Galois Theory Notes

Francesco Chotuck

Abstract

This is KCL undergraduate module 6CCM326A, instructed by Dr. Netan Dogra & Dr. Rachel Newton. The formal name for this class is "Galois Theory".

Contents

1 Review of ring theory

Definition 1.1. A non-trivial ring R is called an **integral domain**

- if it is commutative and,
- if $x \cdot y = 0$ implies $x = 0$ or $y = 0$ for all $x, y \in R$.

Proposition 1.2 (Canellation law in integral domains)
In an integral domain for any non-zero element $x \in R$ if

$$xu = xv \Rightarrow u = v$$

holds for all $u, v \in R$.

Definition 1.3. If R is a ring and X is an indeterminate we define the **ring of polynomials** in X over R to be

$$R[X] = \left\{a_0x^0 + a_1x^1 + a_2x^2 + \cdots a_nx^n : n \geq 0, a_i \in R\right\}.$$

Where the addition and multiplication are the obvious ones.

Example 1.4. We denote the set of units by $R^\times$. An interesting example is $(R[X])^\times = R^\times$ when R is an integral domain.

1.1 Fields

Definition 1.5. A **field** is a ring in which every non-zero element is a unit.

Example 1.6
Some examples of fields.

- The rings $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are fields.
- If p is prime then $\mathbb{Z}/p\mathbb{Z}$ is a field. We denote finite fields of cardinality n by $\mathbb{F}_n$.
- $\mathbb{Z}$ is NOT a field.

1.2 Field characteristic

Definition 1.7. The **characteristic** of a ring R is defined as the smallest positive integer n such that

$$n \cdot 1_R = \underbrace{1_R + \cdots 1_R}_{n} = 0,$$

where 1_R is the multiplicative identity in R. If no such n exists, the characteristic is said to be zero, indicating that multiplying 1_R by any integer yields a non-zero result.

Lemma 1.8

Let K be a field of characteristic $p > 0$. We have the following.

1. For all $x \in K$ we have $px = 0$.
2. $(x + y)^p = x^p + y^p$ for all $x, y \in K$.
3. $(x + y)^{p^k} = x^{p^k} + y^{p^k}$ for all $x, y \in K$ and all $k \geq 1$.

Proof. Use binomial expansion. □

1.3 Irreducible and prime elements

Definition 1.9. Let R be an integral and let $r \in R$ be an element such that $r \neq 0$ and $r \notin R^\times$. We say that r is **irreducible** in R if

$$r = st \Rightarrow s \in R^\times \text{ or } t \in R^\times$$

for all $s, t \in R$.

Definition 1.10. We say $r \in R$ is **prime**

- if $r \notin R^\times$ and,
- if $r \mid st \Rightarrow r \mid s$ or $r \mid t$ for $s, t \in R$.

1.4 Polynomial rings

Proposition 1.11

Let R be an integral domain. Then,

- the units of $R[X]$ are just the units of R,
- $R[X]$ is an integral domain.

Definition 1.12. Fix a field K. We say a polynomial $f \in K[X]$ is **irreducible** if

- $f(x) \neq 0$,
- $f(x) \neq$ constant,
- if $f = gh$ with $g, h \in K[X]$ then either g or h is constant.

Theorem 1.13. If K is a field and $f \in K[X]$ is a non-zero polynomial then

$$f = cr_1r_2 \cdots r_k \quad \text{for } c \in K^\times$$

and monic irreducible polynomials $r_1, \ldots, r_k \in K[X]$. This expression is unique up to reordering.

Definition 1.14. If $f \in \mathbb{Z}[X]$ is a non-zero polynomial we define the **content** of f to be the gcd of its coefficients. We denote this by c_f. We say f is **primitive** if $c_f = 1$.

Lemma 1.15. If $f, g \in \mathbb{Z}[X]$ are non-zero polynomials then

- $c_{fg} = c_f c_g$,
- fg is primitive $\iff$ f and g are both primitive.

1.5 Test for irreducibility

Proposition 1.16

Let $f \in K[X]$. We have the following:

- If $\deg(f) > 1$ and has a root in K then it is reducible over K.
- If $\deg(f) = 2, 3$ then $f(x)$ is reducible over K if and only if $f(x)$ has a root in K.

Lemma 1.17 (Gauss' lemma)

Suppose that $f \in \mathbb{Z}[X]$ is primitive. We have that f is irreducible in $\mathbb{Z}[X] \iff f$ is irreducible in $\mathbb{Q}[X]$.

Corollary 1.18. If $f(x) = a_0 + a_1x + \cdots a_nx^m$ and $f(\alpha) = 0$ for some $\alpha \in \mathbb{Q}$ then $\alpha = \frac{d}{e}$ for some $d, e \in \mathbb{Z}$ with $d \mid a_0$ and $e \mid a_n$.

Example 1.19

We want to find the root of $f(x) = 3x^3 + 2x - 4$ in $\mathbb{Q}$. By the corollary the only possible values of d and e are given by

$$d = \pm 1, \pm 2, \pm 4$$
$$e = \pm 1, \pm 3.$$

Therefore, the possible roots are given by

$$\alpha = \pm 1, \pm 2, \pm 4, \pm\frac{1}{3}, \pm\frac{2}{3}, \pm\frac{4}{3}.$$

However, $f(\alpha) \neq 0$ for each of these values. Since f has degree 3 and no roots in $\mathbb{Q}$, it follows that f must be irreducible in $\mathbb{Q}[X]$.

Proposition 1.20 (Eisenstein's criterion)

Suppose that p is a prime number and $f(x) = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[X]$ is a polynomial of positive degree such that

1. $p \nmid a_n$,
2. $p \mid a_0, p \mid a_1, \ldots, p \mid a_{n-1}$ and,
3. $p^2 \nmid a_0$.

Then f is irreducible in $\mathbb{Q}[X]$.

Remark 1.21. If Eisenstein's criterion fails for all p, that does not necessarily imply that f is reducible. For example, $f(x) = x^2 + x + 1$ is irreducible over $\mathbb{Q}$, but Eisenstein cannot detect this.

Proposition 1.22

Let K be a field. If $f \in K[X]$ is irreducible then so is $f(x - c)$.

Proof. First note that $f(x)$ has the same degree as $f(x - c)$. If $f(x - c) = g(x)h(x)$ for some polynomials $g, h \in K[X]$ then

$$f(x) = g(x + c)h(x + c).$$

If $f(x)$ is irreducible then either $g(x+c)$ or $h(x+c)$ is an element of $K^\times$ therefore, either g or h are in $K^\times$. We conclude that $f(x - c)$ is also irreducible. □

Example 1.23

Using this proposition, we can prove that $f(x) = x^2 + x + 1$ is irreducible over $\mathbb{Q}$. It suffices to consider $f(x + 7) = x^2 + 15x + 57$ then use Eisenstein's with $p = 3$.

Definition 1.24. If p is prime then the p-th **cyclotomic polynomial** is

$$\begin{aligned}\Phi_p(x) &= \frac{x^p - 1}{x - 1} \\ &= x^{p-1} + x^{p-2} + \cdots + x + 1.\end{aligned}$$

Proposition 1.25

The p-th cyclotomic polynomial is irreducible in $\mathbb{Q}[X]$ for every prime p.

Proof. We have that $\Phi_p(x)$ is irreducible if and only if

$$\begin{aligned}\Phi_p(x + 1) &= \frac{(x + 1)^p - 1}{x} \\ &= x^{p-1} + px^{p-2} + \binom{p}{2} x^{p-3} + \cdots + p\end{aligned}$$

is irreducible. Since p is prime $p \mid \binom{p}{i}$, so we can use Eisenstein's criterion for any p. □

1.6 Fraction fields

Definition 1.26. A **fraction field** of the ring is a field $\mathrm{Frac}(R)$ containing a subring R' isomorphic to R, such that every element of $\mathrm{Frac}(R)$ can be expressed in the form $\frac{r}{s}$ for $r, s \in R'$ where $s \neq 0$.

Note 1.27. It is the smallest field that contains R.

Proposition 1.28

Some common fraction fields.

- $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q}$.
- If R is a field then $\mathrm{Frac}(R) = R$.
- If K is a field then

$$\begin{aligned}\mathrm{Frac}(K[X]) &= K(X) \\ &= \left\{ \frac{f}{g} : f, g \in K[X], g \neq 0 \right\}.\end{aligned}$$

We call the field $K(X)$ the **field of rational functions over** K (in the variable X).

Remark 1.29. More generally, we denote $\mathrm{Frac}\left(K[X_1, \ldots, X_n]\right) = K(X_1, \ldots, X_n)$.

Definition 1.30. Let $K \subset L$ be a subfield of the field L and let $\alpha \in K$. Then $K(\alpha) = \mathrm{Frac}(K[\alpha])$ is the smallest subfield of L containing K and α. We call it the **subfield of L generated over K by α**.

Example 1.31. We have $\mathbb{Q}\left(\sqrt[4]{2}\right) = \mathbb{Q}\left[\sqrt[4]{2}\right]$ since $\mathbb{Q}\left[\sqrt[4]{2}\right]$ is already a field. On the other hand, we have that $\mathbb{Q}[\pi] \subset \mathbb{Q}(\pi)$.

Note 1.32. What is the point of this? If we want to find the smallest of a field L of $\mathbb{Q}$ such that it contains $\alpha \notin \mathbb{Q}$ we can imply adjoin α to L by way of a fraction field i.e. $L(\alpha)$ and this is to be guaranteed to be a field.

Example 1.33. What is the smallest extension field L of $\mathbb{Q}$ that contains $\sqrt{2}$ and i?

Solution. We simply adjoin them to $\mathbb{Q}$ and obtain $\mathbb{Q}(\sqrt{2})(i) = \mathbb{Q}(\sqrt{2}, i)$. We can see this by taking an arbitrary element from $\mathbb{Q}(\sqrt{2})(i)$, which has the form $\alpha + i\beta$ where $\alpha, \beta \in \mathbb{Q}(\sqrt{2})$. Let us expand,

$$\begin{aligned}\alpha + i\beta &= (a + b\sqrt{2}) + i(c + d\sqrt{2}) \\ &= a + b\sqrt{2} + ci + di\sqrt{2}.\end{aligned}$$

Therefore, we can write $\mathbb{Q}(\sqrt{2}, i) = \left\{a + b\sqrt{2} + ci + di\sqrt{2} : a, b, c, d \in \mathbb{Q}\right\}$.

2 Field extensions

Definition 2.1. A **field extension** is a field homomorphism $\phi : K \to L$.

Remark 2.2. Field homomorphisms are injective so $K \cong \phi(K) \subseteq L$ (i.e. $\phi(K)$ is a subfield of L). In practice, K will often be a subfield of L and ϕ will be the inclusion map ι. Sometimes even when $\phi \neq \iota$ we will identify K with $\phi(K)$.

Proposition 2.3

From now on we will refer to the field extension $\phi : K \to L$ as "L/K" which is read as "L over K".

Example 2.4

Some examples of field extensions.

- $\mathbb{R}$ is a field extension of $\mathbb{Q}$.
- $\mathbb{C}$ is a field extension of $\mathbb{R}$.
- A field K is a field extension of K. To do so we can use the obvious choice of the identity map however, there may be other homomorphisms from $K \to K$. For example $\psi : \mathbb{C} \to \mathbb{C}$ with $\psi(z) = \overline{z}$ is also a field extension of $\mathbb{C}$.

Theorem 2.5. Suppose that L/K is an extension. Under the operations

$$\begin{aligned} L \times L &\to L \\ (l_1, l_2) &\mapsto l_1 + l_2 \end{aligned}$$

and

$$\begin{aligned} K \times L &\to L \\ (k, l) &\mapsto kl \end{aligned}$$

we have that L is a vector space over K.

Definition 2.6. For a field extension $\phi : K \to L$, we define the **degree** of L over K to be the dimension of L as a vector space over K, we denote this by $[L : K]$. Furthermore,

- We say the field extension is **finite** whether its degree is finite, we denote this by $[L : K] < \infty$.
- We say the field extension is **infinite** whether its degree is infinite, we denote this by $[L : K] = \infty$.

Remark 2.7. The degree may depend on the homomorphism. The example to consider is $\phi : \mathbb{Q}(t) \to \mathbb{Q}(t^2) \subset \mathbb{Q}(t)$ with the map $t \mapsto t^2$. Indeed, $[\mathbb{Q}(t), \mathbb{Q}(t)]_\iota = 1$ whereas $[\mathbb{Q}(t) : \mathbb{Q}(t^2)]_\phi = 2$.

Example 2.8. We have that:

- $[\mathbb{C} : \mathbb{R}] = 2$ since $\{1, i\}$ is a basis for $\mathbb{C}$ over $\mathbb{R}$ (since every complex number can be uniquely written as $a + ib$) for $a, b \in \mathbb{R}$.

- $[\mathbb{R} : \mathbb{Q}] = \infty$ since any finite-dimensional vector space over $\mathbb{Q}$ is countable but $\mathbb{R}$ is uncountable.

Definition 2.9. We provide the following definitions.

- If $a \in S$, define the **evaluation homomorphism**

$$\begin{aligned} \mathrm{ev}_a : R[X] &\to S \\ f(x) = \sum r_i x^i &\mapsto \sum r_i a^i. \end{aligned}$$

  We denote the element $\mathrm{ev}_a(f)$ by $f(a)$.

- The image of ev_a is a subring of S which we denote by $R[\alpha]$.
- We call $R[\alpha]$ the **subring of S generated over R by α**.

Remark 2.10. More generally for any $\alpha_1, \ldots, \alpha_n$ we similarly define $R[\alpha_1, \ldots, \alpha_n]$ called subring of S generated over R by $\alpha_1, \ldots, \alpha_n$ to be the image of $R[X_1, \ldots, X_n]$ under the map sending f to $f(\alpha_1, \ldots, \alpha_n)$.

Proposition 2.11. $R[\alpha]$ is the smallest subring of S containing R and α.

Proposition 2.12
Let K be a field and let $f \in K[X]$ be irreducible. We have that $K[X]/(f)$ is a field and that $[K[X]/(f) : K] = \deg(f)$.

Remark 2.13. Let $\deg(f) = d$. The proof of this proposition shows that the set

$$\mathcal{B} = \left\{ [1], [x], \ldots, [x]^{d-1} \right\} \subset K[X]/(f)$$

is a basis for $K[X]/(f)$ as a vector space over K.

Proof.

Proof. Let d be the degree of f. We will show that the subset

$$S = \{\, [1], [X], \ldots, [X]^{d-1} \,\} \subset K[X]/(f)$$

is a basis for $K[X]/(f)$ as a vector space over K

We first prove that S is linearly independent over K. We must prove that if

$$\iota(a_0) + \iota(a_1)[X] + \cdots + \iota(a_{d-1})[X]^{d-1} = [0], \qquad a_0, a_1, \ldots, a_{d-1} \in K,$$

then $a_0 = a_1 = \cdots = 0$. But note that

$$\begin{aligned} \iota(a_0) + \iota(a_1)[X] + \cdots + \iota(a_{d-1})[X]^{d-1} &= [a_0] + [a_1][X] + \cdots + [a_{d-1}][X]^{} \\ &= [a_0 + a_1 X + \cdots + a_{d-1}X^{d-1}], \end{aligned}$$

and for this to be $[0]$ means that $a_0 + a_1X + \cdots + a_{d-1}X^{d-1}$ is in the ideal (f). Since this polynomial has degree at most $d-1$, and f has degree d, this implies that $a_0 = a_1 = \cdots = a_{d-1} = 0$.

Now we prove that S spans $K[X]/(f)$ over K. Suppose that $[g] \in K[X]/(f)$ (so $g \in K[X]$). We must show that

$$[g] = \iota(a_0) + \iota(a_1)[X] + \cdots + \iota(a_{d-1})[X]^{d-1}$$

16

for some $a_0, a_1, \ldots, a_{d-1} \in K$. By the Division Algorithm, we have $g = qf + r$ for some $q, r \in K[X]$ with $\deg r < d$. Note that $g - r = qf \in (f)$, so $[g] = [r]$. Writing $r = a_0 + a_1X + \cdots + a_{d-1}X^{d-1}$, we have

$$[r] = [a_0] + [a_1][X] + \cdots + [a_{d-1}][X]^{d-1} = \iota(a_0) + \iota(a_1)[X] + \cdots + \iota(a_{d-1})[X]^{d-1},$$

so $[g] = [r]$ is in the span of S over K.

□

Example 2.14

Let $\alpha = \sqrt[4]{2}$. Then $\mathbb{Q}[\alpha]$ is the image of the homomorphism $\mathrm{ev}_\alpha : \mathbb{Q}[X] \to \mathbb{R}$ defined by $\mathrm{ev}_\alpha(g) = g(\alpha)$. The polynomial $f(x) = x^4 - 2$ is the kernel of ev_α which is an ideal of $\mathbb{Q}[X]$ containing (f). Since f is irreducible the only ideals containing (f) are (f) and $\mathbb{Q}[X]$ but $1 \notin \ker(\mathrm{ev}_\alpha)$ therefore $\mathrm{ev}_\alpha = (f)$. By the isomorphism theorem we have that $\mathbb{Q}[X]/(f) \cong \mathbb{Q}[\alpha]$. The proof the proposition above gives us a basis for $\mathbb{Q}[\alpha]/(f)$ as a $\mathbb{Q}$-vector space given by $\{1, \alpha, \alpha^2, \alpha^3\}$.

Remark 2.15. By the first isomorphism theorem $R[\alpha] \cong R[X]/\ker(\mathrm{ev}_\alpha)$. Therefore, $R[\alpha]$ and $R[X]$ mean different things.

Theorem 2.16 (Tower law)

If $\phi : K \to L$ and $\psi : L \to M$ are field extensions then so is $\psi \circ \phi : K \to M$, and

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

Example 2.17

The set $\mathbb{Q}[\sqrt[4]{2}] = \left\{a + b\sqrt[4]{2} + c\sqrt{2} + d(\sqrt[4]{2})^3 : a, b, c, d \in \mathbb{Q}\right\}$, as such $\left[\mathbb{Q}[\sqrt[4]{2}] : \mathbb{Q}\right] = 4$. A similar argument shows that $\left[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}\right] = 2$ therefore, by the tower law we have

$$\left[\mathbb{Q}[\sqrt[4]{2}] : \mathbb{Q}\right] = \left[\mathbb{Q}[\sqrt[4]{2}] : \mathbb{Q}[\sqrt{2}]\right]\left[\mathbb{Q}[\sqrt{2}] : \mathbb{Q}\right].$$

It follows that $\left[\mathbb{Q}[\sqrt[4]{2}] : \mathbb{Q}[\sqrt{2}]\right] = 2$.

Remark 2.18. This formula is still valid if any of the degrees are infinite. Furthermore, we can extend this result in an obvious way. Consider a sequence $K_n/K_{n-1}, K_{n-1}/K_{n-2}, \ldots, K_1/K_0$ of field extension, clearly

$$[K_n : K_0] = [K_n : K_{n-1}][K_{n-1} : K_{n-2}] \cdots [K_1 : K_0].$$

3 Algebraicity

Definition 3.1. Let L/K be a field extension. We say:

- $\alpha \in L$ is **algebraic** over K if there exists a non-zero polynomial $f \in K[X]$ such that $f(\alpha) = 0$;
- L is **algebraic** over K if every element of L is algebraic over K;
- $\alpha \in L$ is transcendental if α is not algebraic over K;
- L is **transcendental** over K if not algebraic over K.

Example 3.2

We provide some examples.

- Every element of K is algebraic over K when the field extension is the identity.
- Given $\lambda \in K$ we have that $f = x - \lambda \in K[X]$. Hence, λ is algebraic since $f(\lambda) = 0$.

Proposition 3.3

If L/K is a finite field extension then L is algebraic over K.

Proof. Let $d = [L : K]$ and suppose that $\alpha \in L$. There must be a dependence relation among the $d + 1$ elements: $1, \alpha, \alpha^2, \ldots, \alpha^d$ i.e. there exists coefficients in K not all zero such that

$$\sum_{n=0}^{d} a_n \alpha^n = 0.$$

Letting $f(x) = \sum_{n=0}^{d} a_n x^n$ we have $f(\alpha) = 0$. Therefore, α is algebraic over K. □

Theorem 3.4

Suppose L/K is a field extension and let $\alpha \in L$.

1. If α is algebraic over K, then there exists a unique monic irreducible $f \in K[X]$ such that $f(\alpha) = 0$. Furthermore,
   (a) if $g \in K[X]$ then $g(\alpha) = 0 \iff f \mid g$.
   (b) $\mathrm{ev}_\alpha : K[X]/(f) \to K(\alpha)$ is an isomorphism.
   (c) $K[\alpha]$ is a field thus, $K[\alpha] = K(\alpha)$, and $[K(\alpha) : K] = \deg(f)$.
2. If α is transcendental over K, then ev_α defines an isomorphism $K[X] \to K[\alpha]$. So, $K[\alpha]$ is not a field and $[K(\alpha) : K] = \infty$.

3.1 Minimal polynomial

Definition 3.5. If L/K is a field extension and $\alpha \in L$ is algebraic over K, then the unique monic irreducible polynomial $m_{\alpha,K} \in K[X]$ of the smallest degree such that $m_{\alpha,K}(\alpha) = 0$ is called the **minimal polynomial** of α over K.

Remark 3.6. The minimal polynomial of α depends on L, but also on K.

Corollary 3.7. Let L/K be a field extension and let $\alpha \in L$. The following are equivalent.

1. α is algebraic over K.
2. $K[\alpha] = K(\alpha)$.

3. $[K(\alpha) : K] < \infty$.
4. $\alpha \in E$ for some field extension E (of K) which is contained in L and $[E : K] < \infty$.

Corollary 3.8
If L/K is a field extension then the following are equivalent.

1. $[L : K] < \infty$.
2. $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ for some $\alpha_1, \alpha_2, \ldots, \alpha_n \in L$, each of which is algebraic over K.

Proposition 3.9
Let $K(\alpha)/K$ be a field extension and let $m_{\alpha,K}$ be the minimal polynomial of α then $[K(\alpha) : K] = \deg(m_{\alpha,K})$.

Lemma 3.10. Suppose L/K is a field extension and $\alpha, \beta \in L$ are algebraic over K. Then

- $\alpha + \beta$ is algebraic over K,
- $\alpha\beta$ is algebraic over K,
- if $\alpha \neq 0$ then α^{-1} is algebraic over K.

Furthermore, $\alpha + \beta, \alpha\beta, \alpha^{-1} \in K(\alpha, \beta)$.

Proof. Since α be β are algebraic over K the corollary above shows that $K(\alpha, \beta)$ is finite over K and hence algebraic over K. Since $\alpha + \beta, \alpha\beta$ and α^{-1} (if $\alpha \neq 0$) are elements of $K(\alpha, \beta)$ they are algebraic over K. □

Lemma 3.11. Let L/K be a field extension and suppose $\alpha, \beta \in L$ are algebraic. We have $[K(\alpha, \beta) : K(\alpha)] \leq [K(\beta) : K]$.

Proof. Since α and β are algebraic over K we have that $[K(\alpha) : K][K(\beta) : K] < \infty$. □

Lemma 3.12. Let L/K be a field extension and let $M \subset L$ be a subfield containing the image of K. If $\alpha \in L$ then $[M(\alpha) : M] \leq [K(\alpha) : K]$.

Corollary 3.13
Suppose L/K is a field extension. Then the set

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

is a subfield of L.

Example 3.14

$\mathbb{C}/\mathbb{Q}$ is a field extension the set

$$\mathbb{A} = \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}$$

is called the **field of algebraic numbers**. We have that $\mathbb{A}$ is algebraic over $\mathbb{Q}$ but is not finite over $\mathbb{Q}$. This is because $\mathbb{A}$ contains $\mathbb{Q}\left(\sqrt[n]{2}\right)$ for all $n \geq 1$ and $[\mathbb{Q}\left(\sqrt[n]{2}\right) : \mathbb{Q}] = n$ and so $\mathbb{A}$ must have degree at least n.

Note 3.15. We say that every finite extension is algebraic. This example proves the converse is false.

Proposition 3.16

Let L/K be a field extension. If $\alpha \in L$ is algebraic over K with minimal polynomial $f(x) \in K[X]$ then $f(x-c)$ is the minimal polynomial of $\alpha + c$.

Proof. If f is the minimal polynomial of α then $f(x)$ is a monic irreducible polynomial and $f(\alpha) = 0$. Let $g(x) = f(x-c)$, we have that $g(x)$ is monic and also irreducible. Since

$$g(\alpha + c) = f(\alpha + c - c) = f(\alpha) = 0,$$

it follows that $g(x)$ is the minimal polynomial of $\alpha + c$. □

3.2 Splitting field

Definition 3.17. Suppose L/K is a field extension and that $f \in K[X]$. We say that:

- f **splits completely** over L if there exists $c, \alpha_1, \alpha_2, \ldots, \alpha_n \in L$ such that

$$f(x) = c(x - \alpha_1)(x - \alpha_2)\cdots(x - \alpha_n) \in L[X];$$

- if $L = K(\alpha_1, \alpha_2, \ldots, \alpha_n)$ then we call L a **splitting field** of f over K.

Note 3.18. We can think of a splitting field as the smallest extension of K which contains all the roots of f.

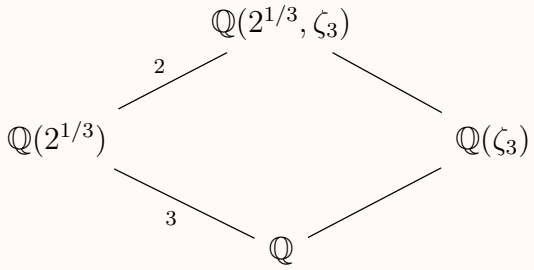
Example 3.19. By the Fundamental theorem of algebra every polynomial $f \in \mathbb{Q}[X]$ splits completely in $\mathbb{C}$. Furthermore, given $f \in \mathbb{Q}[X]$ and let $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ be its roots, then $\mathbb{Q}(\alpha_1, \ldots, \alpha_n)$ is the splitting field.

Example 3.20 (IMPORTANT EXAMPLE)

Consider $f(x) = x^3 - 2 \in \mathbb{Q}[X]$. We want to find the roots of f to do so we proceed with the substitution $x = z\sqrt[3]{2}$. With this we can rewrite $x^3 - 2 = 0$ as $2z^3 - 2 = 0$ and equivalently $z^3 - 1 = 0$. Now, it follows that the roots of this are precisely the third roots of unity $2^{1/3}, \zeta_3 2^{1/3}, \zeta_3^2 2^{1/3}$ where $\zeta = e^{2\pi i/3}$. Hence, the splitting field is given by

$$\mathbb{Q}\left(2^{1/3}, \zeta_3 2^{1/3}, \zeta_3^2 2^{1/3}\right).$$

We can also write this field as $\mathbb{Q}(2^{1/3}, \zeta_3)$. So we have the following tower of field extensions.



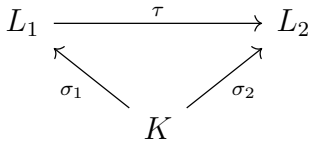
We used the fact that $\left[\mathbb{Q}(2^{1/3}, \zeta_3) : \mathbb{Q}(2^{1/3})\right] = \deg(m_{\zeta_3, \mathbb{Q}(2^{1/3})})$. Where $m_{\zeta_3, \mathbb{Q}(2^{1/3})} = x^2 + x + 1$.

Proposition 3.21

Let K be a field and $f \in K[X]$. Then there exists a field extension L/K which is a splitting field of f.

4 Field embeddings

Definition 4.1. Let K be a field and, let $\sigma_1 : K \to L_1$ and $\sigma_2 : K \to L_2$ be two field extensions of K. A **K-embedding** (from L_1 to L_2) is a homomorphism of rings $\tau : L_1 \to L_2$ such that $\tau \circ \sigma_1 = \sigma_2$. That is the following diagram commutes:



Remark 4.2. We can think of K as a subfield of both L_1 and L_2 so, σ_1 and σ_2 are inclusion maps. As such a K-embedding $\tau : L_1 \to L_2$ is a field homomorphism such that $\tau(x) = x$ for all $x \in K$.

Example 4.3

Some examples of field embeddings.

- For any field extension the identity map is a K-embedding.
- Let $\mathbb{Q}\left(2^{1/4}\right)/\mathbb{Q}$ and $\mathbb{C}/\mathbb{Q}$ be field extension then,
  - The inclusion $\tau_1 : \mathbb{Q}\left(2^{1/4}\right) \hookrightarrow \mathbb{C}$ is a $\mathbb{Q}$-embedding because all elements of $\mathbb{Q}$ are stabilised by the inclusion and,
  - $\tau_2 : \mathbb{Q}\left(2^{1/4}\right) \to \mathbb{C}$ with $2^{1/4} \mapsto i2^{1/4}$ is also a $\mathbb{Q}$-embedding, because $2^{1/4} \notin \mathbb{Q}$, so it does not matter what it is mapped to, as the other elements in $\mathbb{Q}(2^{1/4})$ are stabilised under τ_2.
- $\mathbb{Q}\left(2^{1/4}\right)/\mathbb{Q}\left(\sqrt{2}\right)$ and $\mathbb{C}/\mathbb{Q}\left(\sqrt{2}\right)$ are field extensions. We have that
  - τ_1 is a $\mathbb{Q}(\sqrt{2})$-embedding. We need to check that $\sqrt{2}$ is stabilised under the inclusion map, that is τ_1: we can write
  $$\tau_1(\sqrt{2}) = \tau((2^{1/4})^2) = \tau_1(2^{1/4})^2 = \sqrt{2}.$$
  - τ_2 is NOT a $\mathbb{Q}(\sqrt{2})$-embedding. This is because $\sqrt{2}$ is not stabilised under $\tau_2 : 2^{1/4} \mapsto i2^{1/4}$:
  $$\tau_2(\sqrt{2}) = \tau_2((2^{1/4})^2) = \tau_2(2^{1/4})^2 = -\sqrt{2}.$$

Note 4.4. By 'stabilised' we mean that $\tau(x) = x$ for all $x \in K$ is satisfied.

By the remark above we must check the adjoint element is stabilised under the embedding.

Proposition 4.5

If $\tau : K_1 \to K_2$ is a field homomorphism we have the following.

1. $\text{char}(K_1) = \text{char}(K_2)$.
2. Let $\phi_1 : F \to K_1$ and $\phi_2 : F \to K_2$ be field extensions. Then $\tau \circ \phi_1 : F \to K_2$ so $\tau \circ \phi_1 = \phi_2$ i.e. τ is an F-embedding.

Remark 4.6. We can take $F = \mathbb{Q}$ or $\mathbb{F}_p$.

Example 4.7

We have that

$$\tau : \mathbb{Q}(2^{1/3}) \to \mathbb{Q}(\zeta_3 2^{1/3})$$
$$2^{1/3} \mapsto \zeta_3 2^{1/3}$$

is a $\mathbb{Q}$-embedding. This is because by the first isomorphism theorem we have that

$$\mathbb{Q}(2^{1/3}) \cong \mathbb{Q}[X]/(x^3 - 2) \cong \mathbb{Q}(\zeta_3 2^{1/3}).$$

Definition 4.8. If L_1/K and L_2/K are field extensions we write

- $\mathrm{Hom}_K(L_1, L_2)$ for the set of K-embeddings $L_1 \to L_2$.
- $\mathrm{Iso}_K(L_1, L_2)$ for the set of K-embeddings which are (K-)isomorphism.
- $\mathrm{Aut}_K(L_1)$ for the set of K-automorphism.

Theorem 4.9 (Artin's extension theorem)

Let $K(\alpha)/K$ and L/K be field extensions with $K(\alpha)$ algebraic over K. Let $m_{\alpha,K} \in K[X]$ be the minimal polynomial of α in $K[X]$. Then, we have the following bijection

$$\mathrm{Hom}_K(K(\alpha), L) \to \{\text{roots of } m_{\alpha,K} \text{ in } L\}$$
$$\sigma \mapsto \sigma(\alpha).$$

Lemma 4.10. In the notation of the theorem above $\sigma(\alpha)$ is a root of $m_{\alpha,K}$.

Example 4.11

We illustrate some examples.

- By the theorem we can say that there is a bijection between

$$\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(2^{1/4}), \mathbb{C}) \longleftrightarrow \left\{\text{roots of } x^4 - 2 \text{ in } \mathbb{C}\right\},$$

  which implies there exactly 4 $\mathbb{Q}$-embeddings given by

$$2^{1/4} \mapsto i^k 2^{1/4} \quad \text{for } k \in \{0, 1, 2, 3\}.$$

- By the theorem we can say that there is a bijection between

$$\mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}(2^{1/3}), \mathbb{Q}(\zeta_3, 2^{1/3})) \longleftrightarrow \left\{\text{roots of } x^3 - 2 \text{ in } \mathbb{Q}(\zeta_3, 2^{1/3})\right\}.$$

Corollary 4.12

A set of corollaries.

1. Let L_1/K be a finite extension and L_2/K be an extension then we have that $\#\mathrm{Hom}_K(L_1, L_2) \leq [L_1 : K]$.
2. If L_1/K and L_2/K are finite extensions and $\tau : L_1 \to L_2$ is a K-embedding then
$$[L_1 : K] \leq [L_2 : K]$$
and if equal then τ is a K-isomorphism.
3. If $f \in K[X]$ then any two splitting fields of f are K-isomorphic.

5 Separability

Definition 5.1. Let K be a field and $f \in K[X]$ with $\deg(f) = d$. We say f is **separable** if it has d distinct roots in the splitting field over K. That is, if

$$f(x) = c(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_d)$$

for some $c \in K$ and distinct elements $\alpha_1, \ldots, \alpha_d \in L$, where L is the splitting field. Otherwise, we say f is **inseparable**.

Example 5.2

Some examples of separable and inseparable polynomials.

- $x^2 - x$ is separable in any field K.
- $x^2 + 2x + 1 = (x + 1)^2$ is not separable in any field, as it has only one root.
- $x^2 + 2 \in \mathbb{Q}[X]$ is irreducible. Its splitting field is $\mathbb{Q}[\sqrt{-2}]$, and we can factor $x^2 + 2 = (x - \sqrt{-2})(x + \sqrt{-2})$. Since $\pm\sqrt{-2}$ are roots, we have that $x^2 + 2$ is separable.
- If K is a field of characteristic $p > 0$ prime then $x^p - 1$ and $x^p - \lambda$ for $\lambda \in K$ are NOT separable in $K[X]$. In fact, we have that $(x - 1)^p = x^p - 1$ in such fields.

Definition 5.3. Let L/K be a field extension. We say $\alpha \in L$ is **separable** over K if

- α is algebraic over K and,
- $m_{\alpha,K} \in K[X]$ is separable.

We say L/K is **separable** if every element of L is separable over K.

Definition 5.4. Suppose K is a field and $f \in K[X]$. We define the derivative as usual.

Proposition 5.5. The usual laws of derivative hold.

Lemma 5.6. Let K be a field, $f \in K[X]$ and $\alpha \in K$. Then α is a repeated root of $f \iff f(\alpha) = 0$ and $f'(\alpha) = 0$.

Lemma 5.7. Let L/K be a field extension and $g, h \in K[X]$. Then $\gcd(f, g) \in K[X]$ is equal to the $\gcd(f, g) \in L[X]$.

Proposition 5.8

Let K be a field and $f \in K[X]$ be a non-zero polynomial. We have the following.

1. f is separable $\iff \gcd(f, f') = 1$.
2. Suppose L/K is a field extension. We have that f is separable in $K[X] \iff f$ is separable in $L[X]$.
3. Suppose f is irreducible in $K[X]$, we have that f is separable $\iff f'(x) \neq 0$.
4. If f is irreducible in $K[X]$ and $\text{char}(K) = 0$ then, f is separable.

Corollary 5.9

If K is a field of characteristic 0 then every algebraic field extension of K is separable over K.

Proof. If L/K is algebraic then any $\alpha \in L$ is also algebraic. So $m_{\alpha,K} \in K[X]$ is an irreducible polynomial. By (4) of the proposition $m_{\alpha,K}$ is separable and so L/K is separable. □

Example 5.10 (IMPORTANT)

Recall that the splitting field of $x^p - t$ is given by $\mathbb{F}_p(t)(t^{1/p}) = \mathbb{F}_p(t, t^{1/p})$ since $(x - t^{1/p})^p = x^p - t$. This polynomial is irreducible in $\mathbb{F}_p(t)[X]$ so $x^p - t$ is the minimal polynomial of $t^{1/p}$ in $\mathbb{F}_p(X)$ and is also inseparable. This is because $\dfrac{\mathrm{d}}{\mathrm{d}x}(x^p - t) = px = 0 \in \mathbb{F}_p(t)[X]$.

Theorem 5.11

Suppose that $\sigma : K_1 \to K_2$ is a field homomorphism let $\phi : K_1 \to L_1$. That is,

$$\begin{array}{ccc} L_1 & \xrightarrow{\tau} & L_2 \\ {\scriptstyle\phi}\uparrow & & \uparrow{\scriptstyle\psi} \\ K_1 & \xrightarrow{\sigma} & K_2 \end{array}$$

Then the following are equivalent.

1. L_1 is separable over K_1.
2. There exists $\alpha_1, \ldots, \alpha_n \in L$ such that $L_1 = K(\alpha_1, \ldots, \alpha_n)$ and, each α_i is separable over K_1.
3. There exists $\alpha_1, \ldots, \alpha_n \in L$ such that $L_1 = K(\alpha_1, \ldots, \alpha_n)$ and, each α_i is separable over K_1 and each α_i for $i = 2, \ldots, m$ is separable over $K(\alpha_1, \ldots, \alpha_{i-1})$.
4. There exists a field extension L_2/K_2 such that there $[L_1 : K_1]$ distinct homomorphisms $\tau : L_1 \to L_2$ such that $\sigma = \tau \circ \phi$.

Note 5.12. Suppose $\sigma = \mathrm{id}$, then this theorem says that an extension L_1/K is separable if and only if there is some other field extension L_2/K such that $\#\mathrm{Hom}_K(L_1, L_2) = [L_1 : K]$.

$$\begin{array}{ccccc} L_1 & & \xrightarrow{\tau} & & L_2 \\ & {\scriptstyle\phi}\nwarrow & & \nearrow{\scriptstyle\psi} & \\ & & K & & \end{array}$$

Corollary 5.13. Let L/K be a field extension then the set

$$\{\alpha \in L : \alpha \text{ is separable over } K\}$$

is a subfield of L.

Lemma 5.14. If K is a finite field then, the group $K^\times$ is cyclic.

Theorem 5.15 (Primitive element theorem)

If L/K is a finite separable extension then there exists $\alpha \in L$ such that $L = K(\alpha)$.

Note 5.16. Since L/K is a finite separable extension then we know $L = K(\alpha_1, \ldots, \alpha_m)$ for some $\alpha_1, \ldots, \alpha_m \in K$ each separable over K. The theorem says, we can write $L = K(A)$ for $A \in L$.

- K is finite. We can take a generator $A \in L^\times$.
- K is infinite. To find such L it suffices to consider the case when $L = K(\alpha, \beta)$. We will have that $L = K(\alpha + \lambda\beta)$. To check if a given λ is correct it suffices to check that the K-embeddings $\tau_i(\alpha + \lambda\beta)$ are all distinct, where $\tau_i \in \mathrm{Hom}_K(L, M)$ and $\#\mathrm{Hom}_K(L, M) = [L : K]$.

For 'higher' cases we repeat the process with $K(\alpha+\lambda\beta)(\gamma)$.

Note 5.17. We have $\#\mathrm{Hom}_K(L,M) = [L:K]$ if and only if L/K is a separable extension.

Proof. We will consider two cases.

- K is a finite field. Since L/K is a finite extension it means L is also finite. Therefore, $L^\times$ is cyclic. Now, let $\alpha \in L^\times$ be a generator then, $L = K(\alpha)$ since every non-zero element of L is of the form α^n for some $n \in \mathbb{Z}$ and hence is in $K(\alpha)$.
- K is an infinite field. Since L/K is a finite extension we have $L = K(\alpha_1, \ldots, \alpha_m)$ for some $\alpha_1, \ldots, \alpha_m \in L$ is separable over K. We will use induction on m.
  - $m = 1$ is trivial.
  - $m = 2$ we write $K(\alpha, \beta)$. Since L/K is separable then there exists an extension M/K with $\#\mathrm{Hom}_K(L,M) = [L:K]$. It suffices to prove that there exists $\lambda \in K$ such that $\{\sigma_i(\alpha+\lambda\beta) : \sigma_i \in \mathrm{Hom}_K(L,M)\}$ has size n in M i.e. $\#\mathrm{Hom}_K(K(\alpha+\lambda\beta), M) \geq n$. This would imply that $[K(\alpha+\lambda\beta):K] \geq n = [L:K]$ which by the Tower law would imply $L = K(\alpha+\lambda\beta)$.
    Let us prove this. Since $\sigma_i \in \mathrm{Hom}(L,M)$ is K-linear we can write $\sigma_i(\alpha+\lambda\beta) = \sigma_i(\alpha) + \lambda\sigma_i(\beta)$. We want to find a λ such that
    $$\sigma_i(\alpha) + \lambda\sigma_i(\beta) \neq \sigma_j(\alpha) + \lambda\sigma_j(\beta) \quad \text{for } i \neq j.$$
    We note that if
    $$\sigma_i(\alpha) = \sigma_i(\beta) \quad \text{and} \quad \sigma_j(\beta) = \sigma_j(\beta)$$
    then $i = j$. Hence, if $i \neq j$ then would imply that
    $$\lambda = \frac{\sigma_i(\alpha) - \sigma_j(\alpha)}{\sigma_j(\beta) - \sigma_i(\beta)}.$$
    But $\left\{ \frac{\sigma_i(\alpha)-\sigma_j(\alpha)}{\sigma_j(\beta)-\sigma_i(\beta)} : i \neq j \right\}$ is a finite subset of M, and since K is infinite we can choose λ not in this set then $K(\alpha,\beta) = K(\alpha+\lambda\beta)$.
  - We can argue that $K(\alpha_1, \ldots, \alpha_{m-1})(\alpha_m) = K(\alpha')(\alpha_m) = K(\alpha', \alpha_m)$.

□

Example 5.18

Consider the extension $\mathbb{Q}(i,\sqrt{2})/\mathbb{Q}$. Since the polynomial x^2+1 has no roots in $\mathbb{Q}(\sqrt{2})$ it is irreducible in $\mathbb{Q}(\sqrt{2})[X]$, so it is the minimal polynomial of i over $\mathbb{Q}(\sqrt{2})$. We therefore have $\left[\mathbb{Q}(i,\sqrt{2}):\mathbb{Q}(\sqrt{2})\right]=2$ which by the Tower law implies that the degree $\left[\mathbb{Q}(i,\sqrt{2}):\mathbb{Q}\right]=4$ hence, $\mathbb{Q}(i,\sqrt{2})/\mathbb{Q}$ is a finite extension. Clearly, i and $\sqrt{2}$ are separable over $\mathbb{Q}$ thus, by the primitive element theorem we have that $\mathbb{Q}(i,\sqrt{2})/\mathbb{Q}$ is a simple extension.

It is true that $\left[\mathbb{Q}(i+\sqrt{2}):\mathbb{Q}\right]=4$ and since $i+\sqrt{2}\in\mathbb{Q}(i,\sqrt{2})$, it follows that $\mathbb{Q}(i,\sqrt{2})=\mathbb{Q}(i+\sqrt{2})$.

To tie this in with the preceding proof, we find the four embeddings of $\mathbb{Q}(i,\sqrt{2})$ into some field M and show that their values at $i+\sqrt{2}$ are distinct. To find the embeddings we will take $M=\mathbb{C}$. First, we have two embeddings $\sigma_1,\sigma_2:\mathbb{Q}(\sqrt{2})\to\mathbb{C}$ determined by $\sigma_1(\sqrt{2})=\sqrt{2}$ and $\sigma_2(\sqrt{2})=-\sqrt{2}$. Then there will be two ways to extend each of these embeddings to embeddings $\mathbb{Q}(i,\sqrt{2})\to\mathbb{C}$. We can write this in table of values

	τ_1	τ_2	τ_3	τ_4
$\sqrt{2}$	$\sqrt{2}$	$\sqrt{2}$	$-\sqrt{2}$	$-\sqrt{2}$
i	i	$-i$	i	$-i$
$i+\sqrt{2}$	$i+\sqrt{2}$	$-i+\sqrt{2}$	$i-\sqrt{2}$	$-i-\sqrt{2}$

Note that the values of $\tau_i(i+\sqrt{2})$ are distinct which recovers the fact that $L=\mathbb{Q}(\alpha)$. Note also that the values must be roots of $m_{\alpha,\mathbb{Q}}$ which we can therefore find by computing:

$$\prod_{i=1}^{d}(x-\tau_i(i+\sqrt{2}))=x^4-2x^2+9.$$

Definition 5.19. If L/K is a field extension then we say that L is a **simple** extension of K if $L=K(\alpha)$ for some $\alpha\in L$ which is algebraic over K.

Remark 5.20. The Primitive element theorem says that every finite separable extension is simple and that every finite extension of fields of characteristic 0 is simple.

Proposition 5.21 (Summary)

Suppose L/K is finite. The following are equivalent.

1. L is separable over K.
2. $L=K(\alpha)$ for some $\alpha\in L$ separable over K.
3. $L=K(\alpha_1,\ldots,\alpha_m)$ for some $\alpha_1,\ldots,\alpha_m\in L$ each of which is separable over K.
4. $L=K(\alpha_1,\ldots,\alpha_m)$ for some $\alpha_1,\ldots,\alpha_m\in L$ with α_1 separable over K and α_i separable over $K(\alpha_1,\ldots,\alpha_{i-1})$ for $i=2,\ldots,m$.
5. There is an extension L' of K such that there are $[L:K]$ distinct K-embeddings $\tau:L\to L'$.

6 Galois extensions

Definition 6.1. A field extension L/K is **normal** if

- L is algebraic over K and,
- for all extension M/L and K-embeddings $\sigma : L \to M$ we have $\sigma(L) \subset L$.

Proposition 6.2

Every field extension L/K with $[L : K] = 2$ is normal.

Example 6.3

We provide some examples and non-examples.

- The field extension $\mathbb{Q}(i)/\mathbb{Q}$ is normal. $\mathbb{Q}(i)$ has a $\mathbb{Q}$-basis given by $1, i$ thus, any $\mathbb{Q}$-embedding $\sigma : \mathbb{Q}(i) \to M$ must have that

$$\sigma(1) = 1 \in \mathbb{Q}(i) \quad \text{and} \quad \sigma(i) = \pm i \in \mathbb{Q}(i).$$

  We conclude, $\sigma(\mathbb{Q}(i)) \subset \mathbb{Q}(i)$.

- The field extension $\mathbb{Q}\left(2^{1/3}\right)/\mathbb{Q}$ is NOT normal. That is, there exists a field extension $M/\mathbb{Q}\left(2^{1/3}\right)$ and there exists $\mathbb{Q}$-embedding $\sigma \in \mathrm{Hom}_{\mathbb{Q}}(\mathbb{Q}, M)$ such that $\sigma\left(\mathbb{Q}\left(2^{1/3}\right)\right) \not\subset \mathbb{Q}\left(2^{1/3}\right)$.

  We can consider the extension $\mathbb{C}/\mathbb{Q}\left(2^{1/3}\right)$ and the $\mathbb{C}$-embedding

$$\begin{aligned} \sigma : \mathbb{Q}\left(2^{1/3}\right) &\to \mathbb{C} \\ 2^{1/3} &\mapsto \zeta_3 2^{1/3}. \end{aligned}$$

  Clearly, $\sigma(2^{1/3}) \notin \mathbb{R}$ and $\mathbb{Q}(2^{1/3}) \subset \mathbb{R}$ thus, $\sigma\left(\mathbb{Q}\left(2^{1/3}\right)\right) \not\subset \mathbb{Q}\left(2^{1/3}\right)$.

Lemma 6.4. Let L_1/K be a finite field extension and let $\sigma : K \to L_2$ be a field homomorphism. Then there is a field extension M/L_2 and a field homomorphism $\tau : L_1 \to M$ such that $\tau|_K = \sigma$.

Note 6.5. We have $\tau|_K : K \subset L_1 \to M$.

Proposition 6.6

Let L/K be a finite extension. Then the following are equivalent.

1. L is normal over K.
2. For every $\alpha \in L$ the corresponding minimal polynomial $m_{\alpha,K}$ splits completely over L.
3. L is a splitting field of some polynomial $f \in K[X]$.

Remark 6.7. For (3) in the proof we take f to be the product of the minimal polynomials of each α_i.

Example 6.8 (IMPORTANT)

Not all normal extensions are splitting fields of polynomials. Consider the set

$$\mathbb{A} = \{\alpha \in \mathbb{C} : \alpha \text{ is algebraic over } \mathbb{Q}\}.$$

This is a normal extension of $\mathbb{Q}$ but, it has infinite degree, so it is not the splitting field a polynomial in $\mathbb{Q}[X]$. A splitting field of a polynomial of degree n has finite degree $\leq n!$.

Definition 6.9. We say a field extension L/K is **Galois** if

- it is normal and,
- separable.

Example 6.10

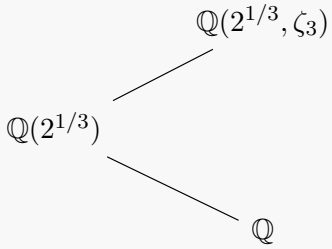
We provide some examples and non-examples.

- The field extension $\mathbb{C}/\mathbb{R}$ is Galois. It is normal since it is the splitting field of x^2+1; it is also separable since it is a field extension of fields with characteristic 0.
- The field extension $\mathbb{Q}(\zeta_3)(2^{1/3})/\mathbb{Q}(\zeta_3)$ is separable since both fields have characteristic 0. This is a normal extension
- The field extension $\mathbb{Q}(2^{1/3}, \zeta_3)/\mathbb{Q}$ is Galois. It is separable because the fields have characteristic 0. It is also normal since we have previously shown that $\mathbb{Q}(2^{1/3}, \zeta_3) = \mathbb{Q}(2^{1/3}, \zeta_3 2^{1/3}, \zeta_3^2 2^{1/3})$ is the splitting field of $x^3 - 2$.
- The field extension $\mathbb{Q}(2^{1/3})/\mathbb{Q}$ is NOT Galois. The extension is separable since both fields are of characteristic 0, but it is NOT normal since the minimal polynomial of $2^{1/3}$ given by $m_{2^{1/3},\mathbb{Q}} = x^3 - 2$ does not split completely in $\mathbb{Q}(2^{1/3})$.
- The field extension $\mathbb{F}_p(t)(\alpha)/\mathbb{F}_p(t)$ is NOT Galois. This is because α is a root of $x^p - t \in \mathbb{F}_p(t)[X]$ (so $\mathbb{F}_p(t)(\alpha) = \mathbb{F}_p(t^{1/p})$). Recall since $(a+b)^p = a^p + b^p$ in $\mathbb{F}_p(t)(\alpha)$ we have that $(x-\alpha)^p = x^p - \alpha^p = x^p - t$, so $x^p - t$ splits completely in $\mathbb{F}_p(t)(\alpha)$. Since $x^p - t$ is irreducible in $\mathbb{F}_p(t)[X]$ we have that $\mathbb{F}_p(t)(\alpha)/\mathbb{F}_p(t)$ is normal but not separable.

Proposition 6.11

If $K \subset E \subset L$ is a tower of field extensions and L/K is Galois then L/E is Galois.

Remark 6.12. Given fields such that $K \subset E \subset L$ and a field extension L/K that is Galois, it does NOT imply that E/K is Galois. We have that E/K is separable, but it may not necessarily be normal. For example consider the tower of field extensions $\mathbb{Q} \subset \mathbb{Q}(2^{1/3}) \subset \mathbb{Q}(2^{1/3}, \zeta_3)$.



Proof. If L/K is Galois then L is normal over K and so is normal over E. Similarly, L is separable over K so every element of L is separable over K and hence separable over E so, L is separable over E. Therefore, L is Galois over E. □

Definition 6.13. Let L/K be a field extension. A **K-automorphism** of L is a K-isomorphism $\sigma : L \to L$. The set of K-automorphism of L is a group under composition, denoted $\mathrm{Aut}_K(L)$.

Proposition 6.14

Suppose L/K is a finite field extension. The following are equivalent.

1. L is Galois over K.
2. For all $\alpha \in L$, the corresponding minimal polynomial $m_{\alpha,K}$ has exactly $\deg(m_{\alpha,K})$ distinct roots in L.
3. $|\mathrm{Aut}_K(L)| = [L : K]$.

Remark 6.15. In particular, if L/K is Galois then $|\mathrm{Gal}(L/K)| = [L : K]$.

6.1 Galois group

Definition 6.16. Let L/K be a Galois extension. The **Galois group** is defined to be

$$\mathrm{Gal}(L/K) = \mathrm{Aut}_K(L) = \{\sigma : L \to L : \sigma|_K = \mathrm{id}\}.$$

Example 6.17. The Galois group of $\mathbb{C}/\mathbb{R}$ is $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{e, \sigma\}$ where e is identity and σ is complex conjugation i.e. $\sigma(z) = \overline{z}$. This is obvious: the group must contain the identity, the id automorphism, and the only other automorphism which stabilises $\mathbb{R}$ in $\mathbb{C}$ is given by complex conjugation.

Example 6.18

The field extension $\mathbb{Q}\left(i, \sqrt[4]{2}\right)/\mathbb{Q}$ is Galois since $\mathbb{Q}\left(i, \sqrt[4]{2}\right)$ is the splitting field of x^4-2 over $\mathbb{Q}$ so, the extension is normal and separable since the fields have characteristic 0.

We aim to describe the elements of the Galois group. From the tower of extensions $\mathbb{Q} \subset \mathbb{Q}\left(\sqrt[4]{2}\right) \subset \mathbb{Q}\left(i, \sqrt[4]{2}\right)$ we know that

$$\left[\mathbb{Q}\left(i, \sqrt[4]{2}\right) : \mathbb{Q}\right] = \left[\mathbb{Q}\left(i, \sqrt[4]{2}\right) : \mathbb{Q}\left(\sqrt[4]{2}\right)\right]\left[\mathbb{Q}\left(\sqrt[4]{2}\right) : \mathbb{Q}\right] = 2 \cdot 4 = 8.$$

Therefore, $\mathrm{Gal}\left(\mathbb{Q}\left(i, \sqrt[4]{2}\right)/\mathbb{Q}\right)$ has order $\left[\mathbb{Q}\left(i, \sqrt[4]{2}\right) : \mathbb{Q}\right] = 8$ and similarly, the order of $\mathrm{Gal}\left(\mathbb{Q}\left(i, \sqrt[4]{2}\right)/\mathbb{Q}\left(\sqrt[4]{2}\right)\right)$ is 2.

We have that $\mathrm{Gal}\left(\mathbb{Q}\left(i, \sqrt[4]{2}\right)/\mathbb{Q}\left(\sqrt[4]{2}\right)\right) = \langle\tau\rangle \cong \mathbb{Z}/2\mathbb{Z}$.

Similarly, we have that $\mathrm{Gal}\left(\mathbb{Q}\left(i, \sqrt[4]{2}\right)/\mathbb{Q}\left(i\right)\right)$ has order 4, but there exists two groups of order 4. For a $\sigma \in \mathrm{Gal}\left(\mathbb{Q}\left(i, \sqrt[4]{2}\right)/\mathbb{Q}\left(i\right)\right)$, we let $\sigma\left(\sqrt[4]{2}\right) = i\sqrt[4]{2}$ since we know $\sqrt[4]{2}$ must be mapped to a root of $x^4 - 2$. We compute the order of $\sigma\left(\sqrt[4]{2}\right)$:

$$\sigma\left(\sqrt[4]{2}\right) = i\sqrt[4]{2}$$
$$\left[\sigma\left(\sqrt[4]{2}\right)\right]^2 = -\sqrt[4]{2}.$$

Since $\sigma^2 \neq \mathrm{id}$ we must have σ being an element of order 4. We conclude that $\mathrm{Gal}\left(\mathbb{Q}\left(i, \sqrt[4]{2}\right)/\mathbb{Q}\left(i\right)\right) = \langle\sigma\rangle \cong \mathbb{Z}/4\mathbb{Z}$.

Since $\mathrm{Gal}\left(\mathbb{Q}\left(i, \sqrt[4]{2}\right)/\mathbb{Q}\left(i\right)\right)$ and $\mathrm{Gal}\left(\mathbb{Q}\left(i, \sqrt[4]{2}\right)/\mathbb{Q}\left(\sqrt[4]{2}\right)\right)$ are subgroups of $\mathrm{Gal}\left(\mathbb{Q}\left(i, \sqrt[4]{2}\right)/\mathbb{Q}\right)$ we know that $\sigma, \tau \in \mathrm{Gal}\left(\mathbb{Q}\left(i, \sqrt[4]{2}\right)/\mathbb{Q}\right)$.

There are many groups of order 8 thus, we claim $\mathrm{Gal}\left(\mathbb{Q}\left(i, \sqrt[4]{2}\right)/\mathbb{Q}\right) \cong D_4$. To show this it suffices to show

$$\tau\sigma\tau^{-1} = \sigma^{-1} \iff \tau\sigma = \sigma^3\tau,$$

a defining relation of D_4.

7 Fundamental theorem of Galois Theory

Definition 7.1. For field extension L/K, we define an **intermediate field** (or **intermediate extension**) of L/K as a field E with $K \subset E \subset L$.

Remark 7.2. By choosing E to be K or L, we have that they are intermediate fields of L/K. Indeed, $L \subset L$ and for the field extension $\phi : K \to L$ we have that $\phi(K) \subset L$.

Definition 7.3. Let L/K be a Galois extension and H a subgroup of $\mathrm{Gal}(L/K)$. We define the **fixed field of** H as

$$L^H = \{x \in L : \sigma(x) = x \text{ for all } \sigma \in H\} \subset L$$

which contains K.

Remark 7.4. L^H is a subfield of L containing K i.e. we have $K \subset L^H \subset L$.

Proposition 7.5. The field L^H is an intermediate field of L/K.

Theorem 7.6 (Fundamental theorem of Galois Theory)
Suppose L/K is a finite Galois extension. We have the following.

1. There is a bijection

$$\begin{aligned} \{\text{subgroups of } \mathrm{Gal}(L/K)\} &\leftrightarrow \{\text{intermediate fields of } L/K\} \\ H &\mapsto L^H \\ \mathrm{Gal}(L/E) &\hookleftarrow E \end{aligned}$$

   where $K \subset E \subset L$. This bijection is inclusion reversing, that is

$$H_1 \subset H_2 \iff L^{H_1} \supset L^{H_2}.$$

2. An intermediate field, E, $K \subset E \subset L$, is Galois over K (i.e. E/K is Galois) if and only if $\mathrm{Gal}(L/E)$ is normal in $\mathrm{Gal}(L/K)$. In this case we have the following

$$\mathrm{Gal}(L/K)/\mathrm{Gal}(L/E) \cong \mathrm{Gal}(E/K);$$

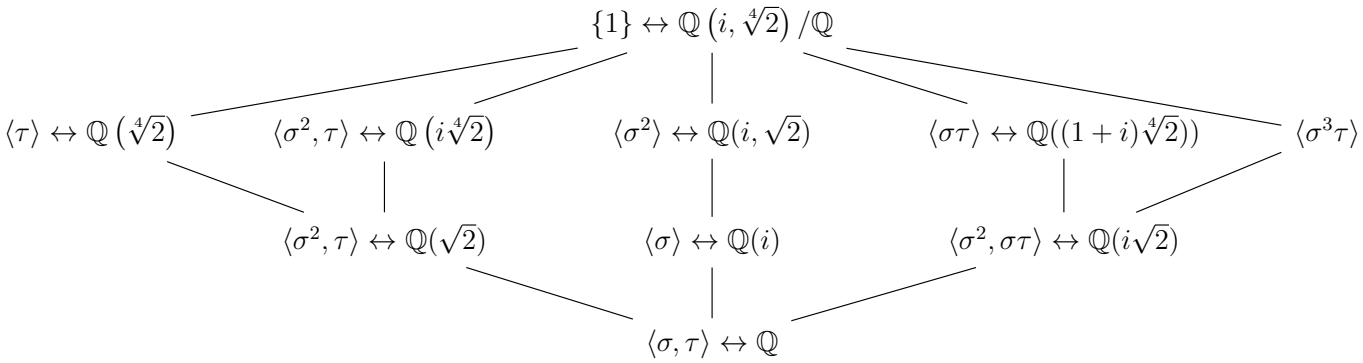
   this is given by

$$\begin{aligned} \mathrm{Gal}(L/K) &\to \mathrm{Gal}(E/K) \\ \sigma &\mapsto \sigma|_E \end{aligned}$$

   by the first isomorphism theorem.

Example 7.7
The onion from Week 5 lecture scan

Example 7.8. From the example involving $\mathrm{Gal}\left(\mathbb{Q}\left(i, \sqrt[4]{2}\right)/\mathbb{Q}\right)$ we match the subgroups with their respective fields.



The lines represent inclusion where from the bottom includes everything from the top. By the fundamental theorem of Galois theory, the bijection is inclusion reversing therefore, the smallest subgroup corresponds to the largest field.

8 Galois groups of polynomials

Proposition 8.1

Suppose L/K is a finite field extension. Then the following are equivalent:

1. L/K is Galois;
2. L is a splitting field over K of some separable polynomial $f \in K[X]$;
3. L is a splitting field over K of some separable irreducible polynomial $f \in K[X]$.

Definition 8.2. For a separable polynomial $f \in K[X]$, the corresponding Galois group of f is $\mathrm{Gal}(L_f/K)$ where L_f is a splitting field for f over K.

Proposition 8.3

If $f \in K[X]$ is a separable polynomial of degree n then its Galois group $\mathrm{Gal}(L_f/K)$ is isomorphic to a subgroup of S_n.

Proof. Since f is separable, it follows that f has n distinct roots in L_f, that is there exists a bijection

$$\pi : \{\text{roots of } f \text{ in } L_f\} \to \{1, 2, \ldots, n\}$$

(so π labels the roots of f as $\alpha_1, \cdots, \alpha_n$). We now consider the map

$$\begin{aligned} \mathrm{Gal}(L_f/K) &\to S_n \\ \sigma &\mapsto \pi \circ \sigma \circ \pi^{-1}; \end{aligned}$$

this is a homomorphism since $\sigma_1 \circ \sigma_2 \mapsto \pi \circ \sigma_1 \circ \sigma_2 \circ \pi^{-1} = (\pi \circ \sigma_1 \circ \pi^{-1})(\pi \circ \sigma_2 \circ \pi^{-1})$.

We prove this map is injective. Suppose $\pi \circ \pi^{-1} = \mathrm{id}_{S_n}$ then $\sigma = \pi^{-1}\,\mathrm{id} \circ \pi = \pi \circ \pi^{-1} = \mathrm{id}_{L_f}$. □

Example 8.4. Applying this proposition to $f(x) = x^3 - 2 \in \mathbb{Q}[X]$ shows that $\mathrm{Gal}(L_f/\mathbb{Q}) \hookrightarrow S_3$. It follows that $L_f = \mathbb{Q}\left(\sqrt[3]{2}, \zeta_3\right)$ where $\zeta_3 = e^{2\pi i/3}$. We have previously seen that $[L_f : \mathbb{Q}] = 6$ therefore, $|\mathrm{Gal}(L_f/\mathbb{Q})| = 6$ which implies $\mathrm{Gal}(L_f/\mathbb{Q}) \cong S_3$.

Example 8.5

Let $f(x) = (x^2 - 2)(x^2 + 1) \in \mathbb{Q}[X]$, it is separable polynomial since the roots are $\pm\sqrt{2}$ and ± 1. The splitting field $L_f = \mathbb{Q}(i, \sqrt{2})$. We label the roots using π, and we have that

$$\begin{aligned} \pi(\sqrt{2}) &= 1 \quad \pi(i) &&= 3 \\ \pi(-\sqrt{2}) &= 2 \quad \pi(-i) &&= 4. \end{aligned}$$

We have previously computed $\mathrm{Gal}(L_f/\mathbb{Q})$ and realised it is generated by some σ and τ such that

$$\begin{aligned} \tau(\sqrt{2}) &= -\sqrt{2} \quad \tau(i) &&= i \\ \sigma(\sqrt{2}) &= \sqrt{2} \quad \sigma(i) &&= -i. \end{aligned}$$

Therefore, τ corresponds to (12) and σ corresponds to (34). In conclusion, $\mathrm{Gal}(L_f/\mathbb{Q}) \cong \langle (12), (34) \rangle = \{e, (12), (34), (12)(34)\} \subset S_4$.

Example 8.6. If we choose a different labelling say $\pi' = (1234) \circ \pi$ that is, $\pi'(\sqrt{2}) = 2$ and $\pi'(-\sqrt{2}) = 3$ etc. Then

$$\begin{aligned} \mathrm{Gal}(L_f/\mathbb{Q}) &\to S_4 \\ \sigma &\mapsto \pi' \circ \sigma(\pi')^{-1} \\ &= (1234) \circ \pi \circ \sigma\pi^{-1} \circ (1234)^{-1}. \end{aligned}$$

Therefore,

$$\tau \mapsto (1234) \circ (12)(1234)^{-1} = (23) \in S^4$$

and now $\mathrm{Gal}(L_f/\mathbb{Q}) \cong \langle (23), (14) \rangle = \{e, (23), (14), (23)(14)\}$. This corresponds to conjugation by (1234) to $\langle (12), (34) \rangle$.

Example 8.7

In this example we explore what happens if we choose a different polynomial with the same splitting field. Consider the field $\mathbb{Q}(\sqrt{2}, i) = \mathbb{Q}(i + \sqrt{2})$, where the minimal polynomial of $i + \sqrt{2}$ is $f(x) = x^4 - 2x^2 + 9$. Since $\mathbb{Q}(i + \sqrt{2})$ is Galois over $\mathbb{Q}$ it contains all the roots of f and is therefore, a splitting field of f. The roots of g are

$$\alpha_1 = i + \sqrt{2}, \quad \alpha_2 = -i + \sqrt{2}, \quad \alpha_3 = i - \sqrt{2}, \quad \alpha_4 = -i - \sqrt{2}.$$

Let σ and τ be as above as

$$\sigma(\alpha_1) = \alpha_3 \quad \text{and} \quad \sigma(\alpha_2) = \alpha_4,$$

we have that σ corresponds to $(13)(24) \in S_4$. Similarly, τ corresponds $(12)(34) \in S_4$. In conclusion,

$$\begin{aligned} \mathrm{Gal}(L_f/\mathbb{Q}) &\cong \langle (12)(34), (13)(24) \rangle \\ &= \{e, (13)(24), (12)(34), (14)(23)\}. \end{aligned}$$

This is not conjugate to any of the previous subgroups we wrote down, as conjugation would preserve the length of the cycle transposition.

Remark 8.8. The key difference between these examples is that $(x^2 - 2)(x^2 + 1)$ is a reducible polynomial in $\mathbb{Q}[X]$ whereas $x^4 - 2x^2 + 9$ is an irreducible polynomial in $\mathbb{Q}[X]$.

Definition 8.9. A subgroup G of S_n is **transitive** if for every $i, j \in \{1, 2, \ldots, n\}$ there exists $g \in G$ such that $g(i) = j$.

Remark 8.10. Alternatively, for $i \in \{1, 2, \ldots, n\}$, the **orbit** of i under G is $\{g(i) : g \in G\}$. The action of G partitions $\{1, 2, \ldots, n\}$ into disjoints orbits. Therefore, G is transitive if and only if all $\{1, 2, \ldots, n\}$ are in one orbit.

Example 8.11. Consider the group $G = \{e, (12), (34), (12)(34)\}$. We have that $\{1, 2, 3, 4\} = \{1, 2\} \cup \{3, 4\}$ therefore, G is not transitive.

Lemma 8.12

Let L/K be a finite Galois extension and $\alpha \in L$ then the set of roots in L of the minimal polynomial $m_{\alpha,K}$ is

$$\{\sigma(\alpha) : \sigma \in \mathrm{Gal}(L/K)\}.$$

Remark 8.13. We can equivalently rewrite this as: if L/K is Galois and $\alpha \in L$ then $m_{\alpha,K}(x)$ is the product of the distinct linear factors $x - \sigma(\alpha)$ for $\sigma \in \mathrm{Gal}(L/K)$.

Note 8.14. We can use this find minimal polynomials.

Example 8.15

Consider the polynomial $f(x) = x^3 - 2 \in \mathbb{Q}[X]$. The splitting field $L_f = \mathbb{Q}\left(\sqrt[3]{2}, \zeta_3\right)$ and its Galois group $\mathrm{Gal}(L_f/\mathbb{Q}) = \langle \sigma, \tau \rangle = \{e, \sigma, \sigma^2, \tau, \sigma\tau, \sigma^2\tau\} \cong S_3$ where

$$\sigma : \begin{cases} \sqrt[3]{2} & \mapsto \zeta_3\sqrt[3]{2} \\ \zeta_3 & \mapsto \zeta_3 \end{cases}$$

and

$$\tau : \begin{cases} \sqrt[3]{2} & \mapsto \sqrt[3]{2} \\ \zeta_3 & \mapsto \zeta_3^2. \end{cases}$$

Applying the elements of $\mathrm{Gal}(L_f/\mathbb{Q})$ to $\sqrt[3]{2}$ we have

$$\begin{aligned} e(\sqrt[3]{2}) &= \sqrt[3]{2} \quad \sigma(\sqrt[3]{2}) \quad &&= \zeta_3\sqrt[3]{2} \quad \sigma^2(\sqrt[3]{2}) = \zeta_3^2\sqrt[3]{2} \\ \tau(\sqrt[3]{2}) &= \sqrt[3]{2} \quad \sigma\tau(\sqrt[3]{2}) \quad &&= \zeta_3\sqrt[3]{2} \quad \sigma^2\tau(\sqrt[3]{2}) = \zeta_3^2\sqrt[3]{2}. \end{aligned}$$

Each root is repeated twice so, $m_{\sqrt[3]{2},\mathbb{Q}}(x) = (x - \sqrt[3]{2})(x - \zeta_3\sqrt[3]{2})(x - \zeta_3^2\sqrt[3]{2})$ since, the minimal polynomial is separable.

Example 8.16. Let us consider the above again but with $\beta = \zeta_3 + \sqrt[3]{2}$. Applying the elements of $\mathrm{Gal}(L_f/\mathbb{Q})$ to β gives

$$\begin{aligned} e(\zeta_3 + \sqrt[3]{2}) &= \zeta_3 + \sqrt[3]{2} \quad \sigma(\zeta_3 + \sqrt[3]{2}) \quad &&= \zeta_3 + \zeta\sqrt[3]{2} \quad \sigma^2 = \zeta_3 + \zeta_3^2\sqrt[3]{2} \\ \tau(\zeta_3 + \sqrt[3]{2}) &= \zeta_3^2 + \sqrt[3]{2} \quad \sigma\tau(\zeta_3 + \sqrt[3]{2}) \quad &&= \zeta_3^2 + \zeta\sqrt[3]{2} \quad \sigma^2\tau = \zeta_3^2 + \zeta^2\sqrt[3]{2}. \end{aligned}$$

We have 6 distinct elements. Therefore, $m_{\beta,\mathbb{Q}}(x)$ is equal to $\prod(x - \text{distinct elements})$. We can actually rewrite $m_{\beta,\mathbb{Q}}(x)$ in terms of $m_{\sqrt[3]{2},\mathbb{Q}}(x)$ to find that

$$m_{\beta,\mathbb{Q}}(x) = x^6 + 3x^5 + 6x^4 + 3x^3 + 9x + 9.$$

Proposition 8.17

If $f \in K[X]$ is separable irreducible polynomial of degree n then its Galois group is isomorphic to a transitive subgroup of S_n and $n \mid \#\mathrm{Gal}(L_f/K)$.

Proof?

9 Polynomials of low degree

Consider $f \in K[X]$ to be a polynomial of degree d. We investigate what the possibilities for $\mathrm{Gal}(L_f/K)$ are. We can assume that f is monic as it would not change the roots and so L_f and $\mathrm{Gal}(L_f/K)$ are unchanged.

9.1 Degree 1

If $d = 1$ then $f(x) = x - \alpha \in K[X]$ therefore, $L_f = K$ and $\mathrm{Gal}(L_f/K) = \{e\}$.

9.2 Degree 2

If $d = 2$ then $f(x) = x^2 + bx + c$. The quadratic formula tells us the roots of f which are given by

$$\alpha_1 = \frac{-b + \sqrt{b^2 - 4c}}{2} \quad \text{and} \quad \alpha_2 = \frac{-b - \sqrt{b^2 - 4c}}{2}.$$

Remark 9.1. Since we are dividing by 2 it must be that K is not of characteristic 2!

Definition 9.2. We call $\Delta_f = b^2 - 4c$ the **discriminant** of f.

Proposition 9.3

We have that $L_f = K\left(\sqrt{\Delta_f}\right)$. Furthermore,

- f is separable if and only if $\Delta_f \neq 0$.
- f is irreducible if and only if Δ_f is not a square in K (i.e. $\sqrt{\Delta_f} \notin K$).
  - If Δ_f is a square in K then $L_f = K$ and $\mathrm{Gal}(L_f/K) = \{e\}$.
  - If Δ_f is NOT a square in K then $[L_f : K] = 2$ and $\mathrm{Gal}(L_f/K) \cong \mathbb{Z}/2\mathbb{Z}$. In particular, we have that $\mathrm{Gal}(L_f/K) = \{e, \sigma\}$ where

$$\sigma : \begin{cases} \sqrt{\Delta_f} & \mapsto -\sqrt{\Delta_f} \\ \alpha_1 & \mapsto \alpha_2 \\ x + y\sqrt{\Delta_f} & \mapsto x - y\sqrt{\Delta_f}. \end{cases}$$

Example 9.4. Consider $f(x) = x^2 + 1 \in \mathbb{R}[X]$ then $\Delta_f = -4$ which is not a square in $\mathbb{R}$. We have that $L_f = \mathbb{C}$ and $\mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \{e, \sigma\}$ where σ is given by complex conjugation.

9.3 Degree 3

Proposition 9.5

Suppose K is a field which is NOT of characteristic 2 or 3 and suppose $f \in K[X]$ is a monic, cubic, irreducible polynomial. Let L_f be the splitting field of f so $L_f = K(\alpha_1, \alpha_2, \alpha_3)$ where $\alpha_1, \alpha_2, \alpha_3$ are the roots of f.

Let

$$\delta = (\alpha_1 - \alpha_2)(\alpha_2 - \alpha_3)(\alpha_3 - \alpha_1) \quad \text{and} \quad \Delta = \delta^2.$$

Then

1. $\Delta \in K^\times$;
2. if $\delta \in K$ (i.e. Δ is a square in K) then $\mathrm{Gal}(L_f/K) \cong A_3 = \{e, (123), (132)\} \subset S_3$;
3. if $\delta \notin K$ then $\mathrm{Gal}(L_f/K) \cong S_3$.

Corollary 9.6. Using the labelling $\alpha_1, \alpha_2, \alpha_2$ we obtain $\phi : \mathrm{Gal}(L_f/K) \hookrightarrow S_3$, we have that

- if $\phi(\sigma) \in A_3$ then $\sigma(\delta) = \delta$,
- if $\phi(\sigma) \notin A_3$ then $\sigma(\delta) = -\delta$.

Definition 9.7. For f as in the proposition, the element $\Delta = \delta^2 \in K$ is called the discriminant for f, and denoted by Δ_f.

Proposition 9.8

If for $f(x) = x^3 + rx^2 + sx + t$ with $r, s, t \in K$ we can let $g(x) = f\left(x - \frac{r}{3}\right)$ to complete the cubic, and we obtain $g(x) = x^3 + ax + b$, where

$$a = s - \frac{r^2}{3} \quad \text{and} \quad b = \frac{2r^3}{27} - \frac{rs}{3} + t.$$

Then $\Delta_f = -4a^3 - 27b^2$ and that if $g(x - c)$ for $c \in K$ then $\Delta_f = \Delta_g$.

Example 9.9. For $f(x) = x^3 - 2$ we have that $a = 0$ and $b = -2$. The discriminant given $\Delta = -27(-2)^2 = -2^2 \cdot 3^3$ which is not a square in $\mathbb{Q}$. Therefore, $\mathrm{Gal}(L_f/\mathbb{Q}) \cong S_3$.

Example 9.10

Let $f(x) = x^3 - 2 \in \mathbb{Z}/7\mathbb{Z}[X]$. Since f is a cubic it suffices to check if f has a root to determine its irreducibility. We see that f has no roots in $\mathbb{Z}/7\mathbb{Z}$ hence it is irreducible. To determine the Galois group of f over k we consider the discriminant and use the proposition. We have that $\Delta_f = -27(-2)^2 = 4$ which is a square in $\mathbb{Z}/7\mathbb{Z}$. Hence, $\mathrm{Gal}(L_f/(\mathbb{Z}/7\mathbb{Z})) \cong A_3$.

9.4 Degree 4

Let K be a field which is not of characteristic 2. Let f be a monic irreducible quartic polynomial in $L[X]$. By some proposition we know that $\mathrm{Gal}(L_f/K)$ is isomorphic to a transitive subgroup of S_4. Any such subgroup is conjugate to one of:

- $\langle(1234)\rangle = C_4 \cong \mathbb{Z}/4\mathbb{Z}$;
- $\{e, (12)(34), (13)(24), (14)(23)\} = V_4 \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$;
- $\langle(1234), (13)\rangle = D_4$ (dihedral group of order 8).
- A_4
- S_4.

Note 9.11. In this section we provide a criterion for deciding which of these is isomorphic to the Galois group.

Definition 9.12. Let K be a field and let $f \in K[X]$ be a monic polynomial of degree $n \geq 1$. We write L_f for a splitting field of f, and we write $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ with $\alpha_i \in K_f$. The discriminant of f is $\Delta_f = \delta^2$ where $\delta = \prod_{1 \leq i \leq j \leq n} (\alpha_i - \alpha_j)$.

Proposition 9.13. We note that f is separable if and only if the roots are distinct which is if and only if $\delta \neq 0 \iff \Delta_f \neq 0$.

Now we assume f is separable so L_f/K is Galois and use the labelling $\alpha_1, \ldots, \alpha_n$ to identify $\mathrm{Gal}(L - f/K)$ with a subgroup of S_n. We write $\sigma \in \mathrm{Gal}(L_f/K)$ as a product of transpositions, then

$$\sigma(\delta) = \begin{cases} \delta & \text{if } \sigma \text{ is a product of transposition i.e. } \sigma \text{ corresponds to an element of } A_n \\ -\delta & \text{otherwise.} \end{cases}$$

So $\Delta_f \in L_f^{\mathrm{Gal}(L_f/K)} = K$ and, if $\mathrm{char}(K) \neq 2$ then $\delta \in K$ if and only if $\mathrm{Gal}(L_f/K) \subset A_n$. In general, we have $K(\sqrt{\Delta_f}) = K(\delta) = L_f^{\mathrm{Gal}(L_f/K) \cap A_n}$.

Definition 9.14. Write $f(x) = (x - \alpha_1)(x - \alpha_2)(x - \alpha_3)(x - \alpha_4) \in K[X]$ and each $\alpha_i \in L_f$. The **cubic resolvent** (or resolvent cubic) of f is

$$g(x) = (x - \beta_1)(x - \beta_2)(x - \beta_3)$$

where

$$\begin{aligned} \beta_1 &= \alpha_1\alpha_2 + \alpha_3\alpha_4 \\ \beta_2 &= \alpha_1\alpha_3 + \alpha_2\alpha_4 \\ \beta_3 &= \alpha_1\alpha_4 + \alpha_2\alpha_3. \end{aligned}$$

If we assume that f is separable then it follows that g is separable since

$$\begin{aligned} \beta_1 - \beta_2 &= (\alpha_1 - \alpha_4)(\alpha_2 - \alpha_3) \neq 0 \\ \beta_1 - \beta_3 - (\alpha_1 - \alpha_3)(\alpha_2 - \alpha_4) &\neq 0 \\ \beta_2 - \beta_3 &= (\alpha_1 - \alpha_2)(\alpha_3 - \alpha_4) \neq 0. \end{aligned}$$

Also,

$$\begin{aligned}\delta_f &= (\alpha_1-\alpha_2)(\alpha_1-\alpha_3)(\alpha_1-\alpha_4)(\alpha_2-\alpha_3)(\alpha_2-\alpha_4)(\alpha_3-\alpha_4)\\ &= (\beta_1-\beta_2)(\beta_1-\beta_3)(\beta_2-\beta_3)\\ &= \delta_g\end{aligned}$$

thus, $\Delta_f = \Delta_g$.

Suppose f is separable and let $\sigma \in \mathrm{Gal}(L_f/K)$ then σ corresponds to an element of S_4. We can check that any such element permutes the $\beta_i's$ and hence $\sigma(g) = g$ for all $\sigma \in \mathrm{Gal}(L_f/K)$ which implies that $g(x) \in K[X]$. Explicitly, writing

$$f(x) = x^4 + ax^3 + bx^2 + cx + d$$

and writing a, b, c, d in terms of the α_i we can check that

$$g(x) = x^3 - bx^2 + (ac - 4d)x + 4bd - a^2d - c^2 \in K[X].$$

Note that if $\mathrm{char}(K) \neq 2$ then one can eliminate the x^3 of $f(x)$ by transforming to $f\left(x - \frac{a}{4}\right)$. Thus, we can reduce to the case where $a = 0$ and

$$g(x) = x^3 - bx^2 - 4dx + 4bd - c^2.$$

From now on we assume that f is a monic irreducible quartic polynomial in $K[X]$ and $\mathrm{char}(K) \neq 2$ (so f is separable). Let g be the cubic resolvent of f.

The Fundamental theorem of Galois Theorem gives the surjection

$$\psi : \mathrm{Gal}(L_f/K) \subset S_4 \to \mathrm{Gal}(L_g/K).$$

We now check for $\sigma \in \mathrm{Gal}(L_f/K) \subset S_4$ we have

$$\sigma \in \ker(\psi) \iff \sigma \in V_4$$

Note 9.15. That is (1234) and (123) each send β_1 to β_3 and so are not in $\ker(\psi)$.

So $\ker(\psi) = \mathrm{Gal}(L_f/K) \cap V_4$ and the Fundamental theorem tell us that $L_g = L_f^{\mathrm{Gal}(L_f/K)\cap V_4}$.

Remark 9.16. The cases are omitted, and the summary is provided.

Proposition 9.17 (Summary)

Let K be a field of characteristic $\neq 2$ and let $f \in K[X]$ be a monic irreducible quartic polynomial (which is automatically separable since f is irreducible and $f'(x) \neq 0$). Let $g \in K[X]$ be the cubic resolvent of f. We have the following.

Criterion	Galois group of f
g is irreducible over K and Δ is a non-square in K	S_4
g is irreducible over K and Δ is square in K	A_4
g has all roots in K	V_4
$g =$ (linear)(irreducible quadratic) over K and f is irreducible over $K(\sqrt{\Delta}) = L_g$	D_4
$g =$ (linear)(irreducible quadratic) over K and f is reducible over $K(\sqrt{\Delta}) = L_g$	C_4

Note 9.18. If we know the degree $[L_f : K]$ then this determines $\mathrm{Gal}(L_f/K)$ except in the case when $[L_f : K] = 4$. But $V_4 = \langle (12)(34), (13)(24) \rangle \subset A_4$ and $C_4 \not\subset A_4$ hence, when $[L_f : K] = 4$ we get $V_4 \iff \Delta$ is a square in K.

Example 9.19

We provide examples for each of these cases.

- Let $f(x) = x^4 - x + 1 \in \mathbb{Q}[X]$, first, we need to show f is irreducible. Indeed, $x^4 - x + 1$ is irreducible in $\mathbb{Z}/2\mathbb{Z}[X]$ then by Gauss' lemma $f(x) \in \mathbb{Q}[X]$ is also irreducible. We now calculate the cubic resolvent which is given by $g(x) = x^3 - 4x - 1$ which we are irreducible since $g(1) \neq 0$ and $g(-1) \neq 0$ (since the roots must divide 1). It follows that $\mathrm{Gal}(L_f/\mathbb{Q}) \cong S_4$.
- Let $f(x) = x^4 - 6x^2 - 8x + 28 \in \mathbb{Q}[X]$. We see that f is irreducible (since it does not have a root, and it does not factorise as a product of two quadratic). Its cubic resolvent is given by $g(x) = x^3 + 6x^2 - 112x - 736$. A change of variables $g(x-2) = x^3 - 124x - 496$ then changing to $g(2x-2) = 8(x^3 - 31x - 62) = 8h(x)$ which is irreducible by Eisenstein's using $p = 31$. We find that $\Delta_h = 4^2 \cdot 31^2$ and $L_h = L_g$. Hence, $\mathrm{Gal}(L_g/\mathbb{Q}) \cong A_3$ and $\mathrm{Gal}(L_f/\mathbb{Q}) \cong A_4$.
- For p prime recall that

$$\frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Q}[X]$$

  is irreducible and has splitting field $\mathbb{Q}(\zeta_p)$ where $\zeta_p = e^{2\pi i/p}$. Take $p = 5$ then $[\mathbb{Q}(\zeta_5) : \mathbb{Q}] = 4$ and $\mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}) \cong C_4$ generated by $\sigma : \zeta_5 \mapsto \zeta_5^2$.
- We have done D_4 in a previous example for the polynomial $x^4 - 2 \in \mathbb{Q}[X]$.
- Let $f(x) = x^4 - 2x^2 + 9 = m_{\mathbb{Q},(i+\sqrt{2})}$. Its splitting field is $L_f = \mathbb{Q}(i + \sqrt{2}) = \mathbb{Q}(i, \sqrt{2})$ and $\mathrm{Gal}(L_f, \mathbb{Q}) \cong V_4$.

10 Finite fields

Let us recall that if K is a finite field then, the characteristic of K is a prime number p (i.e. K contains $\mathbb{Z}/p\mathbb{Z}$) and $|K| = p^r$ where $r = [K : \mathbb{Z}/p\mathbb{Z}]$.

Theorem 10.1

Suppose that p is a prime and r is a positive integer. Let $q = p^r$ and let $\mathbb{F}_q$ denote the splitting field over $\mathbb{Z}/p\mathbb{Z}$ of the polynomial $f(x) = x^q - x$. Then

1. $|\mathbb{F}_q| = q$;
2. if K is any field such that $|K| = q$ then $K \cong \mathbb{F}_q$;
3. $\mathbb{F}_q$ is Galois over $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ and $\mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ is a cyclic group of order r generated by the element $\phi : \mathbb{F}_q \to \mathbb{F}_q$ defined by $\phi(\alpha) = \alpha^p$.

Remark 10.2. The automorphism ϕ of $\mathbb{F}_q$ is called the **Frobenius** automorphism of $\mathbb{F}_q$. Note that for any field K of characteristic p, the formula $\phi(\alpha) = \alpha^p$ defined an $\mathbb{F}_p$-embedding $\phi : K \to K$, but it might not be an isomorphism if K is infinite. For example if $K = \mathbb{F}_p(X)$ then the image of ϕ is the subfield $\mathbb{F}_p(X^p)$.

Example 10.3

Recall that the splitting field of $x^3 - 2$ over $\mathbb{F}_7$ is a Galois extension with cyclic Galois group of order 3. From the theorem, for any prime $p \equiv 1 \pmod 3$, if $\alpha \in \mathbb{F}_p$ is not a cube in $\mathbb{F}_p$ then the Galois group of $x^2 - \alpha$ over $\mathbb{F}_p$ is cyclic of order 3 (let β be a root in a splitting field then, $\mathbb{F}_p(\beta)/\mathbb{F}_p$ is Galois, cyclic of order 3).

Corollary 10.4. If $K \subset L$ is any extension of finite fields then L is Galois over K and $\mathrm{Gal}(L/K)$ is cyclic generated by the element $\sigma : L \to L$ defined by $\sigma(\alpha) = \alpha^{|K|}$.

Corollary 10.5

Let $q = p^r$ where p is prime and $r \geq 1$. Then the polynomial $f(x) = x^q - x \in \mathbb{F}_p[X]$ is the product of all monic irreducible polynomials in $\mathbb{F}_p[X]$ of degree dividing r.

Example 10.6

Let $f(x) = x^{16} - x \in \mathbb{F}_2[X]$ we have that $p = 2$ and $r = 4$. By the Corollary above f is the product of all monic irreducible polynomials in $\mathbb{F}_2[X]$ of degree dividing 4. Polynomials of degree 1 over $\mathbb{F}_2[X]$ are x and $x + 1$. The only irreducible quadratic polynomial is $x^2 + x + 1$. Comparing degree we see there are 3 irreducible quartics:

- $x^4 + x + 1$,
- $x^4 + x^3 + 1$,
- $x^4 + x^3 + x^2 + x + 1$.

Since these have no roots in $\mathbb{F}_2$ and not equal to $(x^2 + x + 1)^2$. Therefore, f factors as

$$f(x) = x(x + 1)(x^2 + x + 1)(x^4 + x + 1)(x^4 + x^3 + 1)(x^4 + x^3 + x^2 + x + 1).$$

The roots of f are precisely the elements of $\mathbb{F}_{16}$. The product of the first three factors is $x^4 - x$ whose roots are precisely the elements of $\mathbb{F}_4$ viewed as a subfield of $\mathbb{F}_{16}$. The Galois group $\mathrm{Gal}(\mathbb{F}_{16}/\mathbb{F}_2)$ is cyclic of order 4 generated by ϕ (where $\phi(\alpha) = \alpha^2$).

Note that $\mathrm{Gal}(\mathbb{F}_{16}/\mathbb{F}_4) = \{e, \phi^2\}$.

11 Solvability by radicals

Remark 11.1. For simplicity in this section we assume the field K and hence its extensions are all of characteristic 0 unless indicated otherwise.

Definition 11.2. We say L/K is a **radical** extension (or radical over K) if $L = K(\alpha)$ for some $\alpha \in L$ such that $\alpha^n \in K$ for some $n \geq 1$.

Definition 11.3. We say L **solvable by radicals** over K if there is a finite tower of extensions

$$K = L_0 \subset L_1 \subset \cdots L_m,$$

such that $L \subset L_m$ and for each $i = 1, 2, \ldots, m$ the field L_i is a radical extension of L_{i-1}, that is $L_i = L_{i-1}(\alpha_i)$ where $\alpha_i^{n_i} \in L_{i-1}$ for some $n_i \geq 1$.

Note 11.4. Radical extensions are finite hence, so is any extension which is solvable by radicals.

Example 11.5. Every quadratic extension L/K implies $L = K(\alpha)$ for some $\alpha \in L$ such that $\alpha^2 \in K$ so, L/K is radical.

Example 11.6

Let $L = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$ is a splitting field over $\mathbb{Q}$ of $x^3 - 2$. We have that

$$\underbrace{\mathbb{Q}}_{L_0} \subset \underbrace{\mathbb{Q}(\sqrt[3]{2})}_{L_1} \subset L = L_1(e^{2\pi i/3}) = L_2.$$

Note that the tower is not unique: $\mathbb{Q}(e^{2\pi i/3})/\mathbb{Q}$ is radical, so could have taken $L_1 = \mathbb{Q}(e^{2\pi i/3})$. Also, there are choices for the elements α_i showing the extensions are radical. For instance, we could write $L_2 = L_1(\alpha_2)$ where $\alpha_2 = e^{2\pi i/3}\sqrt{2}$.

Example 11.7

We generalise the example above. Let K be any field of characteristic 0, let $a \in K, n \geq 1$ and let L be a splitting field over K of $x^n - a$. Then $L = K(\alpha_1, \ldots, \alpha_n)$ where $\alpha_i^n = a$ for $i = 1, 2, \ldots, n$. The tower of extensions:

$$K = L_0 \subset L_1 \subset \cdots L_n = L$$

with $L_i = L_0(\alpha_1, \ldots, \alpha_i) = L_{i-1}(\alpha_i)$ for $i = 1, 2, \ldots, n$ shows that L is solvable by radicals over K.

Example 11.8. Let $L = \mathbb{Q}(\alpha)$ where $\alpha = \sqrt{2} + \sqrt[5]{7 - 3\sqrt{2} + \sqrt[7]{3}}$. Then L is solvable by radicals over $\mathbb{Q}$ since we have the tower of radical extensions:

$$\underbrace{\mathbb{Q}}_{L_0} \subset \underbrace{\mathbb{Q}(\sqrt{2})}_{L_1} \subset L_1(\sqrt[7]{3}) \subset L_2\left(\sqrt[5]{7 - 3\sqrt{2}} + \sqrt[7]{3}\right).$$

Proposition 11.9

Suppose that

$$K = L_0 \subset L_1 \subset \cdots \subset L_{m-1} \subset L_m$$

is a tower of extensions such that L_i/L_{i-1} is radical for $i = 1, \ldots, m$. Then there exists a tower of extensions

$$K = L_0 \subset L_1 \subset \cdots L_m \subset L_{m+1} \subset L_{m+2} \subset \cdots L_{M-1} \subset L_M$$

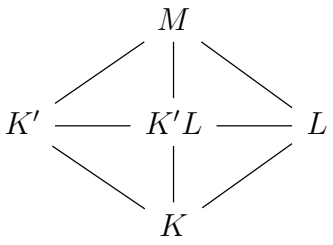
such that L_i/L_{i-1} is radical over $i = 1, \ldots, M$ and L_M is Galois over K.

Example 11.10

If $L = K(\alpha)$ where α is such that $\alpha^n \in K$ for some $n \geq 1$ then L/K is radical, but it might not be Galois. Letting $a = \alpha^n \in K$ in example 11.7 it shows that there exists a tower of radical extensions with the splitting field of $x^n - a$ over K.

Definition 11.11. Suppose M is an extension of K and $K \subset K' \subset M$ and $K \subset L \subset M$. The **composite extensions** of K' and L over K is the smallest subfield of M containing

K' and L. If L/K is finite so $L = K(\alpha_1, \ldots, \alpha_n)$ then $K'L = K'(\alpha_1, \ldots, \alpha_n)$ (notation for composite extension).



Example 11.12

In relation to the previous definition we will consider this example, where $K = \mathbb{Q}, K' = \mathbb{Q}\left(\sqrt[3]{2}\right), L = \mathbb{Q}\left(e^{2\pi i/3}, \sqrt[3]{2}\right)$ and $M = \mathbb{C}$. Then the smallest subfield of M containing K' and L is given by $K'L = \mathbb{Q}\left(\sqrt[3]{2}, e^{2\pi i/3}\sqrt[3]{2}\right) = \mathbb{Q}(\sqrt[3]{2}, e^{2\pi i/3})$.

In this example K' and L are isomorphic so there exists an embedding $\tau : K' \to M$ such that $\sqrt[3]{2} \mapsto e^{2\pi i/3}\sqrt[3]{2}$ whose image is L, and the composite $\tau(K')L = L$.

Lemma 11.13 (Extension of solvability)

We have the following.

- Suppose that M is an extension of K, and K' and L are intermediate extensions of K in M. If L is solvable by radicals over K then $K'L$ is solvable by radicals over K'.
- Suppose that $K \subset E \subset L$. Then L is solvable by radicals over K if and only if L is solvable by radicals over E and E is solvable by radicals over K.

12 Solvability

Definition 12.1. Let G be a finite group. We say that G is **solvable** if there is a chain of subgroups:

$$G = G_0 \supset G_1 \supset \cdots \supset G_{m-1} \supset G_m = \{e\}$$

such that for $i = 1, 2, \ldots, m$ G_i is a normal subgroup of G_{i-1} and G_{i-1}/G_i is cyclic.

Example 12.2. Some examples.

- Any finite cyclic group is solvable as we can take $G_1 = \{e\}$.
- The following chain of subgroups shows that S_4 is solvable:

$$S_4 \supset A_4 \supset V_4 \supset \langle (12)(34) \rangle \supset \{e\}.$$

Each subgroup is a normal subgroup of the preceding one with index 2 or 3, so each successive quotient is cyclic. This is because $S_4/A_4 \cong \mathbb{Z}/2\mathbb{Z}, A_4/V_4 \cong \mathbb{Z}/3\mathbb{Z}$ and $V_4/\langle (12)(34) \rangle \cong \mathbb{Z}/2\mathbb{Z}$.

Lemma 12.3

Let G be a finite group, and let H be a subgroup of G.

1. If G is solvable, then H is solvable.
2. Suppose that H is normal in G. we have that G is solvable if and only if H and G/H are both solvable.
3. If G is abelian then G is solvable.

Example 12.4

Let G and G' be groups, then let $H = \{e\} \times G'$. We have that H is a normal subgroup of $G \times G'$ and the quotient group $G \times G'/H \cong G$. So by part (2) of the lemma shows that $G \times G'$ is solvable if and only if G and G' are both solvable.

Example 12.5. We have that A_5 is not solvable since its only normal subgroups are $\{e\}$ and A_5 hence, by part (1) of the lemma shows that S_n is not solvable for any $n \geq 5$.

Definition 12.6. We say that a finite extension L/K is **solvable** (or that L is solvable over K) if there is a finite extension M/L such that M/K is Galois and $\mathrm{Gal}(M/K)$ is solvable.

Example 12.7

Suppose $L = K(\alpha)$ where α is a root of polynomial $f \in K[X]$ of degree at most 4. Let M be a splitting field of f over L. Then M is also a splitting field of f over K. So, (if $\mathrm{char(K)} = 0$) M/K is Galois and $\mathrm{Gal}(M/K) \hookrightarrow S_n$ for some $n \leq 4$. Thus, $\mathrm{Gal}(M/K)$ is isomorphic to some subgroup of S_4 and since S_4 is solvable it follows from part (1) of the lemma that $\mathrm{Gal}(M/K)$ is solvable, and therefore L/K is solvable.

Lemma 12.8

An extension L/K is solvable if and only if there exists a finite tower of extensions

$$K = L_0 \subset L_1 \cdots \subset L_{m-1} \subset L_m$$

such that

- $L \subset L_m$;
- L_m/K is Galois and,
- for each $1 \leq i \leq m$ L_i/L_{i-1} is Galois and $\mathrm{Gal}(L_i/L_{i-1})$ is cyclic.

Example 12.9

$\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is radical but it is not Galois. However, $M = \mathbb{Q}(\sqrt[3]{2}), e^{2\pi i/3}/\mathbb{Q}$ is Galois with $\mathrm{Gal}(M/\mathbb{Q}) \cong S_3$ which is a solvable group. Therefore, $\mathbb{Q}(\sqrt[3]{2})/\mathbb{Q}$ is solvable. A tower of extensions as is given by

$$\mathbb{Q} \subset \mathbb{Q}(e^{2\pi i/3}) \subset M$$

by the Fundamental theorem of Galois theory since

$$S_3 \supset A_3 \supset \{e\}\,.$$

Definition 12.10. Let $n \geq 1$ and $\mathrm{char}(K) \nmid n$. Denote the splitting field of $X^n - 1$ over K by L. Then $\mu_n = \{\alpha \in L : \alpha^n = 1\}$ are called the **n-th roots of unity** in L.

Remark 12.11. The set μ_n is precisely the kernel of the map $L^\times \to L^\times$ where $\beta \mapsto \beta^n$.

Definition 12.12. A **primitive n-th root of unity** in L is a generator of μ_n i.e. an element of order n in $L^\times$.

Remark 12.13. If $L \subset \mathbb{C}$ then, the primitive n-th roots of unity in L are $\left\{e^{2\pi i a/n} : \gcd(a,n) = 1\right\}$.

Proposition 12.14

Suppose that $n \geq 1$ and $\mathrm{char}(K) \nmid n$.

- Let L_1 be the splitting field of $x^n - 1$. Then $\mathrm{Gal}(L_1/K)$ is isomorphic to a subgroup of $(\mathbb{Z}/n\mathbb{Z})^\times = \{[a] \in \mathbb{Z}/n\mathbb{Z} : \gcd(a,n) = 1\}$.
- Suppose K contains a primitive n-th root of unity ζ and $a \in K^\times$. Let L_2 be a splitting field of $x^n - a$ over K. Then $\mathrm{Gal}(L_2/K)$ is isomorphic to a subgroup of $\mathbb{Z}/n\mathbb{Z}$.

Remark 12.15. Equivalently,

- we can say that $\mathrm{Gal}(L/K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^\times$.
- We can say that $\mathrm{Gal}(L/K) \hookrightarrow \mathbb{Z}/n\mathbb{Z}$.

The isomorphism rises by the first isomorphism theorem since we know that the image of the map $\mathrm{Gal}(L/K) \to \mathbb{Z}/n\mathbb{Z}$ (or the other one) is a subgroup of the respective group and the kernel is trivial.

Proposition 12.16

Suppose that $a \in K$ and let L be a splitting field of $x^n - a$ over K. Then L is a solvable extension of K. In particular, every radical extension of K is solvable.

Theorem 12.17

Suppose that $n \geq 1, \text{char}(K) \nmid n$ and $x^n - 1$ splits completely in K. Let L/K be a Galois extension with $\text{Gal}(L/K) \cong \mathbb{Z}/n\mathbb{Z}$. Then, $L = K(\alpha)$ for some α such that $\alpha^n \in K$.

Proposition 12.18

Let L and K' be extensions of K contained in M. Suppose that L/K if a finite Galois extension. Then

1. The composite extension $K'L/K'$ is Galois and there is an injective homomorphism
$$\psi : \text{Gal}(K'L/K') \to \text{Gal}(L/K)$$
$$\sigma \mapsto \sigma|_L$$
and $\text{Im}(\psi) = \text{Gal}(L/(K' \cap L))$.
2. If K'/K is Galois then $K'L/K$ is Galois and there is an injective homomorphism
$$\text{Gal}(K'L/K) \to \text{Gal}(K'/K) \times \text{Gal}(L/K)$$
$$\sigma \mapsto (\sigma|'_K, \sigma|_L).$$

Theorem 12.19

Let L/K be a finite extension and let K be a field of characteristic 0. Then L/K is solvable if and only if L/K is solvable by radicals.

Corollary 12.20. Some corollaries of the above.

- An extension L of K is solvable (or equivalently solvable by radicals) if and only if there is a finite tower of extensions
$$K = L_0 \subset L_1 \subset L_2 \subset \cdots \subset L_{m-1} \subset L_m$$
such that $L \subset L_m$, and for each $i = 1, 2, \ldots, m$, L_i is Galois over L_{i-1} and $\text{Gal}(L_i/L_{i-1})$ is cyclic.
- Suppose that $\alpha \in L$ is algebraic over K, let f be the minimal polynomial of α. Then $K(\alpha)$ is solvable (by radicals) over K if and only if $\text{Gal}(L_f/K)$ is solvable (where L_f is a splitting field of f).
- If $f \in K[X]$, $f \neq 0$ and $\deg(f) \leq 4$ then the splitting field L_f is solvable (by radicals) over K.
- If $[L : K] \leq 4$ then L is solvable (by radicals) over K.

A Language remarks

60 is divisible by 2.
2 divides 60.

B Common factorisations

Proposition B.1

Some common factorisations.

- $x^n - 1 = (x-1)(x^{n-1} + x^{n-2} + \cdots + x + 1)$.
- $x^n + 1 = (x+1)(x^{n-1} - x^{n-2} + \cdots - x + 1)$.
- $(x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$.
- $(x-y)^n = \sum_{k=0}^{n} (-1)^k \binom{n}{k} x^{n-k} y^k$.

C Binomial expansion

We have the following:

$$\begin{aligned}(x+y)^n &= \sum_{k=0}^{n} \binom{n}{k} x^{n-k} y^k = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k} \\ &= \binom{n}{0} x^n y^0 + \binom{n}{1} x^{n-1} y^1 + \binom{n}{2} x^{n-2} y^2 + \cdots + \binom{n}{n-1} x^1 y^{n-1} + \binom{n}{n} x^0 y^n,\end{aligned}$$

where

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}.$$

D Roots of unity

Definition D.1. A complex number z is said to be an **n-th root of unity** if $z^n = 1$, where n is a positive integer.

Proposition D.2

Properties of the roots of unity.

1. **Existence**: There are always n distinct n-th roots of unity, where n is a positive integer.
2. **Form**: The n-th roots of unity can be expressed in polar form as:

$$z_k = \cos\left(\frac{2\pi k}{n}\right) + i\sin\left(\frac{2\pi k}{n}\right) = e^{2\pi ik/n}$$

   where $k = 0, 1, 2, ..., n-1$.
3. **Sum**: The sum of all n-th roots of unity is zero:
4. **Product**: The product of all n-th roots of unity is 1.
5. **Conjugates**: If z_k is an n-th root of unity, then its complex conjugate $\bar{z_k}$ is also an n-th root of unity.
6. **Multiplicative Inverses**: The multiplicative inverse of an n-th root of unity z_k is z_{n-k}.
7. The roots of unity form a cyclic group of order n. The generators of which are given the elements for which $\gcd(k, n) = 1$.
8. The roots of unity for a cyclic group $C_n = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}$.

Example D.3. We want to find the fourth roots of unity, which are the solutions to the equation $z^4 = 1$.

The general form of a complex number in polar form is $re^{i\theta}$, where r is the magnitude and θ is the argument.

For the fourth roots of unity, $r = 1$ because they lie on the unit circle. The arguments θ can be calculated using the formula:

$$\theta = \frac{2\pi k}{4}$$

where $k = 0, 1, 2, 3$.

Let's calculate the roots:

1. For $k = 0$:

$$\theta_0 = \frac{2\pi \cdot 0}{4} = 0$$

   So, $z_0 = e^{i\cdot 0} = 1$.
2. For $k = 1$:

$$\theta_1 = \frac{2\pi \cdot 1}{4} = \frac{\pi}{2}$$

   So, $z_1 = e^{i\cdot\frac{\pi}{2}} = i$.

3. For $k = 2$:
$$\theta_2 = \frac{2\pi \cdot 2}{4} = \pi$$
So, $z_2 = e^{i\pi} = -1$.

4. For $k = 3$:
$$\theta_3 = \frac{2\pi \cdot 3}{4} = \frac{3\pi}{2}$$
So, $z_3 = e^{i \cdot \frac{3\pi}{2}} = -i$.

Therefore, the fourth roots of unity are 1, i, -1, and $-i$. These are evenly spaced around the unit circle in the complex plane.