MATH594 Algebra II

AResseges Stery

May 27, 2024

Preface

The notes are taken for MATH594 Algebra II by Prof. Mircea Mustaţă in 2024 Winter at University of Michigan. The contents covered are mainly on basic group theory, with its application in representation theory; and field extension with Galois theory. Here I appreciate the kind help of Prof. Mustaţă throughout the whole semester.

Some contents are marked with asterisk (*). These are contents excluded from testing, but out of personal interest I have recorded it. There are also some minor results that I added from the original course contents (which indicates that there may be typos or errors in the notes). Revisions, or pull requests to this repository, are more than welcomed.

For notes separated for each chapter one may consult this repository.

Contents

Chapter 1

Group Theory

1.1 Group Preliminaries

Definition 1.1.1 (Group). A **group** is a set G together with a binary operation $G \times G \to G$, often written $(a, b) \mapsto a \cdot b$ or simply ab, s.t. the following properties are satisfied:

1. *Associativity:* $(ab)c = a(bc)$ for all $a, b, c \in G$.
2. *Existence of Identity*: There exists $e = e_G \in G$ s.t. $\forall a \in G, ae = a = ea$.
3. *Existence of Inverse*: For all $a \in G$. there exists $b \in G$ s.t. $ab = e = ba$.

Furthermore, if the operation is commutative, i.e. for all $a, b \in G$, $ab = ba$, then the group is **commutative**, or **abelian**.

Notation. If the group G is abelian, then the operation is often represented in additive notations (with operation denoted as "$+$", and inverse of $a \in G$ being $-a$).

Remark 1.1.2. One implicitly presented condition is that the operation of groups need to be closed within the set predefined. This is indicated by the signature of the operation, which should land in G. This often needs to be checked when the group structure is defined in some larger structure.

Remark 1.1.3. From the definition of group there are some immediate facts/properties:

1) The identity in the group is unique. Suppose that there exist two identity elements e and e', then by rule 2 $e = ee' = e'$.
2) For a given element in the group, the inverse of it is unique. Let b and b' both be the inverse of some $a \in G$. Then

$$b = b(ab') = (ba)b' = b'$$

the uniqueness allows us to unambiguously denote the inverse of a as a^{-1}. This also implies $(a^{-1})^{-1} = a$, as clearly by the previous process a is the inverse of a^{-1}; and the inverse is unique.

3) $(ab)^{-1} = b^{-1}a^{-1}$. By the uniqueness of the inverse element, it suffices to check that the claimed inverse satisfies rule 2. This is indeed the case as

$$(ab)(b^{-1}a^{-1}) = (a(bb^{-1}))a^{-1} = (ae)a^{-1} = aa^{-1} = e$$

and for multiplication in the other sequence the checking is similar.

4) For $a, b, c \in G$, then $ab = ac \implies b = c$; and $ba = ca \implies b = c$. This results directly from the fact that a is invertible; and multiplying on the left/right, respectively, a, gives the desired result.

Remark 1.1.4. The associativity of operation in the groups gives the unambiguity of writing successive multiplications. Rigorously, when written $x_1 \dots x_n$ for $n \geq 2$, it is defined inductively on n via specifying the result to be $(x_1 \dots x_{n-1})x_n$. The convention is that for $n = 0$ this is simply the identity.

In particular one can unambiguously write out the power of an element:

$$a^n := \begin{cases} \underbrace{a \dots a}_{n} & n > 0 \\ e & n = 0 \\ \underbrace{a^{-1} \dots a^{-1}}_{n} & n < 0 \end{cases}$$

This gives $a^m \cdot a^n = a^{m+n}$ for all $m, n \in \mathbb{Z}$. The cases where m and n are of the same sign are clear; and for those of opposite sign, applying the same elimination process as Remark 1.1.3 3) gives the desired result.

If G is abelian, in additive notation we often denote $n \cdot a := a^n$.

Definition 1.1.5. If G and H are groups, a **group homomorphism** $f : G \to H$ is a map s.t. $f(a \cdot b) = f(a) \cdot f(b)$ for all $a, b \in G$.

Proposition 1.1.6. If $f : G \to H$ is a group homomorphism, then $f(e_G) = e_H$, and $f(a^{-1}) = (f(a))^{-1}$.

Proof. By Remark 1.1.3 4) and the property of identity, we have

$$f(e_G) \cdot e_H = f(e_G) = f(e_G \cdot e_G) = f(e_G) \cdot f(e_G) \implies e_H = f(e_G)$$

For the second statement, use the above result:

$$e_H = f(e_G) = f(a \cdot a^{-1}) = f(a) \cdot f(a^{-1})$$

By the definition $(f(a))^{-1}$ is the inverse of $f(a)$. By the uniqueness of inverse this gives $f(a^{-1}) = f(a^{-1})$. □

Remark 1.1.7. Given $f : G \to H$, $g : H \to K$ which are both f and g are group homomorphisms, then $f \circ g$ is also a group homomorphism. This results from the fact that

$$f(g(a \cdot b)) = f(g(a) \cdot g(b)) = f(g(a)) \cdot f(g(b))$$

The fact that morphism is closed w.r.t. composition implies that the groups form a category Grps.

Definition 1.1.8. If G and H are groups, then $f : G \to H$ is a **group isomorphism** if it is a bijective group homomorphism.

Proposition 1.1.9. $f : G \to H$ being a group homomorphism is a group isomorphism if and only if there exists a group homomorphism $g : H \to G$ s.t. $g \circ f = \mathrm{Id}_G$, and $f \circ g = \mathrm{Id}_H$.

Proof. It suffices to show implication in two directions:

$\Rightarrow$: Since f is bijective, there must admit a (pointwise) inverse of f s.t. $f^{-1} \circ f = \mathrm{Id}_G$, $f \circ f^{-1} = \mathrm{Id}_H$. Define $g = f^{-1}$. It suffices to check that g is a group homomorphism. To prove this we need to verify that for all $u, v \in H$, $g(u \cdot v) = g(u) \cdot g(v)$. Since f is bijective, f is in particular injective, i.e. $a = b$ if and only if $f(a) = f(b)$ for all $a, b \in G$. Therefore to verify the equality above it suffices to verify the equality after applying f, i.e. $f \circ g(u \cdot v) = f \circ g(u) \cdot f \circ g(v)$. Then the equality holds as $f \circ g = \mathrm{Id}_H$.

$\Leftarrow$: Prove the contrapositive. If f is not injective, then g cannot be well-defined; and if f is not surjective, then the domain of the composition $f \circ g$ is not the whole H.

□

Remark 1.1.10. Recall that under the context of categories, isomorphisms are defined as in Proposition 1.1.9. The same proposition implies that group isomorphisms are isomorphisms in the categorical sense.

Remark 1.1.11. If there exists an isomorphism $f : G \to H$ between groups G and H, then G and H are considered as **isomorphic**, denoted $G \cong H$. This is an equivalence relation as compositions of isomorphisms are still isomorphisms.

Definition 1.1.12. Let G be a group. Then a **subgroup** of G is a subset $H \subseteq G$, which is in it self a group; and the inclusion map $i : H \hookrightarrow G$ is a group homomorphism. H being the subgroup of G is denoted as $H \leq G$.

Remark 1.1.13. The fact that the inclusion map is required to be a group homomorphism implies that the operation in H is simply the restriction of the operation in G.

Proposition 1.1.14. Let G be a group, and $H \subseteq G$ a subset. Then the followings are equivalent:

i) H is a subgroup of G.

ii) The following three conditions are satisfied:

   1) For all $a, b \in H$, $a \cdot b \in H$.

   2) $e_G \in H$.

   3) (Under the same operation of G) $a^{-1} \in H$ for all $a \in H$.

iii) H is nonempty; and for all $x, y \in H$, $x \cdot y^{-1} \in H$.

The third condition is often used to test whether $H \subseteq G$ gives a subgroup.

Proof. Verify the following implications:

- i) $\implies$ ii). By the definition of subgroup, H together with the same operation is a group, which by the definition of group is closed w.r.t. the group; and every element should admit an inverse. By the fact that i is an inclusion, and by Proposition 1.1.6 $i(e_H) = e_G$ with $e_G = e_H$.
- ii) $\implies$ i). Check that H is a group: associativity is given by the fact that the operation is identical to that in G. and G is a group; existence of inverse and identity results directly from hypothesis 2) and 3); and the operation is defined as $H \times H \to H$ given by hypothesis 1).
- ii) $\implies$ iii). By 2) H is nonempty. For all $x, y \in H$, by 3) $y^{-1} \in H$; and by 1) $x \cdot y^{-1} \in H$ given that both x and y^{-1} are in H.
- iii) $\implies$ ii). Since H is nonempty, there exists $a \in H$. iii) implies that $a \cdot a^{-1} = e_G \in H$, giving 2). For all $a \in H$, let $x = e_G$ and $y = a$, which gives $a^{-1} \in H$, satisfying 3). For all $a, b \in H$, letting $x = a, y = b^{-1}$ gives $a \cdot b \in H$.

□

Proposition 1.1.15. Let $f : G \to H$ be a group homomorphism, then if $G' \leq G$, then $f(G') \leq H$.

Proof. Apply the result of Proposition 1.1.14. Since $G' \leq G$, $e_G \in G'$, and by Proposition 1.1.6, $f(e_G) = e_H$, giving that $f(G')$ is nonempty. For all $x, y \in f(G')$, let $u, v \in G'$ s.t. $x = f(u), y = f(v)$. Since G' is a subgroup of G, $u \cdot v^{-1} \in G'$. By Proposition 1.1.6, this implies $f(u) \cdot f(v^{-1}) = f(u) \cdot f(v^{-1}) \in f(G')$, which gives that $f(G') \leq H$. □

Proposition 1.1.16. Let $f : G \to H$ be a group homomorphism. If $H' \leq H$, then $f^{-1}(H') \leq G$. In particular, $f^{-1}(e_H) = \ker f := \{u \in G \mid f(u) = e_H\}$ is a subgroup of G.

Proof. Apply the same argument as in the above proposition. $H' \leq H \implies e_H \in H' \implies e_G \in f^{-1}(H')$, i.e. $f^{-1}(H')$ is nonempty. For all $u, v \in f^{-1}(H')$, $f(u \cdot v^{-1}) = f(u)f(v)^{-1} \in H'$ since $H' \leq H$, which implies that $u \cdot v^{-1} \in f^{-1}(H')$, i.e. $f^{-1}(H')$ is a group. □

Proposition 1.1.17. Let $f : G \to H$ be a group homomorphism. Then f is injective if and only if $\ker f = \{e_G\}$.

Proof. Proceed by showing implication in both directions:

$\Rightarrow$: Let $u \in \ker f$. Then $f(a) = f(a) \cdot e = f(a) \cdot f(u) = f(a \cdot u)$. But f being injective implies that $a = a \cdot u$, i.e. $u = e$.

$\Leftarrow$: For $u, v \in G$ s.t. $f(u) = f(v)$, we have $e = f(u) \cdot (f(v))^{-1} = f(u) \cdot f(v^{-1}) = f(u \cdot v^{-1}) \implies thatu \cdot v^{-1} \in \ker f$. But since the only element in $\ker f$ is the identity, this gives $u \cdot v^{-1} = e \implies u = v$, i.e. f is injective.

□

1.2 Group of Permutations

Definition 1.2.1. Given a set Ω, the **permutation group** is defined to be $S_\Omega := \{f : \Omega \to \Omega \mid f \text{ bijection}\}$. Since compositions of bijective maps are still bijective, defining the operation to be composition gives this a group structure.

Remark 1.2.2. Notice that the permutation group structure depends only on the cardinality of the group on which permutations are considered. Explicitly, for $\alpha : \Omega \to \Omega'$ a bijection, there exists an isomorphism between the corresponding groups of permutations: $\beta : S_\Omega \to S_{\Omega'} : f \mapsto \alpha \circ f \circ \alpha^{-1}$. This is indeed an isomorphism as this is first a group homomorphism since

$$\beta(f \circ g) = \alpha \circ f \circ g \circ \alpha^{-1} = \alpha \circ f \circ (\alpha^{-1} \circ \alpha) \circ g \circ \alpha^{-1} = \beta(f) \circ \beta(g)$$

and this being an isomorphism follows from the fact that there exists an obvious inverse $\beta^{-1} : f \mapsto \alpha^{-1} \circ f \circ \alpha$. Therefore it suffices to denote such permutation group by the cardinality of Ω: for $\Omega = \{1, \dots, n\}$ S_Ω is denoted as S_n.

Proposition 1.2.3 (Cayley). Every group can be embedded into some S_Ω. Explicitly, for group G the map $\alpha : G \to S_G$ s.t. $g \mapsto \alpha_g$ where $\alpha_g(h) = gh$ (α_g is the action of G on G defined by multiplication by g.) is an injective group homomorphism.

Proof. It suffices to syntactically check that the following requirements are satisfied:

- $\alpha_g \in S_G$. It suffices to check that indeed multiplication by an element in the group gives a bijection. This is clear as the action has an inverse, namely multiplying the inverse of that element.
- *α gives a group homomorphism.* By definition $\alpha_{gh} = \alpha_g \cdot \alpha_h$.
- *α is injective.* It suffices to check that $\ker \alpha = e_G$. This is indeed the case, as for $g \in G$ s.t. $\alpha_g = \mathrm{Id}$, $\alpha_g(e_G) = g \cdot e_G = e_G \implies g = e_G$.

□

1.3 Groups Generated by a Subset

Remark 1.3.1. If $(H_i)_{i \in I}$ is a family of subgroups of G, then $\bigcap_{i \in I} H_i$ is also a subgroup of G. This can be verified by taking an element in the intersection, and check each rule of group is satisfied in each of the H_is.

Definition 1.3.2. If $A \subseteq G$ is a subset of G, then the **subgroup generated by** A is defined as

$$\langle A \rangle := \bigcap_{A \subseteq H \leq G} H$$

Remark 1.3.3. By definition $\langle A \rangle$ is well-defined as it is described by concrete elements in the group; and as in particular $A \subseteq G \leq G$. By the previous remark, $\langle A \rangle$ is a subgroup of G. It is also the smallest subgroup that contains A.

Proposition 1.3.4. Let $A \subseteq G$ be a subset of G, then $\langle A \rangle = \{x_1 \dots x_n \mid n \in \mathbb{Z}_{>0}; \forall i, x_i \in G \text{ or } x_i^{-1} \in G\}$. For $n = 0$, define $x_1 \dots x_n = e$.

Proof. Proceed by double inclusion:

$\subseteq$: Proceed to show that RHS satisfies the definition of the Hs above. For RHS consider $n = 1$, with $x_1 \in G$ which takes all elements in G. This gives $A \subseteq$ RHS. Further use Proposition 1.1.14, which for any $x_1 \dots x_m, y_1 \dots y_n \in$ RHS, each summand of $x_1 \dots x_m (y_1 \dots y_n)^{-1} = x_1 \dots x_m y_n^{-1} \dots y_1^{-1}$ is either in A or its inverse is in A implying that RHS is a group. Definition above gives the subset relation.

$\supseteq$: It suffices to verify that any element in the specified form is in $\langle A \rangle$. This is the case as for $x_1 \dots x_n$ where for all i, either $x_i \in A$ or $x_i^{-1} \in A$, $x_i \in \langle A \rangle$ by definition, and multiplication of two elements in the group is still in the group by closure of the operation.

□

Definition 1.3.5. The following defines some common terminology for characterization of a group:

- G is **finitely generated** if there exists a finite set $A \subseteq G$ s.t. $G = \langle A \rangle$.
- G is **finite** if it has finitely many elements.
- The **order** of G, denoted $|G|$, is the number of elements in G if it is finite; or ∞ if G is not finite (infinite).
- G is **cyclic** if it attains a generating set with a single element a. In this case G is denoted as $G = \langle a \rangle$.
- The **order** of $a \in G$, denoted $|a|$ is the order of $\langle a \rangle$.

Remark 1.3.6. Cyclic groups are abelian. By the alternative definition provided in Proposition 1.3.4, $\langle a \rangle = \{a^m \mid m \in \mathbb{Z}\}$.

Proposition 1.3.7. A group G is cyclic if and only if $G \simeq \mathbb{Z}$ for G infinite, or $G \simeq \mathbb{Z}/n\mathbb{Z}$ for some $n \in \mathbb{Z}_{>0}$.

Proof. Choose $a \in G$ s.t. $G = \langle a \rangle$. Proceed via showing implication in both directions:

$\Rightarrow$: Consider $f : \mathbb{Z} \to G$ s.t. $f(1) = a$. This is a group homomorphism, Then either

- *f is injective.* By definition of cyclic groups, for any $s \in G$ there exists $m \in G$ s.t. $s = a^m$. Then $f(m) = s$ according to the definition of f, giving that f is surjective. Then this falls into the first case, giving $G \simeq \mathbb{Z}$.
- *f is not injective.* Then there are nonzero elements that are mapped to e by f. Since $\ker f \subseteq \mathbb{Z}$, there exists a smallest positive element. Define the map $f_n : \mathbb{Z}/n\mathbb{Z} \to G$ s.t. $[1] \mapsto a$. Check the followings:
  - *f_n is well-defined.* It suffices to check that if $[m_1] = [m_2]$, then $f([m_1]) = (f[m_2])$. This is indeed the case as

$$f([m_1]) = a^{m_1} \overset{!}{=} a^{m_1} \cdot a^{(m_2 - m_1)} = a^{m_2} \cdot a^{nk} = a^{m_2} \cdot (a^n)^k = a^{m_2} = f([m_2])$$

    for some $k \in \mathbb{Z}$, where $\overset{!}{=}$ holds since $[m_1] = [m_2]$ implies $n \mid (m_1 - m_2)$. This gives $a^{m_1 - m_2} = e$ since $a^n = e$.
  - *f_n is injective.* For $a \in \mathbb{Z}$ s.t. $f_n([a]) = 0$, $a = 0$ as otherwise this conflicts with the hypothesis that n is the smallest of such integers.

– f_n *is surjective.* Follows from the same argument in the case where G is infinite.

$\Leftarrow$: Since $\mathbb{Z} = \langle 1 \rangle$ and $\mathbb{Z}/n\mathbb{Z} = \langle [1] \rangle$, both of which are cyclic.

□

1.4 The Dihedral Group

Definition 1.4.1. Let $n \geq 3$, and $P_n \subset \mathbb{R}^2 \simeq \mathbb{C}$ be the regular n-gon s.t. its vertices are at the n-th roots of 1. Then the **dihedral group** D_{2n} is the group of symmetry of P_n. Alternatively, one can write

$$D_{2n} = \{\varphi \in \mathrm{GL}_2(\mathbb{R}) \mid \varphi(P_n) = P_n\}$$

Remark 1.4.2. We have a injective map $\alpha : D_{2n} \to S_n$, where $\alpha(\varphi)$ is given by the restriction of φ to the vertices of P_n. This map is injective as $\{v_1, \ldots, v_n\}$ spans $\mathbb{R}^2$. Therefore, specifying how the vertices are transformed (permuted) fixes the whole linear transformation.

Remark 1.4.3. Notice the following relations: by definition of rotation $\sigma^n = e$; and $\sigma\tau\sigma = \tau$, which implies $\sigma^{n-1}\tau = \tau\sigma$. This enables changing the sequence of applying σs and τs.

Proposition 1.4.4. For a fixed n, let σ be the operation of counter-clockwise rotation by $\frac{2\pi}{n}$ on P_n; and τ_j be the operation of symmetry w.r.t. the symmetry axis passing through the vertex j (which is a direction; invariant w.r.t. transformations on P_n). Then for every $\alpha \in D_{2n}$, it must be in the form of σ^i or $\sigma^i \cdot \tau_j$, for some $i, j \in \mathbb{Z}$.

Proof. How the operations permute the vertices is characterized by

$$\sigma : v_k \mapsto v_{k+1} \qquad \tau : v_{j+k} \mapsto v_{j-k}$$

Following the strategy of the previous remark, to fix the whole operation α it suffices to fix how vertices are transformed. Since elements of D_{2n} are linear transformations, they map line segments to line segments, and therefore adjacent vertices to adjacent vertices. Then for $v_1 \mapsto v_{i+1}$, either $v_2 \mapsto v_{i+2}$, then $\alpha = \sigma^i$; or $v_2 \mapsto v_i$, then $\alpha = \sigma^i\tau_j$. The indices are considered modulo n and then plus 1. □

Remark 1.4.5. Using Remark 1.4.3, we can check that indeed $\langle D_{2n} \rangle = D_{2n}$, by applying the remark to move all the rotations to the left of symmetries, and the reduce the expression by relations $\sigma^n = \tau^2 = e$.

1.5 Product of Groups

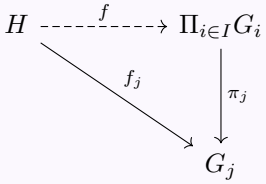
Definition 1.5.1 (Product of Groups). Suppose that we have a family of groups $(G_i)_{i\in I}$. The **product** of groups is defined as

$$\Pi_{i\in I}G_i := \{(x_i)_{i\in I} \mid x_i \in G_i \forall i \in I\}$$

with the operation defined component-wise i.e. $(x_i)_{i\in I} \cdot (y_i)_{i\in I} := (x_i y_i)_{i\in I}$.

Remark 1.5.2. By the definition of the operation, the identity in the product of groups $(G_i)_{i\in I}$ is $(e_i)_{i\in I}$ where e_i is the unique identity element in G_i; and the inverse of $(x_i)_{i\in I}$ is $(x_i^{-1})_{i\in I}$.

Proposition 1.5.3 (Universal Property of Product of Groups). Let group homomorphism $\pi_j : \Pi_{i\in I}G_i \to G_j, (x_i)_{i\in I} \mapsto x_j$ be the projections. Then given group homomorphisms $f_i : H \to G_i$ for all i, there exists a unique group homomorphism $f : H \to \Pi_{i\in I}G_i$ s.t. $\pi_i \circ f = f_i$ for all $i \in I$, i.e. the following diagram commute:



Proof. Since the diagram is required to commute, the homomorphism f can be only defined as $f(x) = (f_i(x))_{i\in I}$, which gives the uniqueness. Existence follows from the fact that f_is are group homomorphisms for all i, which implies that f is also a group homomorphism. □

Example 1.5.4 (Chinese Remainder Theorem). Let $m, n \in \mathbb{Z}_{\geq 0}$ which are relatively prime. Then there exists group isomorphism $\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$.

Proof. Consider group homomorphisms:

$$f : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, \quad [x + mn\mathbb{Z}] \mapsto [x + m\mathbb{Z}]$$

$$g : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, \quad [x + mn\mathbb{Z}] \mapsto [x + n\mathbb{Z}]$$

Check that f and g are well-defined. For f, let $a = [x + mn\mathbb{Z}] = b = [y + mn\mathbb{Z}]$. This implies that $mn \mid (x - y)$. By definition, $f(a) = [x + m\mathbb{Z}], f(b) = [y + m\mathbb{Z}]$. But this implies that $[x + m\mathbb{Z}] = [y + m\mathbb{Z}]$ as $mn \mid (x - y) \implies m \mid (x - y)$. The well-definedness of g is similar.

Use the universal property above (Proposition 1.5.3), there exists a unique $h : \mathbb{Z}/mn\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ s.t. $h_1 = f, h_2 = g$ where h_i indicates the projection to i-th field after applying h. Check that this is an isomorphism:

- h is injective. Consider the kernel of h: for all $[x + mn\mathbb{Z}] \in \ker h$, $[x + m\mathbb{Z}] = 0$ and $[x + n\mathbb{Z}] = 0$ as it must be in the kernel of both h_1 and h_2. But this implies that $m \mid x$ and $n \mid x$, i.e. $mn \mid x$, which gives $[x + mn\mathbb{Z}] = 0$. That is, elements in $\ker h$ are identically zero, which gives the injectivity.
- Notice that $\mathbb{Z}/mn\mathbb{Z}$ has mn elements, while $\mathbb{Z}/m \times \mathbb{Z}/n\mathbb{Z}$ has $m \cdot n = mn$ elements. Therefore h being injective implies h being bijective.

□

1.6 Congruence Relations

Definition 1.6.1 (Left/Right Congruence). Let G be a group, with $H \leq G$. Then for $x, y \in G$,

- x and y are **left congruent** mod H, denoted $x \equiv_\ell y \pmod{H}$ if $x^{-1}y \in H$.
- x and y are **right congruent** mod H, denoted $x \equiv_r y \pmod{H}$ if $xy^{-1} \in H$.

Remark 1.6.2. $\equiv_\ell$ and $\equiv_r$ are equivalence relations. The equivalence classes are noted as xH and Hx for $x \in G$, respectively.

Notation. If G is abelian, the operation is written additively. The congruence classes will then be denoted as $x + H$ and $H + x$ for left and right congruence classes, respectively.

Proof. The proof is similar for two equivalence relations, so we only check for left congruence:

- $\equiv_\ell$ *is Reflexive.* $x^{-1} \cdot x = e \in H$.
- $\equiv_\ell$ *is symmetric.* If $x^{-1}y \in H$, given that H is a subgroup of G, $(x^{-1}y)^{-1} \in H$. This implies that $y^{-1}x \in H$, i.e. $y \equiv_\ell x \pmod{H}$.
- $\equiv_\ell$ *is transitive.* Suppose that $x \equiv_\ell y \pmod{H}, y \equiv_\ell z \pmod{H}$. By the fact that subgroups are closed, $(x^{-1}y)(y^{-1}z) = x^{-1}z \in H$.

□

Remark 1.6.3. G is the disjoint union of equivalence classes w.r.t. $\equiv_\ell$. For $x, y \in G$ s.t. $x \equiv_\ell y \pmod{H}$, there exists $h \in H$ s.t. $x = yh$.

Proposition 1.6.4. There is a bijection between $\{xH \mid x \in G\}$ and $\{Hx \mid x \in G\}$ for all $x \in G, H \leq G$.

Proof. Define the map $\varphi : \{xH \mid x \in G\} \to \{Hx \mid x \in G\}$, $gH \mapsto Hg^{-1}$. Check that this is well-defined: for $g_1, g_2 \in G$ s.t. $g_1H = g_2H$, there exists $h \in H$ s.t. $g_1 = g_2h$. Then $\varphi(g_1H) = Hg_1^{-1} = H(g_2h)^{-1} = Hh^{-1}g_2^{-1} = Hg_2^{-1} = \varphi(g_2H)$. It has inverse $Hg \mapsto g^{-1}H$, with well-definedness similarly proved. This implies that φ is a bijection. □

Remark 1.6.5. In the prove above, we cannot define $\varphi : gH \mapsto Hg$ as in this case this is not well-defined. Specifically, if g_1 does not commute with h for $g_1 = g_2h$, $\varphi(g_2H) = Hg_1h$ which is not necessarily equal to Hg_1.

Since the number of congruence classes w.r.t. $x \in G$ does not change with choice of left or right congruence classes and depends only on H, the following definition is well-defined:

Definition 1.6.6 (Index). Let G be a group, with $H \leq G$. Then the number of distinct xH for $x \in G$ is the **index** of H in G, denoted as $(G : H)$.

Remark 1.6.7. For all $g_1, g_2 \in H$, there exists bijections $g_1H \mapsto g_2H$ and $Hg_1 \mapsto Hg_2$, given by multiplication on the left by $g_2g_1^{-1}$, and multiplication on the right by $g_1^{-1}g_2$, respectively.

Theorem 1.6.8 (Lagrange). Let G be a group. If $H \leq G$, and G is finite, then $|G| = |H| \cdot (G : H)$.

Proof. By Remark 1.6.3, G is the disjoint union of congruence classes. There are $(G : H)$ congruence classes (in the form of xH for $x \in G \setminus H$), with each having $|H|$ elements (given by $\{xh \mid h \in H\}$). □

Corollary 1.6.9. In particular, for all $H \leq G$, $|H| \mid |G|$. If G is finite, for all $g \in G$, $|\langle g \rangle| \mid |G|$, i.e. $g^{|G|} = g^{|\langle g \rangle| \cdot (G:\langle g \rangle)} = e$.

Example 1.6.10 (Fermat's Little Theorem). Let $G = (\mathbb{Z}/p\mathbb{Z})^\times$ with p prime. Then $|G| = p - 1$. For $a \in \mathbb{Z}$ s.t. $p \nmid a$, $|[a]| = p - 1$, which implies that $a^{p-1} \equiv 1 \pmod{p}$ (using the above Corollary).

We now seek to define a group structure on the congruence classes modulo a subgroup $H \leq G$. The issue is that the operation is not necessarily well-defined. The natural definition of the group operation is given via $(g_1H, g_2H) \mapsto (g_1g_2H)$. For $g_1 \equiv_\ell g_1' \pmod{H}, g_2 \equiv_\ell g_2' \pmod{H}$ we would like $g_1g_2 \equiv_\ell g_1'g_2'$. In terms of the elements, we have $g_1g_1'^{-1}g_2g_2'^{-1} \in H$ and we want $g_1g_2g_2'^{-1}g_1^{-1} \in H$. This requires extra requirements on H.

Claim 1.6.11. The following two conditions are equivalent:

- For all $g_1^{-1}g_1' \in H, g_2^{-1}g_2' \in H$, this implies $(g_1g_2)^{-1}(g_1g_2)' \in H$.
- For all $x \in G, h \in H, xhx^{-1} \in H$.

Proof. Consider the following constructions in two directions:

$\Rightarrow$ Notice $g_1^{-1}g_1 \in H$ by hypothesis. Choose $g_2^{-1} = x, g_2' = x^{-1}$.

$\Leftarrow$ Notice $(g_1g_2)^{-1}(g_1g_2)' = g_2^{-1}g_1^{-1}g_1'g_2' \in H$. Choose $g_2 = g_2' = x$, with $g_1^{-1}g_1' = h$. Such g_1 and g_1' exists by first arbitrarily choose $g_1 \in H$ then compute $g_1' = g_1h$.

□

This gives rise to the definition of normal subgroups, and the formulation quotient with respect to it, as follows.

1.7 Normal Subgroup, Quotient Group and Isomorphism Theorems

Definition 1.7.1 (Normal Subgroup). A subgroup $H \leq G$ is **normal** if for all $x \in G, xHx^{-1} \in H$, where

$$xHx^{-1} := \{xhx^{-1} \mid h \in H\}$$

Normal subgroups are denoted by $H \lhd G$.

Definition 1.7.2 (Quotient Group). Let G be a group, and $H \lhd G$. Then the **quotient group** G/H is the set of left equivalence classes w.r.t. H, together with the group operation $(g_1H)(g_2H) := (g_1g_2)H$.

Remark 1.7.3. Explicitly check that this gives a group structure: by definition we have the identity element eH, with the inverse of $g_1H = (g_1^{-1})H$. The well-definedness of the group follows from the fact that all the left congruence classes of H are well-defined, i.e. operations on it does not depends on the choice if representative, by Claim 1.6.11. This also gives a group homomorphism $\pi : G \to G/H$ with $x \mapsto xH$. This is indeed a group homomorphism as $\pi(ab) = (ab)H = aHbH = \pi(a)\pi(b)$.

Remark 1.7.4. The definition above is identical when formulated in terms of left or right congruence classes. Since we have the bijection between left and right congruence classes, to check that the definitions are identical it suffices to check that the bijection is compatible with the group operation specified. This indeed can be defined as such, as denoting the bijection to be $\Phi : xH \mapsto Hx^{-1}$ we have

$$\Phi(xH \cdot yH) = Hx^{-1} \cdot Hy^{-1} := Hy^{-1}x^{-1} = \Phi((xy)H)$$

Example 1.7.5. The followings give some examples of normal subgroups:

1. Trivially, $\{e\}$ and G are normal subgroups of G.
2. If G is abelian, for all $x \in G$, $H \leq G$, we have $xHx^{-1} = xx^{-1}H = H$ which implies that every subgroup is normal. Further the quotient G/H is abelian, as by Remark 1.7.3, the operation in G induces the operation in G/H.
3. Consider the nontrivial case, where $G = D_3 = \langle \sigma, \tau \rangle = \{e, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$. Then
   - Consider $H_1 = \langle \sigma \rangle = \{e, \sigma, \sigma^2\}$. Check $\tau\sigma\tau^{-1} = \tau\sigma\tau = \sigma^2\tau\tau = \sigma^2 \in H_1$; and $\tau\sigma^2\tau^{-1} = \tau\sigma^2\tau = \sigma\tau\tau = \sigma \in H_1$. Similarly for $\sigma\tau$ and $\sigma^2\tau$. This implies that H_1 is normal in G.
   - Consider $H_2 = \{e, \tau\}$. we have $\sigma\tau\sigma^{-1} = \sigma\tau\sigma^2 = \tau\sigma = \sigma^2\tau \notin H_2$ which implies that H_2 is not a normal subgroup.

Proposition 1.7.6. If $H \leq G$, then the following statements are equivalent:

1) H is a normal subgroup of G.
2) $gH = Hg$ for all $g \in G$, i.e. the left and right equivalence classes are equal.
3) $gHg^{-1} = H$ for all $g \in G$.

Proof. First see that statement 2) and 3) are equivalent, by right multiplying g and g^{-1}, respectively. For the rest of the equivalence, consider

- *3) $\implies$ 1).* This in particular implies that $xhx^{-1} \in H$ for all $h \in H$, which is exactly the definition of normal subgroups.
- *1) $\implies$ 3).* The definition of normal subgroups implies that $gHg^{-1} \subseteq H$ for all $g \in G$. Apply this to $g^{-1} \in G$ gives $g^{-1}Hg \subseteq H \implies H \subseteq gHg^{-1}$. Combining the two statements gives the desired equality. Alternatively, one can see that conjugating by g is an isomorphism onto its image, where inclusion in one side implies that this is bijective.

□

Corollary 1.7.7. Every subgroup with index 2 is normal.

Proof. Let $H \leq G$ be index 2. Then the left congruence classes are given by $\{H, gH\}$ for $g \in G \setminus H$; with the right equivalence classes $\{H, Hg\}$. This implies that $gH = Hg$ in terms of individual elements. By Proposition 1.7.6 this implies that H is normal in G. □

Proposition 1.7.8. Let $H \subseteq G$ be a subset. Then H is a normal subgroup in G if and only if there is some group homomorphism $f : G \to G'$ s.t. $\ker f = H$.

Proof. Consider implication in two directions:

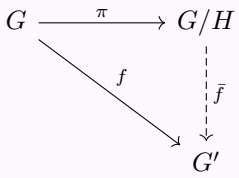
$\Rightarrow$: Consider the group homomorphism induced by the quotient structure: $\pi : G \to G/H$, $g \mapsto gH$. Then $\ker \pi = \{g \in G \mid gH = H\}$. This implies that $g \in H$.

$\Leftarrow$: By Proposition 1.1.16 H is a subgroup in G. Check that it is normal: for all $h \in H$, $g \in G$, we have

$$f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)(f(g))^{-1} = e \implies ghg^{-1} \in H$$

□

Proposition 1.7.9 (Universal Property of Quotient Group). Let G be a group, and H is normal in G. Let $\pi : G \to G/H$, and $f : G \to G'$ be group homomorphisms s.t. $H \subseteq \ker f$. Then there exists a unique group homomorphism $\bar{f} : G/H \to G'$ s.t. $\bar{f} \circ \pi = f$, i.e. the following diagram commutes:



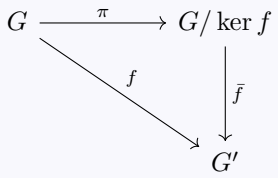
Proof. For uniqueness, notice that since the diagram is required to commute, we have $\bar{f}(gH) = f(g)$ for all $g \in G$. Since π is surjective, the behavior of $\bar{f}$ is described only on image of π, i.e. on congruence classes of form gH for $g \in G$. This gives the uniqueness of the map.

For existence, check that f is well-defined, and is indeed a group homomorphism:

- *$\bar{f}$ is well-defined.* For $gH = g'H$, we want to show that $\bar{f}(gH) = \bar{f}(g'H)$, i.e. $f(g) = f(g')$. But $gH = g'H$ implies $g^{-1}g' \in H$, i.e. $f(g) \cdot (f(g'))^{-1} = f(g \cdot g'^{-1}) \in f(H) = e$, which gives $f(g) = f(g')$.
- *$\bar{f}$ is a group homomorphism.* This is simply paraphrasing of the definition $(gH)(g'H) = (gg')H$.

□

Theorem 1.7.10 (First Isomorphism Theorem). If $f : G \to G'$ is a surjective group homomorphism, then $G' \simeq G/\ker f$, i.e. the following diagram commutes with $\bar{f}$ an isomorphism:



Proof. Uniqueness and existence of $\bar{f}$ follows from Prop 1.7.9.

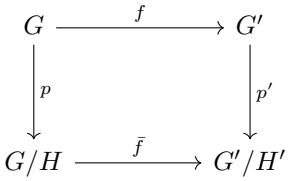
Check that $\bar{f}$ is an isomorphism. Surjectivity follows from the fact that f is surjective, and the diagram is required to commute. To check that $\bar{f}$ is injective, consider $\ker \bar{f}$. For, $x \in \ker \bar{f}$, $\bar{f}(x) = f(x') = e$ for $x' \in G$ s.t. $\pi(x') = x$. But this implies that $x' \in \ker f$, i.e. $\pi(x') = x = e$. □

Corollary 1.7.11. If $f : G \to G'$ is any group homomorphism, then $\operatorname{im} f \simeq G/\ker f$.

Remark 1.7.12. If $f : G \to G'$ is a group homomorphism, and H' is normal in G', then $f^{-1}(H')$ is normal in G.

Proof. Denote $p' : G' \to G'/H'$ which is the projection into the quotient. Notice that $p' \circ f(f^{-1}(H)) = e$, i.e. $f^{-1}H = \ker(p' \circ f)$. Proposition 1.7.8 gives that $f^{-1}(H')$ is normal. □

Remark 1.7.13. Let H and H' be normal in G and G', respectively. Let $f : G \to G'$, $p : G \to G/H$, $p' : G' \to G'/H'$ be group homomorphisms s.t. $f(H) \subseteq H'$. Then there exists a unique group homomorphism $\bar{f} : G/H \to G'/H'$ s.t. the following diagram commutes:



Proof is by applying universal property (Proposition 1.7.9) on p and $p' \circ f$. It is applicable as $f(H) \subseteq H'$, i.e. $H \subseteq \ker(p' \circ f)$.

Parenthesis 1.7.14. Let $p : G \to G/H$ be the projection into the quotient. Then if $H \leq M$, then M is normal in G if and only if $p(M) = M/H$ is normal in G/H.

Proof. Show implications in both directions:

- $\Rightarrow$ Use Remark 1.7.13, with $G = G'$, $H' = M$, and f the identity map. By hypothesis that $H \leq M$, we have $f(H) \subseteq M$. The remark says that there exists a map $\bar{f} : G/H \to G/M$, with kernel $p(M)$ by the fact that the diagram commutes. Proposition 1.7.8 gives the fact that $p(M)$ is normal in G/H.
- $\Leftarrow$ Since M/H is normal in G/H it is valid to consider the quotient $(G/H)/(M/H)$ with the projection $p' : G/H \to (G/H)/(M/H)$, which is a group homomorphism. It is then clear that $\ker(p' \circ p) = M$, i.e. M is a normal subgroup by Proposition 1.7.8.

□

Theorem 1.7.15 (Third Isomorphism Theorem). Let G a group, and H, M subgroups in G s.t. $H \leq M \leq G$. Then $(G/H)/(M/H) \simeq G/M$.

Proof. Let $p : G \to G/H$ be the projection into the quotient. Consider the group homomorphism $\alpha : G/H \to G/M$, given $xH \mapsto xM$. $\ker \alpha = \{xH \mid x \in M\} = p(M)$. By Parenthesis 1.7.14 we know that $p(M)$ is normal in G/H. The First Isomorphism Theorem (Theorem 1.7.10) gives the desired isomorphism. □

The following theorem connects the subgroups in the quotient and the subgroups in the original group:

Theorem 1.7.16 (Correspondence). Let G be a group, and H a normal subgroup in G. Then we have an *order-preserving* bijection:

$$\Phi : \{\text{subgroups in } G/H\} \longleftrightarrow \{\text{subgroups of } G \text{ containing } H\}$$

which maps normal subgroups to normal subgroups. Being *order-preserving* implies that $U \subseteq V$ if and only if $\Phi(U) \subseteq \Phi(V)$.

Proof. Define Φ as p^{-1} with p being the projection $G \to G/H$, as by the definition of quotient groups, we have $K \subseteq G/H \implies p^{-1}K \subseteq G$ by the fact that p^{-1} is order-preserving. Further by Parenthesis 1.7.14 we have $K \lhd G/H \implies p^{-1}K \lhd G$. The images are subgroups containing H, as in particular we have $p^{-1}(K) \supseteq p^{-1}(e) = H$.

Now check that the inverse of Φ exists; and the composition in two directions are both the identity. Check the followings:

- $p(p^{-1}(K)) = K$ for $K \leq G/H$. By definition $p(p^{-1})(K) \subseteq K$. The equality follows from the fact that p is surjective.
- $p^{-1}(p(M)) = M$ for $M \leq G$. $p^{-1}(p(M)) \supseteq M$ is given by definition; while $g \in p^{-1}(p(M))$ implies that $gH = xH$ for $x \in M$ as p is surjective. But this implies that $g = xh$ for some $h \in H$, i.e. $g \in M$.

□

For the formulation of the Second Isomorphism Theorem, we need to first introduce some definitions:

Definition 1.7.17. Let $B \leq G$. Then the **normalizer** of B in G is defined as

$$N_G(B) := \{g \in G \mid gBg^{-1} \subseteq B\}$$

Remark 1.7.18. By definition of normalizer, B is normal in G (the normalizer makes B a normal subgroup). This is also the largest subgroup of G in which B is normal, as suppose that there exists a larger one, it would be included in the normalizer by definition. The normalizer exists as in particular B is normal in B, implying that $B \subseteq N_G(B)$.

Notation. Let $A, B \leq G$ be subgroups. Denote

$$AB := \{ab \mid a \in A, b \in B\}$$

Remark 1.7.19. By definition AB is not necessarily a subgroup in G: for $a_1b_1, a_2b_2 \in AB$, $a_1b_1(a_2b_2)^{-1} = a_1b_1b_2^{-1}a_2^{-1}$ which is not in the form of AB. But if $A \subseteq N_G(B)$, this is the case as we have

$$a_1b_1b_2^{-1}a_2^{-1} = (a_1a_2^{-1})(a_2b_1b_2^{-1}a_2^{-1})$$

which gives $a_1b_1(a_2b_2)^{-1} = a'b'$ for $a' = a_1a_2^{-1}$ and $b = a_2b_1b_2^{-1}a_2^{-1} \in B$.

Theorem 1.7.20 (Second Isomorphism Theorem). Let A and B be subgroups of G. Further let $A \subseteq N_G(B)$. Then $A \cap B \trianglelefteq A$ and $B \trianglelefteq AB$; and we have the isomorphism $A/(A \cap B) \simeq AB/B$.

Proof. Notice $A \cap B \subseteq B$ and $A \subseteq N_G(B)$. Therefore, for all $b \in A \cap B$, $a \in A$, $aba^{-1} \in A \cap B$ by closure of operation in A and B is normal in A. Further $B \lhd AB$ as $(ab)b'(ab)^{-1} = abb'b^{-1}a^{-1} \in B$ since $a \in N_G(B)$. Consider $f : A \to AB$, $a \mapsto ab$ for some fixed $b \in B$. $\operatorname{im} f \in B$ as B is a group, and in particular $A \cap B \subseteq B$. Use the result in Remark 1.7.13 to get the following commutative diagram:

$$\begin{array}{ccc} A & \xrightarrow{\quad f \quad} & AB \\ \downarrow & & \downarrow \\ A/(A \cap B) & \xrightarrow{\quad \bar{f} \quad} & AB/B \end{array}$$

f is an isomorphism by definition, which implies that the induced homomorphism $\bar{f}$ is an isomorphism. □

1.8 The Symmetric and Alternating Group

Recall that the Symmetric group S_n is defined as

$$S_n := \{f : \{1, \dots, n\} \to \{1, \dots, n\} \mid f \text{ bijective}\}$$

with operation given by composition of maps.

Notation. For $\sigma \in S_n$, it is often denoted by the one-to-one mappings:

$$\begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

Example 1.8.1. The composition of maps can be simply read off from the relations: for example

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \mathrm{Id}$$

Definition 1.8.2 (Cycle). In S_n, for $k \geq 2$, a k-**cycle** in S_n is a permutation $\sigma = (a_1, \dots, a_k)$ for $a_1, \dots, a_k \in \{1, \dots, n\}$ where $\sigma(a_i) = a_{i+1}$ for $i < k$; and $\sigma(a_k) = a_1$; and $\sigma(i) = i$ for $i \notin \{a_1, \dots, a_k\}$.

Example 1.8.3. Adopting the notation for cycles, Example 1.8.1 can be written as $(321)(231) = e = \mathrm{Id}$.

Definition 1.8.4 (Transposition)**.** **Transposition**s in Symmetric groups are 2-cycles (ij) for $i < j$.

Remark 1.8.5. The following gives some basic properties of the Symmetric group:

1. Let $\sigma = (a_1 \dots, a_k)$ be a k-cycle. Then $|\sigma| = k$.
2. If σ and τ are disjoint cycles, i.e. the sets of elements that they act nontrivially on are disjoint, then $\sigma\tau = \tau\sigma$.
3. For all $\sigma \in S_n$, it can be written as a product of disjoint cycles, unique up to reordering. This can be constructed by chasing the image of any element x in σ, which decomposes σ into the product of a cycle and something else. The rest part of σ acts trivially on x, which implies that they are disjoint.
4. Cycle $(a_1 \dots a_k) = (a_1 a_k) \dots (a_1 a_3)(a_1 a_2)$. This implies that every $\sigma \in S_n$ can be decomposed into transpositions.

Parenthesis 1.8.6. All groups with 2 elements are isomorphic. $G = \{e, a\}$ gives $a \cdot a = e$, which implies that $G \simeq \mathbb{Z}/2\mathbb{Z}$.

Example 1.8.7. Consider symmetric groups with small n:

1. $S_1 = \{e\}$.
2. $S_2 = \{e, (12)\}$. By Parenthesis 1.8.6, this is isomorphic to $\mathbb{Z}/2\mathbb{Z}$.
3. S_3 is not abelian: Let $\sigma = (123)$, $\tau = (12)$, we have $|\sigma| = 3$, $|\tau| = 2$, and further $S_3 = \{e, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$. This implies that $S_3 \simeq D_3$.

Definition 1.8.8 (Inversion)**.** **Inversion**s in σ are elements in the set $\{(i, j) \mid 1 \le i < j \le n, \sigma(i) > \sigma(j)\}$.

Definition 1.8.9 (Signature)**.** Consider group homomorphism $\varepsilon : S_n \to \{\pm 1\}$ where the operation in $\{\pm 1\}$ is integer multiplication, defined as $\sigma \mapsto (-1)^{(\#\text{ inversions in } \sigma)}$. σ is <u>even</u> if $\varepsilon(\sigma) = 1$; and <u>odd</u> if $\varepsilon(\sigma) = -1$.

Example 1.8.10. Transpositions are odd. For $\sigma = (ij)$ with $i < j$, written out explicitly it is given by the map

$$\begin{pmatrix} 1 & \cdots & i & \cdots & j & \cdots & n \\ 1 & \cdots & j & \cdots & i & \cdots & n \end{pmatrix}$$

The inversions are given by $\{(i, k), (k, j) \mid i < k < j\} \cup \{(i, j)\}$. The first part has even elements which implies that $\varepsilon(\sigma) = (-1)^1 = -1$.

Example 1.8.11. If σ is a product of k transpositions, then $\varepsilon(\sigma) = (-1)^k$. By Remark 1.8.5 4., any k-cycle can be decomposed into $(k - 1)$ transpositions, which implies that its signature is $(-1)^{k-1}$.

Proposition 1.8.12. ε is a group homomorphism.

Proof. Consider $R = \mathbb{Q}[x_1, \ldots, x_n]$ the polynomial ring, where $\mathbb{Q}$ is a field. This gives a domain as every nonzero element in a field is invertible.

Define $\Delta := \Pi_{i<j}(x_i - x_j)$. R being a domain implies that this is nonzero. Given $\sigma \in S_n$, we can construct a map $\varphi_\sigma : R \to R$ which is a morphism of $\mathbb{Q}$-algebra (homomorphism that is $\mathbb{Q}$-linear). By the universal property of multivariate polynomial ring, to specify φ_σ, it suffices to specify the image of x_is. Define $\varphi_\sigma(x_i) = x_{\sigma(i)}$ for all i.

Notice that $\varphi_\sigma(\Delta) = \Pi_{i<j}(x_{\sigma(i)} - x_{\sigma(j)}) = \varepsilon(\sigma) \cdot \Delta$. Now consider the map $\varphi : \sigma \mapsto \varphi_\sigma$. Notice that this is a group homomorphism: in particular $\varphi_\sigma \circ \varphi_\tau = \varphi_{\sigma\tau}$ as maps are associative. Apply to Δ gives $\varepsilon(\sigma)\varepsilon(\tau) = \varepsilon(\sigma\tau)\Delta$, i.e. $(\varepsilon(\sigma)\varepsilon(\tau) - \varepsilon(\sigma\tau))\Delta = 0$. Since R is a domain, and $\Delta \neq 0$, this implies that $\varepsilon(\sigma)\varepsilon(\tau) = \varepsilon(\sigma\tau)$ which gives the desired group homomorphism. □

Definition 1.8.13 (Alternating Group). The **Alternating Group** A_n is defined as $A_n := \ker \varepsilon_n$ for $\varepsilon_n : S_n \to \{\pm 1\} \simeq S_2$

Remark 1.8.14. For $n \geq 2$, transpositions exist, which implies that ε is surjective, with $e \mapsto 1, \tau \mapsto -1$ for τ some transposition. The First Isomorphism Theorem (Theorem 1.7.10) gives that $S_n/A_n \simeq \mathbb{Z}/2\mathbb{Z}$.

1.9 Classification of Groups of Small Order

Proposition 1.9.1. If G is a finite group, and $|G| = p$ which is prime, then $G \simeq Z/p\mathbb{Z}$.

Proof. Choose $x \in G$ s.t. $x \neq e$. Denote $H = \langle x \rangle$. Clearly $|H| \geq 2$, as in particular both x and e are in H. By Lagrange, $|H| \mid p$, which implies that $H = G$, i.e. G is cyclic. Proposition 1.3.7 gives the desired isomorphism. □

The proposition above gives that for $p = 2, 3, 5, 7$, the group of order p is isomorphic to the corresponding $\mathbb{Z}/p\mathbb{Z}$. The following classifies group of order 4 and 6:

Proposition 1.9.2. For group G with order 4, either $G \simeq \mathbb{Z}/4\mathbb{Z}$, or $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Proof. Consider the following two cases:

- There exists some $x \in G$ s.t. $|x| = 4$, i.e. G is cyclic. Then by Proposition 1.1.9, $G \simeq \mathbb{Z}/4\mathbb{Z}$.
- G is not cyclic. Lagrange's Theorem gives that for all $x \in G$, $|x| \mid 4$, where the only nontrivial case is $|x| = 2$. Then $G = \{e, a, b, c\}$ with $a^2 = b^2 = c^2 = e$. Notice $ab \neq a, b, e$, which implies that $c = ab$. This characterization gives the isomorphism to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ given by $a \mapsto (1, 0)$ and $b \mapsto (0, 1)$

□

Remark 1.9.3. In the proof above, notice $ba \neq e, a, b$, i.e. $c = ab = ba$. Therefore it is abelian. This is often referred to as the Klein 4-gruop.

Now consider the case where G has 6 elements:

Proposition 1.9.4. If $|G| = 6$, then either $G \simeq \mathbb{Z}/6\mathbb{Z}$, or $G \simeq D_3$.

Proof. Consider the two cases separately:

- G is abelian. By Proposition 1.3.7, $G \simeq \mathbb{Z}/6\mathbb{Z}$.
- G is not abelian. Lagrange gives that for all $x \in G$ s.t. $x \neq e$, $|x| = 2$ or 3.

  Lemma 1.9.5. If $|G|$ is even, there exists an element of order 2 in G.

  Proof. Suppose not. Then in particular there cannot exist any element of even order, i.e. for all $x \in G$, $x^{-1} \neq x$. Then consider pairs (x, x^{-1}) for all x. Together with e, this gives odd number of elements, which is a contradiction. □

  Claim that there exists $x \in G$ s.t. $|x| = 3$. Suppose not. Then for all $x \in G, x^2 = e$. By proof for the case where there are 4 elements in the group, this gives that G is abelian, i.e. it has a subgroup $\{e, x, y, xy\}$ for $x, y \neq e$. But this gives a contradiction with Lagrange's Theorem.

  Let $|\sigma| = 3$. This gives the explicit expression of elements in G: $G = \{e, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$. Notice that $\tau\sigma \neq e, \tau, \sigma, \sigma^2$ by the fact that they are nontrivial and have different order. Then either

  - $\tau\sigma = \sigma\tau$. But then $(\sigma\tau)^2 = \sigma^2 \neq e$, $(\sigma\tau)^3 = \tau$, which implies that $(\sigma\tau)$ generates G. This is a contradiction.
  - $\tau\sigma = \sigma^2\tau$. Then this characterize that $G \simeq D_3$.

□

Theorem 1.9.6 (Structural Theorem for Finitely Generated Abelian Groups). Let G be a finitely generated abelan group. Then

$$G \simeq \mathbb{Z}^r \times \Pi_{i \in I}(\mathbb{Z}/p_i^{m_i}\mathbb{Z})$$

for $r \in \mathbb{Z}_{\geq 0}$, p_i prime, $m_i \in \mathbb{Z}_{>0}$; and pairs (p_i, m_i) are unique up to reordering.

The proof quite resembles that of Structural Theorem for finitely generated modules over PIDs, and is not repeated here.

Remark 1.9.7. Since $\mathbb{Z}$ has infinitely many elements, this implies that if G being a finitely generated abelian group is finite, then $r = 0$, and $G \simeq \Pi_{i \in I}\mathbb{Z}/p_i^{m_i}\mathbb{Z}$.

Example 1.9.8. Structural theorem directly gives the classification of isomorphism classes of abelian groups with 8 elements: $\mathbb{Z}/8\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}, \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

1.10 Group Action on Sets

Definition 1.10.1 (Group Action). Let G be a group, and X a set. A **(left) action** of G on X is a map $G \times X \to X$, written $(g, x) \mapsto gx$, satisfying

- $ex = x$ for all $x \in X$.
- $g_1(g_2x) = (g_1g_2)x$ for all $g_1, g_2 \in G$, $x \in X$.

Proposition 1.10.2. Left (and therefore right) group actions correspond to group homomorphisms $\varphi : G \to S_X$, where $S_X := \{f : X \to X \mid f \text{ bijection}\}$ is the set of bijective maps from X to itself.

Proof. Notice that $\varphi_e = \mathrm{Id}$; and for all $g, h \in G$, $\varphi_g \circ \varphi_h = \varphi_{gh}$ for all $g, h \in G$, which gives $\varphi_g \circ \varphi_{g^{-1}} = \varphi_e = \mathrm{Id}$. Therefore, taking S_X as a group, with the identity being the identity map, and operation the composition of maps, φ gives a group homomorphism between g and S_X.

For the other direction, given a group homomorphism $\varphi : G \to S_X$, we get a left action on X given by $(g, x) \mapsto \varphi(g)(x)$. □

Example 1.10.3. The following gives some examples of group actions:

1. Recall that S_X attains a group structure. Therefore, for all X, S_X acts on X by $(f, x) \mapsto fx$ with the corresponding homomorphism $S_X \to S_X$.
2. Consider geometrically, D_n acts on the vertices of a regular n-gon.
3. Let G be a group, and $H \leq G$. Then we have an action of G on the left congruence classes of G modulo H, given by $(g, aH) \mapsto (ga)H$. Check that this is well-defined: if $aH = bH$, want to show that $(ga)H = (gb)H$. Hypothesis gives that $aH = bH$, i.e. $a^{-1}b \in H$. But $(ga)^{-1}(gb) = a^{-1}g^{-1}gb = a^{-1}b \in H$, which gives the equality $(ga)H = (gb)H$.
4. A group acts on itself via the action of conjugation, given by $(g, x) \mapsto gxg^{-1}$. Clearly, $(e, x) \mapsto exe^{-1} = x$; and $(gh, x) \mapsto (ghxh^{-1}g^{-1}) = (g, (h, x))$.

Definition 1.10.4. Let $x, y \in X$. Then for a group action of G on X, $x \sim y$ if there exists $g \in G$ s.t. $gx = y$.

Remark 1.10.5. This is an equivalence relation:

- *Reflexive.* let $g = e$.
- *Symmetric.* Suppose that there exists g s.t. $gx = y$. Then multiplying g^{-1} on th left gives $g^{-1}(gx) = g^{-1}y$, i.e. $x = g^{-1}y$.
- *Transitive.* Suppose that there exists $g, h \in G$ s.t. $y = gx$, $z = hy$, then $z = (hg)x$.

Definition 1.10.6 (Orbit). Let there be an action of G on X. the **orbit** of $x \in X$ is defined as

$$\mathcal{O}(x) = \{g(x) \mid g \in G\}$$

Definition 1.10.7 (Stabilizer). For all $x \in X$, the **stabilizer** of x is

$$\mathrm{Stab}_G(x) := \{g \in G \mid gx = x\}$$

Remark 1.10.8. The stabilizer $\mathrm{Stab}_G(x)$ is a subgroup of G. Use the characterization of subgroups:

- By definition of group action, $e \in \mathrm{Stab}_G(x)$, which is the unit element.
- If $g, h \in G$, then $gx = x \implies x = g^{-1}x$, i.e. $g^{-1} \in G$. Therefore $g^{-1}h \in G$.

Lemma 1.10.9. For all $x \in X$, there is a bijection

$$(G/\mathrm{Stab}_G(x))_\ell \longleftrightarrow \mathcal{O}(x)$$

where $(G/\mathrm{Stab}_G(x))_\ell$ denotes the left congruence classes of $\mathrm{Stab}_G(x)$. In particular, $|\mathcal{O}(x)| = (G : \mathrm{Stab}_G(x))$, i.e. if G is finite, then $|\mathcal{O}(x)| \mid |G|$.

Proof. Notice that $gx = hx$ implies that $(g^{-1}h)x = x$, i.e. $g^{-1}h \in \mathrm{Stab}_G(X) \implies g\mathrm{Stab}_G(x) = h\mathrm{Stab}_G(x)$; and the implication in the inverse direction is similar. This gives a bijection $\{gx \mid x \in G\} \to (G/\mathrm{Stab}_G(x))_\ell$ given by $gx \mapsto g\mathrm{Stab}_G(x)$. □

Definition 1.10.10 (Transitive). The action of G on X is **transitive** if there is only one orbit, i.e. for all $x, y \in X$, there exists some $g \in G$ s.t. $x = gy$.

Corollary 1.10.11. If the action of G on X is transitive, then for all $x \in X$, $\mathcal{O}(x) = X$. Let $H = \mathrm{Stab}_G(x)$, then there exists a bijection $(G/H)_\ell \to X$ given by $gH \mapsto gx$. This corresponds to the action of G on $(G/H)_\ell$: $(g, aH) \mapsto (ga)H$.

Remark 1.10.12. If G acts on X, then $X = \amalg_{i \in I}\mathcal{O}(x_i)$, where x_is are representatives in each orbit. In particular this can be split as

$$|x| = \sum_{x_i} |\mathcal{O}(x_i)| = |\mathrm{Fix}(x)| + \sum_{|\mathcal{O}(x_i)| \geq 2} |\mathcal{O}(x_i)|$$

where $\mathrm{Fix}(x) := \{x \in X \mid gx = x,\ \forall g\}$, i.e. points that are stabilized by the whole group.

Definition 1.10.13 (Center). Let G be a group. The **center** of g is defined as

$$Z(G) := \{x \in G \mid xg = gx,\ \forall g \in G\}$$

Definition 1.10.14 (Centralizer). Given $x \in G$, the **centralizer** of x in G is defined as

$$C_G(x) := \{g \in G \mid xg = gx, \text{i.e. } gxg^{-1} = x\}$$

i.e. in which x is in the center. One can also consider the centralizer of a subgroup in a similar manner.

Example 1.10.15. Fix G a group, and consider the action of G on itself by conjugation. x and y are conjugate if $\mathcal{O}(x) = \mathcal{O}(y)$, i.e. there exists $g \in G$ s.t. $x = gyg^{-1}$. In particular, in this case the stabilizers are the same as the centralizers.

Notice that with the action defined as conjugation, $|\mathcal{O}(x)| = 1$ if and only if $x \in Z(G)$. This gives the class equation

$$|G| = |Z(G)| + \sum_i (G : C_G(x_i)) \tag{1.1}$$

where x_i vary over the set of conjugate classes with more than 1 element.

Definition 1.10.16 (p-group)**.** If p is a prime integer, a **p-group** is a group of order p^m for some $m \geq 1$.

Proposition 1.10.17. If G is a p-group, then $Z(G) \neq \{e\}$. Further by the class equation, $p \mid Z(G)$.

Proof. Consider divisibility by p on both sides of the class equation. For the second term on RHS, for all i s.t. $G \neq C_G(x_i)$, since $C_G(x_i)$ is a subgroup by Lagrange $(G : C_G(x)) \mid |G| = p^m$. Further as $G \neq C_G(x_i)$, $p \mid (G : C_G(x))$, $|G| = p^m$ gives $p \mid |G|$, which implies that $p \mid |Z(G)|$. □

Corollary 1.10.18. If p is prime, then every group with p^2 elements is abelian:

Proof. By structrual theorem, either $G \simeq \mathbb{Z}/p^2\mathbb{Z}$, or $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Since G is a p-group, by Proposition 1.10.17, $p \mid |Z(G)|$. Lagrange gives $|Z(G)| \mid p^2$. Then either:

- $|Z(G)| = p^2$. Then G is by definition abelian.
- $|Z(G)| = p$. Notice that $Z(G) \trianglelefteq G$. Consider the group $G/Z(G)$. This has p elements, and is therefore cyclic. Let $xZ(G)$ be a generator of $G/Z(G)$. Then for all $a, b \in G$, there exists $i, j \in \mathbb{Z}$ and $a', b' \in Z(G)$ s.t. $a = x^i a'$, $b = x^j b'$. But notice that $ab = ba$, i.e. G is abelian, which is a contradiction.

□

Remark 1.10.19. The above result cannot be generalized. That is, for $H \triangleleft G$, H abelian and G cyclic, G is not necessarily abelian. Consider the counterexample where $G = S_3$, $H = \langle \sigma \rangle = \{e, \sigma, \sigma^2\}$.

Remark 1.10.20. If G acts on X, G also acts on $\mathcal{P}(X)$, the power set of X. Explicitly, for $A \in \mathcal{P}(X)$, $gA = \{gx \mid x \in A\}$. This also extends to the conjugacy of a subset in a similar manner.

If X is a group (e.g. G itself) then this gives a group automorphism, which sends subgroups by subgroups, via left-composing with a group element.

1.11 Sylow Theorems

Lagrange gives that for a finite group G and $H \leq G$, $|H| \mid |G|$, and $|x| \mid |G|$ for all $x \in G$. It is then of our interest to see how much we can get in the other direction: given a group G, can we get any information the order of its subgroups, and the number of them?

It is impossible that we have the followings:

- For all $m \mid |G|$, there exists $x \in G$ s.t. $|x| = m$. For example, it is impossible to have such x for $m = |G|$ in G non-cyclic.
- For all $m \mid |G|$, there exists a subgroup of G of order m. In particular, in a subsequent theorem (Theorem 1.13.3) we will show that A_5 has non nontrivial normal (e.g. index-2) subgroups, i.e. no subgroup of order 30.

Theorem 1.11.1 (Cauchy). For G a finite group, and p prime s.t. $p \mid |G|$, there exists $x \in G$ s.t. $|x| = p$.

Proof. First consider the simple case where G is abelian, and then reduce the general case to the abelian one.

Case 1. G is abelian. Follows from the structural theorem for finite abelian groups: G is isomorphic to a product of groups where one of them is $\mathbb{Z}/p^m\mathbb{Z}$ for $m \in \mathbb{Z}_{>0}$. This gives an element with order p.

Alternatively, prove by contradiction. Suppose that for all $x \in G$, $|x| \neq p$. Then for all $x \in G$, $p \nmid |x|$. (Otherwise for $|x| = m$ and $p \mid m$, $\left|x^{m/p}\right| = p$.) Let N be the largest common multiple of all order of elements in G, then $(p, N) = 1$. Let $x_1, \dots, x_n$ be the elements of G. Consider the group homomorphism

$$f : \mathbb{Z}^n \to G, \qquad f(a_1, \dots, a_n) = x_1^{a_1} \cdots x_n^{a_n}$$

Notice that if $(a_1, \dots, a_n) \in H := \{(b_1, \dots, b_n) \mid N \mid b_i, \forall i\}$, then $f(a_1, \dots, a_n) = e$ since $|x_i| = a_i \mid N \implies x_i^N = e$. This implies that $H \subseteq \ker f$. Using the universal property of quotient groups, we have a group homomorphism

$$\bar{f} : \mathbb{Z}^n/H \simeq (\mathbb{Z}/N\mathbb{Z})^n \to G, \qquad \overline{(a_1, \dots, a_n)} \mapsto x_1^{a_1} \cdots x_n^{a_n}$$

Since taking $a_i = 1$ and $a_{j(\neq i)} = 0$ gives x_i, $\bar{f}$ is surjective. the first isomorphism theorem gives $G \simeq (\mathbb{Z}/N\mathbb{Z})^n / \ker(\bar{f})$. Lagrange gives $|G| \mid |\mathbb{Z}/N\mathbb{Z}|^n = N^n$, which gives a contradiction as $p \mid |G| \mid N^n$, but $(p, N) = 1$ by hypothesis.

Case 2. G is not necessarily abelian. Argue by induction on the order of the group:

- *Base case.* $|G| = 1$. The statement is vacuous as the hypothesis is not satisfied.
- *Inductive step.* Suppose that the theorem is true for all groups G' with $|G'| < |G|$. Use the class equation

$$|G| = |Z(G)| + \sum_i (G : C_G(x_i)) \qquad \text{where } x_i \text{ runs over set of representatives of conjugacy classes}$$

If we can find a subgroup $H < G$ s.t. $p \mid |H|$, then we can find $x \in H < G$ of order p by induction hypothesis, which by definition also has order p in G.

Now assume that $p \nmid |H|$ for all $H < G$. Lagrange gives $p \mid (G : H)$ for all H as $p \mid |G|$. In particular, for all representative of conjugacy classes x_i, $p \mid (G : C_G(x_i))$, and by class equation we have $p \mid Z(G)$. Since $Z(G) \lhd G$, this gives a contradiction.

□

Corollary 1.11.2. If G is a finite group and p is a prime, then G is a p-group if and only if the order of any element in G is a power of p.

Proof. $\Rightarrow$: Lagrange. $\Leftarrow$: Cauchy, via considering the quotient by subgroup generated by any element recursively. □

Definition 1.11.3 (p-Sylow Subgroup)**.** Let G be a finite group with order $|G| = p^m n$ for p prime, and $(n, p) = 1$. A **p-Sylow subgroup** is a subgroup $H \leq G$ satisfying $|H| = p^m$.

Theorem 1.11.4 (Sylow I)**.** Let G be a finite group and p a prime. If $p \mid |G|$, then G has a p-Sylow subgroup

Proof. Apply induction on $|G|$. The theorem is vacuous for $|G| = 1$. Now assume that for all G' s.t. $|G'| < |G|$ the theorem holds.

Case 1. $p \mid Z(G)$. By the result from the abelian case of Cauchy, there exists $g \in Z(G)$ s.t. $|g| = p$. Let $k = \langle g \rangle$. Then $K \trianglelefteq G$ as in particular $K \leq Z(G)$. Consider $G' = G/K$, and apply the inductive hypothesis. Since $|G| = p^m n$, either $m = 1$, where K gives the desired p-Sylow group; or for $m > 1$ since $|K| = p$, $|G'| = p^{m-1} n < |G|$. Inductive Hypothesis gives that there exists a p-Sylow subgroup $H' \leq G'$ with $|H'| = p^{m-1}$. Use this in the quotient to construct a p-Sylow subgroup in G: Let $\pi : G \to G/K$ be the quotient, and consider $H = \pi^{-1}(H')$. Notice that $K = \pi^{-1}(e) < \pi^{-1}(H') = H$, and $H' \simeq H/K$. Lagrange gives $|H| = |H'| \cdot p = p^m$, which implies that H is a p-Sylow subgroup.

Case 2. $p \nmid |Z(G)|$. Consider again the class equation

$$|G| = |Z(G)| + \sum_i (G : C_G(x_i)) \qquad \text{where } x_i \text{ runs over set of representatives of conjugacy classes}$$

Since $|G| = p^m n$, in particular $p \mid |G|$. By divisibility, there exists x_i s.t. $p \nmid (G : C_G(x))$. Since $C_G(x_i) \leq G$, hyperref[thm: Lagrange]Lagrange gives $p \mid C_G(x_i)$, i.e. $|C_G(x_i)| = p^m q$ for $q < n$ (otherwise $x_i \in Z(G)$, which falls back to the first case). In particular, $|C_G(x_i)| < |G|$. Apply the inductive hypothesis gives that there exists a p-Sylow subgroup in $C_G(x_i)$, which by counting the order is also a p-Sylow subgroup in G.

□

Remark 1.11.5. Sylow I implies Cauchy, as by the existence pf a p-Sylow subgroup using Corollary 1.11.2 the order of any element must be a power of p; and there is only one element of order 1 (the unit). We present the prove in such sequence as we have used Cauchy in the proof of Sylow I.

Theorem 1.11.6 (Sylow II)**.** For G a finite group, and p a prime s.t. $p \mid |G|$. For $K \leq G$ any p-subgroup and $H \leq G$ any p-Sylow subgroup, then there exists $a \in G$ s.t. $K \subseteq aHa^{-1}$.

Corollary 1.11.7. For H and H' p-Sylow subgroups of G, there exists $a \in G$ s.t. $H' = aHa^{-1}$ (by argument on order). That is, p-Sylow subgroups conjugate into each other.

Theorem 1.11.8 (Sylow III)**.** Let n_p be the number of p-Sylow subgroups in G. Then

1) $n_p \equiv 1 \pmod{p}$.

2) $n_p = (G : N_G(H))$ for any H that is a p-Sylow subgroup. Since $H \leq N_G(H) \leq G$, in particular by Lagrange we have $n_p \mid \frac{|G|}{|H|}$.

Remark 1.11.9. More generally, for all $H \leq K \leq G$ we have $(G : H) = (G : K) \cdot (K : H)$ for G finite, via counting the elements.

Proof of Theorem 1.11.6 and 1.11.8. We first prove a general result, and then use it to show both Sylow II and Sylow III.

Consider the action of G on subgroups of G by conjugation. Given $H' \leq G$, by definition we have $\mathrm{Stab}_G(H') = N_G(H')$. Fix a p-Sylow subgroup H of G. Let $\mathcal{H} = \{H = H_1, \dots, H_r\}$ be the orbit of H under conjugation of elements in G. Let $A \leq G$ a p-subgroup, and consider the inclusion

$$L = A \cap N_G(H)/A \cap H \hookrightarrow N_G(H)/H = R$$

Since A is a p-subgroup, L can be identified as a subgroup of A, whose order is a power of p. On the other hand, $|R| = \frac{|N_G(H)|}{|H|} \mid \frac{|G|}{|H|} \nmid p$. Further Lagrange gives $|L| \mid |R|$, i.e. $L = \{e\} \implies A \cap N_G(H) = A \cap H$.

Conjugation induces an action of A on $\mathcal{H}$. After reordering, let $H_1, \dots, H_s \in \mathcal{H}$ be the representatives of the orbits of the action. Then

$$r = \sum_{i=1}^{s} |\mathcal{O}(H_i)| = \sum_{i=1}^{s} (A : \mathrm{Stab}(H_i)) = \sum_{i=1}^{s} (A : A \cap N_G(H_i)) = \sum_{[} i = 1]^{s} (A : A \cap H_i)$$

Now use the equality above to prove the theorems:

1) Take $A = H$. Since for all i, $|H_i| = |H|$, $H \subseteq H_i$ if and only if $i = 1$. Further since A is a p-group, $(A : A \cap H_i)$ is a power of p for all i. This gives $r \equiv 1 \pmod{p}$ (Sylow III 1)).

2) Take $A = K$ in Sylow II. By the construction in 1), there exists $i \leq s$ s.t. $A \subseteq H_i$. This proves Sylow II.

3) By Sylow II any two p-Sylow subgroups are conjugate, which implies that $r = n_p$ and that there is only one orbit for such H_i. Then

$$r = |\mathcal{O}(H)| = \frac{|G|}{|\mathrm{Stab}_G(H)|} = (G : \mathrm{Stab}_G(H)) = (G : N_G(H))$$

□

Definition 1.11.10 (Characteristic Subgroup)**.** A subgroup $H \leq G$ is a **characteristic subgroup** of G if it is preserved by any $\sigma \in \mathrm{Aut}(G)$.

Remark 1.11.11. In Sylow III, suppose that $n_p = 1$, and let H be the unique p-Sylow subgroup. Since $\sigma \in \mathrm{Aut}(G)$ maps subgroups to subgroups, $|\sigma(H)|$ is also a p-Sylow subgroup (as p-Sylow subgroups are constrained by only cardinality). This implies that $\sigma(H) = H$, i.e. H is a characteristic subgroup of G.

Example 1.11.12. Let G be a finite group, with $H \trianglelefteq G$. Suppose that $p \mid |H|$. Let K be the unique p-Sylow subgroup of H. Then $K \trianglelefteq G$ as $g \in G$ gives $\sigma \in \mathrm{Aut}(H)$ which preserves K. However, in general from $K \trianglelefteq H$ and $H \trianglelefteq G$ we cannot necessarily get $K \trianglelefteq G$.

1.12 Application of Sylow Theorems

Sylow theorems, especially Sylow III, gives constraints on the number of p-Sylow subgroups. This, together with the constraint of the order of the group, could reveal the group structure with little extra information.

The first application involves classifying groups with order a product of two primes.

Proposition 1.12.1. Let G be a group of order pq, with p and q distinct primes, and $p < q$. If $n_p = 1$, then G is abelian and cyclic.

Proof. Notice first that $n_q = 1$ as by Sylow III $n_q \mid \frac{|G|}{q} = p$, and $n_q \not\equiv 1 \pmod q$. Since $p < q$, $n_q = 1$.

Therefore in G we have a unique p- and q-Sylow subgroup. Let them be P and Q, with p and q elements, respectively. Since $n_p = 1$, by Corollary 1.11.7 $P \trianglelefteq G$. Consider the map

$$\varphi : Q \to \mathrm{Aut}(P) \qquad y \mapsto (x \mapsto (yxy^{-1}))$$

This is indeed an automorphism on P as P is normal in G. Since both P and Q has prime order, they are both cyclic. Then $\varphi \simeq (\mathrm{Hom}(\mathbb{Z}/q\mathbb{Z}, \mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})))$ where LHS has q elements and RHS has $(p-1)$ elements. Lagrange implies that $|\mathrm{im}\ \varphi| \mid (p-1)$ and $|\mathrm{im}\ \varphi| \mid (q)$ as $\mathrm{im}\ \varphi$ is a subgroup of Q and $\mathrm{Aut}(P)$. Since q is prime, and $q > p > p-1$, $|\mathrm{im}\ \varphi| = 1$, i.e. for all $x \in P, y \in Q$, $yxy^{-1} = x \implies yx = xy$, that is elements in P and Q commute.

Since both P and Q are cyclic, there exists $x \in P$ and $y \in Q$ s.t. $P = \langle x \rangle, Q = \langle y \rangle$. Consider the order of pq: let it be m, i.e. $(xy)^m = e$. This gives $x^m = y^{-m} = (y^m)^{-1}$. Lagrange gives $|P \cap Q| \mid p, q$, which implies that $|P \cap Q| = 1$, $P \cap Q = \{e\}$. Further notice that $x^m, (y^m)^{-1} \in P \cap Q$, which gives $p \mid m, q \mid m \implies pq \mid m$, i.e. $pq \mid |xy|$. Using the fact that $|xy| \mid |G| = pq$ we get $|xy| = pq$. Therefore, $G = \langle pq \rangle$, which is cyclic. □

Proposition 1.12.2. Let G be a group of order pq, with p and q distinct primes, and $p < q$. If $q \equiv 1 \pmod p$ (i.e. n_p is not necessarily 1), then there exists non-abelian group G with order pq.

Proof. Construction of non-abelian groups often results from maps as they generally do not commute.

Consider $(\mathbb{Z}/q\mathbb{Z})^\times$ with order $(q-1)$. Since $p \mid (q-1)$, Cauchy gives that there exists $r \in \mathbb{Z}$ s.t. $r \not\equiv 1 \pmod q$, and $r^p \equiv 1 \pmod q$ (i.e. r is a nontrivial element in $\mathbb{Z}/q\mathbb{Z}$ with order p). Consider

$$\alpha, \beta : \mathbb{Z}/q\mathbb{Z} \to \mathbb{Z}/q\mathbb{Z} \qquad \alpha : x \mapsto (x+1) \qquad \beta : x \mapsto \bar{r}x$$

Since q is prime, $\bar{r}$ has an inverse for all r, which implies that α and β are bijections. Further notice that $|\alpha| = q$, $|\beta| = |\bar{r}| = p$. Notice

$$\beta\alpha\beta^{-1}(x) = \bar{r}(\bar{r}^{-1}x + 1) = x + \bar{r} \implies \beta\alpha = \alpha^r\beta$$

which does not necessarily commute. This gives a non-abelian group with order pq:

$$\langle \alpha, \beta \rangle = \{\alpha^i\beta^j \mid i \in [\![0, q-1]\!], j \in [\![0, p-1]\!]\}$$

□

Remark 1.12.3. Up to isomorphism, this is the only non-abelian group of order pq. The only adjustment that we can make is to vary r; but to maintain its order p, it can only vary through the primitive p-th roots in $\mathbb{Z}/q\mathbb{Z}$; and we have the isomorphism via varying r.

The second application uses Sylow Theorems to count elements, which narrows down the possibilities of the structure of a particular group.

Proposition 1.12.4. Suppose that G is a group, with $|G| = 30 = 2 \cdot 3 \cdot 5$. Then there is an index-2 subgroup H.

Proof. Let P and Q be the p-Sylow subgroups with 3 and 5 elements, respectively. They exist by Sylow I.

Case 1. $P \trianglelefteq G$ (or $Q \trianglelefteq G$, respectively). By the Second Isomorphism Theorem we have $P/P \cap Q \simeq PQ/Q$. This is applicable as we have $Q \leq N_G(P) = G$. Use with the corresponding result for Q we get $|P \cap Q| \mid 3, 5 \implies |P \cap Q| = 1$. Then $|PQ| = |P| \cdot |Q| = 3 \cdot 5 = 15$ which gives a valid H,

Case 2. Neither P or Q is normal in G. Sylow II gives $n_3(G) > 1$, and $n_5(G) > 1$. Since $|G| = 30$, we have $n_5(G) \mid \frac{30}{5} = 6 \implies n_5(G) = 6$ since $n_5(G) \equiv 1 \pmod 5$. Similarly we get $n_3(G) = 10$. Since any two 5-Sylow subgroups have intersection $\{e\}$, G has $6 \times (5-1) = 24$ elements of order 5. Similarly G has $10 \times (3-1) = 20$ elements of order 3. But then G has at least $20 + 24 = 44 > 30$ elements, which is a contradiction.

□

1.13 Finite Simple Groups

Consider G a finite group, with $H \lhd G$. We would like to build G with H and G/H. In the opposite direction, we would like to know when the group cannot be further decomposed in this manner.

Definition 1.13.1 (Simple). A group G is **simple** if $G \neq \{e\}$, and there does not exist a normal subgroup H s.t. $H \neq G$ and $H \neq \{e\}$.

Proposition 1.13.2. An abelian group G is simple if and only if $G \simeq \mathbb{Z}/p\mathbb{Z}$ for p prime.

Proof. Since G is abelian, every subgroup is normal. Therefore, G is simple if and only if it has non nontrivial subgroups. $G \neq \{e\}$ implies that for all $x \in G$, $x \neq e$, $\langle x \rangle = G$, then $G \simeq \mathbb{Z}/n\mathbb{Z}$. Suppose that $n = pq$ for $p, q \neq 1$, then $|x^p| = \frac{n}{p} < n$.

Converse is clear: $\mathbb{Z}/p\mathbb{Z}$ only has trivial proper subgroups for p prime, by divisibility. □

Theorem 1.13.3. If $n \geq 5$, then A_n is simple.

Remark 1.13.4. For $n = 1, 2$, $A_n = \{e\}$, which is trivial. For $n = 3$, $A_3 \simeq \mathbb{Z}/3\mathbb{Z}$ which is simple since 3 is a prime.

For $n = 4$, we have $\{e\} \lhd K_4 \lhd A_4$, where K_4 embeds into A_4 via

$$H = \{e, (12)(34), (13)(24), (14)(23)\} = \{\sigma \in A_4 \mid \sigma^2 = e\}$$

> which is a subgroup preserved by conjugation.

Proof of Theorem 1.13.3. Proceed via induction:

- *Base case.* $n = 5$. $|A_5| = 3 \cdot 4 \cdot 5 = 60$. Argue by contradiction: suppose that there exists $H \trianglelefteq A_5$, with $H \neq A_5$, $H \neq \{e\}$.

Case 1. $5 \mid |H|$. First notice that $n_5(A_5) > 1$, as we have two distinct 5-cycles $\langle (12345) \rangle, \langle (13425) \rangle$. By divisibility there exists a 5-Sylow subgroup in H, which is also a 5-Sylow subgroup in A_5. Since $H \trianglelefteq A_5$, and by Sylow II all p-Sylow subgroups conjugate into each other, all 5-Sylow subgroups in A_5 are also in H. In particular, this implies that $n_5(H) = n_5(A_5) > 1$, and Sylow III gives

$$n_5(A_5) \mid \frac{60}{5} = 12, n_5(A_5) \equiv 1 \pmod 5 \implies n_5(A_5) = 6$$

which gives that H has $6 \times (5-1) = 24$ elements of order 5. Further by Lagrange $5 \mid |H| \mid 60$, giving $|H| = 30$. By the intermediate result in Proposition 1.12.4 any group of order 30 can only have one subgroup of 5 elements, which is a contradiction.

Case 2. $5 \nmid |H|$. Then by Lagrange $|H| \nmid 12$. Since H is nontrivial, $|H| \in \{2, 3, 4, 6, 12\}$. First reduce to the case where there exists $H \lhd A_5$ with $|H| \in \{2, 3, 4\}$:

- If $|H| = 12$, then $n_3(H) \mid \frac{12}{3} = 4$, $n_3(H) \equiv 1 \pmod 3$. Either
  - $n_3(H) = 1$. By Sylow II $n_3(A_5) = 1$, i.e. there exists a normal subgroup of A_5 of order 3.
  - $n_3(H) = 4$. Then there are $4 \times (3-1) = 8$ elements of order 3. Furthermore, $n_2(H) \mid \frac{12}{2} = 6$, $n_2(H) \equiv 1 \pmod 2$. Then $n_2(H) = 1$ or 3. Suppose that $n_2(H) = 3$, then there are $3 \times (2-1) = 3$ elements of order 2. Consider the subgroup generated by the product of an element of order 2 and an element of order 3. The order of the product is divisible by 2 and 3, i.e. we have an element of order 6, which is a contradiction as we have too many elements in H. Therefore there exists a unique 2-Sylow subgroup; and similarly by Sylow II $n_2(A_5) = 1$.

Now for the case where $|H| \in \{2, 3, 4\}$, Consider the group G/H where $G = A_5$, with order $|G/H| \in \{15, 20, 30\}$. Seek to get a contradiction with the hypothesis:

> **Claim 1.13.5.** There exists $K \trianglelefteq G/H$ nontrivial with $5 \mid |K|$.

Proof. Consider the cases separately:

- $|G/H| = 30$. By Proposition 1.12.4 there exists $K \trianglelefteq G/H$ with $|K| = 15$.
- $|G/H| = 15$. Using Sylow III we have

  $$n_5(G/H) \mid \frac{15}{5} = 3, n_5(G/H) \equiv 1 \pmod 5 \implies n_5(G/H) = 1$$

  By Corollary 1.11.7 the 5-Sylow subgroup is a normal subgroup in G/H.
- $|G/H| = 20$. Same as above we have

  $$n_5(G/H) \mid \frac{20}{5} = 4, n_5(G/H) \equiv 1 \pmod 5 \implies n_5(G/H) = 1$$

  which gives a normal subgroup of order 5.x

□

Now use the claim. By Correspondence, there exists $K' \leq G$ s.t. $K \simeq K'/H \trianglelefteq G/H$ which is nontrivial. This gives $K' \trianglelefteq G$ and $5 \mid |K| \implies 5 \mid |K'| = |K| \cdot |H|$, i.e. K' is a normal subgroup in G with order divisible by 5, which is a contradiction.

- *Inductive step.* For $n \geq 6$, we know that A_{n-1} is simple; and we want to show that A_n is simple.

  Argue by contradiction. Suppose that we have $H \triangleleft A_n$ with $H \neq \{e\}$. Let $G_i = \{\sigma \in A_n \mid \sigma(i) = i\} \leq G = A_n$. $G_i \simeq A_{n-1}$, which by inductive hypothesis is simple. For each $1 \leq i \leq n$, consider $H \cap G_i \trianglelefteq G_i$ (this is normal since $H \triangleleft G$). This is a subgroup, which can be only either G_i or $\{e\}$, as G_i is simple.

Case 1. There exists i s.t. $H \cap G_i = G_i$, i.e. $G_i \subseteq H$. This implies that $G_j \subseteq H$ for all j: Consider $\tau \in A_n$, then

$$\tau G_i \tau^{-1} = \{\sigma \in A_n \mid \tau^{-1}\sigma\tau \in G_i \Leftrightarrow \sigma\tau(i) = \tau(i)\}$$

i.e. $\tau G_i \tau^{-1} = G_{\tau(i)}$. But since $G_i \subseteq H \trianglelefteq G$, $\tau G_i \tau^{-1} \subseteq H$ which gives $G_j \subseteq H$ for all j. On the other hand, $\langle G_1, \dots, G_n \rangle = A_n$; and for $\sigma \in A_n$, we can write $\sigma = \sigma_1 \dots \sigma_n$ where each σ_i is the product of two transpositions. Since $n \geq 5$, any such product of two transpositions lies in some G_i. Then $\sigma \in \langle G_1, \dots, G_n \rangle = A_n \subseteq H$ which implies that $A_n \subseteq H$. Contradiction.

Case 2. $H \cap G_i = \{e\}$ for all i. This gives that for $\sigma_1, \sigma_2 \in H$ satisfying $\sigma_1(i) = \sigma_2(i) = j$, then $\sigma_1 \sigma_2^{-1} \in G_j$; and since $H \cap G_j = \{e\}$, $\sigma_1 = \sigma_2$.

Let $\sigma \in H \setminus \{e\}$. Write that as a product of disjoint cycles. Then either

* There exists a cycle of length at least 3, i.e. there exists a_1, a_2, a_3 s.t. $\sigma = (a_1 a_2 a_3) \cdots$. Take $\tau \in A_n$ s.t. τ fixes a_1, a_2 but not a_3. This indeed exists as $n \geq 5$, so after fixing two elements there can still exist cycle of length 3. Then

  $$\tau\sigma\tau^{-1} = (a_1 a_2 \sigma(a_3)) \quad \text{as product of disjoint cycles}$$

  Since H is normal, $\tau\sigma\tau^{-1} \in H$; but we have $\tau\sigma\tau^{-1}(a_1) = \sigma(a_1)$ with $\tau\sigma\tau^{-1} \neq \tau$ as they do not agree on a_3, which is a contradiction.

* σ is a product of disjoint transpositions. Since $n \geq 6$, we can write

  $$\sigma = (a_1 a_2)(a_3 a_4)(a_5 a_6)$$

  Let $\tau = (a_1 a_2)(a_3 a_5)$, and by the same reasoning as above $\sigma' = \tau\sigma\tau^{-1} \in H$. σ and σ' agrees on a_1 but disagrees on a_3, which gives a contradiction.

□

We then give a statement of the famous theorem classifying finite simple groups. The proof is far beyond the scope of this course and is omitted.

Theorem 1.13.6 (Classification of Finite Simple Groups)**.** Every finite simple group is isomorphic to one of the followings:

1. $\mathbb{Z}/p\mathbb{Z}$ with p prime, $p \in \mathbb{Z}_{>0}$.
2. A_n, $n \geq 3$.
3. Finite groups of Lie type: these occur in several series given by taking $\mathbb{F}_q$-points of certain algebraic groups, where $\mathbb{F}_q$

is the finite field of q elements.

Example 1.13.7. Consider the projective special linear group $\mathrm{PSL}_n(\mathbb{F}_q)$ for $n \neq 2, q \neq 2, 3$. This is defined as:

$$\mathrm{SL}_n(\mathbb{F}_q) = \{A \in M_n(\mathbb{F}_q) \mid \det A = 1\} \qquad \mathrm{PSL}_n(\mathbb{F}_q) = \mathrm{SL}_n(\mathbb{F}_q)/\{A = \lambda \mathrm{Id} \mid \lambda^n = 1\}$$

where the group in the quotient $\{A = \lambda \mathrm{Id} \mid \lambda^n = 1\}$ is the center of $\mathrm{SL}_n(\mathbb{F}_q)$.

4. 26 sporadic (isolated) groups, considered via embedding in $\mathrm{GL}_n(K)$ for some field K.

1.14 Composition Series and the Jordan Hölder Theorem

With the introduction of simple groups, given an arbitrary group one may want to decompose it into simple groups.

Definition 1.14.1 (Composition Series). If G is a finite group, a **composition series** of G is a sequence of subgroups

$$\{e\} = G_0 \leq G_1 \leq \cdots \leq G_n = G$$

satisfying

1) $G_{i-1} \lhd G_i$ for $1 \leq i \leq n$.

2) G_i/G_{i-1} is simple.

Remark 1.14.2. Notice that since normality of groups is not transitive, G_{i-1} is not necessarily normal in G; and this is not required by the definition.

Proposition 1.14.3. Every finite group has a composition series

Proof. Apply induction on $|G|$:

- $|G| = 1$. Then $G = G_0 = \{e\}$.
- $|G| > 1$. Then either
  - G is simple. Then $G_0 = \{e\} \lhd G_1 = G$.
  - G is not simple. Then there exists $N \lhd G$, $N \neq \{e\}$. Notice that $|N|$ and $|G/N|$ are both smaller than $|G|$. Applying inductive hypothesis we have the composition series

$$\begin{cases} N_0 = \{e\} \lhd \cdots \lhd N_p = N \\ K_0 = \{e\} \lhd \cdots \lhd K_q = G/N \end{cases}$$

By Correspondence, for all $i \leq q$, $K_i = H_i/N$ for some $H_i \leq G$. This gives a composition series:

$$N_0 \lhd \cdots \lhd N_p \lhd H_1 \lhd \cdots \lhd H_q$$

Check that this is indeed a composition series: $H_{i-1} \lhd H_i$ as $K_{i-1} \lhd K_i$. Second Isomorphism Theorem gives $H_i/H_{i-1} \simeq K_i/K_{i-1}$ which is simple.

□

The composition series characterizes the group structure up to reordering of the subgroups, by the following theorem:

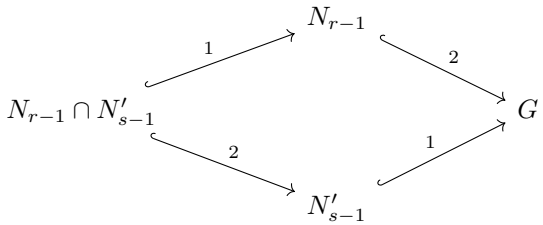
Theorem 1.14.4 (Jordan-Hölder). If we have two composition series of G

$$\begin{cases} \{e\} = N_0 \leq \cdots \leq N_r = G \\ \{e\} = N_0' \leq \cdots \leq N_s' = G \end{cases}$$

Then $r = s$, and $N_k/N_{k-1}, N_m'/N_{m-1}'$ are pairwise isomorphic after reordering.

Proof. Apply induction on $\min\{r, s\}$. Without loss of generality let this be r:

- $r = 0$ is trivial. $r = 1$ is the case where G is simple.
- $r \geq 2$, with the inductive hypothesis holds for smaller rs. Then either
  - $N_{r-1} = N_{s-1}'$. Then the result follows from inductive hypothesis for $\min\{r-1, s-1\}$.
  - $N_{r-1} \neq N_{s-1}'$. Consider the following map



Since both N_{r-1} and N_{s-1}' are normal in G, we have $N_{r-1} \leq N_{r-1}N_{s-1}' \trianglelefteq G$. Since G/N_{r-1} is simple, and $N_{r-1} \neq N_{r-1}N_{s-1}'$, $N_{r-1}N_{s-1}' = G$. Similarly $N_{s-1}'N_{r-1} = G$. Using the Second Isomorphism Theorem we get the following isomorphisms:

$$N_{r-1}/(N_{r-1} \cap N_{s-1}') \simeq G/N_{s-1}' \qquad N_{s-1}'/(N_{r-1} \cap N_{s-1}') \simeq G/N_{r-1} \tag{$*$}$$

Also by the definition of the composition series and the isomorphisms above, both the quotients 1 and 2 in the commutative diagram are simple.

Now let $M_1 \leq \cdots \leq M_k = N_{r-1} \cap N_{s-1}'$ be a composition series. This together with N_{r-1} or N_{s-1}' gives a composition series as well. Inductive hypothesis gives $k + 1 = r - 1 = s - 1$. Use the isomorphisms in ($*$) to get the conclusion.

□

1.15 Solvable Groups

Using the composition series we could further describe the structure of a group, via adding constraints on its "composition series" (as we will see, such properties do not require each successive quotient is simple). This and the next section introduces two such

formalizations, the solvable groups and nilpotent group. We will see in the last part of the course, that solvable groups are related to the solvability of polynomials.

Definition 1.15.1. Solvable A group G is **solvable** if there exists a finite sequence of subgroups

$$\{e\} = G_0 \trianglelefteq \cdots \trianglelefteq G_r = G$$

s.t. G_i/G_{i-1} is abelian for all $1 \leq i \leq r$.

Remark 1.15.2. Equivalently, we can require that each G_i/G_{i-1} should be cyclic, or isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for p prime, in the case where G is finite. This is indeed the case, as subgroups of abelian groups are normal; and applying the Structural Theorem for Abelian groups gives the desired result.

Example 1.15.3. The following gives some examples for solvable groups:

1) Every abelian group is solvable, by taking $G_1 = G$.
2) D_n is solvable since it contains an abelian group of index 2, i.e. the subgroup generated by σ, using the notation in Remark 1.4.3.
3) For $n \geq 5$, A_n is not solvable, as by Theorem 1.13.3 it is simple; but not abelian.
4) S_4 is solvable as we have the sequence of subgroups $\{e\} \trianglelefteq K_4 \trianglelefteq A_4 \trianglelefteq S_4$.

Proposition 1.15.4. Let $N \subseteq G$. Then

i) If G is solvable, then N is solvable.
ii) If $N \trianglelefteq G$, and G is solvable, then G/N is solvable.
iii) If $N \trianglelefteq G$, and both N and G/N are solvable, then G is solvable.

Proof. Verify the assertions respectively:

i) Suppose that G is solvable. Then there exists a sequence of subgroups

$$\{e\} = G_0 \trianglelefteq G_1 \trianglelefteq \cdots \trianglelefteq G_r = G \quad \text{s.t. } G_i/G_{i-1} \text{ is abelian for all } 1 \leq i \leq r$$

Now consider the sequence of subgroups of N

$$\{e\} = G_0 \cap N \trianglelefteq G_1 \cap N \trianglelefteq \cdots \trianglelefteq G_r \cap N = G \cap N = N$$

Check that this gives the sequence which satisfies the definition of solvable groups:

- $G_{i-1} \cap N \trianglelefteq G_i \cap N$. This results from $G_{i-1} \trianglelefteq G_i$ and $N \trianglelefteq G$; and in particular $G_i \cap N \subseteq G_i$ and $G_i \subseteq G$.
- $(G_i \cap N)/(G_{i-1} \cap N)$ is abelian. Check the map

$$\psi : (G_i \cap N)/(G_{i-1} \cap N) \to G_i/G_{i-1} \qquad (G_{i-1} \cap N)x \mapsto G_{i-1}x$$

Notice that $\ker\psi \subseteq G_{i-1}$; and by definition $x \in G_i \cap N \subseteq N$. Therefore ψ is injective; and since G_i/G_{i-1} is abelian $(G_i \cap N)/(G_{i-1} \cap N)$ is also abelian.

ii) Let G decompose into the same sequence of subgroups. Consider now

$$N = G_0N \leq G_1N \leq \cdots G_rN = G$$

Claim: $G_{i-1}N \trianglelefteq G_iN$. This holds as $G_{i-1} \trianglelefteq G_i$, i.e. for all $x \in G_i$, $g \in G_{i-1}$, $xgx^{-1} \in G_{i-1}$. Since N is normal in G, and $G_i \subseteq G$, $G_{i-1}N$ has a group structure. Consider the conjugation: for all $n, n' \in N$

$$(xn')^{-1}(gn)(xn') = (n')^{-1}x^{-1}gnxn' = (n')^{-1}(x^{-1}gx)(x^{-1}nx)n'$$

where all the multiplicands are in $G_{i-1}N$ as a group.

For abelianity, consider similarly the map

$$G_i/G_{i-1} \to G_iN/G_{i-1}N, \qquad G_{i-1}x \mapsto G_{i-1}Nx$$

which is surjective as for $G_{i-1}Nx \neq e$, $x \notin G_{i-1}N$, which in particular implies that $x \notin G_{i-1}$. Therefore G_i/G_{i-1} being abelian implies that $G_iN/G_{i-1}N$ is abelian.

iii) Suppose that both N and G/N are solvable. Then we have two sequences

$$\begin{cases} \{e\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_r = N \\ N/N = H_0/N \trianglelefteq H_1/N \trianglelefteq \cdots \trianglelefteq H_s/N = G/N \end{cases}$$

Then we have the sequence for G:

$$\{e\} = N_0 \trianglelefteq N_1 \trianglelefteq \cdots \trianglelefteq N_r \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_s = G$$

with normality and abelianity following from the Third Isomorphism Theorem.

□

Corollary 1.15.5. Proposition 1.15.4 i) gives S_n is not solvable for $n \geq 5$, as in particular we have $A_n \leq S_n$, with A_n not abelian but simple for $n \geq 5$.

Definition 1.15.6 (Commutator). Let G be a group. The **commutator** of G is

$$G^{(1)} := \langle [x,y] := xyx^{-1}y^{-1} \mid x, y \in G \rangle =: [G,G]$$

Remark 1.15.7. $G^{(1)}$ is a characteristic subgroup of G, as for all $\sigma \in \mathrm{Aut}(G)$ we have $\sigma([x,y]) = [\sigma(x), \sigma(y)]$. In particular, $G^{(1)}$ is normal in G. The abelianization of G is the group $G^{\mathrm{ab}} := G/G^{(1)}$ which is abelian since two elements in G do not commute if and only if their commutator is in $G^{(1)}$.

Definition 1.15.8 (Derived Series)**.** Given a group G, its **derived series** is defined as

$$G^{(0)} = G, \quad G^{(i)} = [G^{(i-1)}, G^{(i-1)}] \quad \text{for all } i > 0$$

Proposition 1.15.9. A group G is solvable if and only if there exists r s.t. $G^{(r)} = \{e\}$.

Proof. Proceed via showing implication in both directions:

$\Rightarrow$ Suppose that we have a sequence of subgroups

$$\{e\} = G_r \trianglelefteq G_{r-1} \trianglelefteq \cdots \trianglelefteq G_0 = G$$

s.t. G_i/G_{i-1} is abelian for all i. Claim that $G^{(i)} \subseteq G_i$ for all i. Suppose that this is true, then $G^{(r)} \subseteq G_r = \{e\} \implies G^{(r)} = \{e\}$. To prove the claim, apply induction on i. For $i = 0$ this is clear. For $i > 0$, since G_{i-1}/G_i is abelian, for all $x, y \in G_{i-1}$, $[x, y] \in G_i$, i.e. $[G_{i-1}, G_{i-1}] \subseteq G_i$. Now use the inductive hypothesis to get

$$G^{(i)} = [G^{(i-1)}, G^{(i-1)}] \subseteq [G_{i-1}, G_{i-1}] \subseteq G_i$$

$\Leftarrow$ The derived series gives the sequence where every subsequent group is normal in the larger group. Further by Remark 1.15.7 every successive quotient is abelian.

□

1.16 Nilpotent Groups

Definition 1.16.1 (Upper Central Series). Given a group G, its **upper central series** is given by

$$Z_0(G) = \{e\} \quad Z_1(G) = Z(G) \trianglelefteq G \quad Z_i(G)/Z_{i-1}(G) \simeq Z(G/Z_{i-1}(G))$$

Remark 1.16.2. From the definition of subsequent central series, which is based on the center of the quotient, $Z_i(G) \trianglelefteq G$; and the inclusion is given by $Z_{i-1}(G) \leq Z_i(G)$, i.e. opposite from the inclusion of derived series.

Definition 1.16.3 (Nilpotent). A group G is **nilpotent** if there exists r s.t. $Z_r(G) = G$. The smallest such r is the **nilpotent index**.

Remark 1.16.4. Every nilpotent group is solvable, as the upper central series gives the corresponding series required for a group to be solvable. In particular, $Z_i(G)/Z_{i-1}(G) \simeq Z(G/Z_{i-1}(G))$ is abelian; and center of a group is a normal subgroup.

Example 1.16.5. The following gives some (counter-)examples of nilpotent groups:

1. S_3 is not nilpotent, as $Z(S_3) = \{e\}$.
2. Every abelian group is nilpotent with index ≤ 1.
3. Every p-group is nilpotent. Recall that by using a divisibility argument in the class equation, any p-group has a nontrivial center. Lagrange gives that $G/Z(G)$ is either $\{e\}$ or also a p-group. The construction can continue as long as $G/Z(G) \neq \{e\}$, which gives a sequence. This must terminate as G is finite; and each subsequent group shrinks in order.

Proposition 1.16.6. A group G is nilpotent if and only if there exists a sequence

$$\{e\} = G_0 \leq G_1 \leq \cdots \leq G_r = G \quad \text{s.t. } G_i/G_{i-1} \subseteq Z(G/G_{i-1}) \text{ for all } 1 \leq i \leq r$$

Proof. Verify the implication in both directions:

$\Rightarrow$ By definition the upper central series gives a such sequence.

$\Leftarrow$ First notice that $G_{i-1} \trianglelefteq G$ for all i, since the inclusion gives G_i is contained in the center of a quotient of G. Show inductively that $G_i \leq Z_i(G)$, which implies that $Z_r(G) \geq G_r = G$.

For $i = 0$ this is trivial. For $i = 1$ this is clear as we have inclusion instead of equality. Now suppose that $G_i \leq Z_i(G)$ for a fixed i. Consider the group homomorphism

$$\psi : G/G_i \to G/Z_i(G), \qquad xG_i \mapsto xZ_i(G)$$

This is surjective by $G_i \leq Z_i(G)$. Then $\psi(Z(G/G_i)) \subseteq Z(G/Z_i(G))$ as group homomorphism preserves commutativity. Then

$$\psi(G_{i+1}/G_i) \subseteq \psi(Z(G/G_i)) \subseteq Z(G/Z_i(G)) \simeq Z_{i+1}(G)/Z_i(G)$$

which gives a map from G_{i+1} to Z_{i+1}, i.e. $G_{i+1} \leq Z_{i+1}$.

□

Similar to Proposition 1.15.4, we have the corresponding relations for nilpotent groups. The proof is also similar and is therefore omitted.

Proposition 1.16.7. Let $N \leq G$. Then

i) If G is nilpotent, then N is nilpotent.

ii) If N is normal in G, and G is nilpotent, then G/N is nilpotent.

iii) If $N \leq Z(G)$, and both N and G/N are nilpotent, then G is nilpotent.

Theorem 1.16.8. Let G be a finite group. Let $p_1, \ldots, p_r$ be the primes dividing $|G|$; and $P_1, \ldots, P_r$ the corresponding p-Sylow subgroups, then the following statements are equivalent:

1) G is nilpotent.

2) For all $H < G$, $H < N_G(H)$ (inequality here).

3) For all i, $P_i \lhd G$.

4) $G \simeq P_1 \times \cdots \times P_r$.

Proof. Proceed via showing the implication cyclically:

- *1) $\implies$ 2).* Argue by applying induction on $|G|$. For $|G| = 1$ the statement is clear. For $|G| > 1$, we can assume $|H| > 1$ ($N_G(\{e\}) = G$). Then either
  - $Z(G) \not\subseteq H$. Then for all a there exists $a \in Z(G) \setminus H$ satisfying $a \in N_G(H) \setminus H$.
  - $Z(G) \subseteq H$. Proposition 1.16.7 gives $G/Z(G)$ nilpotent, as $Z(G) \trianglelefteq G$. Further since G is nilpotent, $Z(G)$ is nontrivial, giving $|G/Z(G)| < |G|$. The result follows from applying inductive hypothesis on $H/Z(G) \leq G/Z(G)$.
- *2) $\implies$ 3).* We need to show that $N_G(P_i) = G$ for all i. It suffices to show that $N_G(P_i) = N_G(N_G(P_i))$, and by 2) we have 3).

  This is indeed true, as by definition P_i is normal in $N_G(P_i)$. By Sylow II since p-Sylow subgroups conjugate into each other, this is the unique p-Sylow subgroup in $N_G(P_i)$. As group automorphisms fix the order the group, P_i is a characteristic subgroup in $N_G(P_i)$. In particular, conjugation in G fixes P_i, giving $P_i \trianglelefteq N_G(N_G(P_i)) \subseteq N_G(P_i)$; and the inclusion in the other direction is by definition.
- *3) $\implies$ 4).* First prove a general result:

  Parenthesis 1.16.9. Given a group G with H and K its normal subgroups. Then $G \simeq H \times K$ if and only if $H \cap K = \{e\}$, and $G = HK$.

  Proof. Verify using the universal property of product of groups:

  $\Rightarrow$ Suppose that $G \simeq H \times K$. Then $e_G = (e_H, e_K)$; and for all $G \ni g = (g_H, g_K) = (g_H, e_K)(e_H, g_K)$.

$\Leftarrow$ For any two group homomorphisms $\psi_H : L \to H, \qquad \psi_K : L \to K$. This gives a map

$$\psi : L \to G, \qquad x \mapsto \psi_H(x)\psi_G(x)$$

This is well defined, as $H \cap K = \{e\}$ implies that every element in G decomposes uniquely into a product of two elements from H and K.

□

The parenthesis can be easily generalized to the product of finitely many groups. Now use it to prove the implication: notice that for any $i \neq j$, $P_i \cap P_j = \{e\}$ as this is a subgroup whose order divides both p_i and p_j. Further $G = P_1 \cdots P_r$, as $P_1 \cdots P_r \subseteq G$; and $|G| = |P_1| \cdots |P_r|$ gives the equality.

- *4) $\Longrightarrow$ 1).* By Example 1.16.5 iii), P_is are all nilpotent. Since r is finite we only need to show that if H_1 and H_2 are nilpotent, then $H_1 \times H_2$ is nilpotent. This is indeed true, as
  - $Z(H_1 \times H_2) \simeq Z(H_1) \times Z(H_2)$.
  - $(H_1 \times H_2)/Z(H_1 \times H_2) \simeq H_1/Z(H_1) \times H_2/Z(H_2)$.

  which allows construction of the sequence for $H_1 \times H_2$ based on the sequences of H_1 and H_2.

□

1.17 Free Groups*

A general in the categorical perspective is, whether its structure can be "naturally derived" from its elements.

Definition 1.17.1 (Free Object). Given a category $\mathscr{C}$, in which objects are sets (probably with extra structure, e.g. groups, modules, etc.). A **free object** X associated to a set S is an object where we have the identification of morphisms:

$$\{X \to Y \text{ morphisms in } \mathscr{C}\} \leftrightarrow \{\text{map of sets } S \to Y\}$$

Example 1.17.2. Let $\mathscr{C}$ be the category of abelian groups, and I an arbitrary set. The corresponding free objects are $\mathbb{Z}^{(I)}$, which has a $\mathbb{Z}$-basis $\{e_i \mid i \in I\}$, indexed by elements in I.

If $\mathscr{C}$ is the category of rings, and $I = \{1, \ldots, n\}$, the corresponding free object is $\mathbb{Z}[x_1, \ldots, x_n]$.

The motivation of constructing a free group, is to give a group with only a system of generators S (a set) with "no other relations". We need some setup before giving the definition:

Definition 1.17.3 (Word). Given a set S, choose a set S^{-1} that has a bijection φ with S. For $x \in S$, denote $\varphi(x) =: x^{-1} \in S^{-1}$. Choose also a special element 1 with $1^{-1} = 1$. Define $\widetilde{S}$ as $\widetilde{S} := S \sqcup S^{-1} \sqcup \{1\}$.

A **word** (with letters) in S is given by an $\mathbb{N}$-tuple $(x_1, x_2, \ldots, x_n, \ldots)$ s.t. $x_i \in \widetilde{S}$, and there exists i_0 s.t. $x_{i_0} = 1$ for all $i > i_0$ (or equivalently, the tuple is finite; but we need the lagging 1s to define the group operation)

Definition 1.17.4 (Reduced Word). A **reduced word** $(x_1, x_2, \dots)$ is a word satisfying

1) $x_i = 1 \implies x_j = 1$ for all $j > i$.

2) For all i, $x_{i+1} \neq x_i^{-1}$ unless $x_i = 1$.

Definition 1.17.5 (Free Group). The free group $F(S)$ on set S is the set of reduced words on S, with operation given as follows:

Given $u, v \in F(S)$, write

$$u = (u_1, u_2, \dots, u_p \neq 1, 1, 1, \dots) \quad v = (v_1, v_2, \dots, v_q \neq 1, 1, 1, \dots)$$

If $w = (u_1, u_2, \dots, u_p, v_1, v_2, \dots, v_q, 1, 1, \dots)$ is a reduced word, then define this as $u \cdot v$. Otherwise, $u_p = v_1^{-1}$. Then replace $w = (u_1, u_2, \dots, u_{p-1}, v_2, \dots, v_q, 1, 1, \dots)$ until it is reduced. This process will terminate as both p and q are finite.

Associativity is clear. We have the identity $(1, 1, \dots)$; and the inverse of $(x_1, \dots, x_n, 1, 1, \dots)$ is $(x_1^{-1}, \dots, x_n^{-1}, 1, 1, \dots)$.

Notice we have the reduced word $(1, 1, \dots)$; and we have the injective map

$$S \sqcup S^{-1} \to F(S) \quad x \mapsto (x, 1, 1, \dots)$$

i.e. S is a subset of $F(S)$.

Further, if $u = (x_1, \dots, x_n, 1, 1, \dots)$ is a reduced word, then

$$u = (x_1, 1, \dots)(x_2, 1, \dots)\cdots$$

Proposition 1.17.6. For all group G, the following map is a bijection:

$$\{\text{group homomorphisms } F(S) \to G\} \to \{\text{functions } S \to G\}, \quad \varphi \mapsto \varphi|_S$$

Proof. Let $f : S \to G$ be any function. Since S generates $F(S)$ as a group, the uniqueness of the group homomorphism $\varphi : F(S) \to G$ extending f is clear, via extending in terms of a system of generators. Therefore, we only need to check existence: define

$$\varphi : F(S) \to G, \quad \varphi(x_1, \dots, x_n, 1, 1, \cdots) = u(x_1) \cdots u(x_n) \quad \text{where } u_i = \begin{cases} f(x_i) & x_i \in S \\ (f(x_i))^{-1} & x_i \in S^{-1} \end{cases}$$

This is well defined as 1 is in both S and S^{-1}, and clearly this is a group homomorphism. Definition gives $\varphi|_S = f$. □

Remark 1.17.7. Let $\alpha : S \to T$ be any map. Proposition 1.17.6 gives that there exists a unique group homomorphism $F(\alpha)$ that makes the following diagram commute:

$$\begin{array}{ccc} S & \xrightarrow{\alpha} & T \\ \downarrow & & \downarrow \\ F(S) & \xrightarrow{F(\alpha)} & F(T) \end{array}$$

Moreover, if we have another map $\beta : T \to U$, we have $F(\beta \circ \alpha) = F(\beta) \circ F(\alpha)$; and $F(\alpha)$ is a group isomorphism if α is a bijection. Therefore, $F(S)$ is unique up to isomorphism, and depends only on the cardinality of S.

Example 1.17.8. The free group is very complex; and we can only clearly classify the free groups with S of small cardinality.

1) $S = \emptyset$. Then $F(S) = \{e\}$.
2) $|S| = 1$. Then $F(S) \simeq \mathbb{Z}$.
3) $|S| = 2$. Then elements of $F(S)$ take the form of $x^{a_1}y^{a_2}x^{a_3}\dots$ with $a_i \in \mathbb{Z}$.

We have the following theorem whose proof is from topology and is omitted:

Theorem 1.17.9 (Schreier)**.** Every subgroup of a free group is free.

1.18 Presentation of Groups*

Fix a group G and let $S \subseteq G$ be a subset. Proposition 1.17.6 gives that there exists a unique group homomorphism $\varphi : F(S) \to G$ extending the inclusion $S \hookrightarrow G$. This is surjective if and only if $\langle S \rangle = G$. In this case, we would like to understand $\ker \varphi$, as $G \simeq F(S)/\ker \varphi$.

Definition 1.18.1 (Normal Closure)**.** Given any group H, and subset $A \subseteq H$, the **normal closure** of A is defined as

$$\bigcap_{A \subseteq H' \trianglelefteq H}, \quad \text{or equivalently} \quad \{xax^{-1} \mid x \in H, a \in A\}$$

This is the smallest normal subgroup containing A.

Definition 1.18.2 (Presentation of Group)**.** A **presentation** of a group G by generators and relations is given by

1) A set S with the group homomorphism $F(S) \to G$ induced by the inclusion $S \to G$ being surjective.
2) A subset $R \subseteq F(S)$ s.t. if K is the normal closure of R in $F(S)$, then we have the induced isomorphism $F(S)/K \simeq G$.

Example 1.18.3. Let G be the dihedral group D_n with $n \geq 3$. Recall that we have the rotation σ of order n, and symmetry τ of order 2; and we have the relation $\tau\sigma = \sigma^{n-1}\tau$. Then G is presented by

$$\langle \sigma, \tau \mid \sigma^n = e, \tau^2 = e, \tau\sigma = \sigma^{n-1}\tau \rangle$$

which is indeed the case as the cardinality of the group given by the presentation is at most $2n$.

Remark 1.18.4. Typically the presentation we give is simpler than the restriction required by the whole group, i.e. R is much smaller than K.

Remark 1.18.5. In general, it is very hard to see the group structure with the generators and relations. For example, the isomorphism problem, i.e. given the presentation of G_1 and G_2, to determine whether $G_1 \simeq G_2$ is undecidable.

Definition 1.18.6 (Finitely Presented). A group G is **finitely presented** if there is a presentation by generators and relations consisting of finitely many generators and relations.

Proposition 1.18.7. Every finitely group G is finitely presented.

Proof. Consider $S = G$. This extends to $\varphi : F(S) = F(G) \to G$ surjective. Let $A \subseteq F(G)$ be the set $\{(g_1, g_2, \dots, g_n, 1, \cdots) \mid g_n^{-1} = g_1 \cdots g_{n-1}\}$. A is clearly finite; and $A \subseteq \ker \varphi$. Let K be the normal closure of A. This gives a surjective map $\bar{\varphi} : F(G)/K \to G$. Let $B = \{\bar{g} \in F(G)/K \mid g \in G\}$ which is the presentation. Notice that $\bar{g_1}\bar{g_2} = \overline{g_1 g_2}$, which implies that $(\bar{g})^{-1} = \overline{(g^{-1})}$ for all $g \in G$. Since B is closed on taking inverses and multiplication, B is a subgroup. Further since B generates $F(G)/K$, $B = F(G)/K$. But $|B| \leq |G|$; and together with φ surjective we have $|B| = |G|$; and φ is a bijection. □

Chapter 2

Representation of Finite Groups

2.1 Complex Representation

The motivation of introducing the representation of G is to have a linearized version of group action on sets. Recall that we have the correspondence between action of G on a set X and group homomorphism $G \to S_x$ where S_x is the group of bijective maps on S, with the operation defined as composition. Explicitly, this is given by

$$\varphi : G \times X \to X \quad \rightsquigarrow \quad G \to S_x,\ g \mapsto \varphi(g, -) : (X \to X)$$

We now give the formal definition on vector spaces:

Definition 2.1.1 (Representation)**.** A **(complex) representation** of a group G is a vector space V over $\mathbb{C}$, together with a group homomorphism

$$\rho : G \to \mathrm{GL}(V) := \{\varphi : V \to V \mid \varphi \ \mathbb{C}\text{-linear isomorphism}\}$$

Equivalently, a representation of G is a vector space V over $\mathbb{C}$ with an action of G on it $\rho : G \times V \to V$ s.t. for all $g \in G$, the induced map $\rho(g, -)$ is $\mathbb{C}$-linear.

Notation. The map $\rho(g, -) : V \to V$ is often abbreviated as ρ_g. The representation is denoted by V or ρ, with V emphasizing the vector space structure.

Definition 2.1.2 (Degree of Repr.)**.** The **degree** of a representation V of G is $\dim_{\mathbb{C}} V$.

For most of the time, we will only consider the representation of finite groups on finite-dimensional vector spaces.

Remark 2.1.3. In general, one can consider representations over other fields than $\mathbb{C}$. The reasons why $\mathbb{C}$ is chosen are the followings:

1) If G is finite, then $|G| \in \mathbb{C}$ is always invertible.
2) $\mathbb{C}$ is algebraically closed. The implications include, for example, every linear map has an eigenvalue.

These specialties will often appear in subsequent proofs.

Definition 2.1.4 (Morphism of Repr.)**.** Given two representations of G, V and W, a **morphism of representations** (or simply G**-morphism**) is a linear map $f : V \to W$ s.t. $f(gv) = g(f(v))$ for all $g \in G$, $v \in V$. This is an **isomorphism** if f is further bijective.

Remark 2.1.5. Following from the definitions we have the immediate results:

1) If $V_1 \xrightarrow{f} V_2 \xrightarrow{g} V_3$ are morphisms of representation, then so is $g \circ f$ since $g(f(hv)) = g(hf(v)) = h(g(f(v)))$ for all $h \in G$, $v \in V$. This gives the morphisms of objects, which implies that representations of G give a category.
2) If $f : V \to W$ is an isomorphism of representations, then so is f^{-1} (simply by writing the equation for definition in the inverse order).
3) If V and W are representations of G, then $\{f : V \to W \mid f \text{ is a } G\text{-morphism}\} \subseteq \mathrm{Hom}_{\mathbb{C}}(V, W)$ gives a $\mathbb{C}$-vector subspace. This is clear as by the fact that f is linear, V as a representation is closed under addition and scalar multiplication.

Remark 2.1.6. Given a finite-dimensional representation $\rho : G \to \mathrm{GL}(V)$, choosing a basis $\{e_1, \dots, e_n\}$ of V gives us an isomorphism $V \simeq \mathbb{C}^n$, i.e. we have the description of representations in matrices

$$\rho : G \to \mathrm{GL}(V) \simeq \mathrm{GL}_n(\mathbb{C}), \qquad g \mapsto \rho_g = (a_{ij}(g))$$

Let A be the matrix representation of a morphism of representations f (which is also a linear map on V). Denote the corresponding linear map of g in two representations by ρ_g and ρ'_g, respectively. Since it is required that a morphism of representations should be compatible with application of $g \in G$, we have $A \circ \rho_g = \rho'_g \circ A$. This implies that $\rho'_g = A \circ \rho_g \circ A^{-1}$, i.e. two representations are isomorphic if and only if they are conjugate in matrix presentation of the map represented by the same group element g; and the matrix that describes the conjugation is the same for all elements $g \in G$.

Definition 2.1.7 (Sub-representation)**.** Given a representation V of G, a **sub-representation** of V is a vector space $W \subseteq V$ s.t. $gv \in W$ for all $v \in W, g \in G$.

Remark 2.1.8. In particular, for W a sub-representation of V, it is itself a representation with the map ρ' being $\rho(-)|_W$. The inclusion $W \hookrightarrow V$, $v \mapsto v$ is a morphism of representation. This clearly commutes with actions of $g \in G$ as this is identity on W.

2.2 Interpretation via the Group Algebra

Similar to the case of group action where we interpreted the structure of group action by the group homomorphism $G \to S_x$, we would like to have some equivalence to structures that are more explicit, and easier to analyze. This utilizes the following definitions:

Definition 2.2.1 (Group Algebra). Let G be a group. Then the **group algebra over** $\mathbb{C}$, denoted $\mathbb{C}[G]$, is a vector space with a basis $\{\alpha(g) \mid g \in G\}$ in bijection with elements in G (formally). Endow it with a multiplication $\alpha(g) \cdot \alpha(h) = \alpha(gh)$ compatible with the group structure gives the desired ring structure.

Remark 2.2.2. Verifying the ring axioms, we have the fact that the identity in $\mathbb{C}[G]$ to be $\alpha(e)$. This is in fact a $\mathbb{C}$-algebra, with the associated morphism given by $\mathbb{C} \to \mathbb{C}[G]$. Since the image of it are multiples of the identity element, it is clearly in the center of the group.

Notice that G is not necessarily a finite group. Therefore the vector space can be infinite-dimensional, where we have imposed the requirement that every element should be a finite sum of linear combination of basis. In the following deduction, denote $\sum'$ to be the finite sum.

Proposition 2.2.3. The group algebra is well-defined.

Proof. This is clear for the cases where G is finite. Consider the case where G is infinite. Then by definition of the group algebra, for all $u, v \in \mathbb{C}[G]$, we have their decomposition into elements in the basis:

$$u = \sum_{g \in G}{}' a_g \alpha(g), \qquad v \in \sum_{g \in G}{}' b_g \alpha(g)$$

Multiplying these two terms together gives

$$u \cdot v = \sum_{g \in G} \left(\sum_{g_1 g_2 = g} (a_{g_1} b_{g_2}) \right) \alpha(g)$$

Furthermore there are only finitely many such a_gs and b_gs being nonzero, implying that there are only finitely many nonzero such products. □

Notation. If G is abelian, and the correspondence of elements in G and in $\mathbb{C}[G]$ is written additively. Instead of $\alpha(g)$ one usually writes χ^g (with the convention that $\chi^g \cdot \chi^h = \chi^{g+h}$).

Remark 2.2.4. $\mathbb{C}[G]$ is a commutative ring if and only if G is an abelian group. "Only if" is clear as if $\mathbb{C}[G]$ is commutative implies for all $g, h \in G$, they commute. "If" results from the fact that for every element in $x \in \mathbb{C}[G]$ there exists a scalar λ s.t. $\lambda x = \alpha(g)$ for some $g \in G$ as $\mathbb{C}$ is a field.

Example 2.2.5. If $G = (\mathbb{Z}, +)$, identifying $x \leftrightarrow \chi^x$ for $x \in \mathbb{Z}$, we have $\mathbb{C}[G] \simeq \bigoplus_{m \in \mathbb{Z}} \mathbb{C}\chi^m \simeq S^{-1}\mathbb{C}[x]$ for $S = \langle x \rangle = \{1, x, x^2, \dots\}$. These are the Laurent Polynomials.

If $G = (\mathbb{Z}/n\mathbb{Z}, +)$, we have the identification $x^n = 1$, giving $\mathbb{C}[G] \simeq \mathbb{C}[x]/(x^n - 1)$.

Proposition 2.2.6. We have the identification between representations of G and $\mathbb{C}[G]$-modules. Morphisms and sub-objects (sub-representations and submodules) are also in correspondence.

Proof. It suffices to verify 1), as identifications in 2) and 3) are induced by 1).

Suppose that V is a representation of G, Then V has a structure of $\mathbb{C}[G]$-module, whose addition is the same as in the vector space, and scalar multiplication is given by

$$\left(\sum_{g\in G}(a_g\cdot\alpha(g))\right)\cdot v=\sum_{g\in G}(a_g\cdot g(v))$$

where the sums are finite. Conversely, if M is a $\mathbb{C}[G]$-module, then it has a $\mathbb{C}$-vector space structure via considering the scalar multiplication as the action $\mathbb{C}\hookrightarrow\mathbb{C}[G]$ which acts on M; and the $\mathbb{C}$-linear map associated to each group element g is given by $(g,-)$, where $(g,x)\mapsto\alpha(g)\cdot x$ as specified by the $\mathbb{C}[G]$-module. The linearity is guaranteed by the linearity of scalar multiplication in modules. □

Corollary 2.2.7. If $F:V\to W$ is a morphism of G-representations, then $\ker f\subseteq V$ and $\operatorname{im} f\subseteq W$ are sub-representations. This can be seen via using Proposition 2.2.6 to identify representations with $\mathbb{C}[G]$-modules, and see that the kernel and image of a morphism of R-modules are both submodules.

Remark 2.2.8. In general, for a representation over a field $\mathbb{F}$ of G, it can be identified with $\mathbb{F}[G]$.

2.3 Examples of Representations

The following gives some common examples of representations:

1) Suppose that G acts on a set X. Let V be the free $\mathbb{C}$-vector space associated to X, with basis $\{\alpha(u)\mid u\in X\}$ in bijection with X. Define $G\xrightarrow{\rho}\mathrm{GL}(V), g\mapsto\rho_g$, with $\rho_g(\alpha(u))=\alpha(gu)$. This is the permutation representation associated with X where action of elements in the group corresponds to a permutation of the set. This is essentially just the group action, as the representation is completely fixed via specifying its behavior on elements in X (i.e. with coefficient 1).

2) Example 1) applied to the action of G on itself, $G\times G\to G$, $(g,h)\mapsto(gh)$ induces a representation $\mathbb{C}[G]$. This is the regular representation of G. Viewed under the context of Proposition 2.2.6, this is the standard left $\mathbb{C}[G]$-module structure of itself (rings are left-modules over itself).

3) Direct sum of representations. If $\rho_V:G\to\mathrm{GL}(V)$ and $\rho_W:G\to\mathrm{GL}(W)$ are representations of G, then we can get a representation $\rho:G\to\mathrm{GL}(V\oplus W)$, given by

$$\rho_g=(\rho_g^V,\rho_g^W):G\times(V\oplus W)\to(V\oplus W),\quad (g,(v,w))\mapsto(gv,gw)$$

Under the context of Proposition 2.2.6, this corresponds to the direct sum of modules.

4) Tensor product of representations. Suppose that we have $\rho:G\to\mathrm{GL}(V)$ and $\rho':G\to\mathrm{GL}(V')$ two representations of G. Then we can have

$$\widetilde{\rho}=\rho\otimes\rho':G\to\mathrm{GL}(V\otimes_{\mathbb{C}}V'),\quad g\mapsto(\rho_g\otimes\rho'_g)$$

This is indeed a group homomorphism, as tensor product of maps behave functorially. That is, it commutes with composition of maps by the universal property of tensor product:

$$(f\otimes g)\circ(f'\otimes g')=(f\circ f')\otimes(g\circ g')$$

2.4 Irreducible Representations

Similar to the introduction of simple groups in group theory, we would like to have some simple objects in terms of representation, such that for any representation it can be decomposed into the "combination" of these simple objects, and understanding these simple objects provides understanding of the whole object.

Consider the simplest case of representation of G, where the associated vector space is 1-dimensional, i.e. is given explicitly by $G \to \mathrm{GL}_1(\mathbb{C}) \simeq \mathbb{C}^*$ as a group homomorphism. The composition of $\mathbb{C}^*$ is the multiplication, as here $\mathbb{C}^*$ is considered as the 1-by-1 complex matrix (1-dimensional linear map). Since $\mathbb{C}^*$ is commutative, this is the same as the representation $\bar{\rho} : G^{\mathrm{ab}} \to \mathbb{C}^*$. By Remark 2.1.6, two representations are isomorphic if and only if they are conjugate; and since $\mathbb{C}^*$ is commutative, this implies that two representations on $\mathbb{C}$ are isomorphic if and only if they are identical.

The following gives some tools for properly define the concept of "simple" objects in terms of representations, and decompose complex objects to those simple ones. From now on, we will consider only G being finite groups, and all representations are finite-dimensional.

Parenthesis 2.4.1. Let V be a vector space, and $W \subseteq V$ a linear subspace. Then giving the followings are equivalent:

1) A vector subspace $W' \subseteq V$ s.t. $V = W \oplus W'$ which is the internal direct sum, i.e. every element in V can be uniquely decomposed into the sum of an element in W and an element in W'; and the two vector subspaces W and W' are linearly independent, i.e. $W \cap W' = \{0\}$.

2) A linear map $p : V \to V$ s.t. $p^2 = p$, and $\mathrm{im}\, p = W$.

Proof. Consider implication in two directions:

- *1) $\implies$ 2).* Given $V = W \oplus W'$, we know that for all $v \in V$, there exists unique $w \in W$ and $w' \in W'$ s.t. $v = w + w'$. Define $p : V \to W$ s.t. $p(v) = w \in W$ with w the same as in the decomposition above. It is then clear that $p^2 = p$.
- *2) $\implies$ 1).* Define $W = p(V)$, and $W' = \ker p$. Check: $W \cap W' = \{0\}$, as $v \in W' \implies p(v) = 0$; and $v \in W \implies p(v) = v$, which gives $W \cap W' = \{0\}$; and the decomposition can be seen by $v \mapsto (p(v), v - p(v))$.

It is further clear that these two transforms are inverse to each other, which proves the assertion. □

The general result above is also true for representations:

Theorem 2.4.2. Let G be a finite group. Let V be a finite-dimensional $\mathbb{C}$-representation of G, and $W \subseteq V$ a sub-representation. Then there exists another sub-representation W' of V s.t. $V = W \oplus W'$.

First show that we have similar identifications as in the scenario for vector spaces:

Proposition 2.4.3. For V a representation of G, and $W \subseteq V$ a sub-representation, then

$$\text{Giving } W' \text{ sub-repr. s.t. } V = W \oplus W' \iff \text{Giving } p : V \to V \text{ morphism of repr. s.t. } p^2 = p, \text{ and } \mathrm{im}\, p = W$$

Proof. Prove the equivalence in two directions:

$\Rightarrow$: For W' being a sub-representation, it is in particular a vector subspace of V. Then by Parenthesis 2.4.1 we have $p : V \to V$ linear map which satisfies the desired conditions. Further verify that this is a morphism of representation: for all $v \in V, g \in G$ we have

$$g(p(v)) = g(p(w + w')) = g(p(w)) = g(w) = p(g(w))$$

where the last equality results from the fact that $g(w) \in W$ as W is a sub-representation of V.

$\Leftarrow$: The decomposition is clear from the result when considering V, W, W' as vector spaces; and the fact that W' is a sub-representation results from the result that $W' = \ker p$ and kernel of morphism of representations is still a representation (Corollary 2.2.7).

□

Proof of Theorem 2.4.2. Approach the proof via providing the construction in RHS. For $W \subseteq V$ being a sub-representation, by Parenthesis 2.4.1 we have a linear map $p : V \to V$ s.t. $p^2 = p$ and $\operatorname{im} p = W$. Now seek using p to construct a morphism of representations: Define

$$\tilde{p} : V \to V, \quad v \mapsto \frac{1}{|G|} \sum_{g \in G} g^{-1} p(gv)$$

Verify that this is a morphism of representations. For all $v \in V$ and $h \in G$, we have

$$\begin{aligned} \tilde{p}(hv) &= \frac{1}{|G|} \sum_{g \in G} g^{-1} p(ghv) = h \left(\frac{1}{|G|} \sum_{g \in G} h^{-1} g^{-1} p(ghv) \right) \\ &= h \left(\frac{1}{|G|} \sum_{g' \in G} (g')^{-1} p(g'v) \right) && \text{(Apply substitution } g' = gh\text{)} \\ &= h(\tilde{p}(v)) \end{aligned}$$

Check that $\tilde{p}$ also satisfies the other two conditions, i.e. $\tilde{p}^2 = \tilde{p}$, and $\operatorname{im} \tilde{p} = W$. Notice $p(\tilde{hv}) = h\left(\frac{1}{|G|} \sum_{g' \in G} (g')^{-1} p(g'v)\right)$, where $p(g'v) \in W$, and for elements in W RHS evaluates to be exactly hv; and linear combination of elements in W still remains in W. Further W is a sub-representation gives the fact that W is invariant under g-actions. Let $W' = \ker \tilde{p}$ finishes the proof. □

> **Remark 2.4.4.** In general linear maps between vector spaces, or even endomorphisms on a specific vector space, are not morphisms of representations, as ρ_g as a linear map in general does not commute with p (which is required by the definition of morphism of representations).

> **Remark 2.4.5.** It is also vital that we require G to be finite; and the field is of characteristic zero. Otherwise the "averaging" process where we divide the sum of all possible representations by the order of G is not valid; and in general Theorem 2.4.2 is *not* true for representations over positive-characteristic fields, or for infinite groups.
>
> A good example given in the homeworks is the followings: take $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ acting on $K^2 = V$ for K some field, and consider the representation $\rho : G \to \mathrm{GL}(V)$. Such projection p (as in the proof) does not exist for the following cases:
>
> - $K = \mathbb{C}$, $G = \mathbb{Z}$, and $\rho(1) = A$.

- $K = \mathbb{Z}/2\mathbb{Z}$, $G = \mathbb{Z}/2\mathbb{Z}$, and $\rho(\bar{1}) = A$.

where the sub-representation is the vector subspace of V preserved by A.

Remark 2.4.6. By Proposition 2.2.6 we have the identification between G-representations on V and $\mathbb{C}[G]$-module structure on V. This implies that for G finite, $W \subseteq V$ (finite-dimensional as a $\mathbb{C}$-vector space) being a $\mathbb{C}[G]$-submodule implies that there exists another $\mathbb{C}[G]$-submodule W' s.t. $V = W \oplus W'$.

Definition 2.4.7 (Irreducible)**.** A representation V of G is **irreducible** if

- $V \neq \{0\}$.
- For every representation $W \subseteq V$, either $W = \{0\}$ or $W = V$.

Corollary 2.4.8. By applying iteratively Theorem 2.4.2 for V any representation of a finite group we have the irreducible decomposition $V = W_1 \oplus \cdots \oplus W_r$ for W_is irreducible decompositions.

Remark 2.4.9. In general irreducible representations do not have to be degree-1. The examples provided in Remark 2.4.5 are good counterexamples.

Remark 2.4.10. The $W_i \subseteq V$ as sub-representations of G are not necessarily unique. For example let V being the trivial representation with degree greater than 1; then any decomposition of V into 1-dimensional subspaces gives the irreducible decompositions, and they are not unique as they can be any linearly-independent subspaces.

However they are unique up to isomorphisms, i.e. given any irreducible representation W, and $V = \bigoplus_{i \in I} W_i$, $\#\{i \mid W_i \simeq W\}$ and $\sum_{W_i \simeq W} W_i$ are independent of the decomposition. That is, the "subspace" that can be represented by W (up to isomorphism) is fixed in for a given V.

The following lemma gives important foundation for computing morphisms between irreducible representations:

Lemma 2.4.11 (Schur)**.** Suppose that V and W are irreducible representations of G; and $f : V \to W$ morphism of representations. Then

- If $V \not\simeq W$, then $f = 0$.
- If $V \simeq W$, then $f = \lambda \cdot \mathrm{Id}$ for some $\lambda \in \mathbb{C}$.

Proof. Use the result from Corollary 2.2.7, that kernel and image of morphism of representations are also representations. Consider $\ker f$ and $\operatorname{im} f$. Since V is irreducible, either $\ker f = V$ (where $f = 0$) or $\ker f = \{0\}$. Similarly either $\operatorname{im} f = \{0\}$ or $\operatorname{im} f = W$.

Since a morphism of representations is in particular a linear map, $\dim \ker f + \dim \operatorname{im} f = \dim V$; and in particular we cannot have both $\operatorname{im} f = \{0\}$ and $\ker f = \{0\}$. Therefore if $\ker f = \{0\}$, $\operatorname{im} f = W$, which implies that f is an isomorphism. Since $\mathbb{C}$ is algebraically closed, we know that f (as a linear map) has an eigenvalue λ, i.e. $f - \lambda \cdot \mathrm{Id}$ is not injective. But by the fact that W is irreducible, $f - \lambda \cdot \mathrm{Id} = 0$, i.e. $f = \lambda \cdot \mathrm{Id}$. □

Now we seek to prove the first assertion in Remark 2.4.10. First we need to introduce the structure of representations on the linear maps $\mathrm{Hom}_{\mathbb{C}}(V, W)$.

We have seen that $\mathrm{Hom}_{\mathbb{C}}(V,W)$ obtains a vector space structure with addition and scalar multiplication given by the corresponding operation on the output of the map in W. Now suppose that V and W are both G-representations. Then there exists a natural G-representation structure in $\mathrm{Hom}_{\mathbb{C}}(V,W)$, given by

$$(g\varphi)(v) := g\left(\varphi(g^{-1}(v))\right)$$

It is clear that this is linear. Check that this is a group homomorphism:

$$((g_1g_2)\varphi)(v) = (g_1g_2)(\varphi(g_2^{-1}g_1^{-1}(v))) = g_1\left(g_2(\varphi(g_2^{-1}(g_1^{-1}(v))))\right) = (g_1(g_2\varphi))(v)$$

> **Remark 2.4.12.** For V any G-representation, define $V^G := \{v \in V \mid gv = v,\ \forall g \in G\}$ which is the largest trivial subrepresentation of G. Then representations of $\mathrm{Hom}_{\mathbb{C}}(V,W)^G$ (as a $\mathbb{C}$-vector space) can be identified with $\{\varphi : V \to W \mid \varphi \text{ morphism of repr.}\}$. This follows directly from the fact that $g\varphi(g^{-1}-) = \varphi(-)$ (LHS is the representation defined on $\mathrm{Hom}_{\mathbb{C}}(V,W)^G$) implies that $g^{-1}\varphi(-) = \varphi(g^{-1}-)$ which is exactly the definition of morphism of representations.

> **Corollary 2.4.13** (Result 1 in Remark 2.4.10)**.** If V is a G-representation with irreducible decompositions $V = W_1 \oplus \cdots \oplus W_r$. Then $\#\{i \mid W_i \simeq W\} = \dim_{\mathbb{C}}\left(\mathrm{Hom}_{\mathbb{C}}(V,W)^G\right)$

Proof. By the structure of representations in V, we have the isomorphism of representations:

$$\mathrm{Hom}_{\mathbb{C}}(W,V)^G \simeq \mathrm{Hom}_{\mathbb{C}}(W,W_1) \oplus \cdots \oplus \mathrm{Hom}_{\mathbb{C}}(W,W_r)$$

Schur (Lemma 2.4.11) gives

$$\dim_{\mathbb{C}}(W,W_i)^G = \begin{cases} 0, & W \not\simeq W_i \\ 1, & W \simeq W_i \end{cases}$$

Since we are in the context of vector spaces, we have

$$\dim_{\mathbb{C}}(W,V) = \sum_{i=1}^{r} \dim \mathrm{Hom}_{\mathbb{C}}(W,W_i)$$

and summing up the dimensions gives the desired result. □

2.5 Character Theory

> **Definition 2.5.1** (Character)**.** Fix a representation $\rho : G \to \mathrm{GL}(V)$, with $g \mapsto \rho_g$, the **character** of ρ is a function
>
> $$\chi_\rho : G \to \mathbb{C}, \quad g \mapsto \mathrm{Tr}(\rho_g)$$

> **Remark 2.5.2.** The definition of character is invariant w.r.t. choice of basis as the trace of a linear map is independent of the choice of basis.

Notation. $\chi_\rho(g) \in \mathbb{C}$ is sometimes abbreviated to be χ_{ρ_g} as is in the notation of representation.

The following gives some immediate properties of trace function:

1) If $\rho \simeq \rho'$, then $\chi_\rho = \chi_{\rho'}$. Recall that by Remark 2.1.6, $\rho \simeq \rho'$ if and only if there exists some linear map A s.t. for all $g \in G$. $\rho_g = A \circ \rho'_g \circ A^{-1}$, i.e. they are similar. Then the equality in character results directly from the fact that similar matrices have identical trace.

2) An immediate corollary to 1) is the fact that each χ_ρ is a class function, i.e. takes constant value on the conjugacy class of any $g \in G$. This can be seen via taking $A = \rho_g$, and apply the fact that ρ is a group homomorphism, i.e. $\rho_{g^{-1}} = \rho_g^{-1}$.

3) $\chi_\rho(e) = \mathrm{Tr}(\mathrm{Id}) = \dim_{\mathbb{C}} V$.

The following results are also quite useful but are not so immediate, so we formalize them as propositions:

Proposition 2.5.3. Let ρ be a representation of a finite group G. Then $\chi_\rho(g^{-1}) = \overline{\chi_\rho(g)}$.

Proof. Since we have $V \simeq \mathbb{C}^n$, we have the identification of ρ as $\rho : G \to \mathrm{GL}(\mathbb{C}^n)$. Gram-Schmidt gives a basis in which the matrix representation of ρ_g is upper-triangular, i.e. in the form of $\begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ & & \lambda_n \end{pmatrix}$ with λ_is the eigenvalues. It is clear then that the inverse must also be in the form of $\begin{pmatrix} \lambda_1^{-1} & & * \\ & \ddots & \\ & & \lambda_n^{-1} \end{pmatrix}$. This gives

$$\mathrm{Tr}(\rho_g) = \sum_{i=1}^{n} \lambda_i, \quad \mathrm{Tr}(\rho_{g^{-1}}) = \sum_{i=1}^{n} \lambda_1^{-1}$$

But since we have the requirement that ρ is a group homomorphism, and as $|G| = m$ we have the constraint $\rho_{g^{|G|}} = \mathrm{Id}$, i.e. in matrix form

$$\begin{pmatrix} \lambda_1 & & * \\ & \ddots & \\ & & \lambda_n \end{pmatrix}^m = \begin{pmatrix} \lambda_1^m & & * \\ & \ddots & \\ & & \lambda_n^m \end{pmatrix} = \mathrm{Id} \implies \lambda_i^m = 1 \ \forall i$$

In particular we have $|\lambda_i| = 1$, which gives $\lambda_i^{-1} = \overline{\lambda_i}$. Summing together gives the desired result. □

Proposition 2.5.4. The characters of direct sum of representations, and tensor product of representations have the following relations:

- For $\rho = \rho_1 \oplus \rho_2$, $\chi_\rho = \chi_{\rho_1} + \chi_{\rho_2}$.
- For $\rho = \rho' \otimes \rho''$, $\chi_\rho = \chi_{\rho'} \cdot \chi_{\rho''}$.

Proof. Choose an appropriate basis for the vector space, and express the representations in that correspondingly.

Let V_1 and V_2 be the corresponding vector spaces of ρ_1 and ρ_2. Then given bases in both V_1 and V_2, we have a basis of $V = V_1 \oplus V_2$, and the corresponding matrix representation of ρ: $\left(\begin{array}{c|c} (\rho_1)_g & \\ \hline & (\rho_2)_g \end{array}\right)$ which is block diagonal. The trace corresponding to the character can then be computed via

$$\mathrm{Tr}(\rho) = \mathrm{Tr}((\rho_1)_g) + \mathrm{Tr}((\rho_2)_g)$$

For the case with tensor product, consider the representations to be $\rho' : G \to \mathrm{GL}(V_1)$ and $\rho'' : G \to \mathrm{GL}(V_2)$. Choose bases $e_1, \dots, e_n$ for V_1, and $f_1, \dots, f_m$ for V_2. Let $(a_{ij})_{n\times n}$ and $(b_{kl})_{m\times m}$ be the corresponding matrix representations for ρ' and ρ''. Then $V_1 \otimes V_2$ has a basis $e_i \otimes f_j$. Compute the matrix representation for ρ:

$$\begin{aligned}\rho_g(e_j \otimes f_\ell) &= \rho'_g(e_j) \otimes \rho''_g(f_\ell) \\ &= \left(\sum_{i=1}^{n} a_{ij} e_i\right) \otimes \left(\sum_{k=1}^{m} b_{k\ell} f_k\right) \\ &= \sum_{i,k} a_{ij} b_{k\ell} \, (e_i \otimes f_k)\end{aligned}$$

Then

$$\mathrm{Tr}(\rho_g) = \sum_{i=j,k=\ell} a_{ij} b_{k\ell} (e_i \otimes f_k) = \sum_{i,k} a_{ii} b_{kk} (e_i \otimes f_k) = \left(\sum_i a_{ii}\right)\left(\sum_k b_{kk}\right) = \mathrm{Tr}(\rho'_g) \cdot \mathrm{Tr}(\rho''_g)$$

□

The character of a representation gives information on its properties, e.g. checking whether a given set of sub-representations gives a decomposition, or checking whether a representation is irreducible, etc. To utilize this concept we need some extra tools on the object:

Notation. Define $\mathrm{Func}(G) := \{f : G \to \mathbb{C}\}$. This gives a $\mathbb{C}$-vector space of $\dim |G|$. Explicitly, for $G = \{g_1, \dots, g_m\}$ we have the isomorphism $\mathrm{Func}(G) \simeq \mathbb{C}^m$, $f \mapsto (f(g_1), \dots, f(g_m))$.

Definition 2.5.5 (Inner Product of Functions)**.** Let $f, g \in \mathrm{Func}(G)$. Define

$$\langle f, g \rangle := \frac{1}{|G|} \sum_{x \in G} f(x)\overline{g(x)}$$

Remark 2.5.6. The inner product gives a Hermitian product on $\mathrm{Func}(G)$. Recall that Hermitian product needs to satisfy $\mathbb{C}$-linearity in the first entry, conjugate $\mathbb{C}$-linear in the second entry, and positive-definite, i.e. for all $f \neq 0, \langle f, f \rangle > 0$.

The following is the main theorem for character of representations, that is the character of a representation uniquely characterizes a representation up to isomorphism:

Theorem 2.5.7. Let ρ and ρ' be irreducible representations, then $\langle \chi_\rho, \chi_{\rho'} \rangle = 1$ if they are isomorphic, and $\langle \chi_\rho, \chi_\rho \rangle = 0$ otherwise.

The tools we have for such situations are Schur's result (Lemma 2.4.11), and the averaging process which makes a linear map into a morphism of representations used in the proof of Theorem 2.4.2. The general strategy is to notice that we have application of g both in the domain and image in the "averaged" representation, and $\chi(g^{-1}) = \overline{\chi(g)}$ gives the conjugacy and thus the desired form of the inner product.

Notation. In the proof we use $(a_{ij})_{m\times n}$ to denote the matrices, with the indices dropped if apparent; and a_{ij} (without the parenthesis) to denote entries in the matrix.

Proof of Theorem 2.5.7. Assume that $\rho : G \to \mathrm{GL}_n(\mathbb{C})$ and $\rho' : G \to \mathrm{GL}_m(\mathbb{C})$ are the representations. Denote the matrix representations for ρ_g, ρ'_g and $\rho'_{g^{-1}} = (\rho'_g)^{-1}$ to be $(a_{ij})_{n\times n}$, $(b_{ij})_{m\times m}$ and $(c_{ij})_{m\times m}$, correspondingly. Consider a linear map

$\varphi : V \to V'$ with matrix representation $(\varphi_{ij})_{m\times n}$, and the induced morphism of representations $\psi : V \to V'$ given by

$$\psi(v) := \sum_{g\in G} g^{-1}(\varphi(gv))$$

For proof of this being indeed a representation check Proof of Theorem 2.4.2. Now consider the matrix representation of $\psi(v)$:

- Consider $\rho \not\simeq \rho'$. Then by Schur's Lemma (Lemma 2.4.11), we have $\psi = 0$. In particular, every entry of matrix representation of ψ is 0, which gives

  $$\psi_{ik} = \sum_{g\in G}\left(\sum_{j,\ell} c_{ij}(g)\varphi_{j\ell}a_{\ell k}\right)$$

  Since this holds for all $\varphi : V \to V'$, decomposing φ into the basis given by each entry in the m-by-n matrix i.e. with

  $$\varphi_{j\ell} = \begin{cases} 1, & j = j',\ \ell = \ell' \\ 0, & \text{otherwise} \end{cases}$$

  we have for all i, j', ℓ', k, $\sum_{g\in G}(\sum_{i,k} c_{ij'}a_{\ell' k}(g)) = 0$. In particular, we can take $i = j'$ and $\ell' = k$, and summing up along the diagonal entries, which gives

  $$0 = \sum_{g\in G}\left(\sum_{i=1}^{n} c_{ii}\right)\left(\sum_{k=1}^{n} a_{kk}\right) = \sum_{g\in G}\chi_{\rho'}(g^{-1})\cdot\chi_\rho(g) = \sum_{g\in G}\overline{\chi_{\rho'}(g)}\cdot\chi_\rho(g) = \langle\chi_\rho, \chi_{\rho'}\rangle$$

- Now consider the case where $\rho = \rho'$, i.e. $V \simeq V'$. Then Schur (Lemma 2.4.11) gives that there exists $\lambda_{j\ell}$ s.t. for $\varphi_{j'\ell'}$ as defined in the previous case

  $$\psi_{j'\ell',ik} = \sum_{g\in G} c_{ij'}(g)a_{\ell' k}(g) = \lambda_{j',\ell'}\delta_{i,k}$$

  Now consider $\varphi = \mathrm{Id}$, i.e. $\varphi_{ij} = \delta_{i,j}$. Taking $i = j$ and $k = \ell$ we have

  $$\sum_{g\in G}\left(\sum_{i,k} c_{ii}(g)a_{kk}(g)\right) = \sum_{i,k}\lambda_{i,k}\delta_{i,k} = \sum_q \lambda_{q,q}$$

  But $\lambda_{i,i} = 1$ for all i, which gives

  $$\begin{aligned} |G| = \sum_k \lambda_{k,k} &= \sum_{g\in G}\left(\sum_{i,k} c_{ii}(g)a_{kk}(g)\right) \\ &= \sum_{g\in G}\left(\sum_i c_{ii}(g)\right)\left(\sum_k a_{kk}(g)\right) \\ &= \sum_{g\in G}\chi_\rho(g)\cdot\chi_\rho(g^{-1}) = \sum_{g\in G}\chi_\rho(g)\cdot\overline{\chi_\rho(g)} \\ &= \sum_{g\in G}\langle\chi_\rho, \chi_\rho\rangle \end{aligned}$$

  where dividing both sides by $|G|$ gives the desired result.

□

Corollary 2.5.8. From the theorem we have the following immediate results:

1) The number of isomorphism classes of irreducible representations is bounded above by $\dim_{\mathbb{C}} \mathrm{Func}(G) = |G|$. Notice that if $\rho_1, \dots, \rho_r$ are pairwise non-isomorphic irreducible representations, then by Theorem 2.5.7 $\langle \chi_i, \chi_j \rangle = 0$ for all $i \neq j$, i.e. they are orthonormal, and in particular linearly independent. But $\dim_{\mathbb{C}} \mathrm{Func}(G) = |G|$, so there are at most $|G|$ of them.

2) Let V be any representation of G, and W an irreducible representation of G, then for irreducible decomposition of V: $V = \bigoplus_{i=1}^{r} W_i$, $\#\{i \mid W_i \simeq W\} = \langle \chi_V, \chi_W \rangle$.

   Proof. To see this, by Proposition 2.5.4 we have $\chi_V = \sum_{i=1}^{r} \chi_{W_i}$. Then

   $$\langle \chi_V, \chi_W \rangle = \left\langle \sum_{i=1}^{r} \chi_{W_i}, \chi_W \right\rangle = \sum_{i=1}^{r} \langle \chi_{W_i}, \chi_W \rangle$$

   where since both W_i and W are irreducible, we have $\langle \chi_{W_i}, \chi_W \rangle = 1$ if and only if $W \simeq W_i$; and 0 otherwise. □

3) A representation V of G is irreducible if and only if $\langle \chi_V, \chi_V \rangle = 1$.

   Proof. The "only if" part is prove in the theorem above. To see the "if" part, consider the decomposition of V:

   $$V \simeq W_1^{\oplus a_1} \oplus \cdots \oplus W_r^{\oplus a_r}, \quad \chi_V = \sum_{i=1}^{r} a_i \chi_{W_i}$$

   Then use the formula given in the theorem, we have $\langle \chi_V, \chi_V \rangle = \sum_{i=1}^{r} a_i^2$, which is 1 if and only if $r = 1$ and $a_1 = 1$. But this is exactly paraphrasing of the V being irreducible. □

4) For every representation V, we have $V \simeq W$ if and only if $\chi_V = \chi_W$.

   Proof. The "only if" part results from Remark 2.1.6, where representations are isomorphic if and only if they are conjugate; but conjugate matrices have the same trace, i.e. the representations have the same character.

   To see the "if" part, since $\chi_V = \chi_W$, in particular for every irreducible G-representation W' we have $\langle \chi_V, \chi_{W'} \rangle = \langle \chi_W, \chi_{W'} \rangle$. Testing this through all non-isomorphic irreducible G-representations gives the irreducible decomposition of V and W, which are the same as the inner products which gives the powers (a_is as in part 3) are the same. This implies that they are actually isomorphic. □

The following provides an application of the theorem above and immediate results to the regular representation of a group, which provides a view on all the irreducible G-representations.

Recall the regular representation is defined as $\rho^{\mathrm{reg}} : G \to \mathrm{GL}(\mathbb{C}[G])$, where $\mathbb{C}[G] := \bigoplus_{g \in G} \mathbb{C}\alpha(g)$ where α is a formal bijection on the group G. The operation is given by $\rho_h^{\mathrm{reg}}(\alpha(g)) := \alpha(gh)$.

Lemma 2.5.9. The character of the regular representation is $\chi_{\rho^{\mathrm{reg}}}(g) = 0$ if $g \neq e$; and $\chi_{\rho^{\mathrm{reg}}}(e) = \dim_{\mathbb{C}} \mathbb{C}[G] = |G|$.

Proof. Recall that the basis of $\mathbb{C}[G]$ is given by all the elements in G. In terms of matrix representations, this implies that ρ_h^{reg} corresponds to the h-gh entry being 1 in the matrix for all $h \in G$. In particular, these entries contribute to the trace if and only if

$gh = h$, i.e. $g = e$, in which case we have 1s on the diagonal, giving $\mathrm{Tr}(\rho^{\mathrm{reg}}(g)) = \dim_{\mathbb{C}}(\mathbb{C}[G]) = |G|$. □

Proposition 2.5.10. Let $\rho_1, \dots, \rho_r$ be all the (non-isomorphic) irreducible G-representations, with their corresponding degree d_i. Then

$$\rho^{\mathrm{reg}} \simeq \bigoplus_{i=1}^{r} \rho_i^{\oplus d_i}$$

Proof. Use the result in the lemma above, we have by definition

$$\langle \chi_{\rho^{\mathrm{reg}}}, \chi_{\rho_i} \rangle := \frac{1}{|G|} \sum_{g \in G} \chi_{\rho^{\mathrm{reg}}}(g) \overline{\chi_{\rho_i}(g)} = \frac{1}{|G|} \chi_{\rho^{\mathrm{reg}}}(e) \overline{\chi_{\rho_i}(e)} = d_i$$

since $\chi_{\rho^{\mathrm{reg}}}$ is zero except at the identity, where it evaluates to the dimension of the vector space; and as the representation ρ_i is a group homomorphism, we have $\rho_i(e) = \mathrm{Id}$, i.e. $\chi_{\rho_i}(e) = \mathrm{Tr}(\mathrm{Id}) = d_i$. The number of copies are then given by the decomposition according to Corollary 2.5.8 2). □

Corollary 2.5.11. Taking dimensions on the result of Proposition 2.5.10 gives

$$|G| = \sum_{i=1}^{r} d_i^2$$

for d_i being the degree of irreducible representation ρ_i. A theorem in the next section gives the fact that the number of G-representations is the same as the number of conjugacy classes of G. This equation, together with that theorem gives a tool to check whether we have found of all G-representations given a group G.

Corollary 2.5.12. By the formula for computing the character for direct sum of representations (Proposition 2.5.4), we have

$$\chi_{\rho^{\mathrm{reg}}} = \sum_{i=1}^{r} d_i \chi_{\rho_i} \implies \sum_{i=1}^{r} d_i \chi_{\rho_i}(g) = 0 \ (\forall g \neq e)$$

2.6 Counting Irreducible G-Representations

As we have seen in the previous section, since the trace of a function is preserved through conjugation, the characters of an irreducible representation of G evaluated at g is determined uniquely by the conjugacy class that g is in. This, together with the formula in Corollary 2.5.11 provide the tool for finding all irreducible G-representations. This section is devoted to the introduction of the formulation of the above process.

Definition 2.6.1 (Class Function). The **class functions** of G is a subset of $\mathrm{Func}(G)$, where its elements $\varphi : G \to \mathbb{C}$ satisfies the property that it evaluates to the same value on conjugate elements in G. The set of class functions in G is denoted as $\mathcal{C}(G)$.

Remark 2.6.2. Considering $\mathcal{C}(G)$ as a $\mathbb{C}$-vector space where the addition and scalar multiplication is applied to the result of evaluation of the class functions, $\dim_{\mathbb{C}} \mathcal{C}(G)$ is the number of conjugacy classes of G.

For objects that are invariant w.r.t. the action of conjugation, the most straightforward ones are G-representations and characters. The following theorem seeks to describe the relation between these objects:

Theorem 2.6.3. Let $\rho_1, \dots, \rho_r$ are the irreducible G-representations, and $\chi_1, \dots, \chi_r$ be the corresponding characters. Then χ_is give an orthonormal basis of $\mathcal{C}[G]$. In particular r is the number of conjugacy classes of G.

Before proving the theorem, we first prepare some notations for the class functions. This generalizes the common "averaging" technique making a linear map a morphism of representations, or preserving the structure of morphisms of representation (for example, cf. Theorem 2.4.2):

Notation. Given $f \in \mathcal{C}(G)$, and $\rho : G \to \mathrm{GL}(V)$ a representation, denote

$$\rho_f := \sum_{g \in G} f(g)\rho_g \in \mathrm{End}_{\mathbb{C}}(V)$$

That is, identify the class function f with the element $\sum_{g\in G} f(g)g \in \mathbb{C}[G]$. Notice that this sums over all $g \in G$ and therefore is determined solely by the function f and the G-representation.

Then we have the following immediate results:

1) For $\rho = \rho' \oplus \rho''$, $\rho_f = \rho'_f \oplus \rho''_f$.

2) ρ_f gives a morphism of G-representations. By definition, we only need to check that for all $h \in G$, $v \in V$, we have $\rho_f(hv) = h\rho_f(v)$. But this is indeed the case, as

$$\rho_f(hv) = \sum_{g\in G} f(g)g(hv) = \sum_{g\in G} f(g)h(h^{-1}gh)(v) = h\left(\sum_{h^{-1}gh\in G} f(h^{-1}gh)(h^{-1}gh)(v)\right) = h(\rho_f(v))$$

where the penultimate equality uses the fact that f is a class function, where in particular for all $g, h \in G$ we have $f(g) = f(h^{-1}gh)$.

Proposition 2.6.4. If ρ is irreducible, then $\rho_f = \lambda \cdot \mathrm{Id}$ where

$$\lambda = \frac{|G|}{\deg(\rho)} \langle f, \overline{\chi_\rho} \rangle \tag{(*)}$$

Proof. Express the trace of ρ_f in two ways. $\rho_f = \lambda \mathrm{Id} \implies \mathrm{Tr}(\rho_f) = \lambda \cdot \deg(\rho)$. For the other expression, since $\rho_f = \sum_{g\in G} f(g)\rho_g$, we have

$$\mathrm{Tr}_{\rho_f} = \sum_g \in G f(g) \mathrm{Tr}(\rho_g) = \sum_{g\in G} f(g)\chi_\rho(g) = |G| \cdot \langle f, \overline{\chi_\rho} \rangle$$

□

Proof of Theorem 2.6.3. By Theorem 2.5.7 we know that $\{\chi_1, \dots, \chi_r\}$ gives an orthonormal subset of $\mathcal{C}(G)$. This implies that $\overline{\chi_1}, \cdots, \overline{\chi_r}$ are all linearly independent, i.e. we can express $\mathcal{C}(G)$ as

$$\mathcal{C}(G) = \mathrm{span}(\overline{\chi_1}, \cdots, \overline{\chi_r}) \oplus \mathrm{span}(\overline{\chi_1}, \cdots, \overline{\chi_r})^\perp$$

Therefore, to conclude the proof, we only need to show that the second part of the direct sum vanishes; that is, if $f \in \mathcal{C}(G)$ s.t. $\langle f, \overline{\chi_i}\rangle = 0$ for all i, then $f = 0$. First notice that by Eq. $(*)$ we have $\lambda = 0$; and $(\rho_i)_f = \lambda \cdot \mathrm{Id}$ this implies that $(\rho_i)_f = 0$. Given any representation ρ, writing it as a direct sum of irreducible decompositions gives $\rho_f = 0$.

Now apply this for $\rho = \rho^{\mathrm{reg}}$:

$$(\rho^{\mathrm{reg}})_f = \sum_{g\in G} f(g)\rho_g^{\mathrm{reg}}, \quad (\rho_f^{\mathrm{reg}})(\alpha(e)) = \sum_{g\in G} f(g) \underbrace{(\rho_g^{\mathrm{reg}})(\alpha(e))}_{\alpha(g)}$$

where the second equality is zero by hypothesis. Then $f(g) = 0$ for all g since $\{\alpha(g) \mid g \in G\}$ is a basis for the group algebra. □

Notation (Character Table)**.** The **character table** gives information on the character evaluated on conjugacy classes of a group:

	χ_1	$\cdots$	χ_r
g_1			
$\vdots$		$\chi_i(g_j)$	
g_r			

where the columns are the character of irreducible representations of G; and rows are system of representatives for conjugacy classes of G. Summing over the rows by squares give the order of G, by Corollary 2.5.11

Since character is a class function, it is related to the cardinality of the conjugacy classes: Fix $h \in G$, and consider its conjugacy class:

$$\varphi : G \to \mathbb{C}, \qquad g \mapsto \begin{cases} 1, & g, h \text{ conjugate} \\ 0, & \text{otherwise} \end{cases}$$

It is clear that $\varphi \in \mathcal{C}(G)$. By Theorem 2.6.3 we can write $\varphi = \sum_{i=1}^r a_i\chi_i$. Then we can write

$$a_i = \langle \varphi, \chi_i\rangle = \frac{1}{|G|}\sum_{g\in G} \varphi(g)\overline{\chi_i(g)} = \frac{c(h)}{|G|}\overline{\chi_i(h)}$$

where $c(h)$ is the cardinality of the conjugacy class of h. Taking $\varphi = \chi_i$ we have

1) If g and h are not conjugate, then $\sum_{i=1}^r \chi_i(g)\overline{\chi_i(h)} = 0$ (taking $h = e$ gives the previous result).

2) If g and h are conjugate, then

$$1 = \langle \chi_i, \chi_i\rangle = \frac{c(h)}{|G|}\sum_{i=1}^r \chi_i(h)\overline{\chi_i(h)} \implies \frac{|G|}{c(h)} = \sum_{i=1}^r |\chi_i(h)|^2$$

Proposition 2.6.5. G is abelian if and only if all G-representations have degree 1.

Proof. If G is abelian, then all conjugacy classes of G have 1 element, i.e. there are $|G|$ conjugacy classes. Let $d_1, \ldots, d_n$ for $n = |G|$ be the degree of G-representations. By Corollary 2.5.11 we have $|G| = \sum_{i=1}^r d_i^2$, giving that all d_is are 1. For the other direction letting $d_i = 1$ for all i gives that there are $|G|$ conjugacy classes, i.e. G is abelian. □

Example 2.6.6. Suppose that $G = \mathbb{Z}/n\mathbb{Z}$, we have seen that 1-dimensional G-representations corresponds to $\lambda \in \mathbb{C}$ s.t. $\lambda^n = 1$. Notice also, that for $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*$, since $\mathbb{C}^*$ is abelian it is equivalent to giving both $\mathbb{Z}/m\mathbb{Z} \to \mathbb{C}^*$ and $\mathbb{Z}/n\mathbb{Z} \to \mathbb{C}^*$. In general, 1-dimensional representations of $\mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_d\mathbb{Z}$ corresponds to $\{(\lambda_1, \ldots, \lambda_d) \in (\mathbb{C}^*)^d \mid \lambda_i^{n_i} = 1, \forall i\}$.

Example 2.6.7. Use the result from Corollary 2.5.11 to construct part of the character table of $G = S_3$. The conjugacy classes of G are the identity, 2-cycles and 3-cycles. Then there are 3 irreducible representations:

- The identity 1-dimensional representation $\rho : S_3 \to \mathbb{C}^*$ identically 1.
- The sign permutation $S_3 \to \{\pm 1\}$, with $\sigma \mapsto \varepsilon(\sigma)$.
- Corollary 2.5.11 implies that there exists an irreducible representation of degree 2. This is the standard representation, given by S_3 permuting the entries in $\{(x_1, x_2, x_3) \in \mathbb{C}^3 \mid x_1 + x_2 + x_3 = 0\} \subseteq S_3$.

Then we have the character table

	χ_1	χ_2	χ_3
e	1	1	2
(12)	1	-1	0
(123)	1	1	-1

2.7 Induced Representations

Recall that we have by Proposition 2.2.6 the identification of G-representations and $\mathbb{C}[G]$-modules. As in module theory we have the extension of scalars, where given a ring homomorphism $R \to S$ (often an inclusion or embedding), we have the extension ${}_R\underline{\text{Mod}} \to {}_S\underline{\text{Mod}}$. We can have similar construction in the representation theory.

Let G a finite group, and $H \leq G$ a subgroup. Let $\rho : G \to \text{GL}(V)$ be a G-representation. We have a representation of H simply by restriction: $\rho|_H : H \to \text{GL}(V)$. This is often written $\rho|_H = \text{Res}^G_H(\rho)$. It is clear from definition that $\chi_{(\rho|_H)} = \chi_\rho|_H$. Further we can similarly restrict a morphism of G-representations to get a morphism of H-representations. The goal is find the construction in the inverse direction, i.e. find out how an H-representation induces a G-representation.

Remark 2.7.1. As a review of the extension of scalars, we have an injective of $\mathbb{C}$-algebras $\varphi : \mathbb{C}[H] \hookrightarrow \mathbb{C}[G]$. This enables viewing $\mathbb{C}[G]$-modules as $\mathbb{C}[H]$-modules, given by $a \cdot u := \varphi(a)u$ for all $a \in \mathbb{C}[H]$, $u \in V$ (considered as a $\mathbb{C}[G]$-module). In particular, this gives the result of restriction of representations as above.

Proposition 2.7.2. If every irreducible representation of H has dimension at most r, then every irreducible representation of G has dimension at most $r \cdot (G : H)$.

Example 2.7.3. If H is abelian, then since H is finite every element must be mapped to the unit circle, i.e. all H-representations are irreducible if and only if it is of dimension 1; and then every irreducible G-representation has dimension at most $(G : H)$.

To prove the proposition above we need some further results:

Notation. The left congruence classes of H in G is denoted as $(G:H)_\ell = (G/H)_\ell := \{gH \mid g \in G\}$,

Lemma 2.7.4. Let V be a G-representation, $W \subseteq V$ be a H-representation (for $H \leq G$). Pick $\sigma \in (G:H)_\ell$, i.e. $\sigma = gH$ for some $g \in G$. Denote $W_\sigma := \{gw \mid w \in W\}$.

If V is an irreducible G-representation, then $V = \bigoplus_{\sigma \in (G:H)_\ell} W_\sigma$.

Proof. Notice that for $\sigma \in (G:H)_\ell$, W_σ depends only on σ. Written explicitly, if $gH = g'H = \sigma$, then $g^{-1}g' \in H$. In terms of representation this gives

$$\{g'w \mid w \in W\} = \{g(g^{-1}g')w \mid w \in W\} = \{g((g^{-1}g')w) \mid w \in W\} = \{gw \mid w \in W\}$$

Since W is an H-representation; and $g^{-1}g' \in H$ induces an automorphism on W.

Further for all $g' \in G$ we have $W_{(g'\sigma)} = g'W_\sigma$. This can be seen via first consider by definition $g'(W_\sigma) \subseteq W_{(g'\sigma)}$. The inclusion in the other direction is also clear as $gW = W$ implies that g induces an automorphism on W; or more explicitly, apply the previous result with $(g')^{-1}$, which gives

$$(g')^{-1}W_{g'\sigma} \subseteq W_\sigma \implies W_{g'\sigma} \subseteq (g')W_\sigma$$

Therefore, $\sum_{\sigma \in (G:H)_\ell} W_\sigma$ gives a G-subrepresentation of V. Moreover, since all such σs are disjoint (by the fact that the left equivalence classes are disjoint), this gives the direct sum decomposition. □

Proof of Proposition 2.7.2. Use Lemma 2.7.4: if $\dim_{\mathbb{C}}(V) \leq r$, for V being irreducible we have $V = \sum_{\sigma \in (G:H)_\ell}$, and in particular

$$\dim_{\mathbb{C}}(V) \leq \sum_\sigma \dim_{\mathbb{C}}(W_\sigma) \leq \dim_{\mathbb{C}}(W) \cdot (G:H) \leq r \cdot (G:H)$$

□

The following recalls results of extension of scalars in ring theory.

Fix K to be a field, and R a K-algebra. Left M and N be a right and left R-module, respectively. In particular, both M and N are K-vector spaces. Given the tensor product on vector spaces, we have the induced tensor product in R-modules:

Notation. Denote $M \otimes_R N := M \otimes_K N / \{\text{linear subspaces spanned by } (ua \otimes_K v - u \otimes_K av) \mid u \in M, v \in N, a \in R\}$. $u \otimes_R v$ is the image of $u \otimes_K v$ in the quotient in RHS above.

Remark 2.7.5. Since $M \otimes_K N$ has a natural K-vector space structure, and the subspace vanishing in the quotient is a linear subspace, $M \otimes_R N$ is also a K-vector space.

Definition 2.7.6 (Balanced). If P is a vector space over K, and M, N a right, left R-module, respectively; where R is a K-algebra. a K-bilinear map $\varphi : M \times N \to P$ is **R-balanced** if $\varphi(u, av) = \varphi(ua, v)$ for all $u \in M, a \in R, v \in N$.

Proposition 2.7.7 (Universal Property of $M \otimes_R N$). For all P K-vector space, and $\psi : M \times N \to P$ R-balanced map, there exists a unique K-linear map $f : M \otimes_R N \to P$ s.t. $f \circ \varphi = \psi$ for φ the induced map of tensor product $\varphi : M \times N \to M \otimes_R N$.

Example 2.7.8. The following gives some simple example of tensor product:

1) $M = R$ has the canonical right R-module structure. Then we have the the isomorphism $M \otimes_R N \simeq N$ as K-vector spaces (for R as a K-algebra).

2) If M is a free R-module with basis $e_1, \dots, e_n$, then $M \otimes_R N \simeq N^n$ via the map

$$N^n \to M \otimes_R N, \quad (v_1, \dots, v_n) \mapsto \sum_{i=1}^{n} e_i \otimes_R v_i$$

3) Suppose that we have $f : R \to S$ a morphism of K-algebras; we have the restriction of scalars: for M an S-module, f also gives it an R-module structure, by specifying that for all $a \in R, u \in M$, $a \cdot u := f(a) \cdot u$.

   The inverse direction, extension of scalar, can be constructed for N a left R-module, by considering $S \otimes_R N$, which has a left S-module structure. Here S is viewed as a right R-module, via $u \cdot a := u \cdot f(a)$ for all $u \in S, a \in R$. For all $b \in S$, we can define an R-balanced map

$$S \times N \mapsto S \otimes_R N, \quad (u, v) \mapsto bu \otimes_R v$$

   which by universal property of tensor product induces a map $u \otimes_R v \mapsto bu \otimes_R v$, which defines the scalar multiplication by b

Proposition 2.7.9 (Universal Property of Extension of Scalar)**.** For all left S-module M and left R-module N, we have a bijection

$$\mathrm{Hom}_R(N, M) \simeq \mathrm{Hom}_S(S \otimes_R N, M), \quad f \circ (v \mapsto 1 \otimes_R v) \hookleftarrow f, g \mapsto (a \otimes_R v \mapsto a \cdot g(v))$$

Now we formalize the induced representation. Suppose that G is a finite group, $H \leq G$ a subgroup, and $i : \mathbb{C}[H] \to \mathbb{C}[G]$ the inclusion map. If W is a representation of H, i.e. can be identified with a $\mathbb{C}[H]$-module, then this induces a G-representation (in turns of group algebra)

$$\mathrm{Ind}_H^G(W) := \mathbb{C}[G] \otimes_{\mathbb{C}[H]} W$$

Claim 2.7.10. $\mathbb{C}[G]$ is a free right $\mathbb{C}[H]$-module, with basis $\{\alpha(a) \mid a \in R\}$ where $R \subseteq G$ is a system of representations of $(G/H)_\ell$.

Proof. By definition every $u \in \mathbb{C}[G]$ can be uniquely written as $u = \sum_{g \in G} c_g \alpha(g)$; and $g = ah$ for $a \in R, h \in H$. Then

$$u = \sum_{g \in G} c_g \alpha(g) = \sum_{a \in R} \sum_{h \in H} c_{ah} \alpha(a)\alpha(h) = \sum_{a \in R} \alpha(a) \underbrace{\left(\sum_{u \in H} c_{ah} \alpha(h) \right)}_{\in \mathbb{C}[H]}$$

□

This allows explicitly writing out the induced representation: with the same setting as above, if W is an H-representation, then

$$\mathbb{C}[G] \otimes_{\mathbb{C}[H]} W = \bigoplus_{a \in R} (\alpha(a) \otimes W) = \bigoplus_{a \in R} \{\alpha(a) \otimes w \mid w \in W\}$$

In particular, we have an injective map $W \hookrightarrow V$, $w \mapsto 1 \otimes w = \alpha(e) \otimes w$. Then this gives $W \xrightarrow{\sim} W_e = W_H$, $w \mapsto 1 \otimes w$ an isomorphism of H-representations, since we have

$$h(1 \otimes w) = \alpha(g) \otimes w = 1 \otimes \alpha(h)w = 1 \otimes hw$$

which agrees with the earlier notation $W_{gH} = gW_H$ for all g (in Lemma 2.7.4), as $g(1 \otimes w) = \alpha(g) \otimes w$.

Proposition 2.7.11 (Induced Character). Let G be a finite group, $H < G$, and $R = (G/H)_\ell$ system of representatives. Let W be an H-representation, with V its induced G-representation. Then

$$\chi_V(g) = \frac{1}{|H|} \sum_{u \in G, u^{-1}gu \in H} \chi_W(u^{-1}gu)$$

Proof. Write out explicitly the representation, given by

$$V = \bigoplus_{u \in R} \{\alpha(u) \otimes w \mid w \in W\} =: \bigoplus_{u \in R} W_{uH}$$

Then the action of g is given by $(gu)H = vH$ for $v \in R$, implying that $v^{-1}gu \in H$. Then the corresponding map on W is given as follows:

$$\begin{array}{ccccc} & & \alpha(u) \otimes w & \longleftarrow\!\shortmid & u \\ \alpha(u) \otimes w & & W_{uH} & \simeq & W \\ \downarrow & & \downarrow & & \downarrow \\ \alpha(gu) \otimes w & & W_{vH} & \simeq & W \\ & \searrow\!\!\searrow & & & \\ & & \alpha(v) \otimes (v^{-1}guw) & \longmapsto & (v^{-1}gu) \cdot w \end{array}$$

In particular, setting $v = u$, action of g gives $\alpha(u) \otimes w \mapsto \alpha(u) \otimes (u^{-1}guw)$. Notice $\chi_W(u^{-1}gu)$ is invariant in the same left congruence class: if $uH = u'H$, then $(u')^{-1}u \in H$, giving

$$\chi_W(u^{-1}gu) = \chi_W(\underbrace{((u')^{-1}u)}_{\in H} u^{-1}gu \underbrace{u^{-1}u'}_{((u')^{-1}u)^{-1}})$$

Decomposing the representation into left congruence classes we have

$$\chi_V(g) = \sum_{u \in R, u^{-1}gu \in H} \chi_W(u^{-1}gu) = \frac{1}{|H|} \sum_{u \in G, u^{-1}gu \in H} \chi_W(u^{-1}gu)$$

□

Recall that by Theorem 2.6.3 χ_Vs for V irreducible representations give an orthonormal basis of the class function on G $\mathcal{C}(G)$. The extension of representation then gives an extension of class functions

$$\mathcal{C}(H) \to \mathcal{C}(G), \quad \psi \mapsto \mathrm{Ind}_H^G(\psi) \quad \text{where } \mathrm{Ind}_H^G(\psi)(g) = \frac{1}{|H|} \sum_{u \in G, u^{-1}gu \in H} \psi(u^{-1}gu)$$

which is indeed in $\mathcal{C}(G)$ by the same reasoning as in the proof above. The result in Proposition 2.7.11 then can be formalized as $\chi_{\mathrm{Ind}_H^G}(p) = \mathrm{Ind}_H^G(\chi_p)$. We have the result in the inverse direction by definition: for $\alpha : G \to \mathrm{GL}(V)$ a representation, $\chi_{(\alpha|_H)} = \chi_\alpha|_H$.

Theorem 2.7.12 (Frobenius Reciprocity). For $H < G$, $\varphi \in \mathcal{C}(G)$ and $\psi \in \mathcal{C}(H)$, we have

$$\left\langle \mathrm{Ind}_H^G(\psi), \varphi \right\rangle_G = \langle \psi, \varphi|_H \rangle_H$$

Proof. Since $\mathcal{C}(G)$ and $\mathcal{C}(H)$ have a basis given by the character of irreducible representations, we may assume $\psi = \chi_W$ and $\varphi = \chi_{W'}$, where W is an H-representation, and W' is a G-representation. We need the following extra result:

Parenthesis 2.7.13. If V and V' are (without loss of generality, irreducible) G-representations, then

$$\langle \chi_V, \chi_{V'} \rangle = \dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}[H]}(V, V'|_H)$$

Proof. For LHS = 0 this is given by the orthogonality given by Theorem 2.6.3; and for LHS $\neq 0$ this is given by Schur. □

Use the parenthesis. In this setup, we have

$$\langle \psi, \varphi|_H \rangle_H = \langle \chi_W, \chi_{W'}|_H \rangle = \dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}[H]}(W, W'|_H)$$

On the other hand, by the explicit expression of induced representations we have

$$\left\langle \mathrm{Ind}_H^G(\psi), \varphi \right\rangle_G = \dim_{\mathbb{C}} \mathrm{Hom}_{\mathbb{C}[G]}(\mathbb{C}[G] \otimes_{\mathbb{C}[H]} W, W')$$

where the two spaces we take dimension on are isomorphic by Universal Property of Extension of Scalar. □

Example 2.7.14 (Representations of D_n). We use the induced representation to find out representations on D_n for n even.

Consider $G = D_n = \langle \sigma, \tau \mid \sigma^n = e, \tau^2 = e, \tau\sigma = \sigma^{n-1}\tau \rangle$, $H := \langle \sigma \rangle \subseteq G$. Notice $(G : H) = 2$, $H \trianglelefteq G$, and H is commutative as it is in particular cyclic.

By Example 2.7.3 since H is abelian, every irreducible representation of G has degree $\leq (G : H) = 2$. Consider the 1-dimensional representations of G, which is a group homomorphism $G \to \mathbb{C}^*$, corresponding to $G^{\mathrm{ab}} \to \mathbb{C}^*$.

Now we seek to describe G^{ab}. Compute

$$[\sigma, \tau] = \sigma\tau\sigma^{-1}\tau^{-1} = \sigma\tau\sigma^{n-1}\tau = \sigma(\sigma^{n-1})^{n-1}\tau^2 = \sigma^{n(n-2)+2} = \sigma^2$$

giving $[G, G] \supseteq \langle \sigma^2 \rangle \implies \left| G/\langle \sigma^2 \rangle \right| = 4$. G^{ab} is generated by $\bar{\sigma}$ and $\bar{\tau}$, both of order 2. This implies that $G/\langle \sigma^2 \rangle$ is abelian, and is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. Then σ and τ can only go to ± 1. This gives 4 1-dimensional irreducible representations. Use the result from Corollary 2.5.11, if there are d isomorphic classes of representations we have

$$4 + \sum_{i=1}^{d} 2^2 = |D_n| = 2n \implies d = \frac{n}{2} - 1$$

the other representations cannot be higher as D_n is generated by 2 elements.

Notice that every irreducible G-representation appears in $\mathrm{Ind}_H^G(\rho)$ for ρ some irreducible H-representation (as any decomposition of G-representation restricted to H gives a decomposition of H-representation), we have $\dim_{\mathbb{C}}(\mathrm{Ind}_H^G(W)) = \dim_C(W)\cdot(G:H)$. Therefore, every irreducible representation of D_n with dimension 2 is isomorphic to $\mathrm{Ind}_H^{D_n}(\rho)$ for ρ some 1-dimensional H-representation.

Now consider the 1-dimensional representation of $H = \langle\sigma\rangle \simeq \mathbb{Z}/n\mathbb{Z}$. Since the representatives for G/H are $\{1,\tau\}$, explicitly we have $\mathrm{Ind}_H^{D_n}(\rho) = \mathbb{C}e \oplus \mathbb{C}\tau$ for any H-representation ρ. 1-dimensional representation of H maps σ to powers of $w = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n})$. Denote them to be $\rho_j(\sigma) = w^j$. Viewing $\mathrm{Ind}_H^{D_n}(\rho) = \mathbb{C}e \oplus \mathbb{C}\tau$ as a 2-dimensional $\mathbb{C}$-vector space we have (by $e_2 = \tau e_1$)

$$\text{Action of } \sigma\text{: } \begin{pmatrix} w^j & \\ & w^{-j} \end{pmatrix} \qquad \text{Action of } \tau\text{: } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

Notice that $\mathrm{Ind}_H^{D_n}(\rho_j) = \mathrm{Ind}_H^{D_n}(\rho_{n-j})$, via swapping e_1 and e_2. By symmetry the eigenvectors of τ are given by $\mathbb{C}(e_1+e_2)$ and $\mathbb{C}(e_1-e_2)$. Then $\mathrm{Ind}_H^G(\rho_j)$ is not irreducible if and only if τ and σ maps independently on the vector subspace generated by e_1 and e_2, i.e.

$$\begin{cases} \sigma(e_1+e_2) \in \mathbb{C}(e_1+e_2) \\ \sigma(e_1-e_2) \in \mathbb{C}(e_1-e_2) \end{cases} \implies w^j = w^{n-j} \implies j = 0 \text{ or } \frac{n}{2}$$

Conclusion: There are $\left(\frac{n}{2}-1\right)$ isomorphic classes of irreducible 2-dimensional representations, namely $\mathrm{Ind}_H^{D_n}(\rho_j)$ for $0 < j < \frac{n}{2}$. Any two of them are non-isomorphic, which can be seen via computing the character:

$$\chi(\mathrm{Ind}_H^{D_n}(\rho_j)): \qquad \sigma \mapsto 2\cos\frac{2\pi j}{n}, \quad \tau \mapsto 0$$

which are all distinct (for different j)

As we have seen in the example above, for $H < G$, every irreducible G-representation appears in $\mathrm{Ind}_H^G(\rho)$ for ρ some irreducible H-representation. The question now is, when is $\mathrm{Ind}_H^G(W)$ irreducible for a given H-representation W?

Definition 2.7.15 (Double Coset). Given a group G and a subgroup $H < G$, the **double coset** of H in G is defined as

$$HgH := \{h_1gh_2 \mid h_1, h_2 \in H, g \in G\} = \bigcup_{h\in H}(hg)H$$

where the last union is considered as union of left equivalence classes.

Remark 2.7.16. The double cosets give a partition of G, as for $Hg_1H \cap Hg_2H \neq \emptyset$ we have $g_1 \in Hg_2H$ and therefore $Hg_1H = Hg_2H$.

Notation. The set equivalence classes corresponding to the double coset is denoted $H\backslash G/H$.

Suppose that we have $H \leq G$ a subgroup, Choose S be the set of representatives of double cosets. For each $s \in S$, consider

$H_s := H \cap sHs^{-1}$. Given an H-representation $\rho : H \to \mathrm{GL}(W)$, we get two representations:

$$\begin{cases} \mathrm{Res}_s(\rho) := \rho|_{H_s} \\ \rho_s(u) := \rho(s^{-1}us) \end{cases}$$

Theorem 2.7.17. If ρ is an H-representation, then

$$\mathrm{Ind}_H^G(\rho)\Big|_H = \bigoplus_{s\in S} \mathrm{Ind}_{H_s}^H(\rho_s)$$

Outline of Proof. The proof quite resembles the explicit expression of induced representations: recall that by Lemma 2.7.4 we have

$$\mathrm{Ind}_H^G(\rho)\Big|_H = \bigoplus_{\sigma\in(G/H)_\ell}$$

Define for $\tau \in H\backslash G/H$ $V(\tau) = \bigoplus_{\sigma\in(G/H)_\ell, \sigma\in H\tau H} W_\sigma$ an H-representation. This gives the isomorphism $V(HsH) = \mathrm{Ind}_{H_s}^H(\rho_s)$. □

Remark 2.7.18. An important special case for the discussion is for $H \trianglelefteq G$. Then $H\backslash G/H = G/H$, and $sHs^{-1} = H$ for all $s \in G$. The decomposition above then becomes $\mathrm{Ind}_H^G(\rho)\Big|_H \simeq \bigoplus_{s\in S} \rho_s$.

Remark 2.7.19. In general, for all $H < G$, if $s \in H$, the representation $\rho_s : H \to \mathrm{GL}(W)$ is isomorphic to ρ, with the isomorphism given by

$$\rho \xrightarrow{\sim} \rho_s, \quad w \mapsto s^{-1}w (hw \mapsto (s^{-1}hs)(s^{-1}w)) = s^{-1}hw$$

This is clearly a group homomorphism.

Theorem 2.7.20 (Mackey's Irreducible Criterion)**.** Let $H < G$ be a subgroup, and $\rho : H \to \mathrm{GL}(W)$ a subrepresentation.Then $\mathrm{Ind}_H^G(\rho)$ is irreducible if and only if ρ is irreducible, and for all $s \in S \setminus H$ (where S set of representatives of $H \setminus G/H$), $\rho|_{H_s}$ and ρ_s have no common irreducible components.

Proof. Let $\psi = \mathrm{Ind}_H^G(\rho)$. Then ψ is irreducible if and only if $\langle \chi_\psi, \chi_\psi \rangle_G = 1$. Frobenius Reciprocity gives $\langle \chi_\psi, \chi_\psi \rangle_G = \left\langle \chi_\rho, \chi_{\psi|_H} \right\rangle_H$. Apply the decomposition in Theorem 2.7.17:

$$\text{LHS} = \sum_s \in S \left\langle \chi_\rho, \chi_{\mathrm{Ind}_{H_s}^H(\rho_s)} \right\rangle_H \overset{\text{Frobenius Reciprocity}}{=} \sum_{s\in S} \left\langle \chi_{\rho|_{H_s}}, \chi_{\rho_s} \right\rangle_{H_s}$$

By the remark above, for $s \in S$, $\rho_s \simeq \rho$, giving

$$\text{LHS} = \underbrace{\langle \chi_\rho, \chi_\rho \rangle_H}_{\geq 1, \text{equal iff } \rho \text{ irreducible}} + \sum_{s\in S\setminus H} \underbrace{\left\langle \chi_{\rho|_{H_s}}, \chi_{\rho_s} \right\rangle}_{\geq 0}$$

This is 1 if and only if $\langle \chi_\rho, \chi_\rho \rangle_H = 1$; and $\left\langle \chi_{\rho|_{H_s}}, \chi_{\rho_s} \right\rangle = 0$ for all s, i.e. ρ is irreducible, and $\rho|_{H_s}$ and ρ_s have no common component. □

Chapter 3

Finite Fields and Galois Theory

3.1 Review of Ring Theory

The Galois Theory originates from the question: Given a polynomial with coefficients in a field (e.g. $\mathbb{Q}$), we want to understand the property of its solutions, and the algebraic structure in which the root lies. This section lays some fundamental notions and results for introducing the whole theory.

Setup the convention. All rings have unit element 1; and all ring homomorphisms map 1 to 1. Inclusion maps, in particular, implies that all subrings of a certain ring must include 1.

Remark 3.1.1. An immediate result is that finite domains that are not the zero ring are fields.

Recall that a ring R is a domain if and only if zero does not have non-trivial divisors. That is, for all $x, y \in R \setminus \{0\}$, $xy = 0$. For $a \in R$, $a \neq 0$, consider the map

$$\varphi : R \to R \qquad x \mapsto ax$$

Since R is a domain φ maps nonzero elements to nonzero elements, which implies that there exists some x_a s.t. $ax_a = 1$. This gives an inverse of a.

Proposition 3.1.2. If $f : K \to R$ is a ring homomorphism, and K is a field. Then $R \neq \{0\}$ implies that f is injective.

Proof. Recall that the kernel of a particular ring homomorphism is an ideal. Denote $I = \ker(f) \subseteq K$. Suppose that $a \in I$ s.t. a is nonzero. Then $a^{-1} \in I$ which gives $I = (1) = K \implies f(I) = 0$. But as we requre $f(1) = 1_R \implies 1_R = 0_R$, i.e. $R = \{0\}$ which is a contradiction. □

Corollary 3.1.3. In particular, ring homomorphisms between fields (field extensions) $K \to L$ are injective. Not all fields have extensions (ring homomorphisms) between them.

A class of extensions of which we are particularly interested in, is the extension which gives polynomial a root. $f \in K[x]$ may not have a root; and by extending it $K[x] \hookrightarrow L[x]$ we may consider roots of $f \in L[x]$ which may have a root.

Notation. A field extension $k \hookrightarrow K$ is also denoted as K/k. These two notations will be used interchangeably.

Proposition 3.1.4. Let k be a field, and $R = k[X]$. Let $f \in R \setminus \{0\}$. Then the followings are equivalent:

1) f is irreducible.

2) (f) is a prime ideal.

3) (f) is a maximal ideal.

Proof. Prove the implications cyclically:

- *3) $\implies$ 2).* It is a general fact that maximal ideals are prime. Prove the contrapositive: suppose that an ideal $(f) \subset R$ is not prime, then there exists $a, b \in R$ s.t. $ab \in (f)$ and neither a and b are in (f). Then $(f) \subset (a) \subset R$ which implies that (f) is not maximal.
- *2) $\implies$ 1).* (f) being a prime ideal in R implies that in particular $(f) \neq R$, i.e. f is not invertible. Suppose that there exists g, h not invertible s.t. $f = gh$. Without loss of generality, assume that $g \in (f)$. Then there exists some $u \in R$ s.t. $g = fu$. Multiply on the right by h gives $f = gh = fuh$ which implies that h is invertible, giving a contradiction.
- *3) $\implies$ 1).* f being irreducible implies that f is not invertible, i.e. $(f) \neq R$. Suppose that there exists some maximal ideal J s.t. $(f) \subset J \subset R$. Then since maximal ideals are in particular prime, $J = (g)$ for some $g \in R$. But then this implies that $f = gu$ giving that u is invertible, and therefore $(f) = J$, which is a contradiction.

□

Recall that two elements f, g are relative prime if for all $p \in R$ s.t. $p \mid f, p \mid g$, p is invertible. Then we have the following result similar to the case for integer divisibility:

Proposition 3.1.5. Let k be a field, and $R = k[x]$. For $f, g, h \in R$ s.t. $f \mid gh$, if f and g are relative prime, then $f \mid h$.

Proof. Since k is a field, $k[x]$ is a PID (as every element in the coefficient is invertible, for a, b relative prime $(a, b) = (1) = k[x]$). Consider $I = (f, g) \subseteq R$. Since I is principal, $I = (p)$ for some $p \in k[x]$. Therefore $p \mid f, p \mid g$, which implies that p is invertible. Then $I = R$. This gives that there exists $A, B \in R$ s.t. $Af + Bg = 1$. Multiplying h on the right gives $Afh + Bgh = h$. Since f divides LHS, $f \mid h$. □

Proposition 3.1.6. Let k be a field, and $R = k[x]$. If $f \in R \setminus \{0\}$, and denoting $d = \deg f$, then there exists field extensions $k \hookrightarrow L$ and $a_1, \ldots, a_d \in L$, $c \in k$ s.t. $f = c(x - a_1) \cdots (x - a_d)$ in $L[x]$.

Proof. The key step is to show that if f is irreducible in R, then there exists a field extension $k \hookrightarrow k'$ s.t. f has a root in k'.

Consider $k' = k[x]/(f)$. Since f is irreducible, (f) is a maximal ideal in R, and therefore k' is a field. Since elements in k are of degree 0 in $k[x]$. Considering $k \longrightarrow k[x] \longrightarrow k' := k[x]/(f)$ gives the injective ring homomorphism (field extension). Let $a = \overline{x} \in k'$. Then $f(a) = \overline{f(x)} = 0$, which implies that a is a root of f.

Proceed the rest of the proof by induction:

- $d = 0$. This is the trivial case.
- $d = 1$. Then $f = c(x - a)$ for some $c, a \in k$.
- $d \geq 2$. Apply the above steps iteratively. Then there exists some $a \in k'$ s.t. $(x-a) \mid f$, i.e. in $k'[x]$ we have the decomposition $f = (x - a)g$ for some $g \in k'[x]$ with $\deg g = \deg f - 1$. Applying the inductive hypothesis (the results holds in lower degrees) gives the full decomposition in $L := k'$.

□

Notation. Denote the image of the map $(k[y] \to k, y \mapsto a)$ by $k[a]$. This is the smallest k-algebra containing a.

Proposition 3.1.7. Let k be a field, and $R = k[x]$. Let $f \in R \setminus \{0\}$ be irreducible. Suppose that we have the field extension $k \hookrightarrow K$, and $a \in K$ is a root of f. Then $k[a] \simeq k[x]/(f)$. In particular, $k[a]$ is a field.

Proof. Consider the ring homomorphism $\varphi : k[y] \to K$ s.t. $\varphi(y) = a$. Then by the First Isomorphism Theorem, we have $k[a] = \operatorname{im} \varphi \simeq k[x]/\ker \varphi \simeq k[x]/(f)$ since $f(a) = 0$. □

Notice that every field extension $k \hookrightarrow K$ is a k-algebra morphism (ring homomorphisms that are k-linear). Since k is a field, this gives K a k-vector space structure.

Definition 3.1.8 (Degree). The **degree** of the field extension $k \hookrightarrow K$, denoted $[K : k]$, is $\dim_k K \in \mathbb{Z}_{\geq 0}$ or infinite.

Definition 3.1.9 (Finite). A field extension is **finite** if the degree of it is finite.

Remark 3.1.10. If $f \in k[x]$ is irreducible, and $K = k[x]/(f)$, then $[K : k] = \deg f$. More generally, if $g \in k[x]$ is a nonzero polynomial, then $\dim_k(k[x]/(g)) = \deg g$.

This can be seen via applying the division algorithm (since $K[x]$ is an Euclidean Domain. This can be seen via computing the division). Then for all $P \in k[x]$, there exists unique $Q, R \in k[x]$ s.t. $P = gQ + R$, with $\deg R < \deg g$. Then since $\overline{P} = \overline{R}$ in $k[x]/(g)$, $\{\bar{1}, \bar{x}, \ldots, \overline{x^{\deg g - 1}}\}$ gives a basis of $k[x]/(g)$ over k.

3.2 Multiplicity of Root

This section provides tools for describing the zeros of a polynomial, and how they in general can look like. The proposition below says that any polynomial can be factored into two parts, with the first part having roots in the field; and the second part requires extension of the field to decompose completely.

Definition 3.2.1 (Multiplicity). Let $f \in k[x]$ be a nonzero polynomial for k a field, and $a \in R$ a root of f, Then a has **multiplicity** m if $(x - a)^m \mid f$, but $(x - a)^{m+1} \nmid f$.

Proposition 3.2.2. If $f \in R \setminus \{0\}$, and $a_1, \ldots, a_r \in k$ are pairwise distinct roots of f s.t. a_i has multiplicity m_i. Then we

have the decomposition of f:

$$f = \prod_{i=1}^{r} (x - a_i)^{m_i} g, \qquad g \in R, g(a_i) \neq 0 \text{ for all } i$$

In particular, $\sum_i m_i \leq \deg f$.

Proof. Apply induction on r:

- *Base case.* Then m_1 is the maximal integer satisfying the condition that $(x - a_1)^{m_1} \mid f$. Then define g be such that $f = (x - a_1)^{m_1} g$.
- *Inductive step.* For $r \geq 2$, denote f_1 be the polynomial s.t. $f = (x - a_1)^{m_1} f_1$. Notice that for all i s.t. $2 \leq i \leq r$, we have $(x - a_i)^{m_i} \mid f$. Then since $(x - a_i)$ and $(x - a_1)$ are relative prime (they are both irreducible) by Proposition 3.1.5 we have $(x - a_i)^{m_i} \mid f_1$. Then applying inductive hypothesis gives the desired decomposition of f.

□

3.3 Characteristic of a Field

Recall that in the first section we mentioned that there does not necessarily exist ring homomorphisms between arbitrary fields. This, as we will see in the following, implies some constraints on the structure that a field can have.

Let S be an integral domain. Let $\varphi : \mathbb{Z} \to S$ s.t. $n \mapsto n \cdot 1_S$. This is the unique ring homomorphism between $\mathbb{Z}$ and S due to the constraint the 1 should be mapped to 1. Since S is a domain, and $\mathbb{Z}$ is a PID, $\ker \varphi = (d)$ for d prime or zero. Then either

1) $\ker \varphi = \{0\}$; or

2) $\ker \varphi = p\mathbb{Z}$ for some p prime.

In case 1), if we suppose further that $S = k$ which is a field, then for all $n \in \mathbb{Z}$ $\varphi(n)$ is invertible. By the universal property of the quotient ring, this induces a ring homomorphism (which is also a field extension) $\mathrm{Frac}(\mathbb{Z}) = \mathbb{Q} \hookrightarrow S$.

In case 2), we have an injective ring homomorphism $\mathbb{Z}/p\mathbb{Z} \hookrightarrow S$ for some p prime. Defining $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, S becomes an $\mathbb{F}_p$-algebra by the φ above.

Definition 3.3.1 (Characteristic)**.** For a field k, the **characteristic** of k is

$$\mathrm{char}(k) = \begin{cases} p, & \text{if } \mathbb{F}_p \hookrightarrow k \text{ (case 1)} \\ 0, & \text{if } \mathbb{Q} \hookrightarrow k \text{ (case 2)} \end{cases}$$

Remark 3.3.2. If S is an $\mathbb{F}_p$-algebra (case 2), the map $F : S \to S$, $u \mapsto u^p$ is the Frobenius homomorphism. Check that this is indeed a ring homomorphism:

- $F(uv) = F(u)F(v)$. Clear as field is commutative: $(uv)^p = u^p v^p$.

- $F(u+v) = F(u) + F(v)$. Compute:

$$(u+v)^p = u^p + v^p + \underbrace{\sum_{i=1}^{p-1} \binom{p}{i} u^{p-i} v^i}_{\text{divisible by } p}$$

  where the last term vanishes, as $\mathbb{F}_p \hookrightarrow S$ should map 0 to 0; and $\bar{p} = \bar{0} \in \mathbb{F}_p$.

3.4 Algebraic Extensions

The field extensions originating solely from "including the roots of polynomials" are the nice ones and deserve a better name. The discussions formalizes the concept of "algebraic closure" in elementary discussions of polynomials.

Proposition 3.4.1. If $k \hookrightarrow K \hookrightarrow L$ is a field extension, then $[L : k] = [L : K][K : k]$.

Proof. First consider the cases where one of the degrees is infinite:

- If $[K : k]$ is infinite, then $[L : k]$ is infinite as $K \subseteq L$ is a K-vector subspace of L.
- If $[L : K]$ is infinite, then there exists an infinite set of elements which are linearly independent over K, which are also linearly independent over k since $k \subseteq K$.

Now consider the case where both $[L : K]$ and $[K : k]$ are finite. Denote $m = [L : K]$ and $n = [K : k]$. Denote $\{a_1, \dots, a_m\}$ be a basis of L over K, and $\{b_1, \dots, b_n\}$ be a basis of K over k. Notice that $\{a_i b_j \mid 1 \le i \le m, 1 \le j \le n\}$ gives a basis for L over k, as for all $u \in L$, there exists $\lambda_i \in K$, and thus $\mu_{ij} \in k$ s.t.

$$u = \sum_{i=1}^{n} \lambda_i b_i = \sum_{i,j} \mu_{ij} a_j b_i, \qquad \text{for } \lambda_i = \sum_j \mu_{ij} a_j \mu_{ij}$$

which is a decomposition. They are further linearly independent, as for $u = 0$, since b_is give a basis, $\lambda_i = 0$ for all i, and therefore $\mu_{ij} = 0$ for all i and j. □

Notation. Let $k \hookrightarrow K$ be a field extension, and $A \subseteq K$ a subset. Then we denote

$$k(A) := \bigcap_{A \subseteq k'} \{k' \mid k \hookrightarrow k' \hookrightarrow K \text{ extension}\}$$

which is the smallest field sub-extension of k inside K containing A.

Remark 3.4.2. It is worth mentioning that this is different from $k[A]$ which is the smallest *k-subalgebra* containing A:

- They are related via $k(A) = \mathrm{Frac}(k[A])$. They are equal in some "nice" extensions (see Remark 3.4.9 below).

  By definition we have $k[A] \subseteq k(A)$, as $k[A]$ is only required to be a k-algebra instead of a field extension of k (as field extending k can be seen as k-vector spaces, which are in particular k-algebras). By the universal property of fraction fields, we have $\mathrm{Frac}(k[A]) \subseteq k(A)$, as ring homomorphisms between fields are injective, and by definition for all $f \in k[A]$, f has an inverse in $k(A)$. Further since $A \subseteq \mathrm{Frac}(k[A])$ (also by definition, we have $k(A) = \mathrm{Frac}k[A]$).

- Considering multiple elements, we can extend the previous notation, by considering for $A = \{a_1, \dots, a_n\}$, then $k[A] = \operatorname{im} \varphi$ for

$$\varphi : k[x_1, \dots, x_n] \to K, \qquad x_i \mapsto a_i$$

Definition 3.4.3 (Finite Generated). A field extension K/k is **finitely generated** if there exists $a_1, \dots, a_n \in K$ s.t. $k(a_1, \dots, a_n) = K$.

Remark 3.4.4. If a field extension K/k is finite, then it is also finitely generated, as K/k being finite implies that there exists some finite basis of K over k; and picking one gives the elements that "finitely generates" K. However, the converse is not true: consider $k \hookrightarrow k(x) = \operatorname{Frac}(k[x])$ is finitely generated (by x) but is not finite (we have the infinite set $\{x^i \mid i \in \mathbb{Z}\}$ whose elements are linearly independent over k)

Definition 3.4.5 (Algebraic; Transcendental). Let $k \hookrightarrow K$ be a field extension. An element $a \in K$ is **algebraic over** k if there exists $f \in k[x] \setminus \{0\}$ s.t. $f(a) = 0$ in $K[x]$. Otherwise a is **transcendental**. An extension K/k is **algebraic** if for all $a \in K$, it is algebraic over k.

Remark 3.4.6. Consider the field extensions $k \hookrightarrow K \hookrightarrow L$. Then if $a \in L$ is algebraic over k, then a is also algebraic over K, as a algebraic over k implies that there exists $f \in k[x]$ s.t. $f(a) = 0$; and by definition we also have $f \in K[x]$.

Remark 3.4.7. Given a field extension $k \hookrightarrow K$, and $a \in K$. Then a is algebraic if and only if the $\varphi : k[x] \to k, x \mapsto a$ has a non-trivial kernel. This is the direct translation of having a polynomial f with a as its root. Then $\ker \varphi$ is a prime ideal.

To prove this, it suffices to show that $k[x]/(\ker \varphi)$ is a domain. This is indeed the case, as $k[x]$ is a domain: for all $g, h \in k[x]$, $g(a) \neq 0$ and $h(a) \neq 0$ implies that $gh(a) \neq 0$, i.e. $gh \notin \ker \varphi$ ($gh \neq \bar{0}$ in $k[x]/(\ker \varphi)$). Therefore, there exists some f s.t. $\ker \varphi = (f)$.

Definition 3.4.8 (Minimal Polynomial). $f \in k[x]$ is the **minimal polynomial** of $a \in K$ if for $\varphi : k[x] \to K$, $x \mapsto a$, $\ker \varphi = (f)$. This is well-defined by the above Remark (Remark 3.4.7).

Remark 3.4.9. For a being algebraic, f is a maximal ideal (by the fact that $k[x]/(\ker \varphi)$ is a domain). Then $k[a] = k[x]/(\ker \varphi)$ is a field. This gives $k[a] = k(a)$.

Remark 3.4.10. Given field extension K/k, if $a \in K$ is transcendental over k, then $k[a] \simeq k[x]$, as since there is no polynomial with root a implies that $k[a]$ can be seen as injecting a formal variable to the field $k[x]$. This further implies $k(a) \simeq k(x)$ (as $k(a) \simeq \operatorname{Frac}(k[a])$; and same for x).

Example 3.4.11. Suppose that $d \in \mathbb{Z}$ is not a square, and let $a = \sqrt{d}$. Consider the field extension $\mathbb{Q} \to \mathbb{C}$.

Since a is not in $\mathbb{Q}$, a cannot be a root of degree 1 polynomials, i.e. the minimal polynomial of a must be of degree at least 2; and we have a as a root of $x^2 - d = 0$, the minimal polynomial of a over k is $x^2 - d = 0$, which also implies that a is algebraic over $\mathbb{Q}$.

Therefore, $\mathbb{Q}(\sqrt{d})$ can be seen as a $\mathbb{Q}$-vector space, which has a basis $\{1, \sqrt{Q}\}$, i.e. $\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$. In

particular we have $\dim_{\mathbb{Q}} \mathbb{Q}(\sqrt{d}) = 2$ as $\deg f = 2$, resulting from Remark 3.1.10.

Proposition 3.4.12. Every finite extension K/k is algebraic.

Proof. Denote $[K : k] = n$ which is finite. Regarding K as a k-vector space, for all $a \in K$ the set of elements $\{1, a, \dots, a^n\}$ are linearly dependent (as there are $(n+1)$ of them). That is, there exists $c_0, \dots, c_n \in k$ s.t. $c_0 + c_1 a + \cdots + c_n a^n = 0$; and $f = c_0 + c_1 x + \cdots + c_n x^n \in k[x] \setminus \{0\}$. This gives a polynomial $f \in k[x]$ s.t. $f(a) = 0$, i.e. a is algebraic. Since $a \in K$ can be taken arbitrarily, we have K/k being algebraic. □

Proposition 3.4.13. Let $k \hookrightarrow K$ be a field extension, and $a_1, \dots, a_n \in K$ are algebraic over k. Then $k[a_1, \dots, a_n] = k(a_1, \dots, a_n)$; and $k(a_1, \dots, a_n)$ is a finite extension over k.

Proof. Remark 3.4.9 gives the case for $n = 1$, $k[a] = k(a)$, and Remark 3.1.10 (using minimal polynomial) gives that the extension is finite.

For $n \geq 2$, repeat the argument with the induction hypothesis. First by definition we have $k[a_1, \dots, a_n] = (k[a_1, \dots, a_{n-1}])[a_n]$; and the same holds for the field extension version (replace brackets with parentheses). Further finite extensions are transitive, by Proposition 3.4.1. Suppose now that $k' = k[a_1, \dots, a_{n-1}] = k(a_1, \dots, a_{n-1})$ is a finite extension over k. Then $k[a_1, \dots, a_n] = k'[a_n] = k'(a_n) = k(a_1, \dots, a_n)$ is finite over k'; and by hypothesis we know $k'[a_n]$ is finite over k since k' is. □

Corollary 3.4.14. Finitely generated algebraic field extensions are finite.

Proposition 3.4.15. If $k \hookrightarrow K \hookrightarrow L$ are both algebraic field extensions, then so is $k \hookrightarrow L$.

Proof. Use the above two propositions. Let $a \in L$. Since L/K is algebraic, there exists $f \in K[x] \setminus \{0\}$ s.t. $f(a) = 0$. Let $f = c_0 + c_1 x + \cdots + c_n x^n$, and $k' = k(c_0, \dots, c_n)$. Since all $c_0, \dots, c_n \in K$ are algebraic over k, Proposition 3.4.13 implies that k' is a finite extension over k. Further since a is algebraic over k', the extension $k' \hookrightarrow k'(a)$ is also finite. Proposition 3.4.12 implies that the extension $k \hookrightarrow k'(a)$ is algebraic. That is, a is algebraic over k.

Since this holds for all $a \in L$, the extension L/k is algebraic. □

Remark 3.4.16. Notice that the converse of the statement is also true. If $k \hookrightarrow L$ is algebraic, then for every element $a \in L$ there exists some $f_a \in k[x]$ s.t. $f_a(a) = 0$. But given extension $k \hookrightarrow K \hookrightarrow L$, $k \subseteq K$, which implies f_a is also in $K[x]$; and therefore L/K is algebraic

Proposition 3.4.17. If $k \hookrightarrow K$ is a field extension, then $k' = \{a \in K \mid a \text{ algebraic over } k\}$ is a subfield of K containing k,

Proof. To prove this we need to check:

- $k \subseteq k'$. This is clear from the construction of the field.

- k' is closed under additive and multiplicative inverse.

  $a \in k'$ implies $-a \in k'$ as $-a$ is the root of a polynomial via considering the minimal polynomial and inverting the corresponding coefficients. $a \in k' \setminus \{0\}$ implies $a^{-1} \in k' \setminus \{0\}$ since $k[a] = k(a)$ as $k(a)$ is finitely generated, and therefore finite and algebraic. $k(a)$ is a field, implying that $a^{-1} \in k(a)$.

- k' is closed under addition and multiplication. That is, for all $a, b \in k'$, $a + b \in k'$ and $ab \in k'$.

  Consider the field $k(a, b)$. Since both a and b are algebraic over k, $k(a, b)/k$ is finite by Proposition 3.4.13; and by Proposition 3.4.12 the extension is algebraic. By definition $k(a, b) \subseteq k'$; and is the smallest field containing both a and b; and therefore both $a + b$ and ab are in k'.

□

Definition 3.4.18 (Algebraic Closure)**.** For a field k with field extension $k \hookrightarrow K$, the field $k' = \{a \in K \mid a \text{ algebraic over } k\}$ is the **algebraic closure** of k in K. By the above Proposition 3.4.17, this is indeed a field.

Definition 3.4.19 (Algebraically Closed)**.** A field k is **algebraically closed** if every nonzero polynomial over k has a root in k.

Remark 3.4.20. By induction, if k is algebraically closed and f is a nonzero polynomial in $k[x]$ with degree n¡ then there exists $a_1, \ldots, a_n \in k$, $c \in k^*$ s.t. $f = c(x - a_1) \cdots (x - a_k)$. That is, every irreducible polynomial in an algebraically closed field has degree 1.

Notation. For a field k, the set of invertible (nonzero) elements in it are often denoted as k^* or $k^\times$.

Proposition 3.4.21. A field k is algebraically closed if and only if for all field extensions $k \hookrightarrow K$, for all $a \in K \setminus k$, a is transcendental over k.

Proof. Prove implication in two directions:

$\Rightarrow$: Suppose that k is algebraically closed, and $a \in K \setminus k$ algebraic over k. Then by definition there exists an irreducible polynomial $f \in k[x]$ s.t. $f(a) = 0$. Since k is algebraically closed, the irreducible polynomials are of degree 1, i.e. $\deg f = 1$. Then $a \in k$, which is a contradiction.

$\Leftarrow$: Suppose that for all $a \in K \setminus k$, a is transcendental. Proceed to prove that k is algebraically closed by showing that every irreducible polynomial has a root.

Consider $f \in k[x] \setminus \{0\}$. Consider $K = k[x]/(f)$. Then since $f(\bar{x}) = 0$, $\bar{x}$ is algebraic over k. But since all elements in $K \setminus k$ are transcendental, $\bar{x} \in k$. Then in K we have $\bar{x} - a = 0$, for some $a \in k$. Then $f(x) = x - a$ in $K[x]$ which has a root a; and as this holds for all f, k is algebraically closed.

□

In summary, a field k being algebraically closed is equivalent to the following conditions:

1) For all field extensions $k \hookrightarrow K$, either $k \simeq K$, or the extension is not algebraic.

2) For all $f \in k[x] \setminus \{0\}$, f factors as a product of polynomials of degree 1.

3) Every irreducible $f \in k[x] \setminus \{0\}$ has a root in k.

Recall that we have the algebraic closure in a specific field. The following theorem seeks to construct such closure without any ambient structure:

Theorem 3.4.22. Given any field k, there exists an algebraic extension $k \hookrightarrow \bar{k}$ s.t. $\bar{k}$ is algebraically closed. Such an extension is an algebraic closure of k.

Parenthesis 3.4.23 (Direct Limit (of rings)). To provide the construction of an algebraic closure, the main step is to iteratively include the roots of the some irreducible polynomials; and we need to ensure that this process terminates. That is, there exists a field containing all the intermediate fields on which we conducted the extension. This parenthesis formalizes this idea.

Definition 3.4.24 (Directed Set). $(I, \leq)$ is a **directed set** if for all $i, j \in I$ there exists $k \in I$ s.t. $i \leq k$ and $j \leq k$.

Definition 3.4.25 (Direct System). Given a directed set I, a **direct system** $(R_i)_{i \in I}$ is a family of rings R_i satisfying:

- For all $i \leq j$ in I, there exists a ring homomorphism $\varphi_{ij} : R_i \to R_j$; and $\varphi_{ii} = \mathrm{Id}_{R_i}$.
- For all $i \leq j \leq k$ in I, the ring homomorphisms above satisfy $\varphi_{ik} = \varphi_{jk} \circ \varphi_{ij}$.

Definition 3.4.26 (Direct Limit). Given a direct system $(R_i)_{i \in I}$, the **direct limit** of the system, denoted $R = \varinjlim R_i$, together with a family of ring homomorphisms $f_i : R_i \to R$ s.t.

- $f_j \circ \varphi_{ij} = f_i$.
- The pair $(R, (f_i)_{i \in I})$ is universal with this property, i.e. every ring homomorphism from R_i for all i factors uniquely through R. That is, for any ring T and family of ring homomorphisms $g_i : R_i \to T$ s.t. $g_j \circ \varphi_{ij} = g_i$ (the g_is are compatible w.r.t. the system), there exists a unique ring homomorphism $g : R \to T$ s.t. $g \circ f_i = g_i$ for all i.

The direct limit exists, by considering the class of elements that are closed along the morphisms of R_is: define $R := \left(\bigsqcup_{i \in I} R_i\right) / \sim$, where the equivalence relation $\sim$ is given by $R_i \ni x_i \sim \varphi_{ij}(x_i)$. The operations are given by for $a_i \in R_i$ and $b_j \in R_j$, finding k s.t. $i \leq k$ and $j \leq k$ (which exists as I is a directed set), and define:

$$a_i + b_j := \varphi_{ik}(a_i) + \varphi_{jk}(b_j) \in R_k, \qquad a_i b_j := \varphi_{ik}(a_i) \cdot \varphi_{jk}(b_j) \in R_k$$

Existence of inverse, and distributivity are guaranteed by the ring structure of R_j. Further see that this is well-defined, as for $k' \neq k$ that we have picked s.t. $i \leq k'$ and $j \leq k'$, since the set is directed there exists ℓ s.t. $k \leq \ell$ and $k' \leq \ell$. Now use the equivalence relation with $\varphi_{k\ell}$ and $\varphi_{k'\ell}$; and the fact that $\sim$ is an equivalence relation and is therefore transitive.

Further the direct limit of a direct system is unique up to isomorphism. Suppose we have two direct limits R and R', there exists $g : R \to R'$ and $g' : R' \to R$, by the universal property of the direct limit s.t. $g \circ f_i = f'_i$, $g' \circ f'_i = f_i$. This implies that $g \circ g' = \mathrm{Id}_{R'}$, and $g' \circ g = \mathrm{Id}_R$ by the symmetric argument. This gives the isomorphism.

The last thing we need to notice is that if all R_is are fields, then R is a field, as in the definition of the operation having multiplicative inverse in R_k induces the multiplicative inverse in R.

Now we can use the above tools to describe the polynomial with variables indexed by a (possibly infinite) set I. Given a commu-

tative ring R, a set I, the polynomial ring $R[x_i \mid i \in I]$ is defined as follows:

For $J \subset I$ finite subset, denote $R_J := R[x_i \mid i \in J]$. Define $\mathcal{P} := \{\text{finite subsets of } I\}$, ordered by inclusion. This is a directed set, as for all $M, N \in \mathcal{P}$, we have $M \subseteq I$ and $N \subseteq I$ by definition.

For $J_1 \subseteq J_2$ in $\mathcal{P}$, we have a morphism of R-algebras $\varphi_{J_1 J_2} : R_{J_1} \to R_{J_2}, x_i \mapsto x_i$ (embeddings). This gives a direct system of R-algebras; and we can define $R[x_i \mid i \in I] := \varinjlim (R_J)_{J \in P}$. Notice:

- All $\varphi_{J_1 J_2}$ are injective (as they are embeddings), and therefore the map $R_J \to R[x_i \mid i \in I]$ is also injective.
- Observe that we have $\bigcup_{J \in \mathcal{P}} R_J$ is a direct limit of the system $(R_J)_{J \in \mathcal{P}}$; and since the direct limit is unique up to isomorphisms for a particular directed system, we have $R[x_i \mid i \in I] = \bigcup_{J \in \mathcal{P}} R_J$.

Now prove the theorem:

Proof of Theorem 3.4.22. As we have mentioned, the idea of the proof is to construct a direct system of fields, where each φ (which is a field extension here) includes the roots of irreducible polynomials in the base field; then taking the direct limit of the system gives the desired algebraic closure.

The first step is to construct a field extension $k \hookrightarrow k_1$ s.t. for all $f \in k[x]$ irreducible, there exists $a \in k_1$ s.t. $f(a) = 0$. Define $A = \{f \in k[x] \mid f \text{ irreducible}\}$. Define $R = k[y_f \mid f \in A]$ and $\underline{a} = (f(y_f) \mid f \in A)$ where y_f are formal variables indexed by polynomials in A; and the parenthesis in $\underline{a}$ implies that this is an ideal generated by such elements.

Claim that $\underline{a} \neq R$. First observe that by definition $\underline{a} \subseteq R$, as in particular we have $f \in k[y_f] \subseteq k[y_f \mid f \in A] =: R$. Suppose that $\underline{a} = R$. Then the condition is translated to:

$$\exists r \in \mathbb{Z}_{>0},\ f_1, \dots, f_n \in A,\ g_1, \dots, g_n \in R, \qquad \sum_{i=1}^{r} \underbrace{g_i}_{\in R} \underbrace{f_i(y_{f_i})}_{\in \underline{a}} = 1 \tag{$*$}$$

as the ideal being equal to the whole ring is the same as the ideal containing 1. By Proposition 3.1.7, for all i there exists field extension $k \hookrightarrow k_i$ s.t. there exists $a_i \in k_i$ satisfying $f_i(a_i) = 0$. Since there finitely many (exactly r) polynomials, we can do this iteratively and get a field extension $k \hookrightarrow K$ s.t. there exists field extensions $k_i \hookrightarrow K$ for all i.

Let $J \subseteq A$ be the finite subset containing all the f_is, and also containing all polynomials g s.t. y_g appears in some $g_i \in k$. Define $\varphi : k[y_g \mid g \in J] \hookrightarrow K$. $y_{f_i} \mapsto a_i$ for all i, and $y_g \mapsto \varepsilon \in K$ which is some value we do not care about. Recall that a_is are defined s.t. $f_i(a_i) = 0$. This is a k-algebra morphism.

Now apply φ to Eq. ($*$). Since φ is k-linear, we have

$$0 = \sum_{i=1}^{r} \varphi(g_i) f_i(a_i) = \varphi(1) = 1$$

which is a contradiction, as for a field we require $0 \neq 1$. Therefore $\underline{a} \neq R$. Further since $\underline{a}$ is an ideal in R, there exists a maximal ideal M in R s.t. $\underline{a} \subseteq R$. Define $k' = R/M$ which is not trivial since $\underline{a} \neq R$. Denote $k_1 := \{a \in k' \mid a \text{ algebraic over } k\}$. By Proposition 3.4.17 this is a subfield of k', and by definition is algebraic over k. Now consider $f \in k[x]$ irreducible, and $\overline{y_f} \in k' = R/M$ a formal variable. By definition of algebraic closure, $f(\overline{y_f}) = 0$ in $\bar{k}$; and since $f(y_f) \in \underline{a} \subseteq M$, $\overline{f(y_f)} = f(\overline{y_f}) = 0 \in R/M$, which implies that $\overline{y_f} \in k_1$. Since $k' = R/M$ with R extending elements in the form of y_f, every element in k' is in the same as

$\overline{y_f}$ for some $f \in A$; and by the previous argument we know $k \hookrightarrow k'$ is algebraic. That is, every $f \in k[x]$ irreducible has a root in k_1.

Now repeat the process with k replace by k_1. Conducting induction gives that for all $f \in k_i[x]$, there exists $a \in k_{i+1}$, $f(a) = 0$ in $k_{i+1}[x]$. This gives algebraic extensions

$$k \hookrightarrow k_1 \hookrightarrow k_2 \hookrightarrow \cdots$$

Now take $\bar{k} := \varinjlim k_i$. This is a field by Parenthesis 3.4.23 satisfying $k \hookrightarrow k_i \hookrightarrow \bar{k}$, and by the following remark $\bar{j} = \bigcup_{i \geq 1} k_i$. Check:

- $\bar{k}$ *is algebraic over* k. This results from the fact that each of the intermediate extension is algebraic; and the result follows from Proposition 3.4.15.
- $\bar{k}$ *is algebraically closed.* For all $f \in \bar{k}[x]$, there exists i s.t. $f \in k_i[x]$. Then f has a root in k_{i+1} which can be extended to K by universal property of direct limit.

□

Remark 3.4.27. If the field k is infinite, the algebraic closure $\bar{k}$ is of the same cardinality as k.

To address the uniqueness of $\bar{k}$, we prove the following theorem that is more general:

Theorem 3.4.28. Given two field extensions $k \hookrightarrow K$ and $k \hookrightarrow L$ s.t. K/k is algebraic, and L is algebraically closed. Then there is a morphism of k-extensions $K \hookrightarrow L$, where a morphism of k-extensions is a morphism of k-algebras which is the identity map when restrict to k.

To prove the theorem we need Zorn's Lemma:

Lemma 3.4.29 (Zorn). Given a nonempty ordered set $(A, \leq)$ s.t. every chain in A has an upper bound in A. Then a has a maximal element. The terminologies are:

- A chain is a totally ordered subset.
- An upper bound for $B \subseteq A$ is an element $a \in A$ s.t. for all $b \in B, b \leq a$.
- A maximal element in A is some $a \in A$ s.t. for all a' s.t. $a \leq a'$, we have $a' = a$.

Proof of Theorem 3.4.28. Consider the set $A = \{(k', \varphi)\}$ where k' is a subfield of K for which there exists extensions $k \hookrightarrow k' \hookrightarrow K$; and for $i : k \to k'$, $j : k \to L$ we have $\varphi \circ i = j$. Define the partial order on A be such that $(K', \varphi) \leq (K'', \psi)$ if and only if $K' \subseteq K$, and $\psi|_{k'} = \varphi$.

Now apply Zorn. Check the followings:

- A is non empty. In particular, $(k, j) \in A$.
- Suppose that $B = \{(K_i, \varphi_i) \mid i \in I\}$ is a chain (totally ordered subset) in A, Then B has a maximal element (which also serves as an upper bound) (K, φ) given by $K = \bigcup_{i \in I} K_i$ and φ be such that $\varphi|_{K_i} = \varphi_i$. Such φ exists as B is totally ordered, i.e. for any subset of B the maximal element gives the corresponding φ.

Then Zorn's Lemma gives that there exists a maximal element $(K', \varphi) \in A$. Then either:

- $K' = K$. This gives the desired result.
- $K' \neq K$. We seek to find a contradiction. Since $K' \subseteq K$, there exists $a \in K \setminus K'$. Since K/k is algebraic by hypothesis, by Remark 3.4.16, K/K' is also algebraic. Let $f \in K'[x]$ be the minimal polynomial of a over K'. Try to extend on a:

$$K' \hookrightarrow K'[a] \simeq K'(a) \simeq K'[x]/(f)$$

  where $K'[a] = K'(a)$ since a is algebraic over k'. Since L is algebraically closed, f (considering it in $L[x]$) has a root $b \in L$. Then there exists a unique K'-algebra morphism $\varphi' : K'(a) \to L$, $a \mapsto b$, which is indeed a K'-algebra morphism as any $g \in K[x]$ s.t. $g(a) = 0$ satisfies $f \mid g$, which has b also as a root. But then $(K'(a), \varphi')$ satisfies the condition, which contradicts with the maximality of (K', φ).

Therefore $K' = K$ and we have the desired result. □

Corollary 3.4.30. The algebraic closure of a given field k is unique up to isomorphism.

Suppose that we have field extensions $k \hookrightarrow K$ and $k \hookrightarrow L$, with both K and L algebraically closed. Then applying the above theorem twice gives field extensions $K \hookrightarrow L$ and $L \hookrightarrow K$, which are both injective by Proposition 3.1.2. This gives the desired isomorphism.

Notation. Since the algebraic closures of a specific field k are isomorphic, we can simply refer to it as *the* algebraic closure, and denote it with $\bar{k}$.

Remark 3.4.31. We have the following immediate results:

1) If $k \hookrightarrow K$ is algebraic, and $K \hookrightarrow \overline{K}$ algebraic closure, then $k \hookrightarrow \overline{K}$ is also an algebraic closure (by considering $f \in k[x]$ as elements of $K[x]$).
2) If we have $k \hookrightarrow K$ a field extension, and K is algebraically closed. Then for $k' := \{a \in K \mid a \text{ algebraic over } k\}$ we have k'/k an algebraic closure. This is clearly algebraic by definition; and it is closed as if $f \in k'[x] \setminus \{0\}$, there exists $a \in K$ s.t. $f(a) = 0$ as K is algebraically closed. Then a is algebraic over $k \implies k' \hookrightarrow k'(a)$ finite $\implies k' \hookrightarrow k'(a)$ algebraic $\implies k \hookrightarrow k' \hookrightarrow k'(a)$ algebraic. But this gives the fact that a is algebraic over k, and since $a \in K$ by definition $a \in k'$.

Notice that we cannot use the same trick in the proof for Theorem 3.4.22 as in that case the extensions $k \hookrightarrow k_1$ is not necessarily algebraic.

Now we can use the above results to classify finite fields:

Let K be a finite field. Since $\mathbb{Z} \to K$ cannot be injective, $\mathrm{char}(K) = p$ for some prime p. This gives a field extension $\mathbb{F}_p \hookrightarrow K$; and since $e = [K : \mathbb{F}_p]$ is finite (since K is finite), $|K| = p^e$ for some e. Denote $\overline{K}$ to be the algebraic closure of K. By Remark 3.4.31 this is also the algebraic closure of $\mathbb{F}_p$.

Claim 3.4.32. $K = \{u \in \overline{K} \mid u^{p^e} = u\}$. This gives the existence of finite fields with order p^e.

Proof. Notice that $(K^\times, \cdot)$ is a finite group with $(p^e - 1)$ elements. Therefore, for all $u \in L$, $u^{p^e - 1} = 1$, which implies that $u^{p^e} = u$ i.e. $K \subseteq$ RHS. Now consider the polynomial $x^{p^e} - x$ in $\overline{K}[x]$, which has p^e roots since $\overline{K}$ is algebraically closed. $|K| = p^e$ gives the desired equality. □

Proposition 3.4.33. If K_1 and K_2 are both fields with p^e elements, then $K_1 \simeq K_2$. Without ambiguity we denote such fields as $\mathbb{F}_{p^e}$.

Proof. Consider the extensions:

$$\begin{array}{ccc} \mathbb{F}_p & \hookrightarrow & K_1 \\ \downarrow & & \downarrow \varphi \\ K_2 & \hookrightarrow & \overline{K_2} \end{array}$$

This existence of φ is guaranteed by Theorem 3.4.28. Since φ is a ring homomorphism between fields, it is injective; and therefore $|\varphi(K_1)| = |K_1| = p^e \implies \varphi(K_1) = \{i \in \overline{K_2} \mid u^{p^e} = u\}$. But this then coincides with K_2. □

Example 3.4.34. There exists a ring homomorphism $\mathbb{F}_{p^e} \to \mathbb{F}_{p^f}$ if and only if $e \mid f$.

Proof. Verify both implications:

- $\Rightarrow$: Since we have the field extension $\mathbb{F}_{p^e} \hookrightarrow \mathbb{F}_{p^f}$, we can view $\mathbb{F}_{p^f}$ as a $\mathbb{F}_{p^e}$-vector space. As further we have two fields being finite, $\left|\mathbb{F}_{p^f}\right| = \left(|\mathbb{F}_{p^e}|\right)^{\dim_{\mathbb{F}_{p^e}} \mathbb{F}_{p^f}}$. In particular this implies that $e \mid f$.
- $\Leftarrow$: By Claim 3.4.32 we know that the elements in the field $\mathbb{F}_{p^f}$ are those in the set $\{u \in \overline{\mathbb{F}_{p^f}} \mid u^{p^f} = u\}$. Now Consider the roots of the polynomial $f = x^{p^f} - x$ in $\overline{\mathbb{F}_{p^f}}$. Since $\mathbb{F}_{p^f}$ embeds naturally into its algebraic closure, the image is exactly the roots of f. Since $e \mid f$, there exists n s.t. $f = ne$. Notice then that f factors as follows:

$$f = x^{p^f} - x = \left(x^{p^e} - x\right)\left(\sum_{i=1}^{n-1} p^{i(p^e-1)}\right)$$

  which implies that elements satisfying the relation $u^{p^e} = u$ in particular also satisfy $u^{p^f} = u$; and by Claim 3.4.32 these give the elements in field $\mathbb{F}_{p^e}$. This gives the field extension $\mathbb{F}_{p^e} \hookrightarrow \mathbb{F}_{p^f} \hookrightarrow \overline{\mathbb{F}_{p^f}}$ (and also by the uniqueness of algebraic closure (Corollary 3.4.30) we have $\overline{\mathbb{F}_{p^e}} = \overline{\mathbb{F}_{p^f}}$).

□

Example 3.4.35. Inside the algebraic closure of $\mathbb{F}_p$, $\overline{\mathbb{F}_p}$, for all $e \geq 1$ we have a unique copy of $\mathbb{F}_{p^e}$; and $\overline{\mathbb{F}_p} = \bigcup_{e \geq 1} \mathbb{F}_{p^e}$.

Proof. Proceed to verify the inclusion in both directions:

- $\subseteq$ For any element $u \in \overline{\mathbb{F}_p}$, consider its minimal polynomial over $\mathbb{F}_p$. Let $f_u \in \mathbb{F}_p[x]$ be the polynomial of u. Then $u \in \mathbb{F}_p(u) \simeq \mathbb{F}_p[x]/(f_u)$. By Remark 3.1.10 we have $|\mathbb{F}_p(u)| = p^{\deg f} \implies u \in \mathbb{F}_{p^{\deg f}} \subseteq \bigcup_{e \geq 1} \mathbb{F}_{p^e}$.

$\supseteq$ By Example 3.4.34 we have the embedding of $\mathbb{F}_{p^e}$ to its algebraic closure; and also such closures can be identified by the uniqueness of algebraic closure and viewing $\mathbb{F}_{p^n}$ as elements satisfying relation $u^{p^n} = u$ by Claim 3.4.32.

□

3.5 The Splitting Field of a Polynomial

Definition 3.5.1 (Splitting Field)**.** Let k be a field, and $f \in k[x] \setminus \{0\}$. A **splitting field** of f is a field extension $k \hookrightarrow K$ s.t.

1) f factors in $K[x]$ as a product of degree-1 polynomials.
2) If there exists K' s.t. $k \subseteq K' \subseteq K$ which also satisfies 1), then $K' = K$,

Equivalently, for a splitting field of f, denoted K, we can write f in $K[x]$ as $f = c(x-a_1)\cdots(x-a_n)$ with $c, a_1, \ldots, a_n \in K$; and $K = k(a_1, \ldots, a_n)$.

Example 3.5.2. $\mathbb{C}$ is the splitting field of x^2+1. $\mathbb{Q}(\sqrt{2})$ is the splitting field of x^2-2.

From what we had proved previously (Corollary 3.4.30), we know that algebraic closure is unique up to isomorphism, so we would expect the splitting field to be unique up to isomorphisms as well. The followings use (which will also be the case for most proofs regarding existence of extensions) the algebraic closure to construct such extensions.

Theorem 3.5.3. If $f \in k[x] \setminus \{0\}$, then

1. There exists a splitting field $k \hookrightarrow K$ of f.
2. If we have $k \hookrightarrow K$, $k \hookrightarrow K'$ splitting fields of f, then $K \simeq K'$ as k-extensions.

Remark 3.5.4. If K is the splitting field of $f \in k[x]$, then K/k is a finite extension, as in particular K is generated (as a k-vector space) by finitely many algebraic elements over k, namely the roots of f. By Proposition 3.4.13 the extension is then finite.

Proof of Theorem 3.5.3. Prove the two statements respectively:

1) Consider $k \hookrightarrow \bar{k}$ the algebraic closure of k. Then there exists $c, a_1, \ldots, a_n \in \bar{k}$ s.t. $f = c(x-a_1)\cdots(x-a_n)$. Then $K = k(a_1, \ldots, a_n)$ is the splitting field of f, by definition.

2) Let $k \hookrightarrow K$ and $k \hookrightarrow K'$ be the splitting fields of f. Let $K' \hookrightarrow \overline{K'}$ be the algebraic closure. By the remark above, K/k is algebraic. Since $\overline{K'}$ is algebraically closed, by Theorem 3.4.28 there exists $\varphi : K \to \overline{K'}$ s.t. $\varphi|_k = \mathrm{Id}_k$. Since K and K' are splitting fields of f over k, we can write $f = c(x-a_1)\cdots(x-a_n)$ in $K[x]$, and $f = c'(x-a_1')\cdots(x-a_n')$ in $K'[x]$. This gives the similar expression of the fields as in the remark:

$$K = k(a_1, \ldots, a_n), \qquad K' = k(a_1', \ldots, a_n')$$

Consider the ring homomorphism $K[x] \hookrightarrow K'[x] \subseteq \overline{K'}[x]$ induced by φ, we have

$$f = \varphi(f) = c(x - \varphi(a_1)) \cdots (x - \varphi(a_n))$$

since $f \in k[x]$ and φ as a morphism between k-extensions is the identity map when restricted to k. Therefore φ permutes a_is, which gives $\varphi(K) \subseteq K'$ and $\varphi(K') \subseteq K$, i.e. $\varphi(K) = K'$, and φ is bijection and thus a ring isomorphism.

□

3.6 Separable Extensions

Definition 3.6.1 (Separable Extension). Let $k \hookrightarrow K$ be an algebraic field extension. An element $a \in K$ is **separable over** k if its minimal polynomial $f \in k[x]$ satisfies any of the following conditions:

1) a is not a multiple root of f.

2) $f' \neq 0$.

3) Either $\mathrm{char}(k) = 0$, or $\mathrm{char}(k) = p > 0$, and $f \notin k[x^p]$.

Such a polynomial f is a **separable polynomial**. A field extension $k \hookrightarrow K$ is **separable** if the minimal polynomial of any element in K is separable.

Proposition 3.6.2. The three conditions in Definition 3.6.1 for separability over a field are equivalent.

Proof. Verify the following implications:

- *2) $\Longrightarrow$ 1).* Prove the contrapositive. Suppose that a is a root of f with multiplicity at least 2. Then we have $(x-a)^2 \mid f \implies (x-a) \mid f'$, i.e. $f'(a) = 0$. Since f is minimal, $f' \mid f$, and yet we require $\deg f' = \deg f$, which implies that $f = 0$.
- *1) $\Longrightarrow$ 2).* Prove the contrapositive by reversing the logic above. f minimal implies $f'(a) = 0$ if and only if $f \mid f'$. But $f'(a) = 0 \implies (x-a)^2 \mid f$, i.e. a is a multiple root of f.
- *3) $\Longrightarrow$ 2).* If $\mathrm{char}(k) = 0$, then $f' = 0$ if and only if f is constant, which cannot be a minimal polynomial. If $\mathrm{char}(k) = p$, then if $f' = 0$ either f is constant (which cannot be the case) or every term of f' vanishes because of characteristic-p, i.e. $f \in k[x^p]$.
- *2) $\Longrightarrow$ 3).* Reverse the logic above and verify by the same computation.

□

Remark 3.6.3. Notice that the condition 2) $f' \neq 0$ does not depend on whether f splits into degree-1 polynomials. Therefore, if $f \in k[x]$ is separable, then f cannot have any multiple roots in any algebraic closure of k.

Definition 3.6.4 (Perfect Field). A field k is **perfect** if every extension $k \hookrightarrow K$ is separable.

Proposition 3.6.5. A field k is perfect if and only if $\mathrm{char}(k) = 0$, or $\mathrm{char}(k) = p$ with $k = k^p$, i.e. the map $\varphi : k \to k, x \mapsto x^p$ is an isomorphism.

Proof. For the case where k is characteristic-0, any minimal polynomial f must be of degree at least 1, giving $f' \neq 0$ which satisfies condition 2).

Now consider the case where $\mathrm{char}k = p$. Show the following two implications:

- *If there exists $a \in k \setminus k^p$, then k is not perfect.* Let $k \hookrightarrow \bar{k}$ be an algebraic closure, and let $b \in \bar{k}$ be a root of $f = x^p - a$. Claim that f is irreducible in k (which implies that b is not separable over k as it is a multiple root). In $k[x]$, $f = x^p - a = x^p - b^p = (x-b)^p$ since $\mathrm{char}k = p$. Therefore, if $f = gh$ in $k[x]$ with $\deg g > 0$ and $\deg h > 0$, g must taken the form of $g = c(x-b)^i$ for $1 \leq i \leq p-1$. But then consider the coefficient of x, which gives $cib \in k$. Since $c, i \neq 0$ in k, $b \in k$, which is a contradiction.
- *If $k = k^p$, then k is perfect.* Suppose that we have the algebraic extension $k \hookrightarrow K$. Choose $u \in K$ arbitrarily, with minimal polynomial f. If u is not separable over k, then by definition $f \in k[x^p]$, i.e. we can write f as

$$f = \sum_{i=0}^{n} a_i x^{p^i} = \sum_{i=0}^{n} b_i^p x^{p^i} = \left(\sum_{i=1}^{n} b_i x^i \right)^p$$

  where the first equality results from $k = k^p$, and the second equality results from $\mathrm{char}k = p$. But this contradicts with the irreducibility of f.

□

Example 3.6.6. The followings give some examples of separability of extensions:

1. Every field of characteristic 0 is perfect by the proposition above.
2. Every algebraically closed field k is perfect, as the only algebraic extension from k is $k \hookrightarrow k$.
3. Every finite field $\mathbb{F}_{p^e}$ is perfect, as Claim 3.4.32 gives that $u \in \mathbb{F}_{p^e} \implies u^{p^e} = u$, i.e. $\left(u^{p^{e-1}}\right)^p = u$; and using the proposition above gives the desired result.
4. Fields in the form of $k(x)$ where $\mathrm{char}k = p > 0$ is not perfect. Suppose that $x \in (k(x))^p$, then $x = \left(\frac{f}{g}\right)^p$ for some $f, g \in K[x]$, i.e. $xg^p = f^p$. Counting the degree of the polynomial on both sides, we have $1 \equiv 0 \pmod{p}$, which is a contradiction.

Proposition 3.6.7. If we have field extensions $k \hookrightarrow k_1 \hookrightarrow k_2$ s.t. the extension $k \hookrightarrow k_2$ is separable, then both $k \hookrightarrow k_1$ and $k_1 \hookrightarrow k_2$ are separable.

Proof. $a \in k_1$ can be considered as an element in k_2; and since $k \hookrightarrow k_2$ is separable, a is not a multiple root of its minimal polynomial over k, which implies that $k \hookrightarrow k_1$ is separable.

For the second result, consider $b \in k_2$. Let g be its minimal polynomial over k, and h be its minimal polynomial over k_1. h being minimal implies that $h \mid g$. Since $k \hookrightarrow k_2$ is separable, b is not a multiple root of g, and therefore is not a multiple root of h. Since this holds for all $b \in k_2$, the extension $k_1 \hookrightarrow k_2$ is also separable. □

The converse of the proposition above also holds, but we will prove this later.

The following results characterize the "nice" feature of a field extension being separable:

Definition 3.6.8 (Primitive Element)**.** Given a field extension E/F, $\alpha \in F$ is a **primitive element** if $E = F(\alpha)$.

Definition 3.6.9 (Simple Extension)**.** A field extension E/F is simple if there exists a primitive element for the extension.

Theorem 3.6.10. Every finite separable extension is simple.

Proof. Since K/k is finite, there exists a basis of K seen as a k-vector field. In particular there exists $a_1, \dots, a_n \in K$ s.t. $K = k(a_1, \dots, a_n)$. Perform induction on n:

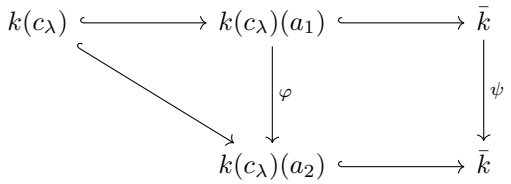
- $n = 1$. Clear.
- $n \geq 2$. It suffices to show the case for $n = 2$, as since the extension is finite, recursively apply the result for $n = 2$ will give the general result. Suppose that $K = k(a, b)$ for $a, b \in K$.

  If k is a finite field, then K is also finite, which implies that $K^\times$ is a cyclic group. Let $c \in K^\times$ be a generator of $K^\times$. Then we have $K = k(c)$.

  Now suppose that k is finite. We seek to prove a stronger result: if $c_\lambda = a\lambda + b$ for $\lambda \in k$, then c_λ is a primitive element for finitely many λ. Fix $\lambda \in k$. Suppose that c_λ is not primitive, i.e. we have $k(c_\lambda) \subsetneq k(a, b)$ a proper extension. Then we must have $a \notin k(c_\lambda)$ (as otherwise we get $k(c_\lambda) \ni c_\lambda - a\lambda = b$). Let $f, g \in k(c_\lambda)[x]$ be the minimal polynomials of a and b over $k(c_\lambda)$. Then in the algebraic closure $K \hookrightarrow \overline{K}$, f and g factors as

  $$f = (x - a_1) \cdots (x - a_n), \qquad g = (x - b_1) \cdots (x - b_m)$$

  Without loss of generality assume that $a = a_1$ and $b = b_1$. Since $a \notin k(c_\lambda)$, $n \geq 2$. Now consider the extensions $k \hookrightarrow k(c_\lambda) \hookrightarrow k(a, b)$. Since $k \hookrightarrow k(a, b)$ is separable, $k \hookrightarrow k(c_\lambda)$ is also separable, which by definition implies that all the a_is are distinct. Now consider $\varphi : k(c_\lambda)(a_1) \xrightarrow{\sim} k(c_\lambda)(a_2)$ which sends $a_1 \mapsto a_2$. We then have the commutative diagram:

  This induces an isomorphism $\psi : \bar{k} \to \bar{k}$ via specifying $\psi(b) = \psi(b_1) = b_i$ for some i. Since ψ should fix $k(c_[\lambda])$, we require

  $$a_2\lambda + b_i = \psi(a\lambda + b) = \psi(c_\lambda) = a\lambda + b \implies \lambda = \frac{b_i - b}{a - a_2}$$

  Such lambda exists since $a \neq a_2$ by the previous result that all a_is are distinct; and there are only finitely many of them as there are finitely many distinct b_is.

□

3.7 Normal Extensions

Definition 3.7.1 (Normal Extension). An algebraic extension $K \hookrightarrow L$ is a **normal extension** if it satisfies one of the following three conditions:

1) For every $f \in K[x]$ irreducible, if f has a root in L, then f factors as degree-1 polynomials in $L[x]$.
2) There is a (possibly infinite) family of polynomials $(f_i)_{i\in I}$ in $K[x]$ s.t. L is the splitting field of this family. That is, all f_i factors as a product of degree-1 polynomials in $L[x]$, and there is no L' with $K \subset L' \subset L$ which satisfies the same property.
3) Given an algebraic closure $L \hookrightarrow \bar{L}$, any ring homomorphism $\sigma : L \hookrightarrow \bar{L}$ satisfying $\sigma|_K = \mathrm{Id}_K$ satisfies $\sigma(L) \subseteq L$.

Proposition 3.7.2. The three conditions in the Definition 3.7.1 for normal extensions are equivalent.

Proof. Verify the following implications:

- *1) $\Longrightarrow$ 2).* Choose a family of elements $(a_i)_{i\in I}$ s.t. $L = K(a_i \mid i \in I)$. Since the extension L/K is algebraic, for all i, a_i has a minimal polynomial f_i. Since f_i has a root a_i in L, it factors as

$$f_i = (x - a_{i1}) \cdots (x - a_{in_i}), \qquad \text{where } a_{i1} = a_i,\ a_{ij} \in L$$

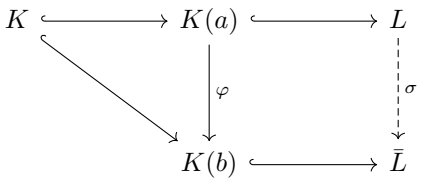
  Then we can write $L = K(a_{ij} \mid i \in I, 1 \le j \le n_i)$, which exactly implies that L is the splitting field of $(f_i)_{i\in I}$.

- *2) $\Longrightarrow$ 3).* If L is the splitting field of $(f_i)_{i\in I}$, then $f_i = (x - a_{i1}) \cdots (x - a_{in_i})$ with $a_{i1} = a_i$, and $a_{ij} \in L$ for all i, j. Since σ fixes elements in K,

$$f_i = \sigma(f_i) = \sigma(c_1)(x - \sigma(a_{i1})) \cdots (x - \sigma(a_{in_i}))$$

  Then $\sigma(a_{ij}) \in \{a_{i1}, \ldots, a_{in_i}\} \subseteq L$ for all j. Since 2) gives that $L = K(a_{ij} \mid i \in I, 1 \le j \le n_i)$, we know $\sigma(L) \subseteq L$ as σ fixes K and is thus uniquely determined by its action on a_{ij}s.

- *3) $\Longrightarrow$ 1).* Let $f \in K[x]$ be irreducible, and has a root $a \in L$. Let $L \hookrightarrow \bar{L}$ be an algebraic closure. Prove by contradiction: suppose that f has a root $b \in \bar{L} \setminus L$. Consider the map $\varphi : K(a) \to K(b)$ fixing K and mapping a to b. Since $K(a) \hookrightarrow L$ is algebraic, and $\bar{L}$ is algebraically closed, by Theorem 3.4.28 there exists a unique $\sigma : L \hookrightarrow \bar{L}$ extending φ, i.e. we have the following commutative diagram:



  But then $\sigma(a) = b \notin L$ which gives a contradiction.

□

Remark 3.7.3. From the proof, if the extension we have $K \hookrightarrow L$ is a finite normal extension, then there exists finitely many $f_1, \ldots, f_r \in K[x]$ s.t. L is the splitting field of $(f_1, \ldots, f_r)$ then equivalently L is the splitting field of $f = \prod_{i=1}^{r} f_i$.

Example 3.7.4. The following gives some examples of normal extensions:

1. The algebraic closure $K \hookrightarrow \bar{K}$ is normal as by definition any ring homomorphism σ has the property $\sigma(K) \subseteq K$.
2. If $K \hookrightarrow L$ is a degree-2 extension, then L/K is normal. If $a \in L \setminus K$, and f is the minimal polynomial of a, then by Remark 3.1.10 $\deg f = 2$, i.e. $f = (x-a)(x-b) \in K[x]$. Then since $a \in L$, $b \in L$ as $a+b \in K \subseteq L$. But this implies that L is the splitting field of f and therefore L/K is normal.
3. The extension $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt[3]{2})$ is normal as $\mathbb{Q}(\sqrt[3]{2})$ does not contain all the roots of $x^3 - 2$.

Proposition 3.7.5. Let $K \hookrightarrow L \hookrightarrow L'$ be algebraic extensions, and L'/K is normal. Then there exists normal sub-extension $L \hookrightarrow \tilde{L} \hookrightarrow L'$ s.t. $\tilde{L}/K$ is normal. This is the normal closure of L over K.

Proof. Write $L = K(a_i \mid i \in I)$. Denote $f_i \in K[x]$ as the minimal polynomial of a_i. Since L'/K is normal, we can factor $f_i = \sigma(f_i) = \sigma(c_1)(x - \sigma(a_{i1})) \cdots (x - \sigma(a_{in_i}))$ with $a_i = a_{i1}$, and $a_{ij} \in L'$ for all j. If we have $L \subseteq \tilde{L} \subseteq L'$ where $\tilde{L}/L$ is normal, then $a_{ij} \in \tilde{L}$, which implies that $K(a_{ij} \mid i \in I, 1 \leq j \leq n_i) \subseteq \tilde{L}$. Since $K \hookrightarrow K(a_{ij} \mid i \in I, 1 \leq j \leq n_i)$ is the splitting field of the family of polynomials $(f_i)_{i \in I}$, $\tilde{L}/K$ is normal. □

Remark 3.7.6. If we have $K \hookrightarrow L \hookrightarrow L_1'$ and $K \hookrightarrow L \hookrightarrow L_2'$ algebraic extensions s.t. L_1'/L and L_2'/L are normal, then the corresponding normal closures of L in L_1' and L_2' are isomorphic as k-extensions.

Proposition 3.7.7. If $K \hookrightarrow L \hookrightarrow L'$ are algebraic extensions, and L'/K is normal, then L'/L is normal.

Proof. Suppose that $f \in L[x]$ is irreducible, and has a root $a \in L'$, then f is a minimal polynomial of a over L. Let $g \in K[x]$ be the minimal polynomial of a over K. By definition $g(a) = 0$, which implies that $f \mid g$ in $L[x]$. Since L'/K is normal, g factors as a product of degree-1 polynomials in $L'[x]$, which implies that f also factors as a product of degree-1 polynomials in $L'[x]$, which is exactly the definition of L'/L being normal. □

3.8 Galois Extensions

Definition 3.8.1 (Galois Group)**.** Let $K \hookrightarrow L$ be an algebraic extension. The **Galois Group** of L/K is

$$G(L/K) := \{\sigma \in \mathrm{Aut}(L) \mid \sigma|_K = \mathrm{Id}_K\}$$

with the group operation defined as composition.

Definition 3.8.2 (Galois Extension)**.** A field extension is **Galois** if it is both normal and separable.

Theorem 3.8.3. For $K \hookrightarrow L$ a finite Galois extension, $|G(L/K)| = [L : K]$.

Proof. Since L/K is finite and separable, by Theorem 3.6.10 there exists a primitive $a \in L$ s.t. $L = K(a)$. Let f be the minimal polynomial of a over K. By Remark 3.1.10 we know $\deg f = [L : K]$.

Now consider the algebraic closure $K \hookrightarrow L \hookrightarrow \bar{L}$. Then f factors as $f = (x - a_1) \cdots (x - a_n)$ with $a_1 = a$, $a_i \in \bar{L}$ for all i, and $n = [L : K]$. Since L/K is normal, $a_i \in L$ for all i as $a \in L$; and since L/K is separable, all a_is are distinct. Further as $f \in K[x]$, for all $\sigma \in G(L/K)$, $f = \sigma(f) = (x - \sigma(a_1)) \cdots (x - \sigma(a_n))$. Then $\sigma(a_i) \in \{a_1, \ldots, a_n\}$ for all i.

Define $\varphi : G(L/K) \to \{a_1, \ldots, a_n\}, \sigma \mapsto \sigma(a_1)$. Check:

- *φ is injective.* Since $L = K(a)$, two automorphisms in $G(L/K)$ agreeing on a must be identical as by definition they must fix K.
- *φ is surjective.* For all i, since f is irreducible over K, we have $K(a) \simeq K[x]/(f) \simeq K(a_i)$ as K-algebras. Extend this to $\sigma : L \to L$, i.e. making the following diagram commute:

$$\begin{array}{ccc} K(a) & \xrightarrow{\sim} & K(a_i) \\ \| & & \cap| \\ L & \xrightarrow{\sigma} & L \end{array}$$

  Notice that σ must be surhective, as

$$[K(a) : K] = [L : K] = [K(a_i) : K] \leq [\sigma(L) : K]$$

  which implies that $L \subseteq \sigma(L)$ and therefore σ is an automorphism, i.e. is in $G(L/K)$. This gives a pre-image and thus implies that φ is surjective. Since $\{a_1, \ldots, a_n\}$ is a finite set, $|G(L/K)| = |\{a_1, \ldots, a_n\}| = n$.

□

Remark 3.8.4. With the same notation as in the proof, we have a group homomorphism $G(L/K) \to S_n \simeq S_{\{a_1,\ldots,a_n\}}$, $\sigma \mapsto (a_i \mapsto \sigma(a_i))$. Since it is both injective and surjective as given by the proof, the induced action of $G(L/K)$ on $\{a_1, \ldots, a_n\}$ is transitive.

Corollary 3.8.5. Automorphisms in $G(L/K)$ permutes the roots of minimal polynomials of elements in L over K.

Example 3.8.6. The followings give some examples of Galois extensions and the corresponding Galois Group:

1. $\mathbb{R} \hookrightarrow \mathbb{C}$ is a Galois extension of degree 2. It is normal as $\mathbb{C}$ is the splitting field of $x^2 + 1$, and it is separable as $\mathbb{R}$ is characteristic-0. $G(\mathbb{C}/\mathbb{R}) = \{\mathrm{Id}, \sigma\}$ where σ is the complex conjugation (corresponding to S_2).
2. For $d \in \mathbb{Z}_{\geq 0}$ not a perfect square, $\mathbb{Q} \hookrightarrow \mathbb{Q}(\sqrt{d})$ is a Galois extension of degree 2. It is normal as $\mathbb{Q}(\sqrt{d})$ is the splitting field of $x^2 - d$, and it is separable as $\mathbb{Q}$ is characteristic-0. $G(\mathbb{Q}(\sqrt{d})/\mathbb{Q}) = \{\mathrm{Id}, \sigma\}$ where $\sigma : (a + b\sqrt{d}) \mapsto (a - b\sqrt{d})$.
3. $\mathbb{F}_p \hookrightarrow \mathbb{F}_{p^e}$ is a Galois extension with degree e. It is normal as $\mathbb{F}_{p^e}$ is the splitting field of $x^{p^e} - x$; and it is separable as $\mathbb{F}_{p^n}$ is perfect for all n. The Galois group is then $G(\mathbb{F}_{p^e}/\mathbb{F}_p) = \langle\sigma\rangle$ where σ is the Frobenius endomorphism: $x \mapsto x^p$, with $\sigma^e = \mathrm{Id}$ and $|\langle\sigma\rangle| = e$.

   A sidenote is that using this perspective it is clearer that there exists an embedding $\mathbb{F}_{p^e} \hookrightarrow \mathbb{F}_{p^f}$ if and only if $e \mid f$, as this is equivalent to saying that $\sigma^f = \mathrm{Id}$.
4. The extension $\mathbb{Q} \overset{\deg 3}{\hookrightarrow} \mathbb{Q}(\sqrt[3]{2}) \overset{\deg 2}{\hookrightarrow} \mathbb{Q}(\sqrt[3]{2}, \omega)$ where ω is the 3-rd root of unity, is Galois, as it is the splitting field of $x^3 - 2$ (normal) and $\mathbb{Q}$ is perfect (separable). Since $G(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q})$ is not cyclic, $G(\mathbb{Q}(\sqrt[3]{2}, \omega)/\mathbb{Q}) \simeq S_3$ by cardinality.

3.9 Algebraic Independence & Transcendence Degree*

The introduction of transcendental degree seeks to give an invariant that measures how far the an extension $k \hookrightarrow K$ is from being algebraic. We would denote this as $\mathrm{trdeg}(K/k)$ and give a formal definition later. But we would desire the following properties from it:

1) $\mathrm{trdeg}\, K/k = 0$ if the extension $k \hookrightarrow K$ is algebraic.

2) If $k \hookrightarrow K = k(x_1, \ldots, x_n)$ where $x_1, \ldots, x_n$ are formal (not algebraic), then $\mathrm{trdeg}(K/k) = n$.

3) Given extensions $k \hookrightarrow K \hookrightarrow L$, $\mathrm{trdeg}(L/k) = \mathrm{trdeg}(K/k) + \mathrm{trdeg}\, L/K$.

Definition 3.9.1 (Algebraic Independence). Given a field extension $k \hookrightarrow K$, a subset $A \subset K$ is **algebraically independent** (over k) if for all n for every $a_1, \ldots, a_n \in A$ distinct, and every $f \in k[x_1, \ldots, x_n]$, $f \neq 0$ implies $f(a_1, \ldots, a_n) \neq 0$. Otherwise we say that A os **algebraic dependent**.

Remark 3.9.2. We have the following immediate results:

1) For $A = \{a\}$, i.e. containing only one element, then A is algebraically independent if and only if a is not algebraic over k.

2) By definition, A is algebraically independent if and only if for all $B \subseteq A$ finite, B is algebraically independent.

3) Given $a_1, \ldots, a_n \in k$, they being algebraically independent if and only if for $\varphi : k[x_1, \ldots, x_n] \to k$, $x_i \mapsto a_i$ as a k-algebra homomorphism satisfies $\ker \varphi = \{0\}$, i.e. $k(a_1, \ldots, a_n) \simeq k(x_1, \ldots, x_n)$.

Example 3.9.3. Take $R = k[x, y]/(x^2 + y^2 - 1)$, consider $k \hookrightarrow R \hookrightarrow \mathrm{Frac}(R)$, $\bar{x}$ and $\bar{y}$ are algebraically dependent, as we have the relation $(\bar{x})^2 + (\bar{y})^2 = 1$.

Proposition 3.9.4. Given a field extension $k \hookrightarrow K$, let A be a set, and $B = A \sqcup \{b\}$ inside field K. Then B is algebraically independent over k if and only if A is algebraically independent over k, and b is not algebraic over $k(A)$.

Proof. By definition if B is algebraically independent, then A must be algebraically independent. For b not algebraic over the $k(A)$ prove the contrapositive: suppose that B is algebraic over $k(A)$, then there exists $0 \neq P = c_0 + c_1 y + \cdots + c_d y^d \in k(A)[y]$ s.t. $P(b) = 0$. Since $c_i \in k(A)$, we can write $c_i = \frac{f_i(a_1, \ldots, a_n)}{g_i(a_1, \ldots, a_n)}$ for $f_i, g_i \in k[x_1, \ldots, x_n]$ and $a_i \in A$. $P(b) = 0$ implies that $\sum_{i=0}^{d} f_i(x_1, \ldots, x_n) b^i = 0$. But notice that $P \neq 0$, and P can be viewed as a polynomial in $\{a_1, \ldots, a_n, b\}$, which implies that A is not algebraically independent.

The other direction is clear by definition. □

Proposition 3.9.5. Every algebraically independent subset $A \subseteq K$ over k is contained in a maximal such subset.

Proof. Apply Zorn's Lemma. Show that the set $\mathcal{B} = \{B \subseteq K \mid A \subseteq B, B \text{ algebrically independent over } k\}$ with order of inclusion satisfies the hypotheses in Zorn's Lemma:

- $\mathcal{B}$ is nonempty. In particular, it contains A.

- If $(B_i)_{i\in I}$ is a chain in $\mathcal{B}$, it is bounded above by $\overline{B} = \bigcup_{i\in I} B_i \in B$. It is indeed algebraically independent as every finite subset of $\overline{B}$ is contained in some B_i since every two such B_is are comparable (as a chain is totally ordered).

□

Proposition 3.9.6. A subset $A \subseteq L$ is a maximal algebraically independent subset over k of K if and only if A is algebraically independent, and $k(A) \hookrightarrow K$ is an algebraic extension.

Proof. By definition, if A is algebraically independent, then it is maximal if and only if for all $b \in K \setminus A$, b is algebraic over $k(A)$ (otherwise by Proposition 3.9.4 we can adjoin an element to this set while keeping its algebraic independence). This is exactly saying that $k(A) \hookrightarrow K$ is algebraic. □

Definition 3.9.7 (Transcendental Basis)**.** Given a field extension K/k, a **transcendental basis** of K/k is a maximal algebraically independent subset of K over k.

Definition 3.9.8 (Transcendental Degree)**.** Given a field extension K/k, the **transcendental degree**, denoted $\mathrm{trdeg}(K/k)$ is the number of elements of a transcendental basis. It is in $\mathbb{Z}_{\geq 0} \cup \infty$.

We are using the similar nomenclature as for vector spaces, so we would expect similar properties for being "independent" or "a basis":

Theorem 3.9.9. If given K/k is a field extension, and $a_1, \ldots, a_n \in K$ s.t. $k(a_1, \ldots, a_n) \hookrightarrow K$ is algebraic (i.e. this is a maximal algebraically independent set), then for all $\{b_1, \ldots, b_m\}$ algebraically independent over k, $m \leq n$.

Proof. After reordering the elements, we may assume that $a_i = b_i$ for all $1 \leq i \leq r$. If $r = m$ then this is exactly hat we need.

Now suppose that $r < m$. It is enough to show that there exists $i > r$ s.t. the extension $k(a_1, \ldots, a_{i-1}, a_{i+1}, \ldots, a_n, b_{r+1}) \hookrightarrow K$ is algebraic. If that is the case, then after finitely many steps we will get the set b_ns (as we can identify $a_1, \ldots, a_r, a_{r+1}$ with the corresponding elements in b and apply the argument recursively). This then implies that $r = m$.

Since b_{r+1} is algebraic over $k(a_1, \ldots, a_n)$, there exists nonzero $f \in k(a_1, \ldots, a_n)[y]$ s.t. $f(b_{r+1}) = 0$. Getting rid of the denominators of the polynomial we can without loss of generality assume that the coefficients of f are in the form of $P(a_1, \ldots, a_n)$, i.e. we have nonzero $g \in k[x_1, \ldots, x_n, y]$ s.t. $g(a_1, \ldots, a_n, b_{r+1}) = 0$ via evaluating f on b_{r+1} on the coefficients given by g. Since $b_1, \ldots, b_r, b_{r+1}$ are algebraically independent over k. Without loss of generality we can assume that x_n appears with nonzero coefficient in g. Now write

$$g = \sum_{i=0}^{p} g_i(x_1, \ldots, x_{n-1}, y) x_n^i$$

If there exists j s.t. $g_j(a_1, \ldots, a_{n-1}, b_{r+1}) \neq 0$, then a_n is algebraic over $k(a_1, \ldots, a_{n-1}, b_{r+1})$. This gives the algebraic extension

$$k(a_1, \ldots, a_{n-1}, b_{r+1}) \hookrightarrow k(a_1, \ldots, a_n, b_{r+1}) \hookrightarrow K$$

Otherwise there exists $g_j \neq 0$ s.t. $g_j(a_1, \ldots, a_{n-1}, b_{r+1}) = 0$. Repeat the process with g replaced with g_j. This process must terminate as $g \neq 0$. □

Corollary 3.9.10. Every two transcendental basis of K over k have the same number of elements (or are in bijection, for the infinite case).

Proposition 3.9.11. If $K = k(a_1, \ldots, a_n)$, then there exists a subset $A \subseteq \{a_1, \ldots, a_n\}$ that is a transcendental basis over k. In particular, $\mathrm{trdeg}(K/k) \leq n$.

Proof. Let $A \subseteq \{a_1, \ldots, a_n\}$ be the maximal subset which is algebraically independent (which exists by Proposition 3.9.5). But by Proposition 3.9.4 this implies that if $a_i \notin A$, then a_i is algebraic over $k(A)$. Therefore, $k(A) \hookrightarrow K = k(a_1, \ldots, a_n)$ is algebraic, i.e. A is a transcendental basis. □

Proposition 3.9.12. If we have $k \hookrightarrow K \hookrightarrow L$ field extensions, then $\mathrm{trdeg}(L/k) = \mathrm{trdeg}(K/k) + \mathrm{trdeg}(L/K)$.

Proof. First deal with the cases where RHS is infinite:

- If $\mathrm{trdeg}(K/k)$ is infinite, then a transcendental basis for K/k is part of a transcendental basis of L/k as L can be viewed as a vector space over K.
- If $\mathrm{trdeg}(L/K)$ is infinite, then in a transcendental basis for L/K are in particular algebraically independent over k, which implies that $\mathrm{trdeg}(L/k)$ is infinite.

Now we may assume that we have a finite transcendental basis $a_1, \ldots, a_m$ for K/k and $b_1, \ldots, b_n$ for L/K. Claim that $\{a_1, \ldots, a_m, b_1, \ldots, b_n\}$ gives a transcendental basis of L/k. Verify the followings:

1) The sub-extensions are algebraic since a_is and b_is are transcendental bases for the corresponding extensions (by Theorem 3.9.6)

$$k(a_1, \ldots, a_m, b_1, \ldots, b_n) \hookrightarrow K(b_1, \ldots, b_n) \hookrightarrow L$$

By Proposition 3.4.15 we have the extension $L/k(a_1, \ldots, a_m, b_1, \ldots, b_n)$ being algebraic.

2) The set $\{a_1, \ldots, a_m, b_1, \ldots, b_n\}$ is algebraically independent over k. Proceed to show by induction on i for $0 \leq i \leq n$ that $\{a_1, \ldots, a_m, b_1, \ldots, b_i\}$ are algebraically independent over k:

For $i = 0$ the result is clear by hypothesis. For the inductive step it suffices to show that b_{i+1} is not algebraically dependent on $\{a_1, \ldots, a_m, b_1, \ldots, b_i\}$, then by Proposition 3.9.4 we have the set $\{a_1, \ldots, a_m, b_1, \ldots, b_i, b_{i+1}\}$ algebraically independent over k. This is clear as b_js give a transcendental basis over K, and are therefore algebraically independent over k. Taking $i = n$ gives the algebraic independence over k.

□

Verify that we indeed have the desired properties of transcendental degree as mentioned in the beginning of the section:

1) $\mathrm{trdeg}(K/k) = 0$ if and only if the extension $k \hookrightarrow K$ is algebraic. This comes as a corollary of Proposition 3.9.6.
2) $K = k(a_1, \ldots, a_n)$ if and only if $\mathrm{trdeg}(K/k) \leq n$, with equality if and only if a_is are algebraically independent. This results from Theorem 3.9.9.
3) The proposition above (Proposition 3.9.12) gives the additivity of transcendental degree.

Remark 3.9.13. The results above implies that $k(x_1, \dots, x_m) \simeq k(x_1, \dots, x_n)$ as k-algebras (where x_is are formal variables) if and only if $m = n$. Notice that for $m \neq n$ they can still be isomorphic as fields: take $k = \mathbb{Q}(x_1, x_2, \dots)$ (with infinitely many variables) and let $m = 0$ and $n = 1$, with the isomorphism $x_i \mapsto x_{i+1}$. But this is clearly not k-linear.

Definition 3.9.14 (Purely Transcendental)**.** A finitely generated field extension K/k is **purely transcendental** if $K \simeq k(x_1, \dots, x_n)$ as k-algebras for some n.

This is somewhat related to ring theory: we state without proof the following results:

Definition 3.9.15 (Dimension (Ring))**.** Given a commutative ring R, its **dimension** is defined as

$$\dim R := \sup_n \{n \mid \exists\, p_0 \subsetneq \cdots \subsetneq p_n,\ p_i \subseteq R \text{ prime ideals}\}$$

Theorem 3.9.16. Given a field k and a domain R, if R is a finitely generated k-algebra, then $\dim R = \operatorname{trdeg}(\operatorname{Frac}(R)/k)$.

3.10 The Fundamental Theorem of Galois Theory

We now return to the discussion of Galois Theory. We have introduced the Galois Group of a field extension $k \hookrightarrow K$:

$$G(K/k) := \{\sigma \in \operatorname{Aut}(K) \mid \sigma(u) = u, \forall u \in k\}$$

The following section seeks to establish the relation between the structure of the Galois Group and the corresponding field extension.

Proposition 3.10.1. If $K = k(\alpha)$, then $|G(K/k)| \leq [K : k]$ with equality if and only if K/k is normal, and α is separable over k.

Proof. Every k-algebra homomorphism $\sigma : K \hookrightarrow \bar{K}$ is uniquely determined by $\sigma(\alpha)$; and if $f \in k[x]$ is the minimal polynomial of α, by Corollary 3.8.5 σ permutes the roots of f in $\bar{K}$. Then we have the chain of inequalities:

$$|G(K/k)| \leq \left|\{\sigma : K \to \bar{K} \mid \sigma \text{ is a morphism of } k\text{-algebra}\}\right| \leq \#\text{ distinct roots of } f \leq \deg f = [K : k]$$

and we have equalities when f is separable, and K is the splitting field of f. □

Theorem 3.10.2 (Fundamental Theorem of Galois Theory)**.** Let K/k be a finite Galois extension. Then we have two maps:

$$\{k \hookrightarrow L \hookrightarrow K\} \underset{\Psi}{\overset{\Phi}{\rightleftarrows}} \{\text{subgroups of } G = G(K/k)\}$$

where $\Phi(L) = G(K/L)$, and for $H \leq G$, $\Psi(H) = K^H := \{u \in K \mid \sigma(u) = u, \forall \sigma \in H\}$. They further satisfy the following two properties:

1) Φ and Ψ are order-reversing, inverse bijections.

2) $H \leq G$ is a normal subgroup if and only if $k \hookrightarrow K^H$ is a normal extension. In this case, the group homomorphism

$$G(K/k) \to G(K^H/k), \qquad \sigma \mapsto \sigma|_{K^H}$$

induces an isomorphism $G/H \simeq G(K^H/k)$.

Remark 3.10.3. We first consider some simple examples of such correspondence:

1) The correspondence is *order-reversing*: If $H_1 \leq H_2 \leq G$, then $K^{H_2} \subseteq K^{H_1}$ (as H_2 fixes fewer elements); and for $k \hookrightarrow L_1 \hookrightarrow L_2 \hookrightarrow K$, $G(K/L_2) \leq G(K/L_1)$.

2) For simplicity in the followings we will write K^H for $\Psi(H)$. Notice for $H \leq G$, $H \leq G(K/K^H)$, as K^H by definition is the set of elements fixed by H; and in the other direction for extensions $k \hookrightarrow L \hookrightarrow K$, $G(K/L)$ fixes L. We need to prove the equality.

Before proving the main theorem we need some more tools to describe $[K : K^H]$ for $H \leq G(K/k)$:

Proposition 3.10.4. Given a field K and a group G, any mutually distinct group homomorphisms $\chi_1, \ldots, \chi_n : G \to K^\times$ are linearly independent as elements of $\mathrm{Func}(G; K)$ as a K-vector space.

Proof. Prove by contradiction. Suppose that we have a relation $\sum_{i=1}^n a_i\chi_i = 0$, with not all a_is being zero. Without loss of generality, assume n is minimal, i.e. all a_is are nonzero. Separate the cases:

- $n = 1$. Then $a_1\chi_1 = 0$; but since $\chi_1 \in K^\times$ which cannot be zero, $a_1 = 0$. Contradiction.
- $n > 1$. By definition we have

$$\sum_{i=1}^n a_i\chi_i(g) = 0 \quad \forall g \in G \tag{$*$}$$

Since χ_is are distinct, there exists $h \in G$ s.t. $\chi_1(h) \neq \chi_n(h)$. Fix h, and choose $g \in G$ arbitrarily. Since χ_is are group homomorphisms, we have by linear independence

$$\sum_{i=1}^n a_i\chi_i(hg) = 0 = \sum_{i=1}^n a_i\chi_i(h)\chi_i(g) \qquad \forall g \in G$$

Multiplying $\chi_1(h)$ on the right of Eq. ($*$), and subtract the RHS of the equality above, we have

$$\sum_{i=0}^n a_i \underbrace{(\chi_i(h) - \chi_1(h))}_{\text{zero iff } i=1}\chi_i(g) = 0 \qquad \forall g \in G$$

which contradicts the minimality of n.

□

Corollary 3.10.5. If $\sigma_1, \ldots, \sigma_n \in \mathrm{Aut}(K)$ are distinct group homomorphisms, and K is a field, then $\sigma_1, \ldots, \sigma_n$ are linearly independent in $\mathrm{Func}(K; K)$ viewed as a K-vector space.

Proof. $\sigma_1|_{K^\times}, \cdots, \sigma_n|_{K^\times}$ are distinct group automorphisms on $K^\times$. Apply the above proposition. □

Proposition 3.10.6. Let K be a field, and $A \subseteq \mathrm{Aut}(K)$ a subset. For $L = \{u \in K \mid \sigma(u) = u, \forall u \in A\}$, $[K : L] \geq |A|$.

Proof. May assume that $[K : L] = n$ is finite, and $u_1, \ldots, u_n$ is a basis of K over L (as a L-vector space).

Argue by contradiction: suppose that we have $\sigma_1, \ldots, \sigma_{n+1} \in A$ distinct. Consider the system of linear equations over L:

$$\sum_{i=1}^{n+1} \sigma_i(u_j) x_i = 0, \qquad 1 \leq j \leq n$$

This is a system with n equations and $(n+1)$ variables, which must exist a nontrivial solution $(a_1, \ldots, a_{n+1})$. Since u_is give a basis of K over L, this is equivalent to having

$$\sum_{i=1}^{n+1} a_i \sigma_i(u_j) = 0 \ (\forall j) \implies \sum_{i=1}^{n+1} a_i \sigma_i = 0$$

contradicting Corollary 3.10.5. □

Proposition 3.10.7. If $A \subseteq \mathrm{Aut}(K)$ is a finite group, with the same notation as above we have equality $[K : L] = |A|$.

Proof. It is already proven that $[K : L] \geq |A|$. Now suppose that $[K : L] > |A|$ for $A = \{\sigma_1, \ldots, \sigma_d\}$. Then there exists elements $u_1, \ldots, u_{d+1} \in K$ that are linearly independent over L.

Apply the similar strategy as before. Consider the linear system of equations over K:

$$\sum_{i=1}^{d+1} \sigma_j(u_i) x_i = 0, \qquad 1 \leq j \leq d$$

As there are d equations with $d+1$ variables, there exists a nontrivial solution $(a_1, \ldots, a_{d+1})$ s.t.

$$\sum_{i=1}^{d+1} a_i \sigma(u_i) = 0 \qquad \forall \sigma \in A$$

In particular we can ignore all nonzero a_is and get L-linearly independent elements $u_1, \ldots, u_m$ in K s.t.

$$\sum_{i=1}^{m} a_i \sigma(u_i) = 0 \qquad a_i \neq 0 \ (\forall i),\ m \text{ minimal} \tag{$*$}$$

Then either

- $m = 1$. $a_1 \sigma(u_1) = 0$. Take in particular $\sigma = \mathrm{Id}$, this gives $a_1 u_1 = 0 \implies u_1 = 0$ but this contradicts with $\{u_1\}$ being linearly independent.
- $m > 1$. Multiply Eq. ($*$) by a_1^{-1} on the left, we can assume that $a_1 = 1$. Further take $\sigma = \mathrm{Id}$ in Eq. ($*$), we have $\sum_{i=1}^{m} a_i u_i = 0$. Suppose that all a_is are nonzero. Since u_is are linearly independent over L, after reordering we may assume that $a_m \notin L$ (otherwise $\{u_m\}$ is not linearly independent). Then there exists $\tau \in A$ s.t. $\tau(a_m) \neq a_m$. Applying τ

to Eq. (∗) gives (recalling that τ is a group homomorphism)

$$\sum_{i=1}^{m} \tau(a_i) \underbrace{\tau\sigma}_{\text{runs through } A}(u_i) = 0 \ (\forall \sigma \in A) \implies \sum_{i=1}^{m} \tau(a_i)\sigma(u_i) = 0 \ (\forall \sigma \in A)$$

Subtracting Eq. (∗) gives (recalling that without loss of generality we may assume $a_1 = 1$, and τ is an automorphism on K)

$$\sum_{i=1}^{m} \underbrace{(\tau(a_i) - a_i)}_{\text{zero iff } i=1} \sigma(u_i) = 0 \qquad \forall \sigma \in A$$

which contradicts the minimality of m.

□

We now use the above results to prove the main theorem:

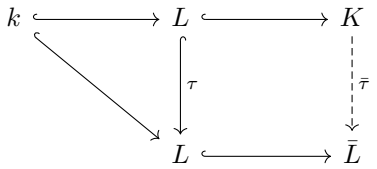
Proof of Theorem 3.10.2. Verify the two extra conditions respectively:

1) Suppose that we have $H \leq G$. This corresponds to the field extensions $k \hookrightarrow K^H \hookrightarrow K$. Proposition 3.10.7 gives $[K : K^H] = |H|$. Since $k \hookrightarrow K$ is Galois, $K^H \hookrightarrow K$ is Galois (use Proposition 3.6.7 for separability and Proposition 3.7.7 for normality). Apply Theorem 3.8.3 we have $G(K/K^H) = [K : K^H] = |H|$. Since $H \subseteq G(K/K^H)$ and they have the same cardinality, $H = G(K/K^H)$. Now for any extension $k \hookrightarrow L \hookrightarrow K$ s.t. $H = G(K/L) \leq G$, Theorem 3.8.3 gives $|H| = [K : L]$ since K/L is Galois by the same reasoning. Consider the extension $L \hookrightarrow K^{G(K/L)} = K^H \hookrightarrow K$. The extension indeed exists as $G(K/L)$ in particular is a subgroup of itself. Use the previous result gives $[K : K^H] = |H| = [K : L]$, which implies $K^H = L$.

2) Prove the implication in both directions:

   ⇒ Suppose that we have the extensions $k \hookrightarrow L \hookrightarrow K$ with both of them normal and separable. Take $H = G(K/L) \leq G$, we want to show that H is normal.

   Proceed via constructing a group homomorphism whose kernel is H. For any $\sigma \in G$, consider its restriction to L $\sigma|_L : L \to K \subseteq \bar{K}$. Since L/k is normal, by 3) in the definition for normal extensions $\sigma|_L(L) \subseteq L$. This implies that by restricting σ to L we have a ring homomorphism $G = G(K/k) \to G(L/k)$, $\sigma \mapsto \sigma|_L$. Notice that the kernel of it is $H(= G(K/L)$, which fixes $L)$. This implies that H is normal in G. It remains to show that the map is surjective. For any $\tau \in G(L/k)$ this induces a group homomorphism $K \to \bar{L}$:

   Since the extension $k \hookrightarrow K$ is also normal, and we have the natural extension $K \hookrightarrow \bar{L}$ (by Theorem 3.4.28), apply again 3) of normal extensions $\bar{\tau}(K) \subseteq K$, which gives a pre-image for any automorphism in $G(L/k)$. Apply the first isomorphism theorem gives $G/H \simeq G(L/k)$.

   ⇐ Suppose now we have $H \trianglelefteq G$. We want to show that the corresponding field extensions $k \hookrightarrow K^H \hookrightarrow K$ is normal.

Since $k \hookrightarrow K$ is Galois it suffices to show that $k \hookrightarrow K^H$ is normal. Suppose that we have a morphism of k-algebras $\tau : K^H \to \bar{K}$. This can be extended to $\sigma : K \to \bar{K}$ via forcing the commutative condition as above. Since $k \hookrightarrow K$, σ fixes k and preserves K, i.e. $\sigma \in G = G(K/k)$. Therefore to show that the extension is normal we need to show that for all $\sigma \in G(K/k)$, $\sigma(K^H) \subseteq K^H$.

Let $u \in K^H$, we need to show that for all $\tau \in H$, $\tau\sigma(u) = \sigma(u)$. $H \trianglelefteq G$ implies $\sigma^{-1}\tau\sigma(u) = u$ (recall K^H consists of elements in K fixed by H). Applying σ on both sides gives the desired result.

□

3.11 Norm and Trace Maps

This section introduces the norm and trace of any extension $K \hookrightarrow L$. They are natural extension of norm amd trace of linear maps, as in particular L can be viewed as a K-vector space. These two maps characterize the extension.

Definition 3.11.1 (Norm; Trace). Let K be a field, A a commutative K-algebra, with $\dim_K(A)$ finite. Define for $a \in A$ the K-linear map $\varphi_a : A \to A, x \mapsto ax$. Define

- The **norm** $\mathrm{N}_{A/K}(a) = \det(\varphi_a) \in K$.
- The **trace** $\mathrm{Tr}_{A/K}(a) = \mathrm{tr}(\varphi_a) \in K$.

Example 3.11.2. Consider the following examples for the norm and trace map:

1) If $a \in K$, $\varphi_a = a \cdot \mathrm{Id}_K$. Let $n = \dim_K A$, then $\mathrm{N}_{A/K}(a) = a^n$, $\mathrm{Tr}_{A/K}(a) = na$.
2) Let $d \in \mathbb{Z}$ be not a square. Consider the field extension $K = \mathbb{Q} \hookrightarrow L = \mathbb{Q}(\sqrt{d})$. L as a K-vector space has a basis $\{1, \sqrt{d}\}$. For $a = a_1 + a_2\sqrt{d}$, we have
$$\varphi_a = \begin{pmatrix} a_1 & da_2 \\ a_2 & a_1 \end{pmatrix} \qquad \text{with } \mathrm{N}_{A/K}(a) = a_1 - da_2^2,\ \mathrm{Tr}_{A/K}(a) = 2a_1$$
3) If $a \in A$ is nilpotent, then φ_a is a nilpotent operator, which implies that $\mathrm{N}_{A/K}(a) = 0$, $\mathrm{Tr}_{A/K}(a) = 0$.

Remark 3.11.3. The norm and trace have similar properties as the determinant and trace of matrices:

1) $\mathrm{Tr}_{A/K} : A \to K$ is K-linear. If $a_1, a_2 \in A$, $\lambda_1, \lambda_2 \in K$, then $\varphi_{\lambda_1 a_1 + \lambda_2 a_2} = \lambda_1\varphi_{a_1} + \lambda_2\varphi_{a_2}$; and taking trace of a matrix (i.e. the map $\mathrm{tr} : M_n(K) \to K$) is K-linear.
2) $\mathrm{N}_{A/K}(a_1a_2) = \mathrm{N}_{A/K}(a_1) \cdot \mathrm{N}_{A/K}(a_2)$. For all $a_1, a_2 \in A$, $\varphi_{a_1a_2} = \varphi_{a_1} \circ \varphi_{a_2}$; and the determinant $\det : M_n(K) \to K$ is multiplicative. If $A = L$ is a field, then $N_{L/K} : L^\times \to K^\times$ is a group homomorphism.
3) We have the transitive formula: given a field extension $k \hookrightarrow A$, we have
$$\mathrm{N}_{A/k} = \mathrm{N}_{K/k} \circ \mathrm{N}_{A/K}, \qquad \mathrm{Tr}_{A/k} = \mathrm{Tr}_{K/k} \circ \mathrm{Tr}_{A/K}$$

Proof. Write out the basis for the corresponding algebras. Choose $e_1, \dots, e_m$ a basis for K as a k-vector space, and $f_1, \dots, f_n$ a basis for A as a K-vector space. Then $(e_i f_r)$ for $1 \le i \le n$, $1 \le r \le m$ gives a basis of A as a k-vector space. Fix $a \in A$, define $(c_{ij}) \in K$ and $(\gamma_{ijrs}) \in k$ as

$$af_j = \sum_{i=1}^{n} c_{ij} f_i, \qquad c_{ij} e_s = \sum_{r=1}^{m} \gamma_{ijrs} e_r$$

Verify the equality of both sides:

$$\mathrm{RHS} = \mathrm{Tr}_{K/k} \circ \mathrm{Tr}_{A/K}(a) = \sum_{i=1}^{n} \mathrm{Tr}_{K/k}(c_{ii}) = \sum_{i=1}^{n} \sum_{r=1}^{m} \gamma_{iirr}$$

while φ_a in the basis for A over k can be expressed as

$$af_j e_s = \sum_{i=1}^{n} c_{ij} f_i e_s = \sum_{i=1}^{n} \sum_{r=1}^{m} \gamma_{ijrs} f_i e_r \quad \Longrightarrow \quad \mathrm{LHS} = \mathrm{Tr}_{A/K}(a) = \sum_{i=1}^{n} \sum_{r=1}^{m} \gamma_{iirr}$$

□

4) Given $K \hookrightarrow K'$ a field extension, we have $\mathrm{Tr}_{(A \otimes_K K')/K'}(a \otimes 1) = \mathrm{Tr}_{A/K}(a)$.

Proof. Notice that for $e_1, \dots, e_n$ a basis of A over K, $e_1 \otimes 1, \dots, e_n \otimes 1$ gives a basis of $A \otimes_K K'$ over K'. The matrix representation of $\varphi_{a \otimes 1}$ and φ_a are the same; and therefore the traces are identical. □

5) For $A = A_1 \times A_2$, via considering the trace and determinant for block matrices we have

$$\mathrm{Tr}_{A/K}(a_1, a_2) = \mathrm{Tr}_{A_1/K}(a_1) + \mathrm{Tr}_{A_2/K}(a_2) \qquad \mathrm{N}_{A/K}(a_1, a_2) = \mathrm{N}_{A_1/K}(a_1) \cdot \mathrm{N}_{A_2/K}(a_2)$$

The trace uniquely characterizes separable extensions:

Theorem 3.11.4. Given $K \hookrightarrow L$ a finite field extension, L/K is separable if and only if $\mathrm{Tr}_{L/K} \neq 0$.

Proof. To prove the proof we need the following intermediate results:

Lemma 3.11.5. Suppose that we have $K \hookrightarrow K' = K(\alpha)$ where α is separable over K. Then $\mathrm{Tr}_{K'/K} \neq 0$.

Lemma 3.11.6. Suppose that we have $K \hookrightarrow K' = K(\alpha)$ where $\mathrm{char}(K) = p$, $\alpha \notin K$, $\alpha^p \in K$. Then $\mathrm{Tr}_{K'/K} = 0$.

These two implies the theorem:

- If L/K is not separable, then there exists $\alpha \in L$ that is not separable over K. Let f be the minimal polynomial of α. By 3) in the definition $f \in k[x^p]$, i.e. $f = g(x^p)$ for $g \in k[x]$. Consider the chain of extensions

$$K \hookrightarrow K(\alpha^p) = K[x]/(g) \hookrightarrow K(\alpha) = K[x]/(f) \hookrightarrow L$$

Lemma 3.11.6 gives $\mathrm{Tr}_{K(\alpha)/K(\alpha^p)} = 0$. Remark 3.11.3 3) gives

$$\mathrm{Tr}_{L/K} = \mathrm{Tr}_{K(\alpha^p)/K} \circ \underbrace{\mathrm{Tr}_{K(\alpha)/K(\alpha^p)}}_{=0} \circ \mathrm{Tr}_{L/K(\alpha)} = 0$$

- If L/K is separable, Primitive Element Theorem gives $L = K(\alpha)$ for $\alpha \in L$. Apply Lemma 3.11.5 gives $\mathrm{Tr}_{L/K} \neq 0$.

Now prove the two lemmas:

Proof of Lemma 3.11.5. Let $K \hookrightarrow \bar{K}$ be the algebraic closure, and $A = K' = K(\alpha)$. By Remark 3.11.3 4), $\mathrm{Tr}_{A\otimes_K \bar{K}/\bar{K}} = 0$ if and only if $\mathrm{Tr}_{A/K} = 0$. Applying with $A = K(\alpha)$ gives

$$A \otimes_K \bar{K} = K(\alpha) \otimes_K \bar{K} = K[x]/(f) \otimes_K \bar{K}$$

where f is the minimal polynomial of α over K, and $K[\alpha] \simeq K[x]/(f)$ (via considering the ring homomorphism $K[x] \to K$, $x \mapsto \alpha$). Since α is separable over K, f splits in $\bar{K}$, i.e. we have

$$K' \otimes_K K \simeq \bar{K}[x]/(f) = \bar{K}[x]/(x-a_1)\cdots(x-a_n) \simeq \prod_{i=1}^{n} \bar{K}[x]/(x-a_i) \simeq \left(\bar{K}\right)^n$$

where all $a_1, \ldots, a_n \in \bar{K}$ are distinct, and $n = \deg f$. Then $\mathrm{Tr}_{A/K} = \mathrm{Tr}_{K'\otimes_K \bar{K}/\bar{K}}(a_1, \ldots, a_n) = a_1 + \cdots + a_n \neq 0$. □

Proof of Lemma 3.11.6. Let $\beta = \alpha^p \in K$. Then the minimal polynomial of α is $x^p - \beta$. The minimal polynomial cannot be of lower degree: suppose the minimal polynomial is g with $\deg g < p$, then the gcd of $g(0)$ and β must also be in K. Further since $\beta = \alpha^p$, $g(0) = \alpha^q$ for $q \nmid p$. But this implies that $\alpha \in K$ which is a contradiction.

Similarly by Remark 3.11.3 4),

$$K' \otimes_K \bar{K} \simeq K[x]/(x^p - \beta) \otimes_K \bar{K} \simeq \bar{K}[x]/(x^p - \beta) \simeq \bar{K}[x]/(x-\alpha)^p$$

A basis of $K' \otimes_K \bar{K}$ as a $\bar{K}$-vector space is $\{\bar{1}, \overline{x-\alpha}, \cdots, \overline{(x-\alpha)^{p-1}}\}$, and is of dimension p. To compute $\mathrm{Tr}_{K'/K}$ we only need to compute $\mathrm{Tr}_{(K'\otimes_K \bar{K})/\bar{K}}$ on the basis elements, but

- $\mathrm{Tr}_{(K'\otimes_K \bar{K})/\bar{K}}(1) = \dim_{\bar{K}}(K' \otimes_K \bar{K}) = p = 0$.
- $\mathrm{Tr}_{(K'\otimes_K \bar{K})/\bar{K}}(\overline{(x-\alpha)^i}) = 0$ since $\overline{(x-\alpha)^i}$ is nilpotent.

□

This finishes the whole proof. □

Recall that in Proposition 3.6.7 we proved the if the large extension is separable, then the intermediate extensions are also separable. With the theorem above the converse is straightforward:

Corollary 3.11.7. If $K_1 \hookrightarrow K_2 \hookrightarrow K_3$ are field extensions, and K_3/K_2 and K_2/K_1 are separable, then K_3/K_1 is separable.

Proof. $\mathrm{Tr}_{K_3/K_1} = \mathrm{Tr}_{K_2/K_1} \circ \mathrm{Tr}_{K_3/K_2} \neq 0$ where by Theorem 3.11.4 Tr_{K_2/K_1} and Tr_{K_3/K_2} are nonzero. Apply the theorem again gives that K_3/K_1 is separable. □

Remark 3.11.8. The reasoning can be conducted backwards to get the previous result (Proposition 3.6.7) as well.

Corollary 3.11.9. Given a field extension $K \hookrightarrow L = K(a_i \mid i \in I)$. If a_is are algebraic and separable over K. Then L/K is a separable algebraic extension.

Proof. For all $a \in L$, it must lie in $K(a_i \mid i \in I_0)$ for some I_0, where I_0 is finite. Therefore, it suffices to deal with the finite case.

Suppose that I is finite. Then we can write $L = K(a_1, \ldots, a_n)$. Apply induction on n:

- For $n = 1$, Lemma 3.11.5 gives $\mathrm{Tr}_{K(a_1)/K} \neq 0$. Apply Theorem 3.11.4 gives $K \hookrightarrow K(a_1)$ separable.
- Inductive step. Consider the field extensions

$$K \hookrightarrow K' = K(a_1, \ldots, a_{n-1}) \hookrightarrow K(a_1, \ldots, a_n) = K'(a_n)$$

  Inductive hypothesis gives that the first extension is separable, and the argument for $n = 1$ gives that the second extension is separable. Proposition 3.6.7 gives that the whole extension is separable.

□

With the theorem and results in corollary we can discuss a bit further about separable extensions:

Proposition 3.11.10. Let $K \hookrightarrow L$ be an algebraic extension, then $L' := \{\alpha \in L \mid \alpha \text{ separable over } K\} \subseteq L$ is a subfield of L containing K.

Proof. By Corollary 3.11.9, $K \hookrightarrow K(L')$ is separable. But $K(L') = L'$: L' contains $K(L')$ as in particular L' contains K; and the inclusion in the other direction is clear. □

Definition 3.11.11 (Separable Closure)**.** $L' := \{\alpha \in L \mid \alpha \text{ separable over } K\} \subseteq L$ is the **separable closure** of K in L. A separable closure of a field K is its separable closure in an algebraic closure $K \hookrightarrow \bar{K}$.

Definition 3.11.12 (Purely Inseparable)**.** An algebraic extension $K \hookrightarrow L$ is **purely inseparable** if for any element $\alpha \in L \setminus K$, the minimal polynomial of α over K is not separable.

3.12 Solvability by Radicals

As we wrap up the discussion of Galois Theory, we would like to see how the Galois group is related to the solvability of polynomials. Towards the end of this section we will relate this to the solvability of the Galois group, which connects to the first part of this course.

Definition 3.12.1 (Compositum)**.** Given a field extension $K \hookrightarrow L$, with subextensions $K \hookrightarrow K_1 \hookrightarrow L$ and $K \hookrightarrow K_2 \hookrightarrow L$. The **compositum** of extensions K_1K_2 is the smallest subfield of L containing both K_1 and K_2

Remark 3.12.2. By definition, we have $K_1K_2 = K_1(K_2) = K_2(K_1)$.

Proposition 3.12.3. If the field extension K_1/K is finite and Galois, then K_1K_2/K_2 is Galois; and we have a group isomorphism $G(K_1K_2/K_2) \simeq G(K_1/K_1 \cap K_2)$, given by $\sigma \mapsto \sigma|_{K_1}$.

Proof. Since K_1/K is separable, by the Primitive Element Theorem there exists $a \in K_1$ s.t. $K_1 = K(a)$. Let f be the minimal polynomial of a over K. Since K_1/K is normal and separable, f has distinct roots $a_1 = a, \dots, a_n \in K_1$. Then $K_1K_2 = K_2(K_1) = K_2(a)$ is Galois if and only if the minimal polynomial of a over K_2 g has distinct roots in K_1K_2. This is indeed the case as we have the field extension $K \hookrightarrow K_2$, $g \mid f$ (since $g(a) = f(a) = 0$), where in particular all roots of g are roots of f and are therefore distinct.

Now consider the group homomorphism

$$\varphi : G(K_1K_2/K_2) \to G(K_1/K_1 \cap K_2), \qquad \sigma \mapsto \sigma|_{K_1}$$

By definition of Galois group, $\sigma|_{K_2} = \mathrm{Id}_{K_2}$. Restricting it further to K_1 gives $\sigma|_{K_1 \cap K_2} = \mathrm{Id}_{K_1 \cap K_2}$. Restricting a ring homomorphism is clearly a group homomorphism. Now check that this gives an isomorphism:

- *Injectivity.* For $\sigma \in \ker \varphi$, we have $\sigma|_{K_1} = \mathrm{Id}_{K_1}$. Further by the definition of Galois group, $\sigma|_{K_2} = \mathrm{Id}_{K_2}$. Therefore σ fixes elements in the field generated by K_1 and K_2, which is exactly the compositum of K_1 and K_2, i.e. $\sigma = \mathrm{Id}_{K_1K_2}$.
- *Surjectivity.* Let $H = \mathrm{im}\, \varphi$. We want to show that $H = G(K_1/K_1 \cap K_2)$. Consider the field extensions

  $$^{(1)}K \hookrightarrow K_1 \cap K_2 \hookrightarrow K_1^H \hookrightarrow K_1 \qquad ^{(2)}K_2 \hookrightarrow K_1^H K_2 \hookrightarrow K_1K_2$$

  where

  $$K_1^H = \{u \in K_1 \mid \sigma(u) = u, \forall \sigma \in H\}$$

  Then for all $\sigma \in G(K_1K_2/K_2)$, by definition $\sigma|_{K_2} = \mathrm{Id}_{K_2}$; and $\sigma|_{K_1^H} = \mathrm{Id}_{K_1^H}$ as by definition of φ, $\sigma|_{K_1} \in H$. By the same reasoning as for injectivity, $\sigma|_{K_1^H K_2} = \mathrm{Id}_{K_1^H K_2}$. By applying Fundamental Theorem of Galois Theory 2) extension (2), the kernel of the map $G(K_1K_2/K_2) \to G(K_1^H K_2/K_2)$ given by restriction to $K_1^H K_2$ has the whole group as the kernel, which implies that $K_1^H K_2 \subseteq K_2$, i.e. $K_1^H \subseteq K_1 \cap K_2$. Apply the same result on extenson (1) gives for $G = G(K_1/K_1 \cap K_2)$, $G/H \simeq G(K_1^H/K_1 \cap K_2) = \{e\}$, i.e. $H = G(K_1/K_1 \cap K_2)$.

□

Remark 3.12.4. The previous result shows that if K_1/K and K_2/K are finite Galois extensions, then K_1K_2/K is also a finite Galois extension. Further $G(K_1K_2/K)$ can be described using $G(K_1/K)$ and $G(K_2/K)$. Further notice that the isomorphism between Galois group resembles the Second Isomorphism Theorem.

We now turn to associating Galois extensions with polynomials, seeking to describe the field "generated via adding its roots":

Definition 3.12.5 (Galois Group of a Polynomial)**.** Let K be a field, and $f \in K[x]$ with $\deg f \geq 1$ and f separable. If $K \hookrightarrow L$ is the splitting field of f, then L/K is a finite Galois extension. The corresponding Galois group $G(L/K)$ is the **Galois group of** f.

Consider the algebraic closure $K \hookrightarrow \bar{K}$, with $a_1, \dots, a_n \in \bar{K}$ roots of f. Then $L = K(a_1, \dots, a_n)$. For $\sigma \in G(L/K)$, since f has coefficients in K, and $\sigma|_K = \mathrm{Id}_K$, each $\sigma(a_i)$ is a root of f, i.e. σ permutes the roots of f. This gives a group homomorphism

$$\varphi : G(L/K) \to S_n, \qquad \sigma \mapsto (i \mapsto j \text{ for } \sigma(a_i) = a_j)$$

As is shown in the previous introduction to Galois extensions, φ is injective, as for $\sigma \in \ker \varphi$, $\sigma(a_i) = a_i$ for all i. By definition σ fixes K, and therefore fixes $L = K(a_1, \dots, a_n)$, i.e. $\sigma = \mathrm{Id}_L$. This implies that $|G(L/K)| \leq |S_n| = n!$. We have also seen that in general φ is not surjective.

Consider now the case where φ is actually an isomorphism. Let F be a field, and $L = F(x_1, \dots, x_n)$ where all the x_is are formal variables. Notice that for all $\sigma \in S_n$, the universal property of $F[x_1, \dots, x_n]$ gives a ring homomorphism

$$g_\sigma : F[x_1, \dots, x_n] \to F[x_1, \dots, x_n], \qquad x_1 \mapsto x_{\sigma(1)}$$

Further by definition we have $g_{\sigma\tau} = g_\sigma g_\tau$. This implies that each g_σ is an F-algebra automorphism. This induces

$$\widetilde{g_\sigma} : F(x_1, \dots, x_n) \to F(x_1, \dots, x_n) = L$$

which is a ring homomorphism fixing F. We then have a group homomorphism $S_n \to G(F(x_1, \dots, x_n)/F)$ (notice that the extension $F \hookrightarrow F(x_1, \dots, x_n)$ is not necessarily Galois). It is injective as for $g_\sigma = \mathrm{Id}$, $g_\sigma(x_i) = x_i$ for all i, i.e. $\sigma(i) = i$ for all i. This gives a subgroup of $G(F(x_1, \dots, x_n)/F)$ isomorphic to S_n.

Now consider $K = \{u \in F(x_1, \dots, x_n) \mid \widetilde{g_\sigma}(u) = u, \forall \sigma \in S_n\}$. By Fundamental Theorem of Galois Theory 2) we have the field extensions $F \hookrightarrow K \hookrightarrow L$. By hypothesis $G(L/K) \simeq S_n$, which by Proposition 3.10.7 the degree of the extension L/K is equal to $|S_n| = n!$.

Define $S_1, \dots, S_n \in F[x_1, \dots, x_n]$ s.t.

$$\prod_{i=1}^{n}(x - x_i) = x^n - S_1(x)x^{n-1} + \cdots + (-1)^n S_n(x)$$

where

$$\left.\begin{aligned} &S_1(x) = x_1 + \cdots + x_n \\ &S_2(x) = \textstyle\sum_{i<j} x_i x_j \\ &\cdots \\ &S_n(x) = x_1 \cdots x_n \end{aligned}\right\} \quad \underline{\text{elementary symmetric functions}} \text{ in } x_1, \dots, x_n$$

Notice that since $\sigma \in G(L/K)$ permutes only the roots of the polynomial, $S_1, \dots, S_n \in K$. This results in the field extension

$$F \hookrightarrow F(S_1, \dots, S_n) \hookrightarrow \underbrace{K \hookrightarrow L}_{\deg = n!}$$

where L is the splitting field of $f \in F(S_1, \dots, S_n)[x]$. Previously we have $|L/F(S_1, \dots, S_n)| \leq |S_n| = n!$. This gives the conclusion $K = F(S_1, \dots, S_n)$ if $\varphi : G(L/K) \to S_n$ is an isomorphism.

Remark 3.12.6. One can also show that for F an infinite field, for $c_1, \dots, c_n \in F$ in genenral the polynomial $g = x^n + c_1 x^{n-1} + \cdots + c_n \in F[x]$ also has the property that there exists an isomorphism between the Galois group of g and S_n, where in general means that there exists $h \in F[x_1, \dots, x_n]$ of degree at least 1 s.t. $h(c_1, \dots, c_n) \neq 0$.

Now we introduce the relation between solvability of Galois groups and solvability of polynomials:

Definition 3.12.7 (Root Extension). Given a field K, an extension $K \hookrightarrow K'$ is a **root extension** if there exists a sequence of field extensions

$$K = K_1 \hookrightarrow K_2 \hookrightarrow \cdots \hookrightarrow K_r = K'$$

s.t. for all $2 \leq i \leq n$, $K_i = K_{i-1}(a_i)$ where $a_i^{m_i} \in K_{i-1}$ for some $m_i \in \mathbb{Z}_{\geq 0}$. Notice that K_i is not required to contain all the roots of $a_i^{m_i}$.

Definition 3.12.8 (Resolved by Radicals). Let K be a field, and $f \in K[x]$ with $\deg f \geq 1$. Then f is **resolved by radicals** if inside the algebraic closure $\bar{K}$ of K, the splitting field L of f lies inside a root extension K' of K.

Theorem 3.12.9. Let K be a field that is characteristic-0. Then $f \in K[x]$ is resolved by radicals if and only if its Galois group is solvable.

Recall that a group is solvable if there exists a chain

$$\{e\} = G_0 \trianglelefteq \cdots \trianglelefteq G_r = G, \qquad G_i/G_{i-1} \text{ abelian}$$

For G finite and solvable, G_i/G_{i-1} is finite and abelian. Applying the Structural Theorem implies that G_i/G_{i-1} is cyclic.

Example 3.12.10. Recall that we discussed about the solvability of symmetric groups of small order:

1. If $\deg(f) \leq 4$, f is solvable by radicals: the case is trivial for S_1 and S_2; and we have

$$\{e\} \trianglelefteq \langle \sigma \rangle \trianglelefteq S_3 \qquad \{e\} \trianglelefteq K_4 \trianglelefteq A_4 \trianglelefteq S_4$$

2. For $n = \deg(f) \geq 5$, S_n is not solvable, which implies that there exists f that is not solvable by radicals (Abel's Theorem).

We omit the proof of the theorem, and instead show some results that are helpful with the proof of theorem.

Proposition 3.12.11. Let K be a field, and $m \in \mathbb{Z}_{\geq 0}$, satisfying either $\mathrm{char}(K) = 0$, or $\mathrm{char}(K) = p \nmid m$; and K contains m-th root of unity in $\bar{K}$.

1) If $K \subseteq K' = K(a)$ s.t. $a^m = b \in K$, then $G(K'/K) \simeq \mathbb{Z}/m'\mathbb{Z}$ with $m' \mid m$.

2) If $K \hookrightarrow L$ Galois, s.t. $G(L/K) \simeq \mathbb{Z}/m\mathbb{Z}$, then there exists $a \in L$ s.t. $L = K(a)$ and $a^m \in K$.

The proof is related to Kummer Theory, and is omitted.

Lemma 3.12.12. If $\mathrm{char}(K) = 0$, and ζ is a primitive n-th root of unit. Then $G(K(\zeta)/K)$ is abelian.

Proof. To get an automorphism, consider σ where $\sigma(\zeta)$ is also a primitive n-th root of unit. Then $\sigma(\zeta) = \zeta^j$ for j relative prime with n. This gives $G(K(\zeta)/K) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$ which is abelian. □