

# Table of Contents

- **0. Preliminaries**
  - Resources Used
  - Notation
  - Currently
- **1. Groups**
  - Def. Group
  - Remarks
  - Thm. Basic Group Properties
  - Thm. Basic *Monoid* Properties
  - Thm. Semigroup to Group
  - Thm. Semigroup to Group 2
  - Thm. Generalized Associative Law
  - Def. Order
  - Notation. Subsets
  - Notation. The Additive Notation
  - Thm. More Group Properties
  - Exercises
    - #1
    - #2
    - #3
- **2. Group Examples**
  - Klein 4-Group
  - Dihedral Groups
  - Symmetric Groups
    - Thm. Symmetric Groups Basics
  - Matrix Groups
    - #1
  - The Quaternion Group
  - The  $Q_p$  Group
  - Def. Homomorphisms
  - Exercise 2
- **3. Subgroups**
  - Def. Subgroup
  - Thm. Equivalent Subgroup Definitions
  - Example. Some Subgroups
  - Thm. Finite and Closed Subset
  - Thm. Intersection of Subgroups
  - Thm. Subgroups Under Multiplication
  - Def. Complement
  - Thm. Basic Complement Properties
  - Def. Maximal Subgroup
  - Def. Frattini Subgroup

- Thm. Frattini Subgroup and Non-Generators
- Exercises
  - #1
  - #2
  - #3
  - #4
- **4. Homomorphisms**
  - Def. Homomorphism
    - Example
  - Def. Kernel
  - Notation. Homomorphisms
  - Thm. Basic Homomorphism Properties
  - Def. Basic Kernel Properties
  - Def. Endomorphisms
  - Def. Automorphisms
  - Exercises
    - #1
    - #2
    - #3
- **5. Generators**
  - Def. Generators
    - Thm. Equivalent Generation Definition
    - Thm. Equivalent Generation Definition 2
  - Def. Join of Subgroups
  - Example. Generator Examples
- **6. Cyclic Groups**
  - Def. Cyclic Group
  - Thm. Basic Element Order Properties
  - Thm. Basic Cyclic Properties
  - Thm. Fundamental Order Property
  - Thm. Every Subgroup of  $\mathbb{Z}$  is Also Cyclic
  - Thm. Same Order Cyclics are Isomorphic
  - Thm. Fundamentals of Element Orders
  - Thm. Orders of Commutative Elements
  - Thm. On Generators of Cyclics
  - Thm. Basic Cyclic Properties
  - Thm. Homomorphisms from Cyclics
  - Thm. Finitely Many Subgroups Imply Finite Group
  - Exercises
    - #1
- **7. Cosets and Indices**
  - Def. Coset
  - Def. Coset Congruence
  - Thm. Coset Congruence
    - Corollary. Coset Congruence
  - Def. Index

- Thm. Index Theorem
  - Corollary: Lagrange's Theorem
  - Corollary: Element Order Divides Group Order
- Thm. Cauchy's Theorem
- Thm. Order of Subgroup Multiplication
- Thm. 1
- Thm. 2
- Exercise
- Thm. Groups of Prime Order
- **8. Conjugates and Normals**
  - Def. Conjugate
  - Thm. Basic Conjugate Properties
  - Def. Normal
  - Thm. Equivalent Normal Definitions
  - Thm. More Normal Properties
  - Thm. Normal and Subgroup Properties
  - Exercises
    - #1
    - #2
- **10. Normalizer And Centralizer**
  - Def. Centralizer
  - Def. Center
  - Def. Normalizer
  - Thm. Basic Properties of Normalizer and Centralizer
  - Thm. '
  - Notation. Normal Generators
  - Thm. Building Normal from a Subgroup
  - Exercise
- **10. Commutators**
  - Def. Commutator
    - Thm. Basic Commutator Properties
  - Def. Commutator Subgroup and Derived Series
  - Thm. Three Commutator Lemma
  - Exercise
- **11. Quotients and Isomorphisms**
  - Def. (Group) Congruence Relation
  - Thm. Group Congruences and Normals
  - Def. Quotient Group
  - Thm. Basic Quotient Properties
  - Def. Projection
    - Thm. Commutativity of Projection
  - Thm. Fundamental Theorem on Homomorphisms
  - Thm. First Isomorphism Theorem
  - Thm. Second Isomorphism Theorem
  - Thm. Third Isomorphism Theorem
  - Thm. Homomorphism Induced Bijection

- Corollary. Normal Subgroups of Quotients
- Def. Inner and Outer Automorphisms
- Thm. Inner Automorphisms
- Def.
- Thm. Equivalent Normal Definition
- **12. Endomorphisms**
  - Def. Inner and Outer Automorphisms
  - Thm. Inner Automorphisms
  - Def. Endomorphic Invariance
  - Thm. Equivalent Normal Definition
  - Notation. Invariance
  - Thm. Invariance Transitivity
  - Def. Characteristic Subgroup
  - Thm. Characteristic Normality
  - Def. Complete Group
  - Exercises
    - #1
    - #2
- **13. Symmetric Groups**
  - Def. Permutation
  - Def. Support
  - Def. Disjoint Permutations
  - Def. Cycle
  - Def. Symmetric Group
  - Thm. Permutations are (Unique) Product of Disjoint Cycles
    - Corollary. Order of Permutation
    - Corollary. Permutations are a Product of Transpositions
  - Def. Odd and Even
  - Thm. Exclusively Odd or Even
  - Thm. Alternating Group
  - Thm.  $A_n$  is (Generally) Simple
    - Lemma. 1
    - Lemma. 2
  - Thm. Hölder
  - Thm. Dihedral Group Generators
  - Exercise. Generator of  $D_n$
  - Thm. Center of  $D_n$
- **14. Direct Products and Sums**
  - Def. Direct Product (of Groups)
  - Def. Natural Projections
  - Def. (External) Weak Direct Product
  - Thm. Normals and Injections
  - Thm. Direct Sum and Family of Homomorphisms
  - Thm. Direct Sum of Normals
  - Def. Internal Product
  - Thm. Normal Decomposition Condition
  - Thm. Internal Direct Sum and Family of Homomorphisms

- Corollary. Normals and Quotients
- **15. Free Groups**
  - Def. Free Generator
  - Def. Word
  - Def. Free Group
  - Thm. Universal Property
    - Corollary
  - Def. Presentation
    - Example
  - Thm. Van Dyck
  - Def. Free Product
  - Exercises
    - Exercise 1
    - Exercise 2
- **16. Free Abelian Groups**
  - Def. Basis
  - Thm. Equivalent Basis Conditions
  - Def. Free Abelian Group
  - Thm. Basis Cardinality
  - Thm. Isomorphism on Free Abelian Groups
  - Thm. Free Abelian Groups and Abelian Groups
  - Thm. Basis for Subgroups
    - Corollary. Rank of Subgroups
- **17. Automorphic Extensions**
  - Def. (Outer) Semidirect Product
  - Thm. Normal Complement
  - Def. Inner Semidirect Product
  - Def. Wreath Product
- **A1. Appendix 1**
  - Def. Semidirect Product etc.
  - Def. Diagonal Subgroup
  - Def. Simple Group
  - Thm. On Simple Groups
  - Def. Perfect Group
  - Thm. Dedekind Modular Law (Identity)
  - Exercises
    - U 2.39
- **A2. Group Actions**
  - Def. Group Action

# 0. Preliminaries

- In these notes, all sets are considered to be proper sets as in ZFC, not classes.
- Basic (at least naive) set theory and simple combinatorics knowledge is assumed. Other than that, notes should be self-sufficient.

At the moment, these notes have a formal and reference-book like approach except these grayed out notes. I plan more intuition baked in for these notes, with much more visuals, examples and geometry involved.

## Resources Used

---

- **Algebra** by Thomas W. Hungerford
- **Fundamentals of the Theory of Groups**, translated second Russian Ed., by M.I. Kargaplov and Ju.I. Merzljakov
- **Group Theory Exercises and Solutions** by Mahmut Kuzucuoğlu
- **Graduate Algebra Problems with Solutions** by Mahmut Kuzucuoğlu
- **Abstract Algebra**, 3rd Ed., by David S. Dummit and Richard M. Foote

## Notation

---

- $0 \in \mathbb{N}$  and  $\mathbb{N}^+ := \mathbb{N} \setminus \{0\}$ .
- $\emptyset$  denotes the empty set.
- $(m, n)$  denotes the **greatest common divisor** of  $m, n \in \mathbb{N}$ .
- $\equiv_m$  denotes integer equivalence in modulo  $m$ .
- Cardinality of a set  $S$  is denoted with  $|S|$ .
- $d_1 \mid d_2 \mid \cdots \mid d_r$  means  $d_1$  divides  $d_2$  divides  $d_3$  etc.

## Currently

---

- There are not many exercises,
- Proofs are mostly absent,
- Typos are possible,
- Ordering is generally good but should be improved, and
- More visuals and intuition should be provided.

# 1. Groups

## Def. Group

---

A **group** is an ordered pair  $(G, \cdot)$  where  $G$  is a set and  $\cdot$  is a binary operation on  $G$  that satisfies:

Simply,  $\cdot$  is a (total) function from  $G$  to  $G$ . Notice that  $G$  is an any set, finite or infinite.

- **Associativity**, that is, for all  $a, b, c \in G$  we have  $(a \cdot b) \cdot c = a \cdot (b \cdot c)$

This alone defines a **semigroup**.

- **Identity**, that is, there exists  $e \in G$  called **identity** (of  $G$ ) such that for all  $a \in G$  we have  $a \cdot e = e \cdot a = a$ .

Until here it defines a **monoid** where identity is two-sided, namely left and right.

- **Inverse**, that is, for each  $a \in G$  there exists an element (called **inverse**)  $b \in G$  such that  $a \cdot b = b \cdot a = e$ .

Noting that the **identity** of a group and the **inverse** of an element in that group is always unique (exercise) we will denote the inverse of an element  $a$  with  $a^{-1}$  unless it is **abelian**.

A group is called **abelian** (or **commutative**) if its elements commute, that is, if for all  $a, b \in G$  we have  $a \cdot b = b \cdot a$ . For abelian groups, we may prefer the additive notation  $+$  instead of  $\cdot$  for the binary operation and denote the inverse with  $-a$  instead.

You might also sometimes want to consider the group as a triplet with identity  $(G, \cdot, e)$  as it is not clear otherwise what is the identity explicitly.

## Remarks

---

The definition (or axioms) given above are not minimal. For example, it's enough to just accept **right-identity** and **right-inverse** for it to be group. Using just these two, you can later prove it also holds for the **left-identity** and **left-inverse** with the help of the associative property.

Associative property by far is the most powerful property of the group. It allows you to write your expression (involving only  $\cdot$ ) without any parentheses and much more.

Indeed a structure which only satisfies associative property is called a **semigroup**. A semigroup with identity is called a **monoid** and a monoid with inverses is called a **group**.

## Thm. Basic Group Properties

---

Remembering any group is also a monoid and thus a semigroup, let  $(G, \cdot)$  be a group. Then:

1. Identity  $e$  is unique. The uniqueness of the identity element does not require the use of associativity.
2. For each  $a \in G$ , inverse of  $a$  is unique.

3. For each  $a \in G$ , we have  $(a^{-1})^{-1} = a$ .

4. For all  $a, b \in G$ , we have  $(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$ . Indeed, in general,  $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$ .

| Exercise

## Thm. Basic *Monoid* Properties

---

If  $M$  is a monoid, then

1. The identity element of  $M$  is unique.

## Thm. Semigroup to Group

---

Let  $(S, \cdot)$  be a semigroup, then it is a group if and only if both of the following hold:

- Left-identity exists, and
- Left-inverse exists for each  $s \in S$ .

| By symmetry, the analogous result holds for rights instead of left.

## Thm. Semigroup to Group 2

---

Let  $S$  be a semigroup, then it is a group if and only if for all  $a, b \in S$  the equations

$$\begin{aligned} ax &= b \\ ya &= b \end{aligned}$$

have solutions in  $G$ .

| Exercise

## Thm. Generalized Associative Law

---

Let  $S$  be a semigroup and  $a_i \in S$ . Associative property implies that the expression  $a_1 \cdot a_2 \cdots a_n$  is the same no matter how the expression bracketed.

### ► Proof

| Similarly one could also prove **Generalized Commutative Law** for the commutative property.

## Def. Order

---

Let  $(G, \cdot)$  be a group and  $a \in G$ .

The **order of (the group)  $G$**  is denoted by  $|G|$  and is the cardinality of the set  $G$ .



The **order of (the element)**  $a$  is denoted by  $|a|$  and (if exists) it is the least positive integer  $n$  such that  $x^n = e$ . If there is no such  $n$ , we say the order is infinite.

| Order of an element  $a$  is sometimes denoted with  $o(a)$ .

If the order of an element  $x$  (or group) is finite, we will denote it with  $|x| < \infty$ . Moreover, if  $x^2 = x$ , then  $x$  is called an **idempotent element** where  $e$  is the **trivial idempotent element**.

We say that a group is **torsion-free** if every non-identity element has infinite order. If every element of a group has finite order then we say the group is **periodic**.

If orders of a periodic group are bounded, then the least common multiple of their orders is called the **exponent** of the group. If the orders of elements of a periodic group are powers of prime  $p$ , then we call the group a  $p$ -group.

## Notation. Subsets

---

Let  $G$  be a group and  $A, B \subseteq G$ , then we define

1.  $AB := \{ ab \in G \mid a \in A, b \in B \},$
2.  $A^0 := \{e\},$
3.  $A^n := AA^{n-1},$
4.  $A^{-1} := \{ a^{-1} \in G \mid a \in A \}.$

## Notation. The Additive Notation

---

If the binary operation is written additively, which is mostly the case for abelian groups, we may write:

- 0 for the identity instead of 1 (or  $e$  for that matter).
- $na$  instead of  $a^n$  where  $n \in \mathbb{Z}$ . Notice that operation between  $n$  and  $a$  is not the binary operation of our structure but rather " $n$  times  $a$ ".

We define  $a^0$  (or  $0a$ ) as the identity element 1 or 0. Notice that, in additive notation,  $0a$  is not the multiplication by the identity but rather " $0$  times  $n$ " which we define to be the identity 0.

## Thm. More Group Properties

---

Let  $G$  be a group, then

1. If  $a^2 = e$  for all  $a \in G$ , then  $G$  is abelian. (Such groups are called **elementary abelian 2-groups**.)
2. If  $|G|$  is finite and even, then it has an element  $x$  of order 2. Moreover,  $x \in Z(G)$  that is  $g^{-1}xg = x$  for all  $g \in G$ .
3. If  $A \subseteq G$  and  $g \in G$ , then  $|A| = |gA| = |Ag|.$

► **Proof**

# Exercises

---

## #1

Let  $G$  be a group and  $x, y \in G$  such that  $xy$  has finite order  $k$ , then  $|xy| = |yx|$ .

## #2

Let  $G$  be a group and  $A, B \subseteq G$  such that  $|A| + |B| > |G|$ , then  $G = AB$ .

► **Proof**

## #3

Let  $G$  be a group of finite order and  $S \subseteq G$  such that  $|S| > \frac{|G|}{2}$ , then  $S^2 = G$ .

► **Proof**

# 2. Group Examples

All of these groups can be considered their own field of research, so it is suggested you visit their wiki, understand the basics, and follow from there as you see fit.

## Klein 4-Group

---

See **Wikipedia: Klein four-group**.

The Klein 4-group can be defined by the group presentation

$$V = \langle a, b \mid a^2 = b^2 = (ab)^2 = e \rangle.$$

Such group is

- of order 4,
- Abelian,
- all non-identity elements have order 2,
- smallest non-cyclic group,
- isomorphic to Dihedral Group of order 4,
- isomorphic to  $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ .

| Also note that any group of order 4 is isomorphic to either  $\mathbb{Z}_4$  or  $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ .

## Dihedral Groups

---

See **Wikipedia: Dihedral group**.

## Symmetric Groups

---

See **Wikipedia: Dihedral group**.

### Thm. Symmetric Groups Basics

- For  $n > 2$  the symmetric group  $S_n$  is nonabelian. So,  $S_3$  is a good example of nonabelian group of order 3.

## Matrix Groups

---

### #1

Find the order of the (general linear) group  $GL(3, \mathbb{Z}_5)$ .

| In General Linear Group, matrix multiplication is the binary operation.

## The Quaternion Group

---

See **Wikipedia: Quaternion group**.

## The $Q_p$ Group

---

Let  $p$  prime. Denote by  $Q_p$  the set:

$$\{m/n^p : m, n \in \mathbb{Z}\}$$

or the group with the usual addition in rationals.

## Def. Homomorphisms

---

Let  $(G, \cdot_G, e_G)$  and  $(H, \cdot_H, e_H)$  be groups.

The (total) function (or map)  $\varphi : G \rightarrow H$  is called a **(group) homomorphism** if, for all  $a, b \in G$ :

$$\varphi(a \cdot_G b) = \varphi(a) \cdot_H \varphi(b)$$

Mostly, we will not be as explicit about the operations and simply write  $\varphi(ab) = \varphi(a)\varphi(b)$ .

The homomorphism  $\varphi : G \rightarrow H$  is called:

- an **monomorphism** if it is injective,
- an **epimorphism** if it is surjective,
- an **isomorphism** if it is bijective.
  
- an **endomorphism** if  $G = H$ , and
- an **automorphism** if it is an endomorphism and bijective.

Notice that if there exists an isomorphism between two groups, then basically, they have the same structure\*.

(Existence of an) isomorphism between two groups  $G$  and  $H$  is denoted with  $G \cong H$ .

## Exercise 2

---

Prove  $Q_p$  is *not* isomorphic to  $Q_r$  for distinct primes  $p$  and  $r$ .

Exercise

# 3. Subgroups

Until now we have explicitly defined and shown which multiplication is to which operator and which identity belongs to which group. From now on, these must be understood from the context. We will prefer little brevity over cumbersome notation.

## Def. Subgroup

---

Let  $G$  be a group and non-empty  $H \subseteq G$ . The non-empty subset  $H$  is called a **subgroup** if  $H$  is again a group under the restriction of  $G$ 's binary operation. This implies  $H$  has the same identity as  $G$  under the same binary operation.

## Thm. Equivalent Subgroup Definitions

---

A subset  $H \subseteq G$  is a subgroup of  $G$  if

- $H$  has the same identity as  $G$ ,
- For all  $a, b \in H$ , we have  $ab \in H$  that is  $HH \subseteq H$ ,
- Every element  $h \in H$  has an inverse that is  $H^{-1} \subseteq H$ .

To be more compact, *non-empty*  $H \subseteq G$  is called a **subgroup** if and only if (exercise):

- For all  $a, b \in H$  we have  $ab^{-1} \in H$ .

From now on, we will denote by  $H \leq G$  that  $H$  is a subgroup of  $G$ , moreover  $H < G$  if  $H \neq G$ . The latter is called a **proper subgroup** of  $G$ .

Any group has two subgroups called the **trivial subgroup** which consists of only the identity and the group itself.

Convention regarding to this **trivial** and **proper** notation differs from author to author — we will stick to this naming.

## Example. Some Subgroups

---

- Under addition,  $\mathbb{Z} < \mathbb{Q}_p, < \mathbb{Q} < \mathbb{R} < \mathbb{C}$ ,
- Under addition,  $\mathbb{Z} = \bigcap \mathbb{Q}_p$ ,
- $\mathbf{GF}(p^m) \leq \mathbf{GF}(p^n)$  if  $m \mid n$  where  $\mathbf{GF}(p^m)$  is the appropriate subset of the algebraic closure of  $\mathbf{GF}(p)$ .
- Under multiplication,  $\mathbb{Z}^* < \mathbb{Q}^*, < \mathbb{R}^* < \mathbb{C}^*$ ,
- Under multiplication,  $\mathbb{C}_p^* < \mathbb{C}_{p^2}^* < \dots < \mathbb{C}_{p^\infty}^*$ ,
- $\mathbb{C}_{p^\infty} = \bigcup \mathbb{C}_{p^n}$ ,
- $\mathbf{GF}(p^m)^* \leq \mathbf{GF}(p^n)^*$  if  $m \mid n$ .

- The subset  $A_n$  of all *even* permutations forms a subgroup called the **alternating group of degree  $n$** , and  $|A_n| = n!/2$ .

## Thm. Finite and Closed Subset

---

Let  $G$  be a group and  $S$  a non-empty subset of  $G$ . If  $S$  is finite and closed under the group product, then  $S$  is a subgroup of  $G$ .

| So, we don't even need the inverse condition if  $S$  non-empty and finite.

### ► Sketch of Proof

## Thm. Intersection of Subgroups

---

Let  $\{H_i\}$  be any non-empty family of subgroups of  $G$ , then  $\bigcap H_i$  is also a subgroup of  $G$ .

| Exercise

## Thm. Subgroups Under Multiplication

---

Let  $G$  be a group and  $H, K \leq G$ , then

- $HH = H$  and  $H^{-1} = H$ , thus obviously
- $HH^{-1} = H$ ,
- $HK$  is a subgroup of  $G$  if and only if  $HK = KH$ , and

| Exercise

## Def. Complement

---

Let  $H \leq G$ . We say  $K$  is a **complement** of a subgroup  $H$  if

- $G = HK$ , and
- $H \cap K = \{e\}$ .

Noting  $KH = HK$ , this complement relation is symmetrical.

## Thm. Basic Complement Properties

---

1. Complements need not to exist, and if they exist they need not to be unique.

Let  $H$  and  $K$  be complements in  $G$ , then

2. Every element of  $G$  has a unique expression as a product  $hk$  or  $k'h'$  where  $h, h' \in H$  and  $k, k' \in K$ .
3.  $K$  forms both left and right transversal of  $H$  for the cosets of  $H$ .

## ► Proof

## Def. Maximal Subgroup

---

Let  $G$  be a group and let  $H$  be a proper subgroups of  $G$ . We say  $H$  is a **maximal subgroup** if  $H \subseteq K$  implies  $K = H$  for all  $K < G$ .

| Simply,  $H$  is maximal if there is no greater proper subgroup which contain it.

## Def. Frattini Subgroup

---

Let  $G$  be a group. We define **frattini subgroup**  $\Phi(G)$  as the intersection of all maximal subgroups of  $G$ . In the case  $G$  has no maximal subgroups, we define  $\Phi(G) = G$ .

| This is analogous to the Jacobson radical in the ring theory.

## Thm. Frattini Subgroup and Non-Generators

---

The frattini subgroup  $\Phi(G)$  of a group  $G$  is equal to the set of all non-generators of  $G$ . Therefore, non-generators of a group form a subgroup — namely the frattini subgroup.

## Exercises

---

### #1

Let  $H \leq G$  and  $g \in G$  such that  $|g| = n$  and  $g^m \in H$  where  $(m, n) = 1$ , then  $h \in G$ .

## ► Help

### #2

Let  $G$  be a group and  $g \in G$  such that  $|g| = n_1 n_2$  where  $(n_1, n_2) = 1$ , then there exists  $g_1, g_2 \in G$  such that

- $g = g_1 g_2 = g_2 g_1$ , and
- $|g_1| = n_1$  and  $|g_2| = n_2$ .

### #3

Let  $H, K \leq G$  such that  $Hx = Ky$  for some  $x, y \in G$ , then  $H = K$ .

### #4

Let  $H \leq G$  and  $x, y \in G$ , then  $Hx = Hy$  if and only if  $x^{-1}H = y^{-1}H$ .

# 4. Homomorphisms

## Def. Homomorphism

---

Let  $(G, \cdot_G)$  and  $(H, \cdot_H)$  be semigroups.

The (total) function (or map)  $\varphi : G \rightarrow H$  is called a **homomorphism** if, for all  $a, b \in G$ :

$$\varphi(a \cdot_G b) = \varphi(a) \cdot_H \varphi(b)$$

Mostly, we will not be as explicit about the operations and simply write  $\varphi(ab) = \varphi(a)\varphi(b)$  instead.

The homomorphism  $\varphi$  is called:

- an **monomorphism** if it is injective,
- an **epimorphism** if it is surjective,
- an **isomorphism** if it is bijective.
- an **endomorphism** if  $G = H$ , and
- an **automorphism** if it is an endomorphism and bijective.

Composition of homomorphisms is again a homomorphism. Respectively, this is also the case for monomorphisms, epimorphisms, isomorphisms and automorphisms.

## Example

If  $A$  is abelian, then the map  $a \mapsto a^{-1}$  is an automorphism, and the map  $a \mapsto a^2$  is an endomorphism.

## Def. Kernel

---

If  $\varphi : G \rightarrow H$  is a group homomorphism, then the **kernel** of  $\varphi$  is defined as

$$\text{Ker } \varphi := \{ g \in G \mid \varphi(g) = e_H \}.$$

## Notation. Homomorphisms

---

We say semigroups  $G$  and  $H$  are **isomorphic** denoted with  $G \cong H$  if there exists an isomorphism between them.

Let  $\phi : G \rightarrow H$  be a group homomorphism,  $g \in G$  and  $A \subseteq G$ . Then

- $g^\phi$  denotes  $\phi(g)$ , and
- $A^\phi$  denotes  $\phi(A)$  called the **homomorphic (respectively monomorphic, epimorphic, ...) image** of  $A$ .



## Thm. Basic Homomorphism Properties

---

Let  $\varphi : G \rightarrow H$  be a group homomorphism, then

1.  $\varphi(e_G) = e_H$ . This is not necessarily true for monoid homomorphisms!
2.  $\varphi(g^{-1}) = \varphi(g)^{-1}$  for all  $g \in G$ ,
3.  $\varphi(g^n) = \varphi(g)^n$  for all  $g \in G$  and  $n \in \mathbb{Z}$ ,
4.  $\text{Ker } \varphi \leq G$ ,
5.  $\text{Im } \varphi := \varphi(G) \leq H$

| Exercise

## Def. Basic Kernel Properties

---

Let  $\varphi : G \rightarrow H$  be a group homomorphism, then

1.  $\varphi$  is a monomorphism if and only if  $\text{Ker } \varphi = \{e_G\}$ .
2.  $\varphi$  is an isomorphism if any only if there exists an homomorphism  $\varphi^{-1} : H \rightarrow G$  such that  $\varphi\varphi^{-1} = \text{id}_H$ .

| Exercise

## Def. Endomorphisms

---

Let  $G$  be a group and  $\text{End } G$  the **set of all endomorphism** on  $G$ , then  $\text{End } G$  is a semigroup under composition. Moreover, if  $G$  is a abelian,  $\text{End } G$  is a ring with pointwise function addition that is, for  $\alpha, \beta \in \text{End } G$

$$(\alpha + \beta)(x) = \alpha(x) + \beta(x) \quad x \in G$$

| Exercise

## Def. Automorphisms

---

The **set of automorphisms** on  $G$  denoted by  $\text{Aut } G$  is a group under function composition. Moreover,  $\text{Aut } G \leq \mathbf{S}(G)$  where  $\mathbf{S}(G)$  is the group of permutations on  $G$ .

| Exercise

## Exercises

---

### #1

$A$  is abelian group if and only if the map  $a \mapsto a^{-1}$  is an automorphism.

**#2**

Let  $\alpha : G \rightarrow G$  be a group automorphism and  $x \in G$ , then  $|\alpha(x)| = |x|$ .

**#3**

Let  $\alpha \in \text{Aut}(G)$  and  $H = \{ g \in G \mid \alpha(g) = g \}$ . Show that  $H$ , which is called the **fixed point subgroup of  $G$  under  $\alpha$**  is indeed a subgroup of  $G$ .

# 5. Generators

## Def. Generators

---

From now on, for a group  $G$  and a subset  $A \subseteq G$ , we will denote by  $L(G, A)$  the set of all subgroups of  $G$  that contain  $A$ . In particular,  $L(G)$  denotes the **set of all subgroups of  $G$** .

Noting that intersection of any collection of subgroups are again a subgroup, we define for any set  $M \subseteq G$ , the **subgroup generated by  $M$** , denoted  $\langle M \rangle$ , as the intersection of all subgroups which contain  $M$ . That is

$$\langle M \rangle := \bigcap_{H_i \in L(G, M)} H_i$$

Elements of  $M$ , or even  $M$  itself, are called the **generators** of the subgroup  $\langle M \rangle$ . If  $M$  is finite, then we say  $\langle M \rangle$  is **finitely generated**.

From now on, when we use set builder notation, instead of  $\langle \{ x_1, x_2, \dots \in X \mid \dots \} \rangle$  we will omit the parentheses and simply write  $\langle x_1, x_2, \dots \mid \dots \rangle$ .

An element is called a **non-generator** of a group  $G$  if it can be omitted from every generating set for  $G$ .

Generally, this definition of a generated subgroup is not really easy to work with. So equivalently...

### Thm. Equivalent Generation Definition

If  $M$  is a subset of a group  $G$ , then

$$\langle M \rangle = \{ a_1^{\epsilon_1} \cdots a_k^{\epsilon_k} \mid a_i \in M, \epsilon_i = \pm 1, k = 1, 2, \dots \}.$$

### Thm. Equivalent Generation Definition 2

Let  $G$  be a group and  $M \subseteq G$ , then

$$\langle M \rangle = \{ a_1^{n_1} \cdots a_k^{n_k} \mid a_i \in M \text{ and } k, n_i \in \mathbb{Z} \}.$$

That is,  $\langle M \rangle$  consists of all finite products of  $a_1^{n_1} \cdots a_k^{n_k}$ .

Therefore, in particular  $\langle x \rangle = \{ x^n \mid n \in \mathbb{Z} \}$ . We will inspect these structures in detail in the next chapter.

#### ► Proof

## Def. Join of Subgroups

---

Let  $H_i$  be subgroups of  $G$ , then their **join** is defined as  $\langle \bigcup H_i \rangle$  or, if finitely many, as  $\langle H_1, \dots, H_n \rangle$ . The join of two subgroups  $H, K$  will simply be denoted as  $H \vee K$ .

| This notation will make sense later on when we define lattices over groups.

## Example. Generator Examples

---

- $\mathbb{Z} = \langle 1 \rangle,$
- $\mathbb{Z}_n = \langle \bar{1} \rangle,$
- $\mathbb{Q} = \left\langle \frac{1}{n} \mid n = 1, 2, \dots \right\rangle,$
- $\mathbb{Z}^* = \langle -1 \rangle,$
- $\mathbb{Q}^* = \langle -1, 2, 3, 5, 11, \dots \rangle,$

# 6. Cyclic Groups

This section contains important counting theorems (not just for cyclic or abelian groups); hence, it is important to be familiar with every proof in this exercise.

## Def. Cyclic Group

---

A group  $H$  is called **cyclic group**, or simply **cyclic**, if  $H$  can be generated by a single element. That is, there exists an element  $x \in H$  such that  $H = \langle x \rangle = \{ x^n \mid n \in \mathbb{Z} \}$ . Such  $x$  is called the **generator** of  $H$  or  $H$  is **generated by  $x$** .

Since cyclic groups are abelian (exercise), additive notation may also be used. In that case,  $x^n$  becomes  $nx$ .

Notice that the order of the element  $x$  and the group  $\langle x \rangle$  are the same.

## Thm. Basic Element Order Properties

---

Let  $G$  be any group and  $a \in G$ , then

**In the case  $|a|$  is not finite,**

1.  $a^k = e$  if and only if  $k = 0$ ,
2. each  $a^k$  is distinct for  $k \in \mathbb{Z}$ .

**In the case  $|a| = n \in \mathbb{N}^+$ ,**

3.  $n$  is the least positive integer such that  $a^n = e$ ,
4.  $a^k = e$  if and only if  $n \mid k$ ,
5.  $a^r = a^s$  if and only if  $r \equiv_n s$ ,
6. for each  $k \mid n$ , we have  $|a^k| = \frac{n}{k}$ .

Exercise

## Thm. Basic Cyclic Properties

---

Let  $H$  be a cyclic group, then

- $H$  is also abelian. So, cyclic implies abelian!
- If  $x$  is a generator of  $H$ , then so is  $x^{-1}$ .
- If  $x$  is a generator of  $H$ , then  $|H| = |x|$ .

## Thm. Fundamental Order Property

---

Let  $G$  be a group,  $g \in G$ , and  $m, n \in \mathbb{Z}$ . If  $x^m = e$  and  $x^n = e$ , then  $x^d = e$  where  $d = (m, n)$ .

In particular, for any  $m$  such that  $x^m = e$ , we have  $|x|$  divides  $m$ .

► **Proof**

## Thm. Every Subgroup of $\mathbb{Z}$ is Also Cyclic

---

Noting subgroup of a cyclic is cyclic, let  $(H, +) \leq (\mathbb{Z}, +)$ . Then, either

- $H = \langle 0 \rangle$  which is the trivial subgroup  $\{0\}$ , or
- $H = \langle m \rangle$  where  $m$  is the least positive integer in  $H$ . In this case,  $H$  is infinite.

► **Proof**

## Thm. Same Order Cyclics are Isomorphic

---

For any two cyclic groups  $\langle x \rangle$  and  $\langle y \rangle$ , if their orders are the same, there exists an isomorphism  $\varphi : \langle x \rangle \rightarrow \langle y \rangle$ .

1. Indeed, if they are finite, then the map

$$\varphi : \langle x \rangle \rightarrow \langle y \rangle$$

$$x^k \mapsto y^k$$

is well-defined and an isomorphism. Therefore, any finite cyclic group of order  $n$  is isomorphic to the cyclic group  $(\mathbb{Z}_n, +_{\mathbb{Z}})$ .

2. If they are infinite, then the map

$$\varphi : \mathbb{Z} \rightarrow \langle x \rangle$$

$$k \mapsto x^k$$

is well-defined and an isomorphism. Therefore, any infinite cyclic group is isomorphic to  $(\mathbb{Z}, +_{\mathbb{Z}})$ .

► **Proof**

## Thm. Fundamentals of Element Orders

---

Let  $G$  be any group,  $x \in G$  and  $a \in \mathbb{Z}^*$ , then

1. If  $|x| = \infty$ , then  $|x^a| = \infty$ .
2. If  $|x| = n$ , then  $|x^a| = \frac{n}{(n, a)}$ .

## Thm. Orders of Commutative Elements

---

Let  $G$  be a group and  $a$  and  $b$  elements of  $G$  whose orders are respectively  $m$  and  $n$ . If  $a$  and  $b$  commute, then

1.  $(m, n) = 1 \implies |ab| = |a| |b|$ ,
2. There exists  $g \in G$  such that  $|g| = \text{lcm}(m, n)$ .

► **Proof**

## Thm. On Generators of Cyclics

---

Let  $H = \langle x \rangle$ , then

1. If  $H$  is infinite, then  $x$  and  $x^{-1}$  are the only generators of  $H$ .
2. If  $H$  is finite of order  $n$ , then  $x^k$  is a generator of  $H$ , if and only if  $(k, n) = 1$ .

| Therefore, the number of generators of  $H$  equals to  $\varphi(n)$  where  $\varphi$  is Euler's  $\phi$ -function.

## Thm. Basic Cyclic Properties

---

Let  $H = \langle x \rangle$  be cyclic, then

1. Every subgroup of  $H$  is also cyclic.
2. If  $H$  is infinite, then for any distinct non-negative integers  $a$  and  $b$ ,  $\langle x^a \rangle \neq \langle x^b \rangle$ .
3. For every integer  $m$  we have  $\langle x^m \rangle = \langle x^{-m} \rangle$ . Therefore, every non-trivial subgroup of  $H$ ...

## Thm. Homomorphisms from Cyclics

---

Let  $G = \langle a \rangle$  be a cyclic group and  $H$  any group, then every homomorphism  $\varphi : G \rightarrow H$  is completely determined by the element  $\varphi(a) \in H$ . In particular,  $\text{Im } \varphi = \langle \varphi(a) \rangle$ .

| Obvious

## Thm. Finitely Many Subgroups Imply Finite Group

---

Any group which has only finitely many subgroups must also be finite.

► **Proof**

# Exercises

---

## #1

Let  $G$  be a finite group such that it has exactly one maximal subgroup  $M$ , then  $G$  is cyclic.

► **Help**



# 7. Cosets and Indices

## Def. Coset

---

Let  $G$  be a group and  $H \leq G$ . Then, for all  $a \in G$  the set  $aH$  is called a **left coset** and the set  $Ha$  is called a **right coset**.

## Def. Coset Congruence

---

Let  $G$  be a group,  $H \leq G$ , and  $a, b \in G$ . We say,

- $a$  is **left-congruent to  $b$  modulo  $H$** , denoted by  $a \equiv_L b \pmod{H}$  when  $a^{-1}b \in H$ .
- $a$  is **right-congruent to  $b$  modulo  $H$** , denoted by  $a \equiv_R b \pmod{H}$  when  $ab^{-1} \in H$ ,

## Thm. Coset Congruence

---

1. The relations  $\equiv_L$  and  $\equiv_R$  are equivalence relations.
2. The left (resp. right) equivalence class of  $a \in G$  is the set  $aH$  (resp.  $Ha$ ).
3. For all  $a \in G$ , cardinalities of the sets  $Ha$ ,  $H$  and  $aH$  are the same.
4. If  $G$  is abelian, then left and right congruence coincide. Moreover, this is also *possible* if  $G$  is not abelian.

### ► Proof

## Corollary. Coset Congruence

Let  $G$  be a group and  $H \leq G$ . Then

1.  $G$  is the union of right (respectively left) cosets of  $H$ ,
2. Two right (respectively left) cosets are either *disjoint* or *equal*,
3. Number of distinct left cosets are equal to number of distinct right cosets.

## Def. Index

---

### Wiki: Index of a subgroup

Let  $G$  be group and  $H \leq G$  then the **index of  $H$  in  $G$** , denoted  $|G : H|$  is the *cardinal number* of the set of distinct right (or left) cosets of  $H$  in  $G$ .

## Thm. Index Theorem

---

Let  $G$  be a group and  $K \leq H \leq G$ , then

$$|G : K| = |G : H||H : K|$$

### Corollary: Lagrange's Theorem

Let  $G$  be a group and  $H \leq G$ , then the order of  $H$  divides the order of  $G$ . In general, even if  $G$  is infinite

$$|G| = |G : H| \cdot |H|$$

### Corollary: Element Order Divides Group Order

Let  $G$  be a group and  $x \in G$ , then  $|x|$  divides  $|G|$ .

## Thm. Cauchy's Theorem

---

Let  $G$  be a finite group of order  $n$  and  $p$  is any prime that divides  $n$ . Then  $G$  contains an element of order  $p$ .

| We will prove this useful theorem later on, after Sylow Theorems.

## Thm. Order of Subgroup Multiplication

---

Let  $G$  be group such that  $H$  and  $K$  are finite subgroups of  $G$ . Then

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}$$

## Thm. 1

---

Let  $G$  be a group and  $H, K \leq G$ . Then we have  $|H : (H \cap K)| \leq |G : K|$ .

If  $|G : K|$  is finite, then  $|H : (H \cap K)| = |G : K|$  if and only if  $G = KH$ .

## Thm. 2

---

Let  $H$  and  $K$  be subgroups of finite index of a group  $G$ . Then

1.  $|G : H \cap K|$  is finite,
2.  $|G : H \cap K| \leq |G : H||G : K|$ , and
3.  $|G : H \cap K| = |G : H||G : K|$  if and only if  $G = HK$ .

## Exercise

---

Let  $G$  be a group and  $H, K \leq G$  such that indices of  $H$  and  $K$  are relatively prime, then  $G = HK$ .

## Thm. Groups of Prime Order

---

Let  $G$  be a group, then the following are equivalent

1.  $|G|$  is prime,
2.  $G \neq \langle e \rangle$  and  $G$  has no proper subgroups,
3.  $G \cong \mathbb{Z}_p$  for some prime  $p$ .

| Notice that (3) implies that every group of prime order is cyclic.

# 8. Conjugates and Normals

## Def. Conjugate

---

Let  $G$  be a group,  $H \leq G$ , and  $a, b \in G$ , then

1. the element  $aba^{-1}$  is called **the conjugate of  $a$  by  $b$** ,
2. the set  $aHa^{-1}$  is called **the conjugate of  $H$  by  $a$** ,
3. the element  $a$  is said to **normalize  $H$**  if  $aHa^{-1} = H$ .

Note that more general definitions would use only commutativity (that is  $gh = hg$ ) instead of inverses for semigroups.

We also say  $a$  is **conjugate to an element  $b$  by an element  $x$**  if  $a = xbx^{-1}$  denoted with  $a = b^x$ . We further define for sets  $A, B \subseteq G$ , and  $g \in G$

$$\begin{aligned} A^B &:= \{ a^b \mid a \in A, b \in B \} \neq BAB^{-1} \\ A^g &:= gAg^{-1} \end{aligned}$$

Note that  $A^B$  is defined as the set of elements  $bab^{-1}$ , not  $ba(b')^{-1}$  for some  $b'$ .

## Thm. Basic Conjugate Properties

---

Let  $G$  a group and  $a, b, x \in G$ , then

- $(ab)^x = a^xb^x$ ,
- $(a^x)^y = a^{xy}$ ,
- $a = b^x \implies |a| = |b|$ .

## Def. Normal

---

Let  $G$  be a group and  $N$  its subgroup. If for all  $a \in G$  we have  $aN = Na$ , then  $N$  is called a **normal subgroup** (or simply a **normal**) of  $G$  denoted by  $N \trianglelefteq G$ .

If  $N \neq G$ , then  $N \triangleleft G$  will also be used to denote  $N$  is a **proper normal subgroup** of  $G$ .

From now on, it should be understood from  $A \trianglelefteq B$  alone that  $B$  is a group and  $A$  is its normal subgroup.

## Thm. Equivalent Normal Definitions

---

Let  $G$  be a group and  $N \leq G$ . Then the following are equivalent

1.  $\equiv_L$  and  $\equiv_R$  modulo  $N$  coincide,

2.  $gN = Ng$ ,
3.  $N^g = gNg^{-1} \subseteq N$  for all  $g \in G$ , that is  $N^G \subseteq N$ ,
4.  $N^g = gNg^{-1} = N$  for all  $g \in G$ , that is  $N^G = N$ .

## Thm. More Normal Properties

---

1. Let  $M, N \trianglelefteq G$ . If  $M \cap N = \{e\}$ , then  $mn = nm$  for all  $m \in M$  and  $n \in N$ .
2. Kernel of any group homomorphism is a normal subgroup.
3. If  $|G : H| = 2$ , then  $H \trianglelefteq G$ .
4.  $A, B \trianglelefteq G$  implies  $AB \trianglelefteq G$ .
5. Find normal subgroups  $A, B, C$  such that  $A \trianglelefteq B \trianglelefteq C$ , but  $A \not\trianglelefteq C$ .

## Thm. Normal and Subgroup Properties

---

Recall that the "join" of two subgroups  $H, K$  denoted  $H \vee K$  is the subgroup  $\langle H \cup K \rangle$ .

Let  $N \trianglelefteq G$  and  $K \leq G$ , then

1.  $(N \cap K) \trianglelefteq G$ , so intersection of any subgroup with a normal is a normal,
2.  $N \vee K = NK = KN$ , so join of any subgroup with a normal is their product,
3.  $N \trianglelefteq (N \vee K)$ .

TODO: Revise (2) noting that we have defined the multiplication as join! Did we define that?

## Exercises

---

### #1

Let  $N \trianglelefteq G$  and  $xy \in H$ , then  $yx \in H$ .

### #2

Let  $G$  be a group of finite order,  $N \trianglelefteq G$  and  $K \leq G$  such that  $|K|$  is relatively prime to  $|G : H|$ , then  $K \leq H$ .

# 10. Normalizer And Centralizer

## Def. Centralizer

---

Let  $G$  be a (sub)group and  $A$  a non-empty subset of  $G$ . Then the **centralizer of  $A$  in a group  $G$**  is defined as

$$C_G(A) := \{ g \in G \mid a^g = a \quad \forall a \in A \}$$

Beware that if we were to write  $A^g = A$  to the right-hand side it wouldn't be the same definition.

Note that a more general definition would use  $ga = ag$  for semigroups.

## Def. Center

---

The **center** of a (sub)group  $G$  denoted with  $Z(G)$  is defined as  $Z(G) := C_G(G)$ .

It is basically the set of all elements in the group that commute with all other elements in the group.

## Def. Normalizer

---

Let  $G$  be a group and  $A$  a non-empty subset of  $G$ . Similar to centralizer (but not necessarily equivalent), the **normalizer of  $A$  in  $G$**  is defined as

$$N_G(A) := \{ g \in G \mid A^g = A \}$$

and it is also a subgroup of  $G$ .

The definitions of centralizer and normalizer are similar but not identical. If  $g \in C_G(A)$  and  $a \in A$ , then it must be the case that  $a^g = a$ , but if  $g \in N_G(S)$ , then  $a^g = a'$  for some  $a' \in A$ , with  $a'$  possibly different from  $a$ .

Obviously a subgroup is a normal subgroup in a group if and only if its normalizer is the whole group.

This is one reason why the notation  $gag^{-1}$  (or  $a^g$ ) is preferred over  $ga = ag$  — unless we working with semigroups of course.

## Thm. Basic Properties of Normalizer and Centralizer

---

Let  $G$  be a group, then

1.  $Z(G) \trianglelefteq G$

## Thm. '

---

| TODO: Revise, define  $a^G$  etc.

Let  $G$  be a group and  $a \in G$ , then

$$|a^G| = [G : N_G(a)]$$

| You may check out Kargapolov p. 16 for a more general version of theorem and the proof.

## Notation. Normal Generators

---

Let  $H \leq G$ , then

- $H^G$  denotes the intersection all normals in  $G$  that contain  $H$ ,
- $H_G$  denotes  $\langle H^g \mid g \in G \rangle$ .

| join and largest normal subgroup contained in H.

## Thm. Building Normal from a Subgroup

---

Let  $H \leq G$ , then the set

$$N = \bigcap_{g \in G} H^g$$

is a normal subgroup of  $G$ . Moreover,  $N = H_G$ .

| Exercise

## Exercise

---

If  $G$  is not abelian, then  $Z(G)$  is *properly* contained in an abelian subgroup of  $G$ .

► Hint

# 10. Commutators

## Def. Commutator

---

Let  $G$  be a group and  $a, b \in G$ . Obviously, two elements  $a$  and  $b$  commute if and only if  $a^{-1}b^{-1}ab = e$ . The left-hand side of this equation will be denoted with  $[a, b]$  called the **commutator** of  $a$  and  $b$ , that is

$$[a, b] := a^{-1}b^{-1}ab$$

For  $A, B \subseteq G$ , we define **mutual commutator subgroup** as

$$[A, B] := \langle [a, b] \mid a \in A, b \in B \rangle$$

More generally,

$$[a_1, a_2, \dots, a_{n+1}] = [[a_1, \dots, a_n], a_{n+1}]$$

and

$$[A_1, A_2, \dots, A_{n+1}] = [[A_1, \dots, A_n], A_{n+1}]$$

## Thm. Basic Commutator Properties

Let  $G$  be a group and  $a, b, c, x \in G$ . Then

- $[a, b] = e$  if and only if  $ab = ba$ , indeed
- $e$  is the only commutator if and only if  $G$  is abelian,
- $[a, b]^{-1} = [b, a]$ ,
- $[a, b]^x = [a^x, b^x]$ ,
- $[ab, c] = [ac]^b[b, c]$ ,
- $[a^{-1}, b] = [b, a]^{a^{-1}}$ ,
- For any group homomorphism  $\phi : G \rightarrow H$ , we have  $\phi([a, b]) = [\phi(a), \phi(b)]$ .

The product of two or more commutators need not be a commutator. Indeed, it is known that the least order of a finite group for which there exists two commutators whose product is not a commutator is 96; in fact there are two nonisomorphic groups of order 96 with this property — See **Stack Exchange**: Mariano Suárez-Álvarez.

## Def. Commutator Subgroup and Derived Series

---

Let  $G$  be a group. Then the **commutator subgroup** (or **derived subgroup**) of  $G$  denoted with  $G'$  or  $G^{(1)}$  is the normal subgroup  $[G, G]$ .

Applied recursively, we get the **derived series** of the group  $G$

$$G^{(0)} := G \supseteq G' \supseteq G'' \supseteq G^{(3)} \supseteq \dots$$



For a finite group this series terminates, to what is called a **perfect group** which may be trivial or not.

## Thm. Three Commutator Lemma

---

Let  $G$  be a group,  $A, B, C \leq G$ , and  $N \trianglelefteq G$ . If any two commutator subgroups

$$[A, B, C], [B, C, A], [C, A, B]$$

lie in  $N$ , then so is the other one.

► **Proof**

## Exercise

---

Let  $A, B, C \leq G$ , then  $[AB, C] = [A, C][B, C]$ .

# 11. Quotients and Isomorphisms

## Def. (Group) Congruence Relation

---

An equivalence relation  $\equiv$  on a group  $G$  is called a (group) **congruence relation** if for all  $x_1, x_2, y_1, y_2 \in G$

$$x_1 \equiv x_2 \wedge y_1 \equiv y_2 \implies x_1 y_1 \equiv x_2 y_2$$

The product of two congruence classes is again a congruence class. Indeed, the set of all congruence classes  $G/\equiv$  is a group under the multiplication of classes called the **quotient group with respect to  $\equiv$** .

## Thm. Group Congruences and Normals

---

The congruence relations on a group  $G$  are in one-to-one correspondence with the normal subgroups of  $G$ .

Usually quotient groups in group theory are defined via normal groups but this paints a much wider picture. Following this motivation, here is the classical definition of quotient groups.

## Def. Quotient Group

---

Let  $G$  be a group and  $N \trianglelefteq G$ . The set of all cosets of  $N$  in  $G$  denoted by  $G/N$  (read as  $G$  modulo  $N$ ) forms a group under the binary operation

$$(aN)(bN) = (ab)N$$

and is of order  $[G : N]$ . This group is called the **quotient group** (or **factor group**) of  $G$  by  $N$ .

Notice how we are not multiplying cosets directly, but rather the elements in front of them.

## Thm. Basic Quotient Properties

---

Let  $G$  be a group and  $N \trianglelefteq G$ .

1. If  $G$  is cyclic, then so is  $G/N$ .
2.  $G/N$  is abelian if and only if  $[G, G] \subseteq N$ .

Exercise

## Def. Projection

---

Let  $N \trianglelefteq G$ . Then

$$\begin{aligned}\pi : G &\rightarrow G/N \\ a &\mapsto aN\end{aligned}$$

is an epimorphism and  $\text{Ker } \pi = N$ . Such  $\pi$  is called the **canonical epimorphism** or **(natural) projection** of  $G$  under  $N$ . Therefore, unless otherwise stated,  $G \rightarrow G/N$  always denotes the natural projection.

If the group is clear from the context, we may make use of the notation  $\pi_N$  to denote the projection  $G \rightarrow G/N$ .

| Exercise

### Thm. Commutativity of Projection

| TODO: Revise, add proof

Let  $\pi_N$  be the natural projection of  $G$  under  $N$ , then  $G/N$  is abelian if and only if  $[G, G] \subseteq N$ .

► **Proof**

## Thm. Fundamental Theorem on Homomorphisms

---

Let  $\varphi : G \rightarrow H$  be a group homomorphism,  $N \trianglelefteq G$ , and  $N \subseteq \text{Ker } \varphi \trianglelefteq G$ . Then there exists a unique homomorphism  $\bar{\varphi}$  where

$$\begin{aligned}\bar{\varphi} : G/N &\rightarrow H \\ aN &\mapsto \varphi(a)\end{aligned}$$

and

- $\varphi(G) = \bar{\varphi}(G/N)$ ,
- $\text{Ker } \bar{\varphi} = (\text{Ker } \varphi)/N$

Therefore,  $\bar{\varphi}$  is an isomorphism if and only if

- $\varphi$  is an epimorphism, and
- $N = \text{Ker } \varphi$ .

► **Proof**

## Thm. First Isomorphism Theorem

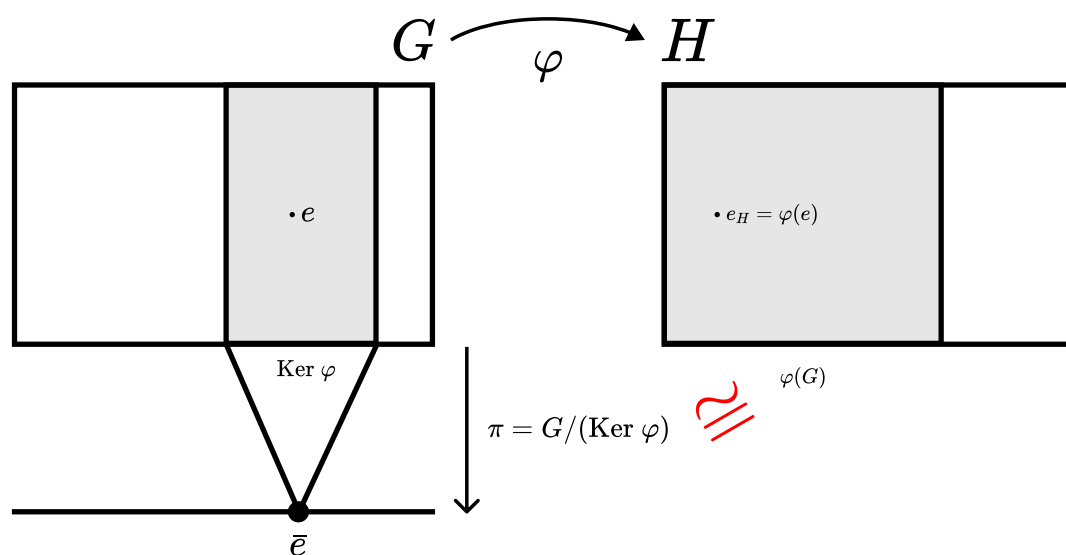
---

Let  $\varphi : G \rightarrow H$  be a group homomorphism. Then

1.  $\text{Ker } \varphi \trianglelefteq G$ , so kernel of any group homomorphism is normal,
2.  $\varphi(G) \leq H$ , so image of any group homomorphism is a subgroup,

3.  $\varphi(G) \cong G/(\text{Ker } \varphi)$ , so if  $\varphi$  is an epimorphism, then  $H \cong G/(\text{Ker } \varphi)$ .

► **Proof**



(Figure 1) First Isomorphism Theorem

## Thm. Second Isomorphism Theorem

This theorem is also called the **Diamond Isomorphism Theorem** or **Parallelogram Theorem** due to lattice it draws.

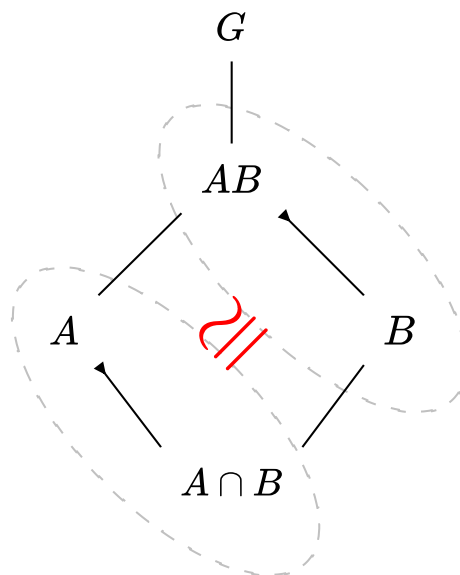
Let  $G$  be a group,  $H \leq G$ , and  $N \trianglelefteq G$ . Then

Recall that since  $N$  is normal and  $H$  is a subgroup, we have  $H \vee N = HN = NH$ .

1.  $N \trianglelefteq HN \leq G$ ,
2.  $H \cap N \trianglelefteq H$ , and
3.  $HN/N \cong H/(H \cap N)$ .

TODO: (Examine) Technically,  $N$  need not to be normal in  $G$ , it suffices  $H$  to be a subgroup of  $N_G(N)$ .

► **Proof**



**(Figure 2)** Second Isomorphism Theorem

TODO: Redraw diagram

## Thm. Third Isomorphism Theorem

---

Let  $K \trianglelefteq H \trianglelefteq G$ , then

1.  $H/K \trianglelefteq G/K$ , and
2.  $(G/K)/(H/K) \cong G/H$ .

► **Proof**

## Thm. Homomorphism Induced Bijection

---

Recall that  $L(G, A)$  was the set of all subgroups of  $G$  which contain the subset  $A$ , and  $L(G) := L(G, e)$ .

Let  $\varphi : G \rightarrow H$  be a group homomorphism. Then  $\varphi$  induces a bijective map

$$\psi : L(G, \text{Ker } \varphi) \rightarrow L(H)$$

such that image of normal subgroups are normal subgroups.

TODO: Proof, omitted.

## Corollary. Normal Subgroups of Quotients

---

Let  $N \trianglelefteq G$ , then every subgroup of  $G/N$  is of the form  $K/N$  where  $N \subseteq K \leq G$ . Moreover,  $K/N \trianglelefteq G/N$  if and only if  $K \trianglelefteq G$ .

## ► Sketch of Proof

## Def. Inner and Outer Automorphisms

---

Let  $G$  be a group,  $a \in G$ , and  $\iota_a : G \rightarrow G$  be a map such that  $x \mapsto x^a$ , then  $\iota_a$  is an automorphism on  $G$  called an **inner automorphism**. Moreover, the **set of all inner automorphism** on  $G$  denoted by  $\text{Inn } G$  is a normal subgroup of  $\text{Aut } G$ .

An automorphism which is not inner is called an **outer automorphism**. Noting  $\text{Inn } G$  is normal, we define the **outer automorphism group** as

$$\text{Out } G := \text{Aut } G / \text{Inn } G$$

## Thm. Inner Automorphisms

---

Let  $G$  be a group, then

$$\text{Inn } G \cong G/C(G)$$

## ► Proof

## Def.

---

## Thm. Equivalent Normal Definition

---

Let  $H \leq G$ , then  $H$  is normal if and only if for all  $\phi \in \text{Inn } G$  we have  $\phi(H) \leq G$ .

| Exercise

# 12. Endomorphisms

## Def. Inner and Outer Automorphisms

---

Let  $G$  be a group,  $a \in G$ , and  $\iota_a : G \rightarrow G$  be a map such that  $x \mapsto x^a$ , then  $\iota_a$  is an automorphism on  $G$  called an **inner automorphism**. Moreover, the **set of all inner automorphism** on  $G$  denoted by  $\text{Inn } G$  is a normal subgroup of  $\text{Aut } G$ .

An automorphism which is not inner is called an **outer automorphism**. Noting  $\text{Inn } G$  is normal, we define the **outer automorphism group** as

$$\text{Out } G := \text{Aut } G / \text{Inn } G$$

## Thm. Inner Automorphisms

---

Let  $G$  be a group, then

$$\text{Inn } G \cong G/C(G)$$

► **Proof**

## Def. Endomorphic Invariance

---

Let  $H \leq G$  and  $\Phi \subseteq \text{End } G$ . We say  $H$  is  **$\Phi$ -invariant** or **invariant with respect to  $\Phi$**  if for all  $\phi \in \Phi$

$$\phi(H) \leq H$$

Noting that  $\langle e \rangle$  and  $G$  is invariant with respect to any arbitrary  $\Phi$ , we say the group is  **$\Phi$ -simple** if it contains no other  $\Phi$ -invariants than these two.

## Thm. Equivalent Normal Definition

---

Let  $H \leq G$ , then  $H$  is normal if and only if  $H$  is invariant with respect to  $\text{Inn } G$ .

| Exercise

## Notation. Invariance

---

Let  $H \leq G$ , then we respectively denote  $\text{End } G$ ,  $\text{Aut } G$ , and  $\text{Inn } G$  with

- $\leq_E$  or  $\leq_{\text{End}}$ ,
- $\leq_A$  or  $\leq_{\text{Aut}}$ ,

- $\leq_I$  or  $\leq_{\text{Inn}}$  which is equivalent to  $\trianglelefteq$  as shown above.

## Thm. Invariance Transitivity

---

The relations  $\leq_{\text{End}}$  and  $\leq_{\text{Aut}}$  are transitive.

| Exercise

## Def. Characteristic Subgroup

---

Let  $H \leq G$ , then we say  $H$  is a **characteristic subgroup** of  $G$  if  $H$  is invariant with respect to  $\text{Aut } G$ , that is  $H \leq_{\text{Aut}} G$ .

## Thm. Characteristic Normality

---

Let  $H$  be a characteristic subgroup of  $G$ , then  $H$  is normal in the whole group, that is  $A \trianglelefteq N$  for all  $N \trianglelefteq G$ .

| Exercise

## Def. Complete Group

---

A group  $G$  is called **complete** if it has trivial center and  $\text{Aut } G = \text{Inn } G$ . Therefore,

$$\text{Aut } G \cong G$$

## Exercises

---

### #1

The center  $Z$  of a group  $G$  is always characteristic.

### #2

The Frattini subgroup of any group is characteristic.



# 13. Symmetric Groups

## Def. Permutation

---

A **permutation**  $\sigma$  on a set  $X$  is a bijective function from  $X$  to  $X$ . The permutation  $x \mapsto x$  will be called the **identity permutation**.

We say an element  $x \in X$  is **fixed under**  $\sigma$  if  $\sigma(x) = x$ . Similarly, we say  $x$  is **moved by**  $\sigma$  if  $\sigma(x) \neq x$ .

For simplicity, we will use the set  $\mathbf{I}_n = \{ 1, 2, \dots, n \}$  instead of any  $X$  of any cardinality.

More formally, we could make use of Well-Ordering Principle, initial segments, and ordinals. For now, this definition should suffice.

## Def. Support

---

The **support** of a permutation  $\sigma$  denoted by  $\text{supp } \sigma$  is defined as the set of elements that are moved by  $\sigma$ , that is

$$\text{supp } \sigma := \{ i \in \mathbf{I}_n \mid \sigma(i) \neq i \}.$$

Similarly, the set of fixed elements denoted with  $\text{fix } \sigma$  is the set

$$\text{fix } \sigma := \{ i \in \mathbf{I}_n \mid \sigma(i) = i \}.$$

## Def. Disjoint Permutations

---

The permutations  $\sigma_1, \sigma_2, \dots, \sigma_n$  are said to be **disjoint** if their support is disjoint.

## Def. Cycle

---

Let  $\tau$  be a permutation on  $\mathbf{I}_n$  with the support  $\{ k_1, k_2, \dots, k_r \}$ . Then  $\tau$  is said to be a **cycle** (or **cyclic**) of **length**  $r$  if

$$\begin{array}{ll} k_1 & \mapsto k_2 \\ k_2 & \mapsto k_3 \\ & \vdots \\ k_r & \mapsto k_1 \end{array}$$

denoted with  $(k_1 k_2 \cdots k_r)$ .

A cycle of length  $r$  will be called a  **$r$ -cycle**. A 2-cycle is called a **transposition**.

There is no widespread consensus on how to explicitly define a cycle, but the intuition should be clear.

## Def. Symmetric Group

---

Set of all permutations (bijections) on  $\mathbf{I}_n$  will be denoted with  $\mathbf{S}_n$  and it forms a group under function composition (exercise) called the **symmetric group** (of  $n$  letters).

| Notice that  $\mathbf{S}_n$  is of order  $n!$ .

## Thm. Permutations are (Unique) Product of Disjoint Cycles

---

Every non-identity permutation in  $\mathbf{S}_n$  is uniquely (up to the order of the factors) a product of disjoint cycles, each of which has length at least 2.

### Corollary. Order of Permutation

The order of a permutation is the least common multiple of the orders of its disjoint cycles.

### Corollary. Permutations are a Product of Transpositions

Every permutation can be written as a product of (not necessarily unique) transpositions.

## Def. Odd and Even

---

A permutation is said to be **even** (resp. **odd**) if it can be written as a product of even (resp. **odd**) number of transpositions.

## Thm. Exclusively Odd or Even

---

A permutation  $\sigma \in \mathbf{S}_n$  where  $n \geq 2$  is either even or odd, but not both.

Therefore, the **sign** of a permutation  $\sigma$  denoted  $\text{sgn } \sigma$  is defined to be 1 if even and  $-1$  if odd.

## Thm. Alternating Group

---

Let  $\mathbf{A}_n$  denote the set of all permutations of  $\mathbf{S}_n$ . Then  $\mathbf{A}_n$  is a normal subgroup of  $\mathbf{S}_n$  of index 2. Moreover,  $\mathbf{A}_n$  is the only subgroup of  $\mathbf{S}_n$  of index 2.

$\mathbf{A}_n$  is called the **alternating group** (of **degree**  $n$ ).

## Thm. $\mathbf{A}_n$ is (Generally) Simple

---

The alternating group  $\mathbf{A}_n$  is simple if and only if  $n \neq 4$ .

## Lemma. 1

Let  $r, s \in \mathbf{S}_n$  where  $n \geq 3$ . Then  $A_n$  is generated by 3-cycles such that

$$\{ (rsk) \mid 1 \leq k \leq n, k \neq r, s \}$$

## Lemma. 2

For  $n \geq 3$ , if  $N \trianglelefteq A_n$  and  $N$  contains a 3-cycle, then  $N = A_n$ .

| Proofs are skipped for this theorem, curious reader may checkout Hungerford (pp. 49-50).

## Thm. Hölder

---

The symmetric group  $\mathbf{S}_n$  is complete if  $n \neq 2, 6$ .

| Check out Kargapolov pp. 43-44 for the partial proof.

## Thm. Dihedral Group Generators

---

Let  $n \geq 3$ , then the dihedral group  $\mathbf{D}_n$  (which is of order is  $2n$ ) is a group whose generators  $a$  and  $b$  satisfy

1.  $a^n = b^2 = e$  and  $a^k \neq e$  if  $0 < k < n$ ,
2.  $aba = b$ .

Moreover, for  $n \geq 3$ , any group  $G$  which is generated by  $a$  and  $b$  that satisfy (1) and (2) is isomorphic to  $\mathbf{D}_n$ .

► **Proof**

## Exercise. Generator of $\mathbf{D}_n$

---

Let  $\langle a \rangle \leq \mathbf{D}_n$  for  $a \in \mathbf{D}_n$ , and  $|a| = n$ . Then

1.  $\langle a \rangle \trianglelefteq \mathbf{D}_n$ , and
2.  $\mathbf{D}_n / \langle a \rangle = \mathbb{Z}_2$ .

## Thm. Center of $\mathbf{D}_n$

---

Let  $Z$  be the center of the group  $\mathbf{D}_n$ , then

- $Z = \langle e \rangle$  if  $n$  is odd,
- $Z \cong \mathbb{Z}_2$  if  $n$  is even.

► **Proof**

# 14. Direct Products and Sums

Note that the letter  $I$  denotes any index set which is mostly taken to be  $\mathbb{N}$  or non-empty initial segment of  $\mathbb{N}$ .

## Def. Direct Product (of Groups)

---

This is equivalent to the formal definition of set of tuples from the axiomatic set theory, but for the family of groups instead of family of sets.

Let  $\{G_i\}$  be a family of groups indexed by a non-empty set  $I$ , then the **direct product (or complete direct sum)** of the groups  $G_i$  denoted with  $\prod_{i \in I} G_i$  is the set of all functions

$$f : I \rightarrow \bigcup_{i \in I} G_i$$

such that  $f(i) \in G_i$ . Notice that since each  $G_i$  is a group, thus non-empty, we have  $\prod G_i \neq \emptyset$ .

As a mental image, think of  $\prod G_i$  as the set of all (ordered) tuples where each  $i$ -th element belongs to  $G_i$  so that each  $f \in \prod G_i$  represent a tuple in that set.

## Def. Natural Projections

---

Let  $\{G_i\}$  be a non-empty family of groups, then  $\prod G_i$  is a group under component-wise multiplication and for each  $k \in I$ , the map

$$\begin{aligned} \pi_k : \prod G_i &\rightarrow G_k \\ f &\mapsto f(k) \end{aligned}$$

called the **(natural) projection(s)** of the direct product is an epimorphism of groups.

Exercise

## Def. (External) Weak Direct Product

---

Let  $\{G_i\}$  be a non-empty family of groups, then the **(external) weak direct product** of the groups  $G_i$  denoted with  $\prod^w G_i$  is the set of all  $f \in \prod G_i$  such that  $f(i) = e_i$  for all but a finite number of  $i \in I$ .

That is, non-identity elements of the tuple  $f$  are finite. Tuple consists of "mostly" identity elements.

Notice that if  $I$  is finite, then every direct product is a weak direct product.

Moreover, if each  $G_i$  is additive (that is abelian)  $\prod^w G_i$  is called the **(external) direct sum** denoted with  $\sum G_i$ .

## Thm. Normals and Injections

---

Let  $\{ G_i \}$  be a family of non-empty groups, then

1.  $\prod^w G_i \trianglelefteq \prod G_i$ ,
2. for each  $k \in I$ , the map

$$\begin{aligned} i_k : G_k &\rightarrow \prod^w G_i \\ a &\mapsto f = (e_1, \dots, e_{k-1}, a, e_{k+1}, \dots) \end{aligned}$$

is a monomorphism of groups,

3. for each  $k \in I$ , we have  $i_k(G_k) \trianglelefteq \prod G_i$ .

| Exercise

## Thm. Direct Sum and Family of Homomorphisms

---

Let  $\{ A_i \}$  be a non-empty family of abelian groups, and  $B$  an abelian group. If  $\{ \varphi_i : A_i \rightarrow B \}$  is a family of homomorphisms (with the same index set), then there exists a unique homomorphism

$$\varphi : \sum A_i \rightarrow B$$

such that  $\varphi \circ i_k = \varphi_k$  for all  $k \in I$ . This property determines  $\sum A_i$  uniquely up to isomorphism.

| This theorem is false if the groups are not abelian.

## Thm. Direct Sum of Normals

---

Let  $\{ N_i \}$  be a non-empty family of normal subgroups of a group  $G$  such that

- $G = \langle \bigcup N_i \rangle$ , and
- for each  $k \in K$ , we have  $N_k \cap \langle \bigcup_{i \neq k} N_i \rangle = \langle e \rangle$ .

Then

$$G \cong \prod^w N_i$$

and  $\{ N_i \}$  is called a **normal decomposition** of  $G$ .

## Def. Internal Product

---

Let  $\{ G_i \}$  be a non-empty family of groups and  $\prod G_i = G$ . If  $\{ G_i \}$  is a normal decomposition of  $G$ , then  $G = \prod G_i$  is said to be the **internal weak direct product** (or **internal direct sum** if  $G$  is abelian).

## Thm. Normal Decomposition Condition

---

Let  $\{ N_i \}$  be a non-empty family of normal subgroups of  $G$ . Then,  $\{ N_i \}$  is a normal decomposition of  $G$  if and only if for each non-identity  $g \in G$  is the unique product

$$g = a_{i_1} a_{i_2} \cdots a_{i_n}$$

where each  $i_k \in I$  is distinct and  $e \neq a_{i_k} \in N_{i_k}$  for each  $k = 1, 2, \dots, n$ .

| Exercise

## Thm. Internal Direct Sum and Family of Homomorphisms

---

Let  $\{ \varphi_i : G_i \rightarrow H_i \}$  be a family of homomorphism of groups and let

$$\begin{aligned} \varphi : \prod G_i &\rightarrow \prod H_i \\ (a_i) &\mapsto (\varphi_i(a_i)) \end{aligned}$$

Then  $\varphi$  is a homomorphism of groups such that

$$\varphi \left( \prod^w G_i \right) \subseteq \prod^w H_i$$

and

$$\text{Ker } \varphi = \prod \text{Ker } \varphi_i$$

and

$$\text{Im } \varphi = \prod \text{Im } \varphi_i$$

Moreover,  $\varphi$  is a monomorphism (resp. epimorphism) if each  $\varphi_i$  is.

## Corollary. Normals and Quotients

---

Let  $\{ G_i \}$  be a non-empty family of groups and  $\{ N_i \}$  be a non-empty family of normal subgroups (of same index) such that  $N_i \trianglelefteq G_i$  for all  $i \in I$ . Then

1.  $\prod N_i \trianglelefteq \prod G_i$  and  $(\prod G_i)/(\prod N_i) \cong \prod (G_i/N_i)$ ,
2.  $\prod^w N_i \trianglelefteq \prod^w G_i$  and  $(\prod^w G_i)/(\prod^w N_i) \cong \prod^w (G_i/N_i)$

| Exercise, use First Isomorphism Theorem.

# 15. Free Groups

In this section, we will resort to rather a constructive approach to define free groups.

## Def. Free Generator

---

We say  $S$  is a **free generator** if for each  $s \in S$  there exists a corresponding distinct  $s^{-1} \in S^{-1}$  called the **inverse** of  $s$  such that  $S$  and  $S^{-1}$  are disjoint and  $|S| = |S^{-1}|$ . Moreover, the **identity**  $\epsilon$  of  $S$  is an element such that  $\epsilon \notin S \cup S^{-1}$  whose inverse is itself.

We could have defined the free generator  $S$  more formally with tuples and bijective functions, but the notation becomes very cumbersome very quickly. Intuition and the way to formalize it should be clear.

## Def. Word

---

Let  $S$  be a **free generator**, then a **word** on  $S$  is a countably finite sequence  $(a_1, a_2, \dots)$ , indexed by  $\mathbb{N}^+$ , where

- $a_i \in S \cup S^{-1} \cup \{\epsilon\}$  for each  $i \in \mathbb{N}^+$ , and
- for some  $n \in \mathbb{N}^+$  we have  $a_k = \epsilon$  for all  $k \geq n$ .

The constant sequence  $(\epsilon, \epsilon, \dots)$  is called the **empty word** and denoted with  $1$ .

A word  $w = (a_1, a_2, \dots)$  is said to be **reduced** if

1.  $a_i = x \implies a_{i+1} \neq x^{-1}$  for all  $i \in \mathbb{N}^+$  and  $x \in S \cup S^{-1}$ , that is there are no adjacent inverses (other than  $\epsilon$ ),
2.  $a_k = \epsilon \implies a_i = \epsilon$  for all  $i \geq k$ , that is any identity is followed by an identity.

In particular, every non-empty reduced word is of the form, for some  $n \in \mathbb{N}^+$

$$(x_1^{\lambda_1}, x_2^{\lambda_2}, \dots, x_n^{\lambda_n}, \epsilon, \epsilon, \dots)$$

where  $x_i \in X$  and  $\lambda_i = \pm 1$ . From now on we will omit the parentheses.

Notice that the empty word is reduced and  $x^1 := x$ . Reduction algorithm should be obvious.

This is a rather formal definition of a word, simply put a word on  $X$  is a finite product of elements  $X \cup X^{-1}$  such that inverses cancel each other out where  $\epsilon$  is the identity. Now, we should define the binary multiplication on (reduced) words themselves to make it a group.

## Def. Free Group

---

Let non-empty  $X$  be a free generator, and let  $\mathbf{F}(X)$  be the **set of all reduced words** on  $X$ , then  $\mathbf{F}(X)$  is a group under the binary operation where  $xy$  is the *reduced concatenation* for all  $x, y \in \mathbf{F}(X)$ . The group  $\mathbf{F}(X)$  is called the **free group on the set**  $X$  denoted by  $\langle X \rangle$ .

For a more formal definition check out Hungerford pp. 64-65

Do not mistake  $\langle \cdot \rangle$  here with the notation of cyclic groups or generators.

## Thm. Universal Property

---

Let  $X$  be a set,  $\langle X \rangle$  the free group generated by  $X$ , and  $i : X \rightarrow \langle X \rangle$  an inclusion map. For  $G$  a group and  $\varphi : X \rightarrow G$  a map of sets (a map without any extra structure), there exists an *unique* homomorphism of groups  $\bar{\varphi} : \langle X \rangle \rightarrow G$  such that  $\bar{\varphi} \circ i = \varphi$ .

### ► Proof

### Corollary

Every group  $G$  is the homomorphic image of a free group  $F$ . In particular,  $G$  is isomorphic to the quotient group  $F/\text{Ker } \bar{\varphi}$ .

## Def. Presentation

---

Let  $Y \subseteq \langle X \rangle$ , then a group  $G$  is said to be **defined** by the **generators**  $x \in X$  and **relations**  $w \in Y$  provided that  $N \trianglelefteq \langle X \rangle$  is generated by  $Y$ . Noting that  $G \cong \langle X \rangle / N$ , we say  $\langle X \mid Y \rangle$  is a **presentation** of  $G$ .

Moreover, instead of  $\langle X \mid Y \rangle$ , we may write  $\langle X \mid w_1 = 1, w_2 = 1, \dots \rangle$  for brevity, or even more compactly  $\langle X \mid w_1, w_2, \dots \rangle$

We have previously shown such defined group exists and it is the largest possible group in that sense.

### Example

$\langle a, b \mid a^n = 1 (n \geq 3), b^2 = 1, abab = 1 \rangle$  is a presentation for the dihedral group  $D_n$ .

## Thm. Van Dyck

---

Let  $G = \langle X \mid Y \rangle$  and  $H = \langle X \rangle$  such that  $H$  satisfies all the relations  $w = 1$  where  $w \in Y$ , then there is an epimorphism  $\psi : G \rightarrow H$ .

### ► Proof

## Def. Free Product

---

TODO



# Exercises

---

## Exercise 1

Every non-identity element in a free group  $F$  has infinite order.

## Exercise 2

Show that  $\langle a \rangle \cong \mathbb{Z}$  where  $\langle a \rangle$  is the free group generated by  $\{a\}$ .

# 16. Free Abelian Groups

| In this section we will use additive notation rather than our usual multiplicative notation.

## Def. Basis

---

Noting that the subgroup  $\langle X \rangle$  generated by  $X$  in additive notation consists of all **linear combinations**

$$n_1x_1 + n_2x_2 + \cdots + n_kx_k$$

where  $n_i \in \mathbb{Z}$  and  $x_i \in X$ .

A **basis** of an abelian group  $F$  is a subset  $X$  of  $F$  such that

- $F = \langle X \rangle$ , and
- for distinct  $x_1, \dots, x_n \in X$  and  $n_i \in \mathbb{Z}$  we have

$$n_1x_1 + \cdots + n_kx_k = 0 \implies n_i = 0 \quad \forall i$$

## Thm. Equivalent Basis Conditions

---

Let  $F$  be an abelian group, then the following are equivalent

1.  $F$  has a non-empty basis,
2.  $F$  is the (internal) direct sum of a family of infinite cyclic subgroups,
3.  $F$  is (isomorphic to) a direct sum of copies of  $(\mathbb{Z}, +)$ ,

► **Proof**

## Def. Free Abelian Group

---

Let  $F$  be an abelian group, then it is called a **free abelian group** if it has a non-empty basis.

## Thm. Basis Cardinality

---

Any two bases of a free abelian group  $F$  have the same cardinality called the **rank** of  $F$ .

► **Proof**

## Thm. Isomorphism on Free Abelian Groups

---

Two free abelian groups are isomorphic if and only if they have the same rank.

► **Proof**

## Thm. Free Abelian Groups and Abelian Groups

---

Every abelian group  $G$  is the homomorphic image of a free abelian group of rank  $|X|$  where  $X$  is a set of generators of  $G$ .

► **Proof**

## Thm. Basis for Subgroups

---

Let  $F$  be a free abelian group of finite rank  $n$  with the basis  $\{x_1, \dots, x_n\}$  and  $G$  its non-zero subgroup, then there exists an integer  $r \leq n$  and positive integers  $d_1, \dots, d_r$  such that  $d_1 \mid d_2 \mid \dots \mid d_r$  where  $G$  is free abelian with the basis  $\{d_1x_1, \dots, d_rx_r\}$ .

► **Proof**

### Corollary. Rank of Subgroups

Let  $G$  be a finitely generated abelian group generated by  $n$  elements, then every subgroup  $H$  of  $G$  is generated by  $m$  elements where  $m \leq n$ .

| This corollary is false if abelian is omitted.

# 17. Automorphic Extensions

## Def. (Outer) Semidirect Product

---

Let  $G$  and  $H$  be groups and  $\theta : H \rightarrow \text{Aut } G$  a homomorphism. Let  $G \rtimes_{\theta} H$  be the set  $G \times H$  with the binary operation

$$(g, h)(g', h') = (g[\theta(h)(g')], hh')$$

So that  $G \rtimes_{\theta} H$  is group with the identity  $(e_G, e_H)$  and

$$(g, h)^{-1} = (\theta(h^{-1})(g^{-1}), h^{-1})$$

$G \rtimes_{\theta} H$  is called the **(outer) semidirect product** of  $G$  and  $H$  with respect to  $\theta$ .

## Thm. Normal Complement

---

Let  $N \trianglelefteq G$ , then the following are equivalent

1.  $G = NH$  and  $N \cap H = \{e\}$  for some  $H \leq G$ .
2. For each  $g \in G$ , there are unique  $n \in N$  and  $h \in H$  such that  $g = nh$ .

## Def. Inner Semidirect Product

---

Let  $N \trianglelefteq G$  be a complement of  $H \leq G$  in  $G$ , then define  $\varphi : H \rightarrow \text{Aut } N$ . Then,  $\varphi$  is an inner automorphism given by

$$\varphi_h(n) = hnh^{-1}$$

for some  $h \in H$ .

The semidirect product  $N \rtimes_{\varphi} H$  denoted by  $N \rtimes H$  or  $H \ltimes N$  is called the **inner semidirect product** of  $N$  and  $H$ , so that  $G = N \rtimes H$ . We also say  $G$  is a **semidirect product** of  $H$  acting on  $N$ .

## Def. Wreath Product

---

Let  $G$  and  $H$  be groups,

# A1. Appendix 1

This is not really an appendix, but rather parking space for stuff I wasn't able to locate yet.

## Def. Semidirect Product etc.

---

See: [https://en.wikipedia.org/wiki/Semidirect\\_product](https://en.wikipedia.org/wiki/Semidirect_product)

## Def. Diagonal Subgroup

---

$$\hat{G} := \{ (g, g) \} \cong G.$$

---

$$G^n := \langle x^n \mid x \in G \rangle$$
$$G_n := \langle x \mid x \in G, x^n = 1 \rangle$$

---

## Def. Simple Group

---

A group is said to be **simple** if it has no proper normal subgroups.

## Thm. On Simple Groups

---

1.  $\mathbb{Z}_p$  is simple if  $p$  is prime. Does the converse holds?
- 

## Def. Perfect Group

---

---

## Thm. Dedekind Modular Law (Identity)

---

See <https://math.stackexchange.com/questions/3957388/intuition-behind-dedekinds-modular-law>

## Exercises

---

### U 2.39

If  $H \leq G$ , then  $G \setminus H$  is finite if and only if  $G$  finite or  $H = G$ .



# A2. Group Actions

## Def. Group Action

---

TODO: Create a new section for this and populate it with stabilizers, orbits etc.

See **Wikipedia: Group action**.

Let  $G$  be a group and  $X$  any set. A binary operation  $\bullet : G \times X \rightarrow X$  is called a **(left) group action** if, for all  $a, b \in G$  and  $x \in X$ :

- $a \bullet (b \bullet x) = (ab) \bullet x$ , and
- $e \bullet x = x$

For establishing general properties of group actions, it suffices to consider only left actions. (TODO: Why)