Notes on Galois Theory

Apiros3

First Version : Mar 19, 2025
Last Update : Jan 29, 2025

Contents

1 Introduction

TODO: orbit stabiliser, structure theorem for finitely generated abelian groups

Lemma 1.0.1. *A finite commutative group G is cyclic if and only if for any $d|\#G$, there is at most one subgroup in G with cardinality $\#G$.*

Proof. In the infinite case, we use the fact $G \simeq \mathbb{Z}$. □

Lemma 1.0.2. *Let G be a finite cyclic group. Let $k := \#G$. Define $I : (\mathbb{Z}/k\mathbb{Z})^* \to \mathrm{Aut}_{\mathrm{Groups}}(G)$ by $a \mapsto (\gamma \mapsto \gamma^a)$. Then I is an isomorphism.*

Proof. Note first that this is well defined as $\gamma^k = e$ for any $\gamma \in G$. Also,

$$I([a][b])(\gamma) = \gamma^{ab} = I([a])(\gamma^b) = (I([a]) \circ I([b]))(\gamma)$$

thus is a homomorphism.

Take any $\psi \in \mathrm{Aut}_{\mathrm{Groups}}(G)$. If g is the generator for G, $\psi(g) = g^a$ must also be a generator, with $\gcd(a, k) = 1$. In particular, $I([a]) = \psi$, thus I is surjective.

Suppose $I([a])$ is the identity automorphism. In particular, $g^a = g$ for a generator g. As G is cyclic, this forces $a = 1 \bmod k$. In particular, $[a] = [1]$. □

Definition 1.0.3. *A group G is **simple** if it has no nontrivial normal subgroups.*

Definition 1.0.4. *A subgroup G of S_n is called **transitive** if it has only one orbit in $\{1, \dots, n\}$.*

1.1 Solvable Group

Definition 1.1.1. *Let G be a group. A **finite filtration** of G is a finite ascending sequence $G_\bullet$ of subgroups*

$$0 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_n = G$$

such that G_i is normal in G_{i+1} for all $i \in \{0, \dots, n-1\}$.

*The number n is called the **length** of the finite filtration. The finite filtration $G_\bullet$ is said to have **no redundacies** if $G_i \neq G_{i+1}$ for all $i \in \{0, \dots, n-1\}$. It is said to have **abelian quotients** if the quotient group G_{i+1}/G_i is an abelian group for all $i \in \{0, \dots, n-1\}$.*

*The finite filtration $G_\bullet$ is **trivial** if $n = 1$.*

Note that the trivial filtration always exists and is unique.

Definition 1.1.2. *A group is **solvable** if there exists a finite filtration with abelian quotients on G.*

Lemma 1.1.3 (Solvability via restriction and quotient)**.** *Let G be a group and let H be a subgroup. Then H is solvable. If H is normal in G, then the quotient group G/H is also solvable.*

Proof. Let $G_\bullet$ be a finite filtration with abelian quotients on G. Let n be the length of this filtration. We first claim that $H \cap G_i$ is normal in $H \cap G_{i+1}$. In particular, for any $h \in H \cap G_{i+1}$, the automorphism $\gamma \mapsto h^{-1}\gamma h$ of G_{i+1} sends H into H and G_i into G_i, thus sends $H \cap G_i$ into $H \cap G_i$. In particular,

$$0 = G_0 \cap H \subseteq G_1 \cap H \subseteq \cdots \subseteq G_n \cap H = H$$

is a finite filtration of H. Furthermore, we have an injective map of groups

$$\phi : G_{i+1} \cap H/G_i \cap H \hookrightarrow G_{i+1}/G_i$$

given by $[\gamma]_{G_i \cap H} \mapsto [\gamma]_{G_i}$. Thus this gives a finite filtration with abelian quotients for H. In particular, H is solvable.

Suppose now that H is normal. Consider the ascending sequence of subgroups

$$0 = [G_0]_H \subseteq [G_1]_H \subseteq \cdots \subseteq [G_n]_H = G/H$$

of G/H. Using the fact $[\bullet]_H : G \to G/H$ is a morphism of groups, taking $\gamma \in G_{i+1}$ and $\tau \in G_i$, we have

$$[\gamma]_H^{-1}[\tau]_H[\gamma]_H = [\gamma^{-1}\tau\gamma]_H$$

we have $[\gamma]_H^{-1}[\tau]_H[\gamma]_H \in [G_i]_H$, as $\gamma^{-1}\tau\gamma \in G_i$. In particular, $[G_\bullet]_H$ is a finite filtration of G/H.

Also, we have a surjection of groups

$$\mu : G_{i+1}/G_i \to [G_{i+1}]_H/[G_i]_H$$

such that for any $\gamma \in G_{i+1}$, we have

$$\mu([\gamma]_{G_i}) = [[\gamma]_H]_{[G_i]_H}$$

Noting that we are mapping surjectively from a abelian group, the target is also abelian. In particular $[G_\bullet]_H$ is a finite filtration with abelian quotients for G/H. □

Lemma 1.1.4 (Solvability via inflation)**.** *Let G be a group and $H \subseteq G$ be a normal subgroup. If H is solvable and G/H is solvable, then G is solvable.*

Proof. As H is solvable, we have a finite filtration

$$0 = H_0 \subseteq \cdots \subseteq H_n = H$$

with abelian quotients. Similarly, we G/H is solvable, we have a finite filtration of abelian quotients

$$0 = [G_0]_H \subseteq \cdots \subseteq [G_m]_H = G/H$$

Let $\phi : G \to G/H$ be the standard quotient map. Consider,

$$H = \phi^{-1}([G_0]_H) \subseteq \cdots \subseteq \phi^{-1}([G_m]_H) = G$$

For $i \in \{0, \dots, m-1\}$, $\phi^{-1}([G_i]_H)$ is normal in $\phi^{-1}([G_{i+1}]_H)$. By the third isomorphism theorem, we have

$$\phi^{-1}([G_i]_H)/\phi^{-1}([G_{i+1}]_H) \simeq [G_i]_H/[G_{i+1}]_H$$

Thus by gluing the two finite filtrations,

$$0 = H_0 \subseteq \cdots \subseteq H_n = H = \phi^{-1}([G_0]_H) \subseteq \cdots \subseteq \phi^{-1}([G_m]_H) = G$$

gives a finite filtration of abelian quotients in G. □

Proposition 1.1.5. *Let G be a finite group and let p be a prime number. Suppose there is an $n \geq 0$ such that $\#G = p^n$. Then G is solvable.*

Such groups are called p-groups.

Proof. We proceed by induction on n. For $n = 0$, the proposition clearly holds.

Let $\phi : G \to \mathrm{Aut}_{\mathrm{Groups}}(G)$ be the map of groups such that $\phi(g)(h) = ghg^{-1}$. This gives an action of G on G via conjugation. By the orbit stabiliser theorem, and Lagrange's theorem, the orbits of G in G all have a cardinality a power of p. The orbit of the unit element of G is $\{1_G\}$, and as the orbits partition G, we have $g_0 \in G$ with $g_0 \neq 1_G$ such that g_0 is a fixed point of the action of G on G. Now, $g_0 g = (gg_0g^{-1})g = gg_0$, so $g?0$ commutes with every element of G. In particular, $g_0 \in Z(G)$ is nontrivial. By definition, $Z(G)$ is abelian thus solvable, and $G/Z(G)$ has cardinality p^k for $k < n$, and thus solvable by the inductive hypothesis. Thus, by Lemma 1.1.4, G is solvable. $\square$

Definition 1.1.6. *The **length** of a finite group* $\mathrm{length}(G)$ *is*

$$\sup\{n \in \mathbb{N} \mid n \textit{ is the length of a finite filtration with no redundancies of } G\}$$

This is well-defined as the length of a finite group is finite, as it cannot be larger than $\#G$.

Lemma 1.1.7. *Suppose that G is a finite solvable group and let $G_\bullet$ is a finite filtration with no redundancies of length length(G) on G. Then for all $i \in \{0, \dots, \mathrm{length}(G) - 1\}$, the group G_{i+1}/G_i is a cyclic group of prime order.*

Proof. Let $n := \mathrm{length}(G)$. Suppose there exists an i_0 such that G_{i_0+1}/G_{i_0} is not cyclic of prime order. Then, noting G_{i_0+1}/G_{i_0} is solvable, if it is not abelian, it has some nontrivial proper normal subgroup. If it is abelian but not of prime order, by the structure theorem for finitely generated abelian groups, G_{i_0+1}/G_{i_0} is isomorphic to a finite direct sum of cyclic groups each with order a power of a prime number, giving us a nontrivial subgroup.

Call such a subgroup H. Let $q : G_{i_0+1} \to G_{i_0+1}/G_{i_0}$ be the quotient map. Consider the ascending sequence of subgroups

$$0 = G_0 \subseteq G_1 \subseteq \cdots \subseteq G_{i_0} \subseteq q^{-1}(H) \subseteq G_{i_0+1} \subseteq \cdots \subseteq G_n = G$$

There are no redundancies as H is nontrivial and proper. Note first that $G_{i_0} \triangleleft q^{-1}(H)$ is immediate. We have $q^{-1}(H) \triangleleft G_{i_0+1}$ as it is the kernel of the map

$$G_{i_0+1} \to G_{i_0+1}/G_{i_0} \to (G_{i_0+1}/G_{i_0})/H$$

This gives a longer filtration, contradicting the maximality of n, and in particular every quotient has prime order. $\square$

Remark 1.1.8. If G is a finite group and $G_\#$ is a finite filtration with no redundancies, then we can prove similarly that for the longest sequence, G_{i+1}/G_i is a nonzero simple group (intuitively, if we can pick a nontrivial normal subgroup, we can always extend the sequence).

Example 1.1.9. We note the following facts.

- Abelian groups are solvable (trivially)
- S_3 is solvable. The ascending sequence $0 \subseteq A_3 \subseteq S_3$ is a finite filtration of S_3, with quotients $A_3/0 \simeq \mathbb{Z}/3\mathbb{Z}$ and $S_3/A_3 \simeq \mathbb{Z}/2\mathbb{Z}$.
- The group S_4 is also solvable ($0 \subseteq V_4 \subseteq A_4 \subseteq S_4$).
- A_5 is not solvable, as it is simple but non-abelian. Consequently, any group which contains A_5 as a subgroup is not solvable. In particular, S_n for $n \geq 5$ is not solvable (as $A_5 \leq S_5 \leq S_n$).

2 Properties about Commutative Rings

Definition 2.0.1. *For any ring R, there is a unique ring map (homomorphism) $\phi : \mathbb{Z} \to R$ such that*

$$\phi(n) = \overbrace{1 + \cdots + 1}^{n \text{ times}}$$

*Define the **characteristic** written $\operatorname{char}(R)$ to be the unique $r \geq 0$ such that $(r) = \ker(\phi)$*

Note that if R is a domain, then $\operatorname{char}(R)$ is either 0 or a prime number.

2.1 Fields

Proposition 2.1.1. *Let R be a domain. Then there is a field F and an injective ring map $\phi : R \to F$ such that if*

$$\phi : R \to F_1$$

is a ring map into a field F_1, then there is a unique ring map $\lambda : F \to F_1$ such that $\phi_1 = \lambda \circ \phi$.

Proof. TODO!! □

Definition 2.1.2. *As a consequence of the above proposition, F is determined uniquely up to isomorphism. We call F the **field of fractions**, and write* $\operatorname{Frac}(F)$.

Note that $\operatorname{Frac}(R) = R_{R \setminus \{0\}}$

Lemma 2.1.3. *Let K be a field and $I \subseteq K$ be an ideal. Then $I = (0)$ or $I = K$.*

Proof. Immediate (any non-zero element has an inverse, thus generates K). □

Lemma 2.1.4. *Let K, L be fields and $\phi : K \to L$ be a ring map. Then ϕ is injective.*

Proof. Consider the kernel of ϕ. This is an ideal, thus is either (0) or K. In the former ϕ is injective (by the First Isomorphism Theorem), in the latter K and L are both zero-rings, so it follows. □

2.2 Polynomial Rings

Definition 2.2.1. *Let R be a ring. Write $R[x]$ to be the ring of polynomials in the variable x and coefficients in R (with standard operations). If $r \geq 0$ is an integer, $K[x_1, \ldots, x_r] := K$ if $r = 0$ and*

$$K[x_1, \ldots, x_r] := K[x_1][x_2] \ldots [x_r]$$

*Given $P(x) = a_d x^d + \cdots + a_1 x + a_0 \in R[x]$ with $a_d \neq 0$, $P(x)$ is **monic** if $a_d = 1$ (and $\deg(0) = -\infty$). We define the **degree** of $P(x)$ written $\deg(P) := d$.*

*An element $t \in R$ is a **root** of $P(x)$ if $P(t) = 0$.*

Lemma 2.2.2. *If R is a domain, then $R[x]$ is also a domain.*

Proof. TODO!!! □

Proposition 2.2.3. *If K is a field, $K[x]$ is a euclidian domain.*

Proof. TODO!! □

Consequently, $K[x]$ is a PID.

Definition 2.2.4. *A **unique factorization domain** (UFD) is a domain R such that for any $r \in R\backslash\{0\}$, there is a sequence $r_1, \ldots, r_k \in R$ such that*

1. *r_i is irreducible for all i*
2. *$(r) = (r_1 \cdots r_k)$*
3. *if $r'_1, \ldots, r'_{k'}$ is another such sequence with the above properties, $k = k'$ and there is a permutation $\sigma \in S_n$ such that $(r_i) = (r'_{\sigma(i)})$ for all $i \in \{1, \ldots, k\}$*

Proposition 2.2.5. *Any PID is a UFD.*

Definition 2.2.6. *Write* $\gcd(P_1, \ldots, P_k)$ *for the unique monic generator of the ideal $(P_1(x), \ldots, P_k(x))$.*

Lemma 2.2.7. *Suppose that R is a UFD. An element $f \in R\backslash\{0\}$ is irreducible if and only if (f) is a prime ideal.*

Proof. The forward direction is immediate, noting that if $f|p_1p_2$, $f|p_1$ or $f|p_2$, from the fact that f is irreducible and p_1, p_2 can be split into irreducible components.

On the other hand, if (f) is a prime ideal and f is not irreducible, then $f = f_1f_2$ for some non-units. But as f is prime, $f|f_1$ or $f|f_2$. Without loss of generality, taking $f|f_1$, we have $f_1f_2|f_1$, meaning f_2 is a unit, a contradiction. □

Lemma 2.2.8. *Let R be a PID. Let $I \triangleleft R$ be a nonzero prime ideal. Then I is a maximal ideal.*

Proof. Suppose not. Then we can find an element $r \in R$ such that $r \notin I$ and $([r]_I)$ is not R/I. Also, $([r]_I) = [(r, I)]_I$, and $(r, I) \neq R$ and $I \subsetneq (r, I)$. As we are in a PID, we can find $g, h \in R$ such that $(g) = (r, I)$ and $(h) = I$. Then, $g|h$ but $h \not| g$ (thus h is reducible). But h is irreducible as I is prime and R is a UFD, a contradiction. □

Proposition 2.2.9. *Let K be a field and $f \in K[x], a \in K$. Then,*

1. *a is a root of f if and only if $(x - a)|f$*
2. *there is a polynomial $g \in K[x]$ with no roots and a decomposition*

$$f(x) = g(x) \prod_{i=1}^{k} (x - a_i)^{m_i}$$

where $k \geq 0$ and $m_i \geq 1$ and $a_i \in K$.

Proof. Immediate. For the forward case in (i), we use euclidian division on $(x - a)$ and show the remainder is 0. □

Proposition 2.2.10 (Eisenstein Criterion)**.** *Let*

$$f = x^d + \sum_{i=1}^{d-1} a_i x^k \in \mathbb{Z}[x]$$

Let $p > 0$ be a prime number. Suppose $p|a_i$ and $p^2 \not| a_0$. Then f is irreducible in $\mathbb{Z}[x]$.

Proof. Sketch. The idea is that viewing this polynomial in $\mathbb{F}_p[x]$ gives x^d, and we show that if this is reducible, they are x^n and x^{d-n} in the same field. This contradicts with the assumption $p|a_0$. (Need some algebraic manipulation to show the first statement) $\square$

Lemma 2.2.11. *Let $f \in \mathbb{Z}[x]$ be monic. Let $p > 0$ and $f \pmod p \in \mathbb{F}_p[x]$ is irreducible. Then f is irreducible in $\mathbb{Z}[x]$.*

Proof. TODO!!! $\square$

Lemma 2.2.12 (Gauss Lemma)**.** *Let $f \in \mathbb{Z}[x]$. Then f is irreducible in $\mathbb{Z}[x]$ if and only if it is irreducible in $\mathbb{Q}[x]$.*

Proof. TODO!! $\square$

2.3 Action of Groups on Rings

Definition 2.3.1. *Let S be a set and G be a group. Write $\mathrm{Aut}_{\mathrm{Sets}}(S)$ for the group of bijective maps $a : S \to S$ (where the group operator works by composition). An **action** of G on S is a group homomorphism*

$$\phi : G \to \mathrm{Aut}_{\mathrm{Sets}}(S)$$

Notation 2.3.2. Given $\gamma \in G$ and $s \in S$, we write

$$\gamma(s) := \phi(\gamma)(s)$$

or γs for $\gamma(s)$.

Definition 2.3.3. *The set of invariants of S under the action of G is written*

$$S^G := \{s \in S \mid \gamma(s) = s \ \forall \gamma \in G\}$$

If $s \in S$,

$$\mathrm{Orb}(G, s) := \{\gamma(s) \mid \gamma \in G\}$$

*is the **orbit** of s under G, and*

$$\mathrm{Stab}(G, s) := \{\gamma \in G \mid \gamma(s) = s\}$$

*is the **stabiliser** of s. We omit G when it is clear.*

Definition 2.3.4. *The action of G on a ring R is **compatible** with the ring structure of R, or G acts on a ring R if the image of ϕ lies in the subgroup*

$$\mathrm{Aut}_{\mathrm{Rings}}(R) \subseteq \mathrm{Aut}_{\mathrm{Sets}}(R)$$

where $\mathrm{Aut}_{\mathrm{Rings}}(R)$ is the group of bijective maps $R \to R$ which respects the ring structure.

Intuitively, each group element is mapped to a endomorphism which has some structure.

Lemma 2.3.5. *Let G act on a ring R.*

1. *R^G is a subring of R.*
2. *If R is a field, R^G is a field.*

Proof. The first case is immediate by noting $\gamma(ab) = \gamma(a)\gamma(b) = ab$ and $\gamma(a+b) = \gamma(a)+\gamma(b) = a+b$. The second follows from the fact that $1 = \gamma(aa^{-1}) = \gamma(a)\gamma(a^{-1}) = a\gamma(a^{-1})$. $\square$

Definition 2.3.6. *Let R be a ring and $n \geq 1$. There is a natural action of S_n on the ring $R[x_1, \dots, x_n]$ by*

$$\sigma(P(x_1, \dots, x_n)) = P(x_{\sigma(1)}, \dots, x_{\sigma(n)})$$

*Define a **symmetric polynomial** with coefficients in R to be an element in $R[x_1, \dots, x_n]^{S_n}$.*

Example 2.3.7. For any $k \in \{1, \dots, n\}$, the polynomial

$$s_k := \sum_{i_1 < i_2 < \cdots < i_k} \prod_{j=1}^{k} x_{i_j} \in \mathbb{Z}[x_1, \dots, x_n]$$

is symmetric. We call this the k-th elementary symmetric function (in n variables), and this satisfies

$$(x - \alpha_1)(x - \alpha_2) \cdots (x - \alpha_d) = x^d - s_1(\alpha_1, \dots, \alpha_d)x^{d-1} + \cdots + (-1)^d s_d(\alpha_1, \dots, \alpha_d)$$

Theorem 2.3.8 (Fundamental Theorem of the Theory of Symmetric Functions)**.** *Let $\phi : R[x_1, \dots, x_n] \to R[x_1, \dots, x_n]$ be the map of rings which sends x_k to s_k and constants to themselves. Then,*

1. *$R[x_1, \dots, x_n]^{S_n}$ is the image of ϕ*
2. *ϕ is injective*

Then, by the first isomorphism theorem, we have $R[x_1, \dots, x_n]^{S_n} = R[s_1, \dots, s_n]$.

Proof. For the first case, we show that every symmetric polynomial can be expressed as a polynomial in s_i. Define lexicographic ordering on monomials

$$x_1^{\alpha_1} \cdots x_n^{\alpha_n} \leq x_1^{\beta_1} \cdots x_n^{\beta_n}$$

By $\alpha_1 < \beta_1$ or $\alpha_1 = \beta_1$ and $x_2^{\alpha_2} \cdots x_n^{\alpha_n} \leq x_2^{\beta_2} \cdots x_n^{\beta_n}$. Fix any symmetric polynomial f. Let $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$ be the largest monomial in f. We need $\alpha_1 \geq \cdots \geq \alpha_n$, as any permutation of the powers must also be in f. Also, the largest monomial in $s_1^{\alpha_1-\alpha_2} s_2^{\alpha_2-\alpha_3} \cdots s_n^{\alpha_n}$ is also $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. Thus, there exists a $c \in R$ such that all monomials in $f - c \cdot s_1^{\alpha_1-\alpha_2} s_2^{\alpha_2-\alpha_3} \cdots s_n^{\alpha_n}$ are strictly smaller than $x_1^{\alpha_1} \cdots x_n^{\alpha_n}$. By repeating, we can write f as a polynomial in s_i.

To show (ii), we can show that s_i are algebraicly independent, and therefore that the kernel is 0. TODO!!! $\square$

Definition 2.3.9. *Define,*

1. $\Delta(x_1, \dots, x_n) := \prod_{i<j}(x_i - x_j)^2 \in \mathbb{Z}[x_1, \dots, x_n]^{S_n}$
2. $\delta(x_1, \dots, x_n) := \prod_{i<j}(x_i - x_j) \in \mathbb{Z}[x_1, \dots, x_n]^{A_n}$
3. *If $\sigma \in S_n$, $\delta(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \operatorname{sign}(\sigma) \cdot \delta(x_1, \dots, x_n)$.*

where $\operatorname{sign} : S_n \to \{-1, 1\}$ *gives the **sign** of the permutation, and $A_n := \ker(sign)$ is called the **alternating group**. We call $\Delta(x_1, \dots, x_n)$ the **discriminant**.*

Note the third point follows from the fact that any permutation can be written as a product of transpositions, and $\operatorname{sign}(\sigma) = -1$ if σ is a transposition. The $\in$ in the second point follows from this.

3 Field Extensions

3.1 Field extension

Definition 3.1.1. *Let K be a field. A **field extension** of K, or K-extension is an injection*

$$K \hookrightarrow M$$

of fields. This injection gives M the structure of a K-vector space. We write $M|K$ for the field extension of K to M.

A map from the K extension $M|K$ to $M'|K$ is a ring map $M \to M'$ that is compatible with the injections $K \hookrightarrow M$ and $K \hookrightarrow M'$. Alternatively, it is a map that makes the following commute.

$$\begin{tikzcd} K \arrow[d, hook] \arrow[dr, hook] & \\ M \arrow[r] & M' \end{tikzcd}$$

Given $M|K$ is a field extension, we write $\mathrm{Aut_K}(M)$ for the group of bijective maps of K-extensions from M to M, where the group law is the composition of maps. This is the subgroup of $\mathrm{Aut_{Rings}}(M)$ which are compatible with the K-extension structure of M. We say that the field extension is **finite** if $\dim_K(M) < \infty$.

If M is a finite extension of K, then by rank nullity, any ring map from M to M is a bijection.

Example 3.1.2. If M is not a finite extension of K, then endomorphisms on M need not be bijective. Consider $\phi : \mathbb{Q}(t) \to \mathbb{Q}(t)$ which sends $t \mapsto t^2$. Consequently, $\dim_M(M)$ need not be 1, depending on the structure of the extension.

Proposition 3.1.3 (Tower Law)**.** *If $L|M$ and $M|K$ are finite field extensions, we have*

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

Specificaly, if $m_1, \ldots, m_s$ is a basis of M as a K-vector space and $l_1, \ldots, l_t$ is a basis of L as a M vector space, (as vector spaces induced by the field extensions), then $\{m_i l_j\}$ is a basis for L as a K-vector space (as the composition of extensions).

Proof. TODO!!! □

Definition 3.1.4. *Let $M|K$ be a field extension and $a \in M$. Define*

$$\mathrm{Ann}(a) := \{P(x) \in K[x] \mid P(a) = 0\}$$

We have $\mathrm{Ann}(a) \subseteq K[x]$ is an ideal.

*We say that a is **transcendental** over K if $\mathrm{Ann}(a) = (0)$ and **algebraic** if $\mathrm{Ann}(a) \neq (0)$. If a is algebraic over K, then the **minimal polynomial** m_a is the unique monic polynomial that generates $\mathrm{Ann}(a)$.*

Alternatively the annihalator is the kernel of the map from $K[x]$ to L.

$$\begin{tikzcd} K \arrow[d] \arrow[dr, hook, "\phi"] & \\ K[x] \arrow[r, "e_a"'] & M \end{tikzcd}$$

Consequently, there is a injection $K[x]/\mathrm{Ann}(a) \hookrightarrow M$ where M is a domain. Thus, $\mathrm{Ann}(a)$ is prime. If a is algebraic over K, m_a is irreducible (as (m_a) is a prime ideal in a UFD). Thus a monic irreducible polynomial that annihalates a is the minimal polynomial. Prime ideals in a PID are maximal, so $\mathrm{Ann}(a)$ is maximal.

Definition 3.1.5. *We say that a field extension $M|K$ is **algebraic** if for all $m \in M$, the element m is algebraic over K. Else, we say that the field extension is **transcendental**.*

Lemma 3.1.6. *If $M|K$ is finite, then $M|K$ is algebraic.*

Proof. Let $m \in M$. If m is transcendental over K, there is an injection of a K-vector space $K[x] \hookrightarrow M$. $K[x]$ is infinite dimensional, but this contradicts the fact M is a finite-dimensional vector space over K. □

3.2 Separability

Let K be a field. Let $P(x) \in K[x]$, and suppose

$$P(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$$

Define $P'(x) = \frac{\mathrm{d}}{\mathrm{dx}}P(x) := da_d x^{d-1} + (d-1)a_{d-1}x^{d-2} + \cdots + a_1$, where $d - i$ is $1_K + \cdots + 1_K$ $(d-i)$-times. This is a K-linear map from $K[x]$ to $K[x]$ and satisfies

$$\frac{\mathrm{d}}{\mathrm{dx}}(P(x)Q(x)) = \frac{\mathrm{d}}{\mathrm{dx}}(P(x))Q(x) + P(x)\frac{\mathrm{d}}{\mathrm{dx}}(Q(x))$$

Definition 3.2.1. *$P(x)$ has **multiple roots** if $(P(x), P'(x)) = (1)$. Equivalently, we have that $\gcd(P(x), P'(x)) = 1$ (by Bézout's Lemma).*

Given

$$P(x) = (x - \rho_1)(x - \rho_2)\cdots(x - \rho_d)$$

we see that $P(x)$ has multiple roots if and only if there are $i \neq j$ such that $\rho_i = \rho_j$.

Lemma 3.2.2. *Let $L|K$ be a field extension, $P(x), Q(x) \in K[x]$. Write $\gcd_L(P(x), Q(x))$ for the greatest common divisor of $P(x)$ and $Q(x)$ viewed as polynomials with coefficients in L. Then,*

$$\gcd(P(x), Q(x)) = \gcd_L(P(x), Q(x))$$

Proof. We use the fact that a generator of $(P(x), Q(x))$ can be computed using Euclidian division. We note that the sequence in which we get this by euclidian algorithm is unique and is invariant of the field. □

In particular, the definition of multiple roots captures roots that may not yet be in the base field.

Remark 3.2.3. Let K be a field and $P(x) \in K[x]$. Let $L|K$ be a field extension. Then, $P(x)$ has multiple roots as a polynomial with coefficients in K if and only if it has multiple roots as a polynomial with coefficients in L.

Lemma 3.2.4. *Let $P(x), Q(x) \in K[x]$ and suppose $Q(x)|P(x)$. If $P(x)$ has no multiple roots, $Q(x)$ also has no multiple roots.*

Proof. Let $T(x) \in K[x]$ be such that $Q(x)T(x) = P(x)$. By the Leibniz rule,

$$(P, P') = (QT, Q'T + QT')$$

If Q and Q' were both divisible by some polynomial W with positive degree, it also divides $Q'T+QT'$ and QT, thus 1 would be divisible by W, a contradiction. □

Lemma 3.2.5. *Suppose that K is a field and that $P(x) \in K[x]\backslash\{0\}$. Suppose that* $\mathrm{char}(K)$ *does not divide* $\deg(P)$ *and that $P(x)$ is irreducible. Then $(P, P') = (1)$.*

Proof. Let

$$P(x) = a_d x^d + a_{d-1}x^{d-1} + \cdots + a_0$$

where $a_d \neq 0$. First note that $d = 0_K$ in K as $\mathrm{char}(K)$ does not divide d. Thus, $P'(x) \neq 0$. As P is irreducible, any common divisor of P and P' is a non-zero constant or P times a non zero constant. It is not the latter as $\deg(P') < \deg(P)$. Thus, it must be a non-zero constant. In other words, $(P, P') = (1)$. □

Noting the proof, if $P' \neq 0$, and P is irreducible, the same result follows.

Definition 3.2.6. *Let K be a field. We say that $P(x) \in K[x]\backslash\{0\}$ is **separable** if all the irreducible factors of $P(x)$ have no multiple roots.*

Note that by Remark 3.2.3 and Lemma 3.2.4, this notion is invariant under field extensions. Also, by Lemma 3.2.5, irreducible polynomials with coefficients in K whose degree is prime to the characteristic of K is separable. Specificaly, if $\mathrm{char}(K) = 0$, any irreducible polynomial with coefficients in K is separable.

Definition 3.2.7. *Let $L|K$ be an algebraic field extension. We say that $L|K$ is **separable** if the minimal polynomial over K of any element of L is separable.*

Noting the previous paragraph, if K is a field and $\mathrm{char}(K) = 0$, all algebraic extensions of K are separable (noting that minimal polynomials are irreducible in $K[x]$).

Lemma 3.2.8. *Let $M|L$ and $L|K$ be algebraic field extensions. Suppose $M|K$ is separable. Then, $M|L$ and $L|K$ are both separable.*

Proof. By definition, $L|K$ is separable. Let $m \in M$ and let $P(x) \in K[x]$ be the minimal polynomial over K. Let $Q(x)$ be the minimal polynomial of m over L. By assumption, $Q(x)|P(x)$. By assumption, $P(x)$ has no multiple roots over K thus also over L by Remark 3.2.3. By Lemma 3.2.4, $Q(x)$ also has no multiple roots over L, thus is separable. □

Lemma 3.2.9 (MOVE LATER)**.** *Let $M|L$ and $L|K$ be finite separale extensions. Then $M|K$ is separable.*

Proof. Consider the following commutative diagram of extensions:

$$\begin{tikzcd} & L' \arrow[r] & M' \\ K \arrow[r] & L \arrow[r] \arrow[u] & M \arrow[u] \end{tikzcd}$$

where L' is the normal closure of L over K such that $L'|K$ is Galois, and M' is the smallest field containing M and L'. Then note that $L'|K$ is separable (as it is Galois), and by using the fact that

$L'|L$ is separable, $M'|L$ is also separable. Thus, $M'|L'$ is separable. Thus, we may reduce to the case where $L'|K$ is a Galois extension and take $L := L'$, $M := M'$.

Let $\alpha \in M$ be a root of an irreducible polynomial $f \in L[t]$. By assumption, this is separable. Now let $G := \mathrm{Gal}(L|K)$. For each $\sigma \in G$, we have

$$f^{\sigma}(t) = \sigma(f(t)) = \sum_i \sigma(a_i) t^i$$

This is also irreducible and separable. Taking

$$g(t) = \prod_{\sigma \in G} f^{\sigma}(t)$$

we see that $g \in K[t]$ and is also separable as each f^{σ} is separable. Any minimum polynomial of α in K divides g, so in particular is separable. Thus $M|K$ is separable. □

Example 3.2.10. Finite extensions need not be separable. Noting the proof in Lemma 3.2.5, we at least want to find a polynomial P such that $P' = 0$.

Consider $K := \mathbb{F}_2(t)$ where $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Let $P(x) := x^2 - t$. As $P(x)$ is of degree 2 and has no roots in K (by considering degrees), it is irreducible.

Define $L := K[x]/(P(x))$. As $P(x)$ is irreducible, $(P(x))$ is prime, thus maximal in $K[x]$, meaning L is a field. However, $P'(x) = 0$, thus $(P', P) = (P) \neq (1)$. As $P(x)$ is the minimal polynomial of $x \in L$, $L|K$ is not separable.

Example 3.2.11. Let p be a prime and take $f \in \mathbb{F}_p(t)$. Write

$$f(t) = \sum_{i=0}^{n} a_i t^i$$

where $a_i \in \mathbb{F}_p$. Then, $D(f)(t) = \sum_{i=1}^{n} i a_i t^{i-1}$ By characteristic, this vanishes if and only if $p | i a_i$ for all i, which is equivalent to $a_i = 0$ whenever $p \not| i$. Hence the only possible nonzero terms in f are those with exponent a multiple of p, so

$$f(t) = \sum_j a_{pj} t^{pj} = \sum_j a_{pj} (t^p)^j = g(t^p)$$

Suppose now that the map $x \mapsto x^p$ is bijective (such fields are called perfect). Then, writing $f(t) = g(t^p)$, we can take $g(t^p) = \sum_{j=0}^{m} b_j t^{pj}$ and picking j such that $c_j^p = b_j$, we have

$$g(t^p) = \sum_j (c_j)^p u^{pj} = \left(\sum_j c_j u^j \right)^p = h(u)^p$$

where $h(u) = \sum_j c_j u^j$. In particular, $f(t) = h(t)^p$. But then f is not irreducible. Thus, if f is irreducible and $\mathbb{F}_p$ is perfect, $D(f) \neq 0$, meaning f is separable.

3.3 Simple Extensions

Definition 3.3.1. *Let $\iota : K \hookrightarrow M$ be a field extension and $S \subseteq M$ be a subset. Define*

$$K(S) := \bigcap_{\text{field } L, L \subseteq M, L \supseteq S, L \supseteq \iota(K)} L$$

This is a subfield of M and is called the ***field generated by S over*** *K, and the elements of S are called* ***generators*** *of $K(S)$. The field extensions $M|K$ is the composition of the natural field extensions $K(S)|K$ and $M|K(S)$.*

Note also that if $S = \{s_1, \ldots, s_k\}$, then

$$K(S) = K(s_1)\ldots(s_k)$$

We also say that $M|K$ is a **simple extension** if there is a $m \in M$ such that $M = K(m)$.

Example 3.3.2. Some examples of simple extensions:

- Let $K = \mathbb{Q}$ and $M = \mathbb{Q}(i, \sqrt(2))$ be a field generated by i and $\sqrt{2}$ in $\mathbb{C}$. Then M is a simple algebraic extension of K generated by $i + \sqrt{2}$.
- Let $M = \mathbb{Q}(x) = \mathrm{Frac}(\mathbb{Q}[x])$ and let $K = \mathbb{Q}$. Then M is a simple transcendental extension of K, generated by x.

Proposition 3.3.3. *Let $M = K(\alpha)|K$ be a simple algebraic extension. Let $P(x)$ be the minimal polynomial of α over K. Then, there is a natural isomorphism of K-extensions*

$$K[x]/(P(x)) \simeq M$$

which sends x to α.

Proof. We first note that there is a natural map from $K[x]/(P(x))$ to M by evaluation. As $P(x) \neq 0$, we have $(P(x))$ is a maximal ideal. Thus, the image of $K[x]/(P(x))$ in M is a field. By definition, this is the entirety of M. □

Remark 3.3.4. Noting the above proposition, we can note that $[M : K] = \deg(P)$. Then, the set $\{1, x, \ldots, x^{\deg(P)-1}\}$ is a basis. Also as a consequence, a finitely generated algebraic extension is a finite extension.

Corollary 3.3.5. *Let $M = K(\alpha)|K$ be a simple algebraic extension. Let $K \hookrightarrow L$ be an extension of fields. Let $P(x)$ be the minimal polynomial of α over K. There is a bijective correspondence with the roots of $P(x)$ in L and the maps of K-extensions $M \hookrightarrow L$.*

Proof. The corresponding map is given by the unique map extended from sending α to the root of $P(x)$ in L. □

Example 3.3.6. Let $M := \mathbb{Q}(i) \subseteq \mathbb{C}$ and let $K = \mathbb{Q}$, and $L = \mathbb{Q}(\sqrt{2}) \subseteq \mathbb{C}$. There is no map of K-extensions $M \hookrightarrow L$ because the roots of $x^2 + 1$ do not lie in $L \subseteq \mathbb{R}$. If we change $L = \mathbb{C}$, then there are two maps of K-extensions $M \hookrightarrow L$ corresponding to the function extended by sending $i \mapsto i$ and $i \mapsto -i$.

3.4 Splitting Fields

Definition 3.4.1. *Let K be a field. Let $P(x) \in K[x]$. We say that $P(x)$* ***splits*** *in K if for some $c \in K$ and sequence of $\{a_i \in K\}$, we have*

$$P(x) = c \cdot \prod_{i=1}^{k} (x - a_i)$$

We call a field ***algebraicly closed*** *if any polynomial with coefficients with L splits in L.*

If $P(x) \in K[x]$ is irreducible and $\deg(P) > 1$, $P(x)$ has no roots in K and thus does not split in K.

Definition 3.4.2. *A field extension $M|K$ is a* ***splitting extension*** *for $P(x) \in K[x]$ if*

1. *$P(x)$ splits in M*

2. *M is generated over K by the roots of $P(x)$ in M.*

Theorem 3.4.3. *Let $P(x) \in K[x]$. Then,*

- *There exists a field extension $M|K$ which is a splitting extension for $P(x)$*

- *If $L|K$ is a splitting extension for $P(x)$, then L and M are isomorphic as K-extensions*

- *Let $L|K$ be a splitting extension for $P(x)$ and $J|K$ be any K-extension. Then, the images of all the maps of K-extensions $L \hookrightarrow J$ coincide.*

Proof. (i) We work by induction on $\deg(P)$. If $\deg(P) = 1$, then $K|K$ is a splitting extension for $P(x)$. Suppose that $\deg(P) > 1$. Let P_1 be an irreducible factor of $P(x)$. Consider $M_1 := K[x]/(P_1(x))$. M_1 is a field, and there is a natural map of rings $K \hookrightarrow M_1$.

By definition, $P(x)$ has a root a in M_1 (which is just x in the presentation $M_1 = K[x]/(P_1(x))$). Let M be a splitting field for $P(x)/(x-a) \in M_1[x]$ over M_1, which exists by the inductive hypothesis. By construction, $P(x)$ splits in M. Let $a_2, \dots, a_k$ be roots of $P(x)/(x-a)$ in M. By Proposition 3.3.3, $M = K(a)(a_2)\dots(a_k) = K(a, a_2, \dots, a_k)$ and thus M is generated over K by roots in M. Consequently, M is a splitting field of $P(x)$ over K.

(ii) We work by induction on $\deg(P)$. If $\deg(P) = 1$, we are done. Suppose $\deg(P) > 1$. Let $a \in M$ be a root of $P(x)$ in M and $Q(x) \in K[x]$ be its minimal polynomial. As $Q(x)|P(x)$, $Q(x)$ splits in M and also in L.

Now let a_1 be a root of $Q(x)$ in L. Note from before that $M|K(a)$ is a splitting extension of $P(x)/(x-a) \in K(a)$. Similarly, $L|K(a_1)$ is a splitting extension of $P(x)/(x-a_1) \in K(a_1)$. Define $J := K[x]/(Q(x))$. This is a field as $Q(x)$ is irreducible, and there are natural isomorphisms $J \simeq K(a)$ and $J \simeq K(a_1)$ of K-extensions. Considering the J-extensions $M|J$ and $L|J$ from these isomorphisms, the inductive hypothesis shows the two are isomorphic as J extensions. By construction, this gives an isomorphism of K-extensions.

(iii) If there are no maps of K-extensions $L \hookrightarrow J$, we are done. Else, suppose there is a map $\phi : L \hookrightarrow J$ of K-extensions. As L is generated over the roots of $P(x)$, the image of ϕ are generated over K by the image of these roots in J under ϕ. We claim these images are the roots of $P(x)$ in J.

To prove the above claim, let $\alpha_1, \dots, \alpha_d$ be roots of $P(x)$ in L with multiplicities. Then,

$$P(x) = x^d - s_1(\alpha_1, \dots, \alpha_d)x^{d-1} + \dots + (-1)^d s_d(\alpha_1, \dots, \alpha_d)$$

Thus, the elements of $\phi(\alpha_1), \dots, \phi(\alpha_d)$ are the roots of

$$\begin{aligned} &x^d - s_1(\phi(\alpha_1), \dots, \phi(\alpha_d))x^{d-1} + \dots + (-1)^d s_d(\phi(\alpha_1), \dots, \phi(\alpha_d)) \\ &= x^d - \phi(s_1(\alpha_1, \dots, \alpha_d))x^{d-1} + \dots + (-1)^d \phi(s_d(\alpha_1, \dots, \alpha_d)) \\ &= P(x) \end{aligned}$$

As $P(x)$ has coefficients in K. Now the set of roots of $P(x)$ in J does not depend on ϕ, and so the claim follows. $\square$

Remark 3.4.4. Let K be a field and $P(x) \in K[x]$. Suppose that there is a field extension $K \hookrightarrow L$, where L is algebraicly closed. Let $S \subseteq L$ be the roots of $P(x) \in L$. Then $K(S) \subseteq L$ is a splitting field for $P(x)$. This follows from the fact $P(x)$ splits in $K(S)$ as L is algebraicly closed, and that $K(S)$ is generated by the roots of $P(x)$ by construction.

As a specific example, we can generate a splitting field for any polynomial in $\mathbb{Q}[x]$ by considering $L = \mathbb{C}$.

Remark 3.4.5. Any field K has an algebraic field extension $K \hookrightarrow K'$ such that K' is algebraicly closed. This is unique up to isomorphism and is called the **algebraic closure** of K.

3.5 Normal Extensions

Definition 3.5.1. *An algebraic extension $L|K$ is called* ***normal*** *if the minimal polynomial over K of any element of L splits in L.*

Note that a splitting extension (field) is by definition a normal extension (field).

Example 3.5.2. Some examples of extensions are

- $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ is not normal, as the minimal polynomial for $\sqrt[3]{2}$, namely x^3+2, does not split.
- $\mathbb{Q}(\sqrt{2})|\mathbb{Q}$ is normal, noting that as $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$, any minimal polynomial in $\mathbb{Q}(\sqrt{2})$ has degree at most 2, which if it has a root, splits.

Lemma 3.5.3. *Let $M = K(\alpha_1, \dots, \alpha_k)|K$ be an algebraic field extension. Let $J|K$ be an extension in which the polynomial $\prod_{i=1}^k m_{\alpha_i} \in K[x]$ splits. Then the set of maps of K-extensions $M \to J$ is finite and non-empty. If m_{α_i} are all separable, there are $[M : K]$ such maps.*

Proof. We first prove that this set is finite and non-empty. By Corollary 3.3.5, there is an extension of the map $K \hookrightarrow J$ to $K(\alpha_1)$, and only finitely many choices for such extension. The minimal polynomial of α_2 over $K(\alpha_1)$ divides m_{α_2} and has a root in J as m_{α_2} splits in J. Thus, again, there is an extension from the ring map $K(\alpha_1) \hookrightarrow J$ to $K(\alpha_1)(\alpha_2) = K(\alpha_1, \alpha_2) \hookrightarrow J$, and only finitely many such. Repearing shows the same is the case for $K(\alpha_1, \dots, \alpha_k) = M \hookrightarrow J$.

For the cardinality of the set, we note that there are $[K(\alpha_1) : K] = \deg(m_{\alpha_1})$ extensions of maps $K \hookrightarrow J$ to $K(\alpha_1)$. Continuting, for any ring map $K(\alpha_1) \hookrightarrow J$, there are $[K(\alpha_1, \alpha_2) : K(\alpha_1)]$ extensions of this map to a map $K(\alpha_1, \alpha_2) \hookrightarrow J$. By the tower law, there are

$$[K(\alpha_1) : K][K(\alpha_1, \alpha_2) : K(\alpha_1)] = [K(\alpha_1, \alpha_2) : K]$$

extensions of the map $K \hookrightarrow J$ to a ring map $K(\alpha_1, \alpha_2) \hookrightarrow J$. Continuting,

$$[K(\alpha_1) : K] \cdots [M : K(\alpha_1, \dots, \alpha_{k-1})] = [M : K]$$

extensions of the map $K \hookrightarrow J$ to a ring map $M \hookrightarrow J$. □

Theorem 3.5.4. *A finite field extension $L|K$ is normal if and only if it is a splitting extension for a polynomial with coefficients in K.*

Proof. ($\Rightarrow$) Suppose that $L|K$ is finite and normal. Let $\alpha_1, \dots, \alpha_k$ be generators for L over K (as a K-basis). Define

$$P(x) := \prod_{i=1}^k m_{\alpha_i}(x)$$

where $m_{\alpha_i}(x)$ is the minimal polynomial for α_i over K. Then, by assumption, $P(x)$ splits in L and the roots of $P(x)$ generate L, so L is a splitting field for $P(x)$.

($\Leftarrow$) Suppose that L is a splitting field of a polynomial in $K[x]$. Let $\alpha \in L$ and $\beta_1, \ldots, \beta_k \in L$ be such that $L = K(\alpha, \beta_1, \ldots, \beta_k)$. Let J be a splitting field of the products of the minimal polynomials over K over the elements $\alpha, \beta_1, \ldots, \beta_k$. Choose a root ρ in J of the minimal polynomial $Q(x)$ of α over K. By Corollary 3.3.5, there is an extension of the map $K \hookrightarrow J$ to a ring map $\mu : K(\alpha) \hookrightarrow J$ such that $\mu(\alpha) = \rho$. By Lemma 3.5.3, there is an extension of μ to a ring map $\lambda : L \hookrightarrow J$. By Theorem 3.4.3, the image of λ on L in J is independent of λ and thus of μ. Consequently, as we have not fixed ρ, the image of λ with L in J contains all the roots of $Q(x)$. Thus, $Q(x)$ splits in the image of λ. As $Q(x)$ has coefficients in K and λ gives an isomorphism between L and the image of λ, $Q(x)$ splits in L. □

Theorem 3.5.5. *Let $L|K$ be a splitting field of a separable polynomial over K. Then we have $\#\mathrm{Aut}_K(L) = [L : K]$.*

Proof. Apply Lemma 3.5.3 with $L = M = J$. □

Theorem 3.5.6. *Let $\iota : K \hookrightarrow L$ be a finite field extension. Then $\mathrm{Aut}_K(L)$ is finite. Furthermore, the following are equivalent :*

1. *$\iota(K) = L^{\mathrm{Aut}_K(L)}$*
2. *$L|K$ is normal and separable*
3. *$L|K$ is a splitting extension for a separable polynomial with coefficients in K.*

Proof. We first note that if $\mathrm{Aut}_K(L)$ were infinite, we can obtain infinitely many maps of K extensions $L \hookrightarrow J$ by composing any map $L \hookrightarrow J$ with elements of $\mathrm{Aut}_K(L)$, which contradicts the result from Lemma 3.5.3.

(i) $\Rightarrow$ *(ii)* Let $P(x)$ be the minimal polynomial of some element $\alpha \in L$. We have to show that $P(x)$ splits and is separable. Define

$$Q(x) := \prod_{\beta \in \mathrm{Orb}(\mathrm{Aut}_K(L), \alpha)} (x - \beta)$$

By definition, $Q(x)$ is separable. Let $d := \#\mathrm{Orb}(\mathrm{Aut}_K(L), \alpha)$. Let $\beta_1, \ldots, \beta_d$ be the elements of $\mathrm{Orb}(\mathrm{Aut}_K(L), \alpha)$. Note that

$$Q(x) = x^d - s_1(\beta_1, \ldots, \beta_d)x^{d-1} + \cdots + (-1)^d s_d(\beta_1, \ldots, \beta_d)$$

For any $\gamma \in \mathrm{Aut}_K(L)$ and for any $i \in \{1, \ldots, d\}$ we have

$$\gamma(s_i(\beta_1, \ldots, \beta_d)) = s_i(\gamma(\beta_1), \ldots, \gamma(\beta_d))$$

Noting that s_i is a symmetric function and γ permutes elements of $\mathrm{Orb}(\mathrm{Aut}_K(L), \alpha)$ (by composition), we have

$$s_i(\gamma(\beta_1), \ldots, \gamma(\beta_n)) = s_i(\beta_1, \ldots, \beta_n)$$

As γ was arbitrary, we see that $s_i(\beta_1, \ldots, \beta_d) \in L^{\mathrm{Aut}_K(L)} = \iota(K)$. Thus, $Q(x) \in \iota(K)[x]$. We can therefore identify $Q(x)$ with a polynomial in $K[x]$ with ι.

However, $\alpha \in \mathrm{Orb}(\mathrm{Aut}_K(L), \alpha)$, so $Q(\alpha) = 0$. By definition of $P(x)$, $P(x)|Q(x)$, so $P(x)$ splits in L and has no multiple roots and therefore is separable.

(ii) $\Rightarrow$ *(iii)* Let $\alpha_1, \ldots, \alpha_k$ be generators of L over K. Let $P(x) := \prod_{i=1}^{k} m_{\alpha_i}(x)$, where $m_{\alpha_i}(x)$ is the minimal polynomial of α_i over K. Then, $P(x)$ is a separable polynomial by construction and L is also a splitting extension for $P(x)$.

(iii) $\Rightarrow$ *(i)* Note first that by construction, $\iota(K) \subseteq L^{\mathrm{Aut}_K(L)}$ as any element of $\mathrm{Aut}_K(L)$ fixes the image of K in L by definition. So, $L|K$ is the composition of extensions $L^{\mathrm{Aut}_K(L)}|K$ and $L|L^{\mathrm{Aut}_K(L)}$. Note that $L|L^{\mathrm{Aut}_K(L)}$ is also the splitting field of a separable polynomial over $L^{\mathrm{Aut}_K(L)}$ (by taking the same polynomial for $L|K$). Also note the identity $\mathrm{Aut}_{L^{\mathrm{Aut}_K(L)}}(L) = \mathrm{Aut}_K(L)$

Now, by Theorem 3.5.5, we have

$$[L : L^{\mathrm{Aut}_K(L)}] = \#\mathrm{Aut}_{L^{\mathrm{Aut}_K(L)}}(L)$$

and

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

giving $[L : L^{\mathrm{Aut}_K(L)}] = [L : K]$. The tower law shows that $[L^{\mathrm{Aut}_K(L)} : K] = 1$, or equivalently, $L^{\mathrm{Aut}_K(L)} = \iota(K)$. $\square$

Corollary 3.5.7. *Let $L|K$ be an algebraic field extension. Suppose that L is generated by $\alpha_1, \ldots, \alpha_k \in L$ and the minimal polynomial of each α_i is separable. Then, $L|K$ is separable.*

Proof. By Lemma 3.5.3 and Theorem 3.4.3, there is an extension $M|L$ such that $M|K$ is the splitting field of a separable polynomial (the product of the minimal polynomials). By 3.5.6, the extension $M|K$ is separable. Thus, the extension $L|K$ is also separable. $\square$

3.6 Galois Extensions

Definition 3.6.1. *A field extension $\iota : K \hookrightarrow L$ is called a Galois extension if $L^{\mathrm{Aut}_K(L)} = \iota(K)$. As notation, $\iota(K)$ is often replaced with K (unless there is ambiguity).*

If $L|K$ is a Galois extension, write

$$\mathrm{Gal}(L|K) = \Gamma(L|K) := \mathrm{Aut}_K(L)$$

and call $\mathrm{Gal}(L|K)$ *the Galois group of $L|K$. If $L|K$ is finite, then this is a finite group (by Theorem 3.5.6).*

As a consequence of Theorem 3.5.6, a finite field extension $L|K$ is a Galois extension if and only if L is a splitting field of a separable polynomial over K if and only if it is normal and separable. As a consequence, if $L|K$ is a finite galois extension which is the composition of two extensions $L|K_1$ and $K_1|K$, then $L|K_1$ is a finite galois extension. This is because properties like normal and separable are preserved by such cuts (noting that the minimal polynomial of L over K_1 divides that over K). However, it does not hold in general that $K_1|K$ is a galois extension, noting that this need not be a normal extension.

Definition 3.6.2. *Let K be a field and $P(x) \in K[x]$ be a separable polynomial. Let $L|K$ be a splitting field for $P(x)$. We sometimes write* $\mathrm{Gal}(P) = \mathrm{Gal}(P(x))$ *for* $\mathrm{Gal}(L|K)$*. Note the abuse of notation, as splitting fields are not related by canonical isomorphism. Thus, in the strict sense,* $\mathrm{Gal}(P)$ *refers to an isomorphism class of finite groups.*

Lemma 3.6.3. *Let K be a field and let $G \subseteq \mathrm{Aut}_{\mathrm{Rings}}(K)$ be a finite subgroup. Then $[K : K^G] \leq \#G$.*

Proof. Suppose not. Then, we have a sequence $\alpha_1, \ldots, \alpha_d$ of elements of K which is linearly independent over K^G and such that $d > \#G$. Let $n := \#G$ and let $\sigma_1, \ldots, \sigma_n \in G$ be the enumeration of G. Consider now the matrix defined by $(\sigma_i(\alpha_j))$. The columns are linearly dependent over K as $n < d$. Thus, we have a sequence $\beta_1, \ldots, \beta_d$ with some non-vanishing term such that

$$\sum_{i=1}^{d} \beta_i(\sigma_k(\alpha_i))$$

for all k. Choose a sequence $\beta_1, \ldots, \beta_d$ such that

$$r := \#\{i \in \{1, \ldots, d\} \mid \beta_i \neq 0\}$$

is minimal. By reordering, suppose that $\beta_1, \ldots, \beta_r \neq 0$ and that $\beta_{r+1}, \ldots, \beta_d = 0$. Dividing through by β_r, suppose that $\beta_r = 1$. As $\alpha_1, \ldots, \alpha_d$ are linearly independent over K^G, (noting that β_i kills the identity) we have some $i_0 \in \{1, \ldots, r\}$ such that $\beta_{i_0} \notin K^G$. Note that $r > 1$ as $i_0 \neq r$. By renumbering, we may assume $\beta_1 \notin K^G$.

Now, take $k_0 \in \{1, \ldots, n\}$ such that $\sigma_{k_0}(\beta_1) \neq \beta_1$. Applying σ_{k_0} to our first equation, we get

$$\sum_{i=1}^{d} \sigma_{k_0}(\beta_i)(\sigma_{k_0}\sigma_k)(\alpha_i) = 0$$

for all $k \in \{1, \ldots, n\}$. Noting that σ only permutes, we have

$$\sum_{i=1}^{d} \sigma_{k_0}(\beta_i)(\sigma_k)(\alpha_i) = 0$$

for all $k \in \{1, \ldots, n\}$. Subtracting with the original equation, this gives

$$\sum_{i=1}^{d} (\sigma_{k_0}(\beta_i) - \beta_i)(\sigma_k)(\alpha_i) = 0$$

for all $k \in \{1, \ldots, n\}$. Noting the definition of r and from $\beta_r = 1$, we have

$$\sum_{i=1}^{r-1} (\sigma_{k_0}(\beta_i) - \beta_i)(\sigma_k)(\alpha_i) = 0$$

Now, as $\sigma_{k_0}(\beta_1) \neq \beta_1$, we have a non-zero annihlating sum, which contradicts the minimality of r. Thus $d \leq n$. $\square$

Theorem 3.6.4 (Artin's Lemma)**.** *Let K be a field and let $G \subseteq \mathrm{Aut}_{\mathrm{Rings}}(K)$ be a finite subgroup. Then the extension $K|K^G$ is a finite Galois extension, and the inclusion $G \hookrightarrow \mathrm{Aut}_{K^G}(K)$ is an isomorphism of groups.*

Proof. First we claim that

$$K^G = K^{\mathrm{Aut}_{K^G}(K)}$$

First note that $K^G \subseteq K^{\mathrm{Aut}_{K^G}(K)}$ (if you are in K^G, you are fixed by things that fix K^G). On the other hand, $G \subseteq \mathrm{Aut}_{K^G}(K)$ (automorphisms in G fix K^G). Thus, $K^G \supseteq K^{Aut_{K^G}(K)}$. Thus, we have proven the claim.

Now, as $K|K^G$ is a finite extension by Lemma 3.6.3, we have from Theorem 3.5.6 that $K|K^G$ is a splitting extension of a separable polynomial with coefficients in K^G. By Theorem 3.5.5,

$$[K : K^G] = \#\mathrm{Aut}_{K^G}(K)$$

On the other hand, from Lemma 3.6.3, $[K : K^G] \leq \#G$ so, we have $\#\mathrm{Aut}_{K^G}(K) \leq \#G$. Now, $G \subseteq \mathrm{Aut}_{K^G}(K)$ so, $\#G \leq \#\mathrm{Aut}_{K^G}(K)$, giving $\#G = \#\mathrm{Aut}_{K^G}(K)$. Thus, $G = \mathrm{Aut}_{K^G}(K)$.

Finally, Theorem 3.5.6 implies that $K|K^G$ is a finite Galois extension with Galois group G. $\square$

Theorem 3.6.5 (Fundamental Theorem of Galois Theory)**.** *(i) The map*

$$\{\textit{subfields of } L \textit{ containing } \iota(K)\} \mapsto \{\textit{subgroups of } \mathrm{Gal}(L|K)\}$$

given by

$$M \mapsto \mathrm{Gal}(L|M)$$

is a bijection. The inverse is given by the map

$$H \mapsto L^H$$

(ii) Let M be a subfield of L containing $\iota(K)$. We have

$$[L : M] = \#\mathrm{Gal}(L|M)$$

and

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

(iii) Let M be a subfield of L containing $\iota(K)$. Then $M|K$ is a Galois extension if and only if the group $\mathrm{Gal}(L|M)$ is a normal subgroup of $\mathrm{Gal}(L|K)$. In that case, there is an isomorphism $I_M : \mathrm{Gal}(L|K)/\mathrm{Gal}(L|M) \simeq \mathrm{Gal}(M|K)$.

Proof. (i) By considering the claimed isomorphisms, we want to show that $M = L^{\mathrm{Gal}(L|M)}$ and $\mathrm{Gal}(L|L^H) = H$ for any intermediate field M and any subgroup $H \subseteq \mathrm{Gal}(L|K)$.

The first equality is a consequence of the fact that $L|M$ is a Galois extension. The second follows from Artin's Lemma.

(ii) The equation $[L : M] = \#\mathrm{Gal}(L|M)$ is a consequence of Theorem 3.5.5. The equation $[M : K] = \#\mathrm{Gal}(L|K)/\#\mathrm{Gal}(L|M)$ is a consequence of the tower law and $\#\mathrm{Gal}(L|K) = [L : K]$.

(iii) Suppose that M is an intermediate field and that $M|K$ is a Galois extension. Then for any $\gamma \in \mathrm{Gal}(L|K)$, $\gamma(M) = M$ by Theorem 3.4.3 (iii). In particular, we have a homomorphism

$$\phi_M(\gamma) = \gamma|_M$$

The kernel of this homomorphism is $\mathrm{Gal}(L|M)$ by definition. Hence, $\mathrm{Gal}(L|M)$ is normal in $\mathrm{Gal}(L|K)$ by the first isomorphism theorem.

On the other hand, suppose that $\mathrm{Aut}_M(L)$ is a normal subgroup of $\mathrm{Gal}(L|K)$. Take $\gamma \in \mathrm{Gal}(L|K)$. By definitions,

$$\begin{aligned}
\mathrm{Aut}_{\gamma(M)}(L) = \mathrm{Gal}(L|\gamma(M)) &= \{\mu \in \mathrm{Gal}(L|K) \mid \mu(\alpha) = \alpha,\ \forall \alpha \in \gamma(M)\} \\
&= \{\mu \in \mathrm{Gal}(L|K) \mid \mu(\gamma(\beta)) = \gamma(\beta),\ \forall \beta \in M\} \\
&= \{\mu \in \mathrm{Gal}(L|K) \mid (\gamma^{-1}\mu\gamma)(\beta) = \beta,\ \forall \beta \in M\} \\
&= \gamma \mathrm{Gal}(L|M)\gamma^{-1} \\
&= \mathrm{Gal}(L|M)
\end{aligned}$$

By bijective correspondence given in (i), we have $M = \gamma(M)$. Thus, we have a homomorphism

$$\phi_M : \mathrm{Gal}(L|K) \to \mathrm{Aut}_K(M)$$

given by $\phi_M(\gamma) = \gamma|_M$. From (ii) and the first isomorphism theorem, $\mathrm{im}(\phi_M) \subseteq \mathrm{Aut}_K(M)$ has cardinality $[M : K]$, with kernel $\mathrm{Aut}_M(L)$. On the other hand, by Artin's Lemma, we know $[M : M^{\mathrm{Im}(\phi)}] = \#\mathrm{Im}(\phi_M)$ such that $[M : M^{\mathrm{Im}(\phi)}] = [M : K]$. By the tower law, $K = M^{\mathrm{Im}(\phi)}$. In particular, $M|K$ is a Galois extension and ϕ_M is therefore surjective.

The isomorphism is uniquely determined by the fact that $I_M(\gamma \bmod \mathrm{Gal}(L|M)) = \gamma|_M$ for any $\gamma \in \mathrm{Gal}(L|K)$. $\square$

Remark 3.6.6. Let $\iota : K \hookrightarrow L$ be a Galois extension. Let $M \subseteq L$ be an intermediate field. Then $M|K$ is a Galois extension if and only if the maps of K-extensions $M \to L$ have the same image (which is M).

If all the maps have M as an image, then for all $\gamma \in \mathrm{Gal}(L|K)$, $\gamma(M) = M$, and thus from the proof above, $M|K$ is a Galois extension. On the other hand, if $M|K$ is a Galois extension, then for all $\gamma \in \mathrm{Gal}(L|K)$, $\gamma(M) = M$ by Theorem 3.4.3 (images of embeddings from splitting fields coincide).

Corollary 3.6.7. *Let $\iota : K \to L$ be a finite separable extension. There are only finitely many intermediate fields between L and $\iota(K)$.*

Proof. Without loss of generality, we can extend L to a Galois extension (by Lemma 3.5.3, taking the splitting field over the minimal polynomials of the generators). The Galois group is finite, and bijectively corresponds to intermediate fields. $\square$

Example 3.6.8. We consider the Galois group of the extension $\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}$ and of its subfields. Note first that $\mathbb{Q}(\sqrt{2}, i)$ is the splitting field of the polynomial $(x^2 - 2)(x^2 + 1)$ whose roots are $\pm\sqrt{2}, \pm i$. In particular, $\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}$ is a splitting field of a separable polynomial, thus Galois.

We note the successive extensions $\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}(\sqrt{2})|\mathbb{Q}$. The minimal polynomial of $\sqrt{2}$ over $\mathbb{Q}$ is $x^2 - 2$, and the polynomial $x^2 + 1$ is the minimal polynomial of i over $\mathbb{Q}(\sqrt{2})$. By the tower law, $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}] = 4$. By Theorem 3.5.5, we have $\#\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}) = 4$. Define $G := \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q})$. By the classification of finite groups, we know that G is abelian, and that $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $G \simeq \mathbb{Z}/4\mathbb{Z}$. Note also that $\#\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}(i)) = 2$. This follows from the fact the extension is not trivial (otherwise $[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}]$ would equal 2). With similar logic, $\#\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}(\sqrt{2})) = 2$. Groups of order 2 are isomorphic to $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}(\sqrt{2})) \simeq \mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}(i)) \simeq \mathbb{Z}/2\mathbb{Z}$.

By the fundamental theorem of Galois theory, the two subgroups $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}(i))$ and $\mathrm{Gal}(\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}(\sqrt{2}))$ cannot coincide, as they correspond to different subfields of $\mathbb{Q}(\sqrt{2}, i)$. Consequently, $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ has three non trivial subgroups, and we find the third is given by $\mathbb{Q}(i\sqrt{2})$.

Example 3.6.9. We also note some field extensions that are not Galois.

- The extension $\mathbb{Q}(\sqrt[3]{2})|\mathbb{Q}$ is not a normal extension, thus not Galois.
- The extension $\mathbb{F}_2(t)[x]/(x^2 - t)|\mathbb{F}_2(t)$ is not separable, thus not Galois.

Lemma 3.6.10. *Let $L|K$ be a finite Galois extension. Let $\alpha \in L$. Then the minimal polynomial of α over K is the polynomial*

$$\prod_{\beta \in \mathrm{Orb}(\mathrm{Gal}(L|K), \alpha)} (x - \beta)$$

Proof. Let $P(x) = \prod_{\beta \in \mathrm{Orb}(\mathrm{Gal}(L|K),\alpha)}(x-\beta)$. Let $m_\alpha(x) \in K$ be the minimal polynomial of α over K. We know that $P(x) \in K[x]$, thus we have

$$m_\alpha(x)|P(x)$$

It is therefore sufficient to prove that $P(x)$ is irreducible over K. Suppose for contradiction $P(x) = Q(x)T(x)$ for $Q(x), T(x) \in K[x]$ and $\deg(Q), \deg(T) > 1$. Note that if $\rho \in L$ and $Q(\rho) = 0$, $\gamma(Q(\rho)) = Q(\gamma(\rho)) = \gamma(0) = 0$, thus roots of $Q(x)$ in L are stable under the action $\mathrm{Gal}(L|K)$. As $Q(x)$ has a root in L, noting $P(x)$ splits in L and $Q(x)|P(x)$, the set of roots of $P(x)$ contains a strict subset who is stable under $\mathrm{Gal}(L|K)$. This contradicts the fact the set of roots of $P(x)$ is the orbit of α under $\mathrm{Gal}(L|K)$. $\square$

Lemma 3.6.11. *Let K be a field and let $P(x) \in K[x]$. Let $L|K$ be a splitting extension of $P(x)$ and let $\alpha_1, \ldots, \alpha_n \in L$ be the roots of $P(x)$ with multiplicities. Then,*

1. *If $P(x)$ has no repeated roots, and $\phi : \mathrm{Aut}_K(L) \to S_n$ satisfies $\gamma(\alpha_i) = \alpha_{\phi(\gamma)(i)}$, then ϕ is an injective group homomorphism.*
2. *If $P(x)$ is irreducible over K and has no repeated roots, the image of ϕ is a transitive subgroup of S_n*
3. *The element $\Delta_P := \Delta(\alpha_1, \ldots, \alpha_n)$ lies in K and depends only on $P(x)$*
4. *Suppose that $\mathrm{char}(K) \neq 2$. Suppose also that $P(x)$ has no repeated roots. Then the image of ϕ lies inside $A_n \subseteq S_n$ if and only if $\Delta_P \in (K^*)^2$.*

Proof. (i) The map is tautologically a group homomorphism. It is injective as L is generated by the roots, thus an element γ that acts as the identity on the roots must act as the identity on L.

(ii) We only need to show $\mathrm{Aut}_K(L)$ acts transitively on the roots. As $P(x)$ is irreducible, it is the minimal polynomial of any α_i. By Lemma 3.6.10, the roots are an orbit under $\mathrm{Aut}_K(L)$ over any root, so we are done.

(iii) Note first that

$$P(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0 = x^d + s_1(\alpha_1, \ldots, \alpha_d)x^{d-1} + \cdots + (-1)^d s_d(\alpha_1, \ldots, \alpha_d)$$

By The Fundamental Theorem of Symmetric Functions, there is a unique polynomial $Q(x) \in K[x]$ such that $Q(s_1, \ldots, s_d) = \Delta(x_1, \ldots, x_d)$. Thus,

$$\Delta(\alpha_1, \ldots, \alpha_n) = Q(-a_{d-1}, a_{d-2}, \ldots, (-1)^d a_0)$$

As this function depends only on $P(x)$ and lies in K, we are done.

(iv) Consider $\delta(\alpha_1, \ldots, \alpha_n) := \prod_{i<j}(\alpha_i - \alpha_j)$. For any $\gamma \in \mathrm{Aut}_K(L)$, we have

$$\gamma(\delta(\alpha_1, \ldots, \alpha_n)) = \delta(\gamma(\alpha_1), \ldots, \gamma(\alpha_n)) = \delta(\alpha_{\phi(\gamma)(1)}, \ldots, \alpha_{\phi(\gamma)(n)}) = \mathrm{sign}(\phi(\gamma)) \cdot \delta(\alpha_1, \ldots, \alpha_n)$$

As this is a Galois extension, $\delta(\alpha_1, \ldots, \alpha_n) \in K$ if and only if the image of ϕ lies in A_n. Now also note that $\delta(\alpha_1, \ldots, \alpha_n) \in K$ if and only if $\Delta_P \in (K^*)^2$.

Note the characteristic being non-two is necessary to distinguish between sign, as else $\delta(\alpha_1, \ldots, \alpha_n)$ always lies in K.

$\square$

Remark 3.6.12. The key idea is that the Galois group of the splitting field of a degree n polynomial is a subgroup of S_n. Moreover, if $P(x)$ is irreducible, then it is transitive. If n is prime, then this means it contains an n-cycle (though not generally, as V_4 is transitive on $\{1,2,3,4\}$).

The last case is useful to note for when we consider $\mathrm{Gal}(M|K(\sqrt{\Delta_P}))$.

Example 3.6.13. Note that

$$\Delta(x_1,x_2,x_3) = -4s_1^3s_3 + s_1^2s_2^2 + 18s_1s_2s_3 - 4s_2^3 - 27s_3^2$$

Taking $P(x) = x^3 - x - \frac{1}{3}$, The polynomial has no roots in $\mathbb{Q}$ (moving it to $\mathbb{Z}[x]$ and seeing it has no roots in $\mathbb{F}_2[x]$), thus irreducible. It also has no multiple roots as the characteristic of $\mathbb{Q}$ is 0.

Let $L|\mathbb{Q}$ be a splitting field for $P(x)$ and take $\alpha_1,\alpha_2,\alpha_3$ to be the roots of $P(x)$ in L. Matching coefficients, $s_3(\alpha_1,\alpha_2,\alpha_3) = -1/3, s_2(\alpha_1,\alpha_2,\alpha_3) = -1, s_1(\alpha_1,\alpha_2,\alpha_3) = 0$, so

$$\Delta_P = -4s_2(\alpha_1,\alpha_2,\alpha_3)^3 - 27s_3(\alpha_1,\alpha_2,\alpha_3)^2 = 4 - \frac{27}{9} = 1$$

In particular, $\Delta_P \in (\mathbb{Q}^*)^2$ (as this is nonzero, it is an alternative way to see it has no repeated roots).

By the previous Lemma, $\mathrm{Gal}(L|\mathbb{Q})$ can be seen as a subgroup of A_3. On the other hand, $\mathrm{Gal}(L|\mathbb{Q})$ has order at least 3 as the extension $K(\alpha_i)|\mathbb{Q}$ has degree 3 for any α_i, as $P(x)$ is irreducible. By the tower law, $\mathrm{Gal}(L|\mathbb{Q})$ has order at least 3, thus $\#A_3 = 3$, giving $\mathrm{Gal}(L|\mathbb{Q}) \simeq A_3$.

Theorem 3.6.14 (Primitive Element Theorem)**.** *Let $L|K$ be a finite separable extension of fields. Then there is an element $\alpha \in L$ such that $L = K(\alpha)$*

Proof. We prove the case for K being finite and infinite separately.

In the finite case, we have $K \simeq \mathbb{F}_{p^n}$ for some prime p and positive integer n. Define $G_d := \{x \mid \mathrm{ord}(x) = d\} \subseteq \{x^d = 1\} \subseteq \mathbb{F}_{p_n}^*$. By definition, if $G_d \neq \emptyset, |G_d| = \phi(d)$ and if $G_d = \emptyset, |G_d| = 0$. Now, we have

$$\begin{aligned} p^n &= |\mathbb{F}_{p_n}^*| + 1 \\ &= \sum_{d|p^n-1} |G_d| + 1 \\ &= \sum_{d|p^n-1} \phi(d) + 1 \\ &= (p^n - 1) + 1 = p^n \end{aligned}$$

In particular, G_{p^n-1} is nonempty, thus we have a generator for the field (that is irrespective of the base field).

If K is an infinite field, noting that L is generated over K by a finite number of elements, induction shows that it is sufficient to prove that L is generated by one element if it is generated by two elements. Suppose that $L = K(\beta,\gamma)$. For $d \in K$, consider the intermediate field $K(\beta + d\gamma)$. As there are finitely many such, and as K is infinite, we can find $d_1, d_2 \in K$ such that $d_1 \neq d_2$ and $K(\beta + d_1\gamma) = K(\beta + d_2\gamma)$. We can find a $P(x) \in K[x]$ such that $\beta + d_1\gamma = P(\beta + d_2\gamma)$, meaning we have

$$\gamma = \frac{P(\beta + d_2\gamma) - (\beta + d_2\gamma)}{d_1 - d_2}$$

and

$$\beta = (\beta + d_2\gamma) - d_2\frac{P(\beta + d_2\gamma) - (\beta + d_2\gamma)}{d_1 - d_2}$$

and in particular, $K(\beta,\gamma) = K(\beta + d_2\gamma)$. □

Proposition 3.6.15. *Let F be a field of characteristic 0 and let $K = F(\beta, \gamma)$ where β and γ are algebraic over F. Then there exists a d such that $K = F(\beta + c\gamma)$ for some $c \in F$.*

Proof. We give a minimum polynomial argument. Suppose that $\beta + c\gamma$ is not a primitive element, such that $F(\beta + c\gamma) \subsetneq F(\beta, \gamma)$. In particular, $\gamma \notin F(\beta + c\gamma)$. Consider the minimal polynomials of β and γ over $F(\beta + c\gamma)$, calling them $f(X), g(X) \in F(\beta + c\gamma)[X]$, and take a splitting field L containing all roots of $f(X)$ and $g(X)$. Since $\gamma \notin F(\beta + c\gamma)$, there is another root $\gamma' \neq \gamma$ and a field automorphism which fixes $F(\beta + c\gamma)$ and takes $\sigma(\gamma) = \gamma'$. Then,

$$\beta + c\gamma = \sigma(\beta + c\gamma) = \sigma(\beta) + c\sigma(\gamma)$$

implying

$$c = \frac{\sigma(\beta) - \beta}{\gamma - \sigma(\gamma)}$$

As there are only finitely many field automorphisms $\mathrm{Aut}_{F(\beta+c\gamma)}(L)$ (where L is the splitting field), there are only finitely many $c \in F$ that fail to give the primitive element. All other values give $F(\beta + c\gamma) = F(\beta, \gamma)$. $\square$

4 Special Classes of Extensions

4.1 Cyclotomic Extension

Definition 4.1.1. *Let $n \geq 1$. For any field E, define*

$$\mu_n(E) := \{\rho \in E \mid \rho^n = 1\}$$

*The elements of $\mu_n(E)$ are called the **n-th roots of unity**. $\mu_n(E)$ inherits a group structure from E^*.*

Lemma 4.1.2. *The group $\mu_n(E)$ is a finite cyclic group.*

Proof. This group is clearly finite, as there are at most n elements that satisfy $x^d - 1 = 0$ over a field.

Suppose that we have two distinct subgroups H, K of $\mu_n(E)$ of the same cardinality, say d. By Lagrange's Theorem, we have that elements of both H and K are annihalated by $x^d - 1$, but their union has cardinality larger than d. This is a contradiction, thus $\mu_n(E)$ is finite cyclic. $\square$

Definition 4.1.3. *If $\#\mu_n(E) = n$, we call $\omega \in \mu_n(E)$ a **primitive n-th root of unity** if it is a generator of $\mu_n(E)$ (note the initial condition $\#\mu_n(E) = n$).*

Note that if $\omega \in \mu_n(E)$ is a primitive n-th root of unity, all other primitive n-th roots of unity are of the form ω^k where k is an integer coprime to n.

Remark 4.1.4. Let K be a field and suppose that $(n, \mathrm{char}(K)) = (1)$. Let L be a splitting field for the polynomial $x^n - 1 \in K[x]$. We denote this by $K(\mu_n)$ (though abusing language, as L is only well-defined up to non-canonical isomorphism). By construction, $x^n - 1$ has no repeated roots, thus $\#\mu_n(L) = n$ and $L|K$ is a Galois extension. $L|K$ is also a simple extension as L is generated over K by any primitive n-th root of unity in L.

By Lemma 4.1.2, $\mu_n(L) \simeq \mathbb{Z}/n\mathbb{Z}$, there are $\#(\mathbb{Z}/n\mathbb{Z})^* = \Phi(n)$ primitive n-th roots of unity in L.

Definition 4.1.5. *Define*

$$\Phi_{n,K}(x) := \prod_{\omega \in \mu_n(L), \omega \text{ primitive}} (x - \omega)$$

Note that $\deg(\Phi_{n,K}(x)) = \Phi(n)$.

Lemma 4.1.6. *The polynomial $\Phi_{n,K}(x)$ has coefficients in K and depends only on n and K (does not depend on the choice of splitting field).*

Proof. The coefficients of $\Phi_{n,K}(x)$ are symmetric functions in the primitive n-th roots. As these roots are permuted by $\mathrm{Gal}(L|K)$, the coefficients are invariant under $\mathrm{Gal}(L|K)$, and thus lie in K.

The polynomial $\Phi_{n,K}(x)$ only depends on n and K (and not on the choice of extension), as all the splitting K-extensions for $x^n - 1$ are isomorphic. $\square$

Proposition 4.1.7. *There is a natural injection of groups $\phi : \mathrm{Gal}(L|K) \hookrightarrow \mathrm{Aut}_{\mathrm{Groups}}(\mu_n(L)) \simeq (\mathbb{Z}/n\mathbb{Z})^*$. This map is surjective if and only if $\Phi_{n,K}(x)$ is irreducible over K.*

Proof. The first statement is straightforward, noting that $\mu_n(L)$ generates L and $\mathrm{Gal}(L|K)$ acts on L by ring automorphisms.

Let $\omega \in \mu_n(L)$ be a primitive n-th root of unity. Suppose that $\Phi_{n,K}(x)$ is irreducible over K. Since $\Phi_{n,K}(x)$ annihalates ω, it is the minimal polynomial of ω. In particular, $[L : K] \geq \Phi(n)$, and thus $\#\mathrm{Gal}(L|K) \geq \Phi(n)$. On the other hand, we have an injection from $\mathrm{Gal}(L|K) \hookrightarrow (\mathbb{Z}/n\mathbb{Z})^*$, giving $\#\mathrm{Gal}(L|K) \leq \Phi(n)$. Thus $\#\mathrm{Gal}(L|K) = \Phi(n)$, and by injectivity of this map, ϕ is also surjective.

Conversely, if ϕ is surjective, then the minimal polynomial of ω is $\Phi_{n,K}(x)$ by Lemma 1.0.2 and Lemma 3.6.10. $\square$

Proposition 4.1.8. *The polynomial $\Phi_{n,\mathbb{Q}}(x)$ is irreducible and has coefficients in $\mathbb{Z}$.*

Proof. Let L be a splitting field of $x^n - 1 \in \mathbb{Q}[x]$. Let $\omega \in L$ be a primitive n-th root of unity. Let $Q(x)$ be the minimal polynomial of ω over $\mathbb{Q}$. Then $Q(x)|x^n - 1$, thus we can find a polynomial $T(x) \in \mathbb{Q}[x]$ such that $Q(x)T(x) = x^n - 1$. Note that $T(x)$ and $Q(x)$ are monic. Thus $1/c(T)$ and $1/c(Q)$ are both positive integers. On the other hand, $c(x^n - 1) = 1$, and noting that $1 = c(T)c(Q)$, we see that $c(T) = c(Q) = 1$. In particular, $Q(x)$ and $T(x)$ have coefficients in $\mathbb{Z}$.

Fix a prime number p which is coprime to n. We claim that $Q(\omega^p) = 0$. Else, we have $T(\omega^p) = 0$, as $Q(x)T(x) = x^n - 1$. In particular ω is a root of $T(x^p)$. Thus $Q(x)|T(x^p)$. In particular, we have some $H(x)$ such that $Q(x)H(x) = T(x^p)$, where $H(x)$ is also monic. Repeating the same logic as before, $H(x) \in \mathbb{Z}[x]$.

Now,

$$T(x^p)(\mathrm{mod}\ p) = (T(x)(\mathrm{mod}\ p))^p$$

in $\mathbb{F}_p[x]$ as the p-power function is additive in $\mathbb{F}_p[x]$. In particular, from $Q(x)H(x) = T(x^p)$, we see that $(Q(x)(\mathrm{mod}\ p), T(x)(\mathrm{mod}\ p)) \neq (1)$. Define $J(x) := \gcd(Q(x)(\mathrm{mod}\ p), T(x)(\mathrm{mod}\ p))$. Then, $J(x)^2|x^n - 1(\mathrm{mod}\ p)$, and in particular $x^n - 1(\mathrm{mod}\ p)$ has multiple roots, which is a contradiction. Thus $Q(\omega^p) = 0$.

Generally, $Q(\omega^k) = 0$ for k coprime to n. Thus, all primitive n-th roots of unity are roots of $Q(x)$. We see that $\deg(Q) \geq \Phi(n)$. By definition, $Q(x)|\Phi_{n,\mathbb{Q}}(x)$, so we have $Q(x) = \Phi_{n,\mathbb{Q}}(x)$. In particular, $\Phi_{n,\mathbb{Q}}(x)$ is irreducible with coefficients in $\mathbb{Z}$.

$\square$

Example 4.1.9. Let $p > 2$ be prime and $\zeta_p := \exp(2\pi i/p)$. Let $K = \mathbb{Q}(\zeta_p)$. The cyclotomic polynomial is

$$f(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1 = \Phi_{p,\mathbb{Q}}(x) = \prod_{i=1}^{p-i}(x - \zeta^i)$$

is by the previous proposition and by Gauss's Lemma irreducible in $\mathbb{Q}[x]$.

In particular $[K : \mathbb{Q}] = p - 1$. So a regular p-gon can be constructed with a ruler and compass only if $p - 1$ is a power of 2 (such as 17).

4.2 Kummer Extension

Definition 4.2.1. *Let K be a field and n be a positive integer with $(n, \mathrm{char}(K)) = (1)$. Suppose that $x^n - 1$ splits in K. Let $a \in K$ and let $M|K$ be a splitting extension for the polynomial $x^n - a$. We call such extension a **Kummer extension***

Note that by construction, $x^n - a$ is a separable polynomial. In particular, $M|K$ is a Galois extension.

Lemma 4.2.2. *Let $M|K$ be a Kummer extension. Let $\rho \in M$ be such that $\rho^n = a$. There is a unique homomorphism $\phi : \mathrm{Gal}(M|K) \to \mu_n(K)$ such that $\phi(\gamma) = \gamma(\rho)/\rho$. The map does not depend on the choice of ρ and is injective.*

Proof. First, $(\gamma(\rho)/\rho)^n = \gamma(\rho^n)/\rho^n = a/a = 1$, so in particular $\gamma(\rho)/\rho \in \mu_n(K)$, giving a well-defined map. Uniqueness follows from the fact the map is defined on all γ.

To see this map does not depend on the choice of ρ, if we have $\rho_1^n = a$, then note that $(\rho/\rho_1)^n = a/a = 1$. Thus, there is an n-th root of unity $\mu \in K$ such that $\mu = \rho/\rho_1$ as $x^n - 1$ splits in K. Now,

$$\gamma(\rho)/\rho = \mu\gamma(\rho)/(\mu\rho) = \gamma(\mu\rho)/(\mu\rho) = \gamma(\rho_1)/\rho_1$$

So ϕ does not depend on ρ.

To see that ϕ is a group homomorphism, for any $\gamma, \lambda \in \mathrm{Gal}(M|K)$, we have

$$\phi(\gamma\lambda) = \gamma(\lambda(\rho))/\rho$$

and

$$\phi(\gamma)\phi(\lambda) = (\gamma(\rho)/\rho)(\lambda(\rho)/\rho)$$

thus it suffices to show

$$\gamma(\lambda(\rho)) = \lambda(\rho)\gamma(\rho)/\rho$$

but this follows immediately from the fact $x^n - 1$ splits in K;

$$\lambda(\rho)/\rho = \gamma(\lambda(\rho)/\rho) = \gamma(\lambda(\rho))/\gamma(\rho)$$

Finally ϕ is injective, as if $\phi(\gamma) = 1$, as γ fixes ρ, it fixes any root of $x^n - a$ and hence $\gamma = 1$. □

Remark 4.2.3. Note that from the above proof, $\mathrm{Gal}(M|K)$ is cyclic. Let it be isomorphic to C_d, and pick a generator σ. In particular, taking any root ρ of $x^n - a$, $\sigma(\rho) = \zeta\rho$ for some ζ with order d. σ^i generate distinct images and by dimension argument, we can see that in fact $M|K$ is a simple extension, generated by any root of $x^n - a$.

Definition 4.2.4. *Let E be a field. Let H be a group. A **character** of H is a group homomorphism $H \to E^*$.*

Proposition 4.2.5 (Dedekind)**.** *Let $\chi_1, \dots, \chi_k$ be distinct characters of H with values in E^*. Let $a_1, \dots, a_k \in E$ be such that*

$$a_1\chi_1(h) + \cdots + a_k\chi(h) = 0$$

for all $h \in H$. Then $a_1 = \cdots = a_k = 0$.

Proof. We proceed by induction on k. The result is immediate for $k = 1$. Suppose $k \geq 2$ and the proposition holds for any smaller parameter. If a_i all vanish, we are done. Else, up to reordering, without loss of generality, suppose that $a_2 \neq 0$.

Pick $\alpha \in H$ such that $\chi_1(\alpha) \neq \chi_2(\alpha)$. Now for any $\beta \in H$, we have

$$\sum_{i=1}^{k} a_i\chi_i(\alpha\beta) = \sum_{i=1}^{k} a_i\chi_i(\alpha)\chi_i(\beta) = 0$$

And

$$\chi_1(\alpha)\sum_{i=1}^{k} a_i\chi_i(\beta) = \sum_{i=1}^{k} a_1\chi_1(\alpha)\chi_i(\beta)$$

Subtracting,

$$\sum_{i=2}^{k} a_i(\chi_i(\alpha) - \chi_1(\alpha))\chi_i(\beta) = 0$$

As this holds for any $\beta \in H$, we have from the inductive hypothesis that $a_2 = 0$, a contradiction. $\square$

Theorem 4.2.6. *Let K be a field and n be a positive integer with $(n, \mathrm{char}(K)) = (1)$. Suppose that $x^n - 1$ splits in K. Suppose also that $L|K$ is a Galois extension and that $\mathrm{Gal}(L|K)$ is a cyclic group of order n.*

Now let $\sigma \in \mathrm{Gal}(L|K)$ be a generator of $\mathrm{Gal}(L|K)$ and $\omega \in K$ is a primitive n-th root of unity in K. For any $\alpha \in L$, let

$$\beta(\alpha) := \alpha + \omega\sigma(\alpha) + \omega^2\sigma^2(\alpha) + \cdots + \omega^{n-1}\sigma^{n-1}(\alpha)$$

Then,

- *For any $\alpha \in L$, $\beta(\alpha)^n \in K$*
- *There is an $\alpha \in L$ such that $\beta(\alpha) \neq 0$.*
- *If $\beta(\alpha) \neq 0$, then $L = K(\beta(\alpha))$ (such that L is the splitting field of $x^n - \beta(\alpha)^n$)*

Proof. Let $\alpha \in L$. Compute

$$\sigma(\beta(\alpha)) = \sigma(\alpha) + \omega\sigma^2(\alpha) + \omega^2\sigma^3(\alpha) + \cdots + \omega^{n-1}\alpha = \omega^{n-1}\beta(\alpha) = \omega^{-1}\beta(\alpha)$$

In particular, $\sigma^i(\beta(\alpha)) = \omega^{-i}\beta(\alpha)$ Furthermore, we have

$$\sigma(\beta(\alpha)^n) = \sigma(\beta(\alpha))^n = \omega^{-n}\beta(\alpha)^n = \beta(\alpha)^n$$

As $L|K$ is Galois, we have $\beta(\alpha)^n \in K$. Note that any element of $\mathrm{Gal}(L|K)$ defines a character on L^* with values in L^*. By Dedekind, there is some α such that $\beta(\alpha) \neq 0$. As $\omega^{-i}\beta(\alpha)$ are roots of $x^n - \beta(\alpha)^n$, it splits in L.

Now, $\mathrm{Gal}(L|K)$ acts transitively and faithfully (the only element in $\mathrm{Gal}(L|K)$ that fixes all the roots is the identity) on the roots of $x^n - (\beta(\alpha))^n$. In particular, $x^n - \beta(\alpha)^n$ is irreducible over K. Thus $[K(\beta(\alpha)) : K] = n = [L : K]$, which from the tower law, we conclude $K(\beta(\alpha)) = L$. Thus L is a splitting field for $x^n - \beta(\alpha)^n$.

$\square$

4.3 Radical Extension

Definition 4.3.1. *The field extension $L|K$ is said to be* ***radical*** *if $L = K(\alpha_1, \dots, \alpha_k)$ and there are natural numbers $n_1, \dots, n_k$ such that $\alpha_1^{n_1} \in K, \alpha_2^{n_2} \in K(\alpha_1), \dots, \alpha_k^{n_k} \in K(\alpha_1, \dots, \alpha_{k-1})$.*

By definition, if $L|K$ and $M|L$ are radical extensions, $M|K$ is a radical extension.

Example 4.3.2. Kummer extensions are radical. This is an immediate consequence of the fact Kummer extensions $L|K$ are simple extensions generated by any root of $x^n - a$ for $a \in K$.

Lemma 4.3.3. *Let $L|K$ be a radical extension and let $J|L$ be a finite extension such that the composed extension $J|K$ is a Galois extension. Then there is a field L' which is intermediate between J and L such that $L'|K$ is Galois and radical.*

Proof. Suppose that $L = K(\alpha_1, \dots, \alpha_k)$ and that we have natural numbers $n_1, \dots, n_k$ such that $\alpha_1^{n_1} \in K, \alpha_2^{n_2} \in K(\alpha_1), \dots, \alpha_k^{n_k} \in K(\alpha_1, \dots, \alpha_{k-1})$. Let $G := \mathrm{Gal}(J|K) = \{\sigma_1, \dots, \sigma_t\}$. Then for any $i \in \{1, \dots, k\}$ and $\sigma \in G$, we have

$$\sigma(\alpha_i^{n_i}) = \sigma(\alpha_i)^{n_i} \in \sigma(K(\alpha_1, \dots, \alpha_{i-1})) = K(\sigma(\alpha_1), \dots, \sigma(\alpha_{i-1}))$$

In particular,

$$K(\alpha_1, \dots, \alpha_k, \sigma_1(\alpha_1), \dots, \sigma_1(\alpha_k), \dots, \sigma_t(\alpha_1), \dots, \sigma_t(\alpha_k)) = K(\mathrm{Orb}(\alpha_1), \dots, \mathrm{Orb}(\alpha_k))$$

is a radical extension of K. Now, given $\sigma \in G$, we have

$$\sigma(K(\mathrm{Orb}(\alpha_1), \dots, \mathrm{Orb}(\alpha_k))) = K(\sigma(\mathrm{Orb}(\alpha_1)), \dots, \sigma(\mathrm{Orb}(\alpha_k))) = K(\mathrm{Orb}(\alpha_1), \dots, \mathrm{Orb}(\alpha_k))$$

we see that $K(\mathrm{Orb}(\alpha_1), \dots, \mathrm{Orb}(\alpha_k))|K$ is a Galois extension (field fixed by Galois group actions). Thus we may set $L' := K(\mathrm{Orb}(\alpha_1), \dots, \mathrm{Orb}(\alpha_k))$.

$$\begin{tikzcd}
K \arrow[r, hook] \arrow[rr, hook, bend left] \arrow[dr, hook] & L = K(\alpha_1, \dots, \alpha_k) \arrow[r, hook] \arrow[d, hook] & J \\
& L' = K(\mathrm{Orb}(\alpha_1), \dots, \mathrm{Orb}(\alpha_k)) \arrow[ur, hook] &
\end{tikzcd}$$

□

4.3.1 Solvability by Radical Extensions

Theorem 4.3.4. *Suppose that* $\mathrm{char}(K) = 0$. *Let $L|K$ be a finite Galois extension.*

If $\mathrm{Gal}(L|K)$ *is solvable, then there exists a finite extension $M|L$ with the following properties*

1. *The composed extension $M|K$ is Galois*
2. *There is a map of K-extensions $K(\mu_{[L:K]}) \hookrightarrow M$*
3. *M is generated by the images of L and $K(\mu_{[L:K]})$ in M.*
4. *The extension $M|K(\mu_{[L:K]})$ is a composition of Kummer extensions. In particular, $M|K$ is a radical extension.*

Conversely, if there exists a finite extension $M|L$ such that the composed extension $M|K$ is radical, then $\mathrm{Gal}(L|K)$ *is solvable.*

Proof. First note that the images of L and $K(\mu_c)$ in M do not depend on the maps of K-extensions $L \hookrightarrow M$ and $K(\mu_{[L:K]}) \hookrightarrow M$ as the two are both galois extensions.

Let $d := \#\mathrm{Gal}(L|K) = [L : K]$. There is a Galois extension of K and maps of K extensions $K(\mu_d) \hookrightarrow J$ and $L \hookrightarrow J$ by the existence of splitting extensions and Lemma 3.5.3. Choose such an extension and maps of K-extensions. Now, let P be the field generated by L and $K(\mu_d)$ in J. Then we have

$$\begin{tikzcd} & J & \\ & P \arrow[u, hook] & \\ L \arrow[ur, hook] & & K(\mu_d) \arrow[ul, hook] \\ & K \arrow[ul, hook] \arrow[ur, hook] & \end{tikzcd}$$

Let $G := \mathrm{Gal}(J|K)$. We can observe the following:

1. $P|K$ is a Galois extension, as it is fixed by any $\sigma \in G$ (as the fields they are generated by are Galois)

2. $P|K(\mu_d)$ is Galois by lifting from K.

3. The restriction map $\mathrm{Gal}(P|K(\mu_d)) \to \mathrm{Gal}(L|K)$ is injective. If $\sigma \in \mathrm{Gal}(P|K(\mu_d))$ restricts to the identity in L, it fixed both $K(\mu_d)$ and L, thus fixes P.

Suppose now that $\mathrm{Gal}(L|K)$ is solvable. Then, by Lemma 1.1.3 and injectivity of $\mathrm{Gal}(P|K(\mu_d))$ into $\mathrm{Gal}(L|K)$, $\mathrm{Gal}(P|K(\mu_d))$ is solvable. In particular, there is a finite filtration with abelian quotients

$$0 = H_0 \subseteq H_1 \subseteq \cdots \subseteq H_n = \mathrm{Gal}(P|K(\mu_d))$$

By Lemma 1.1.7, we may assume without loss of generality that the quotients of the filtration are cyclic. By the fundamental theorem of Galois Theory, the subgroups H_i correspond to a descreasing sequence of subfields of P

$$P = P_0 \supseteq P_1 \supseteq \cdots \supseteq P_n = K(\mu_d)$$

such that $P_i|P_{i+1}$ is a Galois extension for any i. Also,

$$H_{i+1}/H_i \simeq \mathrm{Gal}(P|P_i)/\mathrm{Gal}(P|P_{i+1}) \simeq \mathrm{Gal}(P_i|P_{i+1})$$

such that $\mathrm{Gal}(P_i|P_{i+1})$ is cyclic. By Lagrange's Theorem (applied repeatedly) $\#(H_{i+1}/H_i)$ is a divisor of $\#\mathrm{Gal}(P|K(\mu_d))$ and thus of $\#\mathrm{Gal}(L|K) = d$. In particular, $x^{\#\mathrm{Gal}(P_i|P_{i+1})} - 1$ splits in $K(\mu_d)$, and so in P_{i+1}. By Theorem 4.2.6, $P_i|P_{i+1}$ is a Kummer extension, thus a radical extension. Setting $M := P$, we have shown this satisfies all our mentioned properties.

To prove the other direction, suppose that we have a finite extension $M|L$ such that the composed extension $M|K$ is radical. We may thus suppose that $M = K(\alpha_1, \ldots, \alpha_k)$ and there are $n_1, \ldots, n_k$ such that $\alpha_1^{n_1} \in K, \ldots, \alpha_k^{n_k} \in K(\alpha_1, \ldots, \alpha_{k-1})$. Let $t := \prod_{i=1}^{k} n_i$. Choose a Galois extension $J|K$

such that there are maps of K-extensions $M \hookrightarrow J$ and $K(\mu_t) \hookrightarrow J$. Fixing maps, let E be the intermediate field generated by M and $K(\mu_t)$ in J. Thus, we have a diagram of extensions

$$\begin{tikzcd}
 & J & \\
 & E \arrow[u, hook] & \\
M \arrow[ur, hook] & & K(\mu_t) \arrow[ul, hook'] \\
L \arrow[u, hook] & & K \arrow[u, hook] \arrow[ll, hook']
\end{tikzcd}$$

By definition, $E = K(\mu_t)(\alpha_1, \dots, \alpha_k)$, and by construction each $K(\mu_t)(\alpha_1, \dots, \alpha_{i+1})|K(\mu_t)(\alpha_1, \dots, \alpha_i)$ is a Kummer extension, as $n_i|t$. In particular, the Galois group is abelian. Now $\mathrm{Gal}(K(\mu_t)|K)$ is abelian also. By the Fundamental Theorem for Galois groups, we see that $\mathrm{Gal}(E|K)$ is solvable. Finally, as $\mathrm{Gal}(L|K)$ is a quotient of $\mathrm{Gal}(E|K)$, $\mathrm{Gal}(L|K)$ is solvable. □

Definition 4.3.5. *Let $P(x) \in K[x]$ and let $L|K$ be a splitting extension for $P(x)$. We say $P(x)$ is **solvable by radicals** if there is an extension $M|L$ such that the composed extension $M|K$ is radical (as the splitting extensions are isomorphic, the choice does not matter). By the previous theorem, $P(x)$ is solvable by radicals if and only if $\mathrm{Gal}(L|K)$ is solvable.*

Corollary 4.3.6. *Let $n \geq 5$ and K be a field. The extension $K(x_1, \dots, x_n)|K(x_1, \dots, x_n)^{S_n}$ is not radical. (Note the action is induced by the action of S_n on $K[x_1, \dots, x_n]$)*

Proof. By Artin's Lemma, $K(x_1, \dots, x_n)|K(x_1, \dots, x_n)^{S_n}$ is a Galois extension. On the other hand, S_n is not solvable for $n \geq 5$, so by Theorem 4.3.4, is not radical. □

Remark 4.3.7. To see $K(x_1, \dots, x_n)|K(x_1, \dots, x_n)^{S_n}$ is a Galois extension directly, note that it is the splitting field of the polynomial

$$U_n(x) = x^n - s_1(x_1, \dots, x_n)x^{n-1} + \cdots + (-1)^n s_n(x_1, \dots, x_n) \in K(x_1, \dots, x_n)^{S_n}[x]$$

And the roots are $x_1, \dots, x_n$ generate the field.

Example 4.3.8 (Solution to the General Cubic Equation)**.** Let K be a field and suppose that $\mathrm{char}(K) = 0$. We wish to solve the cubical equation

$$y^3 + ay^2 + by + c = 0$$

where $a, b, c \in K$. Letting $x = y + \frac{a}{3}$, we see that this is equivalent to solving

$$x^3 + px + q = 0$$

where $p = -\frac{1}{3}a^2 + b$ and $q = \frac{2}{27}a^3 - \frac{1}{3}ab + c$. So let $P(x) = x^3 + px + q$. We wish to find a solution that starts with p, q and iteratively applies multiplication, addition, multiplication by K, extraction of 2nd and 3rd roots.

Let $L|K$ be a splitting extension for $P(x)$. Let $\omega \in K(\mu_3)$ ne a primitive 3rd root of unity. Now by Lemma 3.5.3 we can choose a finite Galois extension $J|K$ and maps of K extensions $L \hookrightarrow J$ and

$K(\mu_3) = K(\omega) \hookrightarrow J$. Let $M = L(\omega)$ be the field generated in J by the images of L and $K(\omega)$ in J. So we have the following

$$\begin{tikzcd}
 & M = L(\omega) & \\
L \arrow[ur, hook] & & K(\mu_3) = K(\omega) \arrow[ul, hook'] \\
 & K \arrow[ul, hook'] \arrow[ur, hook] &
\end{tikzcd}$$

Now note that $\mathrm{Gal}(L|K)$ is solvable as it injects into S_3, and thus $M|K$ is radical by Theorem 4.3.4 (from which we should be able to retrieve an expression for ω).

Consider the sequence of extensions

$$K \hookrightarrow K(\omega) \hookrightarrow K(\omega, \sqrt{\Delta_P}) \hookrightarrow M$$

As the square root of Δ_P is a polynomial in the roots of $P(x)$, it lies in L.

Now note that

5 Main Ideas in GT - No definitions

The concept of multiple roots (on $P(x) \in K[x]$) is invariant under

- field extension. (Pf. ED algorithm is unique in computing a generator)
- polynomials $Q(x)$ such that $Q(x)|P(x)$

The gcd of P, Q is the generator of (P, Q)

If $P' \neq 0$ and P is irreducible, it has no multiple roots.

Extension of maps :

$$\begin{tikzcd}
K \arrow[r, hook] \arrow[d] & L \\
K(\alpha) \arrow[ur, hook, dashed] &
\end{tikzcd}$$

is determined by sending α to the roots of m_α in L, where m_α is the minimal polynomial of α with coefficients in K. So the cardinality of maps is the number of roots of m_α in L. This is a consequence of the fact $K(\alpha) \simeq K[x]/m_\alpha$.

- composition of normal extensions need not be normal, consider $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt[4]{2})$.

5.1 Relating Field Extensions

- Splitting fields exist for any polynomial

$$K \xhookrightarrow{\exists s_P} M$$

- Lemma 4.3.3: If $L|K$ is a radical extension and $J|L$ is a finite extension such that $J|K$ is a Galois extension, there is an intermediate field L' between J and L such that $L'|K$ is Galois and radical

$$\begin{tikzcd}
K \arrow[r, hook, "r"] \arrow[dr, hook] \arrow[rr, bend left, "g"] & L = K(\alpha_1, \dots, \alpha_k) \arrow[r, hook] \arrow[d, hook, "r"] & J \\
& L' = K(\mathrm{Orb}(\alpha_1), \dots, \mathrm{Orb}(\alpha_k)) \arrow[ur, hook] &
\end{tikzcd}$$

5.2 Examples of Galois Extensions

Example 5.2.1. Consider $K = \mathbb{Q}(\sqrt{2}, \sqrt{3})$ as a field extension over $\mathbb{Q}$. K is the splitting field over the separable polynomial $(x^2 - 2)(x^2 - 3)$, thus is Galois. Field automorphisms must send each generator to their conjugates, so our choice is

$$\sqrt{2} \mapsto \pm\sqrt{2} \qquad \sqrt{3} \mapsto \pm\sqrt{3}$$

giving $G = \mathrm{Gal}(K|\mathbb{Q}) \simeq C_2 \times C_2$. By Galois correspondence, the nontrivial subgroups give intermediate fields, where the correspondence is given by K^H where $H \subseteq G$. Taking the subgroup that flips $\sqrt{2}$, we have

$$K^{H_2} = \{a + c\sqrt{3} \mid a, c \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{3})$$

and similarly with H_3. The map that flips $\sqrt{2}$ and $\sqrt{3}$ would be

$$K^{H_{2,3}} = \{a + \sqrt{d} \mid a, d \in \mathbb{Q}\} = \mathbb{Q}(\sqrt{6})$$

We also give an example of a Kummer extension.

Example 5.2.2. Let $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$ where $\zeta_3 = e^{2\pi i/3}$. This is the splitting field over the separable polynomial $x^3 - 2$. The galois group is generated by choices of maps

$$\sqrt[3]{2} \mapsto \zeta_3^k \sqrt[3]{2}, k = 0, 1, 2 \qquad \zeta_3 \mapsto \zeta_3^{\pm 1}$$

Now note that $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$ and $[\mathbb{Q}(\zeta) : \mathbb{Q}] = 2$, and as $\zeta \notin \mathbb{Q}(\alpha)$,$[K : \mathbb{Q}] = 6$ by the tower law. In particular $|G| = 6$, and we can check via relations that this is S_3. The proper subfields correspond to the subgroups of S_3 which correspond to subfields $\mathbb{Q}(\zeta_3), \mathbb{Q}(\sqrt[3]{2}), \mathbb{Q}(\zeta_3\sqrt[3]{2}), \mathbb{Q}(\zeta_3^2\sqrt[3]{2})$.

Example 5.2.3. Taking $K = \mathbb{Q}(\zeta_5)$ where $\zeta_5 = e^{2\pi i/5}$. This is a cyclotomic field which has Galois group $\mathrm{Gal}(\mathbb{Q}(\zeta_5)|\mathbb{Q}) \simeq (\mathbb{Z}/5\mathbb{Z})^\times \simeq C_4$. C_4 has exactly one nontrivial subgroup of order 2, whose automorphism set is $\{\mathrm{id}, \sigma^2\}$. As σ^2 sends ζ_5 to $\zeta_5^4 = \zeta_5^{-1}$, it fixes $\zeta_5 + \zeta_5^{-1}$ whose minimum polynomial is $x^2 + x - 1$.

Remark 5.2.4. The above give rise to a variety of examples $[K : F]$ such that $K|F$ is Galois but there are intermediate fields $F \subsetneq L \subsetneq K$ such that $L|F$ is not Galois. For instance, take $F = \mathbb{Q}$ and $L = \mathbb{Q}(\sqrt[3]{2})$, $K = \mathbb{Q}(\sqrt[3]{2}, \zeta_3)$.

Example 5.2.5. Let $f := t^4 - 4t^2 + 2$ and $\alpha \in \mathbb{C}$ be a root of f. Then $\mathbb{Q}(\alpha)$ is the splitting field of f, by noting how the roots relate to each other. Also, we have the tower of extensions

$$\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{2}) \subsetneq \mathbb{Q}(\alpha)$$

which shows the extension has degree 4. Explicit mappings of roots shows that $\mathrm{Gal}(\mathbb{Q}(\alpha)|\mathbb{Q}) \simeq C_4$.

5.3 Important Things to Keep in Mind

- Splitting extensions always exist (induction by repeatedly quotienting by irreducible factors of P, and noting this always produces roots)
- Splitting extensions are (non-canonically) isomorphic as K-extensions (induction with quotienting with a min-poly of a root of P)
- Extensions from splitting fields preserve image (because any automorphism only permutes roots)
- Number of injections from simple extensions $K(\alpha)$ to J depends on root presense (of minpoly) in J (bijective correspondence).
- Taking $K(\alpha_1, \dots, \alpha_k)$, there is a nonempty/finite number of injections to fields where the product of the minpoly split. By bijective correspondence, there are 'tower' many ($[M : K]$ many) when the minpolys separate.
- Normal iff splitting extension for poly with coefficients in K ($\Rightarrow$, consider product of minpoly of generators, $\Leftarrow$, pick any $\alpha \in L$, extend to splitting field of prod of minpoly, induce map λ from L to splitter, by image invariance $\lambda(L)$ contains all roots of α, splits.)
- Galois correspondence with intermediate fields and raising base fields, use Artin with identity ($\mathrm{Gal}(K|K^G) = G$), inverse given by $H \mapsto L^H$
- Lowering to subfield from L to M only works if $\mathrm{Gal}(L|M)$ is a normal subgroup of $\mathrm{Gal}(L|K)$ (use FIT, image fixing of M by $\gamma \in \mathrm{Gal}(L|K)$, kernel argument) (reverse, navigate through to show $\mathrm{Gal}(L|\gamma(M)) = \mathrm{Gal}(L|M)$, which implies $M = \gamma(M)$ by FTGT) (image invariance lets us define maps about M) ($\mathrm{Gal}(L|K)/\mathrm{Gal}(L|M) \simeq \mathrm{Gal}(M|K)$).
- $\uparrow$ also lets us lower galois field by image invariance
- Kummer has cyclic Galois group (injects into roots of unity) (injective by root fixing argument)