Galois Theory

May 30, 2024

Contents

0 Introduction **3**

1 Field Extensions **4**

2 Ruler and Compass Constructions **14**

3 Splitting Fields **16**

4 Symmetric Polynomials **24**

5 Normal and separable extensions **28**
5.1 Separability 28

6 Galois Extensions **35**

7 Trace and Norm **45**

8 Finite Fields **51**

9 The Galois Group of a Polynomial **54**

10 Cyclotomic and Kummer extensions **62**
10.1 Kummer Theory 66

11 Algebraic Closure **72**

12 Artin's Theorem **76**

Index **80**

Lectures

Lecture 1
Lecture 2
Lecture 3
Lecture 4
Lecture 5
Lecture 6
Lecture 7
Lecture 8
Lecture 9
Lecture 10
Lecture 11
Lecture 12
Lecture 13
Lecture 14
Lecture 15
Lecture 16
Lecture 17
Lecture 18
Lecture 19
Lecture 20
Lecture 21
Lecture 22
Lecture 23
Lecture 24

Start of

lecture 1

0 Introduction

Galois Theory is named after the French mathematician Evariste Galois (1811-1832). It is the study of roots of polynomials (or more generally field extensions).

It can be used to show that certain classical problems cannot be solved – for example there is no formula (in terms of radicals) for the roots of a general polynomial of degree n when $n \geq 5$. (Radicals means $+$, $-$, $\times$, $\div$, $\sqrt[m]{}$). This is related to the fact that the alternating group A_n is simple for $n \geq 5$.

More positively, Galois theory is foundational to the study of Algebraic Number Theory and Algebraic Geometry.

Prerequisites: Linear Algebra and GRM

1 Field Extensions

Definition (Field)**.** A *field* K is a ring (commutative with a 1, with $0_K \neq 1_K$) in which every non-zero element has an inverse under $\times$.

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

Then K contains a smallest subfield (called its prime subfield) which is isomorphic to $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ if K has characteristic p, and to $\mathbb{Q}$ if it has characteristic 0.

Lemma 1.1. Let K be a field and $0 \neq f \in K[X]$. Then f has $\leq \deg f$ roots in K.

Proof. By induction on $n = \deg f$. If f has no roots then there is nothing to prove.

Otherwise let $a \in K$ be a root of f. Then $f(X) = (X - a)g(X)$ with $g \in K[X]$, where $\deg g = n - 1$. If $b \in K$ is a root of f, then either $b = a$ or $g(b) = 0$. Therefore

$$\begin{aligned} |\{\text{roots of } f \text{ in } K\}| &\leq 1 + |\{\text{roots of } g \text{ in K}\}| \\ &\leq 1 + (n-1) && \text{(by induction)} \\ &= n \end{aligned}$$

□

Definition (Field extension)**.** Let L be a field and $K \subset L$ a subfield (i.e. a subset which is a field under the same operations $+$ and $\times$).

We say L is an *extension* of K, written L/K.

We note that L and K necessarily have the same characteristic.

Example.

(i) $\mathbb{C}/\mathbb{R}$, $\mathbb{Q}(\sqrt{2})/\mathbb{Q}$, $\mathbb{R}/\mathbb{Q}$.

(ii) Adjoining a root of an irreducible polynomial: Let K be a field and $f \in K[X]$ an irreducible polynomial. We recall from GRM that $K[X]$ is Euclidean, hence a PID. Therefore $(f) \subset K[X]$ is a maximal ideal and hence $L = \frac{K[X]}{(f)}$ is a field extension of K and $\alpha = X + (f) \in L$ is a root of f.

For example taking $K = \mathbb{R}$, $f = X^2 + 1$ gives the first example in (i).

Let L/K be a field extension. Then $+$ in L and multiplication by elements in K make L a vector space over K (for example $\mathbb{C}$ is an $\mathbb{R}$ vector space).

Definition (Degree of an Extension)**.** Let L/K be a field extension. We say L/K is *finite* if L is finite dimensional as a K-vector space, in which case we write $[L:K] = \dim_K L$ for its dimension, which we call the *degree* of $L \mid K$.

If not, we say L/K is an *infinite extension* and write $[L:K] = \infty$.

L/K is a quadratic (cubic, quartic, ...) extension if $[L:K] = 2(3, 4, \ldots)$.

Example (Continued)**.**

(i) $[\mathbb{C}:\mathbb{R}] = 2$ (basis 1, i), $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$ (basis 1, $\sqrt{2}$)

$[\mathbb{R}:\mathbb{Q}] = \infty$ (exercise: use countability).

(ii) If $L = \frac{K[X]}{(f)}$ where $f \in K[X]$ irreducible then $[L:K] = \deg f$. Indeed if $\alpha = X + (f) \in L$ and $n = \deg f$ then $1, \alpha, \ldots, \alpha^{n-1}$ is a K-basis for L.

Remark. Let K, L be fields and $\phi : K \to L$ a ring homomorphism. Then $\ker(\phi)$ is an ideal in K, but K is a field, so $\ker(\phi) = \{0\}$ or $\ker(\phi) = K$. But by definition, a ring homomorphism must have $\phi(1_K) = 1_L$, so can't have $\ker(\phi) = K$. So must have $\ker(\phi) = \{0\}$, i.e. ϕ is injective. We call ϕ an *embedding* of K in L.

We may use ϕ to identify K as a subfield of L, i.e. we get a field extension L/K.

Example. Taking $K = \mathbb{F}_2$, $f = X^{+}X + 1 \in \mathbb{F}_2[X]$ (which is irreducible) gives $L = \frac{\mathbb{F}_2[X]}{(X^2+X+1)}$ a field with 4 elements.

Proposition 1.2 (Possible sizes of finite fields)**.** Let K be a finite field of characteristic p (necessarily > 0). Then $|K| = p^n$ where $n = [K:\mathbb{F}_p]$.

Proof. $[K:\mathbb{F}_p] = n \implies K \equiv \mathbb{F}_p^n$ as an $\mathbb{F}_p$-vector space. $\square$

Later we will show that (up to isomorphism) there is exactly one field of order p^n for each prime power p^n.

The multiplicative group of a field K is the set $K^* = K \setminus \{0\}$, which is an abelian group under $\times$.

Proposition 1.3. If K is a field then any finite subgroup $G \subset K^*$ is cyclic. In particular if K is a finite field then K^* is cyclic.

Proof. The structure theorem for finite abelian groups gives

$$G \equiv C_{d_1} \times C_{d_2} \times \cdots \times C_{d_t}$$

where $1 < d_1 \mid d_1 \mid \cdots \mid d_t$. If G is not cyclic then picking a prime dividing d_1 shows that G contains a subgroup isomorphic to $C_p \times C_p$. Hence the polynomial $X^p - 1$ has $\geq p^2$ roots in K, which contradicts Lemma 1.1. $\square$

Start of lecture 2

Proposition 1.4 (Frobenius ring homomorphism)**.** Let R be a ring of characteristic p (p a prime). Then the *Frobenius* $\phi : R \to R$, $x \mapsto x^p$ is a ring homomorphism.

Proof. Clearly $\phi(1) = 1$ and $\phi(xy) = \phi(x)\phi(y)$. Also,

$$(X + y)^p = x^p + y^p + \sum_{r=1}^{p-1} \binom{p}{r} x^{p-r} y^r$$

For $1 \leq r \leq p - 1$ the binomial coefficient $\binom{p}{r} = \frac{p!}{r!(p-r)!}$ is divisible by p (since p is prime). Therefore $\phi(x + y) = (x + y)^p = x^p + y^p = \phi(x) + \phi(y)$. $\square$

Remark. We have $\phi(a) = a$ for all $a \in \mathbb{F}_p \subset R$ (proof by induction on a), which implies $a^p \equiv a \pmod p$ for all integers a (Fermat's Little Theorem).

Theorem 1.5 (Tower Law)**.** Let M/L and L/K be field extensions. Then M/K is finite if and only if M/L and L/K are finite. In this case,

$$[M : K] = [M : L][L : K]$$

Proof. The forwards direction holds since any K-basis for M spans M as an L-vector space, and L is a K-vector subspace of M.

We now suppose that M/L and L/K are finite, say $v_1, \ldots, v_n$ is a K-basis for L, $w_1, \ldots, w_m$ is a L-basis for M. We claim that $\{v_i w_j\}_{\substack{1\le i\le n\\ 1\le j\le m}}$ is a K-basis for M.

(spanning) If $x \in M$ then $x = \sum_j \lambda_j w_j$ for some $\lambda_j \in L$ and $\lambda_j = \sum_i \mu_{ij} v_i$ for some $\mu_{ij} \in K$. Therefore $x = \sum_{i,j} \mu_{ij} v_i w_j$.

(independent) Suppose $\sum_{i,j} \mu_{ij} v_i w_i = 0$ for some $\mu_{ij} \in K$. Then

$$\sum_j \underbrace{\left(\sum_i \mu_{ij} v_i\right)}_{\in L} w_j = 0$$

$w_1, \ldots, w_m$ are linearly independent over L so $\sum_i \mu_{ij} v_i = 0$ for all j. Also, $v_1, \ldots, v_n$ are linearly independent over K so $\mu_{ij} = 0$ for all i, j.

This K-basis for M then easily implies the desired result. $\square$

Definition 1.6. Let L/K be a field extension. Let $\alpha_1, \ldots, \alpha_n \in L$.

$$K[\alpha_1, \ldots, \alpha_n] = \{f(\alpha_1, \ldots, \alpha_n) \mid f \in K[X_1, \ldots, X_n]\}$$

This is the smallest subring of L to contain K and $\alpha_1, \ldots, \alpha_n$.

$$K(\alpha_1, \ldots, \alpha_n) = \left\{ \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} : f, g \in K[X_1, \ldots, X_n], g(\alpha_1, \ldots, \alpha_n) \neq 0 \right\}$$

This is the smallest subfield of L to contain K and $\alpha_1, \ldots, \alpha_n$.

Example. $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\} \subset \mathbb{R}$ (use that $\frac{1}{a+b\sqrt{2}} = \frac{a-b\sqrt{2}}{a^2-2b^2}$).

Note that $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}(1+\sqrt{2}) = \mathbb{Q}\left(\frac{17}{3-\sqrt{2}}\right)$ etc.

Remark. In Definition 1.6, another way to see the “smallest” subring / subfield exists is to take the intersection of all such subrings / subfields.

Exercise: Check that

$$K(\alpha_1) = K(\alpha_1, \ldots, \alpha_{n-1})(\alpha_n) = K(\alpha_1)(\alpha_2, \ldots, \alpha_n)$$

Definition (Simple extension). A field extension L/K is a *simple extension* if $L = K(\alpha)$ for some $\alpha \in L$.

Definition 1.7 (Minimal polynomial). Let L/K be a field extension and $\alpha \in L$. Then there is a unique ring homomorphism $\phi : K[X] \to L$ such that $\phi(c) = c$ for all $c \in K$ and $\phi(X) = \alpha$. Indeed,

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

(i.e. ϕ is "evaluation at α"). Since $K[X]$ is a PID, we have that $\ker(\phi) = (f)$ for some $f \in K[X]$.

We say α is *algebraic* over K if $f \neq 0$. In this case f is irreducible and unique up to multiplication by elements of K^*. We scale f so that it is monic, and call it the *minimal polynomial* of α over K. It is the monic polynomial in $K[X]$ of least degree with α as a root.

By the first isomorphism theorem for rings,

$$\frac{K[X]}{(f)} \cong K[\alpha]$$

Note that by Example Sheet 1, Question 2(ii) we have that the left side is a field. Hence $K(\alpha) = K[\alpha]$. For this reason, we usually write $K(\alpha)$ instead of $K[\alpha]$ in these cases.

Moreover, $[K(\alpha) : K] = \deg f$, since if $\deg f = n$ then $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ is a K-basis for $K(\alpha)$.

Example. $K = \mathbb{Q}$, $L = \mathbb{R}$, $\alpha = \sqrt[d]{2}$. α is a root of $f(X) = X^d - 2$, and f is irreducible in $\mathbb{Z}[X]$ by Eisenstein's criterion (with $p = 2$). Therefore by Gauss' Lemma it is irreducible in $\mathbb{Q}[X]$, so f is the minimal polynomial of α. So $[\mathbb{Q}(\sqrt[d]{2}) : \mathbb{Q}] = d$.

Remark (A method for computing inverse)**.** Let $\alpha \in L$ be algebraic over K with minimal polynomial f. Let $0 \neq \beta \in K[\alpha]$, say $\beta = g(\alpha)$ for some $g \in K[X]$. Since f is irreducible and $\beta \neq 0$, we see that f and g are coprime. Running Euclid's algorithm gives $r, s \in K[X]$ such that $r(X)f(X) + s(X)g(X) = 1$. Plugging in $X = \alpha$, we get

$$r(\alpha)\underbrace{f(\alpha)}_{=0} + s(\alpha)\underbrace{g(\alpha)}_{=\beta} = 1,$$

therefore $\frac{1}{\beta} = s(\alpha)$.

Start of

lecture 3

Definition 1.8 (Transcendental number)**.** Let L/K be a field extension. $\alpha \in L$ is *transcendental* over K if it is not algebraic. In this case $K[\alpha] \cong K[X]$ and $K(\alpha) \cong K(X)$.

Remark. Since $K[X]$ is not a field and $1, X, X^2, \dots$ are linearly independent over K, we have $K(\alpha) \neq K[\alpha]$ and $[K(\alpha) : K] = \infty$.

Definition (Algebraic Field)**.** We say a field extension L/K is *algebraic* if every $\alpha \in L$ is algebraic over K.

Remark.

(i) We have $[K(\alpha) : K] < \infty$ if and only if α is algebraic over K.

(ii) If $[L : K] < \infty$ then for any $\alpha \in L$ we certainly have $[K(\alpha) : K] < \infty$. So any finite extension is algebraic, but the inverse is not true.

Example 1.9. $K = \mathbb{Q}$, $L = \bigcup_{n=1}^{\infty} \mathbb{Q}[\sqrt[2^n]{2}] \subset \mathbb{R}$. This is a union of a nested sequence of fields

$$\mathbb{Q}(\sqrt{2}) \subset \mathbb{Q}(\sqrt[4]{2}) \subset \mathbb{Q}(\sqrt[8]{2}) \subset \cdots$$

and so this is a field. $[L : K] = \infty = \infty$ since $[\mathbb{Q}(\sqrt[2^n]{n}) : \mathbb{Q}] = 2^n$ is unbounded. But every $\alpha \in L$ belongs to a finite extension of $\mathbb{Q}$ and so is algebraic over $\mathbb{Q}$. Therefore $L/\mathbb{Q}$ is algebraic.

Remark 1.10. Classically $\alpha \in \mathbb{C}$ is called algebraic / transcendental if it is algebraic / transcendental over $\mathbb{Q}$.

A countability argument (see IA Numbers and Sets) shows that transcendental numbers exist. Liouville showed that $\sum_{n=1}^{\infty} \frac{1}{10^{n!}}$ is transcendental.

It was proved in the 19th century that e and π are transcendental (Hermite & Lindeman).

Example 1.11.

(i) Let $f(X) = X^d - n$ ($d, n \in \mathbb{Z}$, $d \geq 2$, $n \neq 0$). Suppose there exists a prime p such that when we write $n = p^e m$ with $p \nmid m$, then $(d, e) = 1$. We claim that f is irreducible in $\mathbb{Q}[X]$. Equivalently we show that $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$ where $\alpha = \sqrt[d]{n}$. By Euclid's algorithm there exist $r, s \in \mathbb{Z}$ such that $rd + se = 1$ (we may arrange $s > 0$). Then $p^{dr} n^s = p^{dr}(p^e m)^s = pm^s$. Let $\beta = p^r \alpha^s$ so that $\beta^d = pm^s$. Then β is a root of $g(X) = X^d - pm^s$, which is irreducible in $\mathbb{Z}[X]$ by Eisenstein's criterion, so irreducible in $\mathbb{Q}[X]$ by Gauss' Lemma, therefore $[\mathbb{Q}(\beta) : \mathbb{Q}] = d$. But $\mathbb{Q}(\beta) \subset \mathbb{Q}(\alpha)$ and $[\mathbb{Q}(\alpha) : \mathbb{Q}] \leq \deg f = d$. This gives $[\mathbb{Q}(\alpha) : \mathbb{Q}] = d$ as required.

(ii) Let p be an odd prime, $\zeta_p = e^{2\pi i/p}$ and

$$\alpha = 2\cos\left(\frac{2\pi}{p}\right) = \zeta_p + \zeta_p^{-1}.$$

Let's compute $[\mathbb{Q}(\alpha) : \mathbb{Q}]$. ζ_p is a root of

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

which is irreducible by Eisenstein's criterion applied to $f(X+1)$. Therefore $[\zeta_p(:)\mathbb{Q}] = \deg f = p - 1$. Note that $\mathbb{Q}(\zeta_p)/\mathbb{Q}(\alpha)/\mathbb{Q}$, so we will try to use Tower Law to find the degree of the extension $\mathbb{Q}(\alpha)/\mathbb{Q}$. ζ_p is a root of

$$g(X) = (X - \zeta_p)(X - \zeta_p^{-1}) = X^2 - \alpha X + 1 \in \mathbb{Q}(\alpha)[X]$$

Therefore $[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\alpha)] \leq \deg g = 2$. But $\alpha \in \mathbb{R}$ and $\zeta_p \notin \mathbb{R}$ so $\zeta_p \notin \mathbb{Q}(\alpha) \subset \mathbb{R}$. So $[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\alpha)] = 2$, so by Tower Law $[\mathbb{Q}(\alpha) : \mathbb{Q}] = \frac{p-1}{2}$.

(iii) Suppose m, n and mn are not perfect squares. Let $\alpha = \sqrt{m} + \sqrt{n}$. Let's compute $[\mathbb{Q}(\alpha) : \mathbb{Q}]$. Clearly $\mathbb{Q}(\alpha) \subset \mathbb{Q}(\sqrt{m}, \sqrt{n})$. Conversely we have

$$m = (\alpha - \sqrt{n})^2 = \alpha^2 - 2\alpha\sqrt{n} + n$$

$$\implies \sqrt{n} = \frac{\alpha^2 - m + n}{2\alpha}$$

so $\sqrt{n} \in \mathbb{Q}(\alpha)$, and similarly $\sqrt{m} \in \mathbb{Q}(\alpha)$. So therefore $\mathbb{Q}(\alpha) = \mathbb{Q}(\sqrt{m}, \sqrt{n})$. Note that $\mathbb{Q}(\sqrt{m}, \sqrt{n})/\mathbb{Q}(\sqrt{n})/\mathbb{Q}$, with $[\mathbb{Q}(\sqrt{n}) : \mathbb{Q}] = 2$. We also know $[\mathbb{Q}(\sqrt{n})(\sqrt{m}) : \mathbb{Q}(\sqrt{n})] \leq 2$. Suppose $\sqrt{m} \in \mathbb{Q}(\sqrt{n})$. Then $\sqrt{m} = r + s\sqrt{n}$ for some $r, s \in \mathbb{Q}$. Therefore $m = r^2 + 2rs\sqrt{n} + s^2 n$. Since $\sqrt{n} \notin \mathbb{Q}$ we must have $rs = 0$. If $r = 0$ then mn will be a square, and if $s = 0$ then m is a square. Either way we get a contradiction. So $[\mathbb{Q}(\sqrt{m}, \sqrt{n}) : \mathbb{Q}(\sqrt{n})] = 2$. So by Tower Law, $[\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.

Start of lecture 4

Lemma 1.12. Let L/K be a field extension and $\alpha_1, \dots, \alpha_n \in L$. Then

$$\alpha_1, \dots, \alpha_n \text{ are algebraic over } K \iff [K(\alpha_1, \dots, \alpha_n) : K] < \infty.$$

Proof. The case $n = 1$ was a remark in the previous lecture.

$\Rightarrow$ By induction on on n using Tower Law.

$\Leftarrow$ Clear since $K(\alpha_1) \subset K(\alpha_1, \dots, \alpha_n)$. □

Corollary 1.13. Let L/K be any field extension. Then the set

$$\{\alpha \in L \mid \alpha \text{ is algebraic over } K\}$$

is a subfield of L.

Proof. If α, β are algebraic over K then by Lemma 1.12 $[K(\alpha, \beta) : K] < \infty$. Let $\gamma = \alpha \pm \beta$, or $\alpha\beta$ or (if $\alpha \neq 0$) $\frac{1}{\alpha}$. Then $\gamma \in K(\alpha, \beta)$, so since $[K(\alpha, \beta, \gamma) : K] < \infty$, by Lemma 1.12, we get that γ is algebraic over K. □

Example. Taking $K = \mathbb{Q}$ and $L = \mathbb{C}$ we see that

$$\overline{\mathbb{Q}} = \{\text{algebraic numbers}\}$$

is a field.

Since $\overline{\mathbb{Q}} \subset \mathbb{Q}(()\sqrt[2]{2})$ and $[\mathbb{Q}(()\sqrt[d]{2}) : \mathbb{Q}] = d$ for all d, we see that $[\overline{\mathbb{Q}} : \mathbb{Q}] = \infty$.

Proposition 1.14. Let $M/L/K$ be a field extension. Then

$$M/K \text{ is algebraic} \iff M/L \text{ and } L/K \text{ are both algebraic}$$

Proof. $\Rightarrow$ Every element of M is algebraic over K, hence algebraic over L, so M/L is algebraic. Also, as $L \subset M$, L is algebraic over K.

$\Leftarrow$ Let $\alpha \in M$. We must show that α is algebraic over K. Since M/L is algebraic, α is a root of some

$$f(X) = c_n X^n + \cdots + c_1 X + c_0 \in L[X]$$

Let $L_0 = K(c_0, c_1, \ldots, c_n)$. Since each c_i is algebraic over K, Lemma 1.12 gives $[L_0 : K] < \infty$. But f has coefficients in L_0, so $[L_0(\alpha) : L_0] \leq \deg f < \infty$. By Tower Law $[L_0(\alpha) : K] < \infty$. Therefore α is algebraic over K. $\square$

2 Ruler and Compass Constructions

We use our results on field extensions to show that certain classical problems cannot be solved.

Definition (Ruler and Compass Construction)**.** Let $S \subset \mathbb{R}^2$ be a finite set of points. We may:

(i) Draw a straight line through any 2 distinct points in S.

(ii) Draw a circle with centre any point in S and radius the distance between 2 points in S.

(iii) Enlarge S by adjoining any point of intersection of 2 distinct lines or circles.

A point $(x, y) \in \mathbb{R}^2$ is *constructible* from S if we can enlarge S to contain (x, y) by a finite sequence of the above operations.

A number $x \in \mathbb{R}$ is constructible if $(x, 0)$ can be constructed from $\{(0, 0), (1, 0)\}$.

We will relate this to the following:

Definition (Constructible Field)**.** Let $K \subset \mathbb{R}$ be a subfield. We say that K is constructible if there exists integer $n \geq 0$ and a sequence of subfields of $\mathbb{R}$

$$\mathbb{Q} = F_0 \subset F_1 \subset F_2 \subset \cdots \subset F_n$$

such that $[F_i : F_{i-1}] = 2$ for all i and $K \subset F_n$.

Remark. We see by Tower Law that K constructible $\implies$ $[K : \mathbb{Q}]$ is a power of 2.

Theorem 2.1. If $x \in \mathbb{R}$ is constructible, then $\mathbb{Q}(x)$ is a constructible subfield of $\mathbb{R}$.

Proof. Suppose $S \subset \mathbb{R}^2$ is a finite set of points all of whose coordinates belong to a constructible field K.

It suffices to show that if we adjoin $(x, y) \in \mathbb{R}^2$ to S using (iii), then $K(x, y)$ is also constructible. Since K is constructible, there exists a sequence $\mathbb{Q} = F_0 \subset F_1 \subset \cdots \subset F_n$ with $[F_i : F_{i-1}] = 2$ for all $1 \leq i \leq n$ and $K \subset F_n$.

The lines and circles in (i) and (ii) have equations of the form $ax+by=c$ and $(x-a)^2+(y-b)^2=c$ with $a,b,c \in K$. If (x,y) is a point of intersection of 2 such lines or circles then $x=r+s\sqrt{v}$, $y=t+u\sqrt{v}$ for some $r,s,t,u,v \in K$. Therefore $x,y \in K(\sqrt{v}) \subset F_n(\sqrt{v})$. Since $[F_n(\sqrt{v}) : F_n]$ is 1 or 2, it follows that $K(x,y)$ is constructible. $\square$

Remark. It can be shown that $(x \pm y, 0)$, $(x/y, 0)$ and $(\sqrt{x}, 0)$ are constructible from the set $\{(0,0),(1,0),(x,0),(y,0)\}$.

Using this, one can also prove that the converse of Theorem 2.1 holds, i.e. $\mathbb{Q}(x)$ is constructible implies x is constructible.

Corollary 2.2. If $x \in \mathbb{R}$ is constructible then x is algebraic over $\mathbb{Q}$ and $[\mathbb{Q}(x) : \mathbb{Q}]$ is a power of 2.

Some Classical Problems

(1) **Squaring the circle:** One classical problem is to construct a square whose area is the same as that as a circle with unit radius. This amounts to constructing the real number $\sqrt{\pi}$. This is impossible by and the fact that π is transcendental (Lindeman).

(2) **Duplicating the cube:** Construct a cube whose volume is twice that of a given cube. This amounts to construction of $\sqrt[3]{2}$. But $\sqrt[3]{2}$ has minimal polynomial X^3-2 so $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$, which is not a power of 2.

(3) **Trisecting the angle:** One is to divide a given angle into 3 equal angles. Let us suppose the given angle is $120° = \frac{2\pi}{3}$. Since this is itself constructible, if the trisection problem can be solved, then the angle $\frac{2\pi}{9}$ is constructible, in other words the real numbers $\cos\left(\frac{2\pi}{9}\right)$ and $\sin\left(\frac{2\pi}{9}\right)$ are constructible. From the formula $\cos 3\theta = 4\cos^3\theta - 3\cos\theta$, we see that $2\cos\left(\frac{2\pi}{9}\right)$ is a root of $f(X) = X^3 - 3X + 1$. Noting that $f(\pm 1) \neq 0$, and that f is monic, we can use Gauss' lemma to observe that f is irreducible in $\mathbb{Q}[X]$. Therefore $[\mathbb{Q}(\cos(2\pi/9)) : \mathbb{Q}] = 3$, which is not a power of 2. So this construction is impossible.

Start of lecture 5

Remark. The last example shows that a regular 9-gon cannot be constructed with ruler and compass.

Later we will prove the result of Gauss which says that a regular n-gon is constructible if and only if $\phi(n)$ is a power of 2.

3 Splitting Fields

Question: Let $f \in K[X]$ be a nonconstant polynomial. Is there a field extension L/K in which f has a root? (or even better: an extension in which f splits into linear factors)?

If $K \subset \mathbb{C}$ then the fundamental theorem of algebra shows we can factor f in $\mathbb{C}[X]$ as a product of linear polynomials. But what about $K = \mathbb{F}_p$?

Definition 3.1 (K-homomorphism)**.** Let L/K and M/K be field extensions. A *K-homomorphism* (or *K-embedding*) of L into M is a ring homomorphism $L \to M$ which is the identity on K.

Theorem 3.2. Let $L = K(\alpha)$ where α is algebraic over K with minimal polynomial f. Let M/K be any field extension. Then there is a bijection

$$\begin{aligned} \{K\text{-homomorphism } L \to M\} &\leftrightarrow \{\text{roots of } f \text{ in } M\} \\ \tau &\mapsto \tau(\alpha) \end{aligned}$$

In particular (by Lemma 1.1),

$$\#\{K\text{-homomorphisms } L \to M\} \leq \deg f$$

Proof. Write $f = \sum_{i=0}^{d} c_i X^i$, $c_i \in K$. Let $\tau : L \to M$ be a K-homomorphism. Then

$$\begin{aligned} f(\tau(\alpha)) &= \sum_i c_i \tau(\alpha)^i \\ &= \tau\left(\sum_i c_i \alpha^i\right) \\ &= \tau(f(\alpha)) \\ &= 0 \end{aligned}$$

Therefore $\tau(\alpha) \in M$ is a root of f.

Injectivity: Since $L = K(\alpha)$, and K-homomorphism $\tau : L \to M$ is uniquely determined by $\tau(\alpha)$.

Surjectivity: We saw earlier that evaluation at α gives an isomorphism $K[X]/(f) \to K(\alpha) = L$ where $X + (f) \mapsto \alpha$. Now let $\beta \in M$ be a root of f. Since f is irreducible it is the minimal polynomial for β over K. Evaluation at β gives a ring homomorphism

$$\begin{aligned} K[X] &\to M \\ g &\mapsto g(\beta) \end{aligned}$$

with kernel (f). By the isomorphism theorem we get

$$\begin{aligned} \frac{K[X]}{(f)} &\xhookrightarrow{\psi} M \\ X + (f) &\mapsto \beta \end{aligned}$$

Since ϕ, ψ are K-homomorphisms and ϕ is an isomorphism it follows that

$$\tau = \psi \cdot \phi^{-1} : L \to M$$

is a K-homomorphism with $\tau(\alpha) = \beta$. $\square$

Example. There are exactly 2 $\mathbb{Q}$-homomorphism $\mathbb{Q}(\sqrt{2}) \to \mathbb{R}$ given by $a + b\sqrt{2} \mapsto b\sqrt{2}$ and $a + b\sqrt{2} \mapsto a - b\sqrt{2}$, $a, b \in \mathbb{Q}$. We actually need a slight variant of Theorem 3.2. The proof is exactly the same, but the extra generality is useful for inductive proofs.

Definition 3.3 (σ-embedding)**.** Let L/K and M/K' be field extensions. Let $\sigma : K \to K'$ be a field embedding. A σ-embedding $\tau : L \to M$ is an embedding which extends σ, i.e. $\tau(x) = \sigma(x)$ $\forall x \in K$. Equivalently, $\sigma = \tau|_K$ is the restriction of τ to K.

$$\begin{tikzcd} L \arrow[r, hook, "\tau"] \arrow[d, dash] & M' \arrow[d, dash] \\ K \arrow[r, hook, "\sigma"'] & K' \end{tikzcd}$$

Note. Taking $\sigma = \mathrm{id} : K \to K$ we recover the definition of a K-embedding.

Theorem 3.4. Let $L = K(\alpha)$ where α is algebraic over K with minimal polynomial f. Let $\sigma : K \to K'$ be a field embedding, and M/K' any field extension. Then there is a bijection

$$\begin{aligned} \{\sigma\text{-embeddings } L \to M\} &\to \{\text{roots of } \sigma f \text{ in } M\} \\ \tau &\mapsto \tau(\alpha) \end{aligned}$$

(where σf is the polynomial in $K'[X]$ obtained by applying σ to each coefficient of f). In particular,

$$\#\{\sigma\text{-embeddings } L \to M\} \le \deg f$$

Example. Let $K = \mathbb{Q}(\sqrt{2})$ and let $L = \mathbb{Q}(\alpha)$ where $\alpha = \sqrt{1+\sqrt{2}}$ (exercise: check that $1+\sqrt{2}$ is not a square in K, so that we get $[L : K] = 2$). There are exactly 2 K-embeddings $L \to \mathbb{R}$ given by $\alpha \mapsto \pm\sqrt{1+\sqrt{2}}$.

However, if $\sigma : K \to K$, $a + b\sqrt{2} \mapsto a - b\sqrt{2}$ then there are no σ-embeddings $L \to \mathbb{R}$ (since $1 - \sqrt{2} < 0$).

Definition 3.5 (splitting field)**.** Let K be a field. Let $0 \neq f \in K[X]$. An extension L/K is a *splitting field* of f over K if

(i) f splits into linear factors over L.

(ii) $L = K(\alpha_1, \dots, \alpha_n)$ where α_i are the roots of f in L.

Remark. (ii) is equivalent to saying f does not split into linear factors over any (proper) subfield of L containing K.

Start of lecture 6

Note. (ii) implies that $[L : K] < \infty$.

Theorem 3.6 (Existence of splitting fields)**.** Let $0 \neq f \in K[X]$. Then there exists a splitting field for f over K.

Proof. (We adjoin roots of f one at a time).

The proof is by induction on the degree of f. If $\deg f \leq 1$ then $L = K$ is the splitting field.

Now assume every polynomial of degree $< \deg f$ has a splitting field. Let g be an irreducible factor of f. Let $K_1 = K[X]/(g)$ and $\alpha_1 = X + (g) \in K[X]$, with $K_1 = K(\alpha_1)$. Then $f(\alpha_1) = 0$. So $f(X) = (X - \alpha_1) f_1(X)$ for some $f_1 \in K_1[X]$ with $\deg f_1 < \deg f$.

By induction hypothesis there exists a splitting field L for f_1 over K_1, so $L = K_1(\alpha_2, \dots, \alpha_n)$ where $\alpha_2, \dots, \alpha_n$ are the roots of f_1 in L. We claim that L is a splitting field for f over K. Since f_1 splits in L, so does $f(X) = (X - \alpha) f_1(X)$. Moreover $L = K_1(\alpha_2, \dots, \alpha_n) = K(\alpha_1, \dots, \alpha_n)$ and $\alpha_1, \dots, \alpha_n$ are roots of f. Therefore L satisfies (i) and (ii). $\square$

Theorem 3.7 (Uniqueness of splitting fields)**.** Let $0 \neq f \in K[X]$. Let L be a splitting field of f over K. Let $\sigma : K \hookrightarrow M$ be any field embedding such that $\sigma f \in M[X]$ splits. Then

(i) There exists a σ-embedding $\tau : L \hookrightarrow M$.

(ii) If M is a splitting field for σf over σK then any τ as in (i) is an isomorphism.

In particular any two splitting fields for f over K are K-isomorphic.

$$\begin{tikzcd}
L \arrow[rr, hook, dashed, "\tau"] & & M \\
K(\alpha) \arrow[u, dash] \arrow[urr, hook, "\sigma_1"] & & \\
K \arrow[u, dash, "\deg g"] \arrow[uurr, hook, "\sigma"'] & &
\end{tikzcd}$$

Proof.

(i) By induction on $n = [L : K]$. If $n = 1$ then $L = K$ and there is nothing to prove. So suppose $n > 1$ and let $g \in K[X]$ be an irreducible factor of f, of degree > 1. Let $\alpha \in L$ be a root of g. Let $\beta \in M$ be a root of σg. By Theorem 3.4, σ extends to an embedding $\sigma_1 : K(\alpha) \to M$, $\alpha \mapsto \beta$. Then $[L : K(\alpha)] < [L : K]$. L is a splitting field of f over $K(\alpha)$ and $\sigma_1 f = \sigma f$ splits in M. So by the induction hypothesis σ_1 extends to an embedding $\tau : L \to M$.

(ii) Pick any $\tau : L \hookrightarrow M$ as in (i). Let $\alpha_1, \dots, \alpha_n$ be the roots of f in L. The roots of σf in M are $\tau\alpha_1$, ..., $\tau\alpha_n$ (consider splitting σf as a product of linear factors in two ways, and then use the fact that $M[X]$ is a UFD). So if M is a splitting field for σf over σK then

$$M = \sigma K(\tau\alpha_1, \dots, \tau\alpha_n) = \tau(K(\alpha_1, \dots, \alpha_n)) = \tau(L)$$

So τ is surjective, so it's an isomorphism (recall field embeddings are always injective).

For the final statement, suppose L/K and M/K are splitting fields for f over K, and let $\sigma : K \hookrightarrow M$ be the inclusion map. Then (i) and (ii) give a K-isomorphism $L \to M$. $\square$

Warning. The previous theorem means that we can say "the splitting field of f over K" since all such fields are isomorphic.

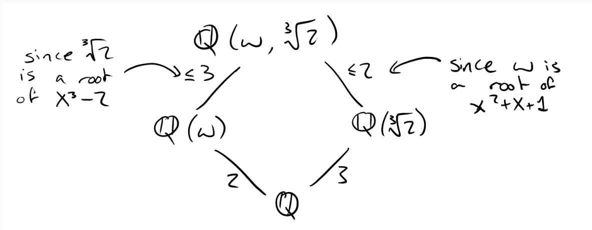
However, the isomorphism between such fields is not necessarily unique, an in fact in some cases we can use a non-identity automorphism.

Example. If $K \subset \mathbb{C}$ then by the fundamental theorem of algebra, one splitting field for f over K is the subfield $K(\alpha_1, \dots, \alpha_n) \subset \mathbb{C}$ where $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ are the roots of f.

(i) Consider

$$f(X) = X^3 - 2 = (X - \sqrt[3]{2})(X - \omega\sqrt[3]{2})(X - \omega^2\sqrt[3]{2}) \in \mathbb{Q}[X]$$

Then $\mathbb{Q}(\omega, \sqrt[3]{2})$ is a splitting field for f over $\mathbb{Q}$.



By the Tower Law $[\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}]$ is ≤ 6 and is divisible by both 2 and 3. Since $\gcd(2, 3) = 1$, we get $[\mathbb{Q}(\omega, \sqrt[3]{2}) : \mathbb{Q}] = 6$.

(ii) Let p be an odd prime and

$$\begin{aligned} f(X) &= \frac{X^p - 1}{X - 1} = X^{p-1} + \dots + X^2 + X + 1 \in \mathbb{Q}[X] \\ &= \prod_{r=1}^{p-1} (X - \zeta_p^r) \end{aligned}$$

where $\zeta_p = e^{2\pi i/p}$. Then f has splitting field

$$\mathbb{Q}(\zeta_p, \zeta_p^2, \dots, \zeta_p^{p-1}) = \mathbb{Q}(\zeta_p)$$

So in this case the splitting field is obtained by adjoining just one root.

(iii) Let $f(X) = X^3 - 2 \in \mathbb{F}_7[X]$. Then f is irreducible (since 2 isn't a cube modulo 7). Let $L = \mathbb{F}_7[X]/(f)$, so $L = \mathbb{F}_7(\alpha)$ with $\alpha^3 = 2$. Noting that $2^3 \equiv 1 \pmod 7$, we get that $f(X) = (X - \alpha)(X - 2\alpha)(X - 4\alpha)$. So $L = \mathbb{F}_7(\alpha)$ is a splitting field for f over $\mathbb{F}_7$.

Start of

lecture 7

Definition (algebraically closed field)**.** A field K is *algebraically closed* if every nonconstant polynomial in $K[X]$ has a root in K.

Equivalently, if every irreducible polynomial in $K[X]$ is linear.

Example. $\mathbb{C}$, by the fundamental theorem of algebra.

Lemma 3.8. Let K be a field. Then the following are equivalent:

(i) K is algebraically closed.

(ii) If L/K is a field extension and $\alpha \in L$ is algebraic over K then $\alpha \in K$.

(iii) If L/K is algebraic then $L = K$.

(iv) If L/K is finite then $L = K$.

Proof. (ii) $\implies$ (iii) $\implies$ (iv) are all clear.

For (iv) $\implies$ (i), let $f \in K[X]$ be an irreducible polynomial. Then $L = K[X]/(f)$ is a finite extension of K with $[L : K] = \deg f$. By (iv) we have $L = K$. Therefore f is linear. $\square$

Definition (algebraic closure)**.** If L/K is algebraic and L is algebraically closed then we say that L is an *algebraic closure* of K.

Lemma 3.9. Let L/K be an algebraic extension such that every polynomial in $K[X]$ splits into linear factors over L. Then L is algebraically closed (and hence an algebraic closure of K).

Proof. If L is not algebraically closed then by Lemma 3.8 there exists M/L algebraic with $[M : L] > 1$. Both M/L and L/K are algebraic. So by Proposition 1.14, M/K is algebraic.

Pick any $\alpha \in M$. Let f be the minimal polynomial for α over K. By our assumption, f splits over L, so $\alpha \in L$. So $M = L$. $\square$

Later we will show that every field K has an algebraic closure. Here are two easy cases:

Theorem 3.10. Suppose that (i) $K \subset \mathbb{C}$ or (ii) K is countable. Then K has an algebraic closure.

Proof.

(i) If $K \subset \mathbb{C}$ then let
$$L = \{\alpha \in \mathbb{C} \mid \alpha \text{ is algebraic over } K\}.$$
L is a field by Corollary 1.13, L/K is algebraic. If $f \in K[X]$ then write $f(X) = \prod_{i=1}^{n}(X - \alpha_i)$ for some $\alpha_i \in \mathbb{C}$. The definition of L implies that all the $\alpha_i \in L$, i.e. f splits into linear factors over L. Then Lemma 3.9 gives that L is algebraically closed. Therefore L is the algebraic closure of K.

(ii) If K is countable then so $K[X]$. Enumerate the monic irreducible polynomials $f_1, f_2, f_3, \ldots$. Let $L_0 = k$ and for each $i \geq 1$ let L_i be a splitting field for f_i over L_{i-1}. Then
$$L_0 \subset L_1 \subset L_2 \subset \cdots$$
Then $L = \bigcup_{n \geq 0} L_n$ is a field, L/K is algebraic, and every polynomial in $K[X]$ splits over L. Then Lemma 3.9 implies that L is algebraically closed. Therefore L is an algebraic closure of K. $\square$

Remark. Taking $K = \mathbb{Q}$ in the proof of (i), we see that $\overline{\mathbb{Q}} = \{\text{algebraic numbers}\} \subset \mathbb{C}$ is algebraically closed.

4 Symmetric Polynomials

Suppose we wish to find the roots of a cubic polynomial $f(X) = X^3 + aX^2 + bX + c \in \mathbb{Q}[X]$. After substituting $X - \frac{a}{3}$ for X we may assume $a = 0$. Writing

$$f(X) = (X - \alpha)(X - \beta)(X - \gamma)$$

and comparing coefficients gives

$$\begin{aligned} \alpha + \beta + \gamma &= -a = 0 \\ \alpha\beta + \beta\gamma + \gamma\alpha &= b \\ \alpha\beta\gamma &= -c \end{aligned}$$

Let $\omega = e^{2\pi i/3}$. Write

$$\alpha = \frac{1}{3}[\underbrace{(\alpha + \beta + \gamma)}_{=0} + \underbrace{(\alpha + \omega\beta + \omega^2\gamma)}_{=u} + \underbrace{(\alpha + \omega^2\beta + \omega\gamma)}_{=v}]$$

Then $u^3 + v^3$ and uv are unchanged under permuting α, β, γ. After some calculation we find (remembering $a = 0$) that

$$u^3 + v^3 = -27c \qquad \text{and} \qquad uv = -3b$$

Therefore u^3 and v^3 are the roots of

$$X^2 + 27cX - 27b^3 = 0$$

Solving this quadratic and taking cube roots gives a formula for the roots of a cube, usually called Cardano's formula.

Let S_n be the symmetric group on n letters.

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

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

If f and g are symmetric then so are $f + g$ and fg. Therefore the symmetric polynomials form a subring of $R[X_1, \ldots, X_n]$.

Definition (elementary symmetric functions)**.** The *elementary symmetric functions* are the polynomials $s_1, \ldots, s_n$ in $\mathbb{Z}[X_1, \ldots, X_n]$ such that

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

Example. When $n = 3$,

$$\begin{aligned} s_1 &= X_1 + X_2 + X_3 \\ s_2 &= X_1X_2 + X_1X_3 + X_2X_3 \\ s_3 &= X_1X_2X_3 \end{aligned}$$

In general,

$$s_r = \sum_{1 \le i_1 < \cdots < i_r \le n} X_{i_1} X_{i_2} \cdots X_{i_r}$$

Theorem 4.1 (Symmetric Function Theorem)**.**

(i) Every symmetric polynomial over R can be expressed as a polynomial in the elementary symmetric functions, with coefficients in R.

(ii) There are no non-trivial relations between the s_i.

Remark. Consider the ring homomorphism

$$\begin{aligned} R[\tau_1, \ldots, \tau_n] &\xrightarrow{\theta} R[X_1, \ldots, X_n] \\ \tau_i &\mapsto s_i \end{aligned}$$

Then part (i) of Symmetric Function Theorem says that

$$\mathrm{Im}(\theta) = \{\text{symmetric polynomials in } R[X_1, \ldots, X_n]\},$$

and part (ii) says θ is injective.

Start of lecture 8

Remark. We can write any $f \in R[X_1, \ldots, X_n]$ as $f = \sum_d f_d$ where f_d is *homogeneous* of degree d (i.e. each monomial has total degree d).

Clearly f symmetric implies all f_d are symmetric. So for the proof of Symmetric Function Theorem(i), it suffices to consider $f \in R[X_1, \ldots, X_n]$ which is symmetric and homogeneous of degree d.

Definition (lexicocraphic ordering)**.** Define the *lexicographic ordering* of monomials such that
$$X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n} > X_1^{k_1}X^{j_2}\cdots X_n^{j_n}$$
if $i_1 = j_1, i_2 = j_2, \dots, i_{r-1} = j_{r-1}, i_r > j_r$ for some $1 \le r \le n$.

This is a total ordering.

Proof of Symmetric Function Theorem.

(i) By previous remark, we may split f into a sum of homogeneous polynomials, and just prove that each term in the sum can be written as a sum of elementary symmetric function.

Let $X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n}$ be the largest monomial (with respect to lexicographic ordering) to appear in f with non-zero coefficient (c say). Since $X_{\sigma(1)}^{i_1}X_{\sigma(2)}^{i_2}\cdots X_{\sigma(n)}^{i_n}$ also appears in f for all $\sigma \in S_n$, we must have $i_1 \ge i_2 \ge i_3 \ge \cdots i_n$.

Write
$$X_1^{i_1}X_2^{i_2}\cdots X_n^{i_n} = X_1^{i_1-i_2}(X_1X_2)^{i_2-i_3}\cdots(X_1X_2\cdots X_n)^{i_{n-1}-i_n}$$
Let $g = s_1^{i_1-i_2}s_2^{i_2-i_3}\cdots s_n^{i_n}$. Then f and g are both homogeneous of degree d and have the same largest monomial. So $f - cg$ is either 0, or it is a symmetric polynomial of degree d, whose leading monomial is smaller than that of f.

Since there are only finitely many monomials of degree d in $R[X_1, \dots, X_n]$, the process stops after finitely many steps. Therefore we can write f as a polynomial in $s_1, \dots, s_n$.

(ii) Write $s_{r,n}$ instead of s_r to indicate the number of variables involved. Suppose $G \in R[Y_1, \dots, Y_n]$ with $G(s_{1,n}, s_{2,n}, \dots, s_{n,n}) = 0$. We must prove that $G = 0$. The proof is by induction on n. The case $n = 1$ is clear.

Write $G = Y_n^k H$ with $Y_n \nmid H$, $k \ge 0$. Since $s_{n,n} = X_1X_2\cdots X_n$, it is not a zero divisor in $R[X_1, \dots, X_n]$, so we have
$$H(s_{1,n}, s_{2,n}, \dots, s_{n,n}) = 0$$
So we may assume that G, if non-zero, is not divisible by Y_n. Replacing X_n by 0 gives
$$s_{r,n}(X_1, \dots, X_{n-1}, 0) = \begin{cases} s_{r,n-1}(X_1, \dots, X_{n-1}) & r < n \\ 0 & r = n \end{cases}$$
Therefore
$$G(s_{1,n-1}, s_{2,n-1}, \dots, s_{n-1,n-1}, 0) = 0$$

By induction hypothesis, $G(Y_1, \ldots, Y_{n-1}, 0) = 0$, hence $Y_n \mid G$. So by the above G must be zero. $\square$

Example 4.2. Let $f = \sum_{i \neq j} X_i^2 X_j$. The leading term (in lexicographic ordering) is $X_1^2 X_2 = X_1(X_1 X_2)$. Calculate:

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

So $f = s_1 s_2 - 3 s_3$.

Example 4.3. Let $f(X) = \prod_{i=1}^n (X - \alpha_i)$ be a monis polynomial with roots $\alpha_1, \ldots, \alpha_n$. The *discriminant of* f is

$$\operatorname{Disc}(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2$$

By the Symmetric Function Theorem, we can write $\operatorname{Disc}(f)$ as a polynomial in the coefficients of f.

$n = 2$, $f(X) = X^2 + bX + c = (X - \alpha_1)(X - \alpha_2)$. Then

$$\begin{aligned} \operatorname{Disc}(f) &= (\alpha_1 - \alpha_2)^2 \\ &= (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 \\ &= b^2 - 4ac \end{aligned}$$

It is clear from the definition that

$$\operatorname{Disc}(f) = 0 \iff f \text{ has repeated roots}$$

5 Normal and separable extensions

Definition (normal extension). An extension L/K is *normal* if it is algebraic and the minimal polynomial of every $\alpha \in L$ splits into linear factors over L.

Equivalently if $f \in K[X]$ is irreducible and has a root in L, then it splits into linear factors over L. (slogan: "one out – all out").

Theorem 5.1 (Splitting fields are normal). Let $[L : K] < \infty$. Then

$$L/K \text{ is normal} \iff L \text{ is a splitting field for some } f \in K[X]$$

Proof.

$\Rightarrow$ Write $L = K(\alpha_1, \dots, \alpha_n)$. Let f_i be the minimal polynomial of α_i over K. Then

$$\begin{aligned} L/K \text{ normal} &\implies f_i \text{ splits into linear factors over } L \\ &\implies L \text{ is a splitting field for } \prod_i f_i \end{aligned}$$

$\Rightarrow$ Let L be the splitting field of $f \in K[X]$ over K. Let $\alpha \in L$ have minimal polynomial g over K. Let M/L be a splitting field for g. We must show that whenever β is a root of g then in fact $\beta \in L$. Then $L = L(\alpha)$ is a splitting field for f over $K(\alpha)$, and $L(\beta)$ is a splitting field for f over $K(\beta)$. α and β have the same minimal polynomial g over K, so $K(\alpha)$ and $K(\beta)$ are K-isomorphic. By Uniqueness of splitting fields, $L(\alpha)$ and $L(\beta)$ are K-isomorphic. Therefore $[L : K] = [L(\beta) : K]$. So by Tower Law, $[L(\beta) : L] = 1$, so $L(\beta) = L$, so $\beta \in L$. □

Start of

lecture 9

5.1 Separability

Over $\mathbb{R}$ or $\mathbb{C}$ we know from calculus that a polynomial f has a repeated root α if and only if

$$f(\alpha) = f'(\alpha) = 0$$

To work over arbitrary fields we proceed purely algebraically (no calculus!).

Note that we call a root *simple* if it is not a repeated root.

Definition (Formal derivative)**.** The *formal derivative* of $f = \sum_{i=0}^{d} c_i X^i \in K[X]$ is

$$f' = \sum_{i=1}^{d} i c_i X^{i-1}.$$

Exercise: Check with this definition that

$$\begin{cases} (f+g)' = f' + g' \\ (fg)' = fg' + f'g \end{cases}$$

Lemma 5.2. Let $f \in K[X]$ and $\alpha \in K$ a root of f. Then α is a simple root if and only if $f'(\alpha) \neq 0$.

Proof. Write $f(X) = (X - \alpha)g(X)$ for some $g \in K[X]$. Then

$$\begin{aligned} \alpha \text{ is a simple root of } f &\iff X - \alpha \text{ is not a factor of } g \\ &\iff g(\alpha) \neq 0 \end{aligned}$$

But $f'(X) = (X - \alpha)g'(X) + g(X)$, so $f'(\alpha) = g(\alpha)$. $\square$

By the GCD of polynomials $f, g \in K[X]$ not both zero, we mean the unique monic polynomial $\gcd(f, g)$ which generates the ideal $(f, g) \subset K[X]$.

This is the unique monic polynomial which divides both f and g and can be written as $af + bg$ for some $a, b \in K[X]$.

We can compute $\gcd(f, g)$, together with a, b, using Euclid's algorithm.

Lemma 5.3. Let $f, g \in K[X]$ and let L/K be any field extension. Then $\gcd(f, g)$ is the same computed in $K[X]$ and in $L[X]$.

Proof. Running Euclid's algorithm on $f, g \in K[X]$ gives the same answer whether we work in $K[X]$ or $L[X]$. $\square$

Definition (Separable)**.** An irreducible polynomial $f \in K[X]$ is *separable* if it splits into distinct linear factors in a splitting field.

The convention in this course is that we use the same definition for any $0 \neq f \in K[X]$. Anything which is not separable is called *inseparable.*

Lemma 5.4. Let $0 \neq f \in K[X]$. Then

$$f \text{ is separable} \iff \gcd(f, f') = 1.$$

Proof. Let L be a splitting field of f. Then

$$\begin{aligned} f \text{ separable} &\iff f \text{ and } f' \text{ have no common roots in } L \\ &\iff \gcd(f, f') = 1 \text{ in } L[X] \\ &\iff \gcd(f, f') = 1 \text{ in } K[X] \end{aligned}$$

□

Theorem 5.5. Let $f \in K[X]$ irreducible. Then f is separable unless $\mathrm{char}(K) = p > 0$ and $f(X) = g(X^p)$ for some $g \in K[X]$.

Proof. Assume f is monic. Since f is irreducible, $\gcd(f, f') = 1$ or f. If $f' \neq 0$ then since $\deg f' < \deg f$ we have $\gcd(f, f') \neq f$, so $\gcd(f, f') = 1$, and f is separable. Now suppose that $f' = 0$. If $f = \sum_{i=0}^{d} c_i X^i$ then $f' = \sum_{i=1}^{d} i c_i X^{i-1}$. So $f' = 0 \implies i c_i = 0 \ \forall 1 \leq i \leq d$.

If $\mathrm{char}(K) = 0$, then this implies that $c_i = 0$ for all $1 \leq i \leq d$, so f is constant (hence not irreducible). If $\mathrm{char}(K) = p > 0$ we still get $c_i = 0$ for all i with $p \nmid i$. Therefore $f(X) = g(X^p)$ for some $g \in K[X]$. □

Definition (Separable element / extension)**.** Let L/K be a field extension. We define:

(i) $\alpha \in L$ is *separable* over K if it is algebraic over K and its minimal polynomial if separable.

(ii) L/K is *separable* if every $\alpha \in L$ is separable over K (in particular L/K is algebraic).

Theorem 5.6 (Theorem of the Primitive Element)**.** If L/K is finite and separable then L/K is simple (that is, $L = K(\theta)$ for some $\theta \in L$).

Proof. Write $L = L(\alpha_1, \dots, \alpha_n)$ for some $\alpha_i \in L$. We must show that $L = K(\theta)$ for some $\theta \in L$. It suffices to prove the case $n = 2$, since the general case follows by induction on n.

Write $L = K(\alpha, \beta)$, and let f and g be the minimal polynomials of α and β over K. Let M be a splitting field for fg over L. Write

$$f(X) = \prod_{i=1}^{r} (X - \alpha_i), \qquad \alpha_i \in M, \alpha = \alpha_1$$

$$g(X) = \prod_{i=1}^{s} (X - \beta_i), \qquad \beta_i \in M, \beta = \beta_1$$

Now L/K separable implies β separable over K, which implies $\beta_1, \dots, \beta_s$ are distinct. We pick some $c \in K$ and let $\theta = \alpha + c\beta$. Let $F(X) = f(\theta - cX) \in K(\theta)[X]$. Then $F(\beta) = f(\theta - c\beta) = f(\alpha) = 0$, and $g(\beta) = 0$.

If $\beta_2, \dots, \beta_s$ are not roots of F then

$$\begin{aligned} \gcd(F, g) = X - \beta \text{ in } M[X] &\implies \gcd(F, g) = X - \beta \text{ in } K(\theta)[X] \\ &\implies \beta \in K(\theta) \end{aligned}$$

But then $\alpha = \theta - c\beta \in K(\theta)$ so $K(\alpha, \beta) \subset K(\theta)$. But clearly $K(\theta) \subset K(\alpha, \beta)$, and hence $L = K(\alpha, \beta) = K(\theta)$.

We are done unless $F(\beta_j) = 0$ for some $2 \le j \le s$. In this case, we have $f(\theta - c\beta_j) = 0$ for some $2 \le j \le s$, and so $\alpha + c\beta = \alpha_i + c\beta_j$ for some $1 \le i \le r$, $2 \le j \le s$. If $|K| = \infty$ then since $\beta \notin \{\beta_2, \dots, \beta_s\}$ we can pick $c \in K$ such that this never happens. If $|K| < \infty$, then $|L| < \infty$ and by Proposition 1.3, L^* is cyclic and generated by θ (say). Then $L = K(\theta)$. □

Start of lecture 10

Remark. Theorem 5.5 and Theorem 5.6 show that if $[K : \mathbb{Q}] < \infty$ then $K = \mathbb{Q}(\alpha)$ for some $\alpha \in K$.

One aim for today: Show that if L/K is a field extension and $\alpha_1, \dots, \alpha_n \in L$, then

$$\alpha_1, \dots, \alpha_n \text{ are separable over } K \implies K(\alpha_1, \dots, \alpha_n)/K \text{ is separable}$$

Notation. Let L/K and M/K be field extensions. We write

$$\operatorname{Hom}_k(L, M) = \{K\text{-embeddings } L \hookrightarrow M\}$$

Lemma 5.7. Let $[L : K] < \infty$. Suppose $L = K(\alpha)$ and f is the minimal polynomial of α over K. Let M/K be any field extension. Then

$$\# \operatorname{Hom}_K(L, M) \leq [L : K],$$

with equality if and only if f splits into linear factors over M.

Proof. By Theorem 3.2,

$$\begin{aligned} \# \operatorname{Hom}_K(L, M) &= \#\{\text{roots of } f \text{ in } M\} \\ &\leq \deg f = [L : K] \end{aligned}$$

with equality if and only if f splits into discinct linear factors over M. □

Theorem 5.8. Let $[L : K] < \infty$. Write $L = K(\alpha_1, \ldots, \alpha_n)$ and let f_i be the minimal polynomial of α_i over K. Let M/K be any field extension. Then

$$\# \operatorname{Hom}_K(L, M) \leq [L : K]$$

with equality if and only if each f_i splits into distinct linear factors over M.

Note that Lemma 5.7 is the case $n = 1$.

Obvious variant of Theorem 5.8: Let $\sigma : K \hookrightarrow M$ be an embedding. Then

$$\#\{\sigma\text{-homomorphisms } L \to M\} \leq [L : K]$$

with equality if and only if each $\sigma(f_i)$ splits into distinct linear factors over M.

We'll use this variant in the induction argument.

Proof of Theorem 5.8. By induction on n. The case $n = 1$ is proved in Lemma 5.7. So suppose $n > 1$. Let $K_1 = K(\alpha_1)$. Then Lemma 5.7 implies

$$\# \operatorname{Hom}_K(K, M) \leq [K_1 : K] \tag{1}$$

$$
\begin{tikzcd}
K(\alpha_1,\dots,\alpha_n)=L \arrow[rr, dashed] \arrow[d, dash] & & M \\
K(\alpha_1)=K_1 \arrow[urr, dashed, "\sigma"] \arrow[d, dash] & & \\
K \arrow[uurr] & &
\end{tikzcd}
$$

Let $\sigma \in \operatorname{Hom}_K(K_1, M)$. By the induction hypothesis,

$$\#\{\sigma\text{-homomorphisms } L = K_1(\alpha_2, \dots, \alpha_n) \to M\} \leq [L : K_1] \tag{2}$$

Then Tower Law with (1) and (2) gives

$$\# \operatorname{Hom}_K(L, M) \leq [L : K_1][K_1 : K] = [L : K]$$

If equality holds then equality holds in both (1) and (2).

Equality in (1) implies f_1 splits into distinct linear factors over M. Reordering the α_i gives the same conclusion for all the f_i. Conversely, if each f_i splits into distinct linear factors over M then Lemma 5.7 gives equality in (1).

For $2 \leq i \leq n$, the minimal polynomial of α_i over K_1 divides f_i and so splits into distinct linear factors over M. Then the induction hypothesis implies that equality holds in (2). Since we now have equality in both (1) and (2), it follows that $\# \operatorname{Hom}_K(L, M) = [L : K]$. □

Corollary 5.9. Let $[L : K] < \infty$. Write $L = K(\alpha_1, \dots, \alpha_n)$ and let f_i be the minimal polynomial of α_i over K. Let M/K be any field extension in which $\prod f_i$ splits as a product of linear factors (for example $M = \overline{K}$). Then the following are equivalent:

(i) L/K is separable.

(ii) Each α_i is separable over K.

(iii) Each f_i splits into distinct linear factors over M.

(iv) $\# \operatorname{Hom}_K(L, M) = [L : K]$.

Proof. (i) $\implies$ (ii) $\implies$ (iii) by definition.

(iii) $\implies$ (iv) see Theorem 5.8.

(iv) $\implies$ (i) Let $\beta \in L$. Applying Lemma 5.7 to $L = K(\alpha_1, \ldots, \alpha_n, \beta)$ shows that β is separable over K. $\square$

Remark. (ii) $\implies$ (i) is the result promised at the start of the lecture.

(i) $\iff$ (iv) is a useful characterisation of separable extensions.

Example 5.10. Let K be any field. The polynomial $T^n - Y \in K[Y,T]$ is irreducible (it suffices to consider factorisations of the form $f(T)(g(T) + Yh(T))$ where $f, g, h \in K[T]$).

Since $K[Y]$ is a UFD with field of fractions $K(Y)$, it follows by Gauss's Lemma that

$$T^n - Y \in K(Y)[T] \tag{$*$}$$

is irreducible. The field extension $K(X)/K(X^n)$ is generated by X which is a root of $T^n - X^n \in K(X^n)[T]$. Putting $Y = X^n$ in $(*)$ shows this is irreducible. Therefore $[K(X) : K(X^n)] = n$. Now take $K = \mathbb{F}_p$ and $n = p$ (p a prime). We claim that $\mathbb{F}_p(X)/\mathbb{F}_p(X^p)$ is an inseparable extension of degree p. Indeed, the minimal polynomial of X over $\mathbb{F}_p(X^p)$ is $f(T) = T^p - X^p \in \mathbb{F}_p(X^p)[T]$, which is inseparable since $f(T) = (T - X)^p$ (compare to Proposition 1.4).

Start of

lecture 11

6 Galois Extensions

Definition (automorphism)**.** An *automorphism* of a field L is a bijective homomorphism $\sigma : L \to L$. We write $\operatorname{Aut}(L)$ for the group of automorphisms of L under composition, i.e.

$$(\sigma\tau)(x) = \sigma(\tau(x)).$$

Exercise: Check inverses (i.e. check that σ^{-1} is a homormorphism).

Definition. Let L/K be a field extension. A K-automorphism of L is an automorphism $\sigma \in \operatorname{Aut}(L)$ whose restriction to K is the identity map. The K-automorphisms of L form a subgroup $\operatorname{Aut}(L/K) \subset \operatorname{Aut}(L)$.

Remark.

(i) $\operatorname{Aut}(\mathbb{Q})$ and $\operatorname{Aut}(\mathbb{F}_p)$ are both trivial. Therefore $\operatorname{Aut}(L) = \operatorname{Aut}(L/K)$ where K is the prime subfield of L.

(ii) If $[L : K] < \infty$ then any K-embedding $L \to L$ is surjective (by rank-nullity), i.e.

$$\operatorname{Hom}_k(L, L) = \operatorname{Aut}(L/K)$$

Lemma 6.1. Let L/K be a finite extension. Then

$$\# \operatorname{Aut}(L/K) \leq [L : K]$$

Proof. Take $M = L$ in Theorem 5.8. □

Definition. If $S \subset \operatorname{Aut}(L)$ is any subset we define the *fixed field* of S to be

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

This is a subfield of L.

Definition. A field extension L/K is *Galois* if it is algebraic and

$$K = L^{\operatorname{Aut}(L/K)}$$

Example.

(i) $\mathrm{Aut}(\mathbb{C}/\mathbb{R}) = \{1, \tau\}$ where τ is complex conjugation. If $z \in \mathbb{C}$, then

$$z \in \mathbb{R} \iff \tau(z) = z$$

therefore $\mathbb{C}/\mathbb{R}$ is Galois.

(ii) Let $L = \mathbb{Q}(\sqrt{2})$. $f(X) = X^2 - 2$.

$$\mathrm{Aut}(L/\mathbb{Q}) \leftrightarrow \{\text{roots of } f \text{ in } L\}$$

Therefore $\mathrm{Aut}(L/\mathbb{Q}) = \{1, \tau\}$ where $\tau : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$, $a + b\sqrt{2} \mapsto a - b\sqrt{2}$, $a, b \in \mathbb{Q}$.

$$\begin{aligned} L^\tau &= \{a + b\sqrt{2} \mid a + b\sqrt{2} = a - b\sqrt{2}\} \\ &= \{a + b\sqrt{2} \mid b = 0\} \\ &= \mathbb{Q} \end{aligned}$$

Therefore $L/\mathbb{Q}$ is Galois.

(iii) Let $L = \mathbb{Q}(\sqrt[3]{2})$, $f(X) = X^3 - 2$. Then

$$\mathrm{Aut}(L/\mathbb{Q}) \leftrightarrow \{\text{roots of } f \text{ in } L\}$$

Since $L \subset \mathbb{R}$ we see that $\# \mathrm{Aut}(L/\mathbb{Q}) = 1$. Therefore $L/\mathbb{Q}$ is not Galois.

(iv) Let $K/\mathbb{F}_p$ be a finite extension ($\implies |K| < \infty$). Let $\phi : K \to K$, $x \mapsto x^p$. By Proposition 1.4, $\phi \in \mathrm{Aut}(K/\mathbb{F}_p)$. Then

$$\begin{aligned} K^\phi &= \{x \in K \mid \phi(x) = x\} \\ &= \{\text{roots of } X^p - X \text{ in } K\} \\ &\supset \mathbb{F}_p \end{aligned}$$

(with equality in the $\supset$ by Lemma 1.1). Therefore $K/\mathbb{F}_p$ is Galois.

Theorem 6.2 (Classification of finite Galois extensions)**.** Let $[L : K] < \infty$ and $G = \operatorname{Aut}(L/K)$. Then the following are equivalent:

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

(ii) L/K is normal and separable.

(iii) L is the splitting field of a separable over K.

(iv) $\#G = [L : K]$ (i.e. equality holds in Lemma 6.1).

Proof. (i) $\implies$ (ii) Let $\alpha \in L$ and $\{\sigma(\alpha) : \sigma \in G\} = \{\alpha_1, \dots, \alpha_m\}$ with $\alpha_1, \dots, \alpha_m$ distinct. Let $f(X) = \prod_{i=1}^m (X - \alpha_i)$. We let $\sigma \in G$ act on $L[X]$ via

$$\sigma\left(\sum c_i X^i\right) = \sum \sigma(c_i) X^i$$

Since G permutes the α_i we have $\sigma f = f$ $\forall \sigma \in G$. L/K Galois implies $f \in K[X]$. Let g be the minimal polynomial of α over K. Since $f(\alpha) = 0$ we have $g \mid f$. Since $g(\sigma(\alpha)) = \sigma(g(\alpha)) = 0$ $\forall \sigma \in G$, every root of f is a root of g. By construction f is separable and monic, so $f = g$. Therefore the minimal polynomial of α over K splits into distinct linear factors over L. Since $\alpha \in L$ is arbitrary, this shows that L/K is normal and separable.

(ii) $\implies$ (iii) By Theorem 5.8, L is the splitting field of some $f \in K[X]$. Write $f = \prod_{i=1}^m f_i^{e_i}$ where ther $f_i \in K[X]$ are distinct and irreducible, and $e_i \geq 1$. Since L/K is separable, each f_i is separable. Moreover, $\gcd(f_i, f_J) = 1$ in $K[X]$ so by Lemma 5.3, $\gcd(f_i, f_j) = 1$ in $L[X]$. Therefore $g = \prod_{i=1}^m f_i$ is separable, and L is a splitting field for g over K.

(iii) $\implies$ (iv) Let L be the splitting field of a separable $f \in K[X]$. Then $L = K(\alpha_1, \dots, \alpha_n)$ where $\alpha_1, \dots, \alpha_n$ are the roots of f. The minimal polynomial f_i of each α_i divides f and so splits into distinct linear factors over L. Taking $M = L$ in Theorem 5.8 gives $\# \operatorname{Aut}(L/K) = [L : K]$.

(iv) $\implies$ (i) $G \subset \operatorname{Aut}(L/L^G) \subset \operatorname{Aut}(L/K) = G$. Therefore $G = \operatorname{Aut}(L/L^G)$.

$$\implies [L : K] \overset{\text{by (iv)}}{=} \#G = \# \operatorname{Aut}(L/L^G) \overset{\text{Lemma 6.1}}{\leq} [L : L^G]$$

So by Tower Law,

$$\cancel{[L : L^G]}[L^G : K] \leq \cancel{[L : L^G]}$$

so $L^G = K$. $\square$

Definition (Galois group)**.** If L/K is a Galois extension then we write $\mathrm{Gal}(L/K)$ for $\mathrm{Aut}(L/K)$ (we call this the *Galois group of* L *over* K).

Start of lecture 12

Remark 6.3. We saw in the proof of (i) $\implies$ (ii) that if L/K is Galois, $G = \mathrm{Gal}(L/K)$, and $\alpha \in L$ then the minimal polynomial of α over K is

$$\prod_{i=1}^{m}(X - \alpha_i)$$

where $\alpha_1, \dots, \alpha_m$ are the distinct elements of $\mathrm{ord}_G(\alpha) = \{\sigma(\alpha) : \sigma \in G\}$.

Theorem 6.4 (Fundamental Theorem of Galois Theory)**.** Let L/K be a finite Galois extension, $G = \mathrm{Gal}(L/K)$.

(a) Let F be an intermediate field, i.e. $K \subset F \subset L$. Then L/F is Galois and $\mathrm{Gal}(L/F)$ is a subgroup of G.

(b) There is an inclusion reversing bijection

$$\begin{aligned} \{\text{intermediate fields } K \subset F \subset L\} &\to \{\text{subgroups } H \subset G\} \\ F &\mapsto \mathrm{Gal}(L/F) \\ L^H &\leftarrow\!\shortmid H \end{aligned}$$

(c) Let F be an intermediate field, i.e. $K \subset F \subset L$. Then

$$\begin{aligned} F/K \text{ Galois} &\iff \sigma F = F \ \forall \sigma \in G \\ &\iff H = \mathrm{Gal}(L/F) \text{ is a normal subgroup of } G \end{aligned}$$

In this case the restriction map

$$\begin{aligned} G &\to \mathrm{Gal}(F/K) \\ \sigma &\mapsto \sigma|_F \end{aligned}$$

is surjective with kernel H, and so

$$\mathrm{Gal}(F/K) \cong G/H$$

(a quotient of G).

Proof.

(a) By Theorem 6.2, L is the splitting field over K of some separable polynomial $f \in K[X]$. Then L is the splitting field of f over F. So L/F is Galois. $\mathrm{Gal}(L/F)$ is a subgroup of $\mathrm{Gal}(L/K)$ since any automorphism of L acting as the identity on F also acts as the identity on K.

(b) To show we have a bijection, we need to check both compositions are the identity.

  (i) $F = L^{\mathrm{Gal}(L/F)}$: This holds since L/F is Galois.

  (ii) $\mathrm{Gal}(L/L^H) = H$: we certainly have $H \subset \mathrm{Gal}(L/L^H)$ so it suffices to show $\#\,\mathrm{Gal}(L/L^H) \leq \#H$. Let $F = L^H$. As L/F is finite and separable, the Theorem of the Primitive Element tells us that $L = F(\alpha)$ for some $\alpha \in L$. Then α is a root of
$$f(X) = \prod_{\sigma \in H} (X - \sigma(\alpha))$$
which has coefficients in $L^H = F$. Therefore $\#\,\mathrm{Gal}(L/L^H) = [L : L^H] = [F(\alpha) : F] \leq \deg f = \#H$.

If $F_1 \subset F_2$ then $\mathrm{Gal}(L/F_2) \subset \mathrm{Gal}(L/F_1)$, so the bijection reverses inclusions.

(c) We first show
$$F/K \text{ Galois} \iff \sigma F = F \ \forall \sigma \in G.$$

$\Rightarrow$ Let $\alpha \in F$ have minimal polynomial f over K. For any $\sigma \in G$, $\sigma(\alpha)$ is a root of f. Since F/K is normal we have $\sigma(\alpha) \in F$, so $\sigma F \subset F$. As $[\sigma F : K] = [F : K]$, it follows that $\sigma F = F$.

$\Leftarrow$ Let $\alpha \in F$. By Remark 6.3, its minimal polynomial over K is
$$f(X) = \prod_{i=1}^{m} (X - \alpha_i)$$
where $\alpha_1, \ldots, \alpha_m$ are the distinct elements of $\{\sigma(\alpha) : \sigma \in G\}$. The assumption $\sigma(F) = F \ \forall \sigma \in G$ tells us that $\alpha_1, \ldots, \alpha_m \in F$. This shows F/K is normal. But also, L/K Galois, so so L/K is separable, so F/K is separable. Hence F/K is normal and separable, so by Theorem 6.2, F/K is Galois.

Suppose $H \subset G$ corresponds to $F = L^H$. For $\sigma \in G$,
$$\begin{aligned}
L^{\sigma H \sigma^{-1}} &= \{x \in L \mid \sigma\tau\sigma^{-1}(x) = x \ \forall \tau \in H\} \\
&= \{x \in L \mid \tau\sigma^{-1}(x) = \sigma^{-1}(x) \ \forall \tau \in H\} \\
&= \{x \in L \mid \sigma^{-1}(x) \in L^H = F\} \\
&= \sigma F
\end{aligned}$$

So

$$\begin{aligned} \sigma F = F \ \forall \sigma \in G &\iff L^{\sigma H \sigma^{-1}} = L^H \ \forall \sigma \in G \\ &\iff \sigma H \sigma^{-1} = H \ \forall \sigma \in G \\ &\iff H \subset G \text{ is a normal subgroup} \end{aligned}$$

Consider the restriction map

$$\begin{aligned} G = \mathrm{Gal}(L/K) &\mapsto \mathrm{Gal}(F/K) \\ \sigma &\mapsto \sigma|_F \end{aligned}$$

Then

$$\ker(\mathrm{res}) = \{\sigma \in \mathrm{Gal}(L/K) \mid \sigma(x) = x \ \forall x \in F\} = \mathrm{Gal}(L/F) = H$$

Therefore $G/H \cong \mathrm{Im}(\mathrm{res}) \leq \mathrm{Gal}(F/K)$. But,

$$\#(G/H) = \frac{\#G}{\#H} = \frac{[L:K]}{[L:F]} = [F:K] = \#\,\mathrm{Gal}(F/K).$$

Therefore res is surjcetive and $\mathrm{Gal}(F/K) \cong G/H$. $\square$

Example 6.5. Let $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$. $K/\mathbb{Q}$ is the splitting field of the polynomial $(X^2 - 2)(X^2 - 3)$. Therefore $K/\mathbb{Q}$ is normal. Separability is automatic in char $= 0$, hence $K/\mathbb{Q}$ is Galois. If $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$, then it is uniquely determined by $\sigma(\sqrt{2})$ and $\sigma(\sqrt{3})$. Since $\sigma(\sqrt{2}) = \pm\sqrt{2}$ and $\sigma(\sqrt{3}) = \pm\sqrt{3}$, we have

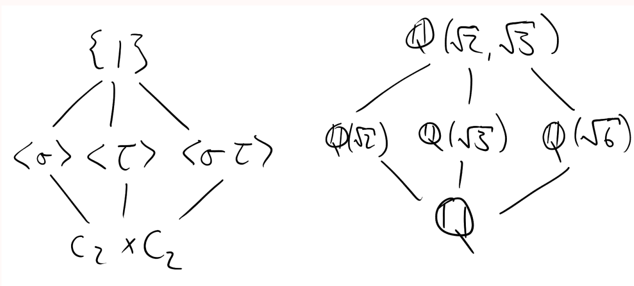
$$\#\,\mathrm{Gal}(K/\mathbb{Q}) \leq 4.$$

We saw in Example 1.11 that $[K : \mathbb{Q}] = 4$. Hence $\#\,\mathrm{Gal}(K/\mathbb{Q}) = 4$. Let

$$\sigma : \sqrt{2} \mapsto \sqrt{2}; \sqrt{3} \mapsto -\sqrt{3}$$

$$\tau : \sqrt{2} \mapsto -\sqrt{2}; \sqrt{3} \mapsto \sqrt{3}$$

Then $\sigma^2 = \tau^2 = \mathrm{id}$ and $\sigma\tau = \tau\sigma$, so $\mathrm{Gal}(K/\mathbb{Q}) \cong C_2 \times C_2$.



Start of lecture 13

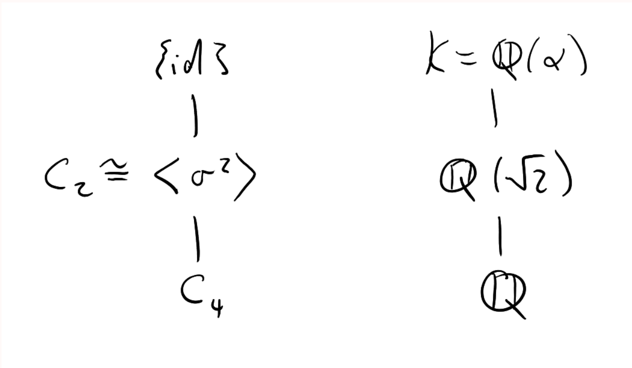
Example 6.6. Let $K = \mathbb{Q}(\alpha)$ where $\alpha = \sqrt{2+\sqrt{2}}$. Then $(\alpha^2 - 2)^2 = 2$, so α is a root of $f(X) = X^4 - 4X^2 + 2$. This is irreducible in $\mathbb{Z}[X]$ by Eisenstein's criterion with $p = 2$. Therefore it is irreducible in $\mathbb{Q}[X]$ by Gauss' Lemma, so $[K : \mathbb{Q}] = 4$.

Now $(2+\sqrt{2})(2-\sqrt{2}) = 2$, so f has roots $\pm\alpha, \pm\frac{\sqrt{2}}{\alpha}$ (note $\sqrt{2} = \alpha^2 - 2$). Therefore K is a splitting field for f over $\mathbb{Q}$, so $K/\mathbb{Q}$ is normal hence Galois (since separability is automatic in $\operatorname{char} 0$).

If $\sigma \in \operatorname{Gal}(K/\mathbb{Q})$ then it is uniquely determined by $\sigma(\alpha)$. But $\sigma(\alpha) \in \{\pm\alpha, \pm\sqrt{2}/\alpha\}$, and $\#\operatorname{Gal}(K/\mathbb{Q}) = [K : \mathbb{Q}] = 4$, so all possibilities must occur (could see this more directly using Theorem 3.2). We fix $\sigma \in \operatorname{Gal}(K/\mathbb{Q})$ with $\sigma(\alpha) = \frac{\sqrt{2}}{\alpha}$, hence $\sigma(\alpha^2) = \frac{2}{\alpha^2}$, so $\sigma(2+\sqrt{2}) = 2 - \sqrt{2}$, so $\sigma(\sqrt{2}) = -\sqrt{2}$.

Therefore
$$\sigma^2(\alpha) = \sigma\left(\frac{\sqrt{2}}{\alpha}\right) = -\frac{\sqrt{2}}{\left(\frac{\sqrt{2}}{\alpha}\right)} = -\alpha$$

Therefore $\sigma^2 \neq \mathrm{id}$, but $\sigma^4 = \mathrm{id}$. So
$$\operatorname{Gal}(K/\mathbb{Q}) \cong C_4$$



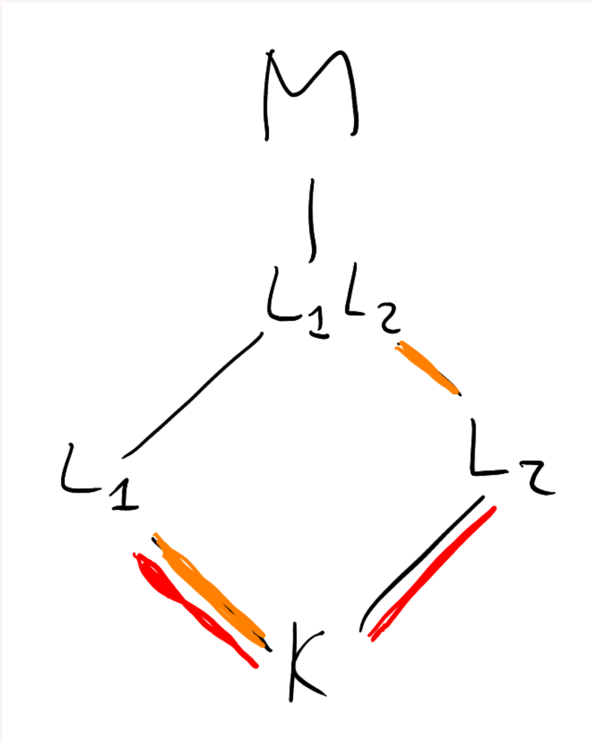
Definition (Composite subfield)**.** Let L_1, L_2 be subfields of a field M. The *composite* L_1L_2 is the smallest subfield of M to contain both L_1 and L_2. (This exists since the intersection of any collection of subfields is a subfield).

Theorem 6.7. Let $[M : k] < \infty$ and let L_1, L_2 be intermediate fields i.e. $K \subset L_i \subset M$ for $i = 1, 2$.

(i) If L_1/K is Galois then L_1L_2/L_2 is Galois and there is an injective group homomorphism

$$\mathrm{Gal}(L_1L_2/L_2) \hookrightarrow \mathrm{Gal}(L_1/K)$$

This is surjective if and only if $L_1 \cap L_2 = K$.



(ii) If L_1/K and L_2/K are both Galois then L_1L_2/K is Galois and there is an injective group homomorphism

$$\mathrm{Gal}(L_1L_2/K) \hookrightarrow \mathrm{Gal}(L_1/K) \times \mathrm{Gal}(L_1/K)$$

This is surjective if and only if $L_1 \cap L_2 = K$.

Proof.

(i) L_1/K Galois $\implies$ L_1 is the splitting field of some separable polynomial $f \in K[X]$. Then L_1L_2 is a splitting field for f over L_2. Therefore L_1L_2/L_2 is Galois. If $\sigma \in \mathrm{Gal}(L_1L_2/L_2)$, then $\sigma|_K = \mathrm{id}$ and since L_1/K is normal we have $\sigma(L_1) \subset L_1$.

We consider the group homomorphism

$$\begin{aligned} \mathrm{Gal}(L_1L_2/L_2) &\xrightarrow{\text{res}} \mathrm{Gal}(L_1/K) \\ \sigma &\longmapsto \sigma|_{L_1} \end{aligned}$$

It is injective since if $\sigma|_{L_1} = \mathrm{id}$ then σ acts trivially on both L_1 and L_2 and hence on L_1L_2. Now suppose $L_1 \cap L_2 = K$. Then L_1/K is finite and separable. So by Theorem of the Primitive Element, $L_1 = K(\alpha)$ for some $\alpha \in L_1$. Let $f \in K[X]$ be the minimal polynomial of α over K. Suppose $f = gh$ for some $g, h \in L_2[X]$, $\deg g, \deg h > 0$. Then f splits into linear factors over L_1, so g and h have coefficients in $L_1 \cap L_2 = K$, which contradicts the fact that f is irreducible over K. Therefore f is irreducible in $L_2[X]$. Therefore

$$[L_1 : K] = \deg f = [L_1L_2 : L_2]$$

The map res is therefore an isomorphism. Conversely, if $\mathrm{Im}(\text{res}) \subset \mathrm{Gal}(L_1/L_1 \cap L_2) \subset \mathrm{Gal}(L_1/K)$. So if res is surjective then $L_1 \cap L_2 = K$.

(ii) L_i/K Galois $\implies$ L_i is a splitting field of some separable polynomial $f_i \in K[X]$. Then L_1L_2 is the splitting field of the separable $\mathrm{lcm}(f_1, f_2)$. Therefore L_1L_2/K is Galois.

$$\begin{aligned} \text{It is surjective} &\iff [L_1L_2 : K] = [L_1 : k][L_2 : K] \\ &\iff [L_1L_2 : L_2]\cancel{[L_2 : K]} = [L_1 : K]\cancel{[L_2 : K]} \\ &\overset{\text{(i)}}{\iff} L_1 \cap L_2 = K \end{aligned}$$

□

Theorem 6.8. Let L/K be finite and separable. Then there exists a finite extension M/L such that

(i) M/K is Galois.

(ii) If $L \subset M' \subset M$ and M'/K is Galois then $M' = M$.

We say M/K is a *Galois closure* of L/K.

Proof. By Theorem of the Primitive Element, $L = K(\alpha)$ for some $\alpha \in L$. Let f be the minimal polynomial of α over K. Then L/K separable implies f is separable. Let M be a splitting field for f over L. Since $L = K(\alpha)$ where α is a root of f, it follows that M is a splitting field of f over K. Now Theorem 6.2 implies that M/K is Galois. Let M' as (ii). As $\alpha \in M'$ and M'/K is normal, f splits into linear factors over M'. Hence $M' = M$. □

Start of lecture 14

Example. $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ has Galois closure $\mathbb{Q}(\omega, \sqrt[3]{2})/\mathbb{Q}$ where $\omega = e^{2\pi i/3}$.

7 Trace and Norm

Let L/K be a finite extension, say $[L:K]=n$. For $\alpha \in L$ the map

$$\begin{aligned} L &\xrightarrow{m_\alpha} L \\ x &\longmapsto \alpha x \end{aligned}$$

is a K-linear endomorphism of L, hence has a trace and a determinant.

Definition (Trace and norm)**.** The *trace* and *norm* of α are

$$\mathrm{Tr}_{L/K}(\alpha) = \mathrm{Tr}(m_\alpha) \qquad N_{L/K}(\alpha) = \det(m_\alpha)$$

Concretely, if L has K-basis $v_1, \dots, v_n$ and $A = (a_{ij})$ is the unique $n \times n$ matrix with entries in K such that

$$\alpha(v_j) = \sum_{i=1}^n a_{ij} v_i \qquad \text{and} \qquad \forall 1 \le j \le n$$

then

$$\mathrm{Tr}_{L/K} = \mathrm{Tr}\, A \qquad \text{and} \qquad N_{L/K}(\alpha) = \det(A)$$

Example. $K=\mathbb{Q}$, $L=\mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z}$ not a square. If $\alpha = x + y\sqrt{d}$, $x, y \in \mathbb{Q}$, then (since L has K-basis $1, \sqrt{d}$):

$$\begin{aligned} \mathrm{Tr}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\alpha) &= \mathrm{Tr}\begin{pmatrix} x & dy \\ y & x \end{pmatrix} = 2x \\ N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\alpha) &= \det\begin{pmatrix} x & dy \\ y & x \end{pmatrix} = x^2 - dy^2 \end{aligned}$$

Lemma 7.1.

(i) $\operatorname{Tr}_{L/K} : L \to K$ is a K-linear map.

(ii) $N_{L/K} : L \to K$ is multiplicative, i.e.

$$N_{L/K}(\alpha\beta) = N_{L/K}(\alpha)N_{L/K}(\beta) \qquad \forall \alpha, \beta \in L$$

(iii) If $\alpha \in K$ tehn

$$\begin{aligned} \operatorname{Tr}_{L/K} &= [L:K]\alpha \\ N_{L/K}(\alpha) &= \alpha^{[L:K]} \end{aligned}$$

(iv) If $\alpha \in L$ then

$$N_{L/K}(\alpha) = 0 \iff \alpha = 0.$$

Proof. (i) and (ii) follow from the corrsponding statements for traces and determinants.

For (iii), if $\alpha \in K$ then m_α is represented by

$$\begin{pmatrix} \alpha & 0 & \cdots & 0 \\ 0 & \alpha & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & \alpha \end{pmatrix}$$

which has trace and determinant as indicated.

For (iv), note

$$N_{L/K}(\alpha) \neq 0 \iff m_\alpha \text{ is invertible} \iff \alpha \neq 0$$

□

Lemma 7.2. Let $M/L/K$ be a field extension and $\alpha \in L$. Then

$$\begin{aligned} \operatorname{Tr}_{M/K}(\alpha) &= [M:L] \operatorname{Tr}_{L/K}(\alpha) \\ N_{M/K}(\alpha) &= N_{L/K}(\alpha)^{[M:L]} \end{aligned}$$

Proof. If A represents m_α with respect to some basis for L/K and B represents m_α with respect to some basis for M/K picked by following the proof of the Tower Law, then

$$B = \begin{pmatrix} A & 0 & \cdots & 0 \\ 0 & A & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & A \end{pmatrix}$$

where A is $[L:K] \times [L:K]$ and B is $[M:K] \times [M:K]$. Then

$$\mathrm{Tr}(B) = [M:L]\,\mathrm{Tr}(A) \qquad \text{and} \qquad \det(B) = \det(A)^{[M:L]}.$$ □

Theorem 7.3. Let $[L:K] < \infty$. Let $\alpha \in L$. Let f be the minimal polynomial of α over K, say

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0 \qquad a_i \in K$$

Then

$$\begin{aligned} \mathrm{Tr}_{L/K}(\alpha) &= -m a_{n-1} \\ N_{L/K}(\alpha) &= ((-1)^n a_0)^m \end{aligned}$$

where $m = [L : L(\alpha)]$.

Proof. By Lemma 7.2 without loss of generality $L = K(\alpha)$, i.e. $m = 1$. If A represents m_α with respect to basis $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$ then

$$A = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -a_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

Therefore

$$\begin{aligned} \mathrm{Tr}_{L/K}(\alpha) &= \mathrm{Tr}(A) = -a_{n-1} \\ N_{L/K}(\alpha) &= \det(A) = (-1)^n a_0 \end{aligned}$$ □

Example. $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{d})$

$$\begin{aligned} \alpha = x + y\sqrt{d} &\implies (\alpha - x)^2 = dy^2 \\ &\implies \alpha \text{ is a root of } T^2 - \underbrace{2x}_{\text{trace}}T + \underbrace{x^2 - dy^2}_{\text{norm}} = 0 \end{aligned}$$

Theorem 7.4 (Transitivity of trace and norm)**.** Let $M/L/K$ be a finite extension and $\alpha \in M$. Then

$$\operatorname{Tr}_{M/K}(\alpha) = \operatorname{Tr}_{L/K}(\operatorname{Tr}_{M/L}(\alpha))$$
$$N_{M/K}(\alpha) = N_{L/K}(N_{M/L}(\alpha))$$

Proof (sketch – non-examinable). By Lemma 7.2, without loss of generality $M = L(\alpha)$. Let f be the minimal polynomial of α over L, say

$$f(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0, \qquad a_i \in L$$

L/K has basis $v_1, \dots, v_m$ and M/L has basis $1, \alpha, \alpha^2, \dots, \alpha^{n-1}$. If A_i represents m_{a_i} with respect to $v_1, \dots, v_m$ and B represents m_α with respect to $(v_i\alpha^{j-1})_{\substack{1\le i\le m\\ 1\le j\le n}}$ then

$$B = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -A_0 \\ I & 0 & 0 & \cdots & 0 & -A_1 \\ 0 & I & 0 & \cdots & 0 & -A_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -A_{n-2} \\ 0 & 0 & 0 & \cdots & I & -A_{n-1} \end{pmatrix}$$

(A_i is $m \times m$, B is $mn \times mn$). We compute

$$\begin{aligned} \operatorname{Tr}_{M/K} &\overset{\text{defn}}{=} \operatorname{Tr}(B) \\ &= -\operatorname{Tr}(A_{n-1}) \\ &\overset{\text{defn}}{=} \operatorname{Tr}_{L/K}(-a_{n-1}) \\ &\overset{\text{Theorem 7.3}}{=} \operatorname{Tr}_{L/K}(\operatorname{Tr}_{M/L}(\alpha)) \\ N_{M/K}(\alpha) &\overset{\text{defn}}{=} \det(B) \\ &\overset{\text{exercise}}{=} (-1)^{mn}\det(A_0) \\ &\overset{\text{defn}}{=} N_{L/K}((-1)^n a_0) \\ &\overset{\text{Theorem 7.3}}{=} N_{L/K}(N_{M/L}(\alpha)) \end{aligned}$$

□

Theorem 7.5. Let L/K be a finite Galois extension with $G = \operatorname{Gal}(L/K)$. Let $\alpha \in L$. Then

$$\operatorname{Tr}_{L/K}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha) \qquad \text{and} \qquad N_{L/K}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha)$$

Proof. By Remark 6.3, the minimal polynomial of α over K is

$$f(X) = \prod_{i=1}^{n} (X - \alpha_i)$$

where $\mathrm{orb}_G(\alpha) = \{\alpha_1, \ldots, \alpha_n\}$. Let $m = [L : K(\alpha)] = \# \mathrm{Stab}_G(\alpha)$. Now

$$\begin{aligned} \mathrm{Tr}_{L/K}(\alpha) &\overset{\text{Theorem 7.3}}{=} m \sum_{i=1}^{n} \alpha_i = \sum_{\sigma \in G} \sigma(\alpha) \\ N_{L/K}(\alpha) &\overset{\text{Theorem 7.3}}{=} \left(\prod_{i=1}^{n} \alpha) i \right)^m = \prod_{\sigma \in G} \sigma(\alpha) \end{aligned}$$

where the final equality on each line follows by the proof of Orbit-Stabiliser Theorem. □

Example. $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{d})$. $\mathrm{Gal}(L/K) = \{1, \sigma\}$, $\sigma(\sqrt{d}) = -\sqrt{d}$. Then for $\alpha = x + y\sqrt{d}$, $x, y \in \mathbb{Q}$,

$$\begin{aligned} \mathrm{Tr}_{L/K}(\alpha) &= (x + y\sqrt{d}) = (x + y\sqrt{d}) + (x - y\sqrt{d}) = 2x \\ N_{L/K}(\alpha) &= (x + y\sqrt{d})(x - y\sqrt{d}) = x^2 - dy^2 \end{aligned}$$

We generalise Theorem 7.5 to L/K separable.

Start of lecture 15

We generalise to L/K separable. Let $\overline{K}$ be an algebraic closure of K. Then implies that $\# \mathrm{Hom}_K(L, \overline{K}) = [L : K]$.

Theorem 7.6. Let L/K be a finite separable extension of degree d. Let $\sigma_1, \ldots, \sigma_d$ be the K-embeddings $L \hookrightarrow \overline{K}$. Let $\alpha \in L$. Then

$$\mathrm{Tr}_{L/K}(\alpha) = \sum_{i=1}^{d} \sigma_i(\alpha), \qquad N_{L/K}(\alpha) = \prod_{i=1}^{d} \sigma_i(\alpha).$$

Proof. Let f be the minimal polynomial of α over K. Let $\alpha_1, \ldots, \alpha_n$ be the roots of f in $\overline{K}$. By ,

$$\begin{aligned} \mathrm{Hom}_K(K(\alpha), \overline{K}) &\leftrightarrow \{\alpha_1, \ldots, \alpha_n\} \\ \sigma &\mapsto \sigma(\alpha) \end{aligned}$$

Since $L/K(\alpha)$ is separable, each K-embedding $K(\alpha) \hookrightarrow \overline{K}$ extends to an embedding $L \hookrightarrow \overline{K}$ in exactly $m = [L : K(\alpha)]$ ways. Therefore

$$\operatorname{Tr}_{L/K}(\alpha) = m \sum_{j=1}^{n} \alpha_j = \sum_{i=1}^{d} \sigma_i(\alpha)$$
$$N_{L/K}(\alpha) = \left(\prod_{j=1}^{n} \alpha_j \right)^m = \prod_{i=1}^{d} \sigma_i(\alpha)$$

(the first equality in each line holds by , and the second equality in each line holds since $\#\{1 \le i \le d \mid \sigma_i(\alpha) = \alpha_j\} = m$). $\square$

8 Finite Fields

Fix p a prime number. Recall $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. We describe all finite fields of characteristic p (these are necessarily finite extensions of $\mathbb{F}_p$) and their Galois theory. We will use Proposition 1.2, Proposition 1.3 and Proposition 1.4, so it is worth revisiting these.

Note. ϕ in Proposition 1.4 is an automorphism of K (injective since a homomorphism of fields, hence surjective since $|K| < \infty$).

Theorem 8.1. Let $q = p^n$ for some $n \geq 1$. Then:

(i) There exists a field with q elements.

(ii) Any field with q elemenst is a splitting field of $X^q - X$ over $\mathbb{F}_p$.

In particular, any two finite fields with the same order are isomorphic (by Uniqueness of splitting fields).

Proof.

(i) Let L be a splitting field of $f(x) = X^q - X$ over $\mathbb{F}_p$. Let $K \subset L$ be the fixed field of $\phi^n : L \to L$ (note $\phi^n(x) = x^q$). Then

$$K = \{\alpha \in L \mid \phi^n(\alpha) = \alpha\} = \{\alpha \in L \mid f(\alpha) = 0\}$$

Therefore $\#K \leq \deg f = q$. But $f'(X) = -1$ so $\gcd(f, f') = 1$ so f is separable (by Lemma 5.2). Therefore $\#K = q$.

(ii) Suppose K is a field with $\#K = q$. Then Lagrange's theorem (group theory) implies that $\alpha^{q-1} = 1 \ \forall \alpha \in K^*$, hence $\alpha^q = \alpha \ \forall \alpha \in K$. So

$$f(X) = X^q - X = \prod_{\alpha \in K} (X - \alpha)$$

splits into linear factors over K, but clearly not over any proper subfield (since f separable as mentioned in (i)). So K is a splitting field for f over $\mathbb{F}_p$.

□

Notation. We write $\mathbb{F}_q$ for any field with q elements. By Theorem 8.1, any two such are isomorphic, although there is no canonical choice of isomorphism.

Theorem 8.2. $\mathbb{F}_{p^n}/\mathbb{F}_p$ is Galois with $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ cyclic of order n, generated by the Frobenius $\phi : x \mapsto x^p$.

Proof. Let $L = \mathbb{F}_{p^n}$. Let $G \subset \mathrm{Aut}(L/\mathbb{F}_p)$ be the subgroup generated by Frobenius. Then

$$\begin{aligned} \#L^G &= \#L^\phi \\ &= \#\{\alpha \in L \mid \alpha^p - \alpha = 0\} \\ &\le p & \text{(Lemma 1.1)} \end{aligned}$$

But $\mathbb{F}_p \subset L^G$, so $L^G = \mathbb{F}_p$. So

$$\mathbb{F}_p \subset L^{\mathrm{Aut}(L/\mathbb{F}_p)} \subset L^G = \mathbb{F}_p$$

so we get $\mathbb{F}_p = L^{\mathrm{Aut}(L/\mathbb{F}_p)}$, i.e. $L/\mathbb{F}_p$ is Galois. Also, we get $L^{\mathrm{Aut}(L/\mathbb{F}_p)} = L^G$, which implies $\mathrm{Aut}(L/\mathbb{F}_p) = G$. Therefore

$$\mathrm{Gal}(L/\mathbb{F}_p) = G = \langle \phi \rangle$$

and it has order $[L : \mathbb{F}_p] = n$. □

Corollary 8.3. Let L/K be any extension of finite fields with $\#K = q$. Then L/K is Galois with $\mathrm{Gal}(L/K)$ cyclic, generated by the q-power Frobenius $x \mapsto x^q$.

Proof. Let $L = \mathbb{F}_{p^n}$. We have $\mathbb{F}_p \subset K \subset L$. By Theorem 8.2, $L/\mathbb{F}_p$ is Galois with

$$G = \mathrm{Gal}(L/\mathbb{F}_p) = \langle \phi \rangle \cong C_n$$

where $\phi : x \mapsto x^p$. Fundamental Theorem of Galois Theory gives that L/K is Galois and $H = \mathrm{Gal}(L/K) \subset G$. Since $G = \langle \phi \rangle \cong C_n$ we have $H = \langle \phi^m \rangle$ for some $m \mid n$. Then

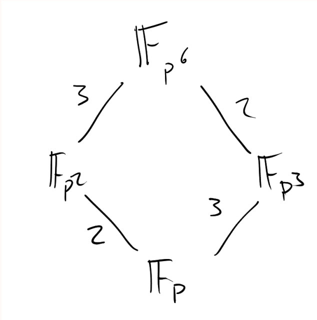
$$[K : \mathbb{F}_p] = \frac{[L : \mathbb{F}_p]}{[L : K]} = \frac{\#G}{\#H} = (G : H) = m \tag{$*$}$$

Therefore $q = \#K = p^m$ and $\phi^m : x \mapsto x^q$. □

Corollary 8.4. $\mathbb{F}_{p^n}$ has a unique subfield of order p^m for each $m \mid n$ and no others.

Proof. We apply the Fundamental Theorem of Galois Theory. The subgroups of $G = \mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \langle \phi \rangle \cong C_n$ are the subgroups $H = \langle \phi^m \rangle$ for $m \mid n$ (and no others). If $K = \mathbb{F}_{p^n}^H$ then $H = \mathrm{Gal}(\mathbb{F}_{p^n}/K)$ and $[K : \mathbb{F}_p] = (G : H) = m$ (see $(*)$). Therefore $\#K = p^m$. □

Example.



All extensions are Galois with cyclic Galois group of orders indicated.

Start of

lecture 16

9 The Galois Group of a Polynomial

Definition (Galois group of a polynomial)**.** Let $f \in K[X]$ be a separable of degree n. Let L be a splitting field for f over K. The action of $G = \mathrm{Gal}(L/K)$ on the roots $\alpha_1, \dots, \alpha_n$ of f determines an injective group homomorphism $\iota : G \to S_n$. It's image is the *Galois group of f over K*, written $\mathrm{Gal}(f)$ or $\mathrm{Gal}(f/K)$.

Lemma 9.1. Let $f \in K[X]$ be a separable. Then

$$f \text{ irreducible} \iff \mathrm{Gal}(f/K) \text{ is transitive}$$

(Recall $H \subset S_n$ is transitive if $\forall i, j \in \{1, \dots, n\}$, there exists $\sigma \in H$ such that $\sigma(i) = j$).

Proof.

$\Rightarrow$ If $f = gh$, $g, h \in K[X]$, $\deg g > 0$, $\deg h > 0$ then $\mathrm{Gal}(f/K)$ sends roots of g to roots of g (and not to roots of h), and so cannot act transitively on the roots of f.

$\Leftarrow$ Without loss of generality, f is monic. Let $\alpha \in L$ be a root of f. Then f is the minimal polynomial of α over K. Then by Remark 6.3,

$$\{\sigma(\alpha) : \sigma \in \mathrm{Gal}(L/K)\} = \{\text{roots of } f \text{ in } L\}$$

Therefore $\mathrm{Gal}(L/K)$ acts transitively on $\alpha_1, \dots, \alpha_n$. Therefore $\mathrm{Gal}(f/K) \subset S_n$ is a transitive subgroup.

□

Remark (Alternative proof of $\Rightarrow$)**.** By Theorem 3.2, there exists [-isomorphismK] $K(\alpha_i) \cong K(\alpha_j)$, $\alpha_i \mapsto \alpha_j$. This extends to an automorphis mof L by Uniqueness of splitting fields.

Let $f \in K[X]$ be a monic separable polynomial with roots $\alpha_1, \dots, \alpha_n$ in a splitting field L. Recall from Section 4,

$$\mathrm{Disc}(f) = \prod_{i<j} (\alpha_i - \alpha_j)^2$$

Lemma 9.2. Assume char $K \neq 2$. Let $\Delta = \mathrm{Disc}(f)$. The fixed field of $\mathrm{Gal}(f/K) \cap A_n$ is $K(\sqrt{\Delta})$. In particular

$$\mathrm{Gal}(f/K) \subset A_n \iff \Delta \text{ is a square in } K$$

Proof. The sign of a permutation $\pi \in S_n$ is defined so that (as an identiy in $\mathbb{Z}[X_1, \dots, X_n]$) we have

$$\prod_{i<j} (X_{\pi(i)} - X_{\pi(j)}) = \mathrm{sign}(\pi) \prod_{i<j} (X_i - X_j)$$

We put $\delta = \prod_{i<j} (\alpha_i - \alpha_j)$ so that $\delta^2 = \Delta$. So if $\sigma \in G = \mathrm{Gal}(f/K) = \mathrm{Gal}(L/K)$ then

$$\sigma(\delta) = \mathrm{sign}(\sigma)\delta.$$

As f is separable and char $K \neq 2$, $\delta \neq -\delta$. Therefore

$$\begin{aligned} G \cap A_n &= \{\sigma \in G \mid \sigma(\sigma) = 1\} \\ &= \{\sigma \in G \mid \sigma(\delta) = \delta\} \\ &= \mathrm{Gal}(L/K(\delta)) \end{aligned}$$

Therefore $L^{G \cap A_n} = K(\delta)$. In particular,

$$\begin{aligned} G \subset A_N &\iff G \cap A_n = G \\ &\iff K(\sqrt{\Delta}) = K \\ &\iff \Delta \text{ is a square in } K \end{aligned}$$

□

Remark. $G = \mathrm{Gal}(g/K) \subset S_n$ is really only defined up to conjugacy, since if we reorder $\alpha_1, \dots, \alpha_n$ using $\sigma \in S_n$ then G changes to $\sigma G \sigma^{-1}$. But we *can* distinguish between

$$\langle (12), (34) \rangle \subset S_4 \qquad \text{and} \qquad \langle (12)(34), (13)(24) \rangle \subset S_4$$

even though both are isomorphic to $C_2 \times C_2$.

What is $G \hookrightarrow S_n$ up to conjugacy?

- $n = 2$: The only transitive subgroup of S_2 is itself.
- $n = 3$: The transitive subgroups of S_3 are S_3 and $A_3 \cong C_3$. So if $f \in K[X]$ is irreducible then $\mathrm{Gal}(f/K)$ is A_3 or S_3. By Lemma 9.2, $\mathrm{Gal}(f/K) = A_3$ if and only if $\mathrm{Disc}(f)$ is a square in K. Taking $n = 3$ in Example Sheet 2, Question 3 gives

  $$\mathrm{Disc}(X^3 + aX + b) = -4a^3 - 27b^2$$

  (LEARN THIS FORMULA).

Example. $f(X) = X^3 - 3X + 1$ (see Section 2 and Example Sheet 1).

$$\mathrm{Disc}(f) = -4(-3)^3 - 27 = 81 = 9^2$$

Therefore $\mathrm{Gal}(f/\mathbb{Q})$ is 1 or A_3. We checked in Section 2 that f is irreducible over $\mathbb{Q}$, so therefore $\mathrm{Gal}(f/\mathbb{Q}) = A_3$.

- $n = 4$: The transitive subgroups of S_4 are

$$S_4, A_4, D_8, C_4, V \cong C_2 \times C_2$$

S_4, A_4, V are normal subgroups where

$$V = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$$

There are 3 conjugate copies of each of C_4 and D_8.

Let S_4 act on $V \setminus \{\mathrm{id}\}$ by conjugation since $g(12)(34)g^{-1} = (g(1)g(2))(g(3)g(4))$ it would be equivalent to let S_4 act on the set of ways of partitioning the set $\{1, 2, 3, 4\}$ into 2 subsets of size 2. The corresponding permutation representation is a group homomorphism $\pi : S_4 \to S_3$. If $H = \{\sigma \in S_4 \mid \sigma(1) = 1\} = \langle (234), (23) \rangle \subset S_4$ then $\pi|_H : H \to S_3$ is an isomorphism. So π is surjective and $\# \ker \pi = 4$. V abelian $\implies V \subset \ker \pi$. Hence $V = \ker \pi$.

If $G \subset S_4$ then applying the isomorphism theorem to $\pi|_G$ gives $G/G \cap V \cong \pi(G) \subset S_4$.

transitive subgroup $G \subset S_4$	$\pi(G) \subset S_3$
S_4	S_3
A_4	A_3
C_4 or D_8	C_2
V	1

Start of lecture 17

Let $f(X) = \prod_{i=1}^{4}(X - \alpha_i)$ be a monic quartic polynomial. Define

$$\beta_1 = (\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4)$$
$$\beta_2 = (\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4)$$
$$\beta_3 = (\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3)$$

Definition. The *resolvent cubic* is

$$g(X) = \prod_{i=1}^{3}(X - \beta_i).$$

Theorem 9.3. Let f, g as above.

(i) If $f \in K[X]$ then $g \in K[X]$.

(ii) If f is separable then g is separable.

(iii) If (i) and (ii) hold then

$$\pi(\mathrm{Gal}(f/K)) = \mathrm{Gal}(g/K)$$

In particular if $f \in K[X]$ is irreducible then $\mathrm{Gal}(g/K)$ determines $\mathrm{Gal}(f/K)$ up to ambiguity between C_4 and D_8 when $\#\,\mathrm{Gal}(g/K) = 2$.

Proof.

(i) More generally each coefficient of g is a symmetric polynomial in $\mathbb{Z}[\beta_1, \beta_2, \beta_3]$, hence a symmetric polynomial in $\mathbb{Z}[\alpha_1, \alpha_2, \alpha_3, \alpha_4]$ and so by the Symmetric Function Theorem, is a $\mathbb{Z}$-coefficient polynomial in the coefficients of f.

(ii)

$$\begin{aligned}
\beta_1 - \beta_2 &= \alpha_1\alpha_3 + \cancel{\alpha_1\alpha_4} + \cancel{\alpha_2\alpha_3} + \alpha_2\alpha_4 - \alpha_1\alpha_2 - \cancel{\alpha_1\alpha_4} - \cancel{\alpha_2\alpha_3} - \alpha_3\alpha_4 \\
&= \alpha_1\alpha_3 + \alpha_2\alpha_4 - \alpha_1\alpha_2 - \alpha_3\alpha_4 \\
&= (\alpha_1 - \alpha_4)(\alpha_3 - \alpha_2)
\end{aligned}$$

If f separable then $\alpha_1, \ldots, \alpha_4$ are distinct, hence $\beta_1 \neq \beta_2$. Similar calculation shows $\beta_1, \beta_2, \beta_3$ are all distinct. Hence g is separable.

(iii) Let M be a splitting field of f over K. Let $\alpha_1, \ldots, \alpha_4 \in M$ be the roots of f. Then $L := K(\beta_1, \beta_2, \beta_3) \subset M$ is a splitting field for g over K. If an element of $\mathrm{Gal}(M/K)$ permutes $\alpha_1, \ldots, \alpha_4$ according to $\sigma \in S_4$, then it restricts to an element of $\mathrm{Gal}(L/K)$ permuting $\beta_1, \beta_2, \beta_3$ according to $\pi(\sigma) \in S_3$. In other words, there is a commutative diagram

$$\begin{tikzcd}
\mathrm{Gal}(M/K) \arrow[r, "\mathrm{res}"] \arrow[d, "\iota_4"] & \mathrm{Gal}(L/K) \arrow[d, "\iota_3"] \\
S_4 \arrow[r, "\pi"] & S_3
\end{tikzcd}$$

By Theorem 6.4(c), the map $\mathrm{res} : \mathrm{Gal}(M/K) \to \mathrm{Gal}(L/K)$ is surjective. Therefore $\pi(\mathrm{Im}\,\iota_4) = \mathrm{Im}\,\iota_3$. Therefore $\pi(\mathrm{Gal}(f/K)) = \mathrm{Gal}(g/K)$. $\square$

Proposition 9.4. Let f be a monic quartic polynomial with resolvent cubic g. Then

(i) $\mathrm{Disc}(f) = \mathrm{Disc}(g)$.

(ii) If

$$f(X) = X^4 + pX^2 + qX + r$$

then

$$g(X) = X^3 - 2pX^2 + (p^2 - 4r)X + q^2$$

Proof.

(i) Exercise (see proof of Theorem 9.3(ii)).

(ii) We must show

$$\begin{aligned} \beta_1 + \beta_2 + \beta_3 &= 2p \qquad (1) \\ \beta_1\beta_2 + \beta_2\beta_3 &= p^2 - 4r \\ \beta_1\beta_2\beta_3 &= -q^2 \end{aligned}$$

We have $\beta_1 + \beta_2 + \beta_3 = 2\sum_{i<j} \alpha_i\alpha_j = 2p$, which proves (1). Since $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$, we have

$$\begin{cases} \beta_1 = -(\alpha_1 + \alpha_2)^2 \\ \beta_2 = -(\alpha_1 + \alpha_3)^2 \\ \beta_3 = -(\alpha_1 + \alpha_4)^2 \end{cases} \qquad (*)$$

$$(\alpha_1 + \alpha_2)(\alpha_1 + \alpha_3)(\alpha_1 + \alpha_4) = \alpha_1^2\cancel{(\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4)} + \overbrace{\sum_{i<j<k} \alpha_i\alpha_j\alpha_k}^{=-q}$$

Therefore $\beta_1\beta_2\beta_3 = -q^2$, which proves (3). (2) is left as an exercise.

$\square$

Example. $f(X) = X^4 - 4X^2 + 2$. Irreducible in $\mathbb{Q}[X]$ by Eisenstein ($p = 2$) and Gauss' Lemma. $g(X) = X(X^2 + 8X + 8)$.

$$\mathrm{Disc}(f) = \mathrm{Disc}(g) = 8^2\,\mathrm{Disc}(X^2 + 8X + 8) = 2^{11}$$

$$\mathrm{Gal}(g/\mathbb{Q}) = C_2 \implies \mathrm{Gal}(f/\mathbb{Q}) = C_4 \text{ or } D_8.$$

But $f(X) = (X^2 - 2 + \sqrt{2})(X^2 - 2 - \sqrt{2})$. Therefore $\mathrm{Gal}(f/\mathbb{Q}) \cap A_4 = \mathrm{Gal}(f/\mathbb{Q}(\sqrt{2}))$ is not a transitive subgroup of S_4. Therefore $\mathrm{Gal}(f/\mathbb{Q}) \cong C_4$ (compare with Example 6.6).

Now we find a formula for the roots of a quartic polynomial.

(i) Replace $f(X)$ by $f(X+c)$ such that f has no X^3 term ($\implies \alpha_1+\alpha_2+\alpha_3+\alpha_4 = 0$).

(ii) Find the roots of $\beta_1, \beta_2, \beta_3$ of the resolvent cubic using the method of Section 4.

By $(*)$ we have

$$\alpha_1 = \frac{1}{2}(\sqrt{-\beta_1} + \sqrt{-\beta_2} + \sqrt{-\beta_3})$$

where we choose square roots such that $\sqrt{-\beta_1}\sqrt{-\beta_2}\sqrt{-\beta_3} = -q$.

Recall $\sigma \in S_n$ has cycle type $(n_1, \ldots, n_r)$ if when written as a product of disjoint cycles, these cycles have lengths $n_1, n_2, \ldots, n_r$.

Lemma 9.5. Let $f \in \mathbb{F}_p[X]$ be a separable polynomial with irreducible factors of degrees $n_1, \ldots, n_r$ ($n = \deg f = \sum n_i$). Then $\mathrm{Gal}(f/\mathbb{F}_p) \subset S_n$ is generated by a single element of cycle type $(n_1, \ldots, n_r)$. In particualr, $\mathrm{Gal}(f/\mathbb{F}_p)$ is cyclic of order $\mathrm{lcm}(n_1, \ldots, n_r)$.

Proof. Let L be a splitting field of f over $\mathbb{F}_p$. Let $\alpha_1, \ldots, \alpha_n$ be the roots of f in L. Then Theorem 8.2 implies that $G = \mathrm{Gal}(L/\mathbb{F}_p)$ is cyclic generated by Frobenius $\phi : x \mapsto x^p$. Write $f = \prod_i f_i$, where $f_i \in \mathbb{F}_p[X]$ is irreducible of degree n_i. Since G permutes the roots of each f_i transitively, the action of ϕ on the roots of f_i is given by a single n_i cycle. $\square$

Start of

lecture 18

Theorem 9.6 ("Reduction modulo p"). Let $f \in \mathbb{Z}[X]$ be a monic separable polynomial of degree $n \geq 1$. Let p be a prime and suppose the reduction of f modulo p, say $\overline{f} \in \mathbb{F}_p[X]$ is also separable. Then $\mathrm{Gal}(\overline{f}/\mathbb{F}_p) \subset \mathrm{Gal}(f/\mathbb{Q})$ as subgroups of S_N (up to conjugacy).

Proof (non-examinable). See below. □

Corollary 9.7. With the same assumptions, suppose $\overline{f} = g_1 g_2 \cdots g_r$ where $g_i \in \mathbb{F}_p[X]$ is irreducible of degree n_i. Then $\mathrm{Gal}(f/\mathbb{Q}) \subset S_n$ contains an element with cycle type $(n_1, n_2, \ldots, n_r)$.

Proof. Combine Lemma 9.5 and Theorem 9.6. □

Example. $f(X) = X^4 - 3X + 1$. Modulo 2, $\overline{f} = X^4 + X + 1 \in \mathbb{F}_2[X]$ is irreducible. Modulo 5, $\overline{f} = (X+1)(X^3 - X^2 + X + 1)$ (noting that the second factor is irreducible in $\mathbb{F}_5[X]$). Therefore $\mathrm{Gal}(f/\mathbb{Q})$ contains a 3-cycle and a 4-cycle. Hence $\mathrm{Gal}(f/\mathbb{Q}) = S_4$.

Let $f \in K[X]$ be a monic separable polynomial of degree n with splitting field L and roots $\alpha_1, \ldots, \alpha_n \in L$. Let

$$\begin{aligned} F(\tau_1, \ldots, \tau_n, X) &= \prod_{\sigma \in S_n} (X - (\alpha_1 T_{\sigma(1)} + \cdots + \alpha_n T_{\sigma(n)})) \\ &\in K[T_1, \ldots, T_n, X] \end{aligned}$$

Indeed, the coefficients of this polynomial are in L, and are fixed by $\mathrm{Gal}(L/K)$ hence are in K.

We define an action $*$ of S_n on $K[T_1, \ldots, T_n, X]$ by permuting the T_i, i.e.

$$(\sigma * h)(T_1, \ldots, T_n, X) = h(T_{\sigma(1)}, \ldots, T_{\sigma(n)}, X)$$

We note that $\sigma * F = F$ for all $\sigma \in S_n$.

Lemma 9.8. Let $F_1 \in K[T_1, \ldots, T_n, X]$ be an irreducible factor of F. Then $\mathrm{Gal}(f/K) \subset S_n$ is conjugate to $\mathrm{Stab}(F_1) = \{\tau \in S_n \mid \tau * F_1 = F_1\}$.

Proof. Without loss of generality F_1 is monic in X. Replacing F_1 by $\tau * F_1$ for suitable $\tau \in S_n$ we may suppose it has a factor

$$X - (\alpha_1 T_1 + \cdots + \alpha_n T_n).$$

Then for each $\sigma \in G = \mathrm{Gal}(f/K)$, it had a factor

$$X - (\alpha_{\sigma(1)} T_1 + \cdots \alpha_{\sigma(n)} T_n)$$

Now

$$\prod_{\sigma \in G} (X - (\alpha_{\sigma(1)} T_1 + \cdots + \alpha_{\sigma(n)} T_n))$$

has coefficients in K, and divides F_1, hence is equal to F_1 (sine F_1 irreducible and monic in X). For $\tau \in S_n$ we have

$$\begin{aligned}
\tau * F_1 &= \prod_{\sigma \in G} (X - (\alpha_{\sigma(1)} T_{\tau(1)} + \cdots + \alpha_{\sigma(n)} T_{\tau(n)})) \\
&= \prod_{\sigma \in G} (X - (\alpha_{\sigma\tau^{-1}(1)} T_1 + \cdots + \alpha_{\sigma\tau^{-1}(n)} T_n)) \\
&= \prod_{\sigma \in G\tau^{-1}} (X - (\alpha_{\sigma(1)} T_1 + \cdots + \alpha_{\sigma(n)} T_n))
\end{aligned}$$

So $\tau * F_1 = F_1$ if and only if $G = G\tau^{-1}$, which happens if and only if $\tau \in G$. $\square$

Proof of "Reduction modulo p" (non-examinable). By the Symmetric Function Theorem the coefficients of F are $\mathbb{Z}$-coefficient polynomials in the coefficients of f. So if $f \in \mathbb{Z}[X]$ then $F \in \mathbb{Z}[T_1, \ldots, T_n, X]$. Let $\overline{f} \in \mathbb{F}_p[X]$ and $\overline{F} \in \mathbb{F}_p[T_1, \ldots, T_n, X]$ be the polynomials obtained by reducing all coefficients modulo p. We may equally construct $\overline{F}$ from $\overline{f}$ in the same way we constructed F from f. Write $F = F_1 F_2 \cdots F_s$, $F_i \in \mathbb{Z}[T_1, \ldots, T_n, X]$ distrinct irreducibles (also irreducible in $\mathbb{Q}[T_1, \ldots, T_n, X]$). Let $\overline{F} = \phi_1 \phi_2 \cdots \phi_t$, $\phi_i \in \mathbb{F}_p[T_1, \ldots, T_n, X]$ distinct irreducibles. Without loss of generality $\phi_1 \mid \overline{F_1}$ (hence $\phi_1 \nmid \overline{F}_j$ for all $j > 1$). Then

$$\{\tau \in S_n \mid \tau * \phi_1 = \phi_1\} \subset \{\tau \in S_n \mid \tau * F_1 = F_1\}.$$

Lemma 9.8 shows that up to conjugacy,

$$\mathrm{Gal}(\overline{f}/\mathbb{F}_p) \subset \mathrm{Gal}(f/\mathbb{Q}). \qquad \square$$

10 Cyclotomic and Kummer extensions

Let K be a field, and $n \geq 1$ an integer. We suppose $\operatorname{char} K \nmid n$ (i.e. either $\operatorname{char} K = 0$, or $\operatorname{char} K = p > 0$ and $p \nmid n$). Let L/K be a splitting field of $f(X) = X^n - 1$. Since $f'(X) = nX^{n-1}$ and $n \cdot 1_K \neq 0$ we have $\gcd(f, f') = 1$ and so f is separable. By Theorem 6.2, L/K is Galois. Let $\mu_n = \{x \in L \mid x^n = 1\}$ be the group of n-th roots of unity. This is a subgroup of L^* of order n (since f splits into distinct linear factors over L) and is cyclic by Proposition 1.3.

Definition. $\zeta_n \in \mu_n$ is a *primitive n-th root of unity* if it has order exactly n in L^*.

Example. If $K \subset \mathbb{C}$ then we can take $\zeta_n = e^{2\pi i/n}$.

Then
$$\mu_n = \langle \zeta_n \rangle = \{1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}\}$$
and
$$L = K(1, \zeta_n, \zeta_n^2, \ldots, \zeta_n^{n-1}) = K(\zeta_n).$$

Definition. $K(\zeta_n)/K$ is called a *cyclotomic extension.*

Next time: we show
$$\operatorname{Gal}(K(\zeta_n)/K) \subset (\mathbb{Z}/n\mathbb{Z})^*.$$
(with equality when $K = \mathbb{Q}$).

Start of lecture 19

Recall that $(\mathbb{Z}/n\mathbb{Z})^* = \{a \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a, n) = 1\}$ is a group under multiplication. It has order $\phi(n)$ (Euler ϕ-function). Let K be a field with $\operatorname{char} K \nmid n$. Let ζ_n be a primitive n-th root of unity (in some field extension of K).

Theorem 10.1. There is an injective group homomorphism
$$\operatorname{Gal}(K(\zeta_n)/K) \overset{\chi}{\hookrightarrow} (\mathbb{Z}/n\mathbb{Z})^*.$$
In particular $\operatorname{Gal}(K(\zeta_n)/K)$ is abelian, and $[K(\zeta_n) : K]$ divides $\phi(n)$.

Proof. Let $G = \operatorname{Gal}(K(\zeta_n)/K)$. If $\sigma \in G$ then ζ_n and hence also $\sigma(\zeta_n)$ are roots of $X^n - 1$. Therefore $\sigma(\zeta_n) = \zeta_n^a$ for some $a \in \mathbb{Z}$. Since ζ_n is a primitive n-th root of unity the value of a is unique modulo n. We define

$$\begin{aligned} \chi : G &\to \mathbb{Z}/n\mathbb{Z} \\ \sigma &\mapsto a \end{aligned}$$

Noe let $\sigma, \tau \in G$ with $\sigma(\zeta_n) = \zeta_n^a$, $\tau(\zeta_n) = \zeta_n^b$. Then

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

so

$$\chi(\sigma\tau) = ab = \chi(\sigma)\chi(\tau).$$

In particular $\chi(\sigma)\chi(\sigma^{-1}) = \chi(1) = 1$ so $\chi(\sigma) \in (\mathbb{Z}/n\mathbb{Z})^*$ and χ is a group homomorphism. Since any $\sigma \in G$ is uniquely determined by $\sigma(\zeta_n)$ it is clear that χ is injective. □

Remark. If $\chi(\sigma) = a$ then $\sigma(\zeta) = \zeta^a$ for all $\zeta \in \mu_n$. So the definition of χ does not depend on the choice of ζ_n.

Example. Let p be a prime with $p \equiv 4 \pmod 5$. Let $K = \mathbb{F}_p$, $L = \mathbb{F}_{p^2}$ and $n = 5$. Since $5 \mid (p^2 - 1)$, there exists $\zeta_5 \in L$ a primitive 5-th root of unity. Since $5 \nmid (p-1)$ we know $\zeta_5 \notin K$. Therefore $L = K(\zeta_5)$. By Theorem 10.1

$$\underbrace{\mathrm{Gal}(L/K)}_{\cong C_2} \overset{\chi}{\hookrightarrow} (\mathbb{Z}/5\mathbb{Z})^*.$$

Therefore $\mathrm{Im}(\chi) = \{\pm 1\} \subset (\mathbb{Z}/5\mathbb{Z})^*$.

Corollary 10.2. Let $K = \mathbb{F}_p$ and suppose $p \nmid n$. Then $[K(\zeta_n) : K]$ is the order of p in $(\mathbb{Z}/n\mathbb{Z})^*$.

Proof. $\mathrm{Gal}(K(\zeta_n)/K)$ is generated by Frobenius homomorphism ϕ which sends $\zeta_n \mapsto \zeta_n^p$. Therefore

$$\begin{aligned} [K(\zeta_n) : K] &= \text{order of } \phi \text{ in } \mathrm{Gal}(K(\zeta_n)/K) \\ &= \text{order of } \underbrace{\chi(\phi)}_{=p} \text{ in } (\mathbb{Z}/n\mathbb{Z})^* \end{aligned}$$

□

Definition (Cyclotomic polynomial)**.** Let $\zeta_n = e^{2\pi i/n}$. The n-th *cyclotomic polynomial* is

$$\Phi_n(X) = \prod_{a \in (\mathbb{Z}/n\mathbb{Z})^*} (X - \zeta_n^a).$$

Its roots are the primitive n-roots of unity. As $\mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ permutes these, we have $\Phi_n \in \mathbb{Q}[X]$. Clearly we have $\zeta^n = 1$ if and only if ζ is a primitive n-th root of unity for some $d \mid n$. Therefore

$$X^n - 1 = \prod_{d \mid n} \Phi_d(X).$$

It follows by induction on n that $\Phi_n \in \mathbb{Z}[X]$.

Example.

$$\begin{aligned}
\Phi_1 &= X - 1 \\
\Phi_p &= \frac{X^p - 1}{X - 1} = X^{p-1} + X^{p-2} + \cdots + X^2 + X + 1 \qquad\qquad (p \text{ prime}) \\
\Phi_4 &= X^2 + 1
\end{aligned}$$

In general, $\deg \Phi_n = \phi(n)$.

Theorem 10.3. If $K = \mathbb{Q}$ then the group homomorphism χ of is an isomorphism. In particular, $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$, and $\Phi_n \in \mathbb{Q}[X]$ is irreducible.

Proof. Let p be a prime with $p \nmid n$. We show that $\mathrm{Im}\,\chi$ contains $p \mod n$. If this is true then $\mathrm{Im}\,\chi$ contains $a \mod n$ for every a coprime to n (by considering the prime factorisation fo a). Therefore χ is surjective as required. Let $f, g \in \mathbb{Q}[X]$ be the minimal polynomials of ζ_n and ζ_n^p over $\mathbb{Q}$. If $f = g$ then by Lemma 9.1 there exists $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_n)/\mathbb{Q})$ with $\sigma(\zeta_n) = \zeta_n^p$ as required. If not then f, g are distinct irreducibles dividing $X^n - 1$. So $f, g \in \mathbb{Z}[X]$ (using Gauss' lemma) and $fg \mid (X^n - 1)$. Now ζ_n is a root of $g(X^p)$, so $f(X) \mid g(X^p)$. Reducing modulo p gives

$$\overline{f}(X) \mid \overline{g}(X^p) = \overline{g}(X)^p.$$

Both $\overline{f}$ and $\overline{g}$ divide the separable polynomial $X^n - 1 \in \mathbb{F}_p[X]$, so $\overline{f}(X) \mid \overline{g}(X)$. Hence

$$\overline{f}(X)^2 \mid \overline{f}(X)\overline{g}(X) \mid (X^n - 1)$$

which contradicts the fact that $X^n - 1 \in \mathbb{F}_p[X]$ is separable. $\square$

Theorem 10.4 (Gauss)**.** Let $n \geq 3$. A regular n-gon is constructible by ruler and compass if and only if $\phi(n)$ is a power of 2.

Proof. Let $\zeta_n = e^{2\pi i/n}$ and $\alpha = \zeta_n + \zeta_n^{-1} = 2\cos\left(\frac{2\pi}{n}\right)$. Since $\alpha \in \mathbb{R}$, $\zeta \notin \mathbb{R}$ and ζ_n is a root of $X^2 - \alpha X + 1 \in \mathbb{Q}(\alpha)[X]$. We have $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\alpha)] = 2$. If a regular n-gon can be constructed then α is constructible. Now Corollary 2.2 implies that $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is a power of 2. By Theorem 10.3, $\phi(n) = [\mathbb{Q}(\zeta_n) : \mathbb{Q}] = 2[\mathbb{Q}(\alpha) : \mathbb{Q}]$ is a power of 2. For the converse we use the converse of Theorem 2.1 (proof omitted). It remains to show that if $\phi(n)$ is a power of 2 there there exist fields

$$\mathbb{Q} = K_m \subset K_{m-1} \subset \cdots \subset K_1 \subset K_0 = \mathbb{Q}(\zeta_n)$$

where $[K_i : K_{i+1}] = 2$ for all i and $K_1 = \mathbb{Q}(\alpha)$. By the Fundamental Theorem of Galois Theory, it suffices to construct subgroups

$$\{1\} = H_0 \subset H_1 \subset \cdots \subset H_{m-1} \subset H_m = (\mathbb{Z}/n\mathbb{Z})^*$$

where $(H_i : H_{i-1}) = 2$ for all i, and $H_1 = \{\pm 1\}$. We must show that if $G = (\mathbb{Z}/n\mathbb{Z})^*$ is an abelian group with order a power of 2 then there exist subgroups $\{1\} = H_0 \subset H_1 \subset H_2 \subset \cdots \subset H_m = G$ such that $(H_i : H_{i-1}) = 2$ for all i. Assuming $H_0, H_1, \ldots, H_j$ have been constructed, and $H_j \neq G$, we note that G/H_j has order a power of 2 hence contains an element gH_j of order 2. Then set $H_{j+1} = \langle H_j, g \rangle$ and repeat. □

Start of lecture 20

Corollary. A regular n-hon is constructible by ruler and compass if and only if n is a power of 2 and distinct primes of the form $F_k = 2^{2^k} + 1$.

Proof. If $n = \prod_i p_i^{\alpha_i}$ then

$$\phi(n) = \prod_i p_i^{\alpha_i - 1}(p_i - 1)$$

so $\phi(n)$ is a power of 2 if and only if n is a product of a power of 2 and distinct odd primes of the form $2^m + 1$. If $2^m + 1$ is prime then m must be a power of 2. Indeed if $m = ab$ with $b > 1$ odd, then putting $x = 2^a$ in

$$x^b + 1 = (x+1)(x^{b-1} - x^{b-2} + \cdots - x + 1)$$

gives a non-trivial factorisation. □

k	0	1	2	3	4
$F_k = 2^{2^k} + 1$	3	5	17	257	65537

$F_0, \ldots, F_4$ are all prime. This prompted Fermat to guess that all the F_k might be prime. However in 1732 Euler showed that

$$F_5 = 641 \times 6700417.$$

Since then many other Fermat numbers have been proved composite and no more have been shown to be prime.

Theorem 10.5 (Linear independence of field embeddings)**.** Let K, L be fields and $\sigma_1, \ldots, \sigma_n : K \hookrightarrow L$ distinct field embeddings ($n \geq 1$). If $\lambda_1, \ldots, \lambda_n \in L$ satisfy

$$\lambda_1 \sigma_1(x) + \cdots + \lambda_n \sigma_n(x) = 0 \qquad \forall x \in K$$

then $\lambda_1 = \lambda_2 = \cdots = \lambda_n = 0$.

Proof. Induction on n. Trivially true for $n = 1$. Now suppose $n \geq 2$ and

$$\lambda_1 \sigma_1(x) + \cdots + \lambda_n \sigma_n(x) = 0 \qquad \forall x \in K. \tag{1}$$

Pick $y \in K$ such that $\sigma_1(y) \neq \sigma_2(y)$. Replacing x by xy in (1) gives

$$\lambda_1 \sigma_1(x) \sigma_1(y) + \cdots + \lambda_n \sigma_n(x) \sigma_n(y) = 0 \qquad \forall x \in K \tag{2}$$

Taking $\sigma_1(y) \times (1) - (2)$ gives a new relation with only $n - 1$ terms. It must be trivial by the induction hypothesis. Therefore $\sigma_1(y)\lambda_i = \sigma_i(y)\lambda_i$ for all $2 \leq i \leq n$. Since $\sigma_1(y) \neq \sigma_2(y)$ we have $\lambda_2 = 0$. Therefore (1) has only $n - 1$ terms, so the induction hypothesis tells us that all $\lambda_i = 0$. $\square$

10.1 Kummer Theory

We continue to assume $\operatorname{char} K \nmid n$, but now further assume that $\mu_n \subset K$, i.e. K contains a primitive n-th root of unity ζ_n.

Let $\alpha \in K^*$. Let L/K be a splitting field of $f(X) = X^n - a$. Since $f'(X) = nX^{n-1}$ and $n1_K \neq 0$ we have $\gcd(f, f') = 1$, so f is separable by Theorem 6.2 L/K is Galois.

Let $\alpha \in L$ be a root of f. Then

$$f(X) = \prod_{j=0}^{n-1} (X - \zeta_n^j \alpha)$$

Therefore $L = K(\alpha, \zeta_n \alpha, \ldots, \zeta_n^{n-1} \alpha) = K(\alpha)$. We sometimes write $\sqrt[n]{\alpha}$ for α.

Definition (Kummer extension)**.** $K(\sqrt[n]{\alpha})/K$ is called a *Kummer extension*.

Theorem 10.6. Assume $\mu_n \subset K$ and $a \in K^*$. There is an injective group homomorphism

$$\mathrm{Gal}((\sqrt[n]{a})/K) \underset{\theta}{\hookrightarrow} \mu_n$$

In particular $\mathrm{Gal}(K(\sqrt[n]{a})/K)$ is a cyclic group and $[K(\sqrt[n]{(a)}) : K]$ divides n.

Proof. Let $G = \mathrm{Gal}(K(\sqrt[n]{a})/K)$. If $\sigma \in G$ then $\sqrt[n]{a}$ and hence also $\sigma(\sqrt[n]{a})$ are roots of $X^n - a$, so $\sigma(\sqrt[n]{a}) = \zeta_n^r \sqrt[n]{a}$ for some $0 \le r < n$. We define

$$\begin{aligned} \theta : G &\to \mu_n \\ \sigma &\mapsto \zeta_n^r = \frac{\sigma(\sqrt[n]{a})}{\sqrt[n]{a}} \end{aligned}$$

Now let $\sigma, \tau \in G$. Then

$$\begin{aligned} \sigma(\sqrt[n]{a}) &= \zeta_n^r \sqrt[n]{a} \\ \tau(\sqrt[n]{a}) &= \zeta_n^s \sqrt[n]{a} \end{aligned}$$

Then

$$\sigma\tau(\sqrt[n]{\alpha}) = \sigma(\zeta_n^s \sqrt[n]{a}) = \zeta_n^{r+s} \sqrt[n]{a}$$

So $\theta(\sigma\tau) = \zeta^{r+s} = \zeta_n^r \zeta_n^s = \theta(\sigma)\theta(\tau)$. Therefore θ is a group homomorphism. Since any $\sigma \in G$ is uniquely determined by $\sigma(\sqrt[n]{a})$, it is clear that θ is injective. □

Remark. The definition of θ does not depend on the choice of $\sqrt[n]{a}$. Indeed if $\alpha^n = \beta^n = a$, then

$$\begin{aligned} \left(\frac{\alpha}{\beta}\right)^n = 1 &\implies \frac{\alpha}{\beta} \in \mu_n \subset K \\ &\implies \sigma\left(\frac{\alpha}{\beta}\right) = \frac{\alpha}{\beta} \qquad \forall \sigma \in G \\ &\implies \frac{\sigma(\alpha)}{\alpha} = \frac{\sigma(\beta)}{\beta} \qquad \forall \sigma \in G \end{aligned}$$

Notation.

$$(K^*)^n = \{x^n : x \in K^*\} \subset K^*.$$

This is a subgroup since K^* is abelian.

Corollary 10.7. Assume $\mu_n \subset K$ and $a \in K^*$. Then

$$[K(\sqrt[n]{a}) : K] = \text{order of } a \text{ in } \frac{K^*}{(K^*)^n}.$$

In particular $X^n - a$ is irreducible in $K[X]$ if and only if a is not an a-th power in K for any $1 < d \mid n$.

Proof. Let $\alpha = \sqrt[n]{a}$ and $G = \mathrm{Gal}(K(\alpha)/K)$.

$$\begin{aligned} a^m \in (K^*)^n &\iff a^m \in K^* && (\text{using } \mu_n \subset K) \\ &\iff \sigma(\alpha^m) = \alpha^m && \forall \sigma \in G \\ &\iff \theta(\sigma)^m = 1 && \forall \sigma \in G \\ &\iff \operatorname{Im} \theta \subset \mu_m \\ &\iff [K(\alpha) : K] = \#\operatorname{Im}(\theta) \text{ divides } m \end{aligned}$$

Therefore $[K(\alpha) : K]$ is the least m such that $a^m \in (K^*)^n$. Now:

$$\begin{aligned} X^n - a \text{ is irreducible in } K[X] &\iff [K(\alpha) : K] = n \\ &\iff a \text{ has order } n \text{ in } \frac{K^*}{(K^*)^n} \\ &\iff \nexists m \mid n, m < n \text{ such that } a^m \in (K^*)^n \\ &\iff \nexists 1 < d \mid n \text{ with } a \in (K^*)^d \end{aligned}$$

(the last $\iff$ is by putting $n = md$ and use that $\mu_n \subset K$). □

Special case: $n = 2$, $\operatorname{char} K \neq 2$. Then $[K(\sqrt{a}) : K] = 2$ provided $a \notin (K^*)^2$.

Start of lecture 21

Theorem 10.8 (Kummer)**.** Assume $\operatorname{char} K \nmid n$ and $\mu_n \subset K$. Then every degree n Galois extension L/K with cyclic Galois group is of the form $L = K(\sqrt[n]{a})$ for some $a \in K^*$.

Proof. Write $\mathrm{Gal}(L/K) = \{\sigma^i : 0 \leq i < n\}$. By Theorem 10.5, there exists $x \in L$ such that

$$\underbrace{\sum_{j=0}^{n-1} \zeta_n^j \sigma^{j(x)}}_{=\alpha} \neq 0$$

(Lagrange resolvent). Then

$$\sigma(\alpha) = \sum_{j=0}^{n-1} \zeta_n^j \sigma^{j+1}(x) = \sum_{j=0}^{n-1} \zeta_n^{j-1} \sigma^j(x) = \zeta_n^{-1}\alpha$$

The Galois conjugates $\sigma^j(\alpha) = \zeta_n^{-j}\alpha$. So $[K(\alpha) : K] = n$ and $L = K(\alpha)$. Finally $\sigma(\alpha^n) = (\zeta_n^{-1}\alpha)^n = \alpha^n$, so $\alpha^n \in K$. ☐

Now let K be a field with $\operatorname{char} K = 0$. Let $f \in K[X]$ be a polynomial.

Definition (Soluble by radicals)**.** f is *soluble by radicals* over K if there exist fields

$$K = K_0 \subset K_1 \subset K_2 \subset \cdots \subset K_m$$

such that f has a root in K_m and for each $1 \le i \le m$, $K_i = K_{i-1}(\alpha_i)$ with $\alpha_i^{d_i} \in K_{i-1}$ for some $d_i \ge 1$.

Definition (Soluble group)**.** A finite group G is *soluble* if there exist subgroups

$$\{1\} = H_0 \subset H_1 \subset H_2 \subset \cdots \subset H_m = G$$

such that for each $1 \le i \le m$, $H_{i-1} \trianglelefteq H_i$ and H_i/H_{i-1} is abelian.

Remark. The definition is unchanged if we replace “abelian” by “cyclic” or “cyclic of prime order”.

Example. S_4 is soluble:

$$\{1\} \subset V \subset A_4 \subset S_4$$

with $V \cong C_2 \times C_2$, $A_4/V \cong C_3$, $S_4/A_4 \cong C_2$.

Lemma 10.9. If G is soluble then so is every subgroup and quotient of G.

Proof. Exercise (Example Sheet 4, Question 7). ☐

Theorem 10.10. Let $f \in K[X]$ irreducible. Then

$$f \text{ is soluble by radicals } \iff \mathrm{Gal}(f/K) \text{ is soluble}$$

Lemma 10.11. Let L/K be a finite Galois extension. Let

$$\mathrm{Gal}(L/K) = \{\sigma_1, \dots, \sigma_m\}$$

(say $\sigma_1 = \mathrm{id}$). Let $a \in L^*$ and $n \geq 1$. Then

$$M = L(\mu_n, \sqrt[n]{\sigma_1(a)}, \dots, \sqrt[n]{\sigma_m(a)})$$

is a Galois extension of K.

Proof. Let

$$f(X) = \prod_{i=1}^{m} (X^n - \sigma_i(a)) \in K[X]$$

Then m is the composite of L and the splitting field of f over K. Therefore M/K is Galois by Theorem 6.7(ii). □

Proof of Theorem 10.10.

⇒ By definition there exist fields $K = K_0 \subset K_1 \subset \cdots K_m$ such that f has a root in K_m and for each $1 \leq i \leq m$, $K_i = K_{i-1}(\alpha_i)$ with $\alpha_i^{d_i} \in K_{i-1}$ for some $d_i \geq 1$. Repeatedly applying Lemma 10.11, we may assume K_m/K is Galois. By adjoining suitable roots of unity first, we may further assume each K_i/K_{i-1} is either cyclotomic or Kummer. By Theorem 10.1 and Theorem 10.6 each $\mathrm{Gal}(K_i/K_{i-1})$ is abelian. So by the Fundamental Theorem of Galois Theory, $\mathrm{Gal}(K_m/K)$ is soluble. Since f has a root in K_m and K_m/K is normal, we know that f slpits in K_m. Therefore $\mathrm{Gal}(f/K)$ is a quotient of $\mathrm{Gal}(K_m/K)$, and hence $\mathrm{Gal}(f/K)$ is soluble by Lemma 10.9.

⇐ By the here exists $K = K_0 \subset K_1 \subset \cdots \subset K_m$ such that f has a root in K_m and each K_i/K_{i-1} is Galois with cyclic Galois group. Let $n = \mathrm{lcm}_{1 \leq i \leq m}[K_i : K_{i-1}]$. Then

$$K = K_0 \subset K_0(\zeta_n) \subset K_1(\zeta_n) \subset \cdots \subset K_m(\zeta_n)$$

By Theorem 6.7(i), $K_i(\zeta_n)/K_{i-1}(\zeta_n)$ is Galois and

$$\mathrm{Gal}(K_i(\zeta_n)/K_{i-1}(\zeta_n)) \hookrightarrow \mathrm{Gal}(K_i/K_{i-1})$$

Therefore $\mathrm{Gal}(K_i(\zeta_n)/K_{i-1}(\zeta_n))$ is cyclic of order dividing n. □

Corollary 10.12. If $f \in K[X]$ is a polynomial of degree $n \geq 5$ with Galois group A_n or S_n, then f is *not* soluble by radicals over K.

Proof. A_5 is non abelian and simple, hence not soluble. By Lemma 10.9, A_n and S_n are not soluble for all $n \geq 5$ (in fact A_n is simple for all $n \geq 5$). □

Example. $K = \mathbb{Q}$, $f(X) = X^5 - X + a$, with $a \in \mathbb{Z}$, $\gcd(a, 10) = 1$. Then

$$f \equiv X^5 + X + 1 = (X^2 + X + 1)(X^3 + X^2 + 1) \pmod 2.$$

Therefore $\mathrm{Gal}(f/\mathbb{Q})$ contains an element σ with cycle type $(2, 3)$. Then σ^3 is a transposition.

Using the trick in Example Sheet 4, Question 5, we find $\overline{f} \in \mathbb{F}_5[X]$ is irreducible, hence $\mathrm{Gal}(f/\mathbb{Q})$ contains a 5-cycle.

Now Example Sheet 3, Question 7(i): Let p be a prime. If $G \subset S_p$ is a subgroup containing both a p-cycle and a transposition, then $G = S_p$. Therefore $\mathrm{Gal}(f/\mathbb{Q}) = S_5$ and f is not soluble by radicals.

Start of

lecture 22

11 Algebraic Closure

Lemma (Zorn's Lemma)**.** Let S be a nonempty partially ordered set. Assume that every chain in S has an upper bound. Then S has a maximal element.

Definition. A relation $\leq$ on a set S is a partial order if for all $x, y, z \in S$:

(i) $x \leq x$.

(ii) If $x \leq y$ and $y \leq z$ then $x \leq z$.

(iii) If $x \leq y \leq z$ and $y \leq x$ then $x = y$.

$(S, \leq)$ is called a *partially ordered set* (or poset).

It is *totally ordered* if moreover for each $x, y \in S$

(iv) Either $x \leq y$ or $y \leq x$.

Let $T \subset S$ be a subset.

- T is a *chain* if it is totally ordered by $\leq$.
- $x \in S$ is an *upper bound* for T if $t \leq x$ for all $t \in T$.
- $x \in S$ is *maximal* if $\nexists y \in S$ with $x \leq y$ and $x \neq y$.

Example. Let V be a vector space and $(S, \leq)$ be the set of linearly independent subsets of V ordered by inclusion. If $T \subset S$ is a chain then let $Y = \bigcup_{X \in T} X$. It may be checked that Y is linearly independent, hence an upper bound for T. Zorn's Lemma shows that S has a maximal B. Then:

(i) B is linearly independent.

(ii) $B \cup \{v\}$ is not linearly independent for any $v \in V \setminus B$.

(i) and (ii) $\implies$ B spans V. Therefore B is a basis for V.

Example (Maximal ideal)**.** Let R be a nonzero ring. Let $(S, \leq)$ be the set of all proper (ie $\neq R$) ideals of R ordered by inclusion. R nonzero implies $\{0\} \in S$ so S is nonempty. If $T \subset S$ is a chain then let $J = \bigcup_{I \in T} I$. If $x, y \in J$ then $x \in I_1$ and $y \in I_2$ for some $I_1, I_2 \in T$. Since T is totally ordered, either $I_1 \subset I_2$ or $I_2 \subset I_1$. Therefore $x + y \in J$. Also, $r \in R$, $x \in J$ implies $rx \in J$. So J is an ideal in R. It is a proper ideal since $1 \notin J$. Therefore $J \in S$ is an upper bound for T. Zorn's Lemma shows that S has a maximal, hence R has a maximal ideal.

Theorem 11.1 (Existence of algebraic closure)**.** Let K be a field. Then

(i) There is an algebraic extension L/K such that every nonconstant $f \in K[X]$ has a root in L.

(ii) K has an algebraic closure $\overline{K}$.

Proof.

(i) Let $S = \{\text{monic constant polynomials in } K[X]\}$. Rough idea: $L = K(\alpha_f : f \in S)$ where α_f is a root of f.

In detail: Let $R = K[X_f : f \in S]$ be the polynomial ring in indeterminates $\{X_f : f \in S\}$. So elements of R are finite K-linear combinations of monomials of the form $X_{f_1}^{d_1} X_{f_2}^{d_2} \cdots X_{f_r}^{d_r}$ where $f_i \in S$ and $d_i \in \mathbb{N}$. Let $I \subset R$ be the ideal generated by $\{f(X_f) : f \in S\}$.

Claim: $I \neq R$.

Proof of claim: If not then $1 \in I$, i.e.

$$1 = \sum_{f \in T} g_f f(X_f) \qquad (*)$$

for some finite subset $T \subset S$ and polynomials $g_f \in R$. Let L/K be a splitting field for $\prod_{f \in T} f$ and for each $f \in T$, let $\alpha_f \in L$ be a root of f. We define a ring homomorphism

$$\begin{aligned} \phi : R &\to L[X_f : f \in S \setminus T] \\ X_f &\mapsto \begin{cases} \alpha_f & f \in T \\ X_f & f \notin T \end{cases} \\ c &\mapsto c \qquad \forall c \in K \end{aligned}$$

Applying ϕ to $(*)$ gives

$$1 = \sum_{f \in T} \phi(g_f) \underbrace{f(\alpha_f)}_{=0} = 0$$

which gives a contradiction. Hence $I \neq R$, which proves the claim.

Since $I \neq R$, by the earlier example (Maximal ideal), we get that R/I has a maximal ideal, so equivalently R has a maximal ideal J containing I. Let $L = R/J$ and $\alpha_j = X_j + J \in L$. Then $f(\alpha_f) = 0$ (since $f(X_f) \in I \subset J$). Since

$$L = \bigcup_{\substack{T \subset S \text{ finite} \\ \text{subsets}}} K(\alpha_f : f \in T)$$

it follows that L/K is an algebraic extension.

(ii) Repeating the construction in (i) gives

$$K \subset K_1 \subset K_2 \subset \cdots$$

Each nonconstant polynomial in $K_n[X]$ has a root in K_{n+1}. If $f \in K[X]$ has degree $n \geq 1$ then is has a root α_1 in K_1. Then $\frac{f(X)}{X - \alpha_1}$ is either a constant, or a nonconstant polynomial, hence has a root α_2 in K_2, and so on, so that f splits into linear factors in K_n. Let

$$\overline{K} = \bigcup_{n \geq 1} K_n.$$

This is a field since it is a union of fields totally ordered by inclusion. Then every polynomial in $K[X]$ splits into linear factors over $\overline{K}$, and each element of $\overline{K}$ belongs to some K_n, so is algebraic over K. Now apply Lemma 3.9. □

Start of lecture 23

Now we want to prove uniqueness of algebraic closures.

Proposition 11.2. Let L/K be an algebraic extension and M/K be a field extension with M algebraically closed. Then there exists a K-embedding $L \hookrightarrow M$.

Proof. Let

$$S = \{(F, \sigma) : (\sigma : F \hookrightarrow M) \text{ a } K\text{-embedding}, K \subset F \subset L\},$$

with partial order $(F_1, \sigma_1) \leq (F_2, \sigma_2)$ if $F_1 \subset F_2$ and $\sigma_2|_{F_1} = \sigma_1$. Then $(S, \leq)$ is a partially ordered set. It is non-empty as $(K, \mathrm{id}) \in S$. Suppose $T = \{(F_i, \sigma_i) : i \in I\}$

is a chain (where I is some indexing set). Let $F = \bigcup_{i \in I} F_i$ (a field since T is totally ordered). Define

$$\begin{aligned} \sigma : F &\to M \\ x &\mapsto \sigma_i(x) \quad \text{if } x \in F_i \end{aligned}$$

This is well-defined since σ_i and σ_j agree on $F_i \cap F_j$ (again since T is totally ordered).

Then $(F, \sigma) \in S$ is an upper bound for T. Hence by Zorn's Lemma, S has a maximal element (F, σ).

Let $\alpha \in L$. Then α is algebraic over K, hence algebraic over F. By Theorem 3.4, we may extend $\sigma : F \hookrightarrow M$ to $\tau : F(\alpha) \hookrightarrow M$ (using here that M is algebraically closed). Then $(F, \sigma) \le (F(\alpha), \tau)$. Since (F, σ) is maximal, we must have $F(\alpha) = F$, so $\alpha \in F$. Therefore $F = L$ and $\sigma : L \hookrightarrow M$ is a K-embedding as required. □

Corollary 11.3 (Uniqueness of algebraic closure)**.** Let K be a field. Let L_1 and L_2 be algebraic closure of K. Then there exists a K-isomorphism $\phi : L_1 \xrightarrow{\sim} L_2$.

Note. ϕ is not necessarily unique.

Proof. Since L_1/K is algebraic and L_2/K is a field extension with L_2 algebraically closed, Proposition 11.2 gives a K-embedding $\phi : L_1 \hookrightarrow L_2$. Any $\alpha \in L_2$ is algebraic over K, hence algebraic over $\phi(L_1)$. But $\phi(L_1) \cong L_1$ is algebraically closed, and therefore $\alpha \in \phi(L_1)$. This shows that ϕ is surjective. □

12 Artin's Theorem

Theorem 12.1 (Artin's Theorem on Invariants)**.** Let L be a field and $G \subset \mathrm{Aut}(L)$ a finite subgroup. Then L/L^G is a finite Galois extension with Galois group G. In particular,

$$[L : L^G] = \#G.$$

Remark. Let $K = L^G$. Then $G \subset \mathrm{Aut}(L/K)$ and

$$K \subset L^{\mathrm{Aut}(L/K)} \subset L^G = K.$$

Therefore $K = L^{\mathrm{Aut}(L/K)}$. *If* we knew L/K is algebraic, then it would follow (by definition) that L/K is Galois. *If* moreover we knew L/K is finite then

$$L^G = L^{\mathrm{Gal}(L/K)} \overset{\text{Theorem 6.4}}{\Longrightarrow} G = \mathrm{Gal}(L/K).$$

Proof. Let $K = L^G$. Pick any $\alpha \in L$. Let

$$f(X) = \prod_{i=1}^{m} (X - \alpha_i)$$

where $\alpha_1, \ldots, \alpha_m$ are the distinct elements of $\mathrm{orb}_G(\alpha) = \{\sigma(\alpha) : \sigma \in G\}$. Then $\sigma f = f$ for all $\sigma \in G$, hence $f \in K[X]$. Therefore α is algebraic and separable over K. Hence L/K is algebraic and separable and

$$[K(\alpha) : K] \leq \#G \qquad \forall \alpha \in L.$$

Now pick $\alpha \in L$ with $[K(\alpha) : K]$ maximal.

Claim: $L = K(\alpha)$.

Proof of Claim: Let $\beta \in L$. Then $K(\alpha, \beta)/K$ is finite and separable so by Theorem of the Primitive Element, $K(\alpha, \beta) = K(\theta)$ for some $\theta \in L$. By our choice of α,

$$[K(\theta) : K] \leq [K(\alpha) : K].$$

Since $K(\alpha) \subset K(\theta)$, this gives $K(\alpha) = K(\theta)$ and hence $\beta \in K(\alpha)$. This proves the claim.

Now

$$\# \mathrm{Aut}(L/K) \leq [L : K] = [K(\alpha) : K] \leq \#G.$$

Since $G \subset \mathrm{Aut}(L/K)$, it follows that

$$\# \mathrm{Aut}(L/K) = [L : K],$$

so by Theorem 6.2, L/K is Galois and $G = \mathrm{Aut}(L/K)$. $\square$

Example. Let $L = \mathbb{C}(X_1, X_2)$. Define $\sigma, \tau \in \mathrm{Aut}(L)$ by

$$(\sigma f)(X_1, X_2) = f(iX_1, -iX_2)$$
$$(\tau f)(X_1, X_2) = f(X_2, X_1)$$

Let $G = \langle \sigma, \tau \rangle \cong D_8$. Aim: compute L^G. We spot that $X_1X_2, X_1^4 + X_2^4 \in L^G$. So we have:

$$\begin{tikzcd}
L \arrow[d, dash, "8"] \\
L^G \arrow[d, dash] \\
\mathbb{C}(X_1X_2, X_1^4 + X_2^4) \arrow[uu, bend left, dash, "\leq 8"]
\end{tikzcd}$$

Let

$$f(T) = (T^4 - X_1^4)(T^4 - X_2^4) = T^8 - (X_1^4 + X_2^4)T^4 + (X_1X_2)^4 \in \mathbb{C}(X_1X_2, X_1^4 + X_2^4)[T]$$

hence

$$[L : \mathbb{C}(X_1X_2, X_1^4 + X_2^4)] \leq 8$$

Then Artin's Theorem on Invariants implies $[L : L^G] = \#G = 8$. Then by the Tower Law,

$$L^G = \mathbb{C}(X_1X_2, X_1^4 + X_2^4).$$

Start of lecture 24

Let R be a ring and $G \subset \mathrm{Aut}(R)$ a subgroup. *Invariant theory* seeks to describe the cubring $R^G = \{x \in R \mid \sigma(x) = x \ \forall \sigma \in G\}$.

The topic was studied extensively in the 19th century and was the motivation for Hilbert's Basis Theorem. It is also important in modern algebraic geometry for describing the quotient of an algebraic variety by a group action.

Let k be a field and $L = k(X_1, \dots, X_n)$ be the field of rational functions in n variables, i.e. the field of fractions of $R = k[X_1, \dots, X_n]$. Let $G = S_n$ act on L by permutating the X_i.

Aim: compute L^G.

We note that L^G contains the elementary symmetric functions $s_1 = \sum_i X_i$, $s_2 = \sum_{i<j} X_iX_j$, ..., $s_n = \prod_i X_i$. By Symmetric Function Theorem, $R^G = k[s_1, \dots, s_n]$

and there are no polynomial relations satisfied by the s_i.

Theorem 12.2. $L^G = k(s_1, \ldots, s_n)$.

Proof 1. Let $\frac{f}{g} \in L^G$, $f, g \in R$ coprime. Then $\frac{\sigma(f)}{\sigma(g)} = \frac{f}{g}$ for all $\sigma \in G$. Since R is a UFD and the units of R are just k^*, we have $\sigma(f) = c_\sigma f$, $\sigma(g) = c_\sigma g$ for some $c_\sigma \in k^*$. But G has finite order, say $|G| = N$ (in fact $= n!$). Therefore $f = \sigma^N(f) = c_\sigma^N f$ hence $c_\sigma^N = 1$. Therefore $fg^{N-1}, g^N \in R^G = k[s_1, \ldots, s_n]$. Therefore $\frac{f}{g} = \frac{fg^{N-1}}{g^N} \in k(s_1, \ldots, s_n)$. □

Proof 2. Let

$$\begin{aligned} f(T) &= \prod_{i=1}^{n} (T - X_i) \\ &= T^n - s_1 T^{n-1} + s_2 T^{n-2} - \cdots + (-1)^n s_n \end{aligned}$$

Then $f \in k(s_1, \ldots, s_n)[T]$ is a polynomial of degree n and L is a splitting field for f over $k(s_1, \ldots, s_n)$. So we have $L/L^G/k(s_1, \ldots, s_n)$. Example Sheet 1, Question 12 tells us that $[L : k(s_1, \ldots, s_n)] \le n!$. But also $[L : L^G] = \#G = n!$ by Artin's Theorem on Invariants. So by Tower Law, $L^G = k(s_1, \ldots, s_n)$. □

Remark. We have shown that the Galois group of a "generic" monic polynomial of degree n is S_n.

Exercise: Show that for any finite group G there exists a finite Galois extension L/K with Galois group G. This may not be possible if we specify K in advance.

This may not be possible if we specify K in advance, for example $K = \mathbb{C}$ or $K = \mathbb{F}_p$, and is a famous open problem when $K = \mathbb{Q}$ (inverse Galois group).

Corollary 12.3. Let S_n act on $L = k(X_1, \ldots, X_n)$ by permuting the X_i. If $\mathrm{char}(k) \neq 2$, then $L^{A_n} = k(s_1, \ldots, s_n, \delta)$ where $\delta = \prod_{i<j}(X_i - X_j)$.

Proof. $(S_n : A_n) = 2$, hence $[L^{A_n} : k(s_1, .., s_n)] = 2$. We have $\sigma(\delta) = \mathrm{sign}(\sigma)\delta$ for all $\sigma \in S_n$. In particular $\delta \in L^{A_n}$ and $\delta \notin L^{S_n}$. Therefore $L^{A_n} = k(s_1, \ldots, s_n, \delta)$. □

Remark. It can be shown that if $R = k[X_1, \dots, X_n]$ then $R^{A_n} = k[s_1, \dots, s_n, \delta]$.

Idea of proof: Let $f \in R^{A_n}$. Pick $\sigma \in S_n \setminus A_n$. Write $f = \frac{1}{2}((f + \sigma f) + (f - \sigma f))$. Then show $f - \sigma f$ is divisible by δ.

Theorem (Fundamental Theorem of Algebra)**.** $\mathbb{C}$ is algebraically closed.

Proof. We'll use the following facts:

(i) Every polynomial over $\mathbb{R}$ of odd degree has a root in $\mathbb{R}$.

(ii) Every quadratic over $\mathbb{C}$ has a root in $\mathbb{C}$ (use quadratic formula, $\sqrt{re^{i\theta}} = \sqrt{r}e^{i\theta/2}$).

(iii) Every group of order 2^n has an index 2 subgroup (since every group of order p^k has a subgroup of order p^j for all $j \leq k$, by considering the composition series, and using the fact that the centre of a p-group is always non-trivial).

Suppose $L/\mathbb{C}$ is a finite with $L \neq \mathbb{C}$. Replacing L by its Galois closure over $\mathbb{R}$, we may assume $L/\mathbb{R}$ is Galois. Let $G = \mathrm{Gal}(L/\mathbb{R})$. Let $H \subset G$ be a Sylow 2-subgroup. Then $[L^H : \mathbb{R}] = (G : H)$ is odd. So if $\alpha \in L^H$ then $[\mathbb{R}(\alpha) : \mathbb{R}]$ is odd, hence $\alpha \in \mathbb{R}$ by (i). Therefore $L^H = \mathbb{R}$ and $G = H$ is a 2-group. Let $G_1 = \mathrm{Gal}(L/\mathbb{C}) \subset \mathrm{Gal}(L/\mathbb{R}) = G$. Since $L \neq \mathbb{C}$ we have G_1 non-trivial, so by (iii) it has an index 2 subgroup, say G_2. Then $[L^{G_2} : \mathbb{C}] = (G_1 : G_2) = 2$ ⨳ by (ii). $\square$

Index

K-embedding 16, 18

K-homomorphism 16, 17, 19, 20, 28, 31, 35, 49, 54, 74, 75

K-automorphism 35

$Aut(L/K)$ 35, 36, 37

algebraic 9, 12, 23

algebraically closed 21, 22, 23, 74, 75

algebraic closure 22, 23, 49, 73, 74, 75

algebraic 8, 9, 12, 13, 15, 16, 18, 22, 23, 75, 76

algebraic 9, 12, 22, 23, 28, 30, 35, 73, 74, 75, 76

automorphism 35, 39

Aut 35, 52, 76, 77

Cardano's formula 24

chain 72, 74

characteristic 4, 5, 30, 40, 41, 51, 54, 55, 62, 66, 68, 69, 78

composite 41, 70

L_1L_2 41, 42, 43

constructed 14, 65

constructible 14, 15

constructible 14, 15, 64, 65

constructible 14, 15, 65

cyclotomic polynomial 63

Φ_n 63, 64

cyclotomic 62, 70

χ 62, 63, 64

discriminant 27

Disc 27, 54, 55, 57, 58

elementary symmetric function 24, 25, 26, 77

embedding 5, 17, 18, 19, 49, 66

extension 4, 5, 7, 9, 10, 16, 22, 28, 34, 35, 37, 38, 43, 45, 47, 48, 49, 51, 52, 68, 70, 73, 74, 76, 78

degree 5, 10, 34, 49, 68

$[L : K]$ 5, 6, 8, 9, 10, 12, 13, 14, 15, 18, 19, 20, 22, 28, 31, 32, 33, 34, 35, 36, 37, 39, 40, 41, 43, 45, 46, 47, 49, 52, 62, 63, 64, 65, 66, 67, 68, 69, 70, 76, 78, 79

field 4, 5, 6, 8, 9, 12, 14, 17, 18, 20, 21, 22, 23, 28, 34, 35, 38, 41, 51, 52, 62, 66, 69, 70, 73, 75, 76

$K(\alpha)$ 7, 8, 9, 10, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 28, 29, 30, 31, 32, 33, 34, 35, 37, 39, 40, 41, 42, 43, 44, 45, 47, 48, 49, 54, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69, 70, 73, 74, 75, 76, 77, 78, 79

field embedding 5, 19, 20

field extension 4, 5, 6, 7, 8, 9, 12, 14, 16, 17, 18, 22, 29, 30, 31, 32, 33, 34, 35, 46, 62, 74, 75

/ 4, 5, 6, 7, 8, 9, 10, 12, 16, 17, 18, 20, 22, 23, 28, 29, 30, 31, 32, 33, 35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 51, 52, 54, 55, 57, 59, 60, 62, 63, 64, 66, 67, 68, 70, 73, 74, 75, 76, 78, 79

finite 5, 6, 9, 22, 30, 35, 38, 39, 43, 45, 47, 48, 49, 51, 70, 76, 78, 79

F_q 51, 52, 63

fixed field 35, 51, 54

L^S 35, 36, 37, 38, 39, 52, 55, 76, 77, 78, 79

formal derivative 28

’ 28, 29, 30, 51, 62, 66

Frobenius homomorphism 6, 63

Galois closure 43, 44, 79

Galois 35, 36, 37, 38, 39, 40, 41, 42, 43, 48, 51, 52, 62, 66, 68, 70, 76, 78, 79

Galois group 37, 68, 70, 76, 78

Gal 37, 38, 39, 40, 41, 42, 43, 48, 49, 51, 52, 54, 55, 57, 59, 60, 62, 63, 64, 66, 67, 68, 70, 76, 79

Gal(f/K) 54, 55, 56, 57, 58, 59, 60, 61, 69, 70, 71

homogeneous 25, 26

HomK 31, 32, 33

infinite 5

inseparable 29

Kummer extension 66, 70

lexicographic ordering 25, 26, 27

maximal 72, 75

minimal polynomial 8, 15, 16, 18, 22, 28, 30, 31, 32, 33, 34, 37, 38, 39, 43, 47, 48, 49, 54, 64

$\overline{f}$ 59, 60, 61, 64, 71

μ_n 62, 63, 66, 67, 68, 70

multiplicative group 5

K^* 5, 6, 8, 31, 51, 62, 63, 65, 66, 67, 68, 70, 78

$(K^*)^n$ 67, 68

$N_{L/K}(\alpha)$ 45, 46, 47, 48, 49

normal 28, 36, 37, 39, 40, 41, 42, 43, 70

partial order 72, 74

partially ordered set 72, 74

primitive n-th root of unity 62, 63, 66, 70

prime subfield 4, 35

resolvent cubic 56, 57, 59

$K[\alpha]$ 7

separable 30, 31, 33, 76

separable 30, 31, 33, 34, 36, 37, 39, 40, 41, 43, 49, 76

separable 29, 30, 34, 36, 37, 39, 42, 43, 51, 54, 55, 56, 57, 59, 60, 62, 64, 66

σ-embedding 17, 18, 19

σ-homomorphism 17, 32, 33

simple 7, 30

simple 28, 29

soluble 69, 70, 71

soluble by radicals 69, 70, 71

splitting field 18, 19, 20, 23, 28, 29, 30, 31, 36, 37, 39, 40, 41, 42, 43, 51, 54, 57, 59, 60, 62, 66, 70, 73, 78

symmetric polynomial 24, 25, 26

s_i 24, 25, 26, 27, 77, 78

symmetric 24, 25

totally ordered 72, 74

$\mathrm{Tr}_{L/K}(\alpha)$ 45, 46, 47, 48, 49

transcendental 9, 15

transcendental 9

upper bound 72, 75

ζ_n 62, 63, 64, 65, 66, 67, 68, 69, 70