# Abstract Algebra

Jaden Wang

November 9, 2020

# Contents

## 0.1 Complex Numbers

### 0.1.1 Cartesian Coordinates

$a+bi, a, b \in \mathbb{R}, i^2 = -1$ It is convenient to visualize it on a plane. For equivalence, $c + di = e + fi \Rightarrow c = e, d = f$.

$$(a + bi)(c + di) = ac + bic + adi + bidi = (ac - bd) + (ad + bc)i.$$

Complex number multiplication is distributive, commutative, and associative. In division, simplify denominator using complex conjugate.

$$\frac{a + bi}{c + di} = \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{(ac + bd) + (bc - ad)i}{c^2 + d^2}.$$

### 0.1.2 Polar Coordinates

$$e^{i\theta} = \cos\theta + \sin\theta$$
$$re^{i\theta} = r\cos\theta + r\sin\theta$$

$$(r_1 e^{i\theta_1})(r_2 e^{i\theta_2}) = r_1 r_2 e^{i(\theta_1+\theta_2)}$$

$$\frac{r_1 e^{i\theta_1}}{r_2 e^{i\theta_2}} = \frac{r_1}{r_2} e^{i(\theta_1-\theta_2)}$$

Multiplication is easier in exponential form.

$$r_1 e^{i\theta_1} = r_2 e^{i\theta_2} \Rightarrow r_1 = r_2, \theta_1 - \theta_2 = 2k\pi, k \in \mathbb{Z}.$$

Does $x^5 = 12817$ have a real root? Use the horizontal line test. Yes, every real number has a unique odd number root.

Every nonzero complex number has precisely $n$ complex roots. The root is evenly spaced around the circle centered at the origin with such radius.

Example: Find all solutions of $z^2 = i$.
Let's use the exponential form:

$$\left(re^{i\theta}\right)^2 = i$$
$$\left(r^2 e^{2i\theta}\right) = 1e^{i\frac{\pi}{2}}$$

So we require: $r^2 = 1$ and $2\theta - \frac{\pi}{2} = 2k\pi$. Since there are only two roots, we increment $k$ once. So $k = 0, 1$.

### 0.1.3 Roots of Unity

Complex number 1: $1 + 0i$

**Example.** $z^5 = 1$. $z = 1$ is a solution. $\zeta = 1e^{\frac{2\pi}{5}}, \ldots$.

### 0.1.4 Modular Arithmetic

**Example.** For clocks, $11 + 3 =_{12} 2$. $a =_{12} b$ means $a = b \mod 12$.

**Example.** $6 + 8 =_{8.5} 5.5$.

$=_k$ is an equivalence relation, where $k \in \mathbb{Z}$.

Isomorphism between multiplying argument and modulo adding.

**Example.** Find all solutions of $x +_{2\pi} +_{2\pi} x +_{2\pi} x +_{2\pi} x = 0$, where $x \in [0, 2\pi)$.

### 0.1.5 Binary Operations

**Definition: Identity**

A binary structure $(S, *)$ has an **identity** $e \in S$ if

$$e * x = x = x * e \quad \forall x \in S.$$

**Definition: Inverse**

If $e$ is the identity for $(S, *)$, then $y$ is the **inverse** for $x$ if

$$x * y = e = y * x.$$

**Theorem**

An identity is unique if it exists.

**Proof**

Suppose not, $e$ and $e'$ are both identities for $(S, *)$.

$$e * e' = e'$$
$$e * e' = e$$

Hence $e = e'$ □

**Theorem**

Inverses if it exists it is unique if $(S, *)$ is associative.

**Proof**

Suppose not, $y$ and $y'$ are both inverses for $x$.

$$(y * x) * y' = y * (x * y')$$
$$e * y' = y * e$$
$$y' = y$$

□

**Example.** $\{1, 2, 3, 4, 5, 6\}$ under $\times_7$, inverse of 3? 5.

**Definition: Binary operation**

A **binary operation** of a set $S$ is a function $* : S \times S \to S$

**Example.** $S = \mathbb{Z}$, $*$ = subtraction.

Three things that could go wrong with binary operations (due to definition of function):

- not in $S$
- no ambiguity
- no gaps

How many binary operations are there on the $S = \{a, b, c\}$? $3^9$. In general, for an $n$-element set it is $n^{n^2}$.

**Definition: Binary structure**

A **binary structure** $(S, *)$ is a set with a binary operations, $*$, on $S$.

**Theorem**

Composition of functions is associative.

Consider $(\mathbb{C}, \times)$. Let's reduce this operation to $\mathbb{Q}$. If $a * b$ is still in $\mathbb{Q}$, then $*$ induces an operation on $\mathbb{Q}$.

**Example.** $(\mathbb{Z}, +)$ integers under addition. It's closed for even numbers but not for odd numbers.

## 0.2 Isomorphism

**Definition: isomorphism**

Let $(S, *)$ and $(S', *')$ be binary structures. An **isomorphism** $\phi$ from $(S, *)$ to $(S', *')$ is a function $\phi : S \to S'$ such that

(i) $\phi$ is a bijection

(ii) $\phi(x * y) = \phi(x) *' \phi(y)$

**Definition: isomorphic**

$(S, *)$ and $(S', *')$ are called **isomorphic** if there exists an isomorphism between them.

*Remark.* Isomorphism indicates an equivalence relationship and is symmetric. The isomorphism of the other way around is just the inverse of $\phi$.

| * | # | $ | & |
|---|---|---|---|
| # | & | # | $ |
| $ | # | $ | & |
| & | $ | & | # |

**Example** (3.2)**.** $ is the identity. # is the inerse of &. $ is self-inve. $*$ is commutative.

| * | x | y | z |
|---|---|---|---|
| x | x | y | z |
| y | y | z | x |
| z | z | x | y |

**Example** (3.3)**.**

Let's find an isomorphism between these two structures. Try:

$$\phi : \# \mapsto y, \$ \mapsto x, \& \mapsto z.$$

It works. Identity needs to map to identity.

So what structural properties does isomorphism preserve?

**Definition: structural property**

A **structural property** is a property preserved by isomorphism.

*Note.* e.g. "having 4 elements", "being commutative", "having an identity",...

**Theorem**

If $\phi : (S, *) \to (S', *')$ is an isomorphism and $e$ is the identity of $(S, *)$, then $\phi(e)$ is the identity of $(S', *')$.

**Proof**

Let $y \in S'$, we need to show that $\phi(e) *' y = y *' \phi(e)$. Since $\phi$ is a bijection, $\exists x \in S$ s.t. $\phi(x) = y$.

$$\begin{aligned} \phi(e) *' y &= \phi(e) *' \phi(x) \\ &= \phi(ex) \\ &= \phi(x) \\ &= y \end{aligned}$$

Similarly for the other way. □

Example 3.6 doesn't have an identity, but 3.3 has an identity. Hence there doesn't exist an isomorphism between the two structures. Also 3.6 is not commutative but 3.3 is. We know that 3.3 is associative because it is isomorphic to integers mod 3.

*Note.* To prove if a function is a isomorphism. First we prove it's a bijection by either finding a pair of inverses or prove both one-to-one and onto. Then we prove the second property.

**Example.** Show that $(\mathbb{R}, +)$ and $(\mathbb{R}^+, \times)$ are isomorphic.

*Intuition.* We need to map $0 \to 1$ and we need to map $+ \to \times$. Exponential is a good way to do that.

**Example.** Given $(\mathbb{R}, +), (\mathbb{R}^+, \times)$, and $\phi : (\mathbb{R}, +) \to (\mathbb{R}^d +, \times)$, and $\phi(a) = e^a$. Show that $\phi$ is an isomorphism.

**Proof**

1) The inverse of $\phi(a) = e^a$ is ln: given $x \in \mathbb{R}$ and $y \in \mathbb{R}^+$, $e^{\ln x} = x$ and $\ln(e^y) = y$.

2) we want to show that $\phi(a * b) = \phi(a) *' \phi(b)$. Given $a, b \in \mathbb{R}$,

$$e^{a+b} = e^a \times e^b$$

□

*Note.* It is really hard to show that two structures are isomorphic! It's also hard to show that two are not isomorphic. Unless the two have obvious different structural properties.

**Example.** Is there an isomorphism $\phi : (\mathbb{Q}, +) \to (\mathbb{R}, +)$? No! We can't find a bijection between a countably infinite set and an uncountably infinite set.

**Example.** $(\mathbb{R}^*, \times)$ and $(\mathbb{C}^*, \times)$. Is there an isomorphism? They have the same cardinality, both associative, commutative, with identity 1.

**Proof**

Suppose such $\phi$ exists. Consider $x * x * x * x = e$ and $y *' y *' y *' y = e'$. In this case, $\phi$ sends solutions of $x^4 = 1$ in $\mathbb{R}*$ to solutions of $y^4 = 1$ in $\mathbb{C}^*$. However, there are only two solutions in the real but four solutions in the complex. Since the identity has to be preserved, yet the solutions cannot be bijective. By contradiction, no bijection exists. □

## 0.3 Group

**Definition: group**

A **group** is a binary structure $(G, *)$ s.t.

1) $(G, *)$ is associative
2) (G,*) has an identity: there exists $e \in G$ s.t.

$$e * g = g * e = g \quad \forall g \in G.$$

3) $(G, *)$ has two-sided inverses for all $x \in G$, there exists a $y \in G$ s.t.

$$x * y = y * x = e.$$

**Example.** $(\mathbb{Z}, +)$ is a group.

**Definition: abelian group**

A group in which $*$ is commutative is called **abelian**.

**Example.**
- $\mathbb{Z}^+$ under $+$: has no identity.

- $N_0$ under $+$: 1 doesn't have an inverse.
- $(\mathbb{Q}^*, \times)$ nonzero rationals under $\times$: yes
- $(\mathbb{Q}, \times)$: 0 doesn't have an inverse.
- $(\mathbb{Z}^\times, \times)$ nonzero integers under $\times$: 2 doesn't have an inverse.
- $(\mathbb{Z}_n, +_n)$ integers mod n under addition mod n is a group. Associativity is not obvious yet.
- $(\mathbb{Z}_7^*, \times_7)$ is a group.
- $(M_n(\mathbb{R}), +)$ $n \times n$ matrices with real entries under matrix addition: is a group.
- $(M_n(\mathbb{R}), \times)$ under matrix multiplication. The zero matrix have no inverse.
- $(GL_n(\mathbb{R}), \times)$ the invertible $n \times n$ matrices in the general linear group under $\times$.
- $GL_2(\mathbb{R})$ is nonabelian.

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$$

**Theorem**

Let $(G, *)$ be a group.

- If $a * b = a * c$, then $b = c$.
- If $b * a = c * a$, then $b = c$.

**Proof**

Suppose $a * b = b * c$, then

$$\begin{aligned} a^{-1} * (a * b) &= a^{-1} * (a * c) \\ (a^{-1} * a) * b &= (a^{-1} * a) * c \\ e * b &= e * c \\ b &= c \end{aligned}$$

□

**Example** (group with 3 elements)**.** $(\mathbb{Z}_3, +_3)$.

G={e,a,b}.

*Remark.* Any group with 3 elements is isomorphic to $(\mathbb{R}_3, +_3)$.

| * | e | a | b |
|---|---|---|---|
| e | e | a | b |
| a | a | b | e |
| b | b | e | a |

| * | e | a |
|---|---|---|
| e | e | a |
| a | a | e |

**Example** (groups of order 2)**.**

**Example** (groups of order 4)**.** See iPad.

**Example.** $(U, \times)$ (all complex numbers that form unit circle) and $(U_n, \times)$ are groups.

We can show one binary structure is a group if it is isomorphic to another group. Because the required properties for groups are all structural properties.

## 0.4 Subgroups

**Definition: subgroup**

Let $(G, *)$ be a group. Let $H \subseteq G$. We call $H$ a subgroup of $G$ if $H$ is a group under the same operation.

*Note.* Subspace in linear algebra is an example of subgroup.

**Example.**

- $\mathbb{Z}$ is a subgroup of $\mathbb{Q}$ under addition.
- $U_{28}$ is a subgroup of $U$, where $U$ is the unit circle under $\times$.
- $\mathbb{Z}_2$ is the integers mod 2 under $+_2$ is NOT a subgroup of $\mathbb{Z}$ because they don't have the same operation.
- $\{1, 2, 3, \ldots\}$ under addition is NOT a subgroup of the $\mathbb{Z}$ because there is no identity.
- $\{0, 1, 2, \ldots\}$ under $+$ is NOT a subgroup of $\mathbb{Z}$ because 1 doesn't have an inverse.

**Theorem**

Let $(G, *)$ be a group and let $H \subseteq G$. Then $H \leq G$ if

- $e \in H$
- if $x \in H$ then $x^{-1} \in H$
- if $x, y \in H$, then $x * y \in H$

*Note.* Associativity is implied because it's the same operation. The first condition ensures that $H \neq \emptyset$.

**Corollary**

Any group $G$ has the following as subgroups:

- $G$ itself
- $\{e\}$

**Example.** Find the subgroups of $V_4$. See iPad.

- 4 elements: $\{3, a, b, c\}$
- 1 element: $\{e\}$
- 2 elements: $\{e, a\}, \{e, b\}, \{e, c\}$
- 3 elements: nope

There are a total of 5 subgroups.

*Note.* In $V_4$, the smallest subgroup containing $a$ is $\{e, a\}$. Likewise for other non-identity elements. The smallest subgroup for $e$ is $\{e\}$.

**Example.** Find the subgroups of $\mathbb{Z}_4$. See iPad.

- 4 elements: $\{0, 1, 2, 3\}$
- 1 elements: $0$
- 2 elements: only $\{0, 2\}$ works
- 3 elements: nope

There are only 3 subgroups.

*Note.* In $\mathbb{Z}_4$ the smallest subgroup containing 2 is $\{0, 2\}$, the smallest for 0 is $\{0\}$, the smallest for 1 or 3 is $\{0, 1, 2, 3\}$. This is a good thing.

A group with this property is called **cyclic**.

**Definition: generator**

The elements 1 (or 3) for $\mathbb{Z}_4$ is called a **generator** for $\mathbb{Z}_4$.

**Definition: cyclic group**

A group is **cyclic** if it has a generator.

**Definition: generated subgroup**

The **subgroup generated by** $x \in G$ is the smallest subgroup of $G$ that contains $x$. We denote the subgroup generated by $x$ by $\langle x \rangle$.

**Example.** In $V_4$, the following hold:

- $\langle a \rangle = \{e, a\}$
- $\langle b \rangle = \{e, b\}$
- $\langle c \rangle = \{e, c\}$
- $\langle e \rangle = \{e\}$

None of these is the whole group. This means $V_4$ is not cyclic, and has no generator.

**Example.** In $\mathbb{Z}_4$,

- $\langle 0 \rangle = \{0\}$
- $\langle 1 \rangle = \{0, 1, 2, 3\}$
- $\langle 2 \rangle = \{0, 2\}$
- $\langle 3 \rangle = \{0, 1, 2, 3\}$

$\mathbb{Z}_4$ is cyclic, it is generated by 1 or 3.

## 0.5

**Example.** Consider $(\mathbb{Z}, +)$, $\langle 5 \rangle = \{\ldots, -5, 0, 5, 10, \ldots\}$. This is called $5\mathbb{Z}$ (integer multiple of 5). Note that this is not $\mathbb{Z}_5$. The latter doesn't even have the same operation.

Is $\mathbb{Z}$ generated by 5? No. But 1 would do.

$\mathbb{Z} = \langle 1 \rangle = \langle -1 \rangle$.

**Lemma**

The inverse of a generator of a group is also a generator.

Is $\mathbb{Z}$ cyclic? Yes, it is generated by 1 (or -1).

$5\mathbb{Z}$ is a cyclic group generated by 5. $\mathbb{Z}_5$ is generated by 1.

Is $\mathbb{Z}_n$ cyclic? Yes it is generated by 1.

**Theorem**

Any cyclic group is either isomorphic to $(\mathbb{Z}_n, +_n)$ or to $(\mathbb{Z}, +)$.

Question: Is $(\mathbb{R}, +)$ cyclic?

No. Since $\mathbb{R}$ is uncountable, so there is no bijection between $\mathbb{R}$ and $\mathbb{Z}$ or $\mathbb{Z}_n$.

**Definition: greatest common divisors (gcd)**

*Note.* The gcd of $a, b$ can be written as $ra + sb$ with $r, s \in \mathbb{Z}$.

**Example.** $28r + 40s = 4 \Rightarrow 28 \times 3 + 40 \times (-2) = 4$.

**Example.** In $\mathbb{Z}_{40}$, what is $\langle 28 \rangle$?

This is controlled by the gcd(28,40). The key is $r = 3$. What else is in $\langle 28 \rangle$? $\{0, 28, 16, 4\}$. So $4 \in \langle 28 \rangle$. Then we have $\{0, 4, 8, \ldots, 36\}$ with $\frac{40}{4} = 10$ elements !

In $\mathbb{Z}_{40}$, $\langle 28 \rangle = \langle 4 \rangle$.

**Theorem**

In $\mathbb{Z}_n$, the subgroup $\langle r \rangle$ is equal to $\langle d \rangle$, where $d$=gcd$(r, n)$. Then number of elements in $\langle d \rangle$ is $\frac{n}{d} = \frac{n}{\gcd(r,n)}$.

**Theorem**

Every subgroup of a cyclic group is cyclic.

**Corollary**

Every subgroup of $\mathbb{Z}_n$ is of form $\langle r \rangle$, and in fact we can take $r$ to be a divisor of $n$.

**Example.** What are the subgroups of $\mathbb{Z}_{18}$?

We just need to choose an appropriate generator from the divisors of 18. $\langle 1\rangle = \mathbb{Z}_{18}$
$\langle 2\rangle = \{0, 2, 4, \ldots\}$ 9 elements.
$\langle 3\rangle = \{0, 3, \ldots\}$ 6 elements.
$\langle 6\rangle = \{0, 6, 12\}$ 3 elements.
$\langle 9\rangle = \{0, 9\}$ 2 elements.
$\langle 18\rangle = \{18\}$ 1 element.
$\langle 10\rangle = \langle 2\rangle$.
$\langle 7\rangle = \langle 1\rangle$ because 7 and 18 are coprime.

See iPad for subgroup lattice.

**Example.** Subgroup lattice of $\mathbb{Z}_4$. See iPad.

*Notation.* Let $(G, *)$ be a group, and let $g \in G$. For multiplication, we define $g^2 = g * g$,...,$g^n = g * \ldots * g$ with $n$ occurrence of $g$s. $g^0 = e$. $g^{-1}$ is the inverse. $g^{-2} = \left(g^{-1}\right)^2 = \left(g^2\right)^{-1}$ (this is easy to check). $g^{-n} = \left(g^{-1}\right)^n = (g^n)^{-1}$.

The subgroup $\langle g\rangle$ is given by

$$\{g^n : n \in \mathbb{Z}\}.$$

It is true that $g^m * g^n = g^{m+n}$ for all $m, n \in \mathbb{Z}$. Caution: $m, n$ are not elements of $G$.

If the operation is addition. we write $2g = g + g, 0g = e, -1g = g^{-1}$,... then

$$\langle g\rangle = \{ng : n \in \mathbb{Z}\}.$$

**Theorem**

Every cyclic group is abelian.

*Note.* The converse is false. $V_4$ is a counterexample.

**Proof**

If $G$ is cyclic then $G = \{g^n : n \in \mathbb{Z}\}$. For some generator $g$, let $x, y \in G$. Then $x = g^n$ and $y = g^m$. Then

$$x * y = g^n * g^m = g^{n+m} = g^{m+n} = g^m * g^n = y * x.$$

So $G$ is abelian. □

## 0.6

*Note.* Every subgroup of an abelian group is abelian.

**Theorem**

Let $G$ be a group and $H_1, \ldots, H_k$ be subgroups of $G$. Then $H_1 \cap \ldots \cap H_k \cap \ldots$ is a subgroup of $G$.

**Proof**

(i) $e \in H_i$ for all $i$, so $e \in \bigcap H_i$

(ii) Let $x, y \in \bigcap H_i$, then for each $i$, $x \in H_i$ and $y \in H_i \Rightarrow$ for each $i, x * y \in H_i \Rightarrow x * y \in \bigcap H_i$.

(iii) for each $i$, $x \in H_i \Rightarrow$ for each $i, x^{-1} \in H_i \Rightarrow x^{-1} \in \bigcap H_i$.

□

*Note.* Unions of subgroups are usually not subgroups, since $x * y$ might not be in the set.

**Theorem**

Let $G$ be a group and let $a_1, a_2, \ldots, a_k$ be elements of $G$. Then there is a smallest subgroup $H$ of $G$ that contains $a_1, \ldots, a_k$.

*Note.* Smallest means that every other subgroups contains this subgroup.

**Proof**

Take all such subgroups and intersect them. Then

$$H = \bigcap H_i.$$

is the smallest subgroup. $H_i$ is well-defined because at least $G$ is such subgroup. □

**Theorem**

Let $(G, *)$ be a group. Let $a, b, c \in G$. Let $H$ be the smallest subgroup containing $a, b, c$. Then, $H = \langle a, b, c \rangle$.

**Example.** A word in the generators and their inverses: $a^{-2}b^3ca^{-1}c^{-1}b^2a^{-3}$. This lies in $H$.

**Theorem**

The set of "words in the generators and their inverses" forms a subgroup.

**Proof**

(i) $a_1 a_1^{-1}$ the identity is a word.

(ii) Closure: juxtaposition gives another word.

(iii) Inverses: just another word.

□

**Theorem**

The words $a_1, \ldots, a_k$ and their inverses is the smallest subgroup containing $a_1, \ldots, a_k$.

**Proof**

We want to show that $H = \langle a, b, c \rangle = \bigcap H_i$. □

*Intuition.* The intersection starts big and the generator starts small. They both give the same result.

**Definition: finitely generated**

If there exists a finite set $\{a_1, \ldots, a_k\}$ of elements in $G$ with $G = \langle a_1, \ldots, a_k \rangle$, we call $G$ **finitely generated**.

**Example.** $V_4$. $H = \langle a, b \rangle$. Then

$$H = \{e, a, b, c\}.$$

So $V_4$ can be generated by 2 elements but not 1 element.

*Note.* Every finite group is finitely generated. Just take all elements as generators.

**Example.** $\mathbb{Z}$ is an infinite group that is finitely generated. $\mathbb{Z} = \langle 1 \rangle$.

**Example** (Challenge)**.** Show that $\mathbb{Q}$ is not finitely generated.

**Example** (Figure 7.11(b))**.** See iPad.

## 0.7 Permutation Groups

**Definition**

Let $A$ be a set (e.g. $A = \{1, 2, 3, 4, 5\}$). A **permutation** of $A$ is a bijective function $\sigma : A \to A$.

**Theorem**

A function is bijective if and only if it has a two-sided inverse (i.e. the function is invertible).

**Theorem**

A function between two finite sets with the same number of elements is injective if and only if the function is surjective.

**Example.** $A = \{1, 2, 3\}$. A permutation of $A$ might be .... There are 3! permutations. There are $n!$ permutations of an $n$-element set.

**Theorem: permutation group**

Let $A$ be a set. The set permutations of $A$, denoted by $S_A$ is a group under composition of functions.

**Claim.** $\tau \circ \sigma$ is a permutation of $A$.

**Proof**

Let $\sigma, \tau$ be permutations of $A$. So $\sigma$ has a two-sided inverse, $\sigma^{-1}$, and so does $\tau$, $\tau^{-1}$. The inverse of $\tau \circ \sigma$ is $\sigma^{-1} \circ \tau^{-1}$. This gives bijectivity. □

**Proof**

To show it's a group,

1) the identity of $A$ is $\mathrm{id}_A$ where $\mathrm{id}_A(a) = a$.
2) the inverse is $\sigma^{-1}$.
3) composition of functions is associative.
4) the previous claim shows that it is closed under operation.

□

**Definition: symmetric group**

$S_A$ is the **symmetric group** on $A$. If $A = \{1, \ldots, n\}$, we write $S_n$ for $S_A$. It has the order $n!$.

**Example.** $S_3$ permutations of $\{1, 2, 3\}$ with 6 elements. See iPad. $S_3$ is a nonabelian group with order 6, which is the smallest nonabelian group. $V_4$ is the smallest noncyclic group.

*Note.* Let $A$ be a set. Then $S_A$: symmetric group on $A$.

Elements of $S_A$ are permutations of $A$. Operation: composition of functions. $S_n$: symmetric group on $n$ "letters". This is $S_A$ where $A = \{1, \ldots, n\}$. $S_n$ has order $n!$.

$S_n$ is nonabelian if $n \geq 3$.

**Theorem: Cayley**

Every group of order $n$ is isomorphic to a subgroup of $S_n$.

**Example.** $S_4$ is a nonabelian group of order 24. Does $S_4$ have a subgroup isomorphic to $V_4$. Yes!

**Example.** What about $\mathbb{Z}_4$? Yes.

**Example** (8.4)**.** $S_5$. The two-row notation gives:

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix}$$

where the first row is the input and the second row is the output.

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix}.$$

Then

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 5 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 4 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}.$$

Note that we go from right to left.

See iPad. There are $2n$ choices where $n$ is number of vertices.

**Definition: dihedral group**

The **dihedral group** $D_n$ (or $D_{2n}$ ) of order $2n$ consists of the $2n$ sym-

metries of a regular $n$-gon, under the composition of maps. (This can be regarded as a subgroup of $S_n$).

See iPad for a fact of geometry: two reflections is equivalent to a rotation.

**Claim.** If $\alpha$ is an acute angle, then reflections will not commute.

**Theorem**

For $n \geq 3$, $D_n$ is a nonabelian group of order $2n$.

Is there a nonabelian group of order 2020? Yes $D_{1010}$.

**Claim.** The identity is a rotation, not a reflection. Rotation makes a subgroup since rotation composite rotation is still a rotation, but reflection does not. Also the determinant of both rotation and identity is 1, but that of reflection is $-1$.

## 0.8 Orbits, Cycles, and the Alternating Groups

*Note* (equivalence relation). Reflexive: $aRa$ for all $a \in S$. Symmetric: If $aRb$ then $bRa$. Transitive: If $aRb$ and $bRc$ then $aRc$.

**Example.**

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix}.$$

See iPad for orbits. Orbits of $\sigma$ (sets) are: $\{1,3,6\}, \{2,8\}, \{4,5,7\}$. They are disjoint, their union is the whole set, they are a partition of $\{1,2,\ldots,8\}$.

**Definition**

We define an equivalence relation on $\{1,\ldots,8\}$. $a \sim b$ if $b = \sigma^n(a)$ for some $n \in \mathbb{Z}$.

**Claim.** $\sim$ is an equivalence relation.

**Proof**

Reflexive: Take $n = 0$, $a = \sigma^0(a)$.
Symmetric: If $b = \sigma^n(a)$ then $a = \sigma^{-n}(b)$.
Transitive: If $b = \sigma^n(a)$ and $c = \sigma^m(b)$ then $c = \sigma^{n+m}(a)$. □

*Notation* (cycles). (1,3,6) or (1 3 6) means "1 maps to 3 which maps to 6, which maps back to 1". This is the same as (3 6 1) and (6 1 3). We prefer to use (1 3 6) where the smallest number to be in the front. This is called a cycle of length 3 or "3-cycle".

**Example** (other cycles of $\sigma$)**.** (2 8) = (8 2) "2-cycle (transposition)" and (4 7 5) = (7 5 4) = (5 4 7) "3-cycle".

*Notation.* (4 7 5) means

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 1 & 2 & 3 & 7 & 4 & 6 & 5 & 8 \end{pmatrix}.$$

So there is one orbit of length 3 and others are length 1. This permutation would be called "3-cycle". If a permutation has two orbits with more than one element, then it's not a cycle.

**Example.**

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 8 & 6 & 7 & 4 & 1 & 5 & 2 \end{pmatrix} = (1\ 3\ 6)(2\ 8)(4\ 7\ 5).$$

These are disjoint cycles (no elements are mentioned more than once). Any permutation can be written as a product of disjoint cycles.

**Example** (9.10)**.** $S_6$. Consider

$$(1\ 4\ 5\ 6)(2\ 1\ 5) = (1\ 6)(2\ 4\ 5)(3).$$

We start with the smallest number in the permutation and go from right to left. We trace the mapping until they form a cycle, then we close the parenthesis and move on to the next smallest number that hasn't been traced.

*Note.* Disjoint cycles commute.

$$(2\ 1\ 5)(1\ 4\ 5\ 6) = (1\ 4\ 2)(3)(5\ 6).$$

**Corollary: 9.12**

Any permutation of a finite set of at least two elements can be written as a product of its transpositions.

**Example.**

$$(1\ 2)(1\ 3)(1\ 4)(1\ 5) = (1\ 5\ 4\ 3\ 2) \in S_5.$$

We start from right to left. Then for (1 2 3 4 5) we can just use (1 5)(1 4)(1 3)(1 2)

**Example.**

$$\begin{aligned} \sigma &= (1\ 3\ 6)(2\ 8)(4\ 7\ 5) \\ &= (1\ 6)(1\ 3)(2\ 8)(4\ 5)(4\ 7) \end{aligned}$$

**Example.**

$$\begin{aligned}(1\ 2)(2\ 3)(1\ 2)(2\ 3)(1\ 2) &= (1)(2\ 3)\\ &= (2\ 3)\end{aligned}$$

A product of 5 transpositions = product of 1 transposition.

**Example.** Use the same $\sigma$ as above, it is a product of 5 transpositions. We can write it as 7 transposition.

$$\sigma = (1\ 6)(1\ 3)(2\ 8)(4\ 5)(4\ 7)(1\ 2)(1\ 2)\ .$$

Could $\sigma$ be the product of 10 transpositions? No!

**Definition: even permutation**

An **even permutation** is a product of even number of transpositions.

Likewise for odd permutation.

*Note.* So far any permutation is even or odd. Also, $k$-cycle are odd if $k$ is even, and are even if $k$ is odd.

**Example.** Consider (1 2) and (1 2 3) in $S_3$

**Claim.** No permutation is both even and odd.

Let's prove this using permutation matrix from linear algebra. Note that ith column of the permutation matrix tells you where the $e_i$ basis goes.

**Proof**

**Claim.** A permutation is even or odd if its permutation matrix has determinant 1 or -1, respectively.

Since every time swapping rows flips the sign of the determinant. Since it cannot have determinant to be both 1 and -1 at the same time, the permutation cannot be both even and odd. □

**Claim.** There exists an isomorphism between $S_n$ and $n \times n$ permutation matrices under matrix multiplication.

*Note.* The identity is even (12)(12) and has determinant 1.

**Example.** If $\sigma$ is a product of 5, $\tau$ is a product of 4, so $\sigma\tau$ is a product of 9 transposition.

| * | even | odd |
|---|---|---|
| even | even | odd |
| odd | odd | even |

So it adds like even and odd numbers.

**Example.** If $\alpha = (1\ 2)(2\ 4)(3\ 4)$, then $\alpha^{-1} = (3\ 4)(2\ 4)(1\ 2)$.

Then clearly an even permutation's inverse is also even.

**Theorem**

The even permutations in $S_n$ form a subgroup.

**Proof**

(i) the identity is even.

(ii) the product of two even permutations is even.

(iii) the inverse of an even permutation is even.

□

**Definition**

This is called the **alternating group on $n$ letters**, denoted $A_n$.

**Claim.** If $n \geq 2$, then exactly half the elements in $S_n$ are even,

**Proof**

The map $x \mapsto x\ (1\ 2)$ from $S_n$ to $S_n$ sends even to odd and vice versa. And if $n \geq 2$, then $|A_n| = \frac{n!}{2}$. □

*Note.* If $n = 1$, $S_n$ is trivial, and so is $A_n$, so $A_n = S_n$.

If $n = 2$, $S_n = \{id,\ (1\ 2)\}$, and $A_n$ has an order 1.

If $n = 3$, $S_n$ has order 6, and $A_n$ has order 3. So $S_n$ is nonabelian but $A_n$ is abelian! This is the only time it happens.

If $n = 4$, $A_n$ has order 12, is $\{1,\ (1\ 2\ 3),\ (1\ 3\ 2),\ (1\ 2\ 4),\ (1\ 4\ 2),\ (1\ 3\ 4),\ (1\ 4\ 3),\ (2\ 3\ 4),\ (2\ 4\ 3),\ (1\ 2)(3\ 4$

This is nonabelian because

$$(1\ 2\ 3)(1\ 2\ 4) = (1\ 3)(2\ 4)$$
$$(1\ 2\ 4)(1\ 2\ 3) = (1\ 4)(2\ 3)$$

The same counterexample can be used for $A_n$ showing that $A_n$ is nonabelian for $n \geq 4$.

*Note.* $\mathbb{Z}_n$ is abelian. $D_n$ is nonabelian for $n \geq 3$ of order 6, $A_n$ is nonabelian for $n \geq 4$ of order 12, $S_n$ is nonabelian for $n \geq 3$ of order 6.

**Definition: order**

Let $G$ be a group and let $a \in G$. The **order** of $a$ is the number of elements in $\langle a \rangle$. Alternatively, the **order** of $a$ is the smallest $n > 0$ such that $a^n = e$ or $\infty$ if no such $n$ exists. We denote the order of $a$ by $|a|$.

## 0.9 Cosets and Lagrange's Theorem

See iPad screenshots for what cosets look like. We cut $G$ into pieces and each is the same size as $H$. This forms a partition of $G$. None of them are empty, intersection is empty, and union is the whole group. Only one can be a subgroup since identity can only exist in one of them.

**Definition**

$G$ is a group, $H \leq G$. Define a relation, $\sim_L$, on $G$, such that $a \sim_L b \Rightarrow a^{-1}b \in H$ (where the inverse has to be on the left).

WLOG everything below are similar for right cosets.

**Theorem**

$\sim_L$ is an equivalence relationship.

**Proof**

(i) Reflexive: need $a \sim_L a$ for $a \in G$. $a^{-1}a = e \in H$ since $H$ is a subgroup.

(ii) Symmetric: if $a \sim_L b$, then $b \sim_L a$. Since $a^{-1}b$ and $b^{-1}a$ are inverses. Since $H$ is closed under inverses, hence $b^{-1}a \in H$.

(iii) transitive: If $a \sim_L b$ and $b \sim_L c$, then $a \sim_L c$. If $a^{-1}b \in H$ and $b^{-1}c \in H$, then $a^{-1}bb^{-1}c = a^{-1}c \in H$ since $H$ is closed under operation.

□

*Note.* We used all necessary conditions of a subgroup for the above proof.

What is $[a]$, the equivalence class of $a$?

$$[a] = \{g \in G : a \sim_L g\}.$$

$a \sim_L g$ means $a^{-1}g \in H \Leftrightarrow a^{-1}g = h \in H \Leftrightarrow g = ah, h \in H$. Then

$$[a] = \{ah : h \in H\} \coloneqq aH.$$

**Definition: cosets**

Group $G$ and subgroup $H \leq G$. The **left cosets of $H$ in $G$** is $aH = \{ah : h \in H\}$. The **right cosets of $H$ in $G$** is $Ha = \{ha : h \in H\}$ .

*Property.*

- Left cosets of $H$ partition $G$. (Any two left cosets are equal or disjoint).
- $xH = yH$ does **NOT** mean that $x = y$!!!!
- Consider $xH = \{xh : h \in H\}$. Then $xH$ contains $x$ because $e \in H$. So $xH$ is the left coset containing $x$. No other coset of $H$ does because they form a partition of $G$.
- $eH\{eh : h \in H\} = H$. So $H$ is one of the left cosets.
- there is a bijection between $H$ and $xH$. Can always multiply by $x^{-1}$ to undo it. This means that any two left cosets have the same size, and any two right cosets have the same size.
- there is a bijection between left cosets of $H$ and right cosets of $H$. We can just take inverses of each element in the left coset:

$$\begin{aligned} xh &= \{xh : h \in H\} \\ &= \{h^{-1}x^{-1} : h \in H\} \\ &= \{hx^{-1} : h \in H\} \\ &= Hx^{-1} \end{aligned}$$

  This is a bijection. So there are same number of left cosets as right cosets.

Question: What is the condition for $x$ and $y$ to be in the same cosets. Answer: $x \sim y$.

**Theorem**

$xH = yH \Leftrightarrow x^{-1}y \in H$ and $Hx = Hy \Leftrightarrow xy^{-1} \in H$.

*Note.* The important thing is for the inverse to be on the left side for left coset.

**Theorem: Lagrange's Theorem**

Let $G$ be a finite group and let $H \leq G$. Then $|G|$ is equal to $|H|$ times the number of cosets of $H$ in $G$.

See iPad for picture. Each set has the same size and together they form a partition.

**Theorem**

$|H|$ divides $|G|$.

$H \leq V_4$: $H$ cannot have size 3 because 3 cannot divide 4.

*Note.* The converse of Lagrange's Theorem is false.

**Example.** $A_4$ is a group of order $4!/2 = 12$. But $A_4$ has no subgroup of order 6, although Lagrange's Theorem allows it. This is the smallest example for this.

**Example.** $D_6$ has order 12 and does have a subgroup of order 6 which are the rotations.

Question: Is $D_6$ isomorphic to $A_4$? No. Because they have a structural difference described above.

**Definition: index**

Let $G$ be a group and $H \leq G$. The **index of $H$ in $G$** is the number of cosets of $H$ in $G$. We denote this by $|G : H|$ or $\{G : H\}$ or $(G : H)$.

So Lagrange's Theorem implies $|G| = |H| \times \{G : H\}$.

**Example** (infinite group)**.** $G = \mathbb{Z}$ and $H = 3\mathbb{Z}$. If the operation is addition-like, we write $a + H$ for $aH$. If $G$ is abelian, left and right cosets are the same. What are the cosets?

$x + H = y + H \Leftrightarrow y - x \in H$.

**Example.** Question: Are 19 and 6 in the same coset?

No, because $x + H = y + H \Leftrightarrow x - y \in H$. And $19 - 6 = 13 \notin H$.

Are 19 and 7 in the same coset?

Yes, because $7 - 19 = -12 \in H$.

**Example** (easiest one: left/right cosets are different, IMPORTANT)**.** $G = S_3$, $H = \{e, (1\ 2)\}$.

What are the left cosets of $H$ in $G$?

1) H itself.

2) The left coset containing $(1\ 2\ 3)H = \{(1\ 2\ 3)e, (1\ 2\ 3)(1\ 2)\} = \{(1\ 2\ 3), (1\ 3)\}$.

3) by elimination, we know the last left coset is $\{(2\ 3), (1\ 3\ 2)\}$.

Question: is $(1\ 3\ 2)H = (2\ 3)H$? Yes because let $x = (1\ 3\ 2)$ and $y = (2\ 3)$, then $x^{-1} = (1\ 2\ 3)$, so $x^{-1}y = (1\ 2\ 3)(2\ 3) = (1\ 2) \in H$. QUestion: is $(1\ 2\ 3)H = (2\ 3)H$? $x^{-1}y = (1\ 3\ 2)(2\ 3) = (1\ 3) \notin H$, so no.

We can just take every element of the left cosets and individually invert it to convert to right cosets.

Show that $H(1\ 3) = H(1\ 3\ 2)$. $xy^{-1} = (1\ 3)(1\ 2\ 3) = (1\ 2) \in H$.

**Example.** $G = S_3, H = \{e\}$. There are six cosets. Left/right cosets are the same even if the group is nonabelian.

**Example.** $G = S_3, H = S_3$. There is only one coset (left/right).

**Example.** $G = S_3, H = A_3$. There are two cosets. Left and right again agree because there is a subgroup and everything else.

**Claim.** Left and right cosets always agree if there are only two cosets (because one must a subgroup).

**Theorem**

If $G$ is finite, then the order of $x$, $o(x)$ divides $|G|$.

**Proof**

$\langle x \rangle$ is a subgroup of $G$, so $|\langle x \rangle|$ divides $G$ by Lagrange. □

**Theorem: 10.11**

Every group of prime order is cyclic.

**Example.** We know this doesn't have to be true for non-prime number: $V_4$.

**Proof**

Let $G$ be a group of order $p$ and let $H \geq g$. Then $|H|$ divides $|G|$. But since $|G|$ is a prime, so $|H| = 1 \Rightarrow H = \{e\}$ or $|H| = p \Rightarrow H = G$. □

**Claim.** Let $x \in G \setminus \{e\}$. Then $\langle x \rangle = G$. Not only is $G$ cyclic, but any nonidentity element is a generator.

**Definition: direct products**

Let $(G, *_G)$ and $(H, *_H)$ be two groups. The **direct product** $G \times H$ as

$$G \times H = \{(g, h) : g \in G, h \in H\}.$$

Operation: componentwise

$$(g_1, h_2) * (g_2, h_2) = (g_1 * g_2, h_1 * h_2).$$

where closure follows immediately.

Identity: $e = (e_G, e_H)$. $(e_G, e_H) * (g, h) = (e_G * g, e_H * H) = (g, h)$. Same for the other way.

Inverse: $(g^{-1}, h^{-1})$.

Associativity: see book.

**Example.** $\mathbb{Z}_2 \times \mathbb{Z}_2$ under $+_2$. See iPad screenshots for the table. $|A \times B| = |A| \times |B|$. It is isomorphic to $V_4$. This is the proof that $V_4$ is a group and is associative.

Therefore, $\mathbb{Z}_2 \times \mathbb{Z}_2$ is NOT isomorphic to $\mathbb{Z}_4$!

**Example.** $\mathbb{Z}_2 \times \mathbb{Z}_3$ this is an abelian group of order 6. $x = (1, 1) \in \mathbb{Z}_2 \times \mathbb{Z}_3$. $x + x = (0, 2)$. $x + x + x = (1, 0)$. $4x = (0, 1)$. $5x = (1, 2)$. $6x = (0, 0)$. Hence $\mathbb{Z}_2 \times \mathbb{Z}_3$ is generated by $(1, 1)$. So it is a cyclic group of order 6. Then it must be isomorphic to $\mathbb{Z}_6$!

**Claim.** Direct product of abelian groups are abelian.

**Claim.** $\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$ if and only if $\gcd(m, n) = 1$. If $\gcd(m, n) = 1$, then the order of $(1, 1)$ is $\text{lcm}(m, n) = mn$.

Goal: classify all abelian groups of order $n$.

**Definition: Cartesian product**

Given groups $(G_1, *), \ldots, (G_n, *)$. Then $G_1 \times \ldots \times G_n$ are the Cartesian product. The element in this product is the $n$-tuple $(g_1, \ldots, g_n) : g_i \in G_i$. The product of the elements is componentwise.

*Note.*

- a finite group is finitely generated. It's generated by itself.
- $\mathbb{Z}$ is finitely generated. It's generated by 1.

WARNING: $\mathbb{Z}_2 \times \mathbb{Z}_2 \not\simeq \mathbb{Z}_4$. Because the former is isomorphic to $V_4$.

Recall the fundamental theorem of arithmetic claims that any number can be written as a product of primes. The factorization is unique up to permutation. We will generalize this to groups.

*Note.* Rational numbers are not finitely generated.

**Theorem: The Fundamental Theorem of Finitely Generated Abelian Groups**

Any finitely generated abelian group $G$ is isomorphic to

$$G_1 \times G_2 \times \ldots \times G_n$$

where each $G_i$ is either isomorphic to

- a cyclic group of prime power order, $\mathbb{Z}_{p^r}$, where $p$ is prime and $r \in \mathbb{N}$.
- or $\mathbb{Z}$.

Two such groups $G_1 \times \ldots \times G_n$ and $H_1 \times \ldots \times H_m$ are isomorphic if and only if $m = n$ and the factors are rearrangements of each other.

*Note.* Rearrangement is the only way to have isomorphism. Unlike general groups. This theorem is powerful to tell when two finitely generated abelian groups are not isomorphic.

**Example** (abelian group of order 8)**.**

1) $\mathbb{Z}_8$. The building blocks are $\mathbb{Z}_8, \mathbb{Z}_4, \mathbb{Z}_2$.
2) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ not isomorphic to $\mathbb{Z}_8$ by the fundamental theorem, as they are all power of prime numbers but they are not rearrangements.
3) $\mathbb{Z}_4 \times \mathbb{Z}_2$.
4) $\mathbb{Z}_2 \times \mathbb{Z}_4$ is isomorphic to 3) by theorem.

**Claim.** Direct products of abelian groups are abelian.

1) $\mathbb{Z}_{8}\mathbb{Z}_{2^3}$ 3
2) $\mathbb{Z}_4 \times \mathbb{Z}_2\mathbb{Z}_{2^2} \times \mathbb{Z}_{2^1}$ 2+1
3) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2\mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1} \times \mathbb{Z}_{2^1}$ 1+1+1

These are "partitions of 3": Sequences of positive integers that sums to 3 and are decreasing. Partitions of $n$ control abelian groups of order $2^n$.

**Example** (partition of 4)**.** $4, 3+1, 2+2, 2+1+1, 1+1+1+1$. Use this to investigate abelian groups of order $81 = 3^4$.

1) $\mathbb{Z}_{3^4}$
2) $\mathbb{Z}_{3^3} \times \mathbb{Z}_3$
3) $\mathbb{Z}_{3^2} \times \mathbb{Z}_{3^2}$
4) $\mathbb{Z}_{3^2} \times \mathbb{Z}_3 \times \mathbb{Z}_3$
5) $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$

**Example.** Classify all abelian group of order 360.

$360 = 2^3 \times 3^2 \times 5^1$. Consider each power of prime term individually.

1) abelian groups of order 8.

2) order 9: $\mathbb{Z}_9$ and $\mathbb{Z}_3 \times \mathbb{Z}_3$

3) order 5: $\mathbb{Z}_5$.

Then we just pick one out of each and do direct product. Note that $\mathbb{Z}_{360} \simeq \mathbb{Z}_{72} \times \mathbb{Z}_5 \simeq \mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$.

**Example.** Does $\mathbb{Z} \simeq \mathbb{Z} \times \mathbb{Z}_2$? No use theorem and observe these are not rearrangement.

**Example** (11.18)**.** Is $\mathbb{Z}_8 \times \mathbb{Z}_{10} \times \mathbb{Z}_{24}$ isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{40}$?

Former $\simeq \mathbb{Z}_8 \times \mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_3 \times \mathbb{Z}_8$.
Latter $\simeq \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \mathbb{Z}_5 \times \mathbb{Z}_8$. Not isomorphic. This is the repeated application of $\mathbb{Z}_m \times \mathbb{Z}_n \simeq \mathbb{Z}_{mn}$ if $\gcd(m, n) = 1$.

*Note.* Abelian group has subgroups of every allowed orders by Lagrange.

**Example** (11.10)**.** $(8, 4, 10) \in \mathbb{Z}_{12} \times \mathbb{Z}_{60} \times \mathbb{Z}_{24}$. What is the order? Break it down to each. Order of 8 in $\mathbb{Z}_{12}$? 3. 4:15. 10:12. The answer $\text{lcm}(3, 15, 12) = \frac{15 \times 12}{\gcd(15,12)} = 60$.

## 0.10 Homomorphism

*Note.* **Homomorphism** is a structure preserving map.

In linear algebra: it preserves vector addition and scalar multiplication (linear maps).

In group theory: preserves group operation.

**Definition**

Let $(G, *)$ and $(H, *)$ be groups. A **homomorphism** (of groups) from $G$ to $H$ is a function $\phi : G \to H$ such that

$$\phi(g_1 *_G g_2) = \phi(g_1) *_H \phi(g_2).$$

*Note.* This resembles linear maps $T(u + v) = T(u) + T(v)$. Any linear map is a group homomorphism. An isomorphism is a bijective homomorphism.

**Example** (uninteresting)**.** $T : V \to W$? Let $T(v) = 0$ for all $v \in V$. Similarly, let $(G, *_G), (H, *_H)$ be groups. Define $\phi : G \to H$ by $\phi(g) = e_H$ for all $g \in G$. Then $\phi$ is a homomorphism.

**Proof**

$\phi(x *_G y) = e_H = e_H *_H e_H = \phi(x) *_H \phi(y)$ □

**Example.** $T : V \to V$. Another trivial example of homomorphism is the identity map $T(v) = v$. Similarly, $(G, *_G)$ is a group. Let $\phi : G \to G$ be defined as $\phi(g) = g$. The proof is trivial.

**Example** (interesting, not isomorphism)**.** Consider $GL_n(\mathbb{R})$: $n \times n$ invertible matrices with entries from $\mathbb{R}$ under matrix multiplication.

Is it abelian? Counterexample: use $2 \times 2$ upper and lower triangle of all 1 as non-zero entries. Then we can just insert this to any $n \times n$ identity matrices to the top left.

$GL_1(\mathbb{R}) \simeq \mathbb{R}^*$. This is abelian.

So it is abelian if and only if $n = 1$.

It is an infinite group. Just change one element of an identity matrix with infinite number of choices.

$\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$, $A \mapsto \det(A)$.

**Claim.** det is a homomorphism of groups.

It is surjective but not injective. It isn't an isomorphism because det is abelian.

$\det(AB) = \det(A)\det(B)$ by a Theorem from linear algebra. This satisfies the definition of homomorphism.

**Example** (sign map)**.** $\varepsilon : S_n \to \mathbb{Z}_2$.

$$\varepsilon(g) \begin{cases} 0 & \text{if } g \text{ is even} \\ 1 & \text{if } g \text{ is odd} \end{cases}$$

| | even | odd |
|---|---|---|
| even | even | odd |
| odd | odd | even |

| $+_2$ | 0 | 1 |
|---|---|---|
| 0 | 0 | 1 |
| 1 | 1 | 0 |

WLOG assume $x$ is even, $y$ is odd. Then

$$\varepsilon(x * y) =? \varepsilon(x) * \varepsilon(y)$$
$$1 = 0 +_2 1$$

True by table.

*Note.* Given linear map $T : V \to W$. Then $T(0_V) = 0_W$. $T(-v) = -T(v)$.

Similarly, for group homomorphism $\phi : G \to H$.

**Claim.** $\phi(e_G) = e_H$.

**Proof**

$$\phi(x *_G y) = \phi(x) *_H \phi(y)$$
$$\phi(e_G) = \phi(e_G * e_G) = \phi(e_G) *_H \phi(e_G)$$
$$Y = Y *_H Y \Rightarrow Y = \phi(e_G) = e_H$$

□

**Claim.** $\phi(g^{-1}) = \phi(g)^{-1}$.

**Proof**

$$\phi(x *_G x^{-1}) = \phi(x) *_H \phi(x^{-1})$$
$$e_H = \phi(e_G) =$$

Thus $\phi(x^{-1}) = \phi(x)^{-1}$. □

**Example.** Consider $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$. By the theorem above:

$$\det(A^{-1}) = \frac{1}{\det A}$$

.

*Note.* In linear algebra, $T : V \to W$ linear map,

$$\ker T = \{v \in V : T(v) = 0_W\}$$

and

$$\operatorname{im} T = \{w \in W : T(v) = w, v \in V\}$$

**Definition: kernel and image**

$\phi : G \to H$ a homomorphism of groups.

$$\ker \phi = \{g \in G : \phi(g) = e_H\}.$$

$$\operatorname{im} \phi = \{h \in H : \phi(g) = h, g \in G\}.$$

$\ker \phi \leq G$, $\operatorname{im} \phi \leq H$.

See screenshot for illustration.

**Proof**

$\ker \phi \subseteq G$ by definition. Then

1) $\phi(e_G) = e_H$ by previous proof.
2) closure: If $x, y \in \ker \phi$, $\phi(x) = e_H, \phi(y) = e_H$, and $\phi(x * y) = e_H * e_H = e_H$.
3) If $x \in \ker \phi$, $\phi(x^{-1}) = \phi(x)^{-1} = e_H^{-1} = e_H$.

□

**Theorem**

Let $\phi : G \to H$ be a homomorphism, and $K = \ker \phi = \{x \in G : \phi(x) = e_H\}$. The left and right cosets of $K$ are the same. That is,

$$xK = yK \Leftrightarrow Kx = Ky.$$

**Proof**

*Note.* $xK = yK \Leftrightarrow x^{-1}y \in K$.

Thus $x^{-1}y \in \ker \phi \Leftrightarrow \phi(x^{-1}y) = e_H \Leftrightarrow \phi(x)^{-1} *_H \phi(y) = e_H$. Therefore, $xK = yK \Leftrightarrow \phi(x) = \phi(y)$. Similarly, $Kx = Ky \Leftrightarrow \phi(x) = \phi(y)$. □

**Definition: normal subgroup**

Let $H \leq G$. We say $H$ is a **normal subgroup** of $G$ if the left and right cosets of $H$ in $G$ agree. We denote this as $H \trianglelefteq G$.

*Note.* There is no such thing as a "normal group". It only applies to subgroups.

**Claim.**

- If $G$ is a group then $G \trianglelefteq G$.
- The trivial subgroup $\{e\}$ is a normal subgroup.
- If $G = S_3$ and $H = \{e, (1\ 2)\}$, then $H$ is not normal in $G$. This is the smallest example of non-normal subgroup. (even though $H$ is abelian!)
- If $G$ is abelian and $H \leq G$ then $H \trianglelefteq G$. "Any subgroup of an abelian group is normal."
- Any group $G$ has normal subgroups $G$ and $\{e\}$.

- **EVERY SUBGROUP OF INDEX 2 IS NORMAL.**

**Proof**

Suppose $H \leq G$ and $H$ has index 2 (number of cosets). Then the left cosets are: $H$ and everything else. The right cosets are again $H$ and everything else. Therefore they must agree. □

- The kernel of a homomorphism is a normal subgroup.

**Example** (determinant map)**.** $\phi : GL_N(\mathbb{R}) \to \mathbb{R}^*, \phi(A) = \det A$. $\ker \phi = \{A \in GL_n(\mathbb{R}) : \phi(A) = 1\} = \{A \in GL_n(\mathbb{R}) : \det A = 1\} = SL_n(\mathbb{R})$, the special linear group.

Is $SL_n(\mathbb{R}) \trianglelefteq Gl_n(\mathbb{R})$? Yes, because it's the kernel of a homomorphism.

**Example** (sign map)**.** $\ker \varepsilon = A_n$ so $A_n \trianglelefteq S_n$ because 1. it's the kernel of a known homomorphism 2. index of $A_n$ in $S_n$ is 2.

*Intuition.* For linear map T, $T$ is injective iff $\ker T = \{0\}$

**Theorem**

If $\phi : G \to H$ homomorphism, then $\phi$ is injective $\Leftrightarrow \ker \phi = \{e_G\}$

**Proof**

Let's prove the contrapositives:

($\Leftarrow$):If $\ker \phi \neq \{e_G\}$, then there exists $x \in G \setminus \{e_G\}$ such that $\phi(x) = e_H$. Since $e_G \neq x$ and $\phi(x) = \phi(e_G) = e_H$, this implies $\phi$ is not injective.

($\Rightarrow$): We want to use the same idea from linear algebra. If $\phi$ is not injective, then there exist $x \neq y$ with $\phi(x) = \phi(y)$. Then

$$\begin{aligned} \phi(x^{-1}y) &= \phi(x^{-1})\phi(y) \\ &= \phi(x)^{-1}\phi(y) \\ &= e_H \end{aligned}$$

However, $x^{-1}y \neq e_G$ since $x \neq y$. Hence, $e_G$ and $x^{-1}y$ are distinct elements of $\ker \phi \Rightarrow \ker \neq \{e_G\}$. □

**Example.** Read differentiation example in textbook.

**Example.** $\phi : \mathbb{C}^* \to \mathbb{R}*$, $\phi(z) = |z|$. We claim this is a homomorphism.

$$\phi(z *_{\mathbb{C}} w) = |zw| = |z||w| = \phi(z) *_{\mathbb{R}} \phi(w).$$

$\operatorname{im}\phi = \mathbb{R}^+$. This is a subgroup because it is the image of a known homomorphism!

$\ker\phi = U$, the unit circle $\{z \in \mathbb{C}^* : |z| = 1\}$. Hence $U$ is a normal subgroup of $\mathbb{C}^*$. It follows from that the subgroup of an abelian group is normal. Or it's the kernel of a known homomorphism.

*Note.* T/F: If $H \leq G$ and $H$ is abelian, is $H$ a normal subgroup? NO, think $\{e, (1\ 2)\} \leq S_3$.

*Notation.* $\pi$ stands for surjective/projection. $\iota$ stands for injective.

**Example.** $\pi_1 : G_1 \times G_2 \to G_1$, $\pi((g_1, g_2)) = g_1$. "Projection to first component".

$$\begin{aligned}\pi_1((x_1, x_2) * (y_1, y_2)) &= \pi_1((x_1 * y_1, x_2 * y_2)) \\ &= (x_1 * y_1) \\ &= \phi((x_1, x_2))\phi((y_1, y_2))\end{aligned}$$

$\operatorname{im}\pi_1 = G_1$.

$\ker\pi_1 = \{(g_1, g_2) : g_1 = e_1\}$. $K \trianglelefteq G_1 \times G_2$.

## 0.11 Factor/Quotient Groups

*Note.* Quotient groups are NOT a special kind of subgroup. We try to find a group of cosets. See screenshot for the motivation. For some cases, if you call the inputs by different names, we obtain the same result.

Well-defined: the operation is not confused by picking different representations for the inputs.

Goal: $H \leq G$, try to make the left cosets of $H$ in $G$ into a group. That is, $(xH) * (yH) = xyH$. Here we should think of each coset as a single object.

Problem: the result seems to depend on the representatives $x, y$ that were chosen. If $x, x'$ in the same left coset, $xH = x'H \Leftrightarrow h = x^{-1}x' \in H, x' = xh$. So $xH = xhH$. Then

$$(xhH) * (yh'H) = xhyh'H.$$

We need $xhyh'H$ and $xyH$ to be the representations of the same things for all $x, y, h, h'$. Again this means

$$\begin{aligned}xyH = xhyh'H &\Leftrightarrow (xy)^{-1}xhyh'H \in H \\ &\Leftrightarrow y^{-1}x^{-1}xhyh'H \in H \\ &\Leftrightarrow y^{-1}hyh' = h_0 \in H \\ &\Leftrightarrow y^{-1}hy = h_0(h')^{-1} \in H\end{aligned}$$

Summary: this would work iff $y^{-1}hy \in H$ for all $h \in H, y \in G$.

Midterm 1: HW 1-4. Midterm 2: HW 5-9.

VERY IMPORTANT: the easiest example of nonnormal subgroup: $G = S_3$, and $H$ has order 2, *i.e.* $H = \{e, \{1\ 2\}\}$.

True: any subgroup of an abelian group is normal. False: any abelian subgroup of a group is normal. The example above!

The group $G$ and the trivial subgroup are normal.

Any subgroup of index 2 is normal.

The kernel of a homomorphism is normal.

False: subgroup of index 3 is normal. The example above again!

True: $3\mathbb{Z} \trianglelefteq \mathbb{Z}$ because $\mathbb{Z}$ is abelian.

*Note.* $H \trianglelefteq G$ is equivalent to:

- $gH = Hg$ for all $g \in G$. The left/right cosets containing $g$. Because $e$ is in $H$.
- $gHg^{-1} = H$ for all $g \in G$. $gHg^{-1} = \{ghg^{-1} : h \in H\}$.

  *Claim.* $gHg^{-1}$ is a subgroup of $G$ (even if $H$ is not normal).

  **Proof**

  It is clearly a subset.

  Identity: since $e \in H$, $geg^{-1} = gg^{-1} = e \in gHg^{-1}$.

  Closure: $gh_1g^{-1}gh_2g^{-1} = gh_1h_2g^{-1} \in gHg^{-1}$.

  Inverse: $(ghg^{-1})^{-1} = ghg^{-1} \in gHg^{-1}$.

  □

  *Example.* $G = S_3, H = \{e, (1\ 2)\}$. Let $g = (1\ 2\ 3)$.

  $$gHg^{-1} = \{(1\ 2\ 3)e(1\ 3\ 2), (1\ 2\ 3)(1\ 2)(1\ 3\ 2)\} = \{e, (2\ 3)\} \neq H.$$

  This is a subgroup of $S_3$, this proves that it is not normal.

  This form is called **conjugation**. We conjugated $H$ by $g$ to get $gHg^{-1}$. This might not give us the same subgroup but it would have the same order.

  Then $gH = Hg \Leftrightarrow gHg^{-1} = Hgg^{-1} = H$.

- $ghg^{-1} \in H$ for all $g \in G$, $h \in H$. This is very useful if everything else doesn't work.

  Warning: this only checks that a known subgroup is normal. It doesn't prove that something is a subgroup.

  Recall last time we tried to put a group structure on the (left) cosets of $H$ in $G$. That is,

  $$(xH) * (yH) = xyH.$$

  However, this is not well-defined unless $y^{-1}hy \in H$ for all $y \in G, h \in H$. Let $y = g^{-1}$, then $ghg^{-1} \in H \ \forall\ h \in H, g \in G$.

*Example* (not well-defined function). $f\left(\frac{a}{b}\right) = a$ is not well-defined because by choosing different representations we get different answers.

**Definition: quotient group**

Let $G$ be a group and $N \trianglelefteq G$. We define a new group, $G/N$ (read $G$ mod $N$), where $G/N$ is the set of cosets of $N$ in $G$, and the operation is $(xN) * (yN) = xyN$.

*Intuition.* $N$ is normal guarantees that if we choose different elements from the same cosets, we would get answers in another same coset.

To show that the quotient group is indeed a group,

**Proof**

(i) identity: $eH = N$ so that $(eN) * (xN) = exN = xN = (xN) * (eN)$.

(ii) inverses: $(xN) * (x^{-1}N) = xx^{-1}N = N = (x^{-1}N) * (xN)$.

(iii) associativity: $(xN) * (yN) * (zN) = (xyN) * (zN) = xyzN = x(yz)N = (xN) * ((yN) * (zN))$ by associativity in $G$.

□

**Example.** $G = \mathbb{Z}, N = 6\mathbb{Z}$. Note $N$ is normal because it is a subgroup of an abelian group. Then $G/N = \mathbb{Z}/6\mathbb{Z}$ is the definition of the integers mod 6, $\mathbb{Z}_6$. It follows that $\mathbb{Z}_6$ is a group and $+_n$ is associative.

$$G/N = \{0 + 6\mathbb{Z}, 1 + 6\mathbb{Z}, \ldots, 5 + 6\mathbb{Z}\}.$$

Then an example is

$$(3 + 6\mathbb{Z}) + (5 + 6\mathbb{Z}) = 8 + 6\mathbb{Z} = 2 + 6\mathbb{Z}.$$

This is because $8 - 2 \in 6\mathbb{Z}$, so $8 + 6\mathbb{Z} = 2 + 6\mathbb{Z}$.

**Theorem: fundamental homomorphsim theorem (1st isomorphism theorem**

Let $\phi : G \to H$ be a homomorphism. Then $\ker \phi \trianglelefteq G$ and $\operatorname{im} \phi \leq H$, and

$$G/\ker \phi \simeq \operatorname{im} \phi.$$

Furthermore, an isomorphism is given by

$$\psi : g(\ker \phi) \to \phi(g).$$

WARNING: the input of $\psi$ is coset. So we need to prove that it is a function first. Every subgroup of $\mathbb{Z}$ is cyclic. Because every subgroup of a cyclic group

is cyclic. For Problem 13.18, since $5 \in \ker\phi$, $\ker\phi$ is cyclic, 5 as the smallest positive integer is a generator.

Red flags: inputs to $\psi$ are cosets (equivalent classes). We worry that if we call $g\ker\phi$ by a different name, will the output be different?

**Proof: FHT**

Let's first show that $\psi$ is well-defined.

Let $K = \ker\phi, k \in K$. To give $\psi : gK \mapsto \phi(g)$ a different name, we can write

$$\begin{aligned}\psi : (gk)K &\mapsto \phi(gk)\\ &= \phi(g)\phi(k) \text{ since } \phi \text{ is a homomorphism}\\ &= \phi(g)e_H = \phi(g)\end{aligned}$$

So a different name gives us the same answer!

To prove bijectivity, we are going to show that $\psi$ is injective and surjective.

Injective: $\psi(g_1K) = \psi(g_2K) \Rightarrow \phi(g_1) = \phi(g_2) \Rightarrow$

$$\begin{aligned}\phi(g_1^{-1}g_2) &= \phi(g_1^{-1})\phi(g_2)\\ &= \phi(g_1)^{-1}\phi(g_2)\\ &= e_H\end{aligned}$$

Thus, $g_1^{-1}g_2 \in K \Leftrightarrow g_1K = g_2K$.

Surjective: Take $y \in \operatorname{im}\phi$, then $y = \phi(x)$ for some $x \in G$ by definition of image. Then choose $\psi(xK) = \phi(x) = y$.

It remains to show that $\psi$ is a homomorphism:

$$\begin{aligned}\psi(xK *_{G/K} yK) &= \psi(xyK)\\ &= \phi(xy)\\ &= \phi(x) *_H \phi(y)\\ &= \psi(xK) *_H \psi(yK)\end{aligned}$$

Therefore, $\psi$ is an isomorphism. □

Why are quotient groups useful?

Answer: to construct things, *i.e.* $\mathbb{Z}_6$. Also to conceptualize certain complicated construction more easily.

**Example.** What is this group? $GL_n(\mathbb{R})/SL_n(\mathbb{R})$. Let $\phi : GL_n(\mathbb{R}) \to \mathbb{R}^*$ be the determinant map. Then $\operatorname{im}\phi = \mathbb{R}^*$ since it's surjective. $\ker\phi = SL_n(\mathbb{R})$. Then the 1st isomorphism theorem states, $G/\ker\phi \simeq \operatorname{im}\phi, GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^*$. There is also an isomorphism $gSL_n(\mathbb{R}) \mapsto \det g$.

**Example.** In $D_4$, $\{\rho_0, \rho_2\}$ is a normal subgroup. The cosets are $\{\rho_1, \rho_3\}, \{\rho_1, \rho_3\}, \{\mu_1, \mu_2\}, \{\delta_1, \delta_2\}$. Because $\rho_2$ commutes with everything, and $\rho_0$ does nothing. Then $(\rho_1 N) * (\mu_1 N) = \rho_1 \mu_1 N = \delta_1 N$. This is a group of order 4. We can look at the diagonal to identify if it's $V_4$. So $D_4/N \simeq V_4$.

**Example.** Subgroups of $S_3$: $\{e, (1\ 2)\}, \{e, (1\ 3)\}, \{e, (2\ 3)\}, \{e\}, S_3, A_3$. The first three are not normal. The rest are normal. $A_3$ is 1. index is two. 2. kernel of the sign homomorphism.

Let $g \in G$, we have seen that if $H \leq G$, then so is $gHg^{-1}$. Furthermore, the map $\iota_g(x) = gxg^{-1}$ (injective map) is called conjugating by $g$.

**Proposition**

$\iota_g$ is a group homomorphism (in fact an isomorphism) from $G$ to itself.

**Proof**

$$\iota_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = \iota_g(x)\iota_g(y)$$

□

**Example.** Isomorphism of $V_4 \to V_4$. Identity needs to go to itself, but there are 3! different isomorphism. Then the group of isomorphisms are just $S_3$.

But since it's abelian, conjugation is trivial.

**Claim.** The inverse of $\iota_g = \iota_{g^{-1}}$ (conjugation by $g^{-1}$ ).

**Definition: automorphism**

An isomorphism from $G$ to itself is called an **automorphism**.

**Definition: inner automorphism**

Automorphisms that come from conjugation are called **inner automorphism**.

*Note.* Inner automorphism is a subgroup of the group of automorphisms

*Note.* $\iota_g(H)$ is a subgroup of $G$ because it is the image of $\iota_g$.

**Definition**

$$H \simeq gHg^{-1}.$$

is conjugate subgroup.

**Example.** $G = S_3, H = \{e, (1\ 2)\}, g = (1\ 3)$. Then

$$\begin{aligned} gHg^{-1} &= \{geg^{-1}, g(1\ 2)g^{-1}\} \\ &= \{e, (2\ 3)\} \\ gHg^{-1} &\simeq H \text{ but } H \neq gHg^{-1} \end{aligned}$$

Which proves that $H$ is not normal.

**Theorem**

If $G$ is abelian, then $G/N$ is abelian.

**Proof**

Let $xN, yN \in G/N$. Then

$$xN * yN = (xy)N = (yx)N = yN * xN$$

Since $x = y \Rightarrow xN = yN$. □

*Note.* The converse is false. Example is $S_3/A_3$. Or the trivial $N$.

*Note.* $G/N$ is cyclic doesn't imply $G$ is cyclic.

What is the order of $xN \in G/N$? It is the smallest $n > 0$ such that $(xN)^n = N \Rightarrow x^nN = eN \Rightarrow e^{-1}x^n \in N \Rightarrow x^n \in N$.

**Definition**

The order of a coset $xN \in G/N$ is the smallest positive integer $n$ such that $x^n \in N$.

**Example** (15.7)**.** $G = \mathbb{Z}_4 \times \mathbb{Z}_6$. Order is 24. If $G_1$ and $G_2$ are abelian so is $G_1 \times G_2$. If one group is not abelian, then the product isn't abelian. So $G$ is abelian. $G$ isn't cyclic since it isn't isomorphism to $\mathbb{Z}_{24}$.

$H = \langle(0,1)\rangle = \{(0,0), (0,1), \ldots, (0,5)\}$. The order is 6.

Is $H$ normal in $\mathbb{Z}_4 \times \mathbb{Z}_6$? Yes because $G$ is abelian.

Then $G/H$ is abelian with order 4. So it's either $\mathbb{Z}_4$ or $V_4$. We can show $\mathbb{Z}_4$ if we find an element of order 4 (a generator). Then a coset looks like $(1,0) + \langle(0,1)\rangle$.

What is the order of that?

First find all elements of $N$. Then repeat operation on the representative of coset until it's in $N$. It takes 4 steps to get $(0,0) \in N$. Thus it has order 4.

**Example.** $\mathbb{Q}/\mathbb{Z}$ is an infinite group where every element has finite order.

$\mathbb{R}/\mathbb{Q}$ is an infinite group that has no element of finite order apart from the identity.

$\mathbb{R}/\mathbb{Z} \simeq U$. Since $\phi : \mathbb{R} \to C^*, r \mapsto e^{2\pi i r}$.

**Definition: simple group**

A group is **simple** if it is nontrivial and it has no **NORMAL** subgroups other than itself and the trivial subgroup.

**Claim.** $\mathbb{Z}_p$ is a simple group if $p$ is prime. By Lagrange, there aren't any subgroups other than the trivial group and itself. These are the only abelian simple groups!

**Theorem: 15.15**

The alternating groups $A_n$ for $n \geq 5$ are simple and (nonabelian).

*Note.* $A_4$ has a normal subgroup of order 4: $\{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$

*Note.* $(1\ 2\ 3\ 4\ 5) \in A_5$, 5-cycles are even, $(1\ 5)(1\ 4)(1\ 3)(1\ 2)$. $\langle (1\ 2\ 3\ 4\ 5) \rangle$ is a subgroup of $A_5$ of order 5. $A_5$ has many subgroups but only $A_5, e$ are normal.

*Remark.* Finite simple groups were classified in 1981. The largest "sporadic group" is the Monster. It is NOT the largest nonabelian group because $A_n$ can as large as we like.

**Definition: center**

Let $G$ be a group. Then **center** (zentrum) of $G$, $Z(G)$, is the set of elements of $G$ that commute with everything. That is,

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

**Example.** $Z(D_4) = \{$ identity, rotation by 180$\}$

$$Z(D_n) = \begin{cases} \text{trivial group if n is odd} \\ \{e, \text{ identity, rotation by 180}\} \end{cases}$$

*Note.* If $G$ is abelian then $Z(G) = G$.

*Note.* $Z(S_n)$ if $n \leq 3$ is trivial.

**Theorem**

$$Z(G) \leq G.$$

**Proof**

$e \in Z(G)$. If $x \in Z(G)$ then $x^{-1} \in Z(G)$.

$$\begin{aligned} xg &= gx \\ x^{-1}xgx^{-1} &= x^{-1}gxx^{-1} \\ gx^{-1} &= x^{-1}g \end{aligned}$$

If $x, y \in Z(G)$, then show it's closed:

$$xyg = xgy = gxy.$$

To show it's normal, let $g \in G$ and $x \in Z(G)$. Show $gx^{-1}g^{-1} \in Z(G)$. Need to know it is a subgroup which we just proved.

$$gxg^{-1} = xgg^{-1} = x \in Z(G).$$

Thus, $Z(G) \trianglelefteq G$. □

**Example.** What is $Z(A_5)$? It is $\{e\}$ or $A_5$ because $A_5$ is simple and $Z(A_5) \trianglelefteq A_5$. Since $A_5$ is nonabelian, so $Z(A_5) \neq A_5$, so $Z(A_5) = \{e\}$.

*Note.* If a nonabelian group, the center is definitely not itself.

**Definition: commutator**

A **commutator** is an element of for $aba^{-1}b^{-1}$, $[a, b]$.

*Note.* Inverse can either be on the left or right. It doesn't matter.

**Definition: commutator subgroup**

The **commutator subgroup** (derived subgroup) $C(G)$, (or $G'$) of $G$, is the subgroup generated by the commutators.

*Note.* There is no guarantee that products of commutators are commutators.

**Theorem**

$$C(G) \trianglelefteq G..$$

**Proof**

$$gaba^{-1}b^{-1}g^{-1} = gag^{-1}gbg^{-1}ga^{-1}g^{-1}gb^{-1}g^{-1} = [gag^{-1}, gbg^{-1}].$$

□

**Theorem: IMPORTANT**

The commutator subgroup, $C(G)$ of $G$, is the smallest normal subgroup with abelian quotient. That is, $G/C(G)$ is abelian, and if $N \trianglelefteq G$ with $G/N$ abelian, then $C(G) \leq N$.

**Example.** $G = D_4$, normal subgroups of $G$: { rotations} because index is 2, $\{e\}, D_4, \{e,$ rotation by 180$\}$ because it's the center .

- $D_4/D_4$ is trivial group. Abelian
- $D_4/\{e\}$ is isomorphic to $D_4$. Nonabelian.
- $D_4/Z(G)$ has order 4, it's in fact $V_4$. So abelian.
- $D_4/\{$ rotations$\}$ has order 2, so isomorphic to $\mathbb{Z}_2$ abelian.

Now among the three abelian ones, which is the smallest? Guess: $C(D_4) = \{e,$ rotations by 180$\}$.

Let's check. Normal? Yes because it's the center.

Abelian quotient? Yes because has order 4.

Smallest? If not, the smallest would have to be one of its subgroups. The subgroup of this is just the identity. But identity doesn't work as it yields nonabelian group.

*Intuition.* What if $[a, b] = e$?

$$aba^{-1}b^{-1} = e \Rightarrow aba^{-1} = b \Rightarrow ab = ba.$$

*Note.* If $G$ is abelian, $C(G) = \{e\}$ and vice versa. A group is abelian iff it's center is the whole thing.

**Example.** What is $C(A_5)$? It's $A_5$ since $\{e\}$ yields $A_5$ which is nonabelian.

Midterm 2 covers HW 5-8.

## 0.12 Rings

**Definition: ring**

Let $R$ be a set and define two binary operations, $+_R, \times_R$ as following:

$+_R$ : $R$ is an abelian group under $+_R$.

1) $+_R$ is a binary operation.
2) $+_R$ is associative.
3) $+_R$ has an identity, $O_R$.
4) Everything element $r$ has an additive inverse, $-r$.
5) $+_R$ is commutative.

$\times_R$: $R$ is closed under an associative multiplication.

6) $\times_R$ is a binary operation.
7) $\times_R$ is associative.

Axioms governing how the two operations interact.

8) left distributivity law:

$$a \times_R (b +_R c) = a \times_R b + a \times_R c.$$

9) right distributive law:

$$(a +_R b) \times_R c = a \times_R c +_R b \times_R c.$$

**Example.** $(\mathbb{Z}, +_R, \times_R)$ the ring of integers. This is a ring because we assume the axioms are true for addition and multiplication of complex numbers. The same goes for rational, real, and complex numbers.

Additional properties they have:

- commutative multiplication: "commutative ring".
- multiplicative identity, $I_R$, exists and $I_R = O_R$: "ring with identity".

**Example.** $2\mathbb{Z}$, even integers under the usual operations. It is commutative but doesn't have multiplicative identity. Suppose $I_R = 2k$, then $2k \times 2 \Rightarrow 4k = 2 \Rightarrow k = \frac{1}{2} \notin 2\mathbb{Z}$.

**Example.** $(\mathbb{Z}_6, +_6, \times_6)$ is a ring (prove by quotient ring). A subset $\{0, 3\}$.

| $+_6$ | 0 | 3 |
|---|---|---|
| 0 | 0 | 3 |
| 3 | 3 | 0 |

| $\times_6$ | 0 | 3 |
|---|---|---|
| 0 | 0 | 0 |
| 3 | 0 | 3 |

The subring is commutative and has an identity of 3, even though the identity from the ring is not here.

**Example.** $M_n(\mathbb{R})$ $n \times n$ matrices with real entries under matrix addition and matrix multiplication. It is in fact a vector space of order $n^2$. This is also a ring. So are $M_n(\mathbb{Z}), M_n(\mathbb{Q}), M_n(\mathbb{C})$.

Are they commutative? No for $n \geq 2$. Use the usual counterexample.

Do they have an identity? Yes, $I_n$.

*Note.* $M_n(2\mathbb{Z})$: not commutative and no identity.

Homework 8: To check whether a group is isomorphic to $V_4$, we can check whether two unique non-identity elements square to the identity. To tell if two cosets are different, check if their difference is in the subgroup.

**Example.** Not assuming multiplication is commutative.

$$\begin{aligned}(1+1)(a+b) &= (1+1)a + (1+1)b = a+a+b+b \\ &= 1(a+b) + 1(a+b) = a+b+a+b.\end{aligned}$$

So commutativity of addition is forced by multiplicative identity and distributive laws.

What if we had $1_R = 0_R$?

**Theorem: 18.8**

(i) $0a = a0 = 0$.

(ii) $a(-b) = (-a)b = -(ab)$.

(iii) $(-a)(-b) = ab$.

**Proof**

(i)
$$0a = (0 = 0)a = 0a + 0a \Rightarrow y = y + y$$
by an abelian group. Then $0 = y = a0$. Likewise for the other.

(ii)
$$0 = a0 = a(b + (-b)) = ab + a(-b) \Rightarrow a(-b) = -(ab).$$
Likewise for the other.

(iii)
$$(-a)(-b) = -((-a)b) = -(-(ab)) = ab.$$

□

If $1_R = 0_R \Rightarrow 1_R r = 0_R r \Rightarrow r = 0_R$. Then $R = \{0_R\}$. This is why we restrict them to be different.

*Note.* If $A$ is an abelian group, we can make $A$ into a ring in a dull way.

Set: $A$. Addition: addition in $A$. Multiplication: $a \times b = 0$. We can check this is a ring.

**Example.** $R = \{f : \mathbb{R} \to \mathbb{R}\}$.

Addition: pointwise. $(f + g)(c) = f(c) + g(c)$.

Multiplication: pointwise. $(fg)(c) = f(c)g(c)$.

We can check this is a ring (vector space). Let check a distributivity law. Two functions are the same if they always give the same output for the same input.

$$\begin{aligned}((f+g)(h))(c) &= (f+g)(c)h(c) \\ &= (f(c)+g(c))h(c) \qquad \text{just real numbers} \\ &= f(c)h(c) + g(c)h(c) \\ &= fh(c) + gh(c) \\ &= (fh + gh)(c)\end{aligned}$$

They are the same because real numbers are distributive.

Is $R$ commutative? Yes.

Does $R$ have identity? $1_R$.

*Remark.* Composition of functions doesn't distribute over addition.

$f(x) = x^2, g(x) = \sin(x), h(x) = e^x$. Then

$$f(g + h) = (\sin xe^x)^2 \neq \sin^2 x + e^{2x} = fg + fh.$$

**Definition: homomorphism of rings**

A map $\phi : R \to S$ is a **homomorphism of rings** if

$$\phi(a + b) = \phi(a) + \phi(b)$$

$$\phi(a \times b) = \phi(a) \times \phi(b)$$

for all $a, b \in \mathbb{R}$.

**Example.** $\phi : \mathbb{Z} \to \mathbb{Z}, a \mapsto 2a$. We can find a counterexample for multiplication:

$\phi(1 \times 1) = 2 \neq 4 = \phi(1) \times \phi(1)$.

**Example** (evaluation homomorphism)**.** Let $R = \{f : \mathbb{R} \to \mathbb{R}\}$ with pointwise addition and multiplication. Let $a \in \mathbb{R}$, define $\phi_a : R \to \mathbb{R}$ and $\phi_a(f(x)) = f(a)$. This is a ring homomorphism.

$$\phi_a(f(x) + g(x)) = (f + g)(a) = f(a) + g(a) = \phi_a(f(x)) + \phi_a(g(x))$$

By pointwise addition. Similarly,

$$\phi_a(f(x)g(x)) = fg(a) = f(a)g(a) = \phi_a(f(x))\phi_a(g(x)).$$

Suppose $a = 2$, so $\phi_2 : f(x) \mapsto f(2)$.

**Definition**

$\phi : R \to S$ is a homomorphism of rings. Then

$$\ker \phi = \{r \in R : \phi(r) = 0\}.$$

and

$$\operatorname{im} \phi = \{s \in S : \phi(r) = s \text{ for some } r\}.$$

*Note.* Direct product of rings follows intuitively from that of groups. The projection map is again a homomorphism.

**Definition: unit**

Let $R$ be a ring with identity. A **unit** in $R$ is an element with a multiplicative inverse.

**Example.** In $\mathbb{Z}_{12}$, 7 is a unit because $7 \times 7 = 1 \mod 12$. The units are $\{1, 5, 7, 11\}$, coprimes of 12.

In $\mathbb{Z}_7$, 3 is a unit. $3 \times 5 = 1 \mod 7$.

In $\mathbb{Z}$, the units are $\{1, -1\}$. Warning: the answer to "what are the units" is usually not $\pm 1$. This is true for $\mathbb{Z}$.

In $\mathbb{Q}$, the units are all NONZERO elements.

*Note.* 0 is NEVER a unit. Because by Theorem 18.8, $u0 = 0u = 0 \neq 1$ by definition of multiplicative identity.

**Theorem**

The units, $U(R)$ of $R$, form a group under multiplication.

**Proof**

(i) closure: If $u$ and $v$ are units, so is $uv$. The inverse of $uv$ is $v^{-1}u^{-1}$.

(ii) associativity: definition of $\times_R$.

(iii) identity: $I_R$ is a unit. It is its own inverse.

(iv) inverses: If $u$ is a unit, so is $u^{-1}$.

□

**Definition: division ring**

A **division ring** is one in which every nonzero element is a unit.

**Definition: fields**

A **field** is a commutative division ring.

**Example.** $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$.

**Example** (division ring not field)**.** $\mathbb{H}$ real quaternions. They are like complex numbers but worse. Complex numbers are a vector space of dimension 2 over the reals. Quaternions are dimensional 4, $\{a + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$ with basis $\{1, i, j, k\}$, where $i^2 = j^2 = k^2 = -1$. This is not commutative, similar to cross-product. The inverse comes from conjugation.

What is the additive order of $1_R$? We know distributivity laws might be involved.

**Example.** Let $F$ be a field, and let $1_F$ be the multiplicative identity. Could $1_F$ have additive order 6?

No. Suppose $1_F+1_F+1_F+1_F+1_F+1_F = 0_F \Rightarrow (1_F+1_F)\times(1_F+1_F+1_F) = 0_F$. In a field, if $xy = 0$, then $x = 0$ or $y = 0$.

**Proof**

Suppose $x \neq 0$, we will show that $y = 0$. This implies $x$ has a multiplicative inverse, $x^{-1}$. Then

$$\begin{aligned} xy &= 0 \\ x^{-1}(xy) &= x^{-1}0 = 0 \\ (x^{-1}x)y &= 0 \\ 1_R y &= 0 \\ y &= 0 \end{aligned}$$

□

Therefore, $1_F + 1F = 0$ or $1_F + 1_F + 1_F = 0$. So we found a smaller number for the order!

**Definition: characteristic of a field**

Let $n$ be the additive order of $1_F$. If $n$ finite, the characteristic of $F$ is $n$. If $n$ is infinite, the characteristic of $F$ is 0.

**Theorem**

The characteristic of a field is either 0 or a prime.

**Example.** Extreme example: $\mathbb{Z}_2$ is field.

**Example** (zero divisors)**.** In $M_2(\mathbb{R})$. $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ In $\mathbb{Z}_{10}, 4 \times 5 = 0$.

**Definition: zero divisors**

Let $R$ be a ring and $x, y \in R$. If $xy = 0$ but $x \neq 0$ and $y \neq 0$, we call $x, y$ **zero divisors.**

**Definition: integral domain**

An **integral domain** is a commutative ring with identity that has no zero divisors.

**Example.** $\mathbb{Z}$.

**Example** (unrelated)**.** $\mathbb{H}$. Then $\{1, -1, i, -i, j, -j, k, -k\}$ under $\times$ form a group. Then the order of its elements are:

$$\begin{aligned} 1 &: 1 \\ -1 &: 2 \\ i &: 4 \\ -i &: 4 \\ j &: 4 \\ -j &: 4 \\ k &: 4 \\ -k &: 4 \end{aligned}$$

But for $D_4$, the reflections have order 2, and rotations have order $1, 4, 2, 4$. Element order is a structural property. $Q_8$ is not abelian, but every subgroup

is normal.

So the complete list of groups of order 8 is: $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \mathbb{Z}_4 \times \mathbb{Z}_2, \mathbb{Z}_8, D_4, Q_8$.

**Example** (complete list of groups with order 1 to 15)**.** Note that prime orders only have $\mathbb{Z}_p$. Orders of $p^2$ only has $\mathbb{Z}_{p^2}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$.

$$
\begin{aligned}
1 &: \{e\} \\
2 &: \mathbb{Z}_2 \\
3 &: \mathbb{Z}_3 \\
4 &: \mathbb{Z}_4, V_4 \\
5 &: \mathbb{Z}_5 \\
6 &: \mathbb{Z}_6, S_3 \simeq D_3 \\
7 &: \mathbb{Z}_7 \\
8 &: \text{described above} \\
9 &: \mathbb{Z}_9, \mathbb{Z}_3 \times \mathbb{Z}_3 \\
10 &: \mathbb{Z}_{10}, D_5 \\
11 &: \mathbb{Z}_{11} \\
12 &: \mathbb{Z}_{12}, \mathbb{Z}_2 \times \mathbb{Z}_6, D_6, A_4, T \\
13 &: \mathbb{Z}_{13} \\
14 &: \mathbb{Z}_{14}, D_7 \\
15 &: \mathbb{Z}_{15}
\end{aligned}
$$

**Theorem**

Suppose $S \subseteq R$. $S \leq R$ is a subring if

(i) $0_R \in S$ or check $S \neq \emptyset$ if we use it in junction with the negation axiom.

(ii) Closed under $+$.

(iii) Closed under $-$ or negation: if $a, b \in S$ then $a - b \in S$. Or if $a \in S$ then $-a \in S$.

(iv) Closed under $\times$: if $a, b \in S$ then $a \times b \in S$.

*Note.* The first three proves that $S$ is a subgroup.

**Example** (integral domain)**.** $\mathbb{Z}$ is an integral domain (but not a field). Having inverses doesn't mean an element is not a zero divisor.

In a group, recall the cancellation laws: $ab = ac \Rightarrow b = c, ba = ca \Rightarrow b = c$.

In $\mathbb{Z}$, if $3x = 3y$, then $x = y$. If $ab = ac$, then $a = 0$ or $b = c$.

**Proof**

Suppose $ab = ac$. Then

$$\begin{aligned} ab - ac &= 0 \\ a(b-c) &= 0 \\ a = 0 \text{ or } b - c &= 0 \text{ since no zero divisors} \\ a = 0 \text{ or } b &= c \end{aligned}$$

□

**Theorem**

If $R$ is an integral domain and $ab = ac$, then $a = 0$ or $b = c$. The other direction follows from commutativity.

**Example** (bad)**.** $\mathbb{Z}_{12}$ is not an integral domain. It is commutative, has identity 1, but has zero divisors like $3 \times 4 = 0$. In general, any composite (non-prime) order of $\mathbb{Z}_n$ is not an integral domain.

Consider $x^2 - 5x + 6 = 0$ in $\mathbb{Z}_{12}$. 2,3,6,11 are all solutions.

$$(6-2)(6-3) = 4 \times 3 = 0.$$

So what are the zero divisors of $\mathbb{Z}_{12}$?

It's 2,3,4,6,8,9,10. It happens that the non-zero divisors 1,5,7,11 are units. Their inverses are themselves. They form a group isomorphic to $V_4$.

**Proposition**

In $\mathbb{Z}_n$, any nonzero element is either a zero divisor or a unit.

*Note.* In $\mathbb{Z}$, this is not true. Units are $\{\pm 1\}$ but there is no zero divisors.

**Proof**

If $a$ is a zero divisor then $ab = 0$ for $a \neq 0, b \neq 0$. If $a$ is a unit, then there

exists $c \in R : ac = ca = 1$.

$$\begin{aligned} ab &= 0 \\ (ca)b &= c0 \\ 1b &= 0 \\ b &= 0 \end{aligned}$$

which is a contradiction. □

**Theorem**

Any field is an integral domain.

**Proof**

(i) $F$ is commutative by definition of field.

(ii) $F$ has identity by definition of division ring.

(iii) $F$ has no zero divisors. Suppose $ab = 0, a \neq 0, b \neq 0$. Then $a$ is a unit and cannot be a zero divisor. Division ring forces all nonzero elements units.

□

Is every integral domain a field? No. $\mathbb{Z}$.

**Theorem**

Every finite integral domain is a field.

**Corollary**

$\mathbb{Z}_p$ is a field.

*Intuition.* Why is 3 a unit in $\mathbb{Z}_7$?

The function $f_3 : \mathbb{Z}_7 \to \mathbb{Z}_7, x \mapsto 3x \mod 7$ is injective. Thus $f_3$ is surjective. Hence $f_3(y) = 1$ for some $y$.

**Proof**

We use the pigeonhole principle. If we have $f : A \to B$, $|A| = |B| = 5$. Then $f$ injective $\Leftrightarrow$ f surjective.

Let $R = \{a_1 = 1, a_2, \ldots, a_n\}$. Let $a \in R \setminus \{0\}$. We need to show $a$ has a multiplicative inverse.

Consider the sequence $\{aa_1, aa_2, \ldots, aa_n\}$. Suppose there is a repeat $aa_i = aa_j$, by cancellation law (since $a \neq 0$), $a_i = a_j$. So no such repeat exists. Therefore, multiplication by $a$ is injective, thus it's surjective, thus $ax = 1$ holds for some $x$. □

**Example** (zero divisors in $\mathbb{Z}_{12}$)**.** Immediately we can say 2,3,4,6 are zero divisors because they are factors of 12.

All multiples of these are zero divisors too. 8,9,10 are such multiples.

Therefore, as long as $\gcd(a, n) \neq 1$, $a$ is a zero divisor.

*Note.* In $\mathbb{Z}$, the gcd of $a$ and $b$ is of the form $ra + sb$ where $r, s \in \mathbb{Z}$.

So 5 is coprime to 12 means $\gcd(5, 12) = 1 \Rightarrow 5r + 12s = 1$ in integers. Let $r = 5, s = -2$ so it works.