

Lecture 11

For any set S of irreducible polynomials in $K[X]$, define

$$R_S = K[\{X_{f,i}\}_{f\in S, 1\le i\le d(f)}]$$

and I_S to be the ideal of R_s generated by $\{I_f\}_{f\in S}$.

Notice that $R_S = \bigcup_T R_T$, $I_S = \bigcup_T I_T$, where in each case the union is taken over all finite subsets $T \subset S$.

Lemma 8.5. *$I_S \neq R_S$.*

Proof. If S is finite, let M be the splitting field for $f_S = \prod_{f\in S} f$. Then for each f, choose a K-embedding $\psi_f \colon M_f \hookrightarrow M$, hence a K-homomorphism $R_f \to M, X_{f,i} \mapsto \psi_f(x_{f,i})$. These give a homomorphism $R_S \to M$ whose kernel contains each I_f, hence contains I_S. So $I_S \neq R_S$.

In general, if $I_S = R_S$ then $1 \in I_S$, so $1 \in I_T$ for some finite subset $T \subset S$, so $I_T = R_T$, which we have just proved cannot happen. □

Proof of Theorem 8.4 continued. Let S be the set of all irreducible polynomials in $K[X]$. By Zorn's lemma, there exists a maximal ideal $J \subsetneq R_S$ containing I_S. (Equivalently, this is a maximal ideal of R_S/I_S.) Let $\bar{K} = R_S/J$, this is a field and comes with an embedding $K \hookrightarrow \bar{K}$, so we can view it as an extension of K.

For each f, the inclusion $R_f \hookrightarrow R_S$ gives a homomorphism $R_f \to R_S/J = \bar{K}$ whose kernal contains (and therefore equals) I_f, hence by the First Isomorphism Theorem there is a K-embedding $M_f = R_f/I_f \hookrightarrow \bar{K}$, so f splits into linear factors in $\bar{K}$; and $\bar{K}$ is generated by the image of the M_f, so $\bar{K}$ is algebraic over K, i.e. $\bar{K}$ is an algebraic closure of K.

Finally, let $\sigma \colon K \xrightarrow{\sim} K' \subset \bar{K}'$. By Proposition 8.3, σ extends to $\bar{\sigma} \colon \bar{K} \to \bar{K}'$ and $K' \subset \bar{\sigma}(\bar{K}) \subset \bar{K}'$, so $\bar{K}'/\bar{\sigma}(\bar{K})$ is algebraic. But $\bar{K}$ is algebraically closed, so $\bar{\sigma}(\bar{K}) = \bar{K}'$, i.e. $\bar{\sigma}$ is an isomorphism. □

Chapter 9

Field Automorphisms and Galois Extensions

Note $\mathbb{R} = \{z \in \mathbb{C} : z = \bar{z}\}$ is the set of complex numbers fixed by the automorphism $z \mapsto \bar{z}$. In this chapter, we consider automorphisms of general fields and their fixed point sets.

Definition. Let L/K be an extension of fields. An *automorphism of L over K* is a bijective homomorphism $\sigma\colon L \xrightarrow{\sim} L$ which is the identity on K. The set of all automorphisms of L/K is a group under composition, denoted $\mathrm{Aut}(L/K)$.

Example. (i) If $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) \ni \sigma$ then $\sigma(i)^2 = \sigma(i^2) = \sigma(-1) = -1$, so $\sigma(i) = \pm 1$. Hence either $\sigma(x+iy) = x \pm iy$ for all $x, y \in \mathbb{R}$. So $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{\iota, {}^{-}\}$.

(ii) The same argument shows that $|\mathrm{Aut}(\mathbb{Q}(i)/\mathbb{Q})| = 2$ and the non-trivial element is complex conjugation.

(iii) Consider $\mathbb{Q}(\sqrt{3})/\mathbb{Q}$. If σ is an automorphism, then $\sigma(x + y\sqrt{3}) = x + y\sigma(\sqrt{3})$ for all $x, y \in \mathbb{Q}$. Also $\sigma(\sqrt{3})^2 = \sigma(3) = 3$, so $\sigma(\sqrt{3}) = \pm\sqrt{3}$. So $|\mathrm{Aut}(\mathbb{Q}(\sqrt{3})/\mathbb{Q})| \leq 2$. Both occur since as $\sqrt{3}, -\sqrt{3}$ are conjugate over $\mathbb{Q}$ (i.e. they have the same minimal polynomial), there exists $\sigma\colon \mathbb{Q}(\sqrt{3}) \to \mathbb{Q}(-\sqrt{3}) = \mathbb{Q}(\sqrt{3})$ mapping $\sqrt{3}$ to $-\sqrt{3}$.

(iv) Let K be any field, $L = K(X)$ the field of rational functions. Then $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) = g \in GL_2(K)$, the set of invertible matrices over K, defines a map $L \to L$ given by

$$f(X) \mapsto f\left(\frac{aX+b}{cX+d}\right).$$

It is left as an exercises to check this is an automorphism of L and that every automorphism of L over K is of this form and that this gives a surjective homomorphism $GL_2(K) \to \mathrm{Aut}(L/K)$ whose kernel is $\left\{\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) : a \in K^*\right\}$, so by the First Isomorphism Theorem,

$$\mathrm{Aut}(L/K) \cong GL_2(K)/\left\{\left(\begin{smallmatrix} a & 0 \\ 0 & a \end{smallmatrix}\right) : a \in K^*\right\} = PGL_2(K).$$

(v) Consider $L = \mathbb{Q}(\sqrt[3]{2})$ over $K = \mathbb{Q}$. If $\sigma\colon L \to L$ is an automorphism of L over $\mathbb{Q}$, then $\sigma(\sqrt[3]{2})^3 = \sigma(2) = 2$ but since $L \subset \mathbb{R}$, there exists only one cube root of 2 in L, so $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}$, i.e. $\mathrm{Aut}(L/K) = \{\iota\}$, despite the fact that L/K is a non-trivial extension.

Definition. Let L be a field, S any set of automorphisms of L. The *fixed field of S* is

$$L^S = \{x \in L : \sigma(x) = x \ \forall \sigma \in S\}$$

This is a subfield of L. We say that an algebraic extension L/K is *Galois* if it is algebraic and $K = L^{\mathrm{Aut}(L/K)}$, i.e. if $x \in L \setminus K$ then there exists $\sigma \in \mathrm{Aut}(L/K)$ such that $\sigma(x) \neq x$. If this holds, we write $\mathrm{Gal}(L/K)$ for $\mathrm{Aut}(L/K)$, the *Galois group* of L/K.

Remark. We always have $K \subset L^{\mathrm{Aut}(L/K)}$.

Example. Let us again consider the previous set of examples.

(i) $\mathbb{C}^{\mathrm{Aut}(\mathbb{C}/\mathbb{R})} = \mathbb{R}$ since $z \in \mathbb{R}$ if and only if $\bar{z} = z$.
(ii) $\mathbb{Q}(i)^{\mathrm{Aut}(\mathbb{Q}(i)/\mathbb{Q})} = \mathbb{Q}$.
(iii) $\mathbb{Q}(\sqrt{2})^{\mathrm{Aut}(\mathbb{Q}(\sqrt{2})/\mathbb{Q})} = \mathbb{Q}$ as if σ is a non-trivial automorphism of $\mathbb{Q}(\sqrt{2})$, $\sigma(x + y\sqrt{2}) = x - y\sqrt{2}$, so this is equal to $x + y\sqrt{2}$ if and only if $y = 0$, i.e. the fixed field is $\mathbb{Q}$.
(v) As $\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}) = \{\iota\}$, we have $\mathbb{Q}(\sqrt[3]{2})^{\mathrm{Aut}(\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q})} = \mathbb{Q}(\sqrt[3]{2})$.

So (i), (ii), (iii) are Galois extensions, (v) is not. Note (iv) is not a Galois extension because it is not algebraic.

(vi) Let K be any field with $\mathrm{char}\, K = 2$ containing some element b which is not a square, e.g. $K = \mathbb{F}_2(\tau)$, and let $L = K(x)$ where $x^2 = b$, i.e. L is the splitting field of $f(X) = X^2 - b$. Then $[L : K] = 2$. If $\sigma\colon L \to L$ is a K-automorphism, then $\sigma(x)^2 = \sigma(x^2) = b$, so $\sigma(x) = x = -x$ as $\mathrm{char}\, K = 2$. (Note also $X^2 - b = (X - x)^2$.) So $\mathrm{Aut}(L/K) = \{\iota\}$.

Let L/K be finite. We consider the size of $\mathrm{Aut}(L/K)$ and we will show (see Corollary 9.3 and Corollary 9.6) that $|\mathrm{Aut}(L/K)| \leq [L : K]$ with equality if and only if L/K is Galois.

Theorem 9.1 (Linear Independence of Field Automorphisms)**.** If $\sigma_1, \ldots, \sigma_n$ are distinct automorphisms of a field L, then they are linearly independent over L, meaning that if $y_1, \ldots, y_n \in L$ such that for all $x \in L$

$$y_1\sigma_1(x) + \cdots + y_n\sigma_n(x) = 0$$

then $y_1 = \cdots = y_n = 0$.

This follows from the following theorem.

Theorem 9.2 (Linear Independence of Characters)**.** Let L be a field, G a group. Suppose $\sigma_1, \ldots, \sigma_n\colon G \to L^*$ are distinct homomorphisms. (These are called *characters*.) Then they are linearly independent over L.

To prove Theorem 9.1 from this, take $G = L^*$ and note that any automorphism σ of L restricts to a homomorphism $L^* \to L^*$.

Proof. Assume we have n distinct homomorphisms $\sigma_1, \ldots, \sigma_n\colon G \to L^*$ which are linearly dependent, choose such a collection with $n > 0$ minimal. So there exists $y_1, \ldots, y_n \in L$ such that for all $g \in G$

$$y_1\sigma_1(g) + \cdots + y_n\sigma_n(g) = 0 \qquad (*)$$

By minimality, $y_1, \ldots, y_n \neq 0$. Also $n > 1$ since if $n = 1$ then $y_1\sigma_1(g) = 0$ so $\sigma_1(g) = 0 \notin L^*$.

Let $h \in G$. Replacing g by gh in $(*)$, since $\sigma_1, \ldots, \sigma_n$ are homomorphisms, we have

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

Now multiply (∗) by $\sigma_1(h)$ and subtract to obtain

$$y_2'\sigma_2(g) + \cdots + \cdots y_n'\sigma_n(g) = 0 \qquad (**)$$

where $y_i' = y_i(\sigma_i(h) - \sigma_1(h))$ for $2 \leq i \leq n$. As (∗∗) holds for all $g \in G$, by minimality of n we must have $y_2' = \cdots = y_n' = 0$. As $y_1, \ldots, y_n \neq 0$, we deduce that $\sigma_i(h) = \sigma_1(h)$ for all $h \in G$ contradicting the assumption that $\sigma_1, \ldots, \sigma_n$ are distinct. □

Corollary 9.3. Let L/K be a finite extension. Then $|\mathrm{Aut}(L/K)| \leq [L : K]$.

Proof. Let $x_1, \ldots, x_n \in L$ form a basis for L/K where $n = [L : K]$. Let $\sigma_1, \ldots, \sigma_m$ be distinct K-automorphisms of L. Suppose $m > n$, and consider the $m \times n$ matrix $(\sigma_i(x_j))$. Then the rows of this are linearly dependent since $m > n$. So there exists $y_1, \ldots, y_m \in L$ not all zero such that for all $j = 1, \ldots, n$

$$y_1\sigma_1(x_j) + \cdots + y_m\sigma_m(x_j) = 0$$

But any $x \in L$ can be written as $x = \sum_{i=1}^n a_i x_i$ where $a_i \in K$ and then

$$\begin{aligned}\sum_{i=1}^m y_i\sigma_i(x) &= \sum_{i=1}^m \sum_{j=1}^n y_i\sigma_i(a_j x_j) \\ &= \sum_{j=1}^n a_j \sum_{i=1}^m y_i\sigma_i(x_j) \\ &= 0,\end{aligned}$$

contradicting Theorem 9.1. □

Theorem 9.4 (Artin's Theorem)**.** Let L be a field, G a finite group of automorphisms of L. Then $[L : L^G] = |G|$, and L/L^G is a Galois extension with Galois group G.

In particular, $[L : L^G] < \infty$, which is far from obvious.

Proof. Let $K = L^G$, $m = |G|$. We will show that L/K is finite and $[L : K] \leq m$. Then $m = |G| \leq \mathrm{Aut}(L/K) \leq [L : K] \leq m$ as $G \subset \mathrm{Aut}(L/K)$ and by Corollary 9.3, so we have equality at each stage, i.e. $m = [L : K]$ and $G = \mathrm{Aut}(L/K)$, which means that L/K is Galois with Galois group G. (It is Galois since $K \subset L^{\mathrm{Aut}(L/K)} \subset L^G \subset K$, so we have equality.)

Let $x \in L$, and let $\{x_1, \ldots, x_d\} = \{g(x) : g \in G\}$ where $1 \leq d \leq m$ and $x_1 = x$, $x_i \neq x_j$ if $i \neq j$, i.e. the orbit of x under G. The polynomial $f(X) = \prod_{i=1}^d (X - x_i)$ is then separable, and is invariant under G which permutes its roots. So $f \in K[X]$. So x is algebraic and separable over K, and $[K(x) : K] \leq m$.

In particular, L/K is a separable algebraic extension.

Let K' be an intermediate field, finite over K. Then K'/K is separable, hence by the Primitive Element Theorem 7.5, $K' = K(x)$ for some $x \in L$. So by the above, $[K' : K] \leq m$.

Choose any such K' with $[K' : K]$ maximal. Suppose $y \in L$, then $K'(y)$ is a finite extension of K since y is algebraic over K, so $[K'(y) : K] \leq m$. So by maximality of $[K' : K]$, $K'(y) = K'$, i.e. $y \in K'$. So $K' = L$, hence $[L : K] \leq m$. □

Remark. Artin used linear algebra to prove this, his proof is nice but slightly longer.

Corollary 9.5. Let L/K be a finite Galois extension with Galois group G. Let $\{x_1, \ldots, x_d\} = \{\sigma(x) : \sigma \in G\}$ be the orbit under G of some $x \in L$, and $f(X) = \prod_{i=1}^{d}(X - x_i)$. Then $f \in K[X]$ and it is the minimal polynomial of x over K. In particular, f is irreducible, x is separable of degree d over K and its minimal polynomial splits into linear factors in L.

Proof. Since L/K is Galois, $K = L^G$, so Theorem 9.4 applies. We have proved everything except the irreducibility of f. But its linear factors are permuted transitively by G since its roots are a G-orbit, so it has no monic factor other than 1 and f which is invariant under G, i.e. no proper factor in $K[X]$ since $K = L^G$. □

Corollary 9.6. A finite extension L/K is Galois if and only if $[L : K] = |\mathrm{Aut}(L/K)|$.

Proof. Let $G = \mathrm{Aut}(L/K)$, which is finite by Corollary 9.3. Then $|G| = [L : L^G]$ by Theorem 9.4, so by the tower law $|G| = [L : K]$ if and only if $L^G = K$, i.e. if and only if L/K is Galois. □

Chapter 10

The Characterisation of Finite Galois Extensions

Definition. An extension L/K is *normal* if it is algebraic and for all $x \in L$, the minimal polynomial of x over K splits into linear factors in $L[X]$.

The following are equivalent ways of saying this.

- L is algebraic and for all $x \in L$ with minimal polynomial $f \in K[X]$, L contains a splitting field for f.
- L is algebraic and if $f \in K[X]$ is irreducible and has a root in L, then it splits into linear factors over L.

So if $x \in L$ has minimal polynomial $f \in K[X]$ with $\deg f = n$ the following holds.

- If L/K is separable then the roots of f in a splitting field are distinct.
- If L/K is normal then f splits into linear factors in $L[X]$.

Together, both imply that f has n distinct roots in L.

Theorem 10.1. Let L/K be a finite extension. The following are equivalent.

(i) L/K is Galois.
(ii) L/K is normal and separable.
(iii) L is the splitting field of some separable polynomial over K.

Proof. [(i) $\implies$ (ii)] This is Corollary 9.5.

[(ii) $\implies$ (iii)] Let $L = K(x_1, \ldots, x_n)$, let $f_i \in K[X]$ be the minimal polynomial of x_i. As L/K is separable, f_i is separable for $i = 1, \ldots, n$, then so is the least common multiple f, say. As L/K is normal, f splits into linear factors in L and $x_1, \ldots, x_n$ are among the roots of f, so L/K is a splitting field for f.

[(iii) $\implies$ (i)] By Corollary 9.6, it is enough to show that if L is the splitting field of a separable polynomial, then $|Aut(L/K)| = [L : K]$. This follows from part (ii) of Theorem 6.6 (Uniqueness of Splitting Fields), taking $M = L$ and $\sigma = \iota$. □

Theorem 10.2. Let L/K be a finite separable extension. Then there exists a finite extension M/L, called the *Galois closure*, or *Galios hull*, of L/K such that

(i) M/K is Galois;
(ii) no proper subfield of M containing L is Galois over K.

Moreover, if M'/K is any Galois extension containing L, then there exists an L-homomorphism $M \hookrightarrow M'$, i.e. M is the smallest Galois extension of K containing L.

Proof. Let $L = K(x)$ by the Primitive Element Theorem 7.5 and f be the minimal polynomial of x over K, which is separable. Let M be a splitting field of f over L. Then M is also a splitting field for f over K, as $f(x) = 0$. By Theorem 10.1, M/K is Galois.

If $K \subset L \subset M_1 \subset M$ and M_1/K is Galois, then M_1/K is normal and $x \in M_1$. So f splits into linear factors in M_1, so $M = M_1$.

Finally, if $M' \supset L \supset K$, then f splits into linear factors over M', so by Uniqueness of Splitting Fields, there exists an L-homomorphism $M \hookrightarrow M'$. □

Chapter 11

The Galois Correspondence

Let M/K be a finite Galois extension, $G = \mathrm{Gal}(M/K)$. Consider an intermediate field $K \subset L \subset M$. Then M is a splitting field of some separable f over K, so M is also a splitting field for f over L, so M/L is also Galois, and $\mathrm{Gal}(M/L) = \{\sigma \in \mathrm{Aut}(M) : \sigma|_L = \iota_L\}$ is a subgroup of G.

Theorem 11.1 (Fundamental Theorem of Galois Theory)**.** The maps

$$\Xi\colon L \to \mathrm{Gal}(M/L) \leq G$$
$$\Omega\colon H \to M^H$$

give a bijection

$$\left\{\begin{array}{c}\text{intermediate}\\ \text{fields } K \subset L \subset M\end{array}\right\} \longleftrightarrow \left\{\begin{array}{c}\text{subgroups}\\ H \leq G\end{array}\right\}$$

which is inclusion-reversing, i.e. if $L \leftrightarrow L'$ and $L' \leftrightarrow H'$ then $L \subset L'$ is equivalent to $H \supset H'$, and satisfies

(i) $K \subset L \subset L' \subset M \implies [L' : L] = (\mathrm{Gal}(M/L) : \mathrm{Gal}(M/L'))$;
(ii) K corresponds to G, M corresponds to $\{1\} \leq G$;
(iii) if L corresponds to H and $\sigma \in G$, then $\sigma(L)$ corresponds to $\sigma H \sigma^{-1}$;
(iv) L is Galois over K if and only if $\mathrm{Gal}(M/L) \triangleleft G$ and if so then $\mathrm{Gal}(L/K) \cong G/\mathrm{Gal}(M/L)$.

Proof. As M/L is Galois, we have $M^{\mathrm{Gal}(M/L)} = L$ and so $\Omega\Xi(L) = L$. By Artin's Theorem, $\mathrm{Gal}(M/M^H) = H$. Hence $\Xi\Omega(H) = H$. Thus we have a bijection and the inclusion-reversing property is immediate.

(i) $|\mathrm{Gal}(M/L)| = [M : L]$, $|\mathrm{Gal}(M/L')| = [M : L']$. So by the tower law,

$$[L' : L] = \frac{[M : L]}{[M : L']} = \frac{|\mathrm{Gal}(M/L)|}{|\mathrm{Gal}(M/L')|} = (\mathrm{Gal}(M/L) : \mathrm{Gal}(M/L'))$$

(ii) Trivial.
(iii) Let $x \in M, \tau \in G$. Then $(\sigma\tau\sigma^{-1})(\sigma(x)) = \sigma(\tau(x))$, so τ fixes x if and only if $\sigma\tau\sigma^{-1}$ fixes $\sigma(x)$, i.e. $x \in M^H$ if and only if $\sigma(x) \in M^{\sigma H \sigma^{-1}}$.
(iv) Suppose $H = \mathrm{Gal}(M/L) \triangleleft G$. Then for all $\sigma \in G$, $\sigma H \sigma^{-1} = H$, so $\sigma(L) = L$ by (iii), so σ is an automorphism of L, and we have a homomorphism

$$\pi : G = \mathrm{Gal}(M/K) \to \mathrm{Aut}(L/K), \sigma \mapsto \sigma|_L$$

whose kernel is $\{\sigma \in G : \sigma|_L = \iota\} = \mathrm{Gal}(M/L)$, so using (i)

$$[L:K] = \frac{|G|}{|\mathrm{Gal}(M/L)|} = |\mathrm{Im}(\pi)| \leq |\mathrm{Aut}(L/K)| \leq [L:K]$$

So $|\mathrm{Aut}(L/K) = [L:K]|$, i.e. L/K is Galois and $|\mathrm{Im}(\pi)| = |\mathrm{Aut}(L/K)|$, i.e. π is surjective, and so $\mathrm{Gal}(L/K) \cong G/\mathrm{Gal}(M/L)$.
Conversely, suppose L/K is Galois, $H = \mathrm{Gal}(L/K)$, $x \in L$, f its minimal polynomial over K. Then if $\sigma \in G$, $0 = \sigma(f(x)) = f(\sigma(x))$. As L/K is normal, $\sigma(x) \in L$, so $\sigma(L) = L$ for all $\sigma \in G$, i.e. $\sigma H \sigma^{-1} = H$ for all $\sigma \in G$. □

Example. $K = \mathbb{Q}$, M a splitting field of $X^3 - 2$ over $\mathbb{Q}$, so $M = \mathbb{Q}(\sqrt[3]{2}, \omega\sqrt[3]{2}, \omega^2\sqrt[3]{2}) = \mathbb{Q}(\sqrt[3]{2}, \omega)$ where $\omega = e^{2\pi i/3}$. Set $x_j = \omega^j \sqrt[3]{2}$. Note $\omega^2 + \omega + 1 = 0$. So $X^3 - 2\prod_{j=0}^{2}(X - x_j)$ is irreducible over $\mathbb{Q}$.

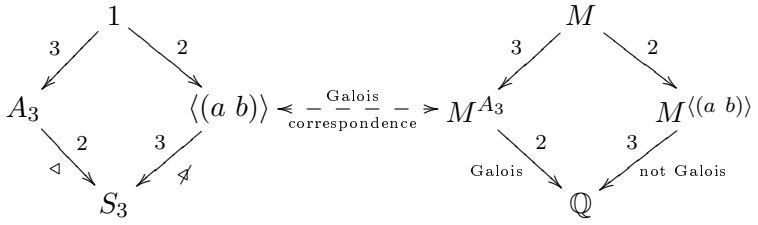
Let $L_j = \mathbb{Q}(x_j)$. So $L_0 = \mathbb{Q}(\sqrt[3]{2})$, $M = L_0(\omega)$, $[L_j : \mathbb{Q}] = 3$, $[M : L_0] = 2$ as $\omega \notin L_0$.

So $[M : \mathbb{Q}] = 6$ and is Galois, so $G = \mathrm{Gal}(M/\mathbb{Q})$ has order 6. G permutes the roots $\{x_0, x_1, x_2\}$ and for all $\sigma \in G$,

$$(\forall j = 0, 1, 2 \quad \sigma(x_j) = x_j) \quad \Longrightarrow \quad \sigma = \iota.$$

So G is isomorphic to a subgroup of S_3, so $G \cong S_3$.

$S_3 = \mathrm{Sym}\{0, 1, 2\}$, subgroups are S_3, $\{1\}$, $\{1, (ab)\} = \langle (ab) \rangle$, $\{1, (012), (021)\} = A_3$.



where $\langle (a\ b) \rangle$ represents three different subgroups. So M^{A_3} has degree 2 over $\mathbb{Q}$, so must be $\mathbb{Q}(\omega)$. $M^{\langle (a\ b) \rangle} = \mathbb{Q}(x_j)$ for different x_js, depending on $\langle (a\ b) \rangle$. Complex conjugation fixes x_0 and permutes x_1, x_2, so $M^{\langle (1\ 2) \rangle} = \mathbb{Q}(x_0)$, for example.

Theorem 11.2. $\mathbb{C}$ is algebraically closed.

Proof. We will use the following.

(i) If $f \in \mathbb{R}[X]$ has odd degree, then f has a root in $\mathbb{R}$. (This is an application of the Intermediate Value Theorem.)
(ii) If $f \in \mathbb{C}[X]$ is quadratic, then it splits into linear factors.

Now (i) and (ii), respectively, imply

(i') If $K/\mathbb{R}$ is finite and $[K : \mathbb{R}]$ odd, then $K = \mathbb{R}$, since if $x \in K$, its minimal polynomial is irreducible of odd degree, hence has degree 1.
(ii') There is no extension $K/\mathbb{C}$ of degree 2.

Furthermore, we use the following two facts from group theory.

(a) If G is a finite group, $|G| = p^n m$ where $\gcd(p, m) = 1$, then G has a subgroup P of order p^n. (This is part of Sylow's theorem.)
(b) If H is a finite group of order $p^n \neq 1$, then H as a (normal) subgroup of index p.

Statement (b) can be proved by induction on $|H|$ as follows. It is clear for $|H| = p$. Suppose $|H| \geq p^2$. Then H has a non-trivial centre $Z(H) = \{x \in H : xy = yx \ \forall y \in H\} \neq \{1\}$. Let $x \in Z(H)$ be of order p, consider $\bar{H} = H/\langle x \rangle$. (This exists since $\langle x \rangle$ is a normal subgroup.) By induction, $\bar{H}$ has a (normal) subgroup $\bar{K} \subset \bar{H}$ of index p, which by the First Isomorphism Theorem corresponds to a (normal) subgroup of H of index p containing $\langle x \rangle$.

Let $K/\mathbb{C}$ be a finite extension. We must prove $K = \mathbb{C}$. Choose a finite extension L/K such that $L/\mathbb{R}$ is Galois, e.g. the Galois closure of $K/\mathbb{R}$. Let $G = \mathrm{Gal}(L/\mathbb{R})$, then since $\mathbb{C} \supsetneq \mathbb{R}$, $L \supsetneq \mathbb{R}$ we have that $[L : \mathbb{R}]$ is even. Let $P \subset G$ a Sylow 2-subgroup.

So $[L^P : \mathbb{R}] = (G : P)$ is odd, so $L^P = \mathbb{R}$, i.e. be the Fundamental Theorem of Galois Theory, $G = P$ is a group of order 2^n.

Therefore, $H = \mathrm{Gal}(L/\mathbb{C})$ is a 2-group, i.e. has order a power of 2, as well. Let $H_1 \subset H$ be a subgroup of index 2 (if it exists). Then $[L^{H_1} : \mathbb{C}] = (H : H_1) = 2$, contradicting (ii'). So $H = \{1\}$, i.e. $L = \mathbb{C}$ and hence $K = \mathbb{C}$. □

Galois Groups of Polynomials

Let $f \in K[X]$ be a separable non-constant polynomial of degree n. Let L/K be a splitting field for f, and $x_1, \ldots, x_n \in L$ the roots of f. So $L = K(x_1, \ldots, x_n)$ is a finite Galois extension of K, let $G = \mathrm{Gal}(L/K)$. If $\sigma \in G$, then $f(\sigma(x_i)) = \sigma(f(x_i)) = 0$, so σ permutes the roots of f. Also, if $\sigma(x_i) = x_i$ for each i, then $\sigma(x) = x$ for all $x \in L$, i.e. $\sigma = \iota$. So we may regards G as a subgroup of the symmetric group S_n. We call G the Galois group of f over K, written $\mathrm{Gal}(f/K)$.

Since $G \subset S_n$, $|G| = [L : K]$ divides $n!$.

Definition. $H \subset S_n$ is *transitive* if for all $i, j \in [n]$ there exists $g \in H$ such that $g(i) = j$. Equivalently, H has exactly one orbit.

Proposition 11.3. f is irreducible over K if and only if G is a transitive subgroup.

Proof. We know from Corollary 9.5 that if $y \in L$ and $\{y_1, \ldots, y_d\}$ is the orbit of y under G, then the minimal polynomial of y over K is $\prod_{i=1}^{d}(X - y_i)$.

So the minimal polynomial of x_1 is the product of $(X - x_j)$ for all x_j which are of the form $\sigma(x_1)$ for some $\sigma \in G$. So f, which may be assumed to be monic, equals die minimal polynomial of x_1 (and hence is irreducible) if and only if every x_j is of the form $\sigma(x_1)$, i.e. if and only if G is transitive. □

Suppose $\deg f = 2$. Then $G = \{1\}$ if f is reducible, and $G = S_2$ if f is irreducible.

Suppose $\deg f = 3$. If $f(X) = (X - a)g(X)$ reducible, $a \in K$, then L is a splitting field for g over K, so the problem is reduced to the degree 2 case, when $|G| = 1$ or $|G| = 2$. If f is irreducible, then $G = \mathrm{Gal}(f/K)$ is a transitive subgroup of S_3, so $G = S_3$ or $G = A_3$.

Recall the following.

$$\Delta(X_1, \ldots, X_n) = \prod_{1 \leq i < j \leq n} (X_i - X_j)$$

$$\mathrm{Disc}(X_1,\dots,X_n) = \Delta^2 = (-1)^{n(n-1)/2} \prod_{\substack{1\le i,j\le n\\ i\ne j}} (X_i - X_j)$$

$$\Delta(X_{\sigma(1)},\dots,X_{\sigma(n)}) = \mathrm{sgn}(\sigma)\Delta(X_1,\dots,X_n)$$

For a monic separable polynomial $f = \prod_{i=1}^n (X - x_i)$ with splitting field L, define

$$\Delta_f = \Delta(x_1,\dots,x_n) \in L \setminus \{0\}$$
$$\mathrm{Disc}(f) = \Delta_f^2$$

which is independent of the listing of roots.

Theorem 11.4. (i) $\mathrm{Disc}(f) \in K^*$;
(ii) $K(\Delta_f) = L^{G\cap A_n}$ where $G = \mathrm{Gal}(f/K) = \mathrm{Gal}(L/K)$.

In particular, $\Delta_f \in K$, i.e. $\mathrm{Disc}(f)$ is a square in K, if and only if $G \subset A_n$.

Proof. Let $\sigma \in G$. Then $\sigma(\Delta_f) = \Delta(\sigma(x_1),\dots,\sigma(x_n)) = \mathrm{sgn}(\sigma)\Delta_f$ and hence $\sigma(\mathrm{Disc}(f)) = \sigma(\Delta_f)^2 = \mathrm{Disc}(f)$. So by the Fundamental Theorem of Galois Theory, $\mathrm{Disc}(f) \in K$, and $\sigma(\Delta_f) = \Delta_f$ if and only if $\sigma \in G \cap A_n$ since we can divide by $\Delta_f \ne 0$. □

Remark. For any monic polynomial, separable or not, we may define $\mathrm{Disc}(f)$ by the same formula as

$$\mathrm{Disc}(f) = \prod_{1\le i<j\le n} (x_i - x_j)^2$$

where $f(X) = \prod_{i=1}^n (X - x_i)$, and $\mathrm{Disc}(f) \ne 0$ if and only if f is separable.

Consider the formal derivate of $f(X) = \prod_{i=1}^n (X - x_i) \in K[X]$.

$$f'(X) = \sum_{i=1}^n \prod_{j\ne i} (X - x_j)$$
$$f'(x_i) = \prod_{j\ne i} (x_i - x_j)$$
$$\mathrm{Disc}(f) = (-1)^{n(n-1)/2} \prod_{i=1}^n f'(x_i)$$

Remark. $\mathrm{Disc}(f)$ is a symmetric function of $x_1,\dots,x_n$, so it can be expressed as a polynomial in the elementary symmetric functions $s(x_1,\dots,x_n)$. But

$$f(X) = \prod_{i=1}^n (X - x_i) = X^n - s_1(x_1,\dots,x_n)X^{n-1} + \cdots + (-1)^n s_n(x_1,\dots,x_n),$$

i.e. $s_r(x_1,\dots,x_n) = (-1)^r \times$ (coefficient of X^{n-r}). So $\mathrm{Disc}(f)$ is a polynomial (with integer coefficients) in the coefficients of f, and in principle it is easy to compute.

Chapter 12

Finite Fields

Let p be a prime number. We will describe all finite fields of characteristic p and their Galois groups. Let F be a finite field of characteristic p. We know the following.

- $|F| = p^n$ where $n = [F : \mathbb{F}_p] = \dim_{\mathbb{F}_p} F$. (Theorem 3.1)
- F^* is cyclic of order $p^n - 1$. (Proposition 3.4)
- $\phi_p \colon F \to F, x \mapsto x^p$ is a homomorphism from f to itself. It is injective and hence is bijective, i.e. it is an automorphism of F. (Proposition 3.5)

Theorem 12.1. For every $n \geq 1$, there exists a finite field $\mathbb{F}_{p^n}$ with p^n elements. Any such field is a splitting field for $f_n(X) = X^{p^n} - X$ over $\mathbb{F}_p$. In particular, any two fields of order p^n are isomorphic.

Proof. Let $|F| = p^n$. Then for all $x \in F^*$, $x^{p^n-1} = 1$, so for all $x \in F$, $x^{p^n} = x$, i.e. $f_n(x) = 0$. So f_n has p^n roots in F, and obviously no proper subfield of F contains them. So F is a splitting field for f_n.

Conversely, let F' be a splitting field for f_n over $\mathbb{F}_p$. So F' is a finite field of characteristic p, and $\phi_p \in \mathrm{Aut}(F'/\mathbb{F}_p)$. Let F be the fixed field of ϕ_p^n. So $F = \{x \in F' : x^{p^n} = x\}$ is the set of roots of f_n in F'. So by definition of splitting fields, $F = F'$, and it is a field with p^n elements. □

Remark. This remark clarifies the last setence in the previous proof.

- By construction, we have $F \subset F'$. Also $\mathbb{F}_p \subset F$, and so $F \subsetneq F'$ implies F' is not a splitting field, contradiction. Hence $F = F'$, as claimed.
- Since $f_n'(X) = p^n X^{p^n-1} - 1 = -1$, we have $\gcd(f_n, f_n') = 1$, so f_n is separable and hence has p^n distinct roots.

Theorem 12.2. (i) $\mathbb{F}_{p^n}$ is a Galois extension of $\mathbb{F}_p$, whose Galois group is cyclic, generated by ϕ_p.

(ii) $\mathbb{F}_{p^n}$ contains a unique subfield of order p^m if $m \mid n$, and has no such subfield if $m \nmid n$, and $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_{p^m}) = \langle \phi_p^m \rangle$.

Proof. (i) f_n is separable since it has p^n roots in $\mathbb{F}^{p^n}$ and also $f_n' = -1$, so $\mathbb{F}_{p^n}$ is the splitting field of a separable polynomial, hence is a Galois extension of $\mathbb{F}_p$.
We have $\phi_p \in \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = G$. Since $n = [\mathbb{F}_{p^n} : \mathbb{F}_p] = |G|$, it is enough to show that the order of ϕ_p in G is n. If not, $\phi_p^m = \iota$ for some m with $1 \leq m < n$, i.e. for all $x \in \mathbb{F}_{p^n}$, $x^{p^m} = x$, which is impossible (as this polynomial has too many roots given its degree).

(ii) If $\mathbb{F}_{p^m} \subset \mathbb{F}_{p^n}$, then let $r = [\mathbb{F}_{p^n} : \mathbb{F}_{p^m}]$, so that as vector spaces $\mathbb{F}_{p^n} \cong (\mathbb{F}_{p^m})^r$. So $p^n = (p^m)^r$, i.e. $m \mid n$ and $r = \frac{m}{n}$.
If $m \mid n$, then consider $H = \langle \phi_p^m \rangle \leq \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$; $|H| = \frac{m}{n}$, so the field $(\mathbb{F}_{p^n})^H$ has degree $m = (\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) : H)$ over $\mathbb{F}_p$, so has p^m elements. □

Galois Group of Polynomials over $\mathbb{F}_p$

Let $f \in \mathbb{F}_q[X]$ be monic and separable, where $q = p^n$, $\deg(f) = d$. Let L be the splitting field of f over $\mathbb{F}_q$, so $L = \mathbb{F}_{q^m}$ for some $m \geq 1$. $G = \mathrm{Gal}(f/\mathbb{F}_q) = \mathrm{Gal}(\mathbb{F}_{q^m}/\mathbb{F}_q)$, regarded as a subgroup of S_d, acts on roots $x_1, \ldots, x_d \in L$ of f. G is cyclic, generated by $\phi_q = \phi_p^n$ by Theorem 12.2, so as a subgroup of S_d, G is determined up to conjugacy by the cycle type of ϕ_d.

Proposition 12.3. Let $f = f_1 f_2 \cdots f_r$ be the factorisation of f as a product of irreducibles in $\mathbb{F}_q[X]$, and let $d_i = \deg(f_i)$. Then, as a permutation, ϕ_q is a product of disjoint cycles of lengths $d_1, \ldots, d_r$.

Proof. Let S_i be the set of roots of f_i, for $i = 1, \ldots, r$. Then since f_i is irreducible, ϕ_q permutes the elements of S_i transitively. So the orbits of ϕ_q on the roots of f are the sets S_i, so ϕ_q has cycle type $(d_1, \ldots, d_r)$. □

Example. Let $f = X^d - 1$ over $\mathbb{F}_p$ where $d \geq 1$, $p \nmid d$. So $f' = dX^{d-1}$ and $\gcd(f, f') = 1$, i.e. f is separable.

When is $\mathrm{Gal}(f/\mathbb{F}_p) \subset A_d \subset S_d$?

Reduction modulo p

Suppose $f \in \mathbb{Z}[X]$. Gauss's lemma states that if $f = gh$ with $g, h \in \mathbb{Q}[X]$ monic, then in fact $g, h \in \mathbb{Z}[X]$. (Note $\mathbb{Z}[X]$ is a UFD.) In particular, for a primitive polynomial f, f is irreducible over $\mathbb{Q}$ if and only if f is irreducible over $\mathbb{Z}$.

So if p is prime and $\bar{}$ denotes reduction modulo p, then $\bar{f} = \bar{g}\bar{h} \in \mathbb{F}_p[X]$. So if $\bar{f}$ is irreducible, so is f.

Example 12.4.

$$f(X) = X^4 + 5X^2 - 2X - 3 \equiv \begin{cases} X^4 + X^2 + 1 \equiv (X^2 + X + 1)^2 & \pmod 2 \\ X^4 + 2X^2 + X \equiv X(X^3 + 2X + 1) & \pmod 3 \end{cases}$$

So f is irreducible, since $f = gh$ implies $\deg g = 1$ or $\deg g = 2$, which is impossible by reduction modulo 2 and 3, respectively.

Remark. This does not always work (see Example Sheet 3 Question 7).

The same idea can be applied to Galois groups.

Theorem 12.5. Let $f \in \mathbb{Z}[X]$ be monic, p prime. Assume f and $\bar{f} \equiv f \pmod p$ are separable. Then as subgroups of S_n, where $n = \deg f$, $\mathrm{Gal}(f/\mathbb{Q})$ contains $\mathrm{Gal}(\bar{f}/\mathbb{F}_p)$.

Proof. The idea is to relate $\mathrm{Gal}(f/\mathbb{Q})$ and $\mathrm{Gal}(\bar{f}/\mathbb{F}_p)$. Let $L = \mathbb{Q}(x_1, \ldots, x_n)$ be a splitting field for $f(X) = \prod_{i=1}^n (X - x_i)$ and $N = [L : \mathbb{Q}]$, $G = \mathrm{Gal}(L/\mathbb{Q}) = \mathrm{Gal}(f/\mathbb{Q}) \leq S_n$ by action on $\{x_1, \ldots, x_n\}$. Let $R = \mathbb{Z}[x_1, \ldots, x_n]$. A basic fact from Algebraic Number Theory is that R is a free $\mathbb{Z}$-module of rank N, contained in the ring of algebraic integers of L. So R/pR is a finite ring with p^N elements, since as a group $R/pR \cong \mathbb{Z}^N/p\mathbb{Z}^N$. Let $P_1, \ldots, P_m$ be the maximal ideals of R containing pR. (These are in a bijective correspondence with the maximal ideals of R/pR.) Let $k = R/P_1$, a finite field with p^l elements, say. Let $\psi \colon R \to k = R/P_1$ be the quotient homomorphism and let $\bar{x}_i = \psi(x_i)$. Then

$$\bar{f}(X) = \psi f(X) = \prod_{i=1}^n \psi(X - x_i) = \prod_{i=1}^n (X - \bar{x}_i)$$

Clearly $k = \mathbb{F}_p[\bar{x}_1, \ldots, \bar{x}_n]$ by definition of R. So k is a splitting field for $\bar{f}$ over $\mathbb{F}_p$. Similarly, each R/P_j is a splitting field for $\bar{f}$ over $\mathbb{F}_p$, so by uniqueness of splitting fields, $|R/P_j| = p^l$ for all $j = 1, \ldots, m$.

The group G maps R to itself, so permutes $P_1, \ldots, P_m$. Let $H = \mathrm{Stab}_G(P_1) = \{\sigma \in G : \sigma(P_1) = P_1\}$. H then acts on $R/P_1 = k$, since if $x \equiv y \mod P_1$ and $\sigma \in H$, then $\sigma(x) \equiv \sigma(y) \mod P_1 = \sigma(P_1)$. And if $\sigma(x_i) = x_j$ then $\sigma(\bar{x}_i) = \bar{x}_j$ (as $\bar{x}_i \equiv x_i \mod P_i$ etc.). So H is a subgroup of $\mathrm{Gal}(\bar{f}/\mathbb{F}_p) \leq S_n$ acting on $\{\bar{x}_1, \ldots, \bar{x}_n\}$.

Fact. $H = \mathrm{Gal}(\bar{f}/\mathbb{F}_p)$. Then we have identified $\mathrm{Gal}(\bar{f}/\mathbb{F}_p)$ with a subgroup of G.

Chinese Remainder Theorem (CRT)**.** Let R be a commutative ring with a multiplicative identity 1, and let $I_1, \ldots, I_m$ be ideals in R such that for all i, j with $i \neq j$, $I_i + I_j = R$. Then $\pi \colon R \to R/I_1 \times \cdots \times R/I_m$, the product of quotient maps, is surjective with kernel $I_1 \cap \cdots \cap I_m$. So $R/(I_1 \cap \cdots \cap I_m) \cong R/I_1 \times \cdots \times R/I_m$.

Proof. The kernel is clearly $I_1 \cap \cdots I_m$. We proof the result in the case $m = 2$ and then the general case follows by induction. Suppose $I_1 + I_2 = R$, so there exist $b_i \in I_i$, $i = 1, 2$, such that $b_1 + b_2 = 1$. π is surjective if and only if

$$\forall a_1, a_2 \in R \quad \exists x \in R \quad x \equiv a_i \mod I_i \text{ for } i = 1, 2 \tag{$*$}$$

Notice $b_i \equiv 0 \mod I_i$, $i = 1, 2$ and $b_1 = 1 - b_2 \equiv 1 \mod I_2$, $b_2 \equiv 1 \mod I_1$. So letting $x = b_2 a_1 + b_1 a_2$, x satisfies ($*$). □

Proof of Fact. Apply the CRT with $I_j = P_j$. Then if $i \neq j$, $P_i \subsetneq P_i + P_j \subset R$, so by maximality of P_i, $P_i + P_j = R$. So we can apply the CRT in this case.

$$\begin{aligned} p^{lm} &= |R/P_1 \times \cdots \times R/P_m| \\ &= |R/(P_1 \cap \cdots \cap P_m)| \\ &\leq |R/pR| \quad \text{since } P_1 \cap \cdots \cap P_m \supset pR \\ &= p^N \end{aligned} \tag{1}$$

i.e. $\frac{N}{m} \geq l$.

By the Orbit-Stabiliser Theorem, $(G : H)$ is the length of the orbit of G containing P_1, so $(G : H) \leq M$, i.e.

$$|H| \geq \frac{|G|}{m} = \frac{N}{m} \geq l. \tag{2}$$

and $H \leq \mathrm{Gal}(\bar{f}/\mathbb{F}_p) = \mathrm{Gal}(k/\mathbb{F}_p)$ which has order l. So we must have $|H| = l$, i.e. $H = \mathrm{Gal}(\bar{f}/\mathbb{F}_p)$. □

Remark. We must also have equality in (1) and (2), i.e. $P_1 \cap \cdots \cap P_m = pR$ and G acts transitively on $\{P_1, \ldots, P_m\}$.

Corollary 12.6. If $\bar{f} = g_1 \cdots g_r$ where $g_i \in \mathbb{F}_p[X]$ is irreducible of degree d_i, then $\mathrm{Gal}(f/\mathbb{Q})$ contains an element of cycle type $(d_1, \ldots, d_r)$.

Proof. Let $K/\mathbb{F}_p$ be a splitting field for $\bar{f}$. Then on the roots of g_i, the Frobenius map ϕ_p acts as a d_i-cycle. So the cycle type of ϕ_p acting on roots of $\bar{f}$ is $(d_1, \ldots, d_r)$. Then apply Theorem 12.5. □

Remark. The "converse" of Corollary 12.6 holds as well. If $\mathrm{Gal}(f/\mathbb{Q})$ contains a permutation of cycle type $(d_1, \ldots, d_r)$ say, then there exists infinitely many p such that $\bar{f} = g_1 \cdots g_r$, where g_i is irreducible of degree d_i. This is the Chebotarev Density Theorem, which belongs to algebraic and analytical number theory.

As a special case, if $(d_1, \ldots, d_r) = (1, \ldots, 1)$ then there exists infinitely many p such that $\bar{f}$ splits into linear factors in $\mathbb{F}_p$.

Recall Example 12.4,

$$f(X) = X^4 + 5X^2 - 2X - 3 \equiv \begin{cases} (X^2 + X + 1)^2 & \pmod 2 \\ X(X^3 + 2X + 1) & \pmod 3 \end{cases}$$

We have already shown f is irreducible. $\mathrm{Gal}(\bar{f}/\mathbb{F}_3)$ is cyclic of order 3 (as $X^3 - X + 1$ is irreducible). So by Theorem 12.5, $\mathrm{Gal}(f/\mathbb{Q})$ contains a 3-cycle, say $(1\ 2\ 3) = \sigma$. As f is irreducible, $\mathrm{Gal}(f/\mathbb{Q})$ is transitive, so for each $i = 1, 2, 3$ there exists τ with $\tau(4) = i$. Then $\tau\sigma\tau^{-1}$ is a 3-cycle fixing i. So taking these elements and their inverses, $\mathrm{Gal}(f/\mathbb{Q})$ contains all 3-cycles, hence $\mathrm{Gal}(f/\mathbb{Q}) \supset A_4$. So $\mathrm{Gal}(f/\mathbb{Q})$ is either A_4 or S_4. Notice that f has two real and two complex roots, so complex conjugation is a 2-cycle on the roots. So $\mathrm{Gal}(f/\mathbb{Q}) = S_4$.

Chapter 13

Cyclotomic and Kummer Extensions

These are two important classes of Galois extensions with abelian Galois groups.

Roots of Unity

Let K be a field, $m \geq 1$ an integer. Define

$$\mu_m(K) = \{x \in K : x^m = 1\}$$

the group of m-th roots of 1 in K. Since $\mu_m(K)$ is finite, it is cyclic of order dividing m. We say $x \in \mu_m(K)$ is a primitive m-th roots of 1 if x has order exactly m. In this case, $\mu_m(K) = \langle x \rangle = \{x^i : 0 \leq i \leq m\}$ has order m.

The polynomial $X^m - 1$ has derivative mX^{m-1}, so f separable if and only if m is non-zero in K, i.e., if and only if $\operatorname{char} K = 0$ or $\operatorname{char} K = p \nmid m$. So if $\operatorname{char} K = p$ and $p \mid m$, there cannot exist a primitive m-th root of 1 in K.

Assume until the end of this chapter that $\operatorname{char} K = 0$ or $\operatorname{char} K = p, p \nmid m$, i.e. assume f is separable.

Let L be a splitting field for $X^m - 1$. Then $\mu_m(L)$, the set of roots of $X^m - 1$ in L, has order m. Fix a generator $\zeta \in \mu_m(L)$ which is a primitive m-th root of 1.

Proposition 13.1. (i) $L = K(\zeta)$

(ii) There is an injective homomorphism

$$\chi \colon G = \operatorname{Gal}(L/K) \hookrightarrow (\mathbb{Z}/m\mathbb{Z})^*$$

given by $\chi(\sigma) = a \pmod m$ if $\sigma(\zeta) = \zeta^a$.

(iii) χ is surjective, i.e. an isomorphism, if and only if G acts transitively on the set of *primitive* roots of unity in L.

Proof. (i) We have

$$X^m - 1 = \prod_{x \in \mu_m(L)} (X - x) = \prod_{a=0}^{m-1} (X - \zeta^a)$$

so $L = K(\zeta)$.

(ii) The primitive m-th roots of 1 in L are $\{\zeta^a : \gcd(a,m) = 1\}$ and $\zeta^a = \zeta^b$ if and only if $a \equiv b \pmod{m}$. Let $\sigma \in G$. Then $\sigma(\zeta) = \zeta^a$ for some $a \in \mathbb{Z}$, $\gcd(a,m) = 1$ and $\sigma = \iota$ if and only if $\sigma(\zeta) = \zeta$, i.e. if and only if $a \equiv 1 \pmod{m}$.
Suppose $\tau(\zeta) = \zeta^b$, then

$$\sigma\tau(\zeta) = \sigma(\zeta^b) = \sigma(\zeta)^b = \zeta^{ab}$$

So we have an injective homomorphism $G \to (\mathbb{Z}/m\mathbb{Z})^*$, $\sigma \mapsto a \pmod{m}$.

(iii) χ is surjective if and only iff for all a with $\gcd(a,m) = 1$ there exists $\sigma \in G$ with $\sigma(\zeta) = \zeta^a$, i.e. if and only if G acts transitively on $\{\zeta^a : \gcd(a,m) = 1\}$. □

Remark. If $K \subset L \subset \mathbb{C}$ then $\mu_m(L) = \{e^{2\pi i a/m}\}$, $\zeta = e^{2\pi i/m}$ for example.

Definition. The *m-th cyclotomic polynomial* is

$$\Phi_m(X) = \prod_{\substack{0 \le a \le m \\ \gcd(a,m)=1}} (X - \zeta^a)$$

Note $\Phi_m(X) \in K[X] = L[X]^G$ since G permutes $\{\zeta^a : \gcd(a,m) = 1\}$.

We can restate (iii) in Proposition 13.1 as follows. χ is an isomorphism if and only if $\Phi_m(X)$ is irreducible over K.

Φ_m does not really depend on K. In fact, any m-th root of unity is a primitive d-th root of unity for some $d \mid m$, so $X^m - 1 = \prod_{d|m} \Phi_d(X)$. So Φ_m is determined inductively by

$$\Phi_1(X) = X - 1$$

and for all $m > 1$

$$\Phi_m(X) = \frac{X^m - 1}{\prod_{\substack{1 \le d < m \\ d|m}} \Phi_d(X)}$$

and so is the image of a polynomial in $\mathbb{Z}[X]$, e.g.

$$\Phi_p(X) = \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + 1$$

There are two important cases.

Proposition 13.2. Let $K = \mathbb{F}_q$, $q = p^n$, $p \nmid m$. Then $\chi(G)$ is the subgroup $\langle \bar{q} \rangle \le (\mathbb{Z}/m\mathbb{Z})^*$.

Proof. $\mathrm{Gal}(L/K) = \langle \phi_q \rangle$ where $\phi_q(x) = x^q$, i.e. $\phi_q = \phi_p^n$, where ϕ_p is the Frobenius endomorphism, $\phi_q(\zeta) = \zeta^q$. So $\chi(\phi_q) = q \pmod{m}$. □

Theorem 13.3. Let $K = \mathbb{Q}$. Then $\mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/m\mathbb{Z})^*$ by χ. In particular,

$$[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(m) = |(\mathbb{Z}/m\mathbb{Z})^*|,$$

where ϕ is Euler's phi function, and $\Phi_m(X)$ is irreducible over $\mathbb{Q}$.

Lecture 18

Proof. We have to show that if $a \in \mathbb{N}$ with $\gcd(a, m) = 1$, then there exists $\sigma \in G$ with $\chi(\sigma) = \bar{a}$. It is enough to do this for $a = p$, p prime, since in the general case we can write $a = \prod p_i^{r_i}$.

Let f be the minimal polynomial of ζ over $\mathbb{Q}$, so $f(X) \mid \Phi_m(X)$, by Gauss's lemma $f \in \mathbb{Z}[X]$. Let $g \in \mathbb{Z}[X]$ be the minimal polynomial of ζ^p. Then $g(\zeta^p) = 0$ implies that $f(X) \mid g(X^p)$. Reducing modulo p, $\bar{f}(X) \mid \bar{g}(X^P) = \bar{g}(X)^p$. Now $\bar{f}$ divides $X^m - 1 \in \mathbb{F}_p[X]$ which is separable, so $\bar{f}(X) \mid \bar{g}(X)$, so $\bar{f}^2 \mid \bar{f}\bar{g}$. If $f \neq g$ then $fg \mid X^m - 1$, so $\bar{f}^2 \mid \bar{f}\bar{g} \mid X^m - 1$, contradicting that $X^m - 1$ is separable. So $f = g$, hence $f(\zeta^p) = 0$, so there exists $\sigma \in G$ such that $\sigma(\zeta) = \zeta^p$. □

We now present a second proof of the irreducibility of cyclotomic polynomials over $\mathbb{Q}$.

Proof. Suppose $m \geq 1$, ζ a primitive mth root of unity, $L = \mathbb{Q}(\zeta)$, and $G = \mathrm{Gal}(L/\mathbb{Q}) \hookrightarrow (\mathbb{Z}/m\mathbb{Z})^*$ such that $\sigma \mapsto a \bmod m$ if $\sigma(\zeta) = \zeta^a$.

It is sufficient to prove χ is surjective. Then $[L : \mathbb{Q}] = \phi(m) = \deg \Phi_m$, so Φ_m is irreducible. For this, it is sufficient to show $\mathrm{Im}(\chi) \ni p \bmod m$ for any prime p, $p \nmid m$.

Let $R = \mathbb{Z}[\zeta]$ as in the proof of Theorem 12.5; choose a prime ideal P of $\mathbb{Z}[\zeta]$ containing p, then $k = R/P = \mathbb{F}_p(\bar{\zeta})$, where $\bar{\zeta}$ is the image of ζ under $R \to k$, is a splitting field for $X^m - 1$ over $\mathbb{F}_p$. So its Galois group is generated by the Frobenius map $\phi\colon \bar{\zeta} \mapsto \bar{\zeta}^p$. So as in the proof of Theorem 12.5, $p \bmod m \in \mathrm{Im}(\chi)$. □

Applications

Construction of Regular Polygons by Ruler and Compass

To construct a regular n-gon is equivalent to constructing the real number $\cos \frac{2\pi}{n}$.

Theorem 13.4 (Gauss)**.** A regular n-gon is constructible if and only if n is a product of a power of 2 and distinct primes of the form $2^{2^k} + 1$.

Proof. Let $\zeta = e2\pi i/n$, so that $\cos \frac{2\pi}{n} = \frac{1}{2}(\zeta + \zeta^{-1})$. We will show that this number is constructible if and only if n has the form stated.

Since $[\mathbb{Q}(\zeta) : \mathbb{Q}(\cos \frac{2\pi}{n})] = 2$, then ζ is constructible if and only if $\cos \frac{2\pi}{n}$ is. Now if ζ is constructible, $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ must be a power of 2. Conversely, if $[\mathbb{Q}(\zeta) : \mathbb{Q}]$ is a power of 2, then since $G = \mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ is *abelian*, it is easy to see that one can find subgroups $G = H_0 \supset H_1 \supset \cdots \supset H_m = \{1\}$ such that $(H_s : H_{s+1}) = 2$. Then we get a chain of subfields

$$\mathbb{Q}(\zeta) = F_m \supset F_{m-1} \supset \cdots F_1 \supset F_0 = \mathbb{Q},$$

where $F_r = \mathbb{Q}(\zeta)^{H_r}$ and $[F_r : F_{r-1}] = 2$, hence ζ is constructible. That is, $\cos \frac{2\pi}{n}$ is constructible if and only if $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*|$ is a power of 2.

By the Chinese Remained Theorem, if $n = \prod p_i^{e_i}$ for distinct primes p_i and $e_i \geq 1$, then

$$\begin{aligned} \phi(n) = |(\mathbb{Z}/n\mathbb{Z})^*| &= \prod_i |(\mathbb{Z}/p_i^{e_i}\mathbb{Z})^*| \\ &= \prod_i p_i^{e_i} - p_i^{e_i - 1} \end{aligned}$$

$$= \prod_i p_i^{e_i-1}(p_i - 1).$$

If $p = 2$ then p^{e-1} is a power of 2. If p is an odd prime, then $p^{e-1}(p-1)$ is a power of 2 if and only if $e = 1$ and $p = 2^m + 1$ for some m. If $m = rs$ with $r, s > 1$, r odd, then $2^{rs} + 1 = (2^s + 1)(2^{(r-1)s} - 2^{(r-2)s} + \cdots - 2^s + 1)$ is not prime. So m must be a power of 2. □

Primes of the form $2^{2^k} + 1$ are called *Fermat primes*; $F_k = 2^{2^k} + 1$. $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65537$ are prime. Fermat guessed that F_k is prime for all $k \geq 1$. But 641 is a non-trivial factor of F_5, as shown by Euler in 1732. Not $k \geq 5$ is known for which F_k is prime.

Quadratic Reciprocity

Let p be an odd prime. The *Legendre symbol* for $a \in \mathbb{Z}$, $(a, p) = 1$ is

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{if } a \pmod p \text{ is a square} \\ -1 & \text{if } a \pmod p \text{ is a non-square} \end{cases}$$

Since $(\mathbb{Z}/p\mathbb{Z})^*$ is cyclic of order $p-1$, we can easily see the following.

- $(p-1)/2$ numbers between 1 and $p-1$ are squares, the others are non-squares.
- Euler's criterion,
$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod p,$$
in particular
$$\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2} = \begin{cases} +1 & \text{if } p \equiv 1 \pmod 4 \\ -1 & \text{if } p \equiv 3 \pmod 4 \end{cases}.$$
- $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Theorem 13.5 (Gauss, Quadratic Reciprocity Law)**.** Let $p \neq q$ be odd primes. Then

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \begin{cases} -1 & \text{if } p \equiv q \equiv 3 \pmod 4 \\ +1 & \text{otherwise} \end{cases}$$

Proof. Consider $f_q(X) = X^q - 1 \in \mathbb{F}_p[X]$, which has splitting field $L = \mathbb{F}_p(\zeta)$. When is $\mathrm{Gal}(f_q/\mathbb{F}_p)$ contained in A_q? We present two answers.

Firstly, if and only if $\mathrm{Disc}(f_q)$ is a square in $\mathbb{F}_p$. Since $f_q' = qX^{q-1}$ and the roots of f_q are $\{\zeta^i : 0 \leq i \leq q-1\}$, we have

$$\begin{aligned} \mathrm{Disc}(f_q) &= (-1)^{q(q-1)/2} \prod_{i=0}^{q-1} f_q'(\zeta^i) = (-1)^{(q-1)/2} \prod_{i=0}^{q-1} q\zeta^{i(q-1)} \\ &= (-1)^{(q-1)/2} q^q \zeta^{(q-1)/2(q-1)q} = (-1)^{(q-1)/2} q^q. \end{aligned}$$

Dividing out the square q^{q-1}, $\mathrm{Disc}(f_q)$ is a square in $\mathbb{F}_p^*$ if and only if $(-1)^{(q-1)/2}q$ is a square.

Secondly, if and only if the cycle type of ϕ_p acting on the roots $1, \zeta, \ldots, \zeta^{q-1}$ is even. $\phi_p(1) = 1$, $\phi_p(\zeta) = \zeta^p$. So we have one orbit of length 1 and $(q-1)/m$ orbits of length m the order of p in $\mathbb{F}_q^*$. So ϕ_p is even if and only if $(m-1)(q-1)/m$ is even if and only if $(q-1)/m$ is even if and only if p is a square in $\mathbb{F}_q^*$. □

Kummer Extensions

Consider $K(x)$ with $x^m \in K$.

Example. $\mathbb{Q}(\sqrt[3]{2})$. The splitting field of $X^3 - 2$ is $\mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$.

Suppose K is a field, $m \geq 1$, $\operatorname{char} K = 0$ or $\operatorname{char} K = p$ with $(p, m) = 1$. Assume K contains a primitive mth root of unity ζ.

Theorem 13.6. Let $L = K(x)$ where $x^m = a \in K^*$. Then L/K is a splitting field for $X^m - a$, so is Galois; $[L : K]$ is the least $d \geq 1$ such that $x^d \in K$ and $\operatorname{Gal}(L/K)$ is cyclic.

Proof. $X^m - a = X^m - x^m = \prod_{i=0}^{m-1}(X - \zeta^i x)$, so L/K is a splitting field for $f(X) = X^m - a$. As $f' = mX^{m-1}$, f is separable, so L/K is Galois.

Let $\sigma \in \operatorname{Gal}(L/K)$. Then $f(\sigma(x)) = 0$, so $\sigma(x) = \zeta^i x$ for some i. Put $\theta(\sigma) = \sigma(x)/x = \zeta^i \in \mu_m(K)$, which is cyclic of order m. This defines a map $\theta\colon \operatorname{Gal}(L/K) \to \mu_m(K) \cong \mathbb{Z}/m\mathbb{Z}$.

- θ is a homomorphism. $\sigma, \tau \in \operatorname{Gal}(L/K)$, $\sigma(x) = \zeta^i x$, $\tau(x) = \zeta^j x$. So $\sigma(\tau(x)) = \sigma(\zeta^j x) = \zeta^j \sigma(x) = \zeta^{i+j} x$, i.e. $\theta(\sigma\tau) = \theta(\sigma)\theta(\tau)$.
- θ is injective. If $\theta(\sigma) = 1$ then $\sigma(x) = x$, i.e. $\sigma = \iota$.

So θ is an isomorphism between $\operatorname{Gal}(L/K)$ and a subgroup of $\mu_m(K)$, so $\operatorname{Gal}(L/K)$ is cyclic. Finally, if $n \geq 1$, $x^n \in K$ if and only if for all σ, $\sigma(x^n) = x^n$. So $x^n \in K$ if and only if for all σ, $\theta(\sigma)^n = 1$, i.e., if and only if $\operatorname{Im}\theta \subset \mu_n(K)$. So $\operatorname{Im}\theta = \mu_d(K)$ where d is the least integer such that $x^d \in K$. □

Corollary 13.7. $X^m - a$ is irreducible in $K[X]$ if and only if a is not a dth power in K for any $d \mid m$, $d \neq 1$.

Proof. Let $L = K(x)$, $x^m = a$. Then $X^m - a$ is irreducible if and only if $[L : K] = m$ if and only if $x^{m/d} \notin K$ for any $d \mid m$, $d \neq 1$ if and only if a is not a dth power. □

Theorem 13.8. Let K be as above, i.e., $\zeta \in K$ a primitive mth root of unity. Suppose L/K is Galois of degree m, with cyclic Galois group. Then $L = K(x)$ for some x with $x^m = a \in K$.

Proof. Let $G = \operatorname{Gal}(L/K) = \{\sigma^i : 0 \leq i \leq m-1\}$. Let $y \in L$ and consider the *Lagrange resolvent*

$$x = R(y) = y + \zeta^{-1}\sigma(y) + \cdots + \sigma^{-(m-1)}\sigma^{m-1}(y)$$

Then

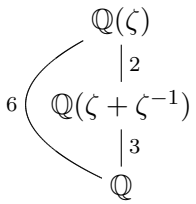
$$\begin{aligned}\sigma(x) &= \sigma(y) + \zeta^{-1}\sigma^2(y) + \cdots + \zeta^{-m+1}\sigma^m(y)\\ &= \zeta x\end{aligned}$$

$$\therefore \quad \sigma(x^m) = \sigma(x)^m = x^m$$

i.e. $a = x^m \in K$. By Theorem 9.1 (Independence of Field Automorphisms), there exists $y \in L$ such that $x = R(y) \neq 0$. For this choice, we have $\sigma^i(x) = \zeta^i x \neq x$ if $0 < i < m$, so $L = K(x)$ (e.g. since $\prod_i (X - \sigma^i(x))$ is irreducible by the transitivity of $\mathrm{Gal}(L/K)$ on the roots). □

If K does not contain a primitive mth root of unity, these all fail in various ways.

For example, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is not Galois, but there exist other Galois extensions of $\mathbb{Q}$ of degree 3, e.g. $\mathbb{Q}(\cos\frac{2\pi}{7}) = \mathbb{Q}(\zeta + \zeta^{-1})$ where $\zeta = e^{2\pi/7}$.



where $\mathrm{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q}) = \mathbb{F}_7^* \cong \mathbb{Z}/6\mathbb{Z}$.

Corollary 13.7 also fails, e.g. $X^4 + 4 \in \mathbb{Q}[X]$ is reducible, although -4 is not a square in $\mathbb{Q}$.

Chapter 14

Trace and Norm

Let L/K be finite of degree n. Then L is a K-vector space of dimension n. If $x \in L$, the map

$$T_x \colon L \to L, T_x(y) = xy$$

is a K-linear map.

Definition. The *trace* and *norm* of x are

$$\mathrm{Tr}_{L/K}(x) = \mathrm{tr}(T_x), \quad N_{L/K}(x) = \det(T_x).$$

The *characteristic polynomial* $f_{x,L/K}$ of x is the characteristic polynomial of T_x.

Explicitly, choose a basis $e_1, \ldots, e_n$ for L/K. Then there exists a unique matrix (a_{ij}) with entries in K such that $xe_j = \sum_{i=1}^n a_{ij}e_i$ for all j and then

$$\begin{aligned} \mathrm{Tr}_{L/K}(x) &= \sum_{i=1}^n a_{ii} \\ N_{L/K}(x) &= \det(a_{ij}) \\ f_{x,L/K} &= \det(IX - (a_{ij})) \end{aligned}$$

Example. Let $L = K(y), y^2 = d \in K, y \notin K$. Taking the basis to be $\{1, y\}$, let $x = a + by$. The matrix of T_x is

$$\begin{pmatrix} a & bd \\ b & a \end{pmatrix}$$

since $xy = ay + by^2 = bd + ay$, so $\mathrm{Tr}_{L/K}(x) = 2a$, $N_{L/K}(x) = a^2 - db^2$.

Lemma 14.1. If $x, y \in L, a \in K$, then

(i) $\mathrm{Tr}_{L/K}(x+y) = \mathrm{Tr}_{L/K}(x) + \mathrm{Tr}_{L/K}(y)$, $N_{L/K}(xy) = N_{L/K}(x)N_{L/K}(y)$.
(ii) $N_{L/K}(x) = 0$ if and only if $x = 0$.
(iii) $\mathrm{Tr}_{L/K}(ax) = a\,\mathrm{Tr}_{L/K}(x)$, $N_{L/K}(ax) = a^{[L:K]}N_{L/K}(x)$.

So $T_{L/K} \colon L \to K$ is a homomorphism of additive groups, $N_{L/K} \colon L^* \to K^*$ is an injective homomorphism of multiplicative groups.

Proof. (i) This follows from $\mathrm{tr}(A+B) = \mathrm{tr}\,A + \mathrm{tr}\,B$, $\det(AB) = \det(A)\det(B)$, since clearly $T_{x+y} = T_x + T_y$, $T_{xy} = T_xT_y$.
(ii) T_x is invertible if and only if $x \in L^*$.

(iii) $T_{ax} = aT_x$. □

Proposition 14.2. Suppose $L = K(x)$, and let $f(X) = X^n + c_{n-1}X^{n-1} + \cdots + c_1X + c_0$ be the minimal polynomial of x over K. Then $f_{x,L/K} = f$, and $\mathrm{Tr}_{L/K}(x) = -c_{n-1}$, $N_{L/K}(x) = (-1)^n c_0$.

Proof. Consider the basis $\{1, x, \ldots, x^{n-1}\}$ for L/K. In terms of this basis, T_x has matrix

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & 0 & -c_0 \\ 1 & 0 & & 0 & 0 & -c_1 \\ 0 & 1 & & 0 & 0 & -c_2 \\ & & \ddots & & & \\ 0 & 0 & & 1 & 0 & -c_{n-2} \\ 0 & 0 & \ldots & 0 & 1 & -c_{n-1} \end{pmatrix}$$

which has characteristic polynomial f. So $f_{x,L/K} = f$; as $\det(T_x) = (-1)^n c_0$, $\mathrm{tr}(T_x) = -c_{n-1}$, the rest follows. □

Example. Let K have characteristic $p > 0$, $L = K(x)$ where $x^p \in K, x \notin K$. So $[L : k] = p$.

Let $y \in L$. Then if $y \in K$, $N_{L/K}(y) = y^{[L:K]} = y^p$, $\mathrm{Tr}_{L/K}(y) = [L : K]y = 0$. On the other hand, if $y \not/nK$, then $y = \sum b_i x^i$, $y^p = \sum b_i^p (x^p)^i \in K$, so $L = K(y)$ and y has minimal polynomial $X^p - y^p$, so $N_{L/K}(y) = y^p$ and $\mathrm{Tr}_{L/K}(y) = 0$. So in every case $\mathrm{Tr}_{L/K}(y) = 0$, i.e. $\mathrm{Tr}_{L/K}$ is the zero map.

For which extensions is L/K is $\mathrm{Tr}_{L/K}$ non-zero? Since $\mathrm{Tr}_{L/K} \colon L \to K$ is K-linear, either $\mathrm{Tr}_{L/K} = 0$ or $\mathrm{Tr}_{L/K}(L) = K$.

Proposition 14.3. Suppose L/K is finite of degree n, M a normal closure of L/K. Assume there exists n distinct K-embeddings $\sigma_1, \ldots, \sigma_n \colon L \hookrightarrow M$. Then for all $x \in L$,

$$\mathrm{Tr}_{L/K}(x) = \sum_{i=1}^{n} \sigma_i(x), \quad N_{L/K}(x) = \prod_{i=1}^{n} \sigma_i(x).$$

The condition on L/K holds if for example $L = K(y)$ with y separable over K, M a splitting field of the minimal polynomial of y.

Proof. Let $\{e_1, \ldots, e_n\}$ be a basis for L/K. Then the matrix $P = (\sigma_i(e_j))$ is non-singular since its rows are linear independent over K, by Theorem 9.1 (Independence of Field Automorphisms). Let $A = (a_{ij})$, $a_{ij} \in K$, be the matrix of T_x. So

$$T_x e_j = x e_j = \sum_{r=1}^{n} a_{rj} e_r$$

$$\therefore \quad \sigma_i(x)\sigma_i(e_j) = \sum_{r=1}^{n} \sigma_i(e_r) a_{rj}$$

$$SP = PA$$

where $S = \mathrm{diag}\{\sigma_i(x)\}$. So $PAP^{-1} = S$, i.e. P diagonalises A. So $\{\sigma_i(x)\}$ are the eigenvalues of A, hence the result. □

Lecture 21

Theorem 14.4. Let $M/L/K$ be finite. Then for all $x \in M$,

$$\mathrm{Tr}_{M/K}(x) = \mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(x)), \quad N_{M/K}(x) = N_{L/K}(N_{M/L}(x))$$

Proof. We consider the trace only.

Choose bases $\{u_1, \ldots, u_m\}$ for M/L, $\{v_1, \ldots, v_n\}$ for L/K. Let the matrix for $T_{x,M/L}$ be (a_{ij}) with $a_{ij} \in L$, so $\mathrm{Tr}_{M/L}(x) = \sum_{i=1}^m a_{ii}$. For each (i,j) let A_{ij} be the matrix of $T_{a_{ij},L/K}$, so

$$\mathrm{Tr}_{L/K}(\mathrm{Tr}_{M/L}(x)) = \sum_{i=1}^m \mathrm{Tr}_{L/K}(a_{ii}) = \sum_{i=1}^m \mathrm{tr}(A_{ii}).$$

In terms of the basis $\{u_1v_1, \ldots, u_1v_n, u_2v_1, \ldots, u_2v_n, \ldots, u_mv_n\}$ for M/K, the matrix of $T_{x,M/K}$ is

$$\begin{pmatrix} A_{11} & \ldots & A_{1m} \\ \vdots & & \vdots \\ A_{m1} & \ldots & A_{mm} \end{pmatrix}$$

whose trace is $\sum_{i=1}^m \mathrm{tr}\, A_{ii}$. □

Theorem 14.5. Let L/K be finite.

(i) Suppose $L = K(x)$ where x separable over K. Then $\mathrm{Tr}_{L/K}$ is surjective.
(ii) Suppose $\mathrm{Tr}_{L/K}$ is surjective. Then L/K is separable.

Proof. (i) The case $x = 0$ is trivial. Assume $x \neq 0$, let $n = [L : K]$. Let $x_1, \ldots, x_n$ be the K-conjugates of x (in some splitting field). We want to find $k \geq 0$ such that

$$\mathrm{Tr}_{L/K}(x^k) = x_1^k + \cdots + x_n^k \neq 0$$

by Proposition 14.3. Recall from the proof of Newton's Formula that if $f(T) = \prod_i (1 - x_i T)$, then

$$\frac{f'(T)}{f(T)} = -T^{-1} \sum_{k=1}^{\infty} p_k T^k$$

where $p_k = x_1^k + \cdots + x_n^k$. Now f is separable, since $x_1, \ldots, x_n$ are distinct and non-zero, so the LHS is non-zero, hence there exists k with $p_k \neq 0$.

(ii) It suffices to prove that if L/K is inseparable then $\mathrm{Tr}_{L/K} = 0$. So let $p = \mathrm{char}\, K > 0$. Let $x \in L$ be inseparable over K; its minimal polynomial is of the form $g(X^p)$ where $g(X) \in K[X]$ is irreducible. So the minimal polynomial of x^p over K is $g(X)$, hence $L \supset K(x) \supset K(x^p) \supset K$ with $[K(x) : K(x^p)] = p$. As shown in the Example after Proposition 14.2, $\mathrm{Tr}_{K(x)/K(x^p)} = 0$. So by Theorem 14.4,

$$\mathrm{Tr}_{L/K}(y) = \mathrm{Tr}_{K(x^p)/K}(\mathrm{Tr}_{K(x)/K(x^p)}(\mathrm{Tr}_{L/K(x)}(y))) = 0.$$ □

Corollary 14.6. A finite extension L/K is separable if and only if $\mathrm{Tr}_{L/K}$ is non-zero.

Corollary 14.7. (i) Let $M/L/K$ be finite. Then M/K is separable if and only if M/L and L/K are separable.

(ii) Let $L = K(x_1, \ldots, x_n)$ be finite over K. Then L/K is separable if and only if $x_1, \ldots, x_n$ are separable over K.

Proof. (i) $\mathrm{Tr}_{M/K} = \mathrm{Tr}_{L/K} = \mathrm{Tr}_{M/L}$, so this follows from Corollary 14.6.

(ii) One direction is clear by definition. To prove the converse by induction, we may assume $K' = K(x_1, \ldots, x_{n-1})$ is separable over K. Then $L = K'(x_n)$ is separable over K' by Theorem 14.5 since x_n is separable over K'. Then conclude by (i). □

Chapter 15

Solving Equations by Radicals

We consider the following problem. Given a polynomial $f(X) \in \mathbb{Q}[X]$, say, try to find a formula for roots of $f(X)$, involving fields operations and nth roots.

Definition. (i) L/K is an *extension by radicals* if there exists extensions $K = K_0 \subset K_1 \subset \cdots \subset K_r = L$ such that $K_i = K_{i-1}(x_i)$ with $x_i^m \in K_{i-1}$ for some $m \geq 1$ for $i = 1, \ldots, r$. (Taking m to be the least common multiple, we may assume m is the same for all i. Notice that if $m = 2$ we would have a constructible extension.)

(ii) Let $f \in K[X]$. f is *soluble*, or *solvable*, by radicals if there exists an extension by radicals L/K in which f splits into linear factors.

Lemma 15.1. Let M/L, L/K be extensions by radicals. Then M/K is an extension by radicals.

Small Degrees

Degree 2

Suppose $\deg f = 2$, $f(X) = X^2 + aX + b$, $a, b \in K$.

If f is reducible, there is nothing to do. Otherwise, f has discriminant $a^2 - 4b = \mathrm{Disc}(f)$. If $\mathrm{Disc}(f) \neq 0$ then f is separable, and the splitting field of f is just $K(\sqrt{a^2 - 4b})$, which is an extension by radicals (here $\mathrm{char}\, K \neq 2$). If $\mathrm{Disc}(f) = 0$ then either f is reducible or f is irreducible and inseparable in which case $f(X) = (X + \alpha)^2$ where $\alpha \in K$ (here $\mathrm{char}\, K = 2$). (The difficult case is when $\mathrm{char}\, K = 2$ and f is irreducible and separable, since if $\mathrm{char}\, K = 2$ and L/K is a separable extension of degree 2, then $L \neq K(\sqrt{\beta})$ for any $\beta \in K$ since $K(\sqrt{\beta})$ is inseparable.)

Degree 3

Assume $\mathrm{char}\, K \neq 2, 3$, $f(X) = X^3 + aX^2 + bX + c$. Replacing X by $X - \frac{1}{3}a$, we can assume $a = 0$, $f(X) = X^3 + bX + c$.

If K does not contain a primitive cube root of unity, replace K by $K(\omega)$ where $\omega \neq 1 = \omega^3$, so $\omega^2 + \omega + 1 = 0$, as $\mathrm{char}\, K \neq 2$, $K(\omega)/K$ is an extension by radicals ($K(\omega) = K(\sqrt{-3})$). So without loss of generality, we may assume $\omega \in K$. Let L be a splitting field for f over K.

If f is reducible over K then we can find all roots of f by solving a quadratic over K, hence we have solutions by radicals.

Assume f is irreducible. Then $\mathrm{Gal}(f/K)$ is A_3 or S_3. Write $f(X) = \prod_i (X - x_i)$, $\Delta = (x_1 - x_2)(x_1 - x_3)(x_2 - x_3)$, so $\Delta^2 = \mathrm{Disc}(f) \in K^*$; then $\mathrm{Disc}(f)$ is a square in K if and only if $\mathrm{Gal}(f/K) = A_3$, so if $K_1 = K(\Delta)$ then $\mathrm{Gal}(L/K_1) = A_3$ (and $K_1 = K$ if and only if $\mathrm{Gal}(f/K) = A_3$). But A_3 is cyclic, and $\omega \in K_1$. Theorem 13.6 then says that $L = K_1(\sqrt[3]{d})$ for some $d \in K_1$. So $L = K_1(\sqrt[3]{d}) \supset K_1 = K(\Delta) \supset K$ is an extension by radicals in which f splits.

We can compute the solutions explicitly as follows.

(i) Suppose $b = 0 \neq c$, $f = X^3 + c$. Then if $\omega \in K$, $L = K(\sqrt[3]{c})$ since f factorises as $f = (X + \sqrt[3]{c})(X + \omega\sqrt[3]{c})(X + \omega^2\sqrt[3]{c})$. If $\omega \notin K$, $L = K(\omega, \sqrt[3]{c})$.

(ii) Suppose $b \neq 0$. Then if $\omega \in K$, we know by the proof of Theorem 13.6 that $\sqrt[3]{d} = z + \omega\sigma(z) + \omega^2\sigma^2(z)$ for some $z \in L$ where $\{1, \sigma, \sigma^2\} = A_3 = \mathrm{Gal}(L/K_1)$. So consider $\{z, \sigma(z), \sigma^2(z)\} = \{x_1, x_2, x_3\}$ roots of f and let $y = x_1 + \omega^2 x_2 + \omega x_3$, so $y^3 \in K$. We know that $x_1 + x_2 + x_3 = a = 0$, so $y = (1 - \omega)(x_1 - \omega x_2)$. Let

$$\begin{aligned} y' &= x_1 + \omega x_2 + \omega^2 x_3 = (1 - \omega^2)(x_1 - \omega^2 x_2) \\ yy' &= (1 - \omega)(1 - \omega^2)(x_1 - \omega x_2)(x_1 - \omega^2 x_2) \\ &= 3(x_1^2 + x_2^2 + x_1 x_2) \\ &= -3b \end{aligned}$$

as $b = x_1 x2 + x_1 x_3 + x_2 x_3 = -x_1^2 - x_2^2 - x_1 x_2$. Therefore, $y' = -3b/y$, $y, y' \neq 0$.

$$\begin{aligned} y + y' &= y + y' + (x_1 + x_2 + x_3) \\ &= 3x_1 \end{aligned}$$

because $1 + \omega + \omega^2 = 0$. So $L = K_1(y)$ since $y \neq 0$ (see the proof of Theorem 13.8),

$$x_1 = \frac{1}{3}(y + y') = \frac{1}{3}\left((y - \frac{3b}{y}\right)$$

Finally,

$$\begin{aligned} y^3 &= (1 - \omega)^3 (x_1 - \omega x_2)^3 \\ &= \frac{1}{2}(-3\sqrt{-3}\Delta + 27c) \in K_1 \end{aligned}$$

using $\omega = (-1 + \sqrt{-3})/2$ and

$$\begin{aligned} \Delta &= (x_1 - x_2)(x_1 - x_3)(x_2 - x_3) \\ &= 2x_1^3 + 3x_1^2 x_2 - 3x_1 x_2^2 - 2x_2^3 \\ \Delta^2 &= -4b^3 - 27c^2. \end{aligned}$$

Theorem 15.2 (Ruffini, Abel's Theorem)**.** The general equation of degree 5 or more cannot be solved by radicals.

Definition. Let G be a finite group. Then G is *soluble*, or *solvable*, if there exists a chain of subgroups $\{1\} = H_r \lhd H_{r-1} \lhd \cdots \lhd H_1 \lhd H_0 = G$ such that H_i/H_{i+1} is cyclic, for $0 \leq i < r$.

Lecture 23

Remark. Here is an equivalent definition. G is soluble if there exists a chain of subgroups, each normal in G, $\{1\} = N_s < N_{s-1} < \cdots < N_1 < N_0 = G$ such that N_i/N_{i+1} is abelian, for $0 \le i < s$. (The proof of this statement uses commutator subgroups.)

Proposition 15.3. (i) If G is soluble, then so is any subgroup and any quotient group of G.
(ii) If $N \lhd G$ and $N, G/N$ are soluble, then so is G.

Proof. (i) Let $K < G$ be a subgroup. Suppose we have subgroups $H_i \subset G$ as in the definition of a soluble group. Consider $\{K \cap H_i\}$. Then $K \cap H_{i+1} \lhd K \cap H_i$ since it is the kernel of the map $K \cap H_i \to H_i/H_{i+1}$, so $(K \cap H_i)/(K \cap H_{i+1}) < H_i/H_{i+1}$ is cyclic.
Let $N \lhd G$; then consider the subgroups

$$\bar{G} = G/N > (H_iN)/N = \bar{H}_i \cong H_i/(N \cap H_i),$$

so

$$\bar{H}_i/\bar{H}_{i+1} \cong (H_iN)/(H_{i+1}N) \cong H_i/(H_i \cap H_{i+1}N)$$

is a quotient of H_i/H_{i+1}, hence is cyclic and (i) follows.
(ii) Suppose $N, G/N$ are soluble,

$$\{1\} = H_r \lhd H_{r-1} \lhd \cdots \lhd H_0 = N,$$
$$\{1\} = \bar{K}_s \lhd \bar{K}_{s-1} \lhd \cdots \lhd \bar{K}_0 = \bar{G} = G/N$$

So $\bar{K}_i = K_i/N$ for some subgroup $K_i < G$ containing N and $K_{i+1} \lhd K_i$, $K_0 = G$, $K_s = N$, $K_i/K_{i+1} \cong \bar{K}_i/\bar{K}_{i+1}$. Therefore, we have the chain of subgroups

$$\{1\} = H_r \lhd H_{r-1} \lhd \cdots \lhd H_0 = N = K_s \lhd K_{s-1} \lhd \cdots \lhd K_0 = G$$

showing that G is soluble. □

Example. (i) Any finite abelian group is soluble.
(ii) S_3 is soluble, $\{1\} \lhd A_3 \lhd S_3$.
(iii) S_4 is soluble. $\{1\} \lhd \langle (12)(34) \rangle \lhd V_4 = \langle (12)(34), (13)(24), (14)(23) \rangle \lhd A_4 \lhd S_4$ where $A_4/V_4 \cong \mathbb{Z}/3\mathbb{Z}$.
(iv) S_n or A_n are *not* soluble if $n \ge 5$. In fact, A_5 has no non-trivial normal subgroup, A_5 is simple so cannot be soluble, hence by (i) neither are S_n, A_n for $n \ge 5$.

Theorem 15.4. Let K be a field with $\operatorname{char} K = 0$ and $f \in K[X]$. Then f is soluble by radicals over K if and only if $\operatorname{Gal}(f/K)$ is a soluble group.

Corollary 15.5. If $\deg f \ge 5$ and $\operatorname{Gal}(f/K) = A_5$ then f is not soluble by radicals.

For the proof of Theorem 15.4 we need the following lemma.

Lemma 15.6. Let L/K be an extension by radicals, and M/K a Galois closure of L/K. Then M/K is also an extension by radicals. (If $L = K(x)$, then M is the splitting field of the minimal polynomial of x over K, containing L.)

Proof. $L = K_r \supset K_{r-1} \supset \cdots \supset K_0 = K$ where $K_i = K_{i-1}(x_i)$, $x_i^m \in K_{i-1}$ for all $i = 1, \ldots, r$. Let $G = \operatorname{Gal}(M/K)$. Let us define $M_0 = K$, and inductively for $1 \le i \le r$, $M_i = M_{i-1}(\{\sigma(x_i) : \sigma \in G\})$. Then

- $M_i \supset K_i$, clear.
- M_i/K is Galois, clear.
- M_i/M_{i-1} is an extension by radicals: $\sigma(x_i)^m = \sigma(x_i^m) \in \sigma(K_{i-1}) \subset M_{i-1}$ as M_{i-1}/K is Galois (hence normal since $\operatorname{char} K = 0$), so M_i/M_{i-1} is an extension by radicals.

Therefore, M/K is an extension by radicals. □

Proof (of Theorem 15.4). Assume $\mathrm{Gal}(f/K)$ is soluble. Let L be the splitting field for f over K, $G = \mathrm{Gal}(L/K)$, $m = |G|$.

Suppose first that K contains a primitive mth root of unity. Then we have $\{1\} = H_r \lhd H_{r-1} \lhd \cdots \lhd H_0 = G$ with H_i/H_{i+1} cyclic of order dividing m. Let $K_i = L^{H_i}$. Then by the Fundamental Theory of Galois Theory, $L = K_r \supset K_{r-1} \supset \cdots \supset K_0 = K$ and each K_{i+1}/K_i is Galois with Galois group H_i/H_{i+1}. So by Theorem 13.6, $K_{i+1} = K_i(x_i)$ where $x_{i+1}^m \in K_i$ (as $\zeta_m \in K$). So L/K is an extension by radicals.

In general, let $K' = K(\zeta_m)$ where ζ_m is a primitive mth root of unity, i.e. K' is the splitting field for $X^m - 1$, $m = |\mathrm{Gal}(L/K)|$. Then the Galois group $\mathrm{Gal}(f/K')$ is a subgroup of $\mathrm{Gal}(f/K)$, so by the above, $L' = L(\zeta_m)$ is an extension by radicals of K'. But K'/K is an extension by radicals, hence L'/K is an extension by radicals in which f splits.

Now assume f is soluble by radicals over K. Then by definition of solubility by radicals and by Lemma 15.6, there exists a finite Galois extension L/K which is an extension by radicals and in which f splits, so $\mathrm{Gal}(f/K)$ is a quotient of $\mathrm{Gal}(L/K)$.

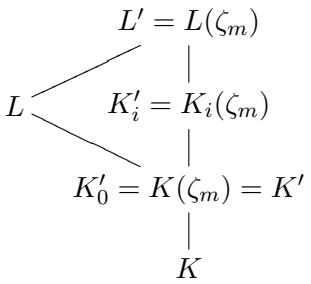
So it is sufficient to prove $\mathrm{Gal}(L/K)$ is soluble. Say

$$L = K_r \supset \cdots \supset K_1 \supset K_0 = K,$$

$K_i = K_{i-1}(x_i)$, $x_i^m \in K_{i-1}$.

Suppose $\zeta_m \in K$. Then by Theorem 13.6, K_i/K_{i-1} is Galois with cyclic Galois group, so if $H_i = \mathrm{Gal}(L/K_i)$, then $\{H_i\}$ gives solubility of $\mathrm{Gal}(L/K)$.

In general, we have



ζ_m is a primitive mth root of unity. $\mathrm{Gal}(L'/K')$ is soluble by the previous argument, as K_i'/K_{i-1}' has a cyclic Galois group, $\mathrm{Gal}(K'/K)$ is abelian, so soluble, then by Proposition 15.3 (ii), $\mathrm{Gal}(L'/K)$ is soluble, so by Proposition 15.3 (i), $\mathrm{Gal}(L/K)$ is soluble. □

Degree 4

Consider an irreducible quartic $f \in K[X]$, where $\operatorname{char} K \neq 2, 3$. We can solve f by radicals.

Lecture 24

Let L be the splitting field of f over K, $G = \mathrm{Gal}(L/K) = \mathrm{Gal}(f/K) \subset S_4$. Write $f(X) = \prod_{i=1}^4 (X - x_i)$, $x_i \in L$.

S_4 is soluble. Consider the three partitions $a = \{12\}\{(34\}$, $b = \{13\}\{24\}$, $c = \{14\}\{23\}$ of $\{1, 2, 3, 4\}$ into two subsets of size 2. These are permuted by S_4, e.g. $(12) \mapsto (b, c)$, giving a homomorphism $\pi\colon S_4 \to S_3$, which is surjective, e.g. since it contains all 2-cycles, and its kernel is $V_4 = \{\iota, (12)(34), (13)(24), (14)(23)\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Therefore, $S_4/V_4 \cong S_3$.

$$\begin{array}{c} L \\ | \\ L^{G \cap V_4} = F \\ | \\ K \end{array}$$

By the Fundamental Theorem of Galois Theory,

- L/F is Galois, $\mathrm{Gal}(L/F) = V \cap G \subset V$;
- F/K is Galois, $\mathrm{Gal}(F/K) = G/(G \cap V) \cong \pi(G) \subset S_3$.

We can write F/K explicitly as the splitting field of a certain cubic, in fact in various ways.

Example. Suppose $f(X) = X^4 + aX^2 + bX + c$, after removing the X^3 term by substituting $X \mapsto X + a$. Then $x_1 + x_2 + x_3 + x_4 = 0$. Let $y_{ij} = x_i + x_j$, i.e.

$$\begin{aligned} y_{12} &= x_1 + x_2 = -(x_3 + x_4) = -y_{34} \\ y_{23} &= -y_{14} \\ y_{13} &= -y_{24} \end{aligned}$$

G permutes the six quantities y_{ij}, so permutes $\{y_{12}^2, y_{13}^2, y_{23}^2\}$. So if $g(T) = (T - y_{12}^2)(T - y_{13}^2)(T - y_{23}^2)$, then $g \in L^G[T] = K[T]$.

What is the Galois group G? Suppose $\sigma \in G \cap V$. Then as σ fixes the partitions $\{12\}\{34\}$ etc., $\sigma(y_{ij}) = \pm y_{ij}$, so $\sigma(y_{ij}^2) = y_{ij}^2$, i.e. $y_{ij}^2 \in F$. Conversely, it is easy to see that since $y_{12}^2, y_{23}^2, y_{13}^2$ are distinct, if $\sigma \in G$ fixes each y_{ij}^2 then it fixes the partitions, i.e. $\sigma \in G \cap V$, i.e. $F = K(y_{12}^2, y_{23}^2, y_{13}^2)$.

$$\begin{aligned} y_{12}^2 - y_{13}^2 &= -(x_1 + x_2)(x_3 + x_4) + (x_1 + x_3)(x_2 + x_4) \\ &= x_1x_2 + x_3x_4 - x_1x_3 - x_2x_4 \\ &= (x_1 - x_4)(x_2 - x_3) \neq 0 \end{aligned}$$

and similarly for all other pairs.

A simple calculation gives $g(T) = T^3 + 2aT^2 + (a^2 - 4c)T - b^2$, and $y_{12}y_{13}y_{23} = b$. So $F = K(y_{12}^2, y_{13}^2)$. Now $x_1 = \frac{1}{2}(y_{12} + y_{13} - y_{23})$ etc., so $L = K(y_{12}, y_{13})$, $y_{12}^2, y_{13}^2 \in F$ and we can explicitly solve f (after first solving g) by radicals.

Here is an alternative way. (This works for any quartic, without the assumption that the coefficient of X^3 is zero.) Consider instead

$$\begin{aligned} z_{12} &= x_1x_2 + x_3x_4 \\ z_{13} &= x_1x_3 + x_2x_4 \\ z_{23} &= x_2x_3 + x_1x_4 \end{aligned}$$

as the three quantities permuted by G.

$$\begin{aligned} z_{12} - z_{13} &= x_1x_2 - x_1x_3 + x_3x_4 - x_2x_4 \\ &= (x_1 - x_4)(x_2 - x_3) \neq 0 \end{aligned}$$

The same argument shows $F = K(z_{12}, z_{13}, z_{23})$ and $\{z_{ij}\}$ are the roots of a cubic over K, call it h. (g, h are called *resolvent cubics*.)

The advantage of using h is that we do not require the coefficient of X^3 to be zero. However, given z_{ij}, the formulae for x_i are not quite as simple.

Consider

$$\begin{array}{c} L \\ | \\ L^{G\cap V_4} = F \\ | \\ K \end{array}$$

where F is the splitting field of g (or h). From this, it follows that $G \subset V_4$ if and only if $F = K$ if and only if the resolvent cubic splits into linear factors over K.

Suppose the resolvent cubic is irreducible. Then $3 \mid |\mathrm{Gal}(f/K)|$, so $3 \mid |G|$; as $G \subset S_4$ is transitive, $4 \mid |G|$ by the Orbit-Stabiliser Theorem, so $12 \mid |G|$, so G is A_4 or S_4.

If the resolvent cubic has one root in K, $[F : K] = 2$, so $|G| = 2|G \cap V|$, so $|G| \mid 8$, i.e. G is a subset of a conjugate of the dihedral group D_4 of order 8 (2-Sylow subgroup of S_4).

Computing a Galois Group

Given a monic polynomial $f(X) \in \mathbb{Z}[X]$, say, how do we find $\mathrm{Gal}(f/\mathbb{Q})$?

If you expect the Galois group to be A_n or S_n, where $n = \deg f$,

- compute $\mathrm{Disc}(f)$ to see whether it is a square;
- compute $f \bmod p$ for lots of primes p to try to force the Galois group to be A_n or S_n.

For example, if $\deg f = l$ prime and there exists p such that $f \bmod p$ is irreducible, then $\mathrm{Gal}(f/\mathbb{Q})$ contains an l-cycle. If it also contains a transposition, then $\mathrm{Gal}(f/\mathbb{Q}) = S_l$.

Algorithms

Let $f(X) = \prod_{i=1}^{n}(X - x_i) \in \mathbb{Q}[X]$, $G \subset S_n$. Consider $H \subset S_n$, and $P(X_1, \ldots, X_n) \in \mathbb{Q}[X_1, \ldots, X_n]^H$.

To illustrate this, take $H = A_n$, $P = \Delta$, and if $n = 4$ then $H = D_4 = \langle (1234), (12)(34) \rangle$, $P = X_1X_3 + X_2X_4$.

Then form

$$\begin{aligned} g(Y) &= \prod_{\sigma \in S_n/H} (Y - \sigma P(x_1, \ldots, x_n)) \\ &= \prod_{\sigma \in S_n} (Y - \sigma P(x_1, \ldots, x_n))^{\frac{1}{|H|}} \end{aligned}$$

where in the first line we consider the coset representations of H in G.

Then $P \in \mathbb{Q}[Y]$ — in the example above, we have $Y^2 - \mathrm{Disc}(f)$ or the resolvent cubic h respectively — and P has a simple root in $\mathbb{Q}$ if and only if $G \subset H$ (up to conjugacy).

- List all transitive $H \subset S_n$;
- find some invariant polynomials P;
- compute the resolvents g (numerically: find $x_i \in \mathbb{C}$ approximately);
- find if g has a rational root.