PMATH347S18 - Groups & Rings

Johnson Ng

June 1, 2018

Table of Contents

List of Definitions

List of Theorems

1 Lecture 1 May 02nd 2018

1.1 Introduction

1.1.1 Numbers

The following are some of the number sets that we are already familiar with:

$$\mathbb{N} = \{1, 2, 3, ...\} \qquad \mathbb{Z} = \{.., -2, -1, 0, 1, 2, ...\}$$

$$\mathbb{Q} = \left\{ \frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{N} \right\} \qquad \mathbb{R} = \text{ set of real numbers}$$

$$\mathbb{C} = \{a + bi : a, b \in \mathbb{R}, i = \sqrt{-1}\} = \text{ set of complex numbers}$$

For $n \in \mathbb{Z}$, let $\mathbb{Z}_n$ denote the set of integers modulo n, i.e.

$$\mathbb{Z}_n = \{[0], [1], ..., [n-1]\}$$

where the $[r], 0 \le r \le n - 1$, are the congruence classes, i.e.

$$[r] = \{z \in \mathbb{Z} : z \equiv r \mod n\}$$

These sets share some common properties, e.g. $+$ and $\times$. Let's try to break that down to make further observation.

NOTE THAT for $R = \mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, or $\mathbb{Z}_n$, R has 2 operations, i.e. addition and multiplication.

Addition   If $r_1, r_2, r_3 \in R$, then

- (**closure**) $r_1 + r_2 \in R$

- (**associativity**) $r_1 + (r_2 + r_3) = (r_1 + r_2) + r_3$

Also, if $R \neq \mathbb{N}$, then $\exists 0 \in R$ (the **additive identity**) such that

$$\forall r \in R \quad r + 0 = r = 0 + r.$$

Also, $\forall r \in R, \exists(-r) \in R$ such that

$$r + (-r) = 0 = (-r) + r.$$

Multiplication For $r_1, r_2, r_3 \in R$, we have

- **(closure)** $r_1 r_2 \in R$

- **(associativity)** $r_1(r_2 r_3) = (r_1 r_2)r_3$

Also, $\exists 1 \in R$ (a.k.a the **mutiplicative identity**), such that

$$\forall r \in R \quad r \cdot 1 = r = 1 \cdot r.$$

Finally, for $R = \mathbb{Q}, \mathbb{R}$, or $\mathbb{C}, \forall r \in R, \exists r^{-1} \in R$ such that

$$r \cdot r^{-1} = 1 = r^{-1} \cdot r.$$

Note that for $R = \mathbb{Z}_n$, where $n \in \mathbb{Z}$, not all $[r] \in \mathbb{Z}_n$ have a multi-plicative inverse. For example, for $[2] \in \mathbb{Z}_4$, there is no $[x] \in \mathbb{Z}_4$ such that $[2][x] = [1]$.[1]

[1] This is best proven using techniques introduced in MATH135/145.

1.1.2 *Matrices*

For $n \in \mathbb{N} \setminus \{1\}$, an $n \times n$ matrix over $\mathbb{R}$ [2] is an $n \times n$ array that can be expressed as follows:

[2] $\mathbb{R}$ can be replaced by $\mathbb{Q}$ or $\mathbb{C}$.

$$A = [a_{ij}] = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & \cdots & a_{nn} \end{bmatrix}$$

where for $1 \leq i, j \leq n, a_{ij} \in \mathbb{R}$. We denote $M_n(\mathbb{R})$ as the set of all $n \times n$ matrices over $\mathbb{R}$.

As in Section 1.1.1, we can perform **addition and multiplication** on $M_n(\mathbb{R})$.

Matrix Addition Given $A = [a_{ij}], B = [b_{ij}], C = [c_{ij}] \in M_n(\mathbb{R})$, we define matrix addition as

$$A + B = [a_{ij} + b_{ij}],$$

which immediately gives the **closure property**, since $a_{ij} + b_{ij} \in \mathbb{R}$ and hence $A + B \in M_n(\mathbb{R})$. Also, by this definition, we also immediately obtain the **associativity property**, i.e.

$$A + (B + C) = (A + B) + C.$$

We define the zero matrix as

$$0 = \begin{bmatrix} 0 & 0 & \ldots & 0 \\ 0 & 0 & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & 0 \end{bmatrix}.$$

Then we have that 0 is the **additive identity**, i.e.

$$A + 0 = A = 0 + A.$$

Finally, $\forall A \in M_n(\mathbb{R}), \exists (-A) \in M_n(\mathbb{R})$ (the **additive inverse**) such that

$$A + (-A) = 0 - (-A) + A.$$

Note that in this case, we also have that that the operation is **commutative**, i.e.

$$A + B = B + A.$$

Matrix Multiplication Given $A = [a_{ij}], B = [b_{ij}], C = [c_{ij}] \in M_n(\mathbb{R})$, we define the matrix multiplication as

$$AB = [d_{ij}] \text{ where } c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} \in \mathbb{R}.$$

Clearly, $AB \in M_n(\mathbb{R})$, i.e. it is **closed under matrix multiplication**. Also, we have that, under such a defintion, matrix multiplication is **associative**, i.e.

$$A(BC) = (AB)C.$$

Define the identity matrix, $I \in M_n(\mathbb{R})$, as follows:

$$I = \begin{bmatrix} 1 & 0 & \ldots & 0 \\ 0 & 1 & \ldots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \ldots & 1 \end{bmatrix}.$$

Then we have that I is the **multiplicative identity**, since

$$AI = A = IA.$$

However, contrary to matrix addition, $\forall A \in M_n(\mathbb{R})$, it is not always true that $\exists A^{-1} \in M_n(\mathbb{R})$ such that

$$AA^{-1} = I = A^{-1}A.$$

This is especially true if the **determinant** of A is 0.

Also, we can always find some $A, B \in M_n(\mathbb{R})$ such that

$$AB \neq BA,$$

i.e. matrix multiplication is not always commutative.

THE COMMON PROPERTIES of the operations from above: **closure, associativity, and existence of an inverse**, are not unique to just addition and multiplication. We shall see in the next lecture that there are other operations where these properties will continue to hold, e.g. **permutations**.

2 Lecture 2 May 04th 2018

2.1 Introduction (Continued)

2.1.1 Permutations

Definition 1 (Injectivity)
Let $f : X \rightarrow Y$ be a function. We say that f is *injective* (or *one-to-one*) if $f(x_1) = f(x_2)$ implies $x_1 = x_2$.

Definition 2 (Surjectivity)
Let $f : X \rightarrow Y$ be a function. We say that f is *surjective* (or *onto*) if $\forall y \in Y \ \exists x \in X \ f(x) = y$.

Definition 3 (Bijectivity)
Let $f : X \rightarrow Y$ be a function. We say that f is *bijective* if it is both *injective* and *surjective*.

Definition 4 (Permutations)
Given a non-empty set L, a permutation of L is a bijection from L to L. The set of all permutations of L is denoted by S_L.

Example 2.1.1
Consider the set $L = \{1, 2, 3\}$, which has the following 6 different permuta-

tions:

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$$

> **Note**
>
> $$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$
>
> *indicates the bijection* $\sigma : \{1,2,3\} \to \{1,2,3\}$ *with* $\sigma(1) = 1$, $\sigma(2) = 3$ *and* $\sigma(3) = 2$.

FOR $n \in \mathbb{N}$, we denote $S_n := S_{\{1,2,...,n\}}$, the set of all permutations of $\{1,2,...,n\}$. Example 2.1.1 shows the elements of the set S_3.

Definition 5 (Order)

*The **order** of a set A, denoted by $|A|$, is the cardinality of the set.*

Example 2.1.2

We have seen that the order of S_3, $|S_3|$ is $6 = 3!$.

Proposition 1

$|S_n| = n!$

Proof

$\forall \sigma \in S_n$, *there are n choices for $\sigma(1)$, $n-1$ choices for $\sigma(2)$, ..., 2 choices for $\sigma(n-1)$, and finally 1 choice for $\sigma(n)$.* $\qquad\square$

Do elements of S_n share the same properties as what we've seen in the numbers? Given $\sigma, \tau \in S_n$, we can **compose** the 2 together to get a third element in S_n, namely $\sigma\tau$ (wlog), where $\sigma\tau : \{1,...,n\} \to \{1,...,n\}$ is given by $\forall x \in \{1,...,n\}$, $x \mapsto \sigma(\tau(x))$.

It is important to note that $\because \sigma, \tau$ are **both bijective**, $\sigma\tau$ is also bijective. Thus, together with the fact that $\sigma\tau : \{1,...,n\} \to \{1,...,n\}$, we have that $\sigma\tau \in S_n$ by definition of S_n.

$\therefore \forall \sigma, \tau \in S_n$, $\sigma\tau, \tau\sigma \in S_n$, but $\sigma\tau \neq \tau\sigma$ in general. The following is an example of the stated case:

Example 2.1.3

Let

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

Compute $\sigma\tau$ and $\tau\sigma$ to show that they are not equal.

Solution

$$\sigma\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \text{ but } \tau\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

Perhaps what is interesting is the question of: **when does commutativity occur?** One such case is when σ and τ have support sets that are disjoint[1].

[1] This is proven in A1

On the other hand, the associative property holds[2], i.e.

[2]

Exercise 2.1.1
Prove this as an exercise.

$$\forall \sigma, \tau, \mu \in S_n \quad \sigma(\tau\mu) = (\sigma\tau)\mu$$

The set S_n also has an identity element[3], namely

[3]

Exercise 2.1.2
Verify that the given identity element is indeed the identity, i.e.

$$\varepsilon = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$$

$$\forall \sigma \in S_n \quad \sigma\varepsilon = \sigma = \varepsilon\sigma.$$

Finally, $\forall \sigma \in S_n$, since σ is a bijection, we have that its inverse function, σ^{-1} is also a bijection, and thus satisfies the requirements to be in S_n. We call $\sigma^{-1} \in S_n$ to be the **inverse permutation** of σ, such that

$$\forall x, y \in \{1, \dots, n\} \quad \sigma^{-1}(x) = y \iff \sigma(y) = x.$$

It follows, immediately, that

$$\sigma(\sigma^{-1}(x)) = x \wedge \sigma^{-1}(\sigma(y)) = y.$$

$\therefore$ We have that

$$\sigma\sigma^{-1} = \varepsilon = \sigma^{-1}\sigma.$$

Example 2.1.4

Find the inverse of

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

Solution

By rearranging the image in ascending order, using them now as the object

and their respective objects as their image, construct

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

It can easily (although perhaps not so prettily) be shown that

$$\sigma\tau = \varepsilon = \tau\sigma.$$

With all the above, we have for ourselves the following proposition:

Proposition 2 (Properties of S_n)
We have

1. $\forall \sigma, \tau \in S_n \ \ \sigma\tau, \tau\sigma \in S_n.$

2. $\forall \sigma, \tau, \mu \in S_n \ \ \sigma(\tau\mu) = (\sigma\tau)\mu.$

3. $\exists \varepsilon \in S_n \ \forall \sigma \in S_n \ \ \sigma\varepsilon = \sigma = \varepsilon\sigma.$

4. $\forall \sigma \in S_n \ \exists! \sigma^{-1} \in S_n \ \ \sigma\sigma^{-1} = \varepsilon = \sigma^{-1}\sigma.$

CONSIDER

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 3 & 1 & 7 & 6 & 9 & 4 & 2 & 5 & 8 & 10 \end{pmatrix} \in S_{10}$$

If we represent the action of σ geometrically, we get

We observe

that σ can be **decomposed** into one 4-cycle, $\begin{pmatrix} 1 & 3 & 7 & 2 \end{pmatrix}$, one 2-cycle, $\begin{pmatrix} 4 & 6 \end{pmatrix}$, one 3-cycle, $\begin{pmatrix} 5 & 9 & 8 \end{pmatrix}$, and one 1-cycle, $\begin{pmatrix} 10 \end{pmatrix}$.

Note that these cycles are (pairwise) **disjoint**, and we can write[4]

[4] We generally do not include the 1-cycle and assume that by excluding them, it is known that any number that is supposed to appear loops back to themselves.

$$\sigma = \begin{pmatrix} 1 & 3 & 7 & 2 \end{pmatrix} \begin{pmatrix} 4 & 6 \end{pmatrix} \begin{pmatrix} 5 & 9 & 8 \end{pmatrix}$$

Note that we may also write

$$\sigma = \begin{pmatrix} 4 & 6 \end{pmatrix} \begin{pmatrix} 5 & 9 & 8 \end{pmatrix} \begin{pmatrix} 1 & 3 & 7 & 2 \end{pmatrix}$$
$$= \begin{pmatrix} 6 & 4 \end{pmatrix} \begin{pmatrix} 9 & 8 & 5 \end{pmatrix} \begin{pmatrix} 7 & 2 & 1 & 3 \end{pmatrix}$$

It is interesting to note that the cycles can rotate their "elements" in a
cyclic manner, i.e.

$$\begin{pmatrix} 1 & 3 & 7 & 2 \end{pmatrix} = \begin{pmatrix} 7 & 2 & 1 & 3 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 & 7 & 3 \end{pmatrix}.$$

Although the decomposition of the cycle notation is not unique (i.e.
you may rearrange them), each individual cycle is unique, and is
proven below[5].

Theorem 3 (Cycle Decomposition Theorem)

*If $\sigma \in S_n$, $\sigma \neq \varepsilon$, then σ is a product of (one or more) disjoint cycles
of length at least 2. This factorization is unique up to the order of the
factors.*

Note (Convention)

*Every permutation in S_n can be regarded as a permutation of S_{n+1} by
fixing the permutation of $n + 1$. Therefore, we have that*

$$S_1 \subseteq S_2 \subseteq \ldots \subseteq S_n \subseteq S_{n+1} \subseteq \ldots$$

3 Lecture 3 May 07th 2018

3.1 Groups

3.1.1 Groups

Definition 6 (Groups)

Let G be a set and $*$ an operation on $G \times G$. We say that $G = (G, *)$ is a **group** *if it satisfies*[1]

1. **Closure**: *$\forall a, b \in G \quad a * b \in G$*

2. **Associativity**: *$\forall a, b, c \in G \quad a * (b * c) = (a * b) * c$*

3. **Identity**: *$\exists e \in G \ \forall a \in G \quad a * e = a = e * a$*

4. **Inverse**: *$\forall a \in G \ \exists b \in G \quad a * b = e = b * a$*

[1] If you wonder why the uniqueness is not specified for **Identity** and **Inverse**, see Proposition 4.

Definition 7 (Abelian Group)

A group G is said to be abelian if $\forall a, b \in G$, we have $a * b = b * a$.

Proposition 4 (Group Identity and Group Element Inverse)

Let G be a group and $a \in G$.

1. *The identity of G is unique.*

2. *The inverse of a is unique.*

Proof

1. If $e_1, e_2 \in G$ are both identities of G, then we have

$$e_1 \overset{(1)}{=} e_1 * e_2 \overset{(2)}{=} e_2$$

   where (1) is because e_2 is an identity and (2) is because e_1 is an identity.

2. Let $a \in G$. If $b_1, b_2 \in G$ are both the inverses of a, then we have

$$b_1 = b_1 * e = b_1 * (a * b_2) \overset{(1)}{=} e * b_2 = b_2$$

   where (1) is by associativity.

Example 3.1.1
The sets $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, and $(\mathbb{C}, +)$ are all abelian, wehre the additive identity is 0, and the additive inverse of an element r is $(-r)$.

Note
$(\mathbb{N}, +)$ is not a group for neither does it have an identity nor an inverse for any of its elements.

Example 3.1.2
*The sets $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ and $(\mathbb{C}, \cdot)$ are **not** groups, since 0 has no multiplicative inverse in $\mathbb{Q}, \mathbb{R}$ or $\mathbb{C}$.*

We may define that for a set S, let $S^* \subseteq S$ contain all the elements of S that has a multiplicative inverse. For example, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$. Then, $(\mathbb{Q}, \cdot), (\mathbb{R}, \cdot)$ and $(\mathbb{C}, \cdot)$ are groups and are in fact abelian, where the multiplicative identity is 1 and the multiplicative of an element r is $\frac{1}{r}$.

Example 3.1.3
The set $(M_n(\mathbb{R}), +)$ is an abelian group, where the additive identity is the zero matrix, $0 \in M_n(\mathbb{R})$, and the additive inverse of an element $M = [a_{ij}] \in M_n(\mathbb{R})$ is $-M = [-a_{ij}] \in M_n(\mathbb{R})$.

CONSIDER the set $M_n(\mathbb{R})$ under the matrix mutiplication operation that we have introduced in Lecture 1 May 02nd 2018. We found that

the identity matrix is

$$
I = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix} \in M_n(\mathbb{R}).
$$

But since not all elements of $M_n(\mathbb{R})$ have a multiplicative inverse[2], $(M_n(\mathbb{R}), \cdot)$ is not a group.

[2] The multiplicative inverse of a matrix does not exist if its determinant is 0.

WE CAN TRY to do something similar as to what we did before: by excluding the elements that do not have an inverse. In this case, we exclude elements whose determinant is 0. We define the following set

Definition 8 (General Linear Group)
*The **general linear group of degree** n **over** $\mathbb{R}$ is defined as*

$$
GL_n(\mathbb{R}) := \{ M \in M_n(\mathbb{R}) \ : \ \det M \neq 0 \}
$$

Note that $\because \det I = 1 \neq 0$, we have that $I \in GL_n(\mathbb{R})$.
Also, $\forall A, B \in GL_n(\mathbb{R})$, we have that $\because \det A \neq 0 \wedge \det B \neq 0$,

$$
\det AB = \det A \det B \neq 0,
$$

and therefore $AB \in GL_n(\mathbb{R})$. Finally, $\forall M \in GL_n(\mathbb{R})$, $\exists M^{-1} \in GL_n(\mathbb{R})$ such that

$$
MM^{-1} = I = M^{-1}M
$$

since $\det M \neq 0$. $\therefore (GL_n(\mathbb{R}), \cdot)$ is a group.

SINCE we have introduced permutations in Lecture 2 May 04th 2018, we shall formalize the purpose of its introduction below.

Example 3.1.4
*Consider S_n, the set of all permutations on $\{1, 2, ..., n\}$. By Proposition 2, we know that S_n is a group. We call S_n the **symmetry group of degree** n. For $n \geq 3$, the group S_n is not abelian[3].*

[3] Let us make this an exercise.

Exercise 3.1.1
For $n \geq 3$, prove that the group S_n is not abelian.

NOW THAT we have a fairly good idea of the basic concept of a

group, we will now proceed to look into handling multiple groups. One such operation is known as the **direct product**.

Example 3.1.5

Let G and H be groups. Their direct product is the set $G \times H$ with the component-wise operation defined by

$$(g_1, h_1) * (g_2, h_2) = (g_1 *_G g_2, h_1 *_H h_2)$$

where $g_1, g_2 \in G$, $h_1, h_2 \in H$, $*_G$ is the operation on G, and $*_H$ is the operation on H.

   *The **closure** and **associativity** property follow immediately from the definition of the operation. The identity is $(1_G, 1_H)$ where 1_G is the identity of G and 1_H is the identity of H. The inverse of an element $(g_1, h_1) \in G \times H$ is (g_1^{-1}, h_1^{-1}).*

   By induction, we can show that if $G_1, G_2, ..., G_n$ are groups, then so is $G_1 \times G_2 \times \ldots \times G_n$.

   To facilitate our writing, use shall use the following notations:

Notation

Given a group G and $g_1, g_2 \in G$, we often denote its identity by 1, and write $g_1 * g_2 = g_1 g_2$. Also, we denote the unique inverse of an element $g \in G$ as g^{-1}.

   We will write $g^0 = 1$. Also, for $n \in \mathbb{N}$, we define

$$g^n = \underbrace{g * g * \ldots * g}_{n \text{ times}}$$

and

$$g^{-n} = (g^{-1})^n$$

  With the above notations,

Proposition 5

Let G be a group and $g, h \in G$. We have

1. $(g^{-1})^{-1} = g$

2. $(gh)^{-1} = h^{-1} g^{-1}$

Exercise 3.1.2
Prove Proposition 5 as an exercise.

3. $g^n g^m = g^{n+m}$ for all $n, m \in \mathbb{Z}$

4. $(g^n)^m = g^{nm}$ for all $n, m \in \mathbb{Z}$

Warning

In general, it is not true that if $g, h \in G$, then $(gh)^n = g^n h^n$. For example,

$$(gh)^2 = ghgh \quad but \quad g^2 h^2 = gghh.$$

The two are only equal if and only if G is abelian.

---

3. $g^n g^m = g^{n+m}$ for all $n, m \in \mathbb{Z}$

4. $(g^n)^m = g^{nm}$ for all $n, m \in \mathbb{Z}$

4 Lecture 4 May 09 2018

4.1 Groups (Continued)

4.1.1 Groups (Continued)

Proposition 6 (Cancellation Laws)

Let G be a group and $g, h, f \in G$. Then

1. (a) (**Right Cancellation**) $gh = gf \implies h = f$

   (b) (**Left Cancellation**) $hg = fg \implies h = f$

2. *The equation $ax = b$ and $ya = b$ have unique solution for $x, y \in G$.*

Proof

1. (a) By left multiplication and associativity,

$$gh = gf \iff g^{-1}gh = g^{-1}gf \iff h = f$$

   (b) By right multiplication and associativity,

$$hg = fg \iff hgg^{-1} = fgg^{-1} \iff h = f$$

2. Let $x = a^{-1}b$. Then

$$ax = a(a^{-1}b) = (aa^{-1})b = b.$$

   If $\exists u \in G$ that is another solution, then

$$au = b = ax \implies u = x$$

by Left Cancellation. The proof for $ya = b$ is similar by letting $y = ba^{-1}$.

□

4.1.2 Cayley Tables

For a finite group, defining its operation by means of a table is sometimes convenient.

Definition 9 (Cayley Table)

*Let G be a group. Given $x, y \in G$, let the product xy be an entry of a table in the row corresponding to x and column corresponding to y. Such a table is called a **Cayley Table**.*

Note

By Cycle Decomposition Theorem 6, the entries in each row (and respectively, column) of a Cayley Table are all distinct.

Example 4.1.1

Consider the group $(\mathbb{Z}_2, +)$. Its Cayley Table is

$\mathbb{Z}_2$	$[0]$	$[1]$
$[0]$	$[0]$	$[1]$
$[1]$	$[1]$	$[0]$

where note that we must have $[1] + [1] = [0]$; otherwise if $[1] + [1] = [1]$ then $[1]$ does not have its additive inverse, which contradicts the fact that it is in the group.

Example 4.1.2

Consider the group $\mathbb{Z}^* = \{1. -1\}$. Its Cayley Table (under multiplication) is

$\mathbb{Z}^*$	1	-1
1	1	-1
-1	-1	1

If we replace 1 by $[0]$ and -1 by $[1]$, the Cayley Tables of $\mathbb{Z}_2$ and $\mathbb{Z}^*$ are the same. In thie case, we say that $\mathbb{Z}_2$ and $\mathbb{Z}^*$ are **isomorphic**, which we denote by $\mathbb{Z}_2 \cong \mathbb{Z}^*$.

Example 4.1.3

Given $n \in \mathbb{N}$, the **Cyclic Group** *of order n is defined by*

$$C_n = \{1, a, a^2, ..., a^{n-1}\} \quad \text{with } a^n = 1.$$

We write $C_n = \langle a : a^n = 1 \rangle$ and a is called a generator of C_n. The Cayley Table of C_n is

C_n	1	a	a^2	...	a^{n-2}	a^{n-1}
1	1	a	a^2	...	a^{n-2}	a^{n-1}
a	a	a^2	a^3	...	a^{n-1}	1
a^2	a^2	a^3	a^4	...	1	a
$\vdots$	$\vdots$	$\vdots$	$\vdots$		$\vdots$	$\vdots$
a^{n-2}	a^{n-2}	a^{n-1}	1	...	a^{n-4}	a^{n-3}
a^{n-1}	a^{n-1}	1	a	...	a^{n-3}	a^{n-2}

Proposition 7

Let G be a group. Up to isomorphism, we have

1. *if $|G| = 1$, then $G \cong \{1\}$.*

2. *if $|G| = 2$, then $G \cong C_2$.*

3. *if $|G| = 3$, then $G \cong C_3$.*

4. *if $|G| = 4$, then either $G \cong C_4$ or $G \cong K_4 \cong C_2 \times C_2$.*

K_n is known as the **Klein n-group**

Proof

1. *If $|G| = 1$, then it can only be $G = \{1\}$ where 1 is the identity element.*

2. *$|G| = 2 \implies G = \{1, g\}$ with $g \neq 1$. The Cayley Table of G is thus*

G	1	g
1	1	g
g	g	1

    where we note that $g^2 = 1$; otherwise if $g^2 = g$, then we would have $g = 1$ by Cycle Decomposition Theorem 6, *which contradicts the fact that $g \neq 1$. Comparing the above Cayley Table with that of C_2, we see that $G = \langle g : g^2 = 1 \rangle \cong C_2$.*

3. *$|G| = 3 \implies G = \{1, g, h\}$ with $g \neq 1 \neq h$ and $g \neq h$. We can then*

start with the following Cayley Table:

G	1	g	h
1	1	g	h
g	g		
h	h		

We know that by Cycle Decomposition Theorem 6, *$gh \neq g$ and $gh \neq h$. Thus $gh = 1$. Similarly, we get that $hg = 1$.*

Claim: Entries in a row (or column) must be distinct. Suppose not. Then say $g^2 = 1$. But since $gh = 1$, by Cycle Decomposition Theorem 6, *we have that $h = g$, which is a contradiction.*

With that, we can proceed to fill in the rest of the entries: with $g^2 = h$ and $h^2 = g$. Therefore,

G	1	g	h
1	1	g	h
g	g	h	1
h	h	1	g

Recall that the Cayley Table for C_3 is:

C_3	1	a	a^2
1	1	a	a^2
a	a	a^2	1
a^2	a^2	1	a

$\therefore G \cong C_3$ (by identifying $g = a$ and $h = a^2$).

4. **Proof will be added once assignment 1 is over**

4.2 *Subgroups*

4.2.1 *Subgroups*

Definition 10 (Subgroup)

Let G be a group and $H \subseteq G$. If H itself is a group, then we say that H is a subgroup of G

5 Lecture 5 May 11th 2018

5.1 Subgroups (Continued)

5.1.1 Subgroups (Continued)

Note (Recall: definition of a subgroup)

Let G be a group and $H \subseteq G$. If H itself is a group, then we say that H is a subgroup of G.

Note

Since G is a group, $\forall h_1, h_2, h_3 \in H \subseteq G$, we have $h_1(h_2 h_3) = (h_1 h_2)h_3$. So H is a subgroup of G if it satisfies the following conditions, which we shall hereafter refer to as the Subgroup Test.

Subgroup Test

1. $h_1 h_2 \in H$

2. $1_G \in H$

3. $\exists h_1^{-1} \in H$ such that $h_1 h_1^{-1} = 1_G$

Note that the identity in H must also be the identity in G. This is because if $h_1, h_1^{-1} \in H$, then $h_1 h_1^{-1} = 1_H$, but $h_1, h_1^{-1} \in G$ as well, and so $h_1 h_1^{-1} = 1_G$. Thus $1_H = 1_G$.

Example 5.1.1

Given a group G, it is clear that $\{1\}$ and G are both subgroups of G.

Example 5.1.2

We have the following chain of groups:

$$(\mathbb{Z}, +) \subseteq (\mathbb{Q}, +) \subseteq (\mathbb{R}, +) \subseteq (\mathbb{C}, +)$$

Recall that the general linear group is defined as:

$$GL_n(\mathbb{R}) = (GL_n(\mathbb{R}), \cdot) = \{A \in M_n(\mathbb{R}) : \det A \neq 0\}$$

Definition 11 (Special Linear Group)

*The **special linear group** of order n of $\mathbb{R}$ is defined as*

$$SL_n(\mathbb{R}) = (SL_n(\mathbb{R}), \cdot) = \{A \in M_n(\mathbb{R}) : \det A = 1\}$$

Example 5.1.3

Clearly, $SL_n(\mathbb{R}) \subseteq GL_n(\mathbb{R})$. Note that the identity matrix I must be in $SL_n(\mathbb{R})$ since $\det I = 1$. Also, $\forall A, B \in SL_n(\mathbb{R})$, we have that

$$\det AB = \det A \det B = 1$$

*$\therefore AB \in SL_n(\mathbb{R})$. Also, since $\det A^{-1} = \frac{1}{\det A} = 1$, we also have that $^{-1} \in SL_n(\mathbb{R})$. We see that $SL_n(\mathbb{R})$ satisfies the **Subgroup Test**, and hence it is a subgroup of $GL_n(\mathbb{R})$.*

Definition 12 (Center of a Group)

*Given a group G, the **the center of a group** G is defined as*

$$Z(G) = \{z \in G : \forall g \in G \ zg = gz\}$$

Example 5.1.4

For a group G, $Z(G)$ is an abelian subgroup of G.

Proof

Clearly, $1_G \in Z(G)$. Let $y, z \in G$. $\forall g \in G$, we have that

$$(yz)g = y(zg) = y(gz) = (yg)z = (gy)z = g(yz)$$

Therefore $yz \in Z(G)$ and so $Z(G)$ is closed under its operation. Also, $\forall h in G$, we can write $h = (h^{-1})^{-1} = g^{-1}$. Since $z \in Z(G)$, we have that

$\forall g \in G$,

$$zg = gz \iff (zg)^{-1} = (gz)^{-1} \iff g^{-1}z^{-1} = z^{-1}g^{-1}$$
$$\iff hz^{-1} = z^{-1}h$$

Therefore $z^{-1} \in Z(G)$. By the Subgroup Test, it follows that $Z(G)$ is a subgroup of G.

Finally, since $Z(G) \subseteq G$, by its definition, we have that $\forall x, y \in Z(G)$, $x, y \in G$ as well, and we have that $xy = yx$. Therefore, $Z(G)$ is abelian. □

Proposition 8 (Intersection of Subgroups is a Subgroup)
Let H and K be subgroups of a group G. Then their intersection

$$H \cap K = \{g \in G : g \in H \land g \in K\}$$

is also a subgroup of G.

Proof
Since H and K are subgroups, we have that $1 \in H$ and $1 \in K$ and hence $1 \in H \cap K$. Let $a, b \in H \cap K$. Since H and K are subgroups, we have that $ab \in H$ and $ab \in K$. Therefore, $ab \in H \cap K$. Similarly, since $a^{-1} \in H$ and $a^{-1} \in K$, $a^{-1} \in H \cap K$. By the Subgroup Test, $H \cap K$ is a subgroup of G. □

Proposition 9 (Finite Subgroup Test)
If H is a finite nonempty subset of a group G, then H is a subgroup if and only if H is closed under its operation.

This result says that if H is a finite nonempty subset, then we only need to prove that it is closed under its operation to prove that it is a subgroup. The other two conditions in the **Subgroup Test** are automatically implied.

Proof
The forward direction of the proof is trivially true, since H must satisfy the closure property for it to be a subgroup.

For the converse, since $H \neq \emptyset$, let $h \in H$. Since H is closed under its

operation, we have that

$$h, h^2, h^3, \dots$$

are all in H. Since H is finite, not all of the h^n's are distinct. Then, $\forall n \in \mathbb{N}$, there must $\exists m \in \mathbb{N}$ such that $h^n = h^{n+m}$. Then by Cycle Decomposition Theorem 6, $h^m = 1$ and so $1 \in H$. Also, because $1 = h^{m-1}h$, we have that $h^{-1} = h^{m-1}$, and thus the inverse of h is also in H. Therefore, H is a subgroup of G as requried. □

6 Lecture 6 May 14th 2018

6.1 Subgroups (Continued 2)

6.1.1 Alternating Groups

Recall that $\forall \sigma \in S_n$, with $\sigma \neq \varepsilon$, σ can be uniquely decomposed (up to the order) as disjoint cycles of length at least 2. We will now present a related concept.

Definition 13 (Transposition)

A **transposition** $\sigma \in S_n$ is a cycle of length 2, i.e. $\sigma = \begin{pmatrix} a & b \end{pmatrix}$, where $a, b \in \{1, ..., n\}$ and $a \neq b$.

Example 6.1.1
We have that[1]

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

Also, we can show that[2]

$$\begin{pmatrix} 1 & 2 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 2 & 5 \end{pmatrix} \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix} \qquad (6.1)$$

Observe that the factorization into transpositions are **not unique or disjoint**. However, the following property is true.

Theorem 10 (Parity Theorem)

If a permutations σ has 2 factorizations

$$\sigma = \gamma_1 \gamma_2 \ldots \gamma_r = \mu_1 \mu_2 \ldots \mu_s,$$

[1] If we apply the permutations on the right hand side, we have that

$$\begin{array}{ccccc} 1 & 2 & 3 & 4 & 5 \\ & & \downarrow & & \\ 1 & 2 & 3 & 5 & 4 \\ & & \downarrow & & \\ 1 & 4 & 3 & 5 & 2 \\ & & \downarrow & & \\ 2 & 4 & 3 & 5 & 1 \end{array}$$

[2]

Exercise 6.1.1
Show that Equation 6.1 is true.

Exercise 6.1.2
Play around with the same idea and create a few of your own transpositions. Note that you will only be able to get an odd number of tranpositions (why?).

where each γ_i and μ_j are transpositions, then $r \equiv s \mod 2$.

Proof

This is the bonus question in A2. Proof shall be included after the end of the assignment.

Definition 14 (Odd and Even Permutations)

A permutation σ is even (or odd) if it can be written as a product of an even (or odd) number of transpositions. By Parity Theorem 10, a permutation must either be even or odd, but not both.

Theorem 11 (Alternating Group)

For $n \geq 2$, let A_n denote the set of all even permutations in S_n. Then

1. $\varepsilon \in A_n$

2. $\forall \sigma, \tau \in A_n \ \sigma\tau \in A_n$ and $\exists \sigma^{-1} \in A_n$ such that $\sigma\sigma^{-1} = \varepsilon = \sigma^{-1}\sigma$

3. $|A_n| = \frac{1}{2}n!$

Note

*From items 1 and 2, we know that A_n si a subgroup of S_n. A_n is called the **alternating subgroup of degree** n.*

Proof

1. We have that $\varepsilon = \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix}$. Thus ε is even and so $\varepsilon \in A_n$.

2. $\forall \sigma, \tau \in A_n$, we may write

$$\sigma = \sigma_1\sigma_2\ldots\sigma_r \quad and$$
$$\tau = \tau_1\tau_2\ldots\tau_s,$$

where σ_i, τ_j are transpositions, and r, s are even integers. Then

$$\sigma\tau = \sigma_1\sigma_2\ldots\sigma_r\tau_1\tau_2\ldots\tau_s$$

is a product of $(r + s)$ transpositions, and thus $\sigma\tau$ is even. THus $\sigma\tau \in A_n$.

For the inverse, note that since σ_i is a transposition, we have that $\sigma_i^2 = \varepsilon$ and thus $\sigma_i^{-1} = \sigma_i$. It follows that

$$
\begin{aligned}
\sigma^{-1} &= (\sigma_1\sigma_2 \ldots \sigma_r)^{-1} \\
&= \sigma_r^{-1}\sigma_{r-1}^{-1} \ldots \sigma_2^{-1}\sigma_1^{-1} \\
&= \sigma_r\sigma_{r-1} \ldots \sigma_2\sigma_1
\end{aligned}
$$

which is an even permutation and

$$
\sigma\sigma^{-1} = \sigma_1\sigma_2 \ldots \sigma_r\sigma_r \ldots \sigma_2\sigma_1 = \varepsilon.
$$

Thus $\exists \sigma^{-1} \in A_n$ such that it is the inverse of σ.

3. Let O_n denote the set of odd permutations in S_n. Then we have $S_n = A_n \cup O_n$, and by the Parity Theorem, we have that $A_n \cap O_n = \varnothing$. Since $|S_n| = n!$, to prove that $|A_n| = \frac{1}{2}n!$, it suffices to show that $|A_n| = |O_n|$.

   Let $\gamma = \begin{pmatrix} 1 & 2 \end{pmatrix}$ and $f : A_n \to O_n$ such that $f(\sigma) = \gamma\sigma$. Since σ is even, $\gamma\sigma$ is odd, and so f is well-defined.

   Also, if $\gamma\sigma_1 = \gamma\sigma_2$, then by Cancellation Laws, $\sigma_1 = \sigma_2$, and hence f is injective.

   Finally, $\forall \tau \in O_n$, we have that $\gamma\tau = \sigma \in A_n$. Note that

   $$
   f(\sigma) = \gamma\sigma = \gamma\gamma\tau = \tau.
   $$

   Therefore, f is surjective.

   It follows that $|A_n| = |O_n|$. $\qquad\square$

For the proof of 3, we know that $|S_n| = n!$, which is twice of the suggested order of A_n. Since we took out the even permutations of S_n, we just need to make the rest of the permutations, the odd permutations, into a set and prove that A_n and this new set has the same size. One way to show this is by creating a bijection between the two.

Also, note that the set of all odd permutations of S_n is not a group, since

- there is no identity element in this set; and
- this set is not closed under map composition.

We have shown that ε is an even permutation, and so by the Parity Theorem, it cannot be an odd permutation, and there is only one identity in S_n. The set is not closed under map composition since if we compose two odd permutations, we would get an even permutation, which does not belong to this set.

Order of Elements

Notation

If G is a group and $g \in G$, we denote

$$
\langle\, g \,\rangle = \{g^k : k \in \mathbb{Z}\}.
$$

Note that $1 = g^0 \in \langle\, g\, \rangle$.

If $x = g^m, y = g^n \in \langle\, g\, \rangle$ where $m, n \in \mathbb{Z}$, then

$$xy = g^m g^n = g^{m+n} \in \langle\, g\, \rangle$$

and we have $\exists x^{-1} = g^{-m} \in \langle\, g\, \rangle$ such that

$$xx^{-1} = g^m g^{-m} = g^0 = 1.$$

Along with the **Subgroup Test**, we have the following proposition:

Proposition 12 (Cyclic Group as A Subgroup)

If G is a group and $g \in G$, then $\langle\, g\, \rangle$ is a subgroup of G.

Definition 15 (Cyclic Groups)

*Let G be a group and $g \in G$. Then we call $\langle\, g\, \rangle$ the **cyclic subgroup** of G generated by g. If $G = \langle\, g\, \rangle$ for some $g \in G$, then we say that G is a **cyclic group**, and g is a **generator** of G.*

7 Lecture 7 May 16th 2018

7.1 Subgroups (Continued 3)

7.1.1 Order of Elements (Continued)

Example 7.1.1

Consider $(\mathbb{Z}, +)$. Note that $\forall k \in \mathbb{Z}$, we can write $k = k \cdot 1 = \underbrace{1 + 1 + \ldots + 1}_{k\,times}$.

So we have that $(\mathbb{Z}, +) = \langle\, 1\, \rangle$. Similarly, we would have $(\mathbb{Z}, +) = \langle\, -1\, \rangle$.

*However, observe that $\forall n \in \mathbb{Z}$ with $n \neq \pm 1$, there is no $k \in \mathbb{Z}$ such that $k \cdot n = 1$. Therefore, ± 1 are the only **generators** of $\mathbb{Z}$.*

LET G be a group and $g \in G$. Suppose $\exists k \in \mathbb{Z}$ with $k \neq 0$ such that $g^k = 1$. Then $g^{-k} = (g^k)^{-1} = 1$. Thus wlog, we can assume that $k \geq 1$. By the **Well Ordering Principle**, $\exists n \in \mathbb{N}$ such that n is the smallest, such that $g^n = 1$.

With that, we may have the following definition:

Definition 16 (Order of an Element)

Let G be a group and $g \in G$. If n is the smallest positive integer such that $g^n = 1$, we say that the order of g is n, denoted by $o(g) = n$.

If no such n exists, then we say that g has infinite order and write $o(g) = \infty$.

Proposition 13 (Properties of Elements of Finite Order)

Let G be a group with $g \in G$ where $o(g) = n \in \mathbb{N}$. Then

1. $g^k = 1 \iff n|k$;

2. $g^k = g^m \iff k \equiv m \mod n$; and

3. $\langle g \rangle = \{1, g, g^2, ..., g^{n-1}\}$ where each g^i is distinct from others.

Proof

1. ($\Longleftarrow$) If $n|k$, then $k = nq$ for some $q \in \mathbb{Z}$. Then

$$g^k = g^{nq} = (g^n)^q = 1^q = 1$$

($\Longrightarrow$) Suppose $g^k = 1$. Since $k \in \mathbb{Z}$, the **Division Algorithm**, we can write $k = nq + r$ with $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Note $g^n = 1$. Thus

$$g^r = g^{k-nq} = g^k (g^n)^{-q} = 1 \cdot 1 = 1.$$

Since $0 \leq r < n$, we must have that $r = 0$. Thus $n|k$.

2. ($\Longrightarrow$) $g^k = g^m \implies g^{k-m} = 1 \overset{by\ 1}{\Longrightarrow} n|(k-m) \iff k \equiv m \mod n$

($\Longleftarrow$) $k \equiv m \mod n \implies \exists q \in \mathbb{Z}\ k = qnm$. The result follows from 1.

3. ($\supseteq$) is clear by definition of $\langle g \rangle = \{g^k : k \in \mathbb{Z}\}$.

To prove ($\subseteq$), let $x = g^k \in \langle g \rangle$ for some $k \in \mathbb{Z}$. By the **Division Algorithm**, $k = nq + r$ for some $q, r \in \mathbb{Z}$ and $0 \leq r < n$. Then

$$x = g^k = g^{nq+r} = g^{nq} g^r \overset{by\ 1}{=} g^r.$$

Since $0 \leq r < n$, we have that $x \in \{1, g, g^2, ..., g^{n-1}\}$. Thus $\langle g \rangle = \{1, g, g^2, ..., g^{n-1}\}$.

It remains to show that all the elements in $\langle g \rangle$ are distinct. Suppose $g^k = g^m$ for some $k, m \in \mathbb{Z}$ with $0 \leq k, m < n$. By 2, we have that $k \equiv m \mod 2$. Therefore, $k = m$.

We can also use 1 by the fact that $g^{k-m} = 1$ from assumption to complete the uniqueness proof.

$\square$

Proposition 14 (Property of Elements of Infinite Order)

Let G be a group, and $g \in G$ such that $o(g) = \infty$. Then

1. $g^k = 1 \iff k = 0$;

2. $g^k = g^r \iff k = m$;

3. $\langle\, g \,\rangle = \{..., g^{-2}, g^{-1}1, g, g^2, ...\}$ where each g^i is distinct from others.

Proof

It suffices to prove 1, since 2 easily becomes true with 1, and 2 $\implies$ 3.

1. $(\impliedby) \; g^0 = 1$

    $(\implies)$ *Suppose for contradiction that $g^k = 1$ for some $k \in \mathbb{Z} \; k \neq 0$. Then $g^{-k} = (g^k)^{-1} = 1$. Then we can assume that $k \geq 1$. This, however, implies that $o(g)$ is finite, which contradicts our assumption. Thus $k = 0$.*

2.
$$g^k = g^m \iff g^{k-m} = 1 \overset{by\ 1}{\iff} k - m = 0 \iff k = m$$

□

Proposition 15 (Orders of Powers of the Element)

Let G be a group, and $g \in G$ with $o(g) = n \in \mathbb{N}$. We have that

$$\forall d \in \mathbb{N} \;\; d \mid n \implies o(g^d) = \frac{n}{d}$$

Proof

Let $k = \frac{n}{d}$. Note that $(g^d)^k = g^n = 1$. It remains to show that k is the smallest such positive integer. Suppose $\exists r \in \mathbb{N} \;\; (g^d)^r = 1$. Since $o(g) = n$, then $n \mid dr$. Then $\exists q \in \mathbb{Z} \;\; dr = nq$ by definition of divisibility. $\because n = dk$ and $d \neq 0$, we have

$$dr = dkq \overset{d \neq 0}{\implies} r = kq \implies r > k \quad \because r, k \in \mathbb{N} \implies q \in \mathbb{N}$$

□

7.1.2   *Cyclic Groups*

Recall the definition of a cyclic groups.

Definition 17 (Cyclic Groups)

*Let G be a group and $g \in G$. Then we call $\langle\, g\, \rangle$ the **cyclic subgroup** of G generated by g. If $G = \langle\, g\, \rangle$ for some $g \in G$, then we say that G is a **cyclic group**, and g is a **generator** of G.*

Proposition 16 (Cyclic Groups are Abelian)

All cyclic groups are abelian.

Proof

Note that a cyclic group G is of the form $G = \langle\, g\, \rangle$. So

$$\forall a, b \in G \ \ \exists m, n \in \mathbb{Z} \ \ a = g^m \wedge b = g^n$$
$$a \cdot b = g^m g^n = g^{m+n} = g^{n+m} = g^n g^m = b \cdot a$$

□

8 Lecture 8 May 18th 2018

8.1 Subgroups (Continued 4)

8.1.1 Cyclic Groups (Continued)

Note

*Consider the converse of Proposition 16: Are abelian groups cyclic? **No!**
For example, $K_4 \cong C_2 \times C_2$ is abelian but not cyclic, since no one element
can generate the entire group.*

Proposition 17 (Subgroups of Cyclic Groups are Cyclic)
Every subgroup of a cyclic group is cyclic.

Proof

Let $G = \langle g \rangle$ and H be a subgroup of G.

$$H = \{1\} \implies H = \langle 1 \rangle$$
$$H \neq \{1\} \implies \exists k \neq 0 \in \mathbb{Z} \ \ g^k \in H$$
$$\implies g^{-k} \in H \quad (\because H \text{ is a group})$$

*We may assume that $k \in \mathbb{N}$. By the **Well Ordering Principle**, let
$m \in \mathbb{N}$ be the smallest positive integer such that $g^m \in H$. We will now
show that $H = \langle g^m \rangle$.*

$$g^m \in H \implies \langle\, g^m \,\rangle \subseteq H$$

$$\because H \subseteq G = \langle\, g \,\rangle \quad \forall h \in H \; \exists k \in \mathbb{Z} \; h = g^k$$

$$\textit{\color{green}Division Algorithm} : \exists q, r \in \mathbb{Z} \; 0 \le r < m \quad k = mq + r$$

$$h = g^k \implies g^r = g^{k-mq} = g^k (g^m)^{-q} = g^k(1) \in H$$

$$r \ne 0 \implies \exists 0 < r < m \quad g^r \in H \quad \text{\textreferencemark} \quad m \text{ is the smallest +ve integer}$$

$$\implies g^k \in \langle\, g^m \,\rangle \implies H \subseteq \langle\, g^m \,\rangle$$

Finally,

$$\langle\, g^m \,\rangle \subseteq H \;\wedge\; H \subseteq \langle\, g^m \,\rangle \implies H = \langle\, g^m \,\rangle$$

$$\square$$

Proposition 18 (Other generators in the same group)

Let $G = \langle\, g \,\rangle$ with $o(g) = n \in \mathbb{N}$. We have

$$G = \langle\, g^k \,\rangle \iff \gcd(k, n) = 1$$

If we have k such that $g^k \in G$, and k and n are coprimes, then g^k is also a generator of G.

Proof

For ($\implies$),

$$G = \langle\, g^k \,\rangle \implies g \in \langle\, g^k \,\rangle \implies \exists x \in \mathbb{Z} \quad g = g^{kx}$$

$$\implies 1 = g^{kx-1} \implies n \,|\, (kx - 1) \quad (\because \textit{\color{purple}Proposition } 13)$$

$$\implies \exists y \in \mathbb{Z} \quad kx - 1 = ny \quad (\because \textit{\color{green}Division Algorithm})$$

$$\implies 1 = kx + ny$$

Then

$$\because 1 \,|\, kx \;\wedge\; 1 \,|\, ny \;\wedge\; 1 = kx + ny$$

$$\gcd(k, n) = 1 \qquad (\because \textit{\color{green}gcd Characterization})$$

For ($\impliedby$), note that $g \in G \implies \langle\, g^k \,\rangle \subseteq G$. It suffices to show that

$G \subseteq \langle g^k \rangle$, *i.e.* $g \in \langle g^k \rangle$.

$$\gcd(k, n) = 1 \implies \exists x, y \in \mathbb{Z} \ \ 1 = kx + ny \quad (\because \textit{Bezout's Lemma})$$
$$\implies g = g^1 = g^{kx+ny} = (g^k)^x (g^n)^y = (g^k)^x \in \langle g^k \rangle$$

$\square$

Theorem 19 (Fundamental Theorem of Finite Cyclic Groups)

Let $G = \langle g \rangle$ *with* $o(g) = n \in \mathbb{N}$.

1. *H is a subgroup of* $G \implies \exists d \in \mathbb{N} \ \ d \mid n \ \ H = \langle g^d \rangle \implies |H| \mid n.$

2. $k \mid n \implies \langle g^{\frac{k}{n}} \rangle$ *is the unique subgroup of G of order k.*

This is a significant result that classifies the structure of a cyclic group (hence its name). The theorem tells us that for a group with finite order, it has only finitely many subgroups, and the order of each of these subgroups are multiples of n. Inversely, there are no subgroups of G where its order is some integer that does not divide n.
Note: It is clear that $d \in \mathbb{N}$ and $d \leq n$.
   In a sense, this theorem is more powerful than Proposition 17.

Proof

1. *Note*

$$\text{Proposition } 17 \implies \exists m \in \mathbb{N} \ \ H = \langle g^m \rangle$$

   Let $d = \gcd(m, n)$. *Want to show that* $H = \langle g^d \rangle$.

$$d = \gcd(m, n) \implies d \mid m \implies \exists k \in \mathbb{Z} \ \ m = dk$$
$$\implies g^m = g^{dk} = (g^d)^k \in \langle g^d \rangle \implies H \subseteq \langle g^d \rangle$$
$$d = \gcd(m, n) \implies \exists x, y \in \mathbb{Z} \ \ d = mx + ny \quad (\because \textit{Bezout's Lemma})$$
$$\implies g^d = g^{mx+ny} = (g^m)^x (g^n)^y = (g^m)^x (1) \in H$$
$$\implies \langle g^d \rangle \subseteq H$$
$$\therefore H = \langle g^d \rangle$$

   Note: $d = \gcd(m, n) \implies d \mid n \implies |H| = o(g^d) = \frac{n}{d}$
   $\because$ *Proposition* 15. *Thus* $|H| \mid n.$

2. *Let K be a subgroup of G with order k such that* $k \mid n$. *By 1, we have*
   $K = \langle g^d \rangle$ *with* $d \mid n$. *Note that*

$$k = |K| \overset{(1)}{=} o(g^d) \overset{(2)}{=} \frac{n}{d}$$

   where (1) *is by Proposition* 13 *and* (2) *is by Proposition* 15. *Thus*
   $d = \frac{n}{k}$ *and* $K = \langle g^{\frac{n}{k}} \rangle$

$\square$

9 Lecture 9 May 22nd 2018

9.1 Subgroups (Continued 5)

9.1.1 Examples of Non-Cyclic Groups

Example 9.1.1

The Klein 4-group is

$$K_4 = \{1, a, b, c\} \text{ where } a^2 = b^2 = c^2 = 1 \text{ and } ab = c.$$

We may also write

$$K_4 = \langle \, a, b : a^2 = 1 = b^2, \, ab = ba \, \rangle.$$

Note that we can replace (a, b) by (a, c) or (b, c).

Example 9.1.2

The symmetric group of degree 3 is

$$S_3 = \{\varepsilon, \sigma, \sigma^2, \tau, \tau\sigma, \tau\sigma^2\}$$

where $\sigma^3 = \varepsilon = \tau^2$ and $\sigma\tau = \tau\sigma^2$. We may also express S_3 as

$$S_3 = \langle \, \sigma, \tau : \sigma^3 = \varepsilon = \tau^2, \, \sigma\tau = \tau\sigma^2 \, \rangle$$

Definition 18 (Dihedral Group)

For $n \geq 2$, the *dihedral group* of order $2n$ is

$$D_{2n} = \{1, a, ..., a^{n-1}, b, ba, ..., b^{n-1}$$

where $a^n = 1 = b^2$ and $aba = b$. Note that a represents a rotation of $\frac{2\pi}{n}$ radians, and b represents a reflection through the x-axis

Recall from Assignment 1 that the dihedral group is a set of rigid motions for transforming a regular polygon back to its original position while changing the index of its vertices.

Example 9.1.3

We may write the dihedral group as

$$D_{2n} = \langle\, a, b : a^n = 1 = b^2, \, aba = b \,\rangle$$

Exercise 9.1.1

Prove the following:

1. $D_4 \cong K_4$

2. $D_6 \cong S_3$

9.2 *Normal Subgroup*

9.2.1 *Homomorphism and Isomorphism*

Definition 19 (Homomorphism)

Let G, H be groups. A mapping

$$\alpha : G \to H$$

is called a **homomorphism** *if $\forall a, b \in G$,*[1]

$$\alpha(ab) = \alpha(a)\alpha(b).$$

[1] Note that ab uses the operation of G while $\alpha(a)\alpha(b)$ uses the operation of H.

Example 9.2.1 (A classical example)

Consider the determinant map:

$$\det : GL_n(\mathbb{R}) \to \mathbb{R}^* \quad \text{given by } A \to \det A$$

Since

$$\det AB = \det A \det B$$

we have that the determinant map is a homomorphism.

Note that $\mathbb{R}^*$ is the set of real numbers that has a multiplicative inverse.

This is a classical example to show a homomorphism, especially since the group $GL_n(\mathbb{R})$ uses **matrix multiplication** while $\mathbb{R}^*$ uses regular **arithmetic multiplication**.

Proposition 20 (Properties of Homomorphism)

Let $\alpha : G \to H$ be a group homomorphism. Then

1. $\alpha(1_G) = 1_H$

2. $\forall g \in G \;\; \alpha(g^{-1}) = \alpha(g)^{-1}$

3. $\forall g \in G \; \forall k \in \mathbb{Z} \;\; \alpha(g^k) = \alpha(g)^k$

Proof

1. *Note that*

$$\alpha(1_G)\alpha(g) = \alpha(1_G \cdot g) = \alpha(g) = \alpha(g \cdot 1_G) = \alpha(g)\alpha(1_G)$$

Thus it must be that $\alpha(1_G) = 1_H$ for only the identity of H satisfies this equation.

2. *Since H is a group, we know that*

$$1_H = \alpha(g)\alpha(g)^{-1}.$$

Now with part 1, we have that

$$\alpha(g)\alpha(g^{-1}) = \alpha(gg^{-1}) = \alpha(1_G) = 1_H = \alpha(g)\alpha(g)^{-1}.$$

By Proposition 6, we have that $\alpha(g^{-1}) = \alpha(g)^{-1}$.

3. *This is simply a result of applying the definition repeatedly, which we can then perform an induction procedure to complete the proof.* □

Definition 20 (Isomorphism)

Let G, H be groups. Consider a mapping

$$\alpha : G \to H$$

*We say that α is an **isomorphism** if it is a homomorphism and bijective.*

*If α is an isomorphism, we say that G is **isomorphic to** to H, or that G and H are **isomorphic**, and denote that by $G \cong H$.*

Proposition 21 (Isomorphism as an Equivalence Relation)

1. **(Reflexive)** *The identity map $G \to G$ is an isomorphism.*

2. **(Symmetric)** *If $\sigma : G \to H$ is an isomorphism, then the inverse map $\sigma^{-1} : H \to G$ is also an isomorphism.*

3. **(Transitive)** *If $\sigma : G \rightarrow H$ and $\tau : H \rightarrow K$, then the composition map $\tau\sigma : G \rightarrow K$ is also an isomorphism.*

Proof

1. *The identity map is clearly bijective. For all $g_1, g_2 \in G$, we have that*

$$\alpha(g_1 g_2) = g_1 g_2 = \alpha(g_1)\alpha(g_2).$$

Thus the identity map is a homomorphism, and hence an isomorphism.

2. *Since σ is a bijective map, its inverse σ^{-1} exists and is also a bijective map. Since σ is bijective, we have that*

$$\forall h_1, h_2 \in H \;\; \exists! g_1, g_2 \in G \quad \sigma(g_1) = h_1, \, \sigma(g_2) = h_2.$$

Note that since σ has a bijective inverse, we also have

$$g_1 = \sigma^{-1}(h_1) \text{ and } g_2 = \sigma^{-1}(h_2).$$

Then since σ is a homomorphism,

$$\sigma^{-1}(h_1 h_2) = \sigma^{-1}(\sigma(g_1)\sigma(g_2)) = \sigma^{-1}(\sigma(g_1 g_2))$$
$$= g_1 g_2 = \sigma^{-1}(h_1)\sigma^{-1}(h_2).$$

3. *We know that the composition map of two bijective map is bijective. Let $g_1, g_2 \in G$, then since both τ and σ are homomorphisms*

$$\tau\sigma(g_1 g_2) = \tau(\sigma(g_1)\sigma(g_2)) = \tau\sigma(g_1)\tau\sigma(g_2),$$

where we note that $\sigma(g_1), \sigma(g_2) \in H$.

$\square$

Example 9.2.2

Let $\mathbb{R}^+ = \{r \in \mathbb{R} : r \geq 0\}$. Show that $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$.

Solution

Consider the map

$$\alpha : (\mathbb{R}, +) \rightarrow (\mathbb{R}^+, \cdot) \quad r \mapsto e^r,$$

where e is the natural exponent. Note that the exponential map from $\mathbb{R}$ to

$\mathbb{R}^+$ *is bijective[2]. Also, $\forall r, s \in \mathbb{R}$ we have that*

$$\alpha(r+s) = e^{r+s} = e^r e^s = \alpha(r)\alpha(s).$$

Therefore, α is an isomorphism and $(\mathbb{R}, +) \cong (\mathbb{R}^+, \cdot)$. □

Example 9.2.3

Show that $(\mathbb{Q}, +) \not\cong (\mathbb{Q}^*, \cdot)$.

Solution

Suppose, for contradiction, that $\tau : (\mathbb{Q}, +) \to (\mathbb{Q}^*, \cdot)$ is an isomorphism. In particular, we have that τ is onto. Then $\exists q \in \mathbb{Q}$ such that $\tau(q) = 2$. Let $\tau(\frac{q}{2}) = \alpha$. Since τ is an isomorphism, we have

$$\alpha^2 = \tau(\frac{q}{2})\tau(\frac{q}{2}) = \tau(\frac{q}{2} + \frac{q}{2}) = \tau(q) = 2.$$

But that implies that $\alpha = \sqrt{2}$, which is clearly not rational. Thus, we know that there is no such τ and

$$(\mathbb{Q}, +) \not\cong (\mathbb{Q}^*, \cdot)$$

as required. □

[2] The image of the map covers all positive real numbers while taking all real numbers, which is the perfect candidate as a map here.

9.2.2 *Cosets and Lagrange's Theorem*

Definition 21 (Coset)

Let H be a subgroup of a group G.

$$\forall a \in G \quad Ha = \{ha : h \in H\} \quad \text{is the right coset of H generated by a}$$

and

$$\forall a \in G \quad aH = \{ah : h \in H\} \quad \text{is the left coset of H generated by a}$$

Note

Note that $1H = H = H1$. Also, since $a1 = a$ and $1 \in H$, we have that $a \in aH$, and similarly so for $a \in Ha$.

In general, aH and Ha are not subgroups of G. See example

Also, in general, $aH \neq Ha$, since not all groups are abelian.

Proposition 22 (Properties of Cosets)

Let H be a subgroup of G, and let $a, b \in G$. Then

1. *$Ha = Hb \iff ab^{-1} \in H$. In particular, $Ha = H \iff a \in H$.*

2. *$a \in Hb \implies Ha = Hb$.*

3. *$Ha = Hb \veebar Ha \cap Hb = \emptyset$.[3] Then the distinct right cosets of H forms a partition of G.[4]*

We can create an analogued version of this proposition for the left cosets.

[3] $\veebar \equiv$ XOR

[4] Note that this is true because by definition, we iterate over all elements of G to construct the cosets of the subgroup H. The earlier part of this statement implies that cosets must be distinct (otherwise, they are the same set), and so if we take the union of these cosets, by iterating through all elements of G, we get that

$$\bigcup_{a \in G} Ha = G.$$

Summarizing the above argument, we observe that the distinct cosets partitions G.

Proof

1. *For ($\implies$),*

$$Ha = Hb \implies a = 1a \in Ha = Hb$$
$$\implies \exists h \in H \ a = hb$$
$$\implies ab^{-1} = h \in H.$$

For ($\impliedby$),

$$ab^{-1} \in H \implies \forall h \in H \ ha = h(ab^{-1})b \in Hb$$
$$\implies Ha \subseteq Hb$$
$$ab^{-1} \in H \implies (ab^{-1})^{-1} = ba^{-1} \in H$$
$$\implies \forall h \in H \ hb = h(ba^{-1})a \in Ha$$
$$\implies Hb \subseteq Ha$$

Let $b = 1$. Then

$$Ha = H \iff a \in H \qquad \because 1^{-1} = 1$$

2. *Note*

$$a \in Hb \implies \exists h \in H \ a = hb \implies ab^{-1} \in H \xRightarrow{\text{by 1}} Ha = Hb$$

3. *Trivially, if $Ha \cap Hb = \emptyset$, we are done.*

$$Ha \cap Hb \neq \emptyset$$
$$\implies \exists x \in Ha \cap Hb$$
$$\implies (x \in Ha \overset{by\ 1}{\implies} Hx = Hb) \wedge (x \in Hb \overset{by\ 1}{\implies} Hx = Hb)$$
$$\implies Ha = Hb$$

$\square$

By Proposition 22, we have that G can be written as a disjoint union of cosets of a subgroup H. We now define the following terminology that we shall use for the upcoming content.

Definition 22 (Index)

Let H be a subgroup of a group G. We call the number of disjoint cosets of H in G as the index of H in G, and denote this number by $[G : H]$.

10 Lecture 10 May 23rd 2018

10.1 Normal Subgroup (Continued)

10.1.1 Cosets and Lagrange's Theorem (Continued)

Theorem 23 (Lagrange's Theorem)

Let H be a subgroup of a **finite** group G. Then

$$|H| \,\big|\, |G| \text{ and } [G:H] = \frac{|G|}{|H|}$$

Proof

Since G is finite, there can only be finitely many cosets of H. Let $k = [G:H]$ and $Ha_1, Ha_2, ..., Ha_k$ be the distinct right cosets of H in G. By *Proposition 22*, we have that these cosets partition G, i.e.

$$G = \bigcup_{i=1}^{k} Ha_i.$$

Note that by the definition of a right coset, the map

$$H \to Hb \text{ defined by } h \mapsto hb$$

is a surjection from H to Hb. By *Cancellation Laws*, the map is injective, since if $hb_1 = hb_2$, then $b_1 = b_2$. Therefore, for $i = 1, ..., k$,

$$|H| = |Ha_i|.$$

Then we have

$$|G| = k\,|H| \implies |H|\,\Big|\,|G| \wedge [G:H] = k = \frac{|G|}{|H|}$$

□

Corollary 24

1. If G is a finite group and $g \in G$, then $o(g)\,\Big|\,G$.

2. If G is a finite group and $|G| = n$, then $g^n = 1$.

Proof

1. Let $H = \langle\, g\, \rangle$. Then by *Lagrange's Theorem 23*, $o(g) = |H|\,\Big|\,|G|$.

2. For some $g \in G$, let $o(g) = m \in \mathbb{Z} \setminus \{0\}$. Then by 1, $m \mid n$ and so $g^n = (g^m)^{\frac{n}{m}} = 1$.

□

Note

Let $n \in \mathbb{N} \setminus \{1\}$. *Euler's Totient Function*, or more generally written as *Euler's ϕ-function* is defined as

$$\phi(n) \equiv \Big|\big\{k \in \{1,...,n-1\} \,:\, \gcd(k,n) = 1\big\}\Big|. \qquad (10.1)$$

Note that the set $\mathbb{Z}_n^*$ under multiplication has a similar definition to the set on the RHS, since the only numbers from 1 to n that has an inverse are those that are coprime with n. Thus $\phi(n) = |\mathbb{Z}_n^*|$.

With *Corollary 24*, we have *Euler's Theorem* that states that

$$\forall a \in \mathbb{Z}\ \ \gcd(a,n) = 1 \implies a^{\phi(n)} \equiv 1 \mod n. \qquad (10.2)$$

If $n = p$ where p is some prime number, then Euler's Theorem implies *Fermat's Little Theorem*, i.e. $a^{p-1} \equiv 1 \mod p$.

Corollary 25

If p is prime, then every group G of order p is cyclic. In fact, $g = \langle\ g\ \rangle$ fpr $g \neq 1 \in G$. Hence, the only subgroup of G are $\{1\}$ and G itself.

Proof

*Let $g \in G$ such that $g \neq 1$. By Corollary 24, $o(g)\,|\,p$. Since $g \neq 1$ and p is prime, by **uniqueness of prime factorization**, it must be that $o(g) = p$. Thus we can write $G = \langle\ g\ \rangle$. If H is a subgroup of G, then by Lagrange's Theorem, we have $|H|\ |\ p$. Since p is prime, we either have $|H| = 1$ or p. In other words, we either have that $H = \{1\}$ or $H = G$, respectively.* □

Corollary 26

Let H and K be finite subgroups of G. If $\gcd(|H|,|K|) = 1$, then $H \cap K = \{1\}$.

Proof

Since $H \cap K$ is a subgroup of H and of K, by Lagrange's Theorem 23, $|H \cap K|\,\big|\,|H| \wedge |H \cap K|\,\big|\,|K|$. By assumption that $\gcd(|H|,|K|) = 1$, we have[1] that $|H \cap K| = 1$, and hence $|H \cap K| = \{1\}$. □

[1] $|H \cap K|$ is a common divisor for $|H|$ and $|K|$. But $\gcd(|H|,|K|) = 1$

10.1.2 *Normal Subgroup*

We have seen that given H is a subgroup of a group G and $g \in G$, gH and Hg are generally not the same.

Definition 23 (Normal Subgroup)

*Let H be a subgroup of a group G. If $\forall g \in G$, we have $Hg = gH$, then we say that H is a **normal subgroup** of G, and write*

$$H \triangleleft G$$

Example 10.1.1
$\{1\} \triangleleft G$ *and* $G \triangleleft G$.

Example 10.1.2
The center, $Z(G)$, *of a group* G *is an abelian group. By* Definition 23,

$$Z(G) \triangleleft G.$$

Example 10.1.3
If G *is abelian, then every subgroup of* G *is normal in* G.

Proposition (Normality Test)
Let H *be a subgroup of* G. *The following are equivalent:*

1. $H \triangleleft G$;

2. $\forall g \in G \quad gHg^{-1} \subseteq H$;

3. $\forall g \in G \quad gHg^{-1} = H$ [2]

[2] This means that

$H \triangleleft G \iff H$ is the only conjugate of H

11 Lecture 11 May 25th 2018

The following theorem is useful for A2. The proof is not provided in this lecture, but expect the corollary to be restated and proven in a later lecture.

Corollary

Let G be a finite group and $H, K \triangleleft G$, $H \cap K = \{1\}$ and $|H|\,|K| = |G|$. Then $G \cong H \times K$.

11.1 Normal Subgroup (Continued 2)

11.1.1 Normal Subgroup (Continued)

Note (Recall)

Recall the definition of a normal subgroup as in Definition 23. Let H be a subgroup of G. If $gH = Hg$ for all $g \in G$, then $H \triangleleft G$.

Proposition 27 (Normality Test)

Let H be a subgroup of a group G. The following are equivalent:

1. $H \triangleleft G$

2. $\forall g \in G \ \ gHg^{-1} \subseteq H$

3. $\forall g \in G \ \ gHg^{-1} = H$

Note

Note that item 3 is indeed a stronger statement that item 2. But since the statements are equivalent, while using the **Normality Test**, if we can show that item 2 is true, item 3 is automatically true.

Proof

(1) $\implies$ (2):

$$x \in gHg^{-1} \implies \exists h \in H \ \ x = ghg^{-1}$$
$$\implies \exists h_1 \in H \ \ gh = h_1 g \qquad \because gh \in gH = Hg$$
$$\implies x = ghg^{-1} = h_1 gg^{-1} = h_1 \in H$$
$$\implies gHg^{-1} \subseteq H$$

(2) $\implies$ (3):

$$(2) \implies \forall g \in G \ \ gHg^{-1} \subseteq H$$
$$\implies \exists g^{-1} \in G \ \ g^{-1}Hg \subseteq H$$
$$\implies H \subseteq gHg^{-1}$$
$$\overset{(2)}{\implies} gHg^{-1} = H$$

(3) $\implies$ (1):

$$(3) \implies \forall g \in G \ \ gHg^{-1} = H$$
$$\implies \forall x \in gH \ \ xg^{-1} \in gHg^{-1} = H$$
$$\implies x \in Hg \qquad \because gg^{-1} = 1$$
$$\implies gH \subseteq Hg$$

*Using a similar argument, we would have $Hg \subseteq Hg$. And so $gH = Hg$
as required.* $\square$

Example 11.1.1

Let $G = GL_n(\mathbb{R})$ and $H = SL_n(\mathbb{R})$.[1] For $A \in G$ and $B \in H$ we have

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

Thus $\forall A \in G, ABA^{-1} \in H$. By Proposition 27, $H \triangleleft G$, i.e. $SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R})$.[2]

[1] Recall Definition 8 and Definition 11.

[2]

Note
The normality is true for any field, not just $\mathbb{R}$.

Proposition 28 (Subgroup of Index 2 is Normal)

$$\forall H \text{ subgroup of } G \wedge [G : H] = 2 \implies H \triangleleft G$$

Proof

Let $a \in G$.

$$a \in H \implies aH = H = Ha$$

$$a \notin H \implies G = H \cup Ha \implies Ha = G \setminus H \quad \because Proposition\ 22$$

$$a \notin H \implies G = H \cup aH \implies aH = G \setminus H \quad \because Proposition\ 22$$

That implies that $aH = Ha$ for any $a \in G$. Hence, by Proposition 27, $H \triangleleft G$. □

Example 11.1.2

Let A_n be the Alternating Group contained by S_n.[3] By Proposition 28, since $[S_n : A_n] = 2$ because $S_n = A_n \cup O_n$ and O_n is a coset of A_n, we have that

$$A_n \triangleleft S_n.$$

[3] Recall the definition of alternating group from Theorem 11 and S_n from Definition 4

Example 11.1.3

Let

$$D_{2n} = \{1, a, a^2, ..., a^{n-1}, b, ba, ba^2, ..., ba^{n-1}\}$$

be the Dihedral Group of order $2n$. Since $[D_{2n} : \langle a \rangle] = 2$,[4] we have that

$$\langle a \rangle \triangleleft D_{2n} \quad \because Proposition\ 27.$$

[4] The coset of $\langle a \rangle$ is $b\langle a \rangle$.

LET H and K be subgroups of a group G. Recall an earlier discussion: $H \cap K$ is the largest subgroup contained in both H and K.

What is the "smallest" subgroup that contains both H and K? Since $H \cap K$ is the largest, it makes sense to think about $H \cup K$. However,

$$H \cup K \text{ is a subgroup of } G \iff H \subseteq K \vee K \subseteq H$$

While we know that $H \cup K$ can indeed be such a subgroup, the price of the restriction is too high, since it is overly restrictive.

A more "useful" construction turns out to be the **product** of the

subgroups.

Definition 24 (Product of Groups)

$$HK := \{hk \; : \; h \in H, k \in K\}$$

However, HK is not necessarily a subgroup. For example, for $h_1k_1, h_2k_2 \in HK$, it is not necessary that $h_1k_1h_2k_2 \in HK$, since k_1h_2 is not necessarily equal to h_2k_1.

Lemma 29 (Product of Groups as a Subgroup)
Let H and K be subgroups of G. The following are equivalent:

1. *HK is a subgroup of G*

2. *HK = KH* [5]

3. *KH is a subgroup of G*

[5] If one of H or K is normal, then the lemma immediately kicks in.

Proof
It suffices to prove (1) $\iff$ (2), since (1) $\iff$ (3) simply through exchanging H and K.

(1) $\implies$ (2): Let $kh \in KH$ such that $k \in K$ and $h \in H$. Their inverses are $k^{-1} \in K$ and $h^{-1} \in H$, since K and H are groups. Note that

$$kh = (h^{-1}k^{-1})^{-1} \in HK \quad \because HK \text{ is a subgroup of } G.$$

Therefore $kh \in HK$, which implies $KH \subseteq HK$. By a similar argument, we can arrive at $HK \subseteq KH$ and so $HK = KH$.

(2) $\implies$ (1): Note that $1 = 1 \cdot 1 \in HK$. For all $hk \in HK$, $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$. For $h_1k_1, h_2k_2 \in HK$, note that $k_1h_2 \in KH = HK$, so there exists $hk \in HK$ such that $k_1h_2 = hk$. Therefore,

$$h_1k_1h_2k_2 = h_1hkk_2 \in HK.$$

*By the **Subgroup Test**, HK is a subgroup of G.* $\qquad\square$

Proposition 30 (Product of Normal Subgroups is Normal)

Let H and K be subgroups of G.

1. *$H \triangleleft G \vee K \triangleleft G \implies HK = KH$ is a subgroup of G*

2. *$H, K \triangleleft G \implies HK = KH \triangleleft G$*

Proof

1. *Without loss of generality, suppose $H \triangleleft G$. Then*

$$HK = \bigcup_{k \in K} Hk = \bigcup_{k \in K} kH = KH \qquad (11.1)$$

   By Lemma 29, $HK = KH$ is a subgroup of G.

2. *Suppose $H, K \triangleleft G$. Then*

   $$\forall g \in G \ \ \forall hk \in HK \quad g^{-1}(hk)g = (g^{-1}hg)(g^{-1}kg) \in HK$$

   Thus $gHKg^{-1} \subseteq HK$. Thus by Proposition 27, we have that $HK \triangleleft G$.

   $\square$

Note

Note that Equation (11.1) is a weaker statement than the regular normality that we have defined, since it only requires all elements of K to work instead of the entire G.

With that, we define the following notion:

Definition 25 (Normalizer)

*Let H be a subgroup of G. The **normalizer of** H, denoted by $N_G(H)$, is defined to be*

$$N_G(H) := \{g \in G : gH = Hg\}$$

Note

By the above definition, we immediately see that $H \triangleleft G \iff N_G(H) = G$ by Equation (11.1). Observe that since we only needed $kH = Hk$ in Equation (11.1) for all $k \in K$, we have that $k \in N_G(H)$.

Corollary 31

Let H and K be subgroups of a group G.

$$K \subseteq N_G(H) \lor H \subseteq N_G(K) \implies HK = KH \text{ is a subgroup of } G$$

The proof of Corollary 31 is embedded in the proof of Proposition 30 while using the definition of a **normalizer**.

12 *Lecture 12 May 28th 2018*

12.1 *Normal Subgroup (Continued 3)*

12.1.1 *Normal Subgroup (Continued 2)*

Theorem 32

If $H \triangleleft G$ and $K \triangleleft G$ satisfy $H \cap K = \{1\}$, then

$$HK \cong H \times K$$

Proof

Claim 1:

$$H \triangleleft G \ \wedge \ K \triangleleft G \ \wedge \ H \cap K = \{1\} \implies \forall h \in H \ \forall k \in K \quad hk = kh$$

Consider $x = hkh^{-1}k^{-1}$. Note that since $H \triangleleft G$, by *Proposition 27*, we have that $\forall g \in G$, $gHg^{-1} = H$. Then $khk^{-1} \in kHk^{-1} = H$. Thus $x = h(kh^{-1}k^{-1}) \in H$. Using a similar argument, we can get that $x \in K$. Since $x \in H \cap K = \{1\}$, we have that $hkh^{-1}k^{-1} = 1$, we have that $hk = kh$ as claimed.

Note that since $H \triangleleft G$, by *Proposition 30*, we have that HK is a subgroup of G.[1] Define $\sigma : H \times K \to HK$ by

$$\forall h \in H \ \forall k \in K \qquad \sigma\big((h,k)\big) = hk$$

[1] We do not need the more powerful statement that says that HK is a normal subgroup.

Claim 2: σ is an isomorphism.

Let $(h,k), (h_1, k_1) \in H \times K$. By Claim 1, note that $h_1 k = k h_1$. Therefore,

$$\sigma\big((h,k) \cdot (h_1, k_1)\big) = \sigma\big((hh_1, kk_1)\big) = hh_1 kk_1$$
$$= hkh_1 k_1 = \sigma\big((h,k)\big)\sigma\big((h_1, k_1)\big)$$

Thus we see that σ is a group homomorphism. Note that by the definition of HK, σ is a surjection. Also, if $\sigma\big((h,k)\big) = \sigma\big((h_1, k_1)\big)$, we have that

$$hk = h_1 k_1 \implies h_1^{-1} h = k_1 k^{-1} \in H \cap K = \{1\}$$
$$\implies h_1^{-1} h = 1 = k_1 k^{-1} \implies h_1 = h \wedge k_1 = k.$$

Thus σ is an injection, and hence σ is bijective. Therefore, σ is an isomorphism. This proves that $HK \cong H \times K$. □

An immediate result is the corollary that we were given in the last class but not proven.

Corollary 33

Let G be a finite group, $H, K \triangleleft G$ such that $H \cap K = \{1\}$ and $|H| \, |K| = |G|$. Then $G \cong H \times K$.

Example 12.1.1

Let $m, n \in \mathbb{N}$ with $\gcd(m,n) = 1$. Let G be a cyclic group of order mn. Write $G = \langle a \rangle$ with $o(a) = mn$. Let $H = \langle a^n \rangle$ and $K = \langle a^m \rangle$. Then we have

$$|H| = o(a^n) = m \wedge |K| = o(a^m) = n.$$

It follows that $|H| \, |K| = mn = |G|$. Note that $H \cong C_m$ and $K \cong C_n$. Since $\gcd(m,n) = 1$, by Corollary 26, we have that $H \cap K = \{1\}$.

Also, since G is cyclic and thus abelian, we have that $H, K \triangleleft G$. Then by Corollary 33, we have that $G \cong C_{mn} \cong C_m \times C_n$.

12.2 Isomorphism Theorems

12.2.1   *Quotient Groups*

Let G be a group and K a subgroup of G. Given a set

$$\{Ka \, : \, a \in G\},$$

how can we create a group out of it?

A "natural" way to define an operation on the set of right cosets above is

$$\forall a, b \in G \qquad Ka * Kb = Kab. \qquad\qquad (\dagger)$$

Note that it is entirely possible that for $a_1 \neq a$ and $b_1 \neq b$, we have $Ka = Ka_1$ and $Kb = Kb_1$. In order for Equation ($\dagger$) to make sense as an operation, it is necessary that

$$Ka = Ka_1 \wedge Kb = Kb_1 \implies Kab = Ka_1 b_1.$$

If the condition is satisfied, we say that the "multiplication" $KaKb$ is well-defined.

Lemma 34 (Multiplication of Cosets of Normal Subgroups)

Let K be a subset of G. The following are equivalent:

1. $K \triangleleft G$;

2. $\forall a, b \in G \ \ KaKb = Kab$ is well-defined.

Proof

(1) $\implies$ (2) *Suppose $K \triangleleft G$. Suppose $Ka = Ka_1$ and $Kb = Kb_1$. Then $aa_1^{-1} \in K$ and $bb_1^{-1} \in K$. To show that $Kab = Ka_1 b_1$, it suffices to show that $(ab)(a_1 b_1)^{-1} \in K$. Note that since $K \triangleleft G$, we have that $aKa^{-1} = K$. Therefore,*

$$ab(a_1 b_1)^{-1} = ab(b_1^{-1} a_1^{-1}) = a(bb_1^{-1})a_1^{-1}$$
$$= (a(bb_1^{-1})a^{-1})(aa_1^{-1}) \in K.$$

Therefore $Kab = Ka_1 b_1$ as required.

(2) $\implies$ (1) *If $a \in G$, we need to show that $\forall k \in K, aka^{-1} \in K$. Since $Ka = Ka$ and $Kk = K(1)$[2], by (2), we have that $Kak = Ka(1)$, i.e. $Kak = Ka$. Thus $aka^{-1} = 1 \in K$, implying that $aKa^{-1} \subseteq K$ and hence*

[2] This is cause 1 is in the same coset.

$K \triangleleft G.$ □

---

13 Lecture 13 May 30 2018

13.1 Isomorphism Theorems (Continued)

13.1.1 Quotient Groups (Continued)

Proposition 35

Let $K \triangleleft G$ and write $G/K = \{Ka \ : \ a \ in G\}$ for the set of cosets of K.

1. G/K is a group under the operation $KaKb = Kab$.

2. The mapping $\phi : G \to G/K$ given by $\phi(a) = Ka$ is a surjective homomorphism.[1]

3. If $[G : K]$ is finite, then $\left| G/K \right| = [G : K]$. In particular, if $|G|$ is finite, then $\left| G/K \right| = \frac{|G|}{|K|}$.

---

[1]

Exercise 13.1.1
Is ϕ injective?

Solution
We know that we cannot uniquely express a coset, since for $a, b \in Ka$ such that $a \neq b$, we have that $Ka = Kb$.

Proof

1. By *Lemma 34*, the operation is well-defined, and G/K is closed under the operation. The identity of G/K is $K = K(1)$ since $\forall Ka \in G/K$,

$$KaK(1) = Ka = K(1)Ka.$$

Also, since
$$KaKa^{-1} = K(1) = Ka^{-1}Ka,$$

the inverse of Ka is Ka^{-1}. Finally, by associativity of G, we have that

$$Ka(KbKc) = Kabc = (KaKb)Kc.$$

It follows that G/K is a group.

2. *Clearly, ϕ is surjective. For $a, b \in G$,*

$$\phi(ab) = Kab = KaKb = \phi(a)\phi(b).$$

Thus ϕ is a surjective homomorphism.

3. *If $[G : K]$ is finite, then by definition of the index $[G : K]$, we have that $[G : K] = \left|G/K\right|$. Also, if $|G|$ is finite, then by* Theorem 23,

$$\left|G/K\right| = [G : K] = \frac{|G|}{|K|}.$$

$\square$

Definition 26 (Quotient Group)

*Let $K \triangleleft G$. The group G/K of all cosets of K in G is called the **quotient group** of G by K. Also, the mapping*

$$\phi : G \to G/K \text{ defined by } a \mapsto Ka$$

*is called the **coset** (pr **quotient**) **map**.*

13.1.2 *Isomorphism Theorems*

Definition 27 (Kernel and Image)

*Let $\alpha : G \to H$ be a group homomorphism. The **kernel** of α is defined by*

$$\ker \alpha := \{g \in G : \alpha(g) = 1_H\} \subseteq G$$

and the image of α is defined by

$$\operatorname{im} \alpha := \alpha(G) = \{\alpha(g) : g \in G\} \subseteq H.$$

Proposition 36

Let $\alpha : G \to H$ be a group homomorphism.

1. *$\operatorname{im} \alpha$ is a subgroup of H*

2. $\ker \alpha \lhd G$

Proof

1. Note that $1_H = \alpha(1_G) \in \alpha(G)$ (i.e. the identity is in $\operatorname{im} \alpha$). Also, for $h_1 = \alpha(g_1)$ and $h_2 = \alpha(g_2)$ in $\alpha(G)$ and $h_1, h_2 \in H$, we have

$$h_1 h_2 = \alpha(g_1)\alpha(g_2) = \alpha(g_1 g_2) \in \alpha(G).$$

(i.e. $\operatorname{im} \alpha$ i closed under its operation). By *Proposition 20*, $\alpha(g)^{-1} = \alpha(g^{-1}) \in \alpha(G)$ (i.e. the inverse of an element is also in $\operatorname{im} \alpha$). Thus by the **Subgroup Test**, we have that $\operatorname{im} \alpha$ is a subgroup of H.

2. For $\ker \alpha$, $\alpha(1_G) = 1_H$. For $k_1, k_2 \in \ker \alpha$, we have

$$\alpha(k_1 k_2) = \alpha(k_1)\alpha(k_2) = 1 \cdot 1 = 1.$$

Also,
$$\alpha(k_1^{-1}) = \alpha(k_1)^{-1} = 1^{-1} = 1.$$

By the **Subgroup Test**, $\ker \alpha$ is a subgroup of G.

If $g \in G$ and $k \in \ker \alpha$, then

$$\alpha(gkg^{-1}) = \alpha(g)\alpha(k)\alpha(g^{-1}) = \alpha(g)\alpha(g^{-1}) = 1.$$

Thus by *Proposition 27*, $\ker \alpha \lhd G$.

$\square$

Example 13.1.1

Consider the determinant map

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

Then $\ker \det = SL_n(\mathbb{R})$. Then $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$, as proven before.

Example 13.1.2

*Define the **sign of a permutation** $\sigma \in S_n$ by*

$$\operatorname{sgn}(\sigma) = \begin{cases} 1 & \text{if } \sigma \text{ is even;} \\ -1 & \text{if } \sigma \text{ is odd.} \end{cases}$$

Then the sign mapping, $\operatorname{sgn} : S_n \to \{\pm 1\}$ defined by $\sigma \mapsto \operatorname{sgn}(\sigma)$ is a

homomorphism.[2] *Also,* $\ker \mathrm{sgn} = A_n$. *Thus, we have* $A_n \lhd S_n$, *as proven before.*

[2] Think about why. It's quite straightforward using the defintion.

Proposition 37 (Normal Subgroup as the Kernel)

If $K \lhd G$, *then* $K = \ker \phi$ *where* $\phi : G \to G/K$ *is the coset map.*

Proof

Recall that $\phi : G \to G/K$ *is defined by* $g \mapsto Kg, \forall g \in G$, *and is a group homomorphism. By* Proposition 22, *we have*

$$Kg = K = K1 \iff g \in K.$$

Thus $K = \ker \phi$. □

Theorem 38 (First Isomorphism Theorem)

Let $\alpha : G \to H$ *be a group homomorphism. We have*

$$G/\ker \alpha \cong \mathrm{im}\,\alpha$$

Proof

Let $K = \ker \alpha$. *Since* $K \lhd G$ *(by* Proposition 36*),* G/K *is a group. Let*[3]

$$\bar{\alpha} : G/K \to \mathrm{im}\,\alpha \text{ be defined by } Kg \mapsto \alpha(g)$$

Note that

$$Kg = Kg_1 \iff gg_1^{-1} \in K \iff \alpha(gg_1^{-1}) = 1 \iff \alpha(g) = \alpha(g_1).$$

Thus $\bar{\alpha}$ *is well-defined and injective. Clearly,* $\bar{\alpha}$ *is surjective. It remains to show that* $\bar{\alpha}$ *is a group homomorphism.* $\forall g, h \in G$, *we have*

$$\bar{\alpha}(KgKh) = \bar{\alpha}(Kgh) = \alpha(gh) = \alpha(g)\alpha(h) = \bar{\alpha}(Kg)\bar{\alpha}(Kh).$$

Therefore, we have that $\bar{\alpha}$ *is an isomorphism and hence* $G/\ker \alpha \cong \mathrm{im}\,\alpha$ *as desired.* □

[3] We must check that the function is well-defined, since cosets are not uniquely represented and so it is likely that a constructed mapping is not well-defined.

14 Lecture 14 Jun 01 2018
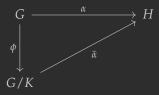
14.1 Isomorphism Theorems (Continued 2)

14.1.1 Isomorphism Theorems (Continued)

Note (Recall)

In *First Isomorphism Theorem 38*, we had that for a group homomorphism $\alpha : G \to H$ where G and H are groups,

$$G/\!\ker\alpha \cong \operatorname{im}\alpha$$

Now let $\alpha : G \to H$ be a group homomorphism, $K = \ker\alpha$, $\phi : G \to G/\!K$ be the coset map, and $\bar{\alpha}$ be as defined in the proof of *First Isomorphism Theorem 38*. We then have the following commutative diagram to illustrate the relationship between the three groups.

A natural question to ask after seeing the relationship is: Is $\bar{\alpha}\phi = \alpha$? If it is, is the definition of $\bar{\alpha}$ unique? The answer is: **YES!** on both accounts.

Proof

Let $g \in G$. Then

$$\bar{\alpha}\phi(g) = \bar{\alpha}\big(\phi(g)\big) = \bar{\alpha}(Kg) = \alpha(g)$$

Suppose $\alpha = \beta\phi$ where $\beta : {}^{G}\!/_{K} \to H$. Then

$$\beta(Kg) \overset{(1)}{=} \beta(\phi(g)) = \beta\phi(g) = \alpha(g) = \bar{\alpha}(Kg)$$

where (1) is because ϕ is surjective by Proposition 35. Therefore, we observe that $\beta = \bar{\alpha}$ for any $Kg \in {}^{G}\!/_{K}$. This proves that $\bar{\alpha}$ is the unique homomorphism such that ${}^{G}\!/_{K} \to H$ satisfying $\alpha = \bar{\alpha}\phi$. $\square$

With that, we have the following proposition.

Proposition 39

Let $\alpha : G \to H$ be a group homomorphism, where G and H are groups. Let $K = \ker\alpha$. Then α factors uniquely as $\alpha = \bar{\alpha}\phi<$ where $\phi : G \to {}^{G}\!/_{K}$ is the coset map and $\bar{\alpha} : GK \to H$ is defined by

$$\bar{\alpha}(Kg) = \alpha(g).$$

Note that ϕ is surjective and $\bar{\alpha}$ is injective.

*In such a scenario, we also say that α **factors through** ϕ.[1]*

[1] Reference for the terminology: `https://math.stackexchange.com/questions/68941/terminology-a-homomorphism-factors`.

Example 14.1.1

Let $G = \langle g \rangle$ be a cyclic group. Consider $\alpha : \mathbb{Z} \to G$, defined as

$$\forall k \in \mathbb{Z} \quad \alpha(k) = g^{k},$$

which is a group homomorphism. By definition, α is surjective. Note that

$$\ker\alpha = \{k \in \mathbb{Z} : g^{k} = 1\}.$$

We have, therefore, two cases to consider.

- *G is an infinite group*
  This would imply that $\ker\alpha = \{0\}$ since only $g^{0} = 1$. Then by First Isomorphism Theorem 38, we have that

  $$\mathbb{Z}\!/_{\ker\alpha} \cong G$$

  Note that[2]

  $$\mathbb{Z}\!/_{\ker\alpha} = \{(\ker\alpha)k : k \in \mathbb{Z}\} = \{0 + k : k \in \mathbb{Z}\} = \mathbb{Z}.$$

[2] We are assuming that the group $\mathbb{Z}$ here works under the operation of addition, otherwise, if we employ multiplication, then $\mathbb{Z}$ would not be a group and α would not be a group homomorphism.

Therefore

$$\mathbb{Z} \cong G$$

- *G is a finite group*
  Suppose that $|G| = o(g) = n \in \mathbb{N}$, which is valid by Corollary 24. Then

$$\ker \alpha = n\mathbb{Z}$$

  Then by the First Isomorphism Theorem 38, we have

$$\mathbb{Z}/n\mathbb{Z} \cong G.$$

  Observe that

$$\mathbb{Z}/n\mathbb{Z} = \{n\mathbb{Z} + k : k \in \mathbb{Z}\} = \mathbb{Z}_n$$

  since the set in the middle is the definition of the set of integers modulo n.[3] Therefore,

$$\mathbb{Z}_n \cong G$$

Therefore, we have that

$$\mathbb{Z} \cong G \text{ or } \mathbb{Z}_{o(g)} \cong G$$

Theorem 40 (Second Isomorphism Theorem)
Let H and K be the subgroups of a group G with $K \triangleleft G$. Then

- *HK is a subgroup of G;*

- *$K \triangleleft HK$;*

- *$H \cap K \triangleleft H$; and*

- *$HK/K \cong H/H \cap K$.*

Proof
Since $K \triangleleft G$, by Lemma 29 and Proposition 30, we have that $HK = KH$ is a subgroup of G. Consequently, we have $K \triangleleft HK$, since K is clearly a subgroup of HK and $K \triangleleft G$, and so $\forall x \in HK \subseteq G$ we have that $gK = Kg$.

  Consider $\alpha : H \to HK/K$, defined by[4]

$$\alpha(h) = Kh$$

Now if $x = kh \in KH = HK$, then

$$Kx = K(kh) = Kh = \alpha(h).$$

Therefore, we have that α is surjective. Now by Proposition 22, observe that

$$\ker \alpha = \{h \in H : Kh = K\} = \{h \in Hh \in K\} = H \cap K.$$

Then by the First Isomorphism Theorem, we have that

$$HK/K \cong H/H \cap K.$$

Since we have that $\ker \alpha = H \cap K$ and $\ker \alpha \triangleleft H$, we have that $H \cap K \triangleleft H$. □

Theorem 41 (Third Isomorphism Theorem)

Let $K \subseteq H \subseteq G$ be groups, with $K \triangleleft G$ and $H \triangleleft G$. Then

$$H/K \triangleleft G/K \text{ and } \left(G/K\right) / \left(H/K\right) \cong G/H$$

Proof

Define $\alpha : G/K \to G/H$ by $\alpha(Kg) = Hg$ for all $g \in G$. Clearly, α is surjective. Now if $Kg = Kg_1$, for any $g, g_1 \in G$, then $gg_1 \in K \subseteq H$. Therefore, $Hg = Hg_1$. Thus α is well-defined. Now

$$\ker \alpha = \{Kg : Hg = H\} = \{Kg : g \in H\} = H/K.$$

Then

$$H/K = \ker \alpha \triangleleft G/K.$$

By the First Isomorphism Theorem, we have

$$\left(G/K\right) / \left(H/K\right)$$

as required. □

14.2 *Group Actions*

One reason that we are interested in the symmetric group is that they contain all finite groups.

Theorem (Cayley's Theorem)

If G is a finite group of order n, then G is isomorphic to a subgroup of S_n.

---

15 *Index*

$M_n(\mathbb{R})$	set of $n \times n$ matrices over $\mathbb{R}$
$\mathbb{Z}_n^*$	set of integers modulo n; each element has its multiplicative inverse
S_n	symmetry group of degree n
D_{2n}	dihedral group of degree n; a subset of S_n
K_n	Klein n-group
A_n	alternating group of degree n; a subset of S_n
$|D_{2n}|$	order of the dihedral group; the size of the dihedral group
$\begin{pmatrix} 1 & 2 & \dots & n \end{pmatrix}$	An n-cycle
$\det A$	determinant of matrix A
$GL_n(\mathbb{R})$	general linear group of degree n; the set that contains elements of $M_n(\mathbb{R})$ with non-zero determinant
$SL_n(\mathbb{R})$	special linear group of order n; the set that contains elements of $GL_n(\mathbb{R})$ with determinant of 1
$Z(G)$	center of group G
$\langle\, g\, \rangle$	cyclic group with generator g
$n \mid d$	n divides d
$H \triangleleft G$	H is a normal subgroup of G
G/H	quotient group of G by $H \triangleleft G$
$\ker \alpha$	kernel of α
$\operatorname{im} \alpha$	image of α