Table of Contents

0. Preliminaries

Resources Used

- **Fundamentals of the Theory of Groups**, translated second Russian Ed., by M.I. Kargapolov and Ju.I. Merzljakov
- **Algebra** by Thomas W. Hungerford
- **Abstract Algebra**, 3rd Ed., by David S. Dummit and Richard M. Foote

Notation

- $0 \in \mathbb{N}$ and $\mathbb{N}^* := \mathbb{N} \setminus \{0\}$.
- (m, n) denotes the **greatest common divisor** of $m, n \in \mathbb{N}$.

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 identiy $(G, \cdot, e)$ 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 *Monoid* Properties

If $(M, \cdot)$ 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 $(S, \cdot)$ 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.

Thm. Generalized Associative Law

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

▶ **Proof**

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

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, $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$.

▶ **Proof**

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 if **torsion-free** if every nonidentity 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. 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.
2. If $|G|$ is finite and even, then it has an element of order 2.

▶ **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.

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

Exercise 1

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

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

▶ **Answer**

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) $\varphi : G \to H$ 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 $\varphi : G \to H$ 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.

▶ **Proof**

Def. Group Action

See **Wikipedia: Group action**.

Let $(G, \cdot, e)$ be a group and X a set. A binary operation $\bullet : G \times X \to X$ 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.

3. Homomorphisms

Def. Homomorphism

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

The (total) function (or map) $\varphi : G \to H$ 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 φ 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 $\varphi : G \to H$ is a group homomorphism, then the **kernel** of φ is the set

$$\{\, g \in G \mid \varphi(g) = e_H \,\}$$

denoted by $\operatorname{Ker} \varphi$.

> This is also sometimes denoted by $\varphi^{-1}(e_H)$.

Notation. Homomorphisms

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

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

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

> $\phi(A)$ is sometimes also denoted with $\text{Im } A$ — we will not prefer this notation.

Thm. Basic Homomorphism Properties

Let $\varphi : G \to H$ 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. $\varphi(G) \leq H$

Def. Basic Kernel Properties

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

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

Thm. More Homomorphism Properies

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

▶ **Proof**

Def. Group Action

See **Wikipedia: Group action**.

Let G be a group and X any set. A binary operation $\bullet : G \times X \to X$ 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.

4. Subgroups

> Until now we have explicitly defined and shown which multiplication is which operator and which identity belongs 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.

Equivalently, a subset $H \subseteq G$ of a group G is called a **subgroup** if

- H has the same identity as G,
- For all $a, b \in H$, we have $ab \in H$,
- Every element $h \in H$ has an inverse.

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, $\mathbb{C}_p^* < \mathbb{C}_{p^2} < \cdots < \mathbb{C}_{p^\infty}$,
- $\mathbb{C}_{p^\infty} = \bigcup \mathbb{C}_{p^n}$,
- $\mathbf{GF}(p^m)^* \leq \mathbf{GF}(p^n)^*$ 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.

▶ **Proof**

Thm. Intersection of Subgroups

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

▶ **Proof**

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 group if and only if $HK = KH$, and
- If A, B are finite subgroups of a group G, then

$$|AB| = \frac{|A| \cdot |B|}{|A \cap B|}$$

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**.

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**

Notation. Generators

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

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 $\langle H_1, ..., H_n \rangle$. The join of two subgroups H, K will simply be denoted as $H \vee K$.

> This should make sense later on when we define lattices over groups. But the notation $H \vee K$ will sometimes be used to denote $\langle H \cup K \rangle$.

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 **cylic**, 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 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 $\varphi : \langle x\rangle \to \langle y\rangle$.

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

$$\varphi: \quad \langle x\rangle \to \langle y\rangle$$

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

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

2. If they are infinite, then the map

$$\varphi: \quad \mathbb{Z} \to \langle x\rangle$$

$$k \mapsto x^k$$

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

▶ **Proof**

Thm. More Group Properties

Let G be a group (not necessarily cyclic), $x \in G$ and $a \in \mathbb{Z} \setminus \{0\}$, then

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

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 φ is Euler's ϕ-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, evey non-trivial subgroup of H...

Def. Locally Cyclic

A group G is said to be **locally cyclic** if every finitely generated subgroup is cyclic.

Thm. Finite Subgroups Imply Finite Group

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

▶ **Proof**

7. Cosets and Index

Def. Coset

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

Def. Coset Congruence

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

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

Thm. Coset Congruence

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

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 $g \in G$, then $|x|$ divides $|G|$.

Corollary: Group of Prime Order is Cyclic

Let G be a group of prime order p. Then G is cyclic, therefore $G \cong \mathbb{Z}_p$.

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 $G = HK$.

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 $g \in G$

$$\begin{array}{lll} A^B & := & \left\{ a^b \,\middle|\, a \in A, b \in B \right\} \neq BAB^{-1} \\ A^g & := & gAg^{-1} \end{array}$$

> Notice 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

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

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. Basic Normal Properties

> Recall that the "join" of two subgroup 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. $N \trianglelefteq (N \vee K)$.

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.

9. Special Subgroups

Def. Simple Group

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

Def. Centralizer

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

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

and it is a subgroup of G.

> Beware that if we were to write $A^g = A$ to 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 that commute with all other elements.

Def. Normalizer

Let G be a (sub)group and A a non-empty subset of G. Similar to centralizer (but not 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 $a^g = s$, but if $g \in N_G(S)$, then $a^g = a'$ for some $a' \in A$, with a' possibly different from s.

> 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. Centralizer, Normalizer and Normals

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.

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,

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

and

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

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 $\phi : G \to H$, 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

$$G^{(0)} := G \trianglerighteq G^{'} \trianglerighteq G^{''} \trianglerighteq G^{(3)} \trianglerighteq \cdots$$

> 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

$$[A, B, C], \quad [B, C, A], \quad [C, A, B]$$

lie in N, then so is the other one.

▸ **Proof**

10. Quotients and Isomorphisms

Def. Quotient Group

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

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

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

Thm. Basic Quotient Properties

Let G be a group and $N \trianglelefteq G$. If G is cyclic, then so is G/H.

▶ **Proof**

Def. Projection

Let $N \trianglelefteq G$. Then

$$\begin{array}{cccc} \pi : & G & \to & G/N \\ & a & \mapsto & aN \end{array}$$

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

▶ **Proof**

Thm. Commutativity of Projection

Let $\pi : G \to G/H$ be the natural projection of G and $N\ (\trianglelefteq G)$. Then G/H is abelian if and only if $[G, G] \subseteq H$.

▶ **Proof**

Thm. Fundamental Theorem on Homomorphisms

Let $\varphi : G \to H$ be a group homomorphism and $N \trianglelefteq \mathrm{Ker}\ \varphi \trianglelefteq G$. Then there exists an unique homomorphism $\bar{\varphi}$ where

$$\begin{array}{rrcl} \bar{\varphi}: & G/N & \to & H \\ & aN & \mapsto & \varphi(a) \end{array}$$

and

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

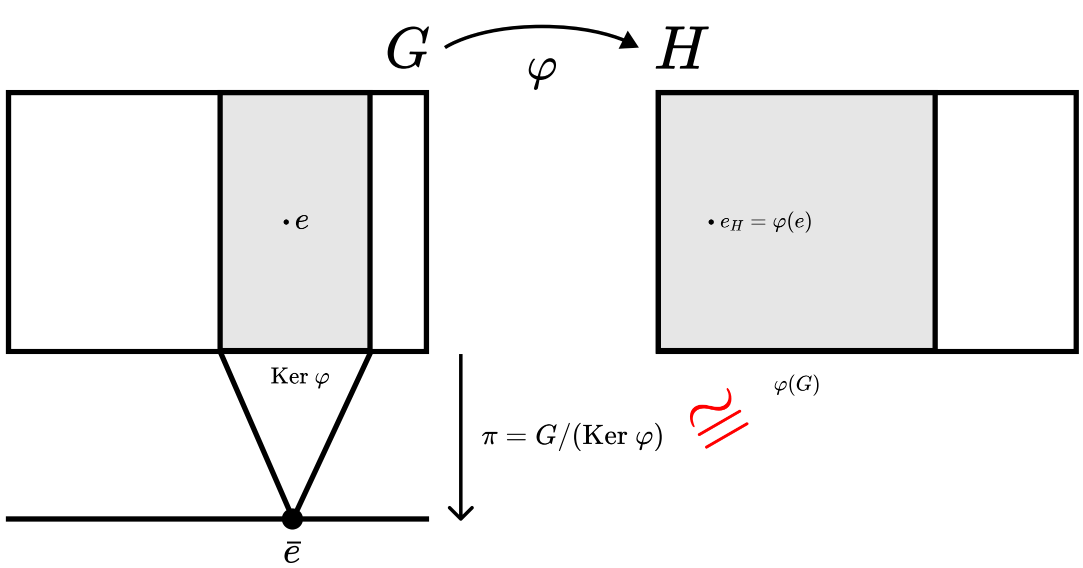
▶ **Proof**

Thm. First Isomorphism Theorem

Let $\varphi : G \to H$ 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 φ is an epimorphism, then $H \cong G/(\text{Ker } \varphi)$.

▶ **Proof**



(Figure 1) First Isomorphism Theorem

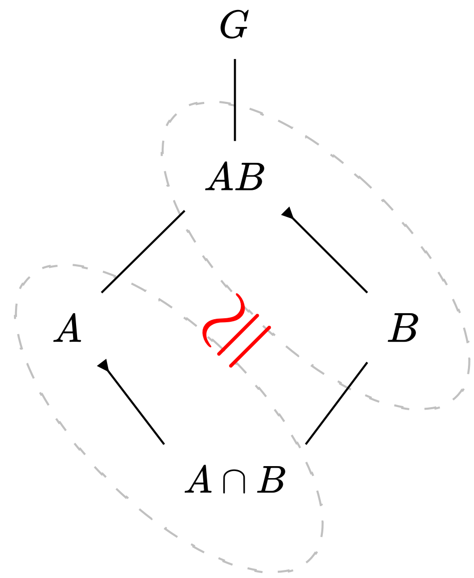
Thm. Second Isomorphism Theorem

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

Let $B \leq G$ and $A \leq N_G(B)$, so that A is a subgroup of the *normalized* B. Then, noting A is normal

1. $AB \leq G$,
2. $B \trianglelefteq AB$,
3. $A \cap B \trianglelefteq A$, and
4. $AB/B \cong A/A \cap B$.

▶ **Proof**



(Figure 2) Second Isomorphism Theorem

Thm. Third Isomorphism Theorem

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

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

▶ **Proof**

11. Symmetric Groups

Def. Permutation

A **permutation** σ 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** σ if $\sigma(x) = x$. Similarly, we say x is **moved by** σ if $\sigma(x) \neq x$.

For simplicity, we will use the set $\mathbf{I}_n = \{ 1, 2, ..., n \}$ 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 σ denoted by $\operatorname{supp} \sigma$ is defined as the set of elements that are moved by σ, that is

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

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

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

Def. Disjoint Permutations

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

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 $n!$.

Def. Cycle

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

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

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

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

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 σ denoted $\operatorname{sgn} \sigma$ 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 $n \neq 4$.