





# Table of Contents

<b>1</b>	<b>Lecture 1 May 02nd 2018</b>	<b>13</b>
1.1	Introduction . . . . .	13
1.1.1	Numbers . . . . .	13
1.1.2	Matrices . . . . .	14
<b>2</b>	<b>Lecture 2 May 04th 2018</b>	<b>17</b>
2.1	Introduction (Continued) . . . . .	17
2.1.1	Permutations . . . . .	17
<b>3</b>	<b>Lecture 3 May 07th 2018</b>	<b>23</b>
3.1	Groups . . . . .	23
3.1.1	Groups . . . . .	23
<b>4</b>	<b>Lecture 4 May 09 2018</b>	<b>29</b>
4.1	Groups (Continued) . . . . .	29
4.1.1	Groups (Continued) . . . . .	29
4.1.2	Cayley Tables . . . . .	30
4.2	Subgroups . . . . .	32
4.2.1	Subgroups . . . . .	32
<b>5</b>	<b>Lecture 5 May 11th 2018</b>	<b>35</b>
5.1	Subgroups (Continued) . . . . .	35
5.1.1	Subgroups (Continued) . . . . .	35
<b>6</b>	<b>Lecture 6 May 14th 2018</b>	<b>39</b>
6.1	Subgroups (Continued 2) . . . . .	39
6.1.1	Alternating Groups . . . . .	39
6.1.2	Order of Elements . . . . .	42
<b>7</b>	<b>Lecture 7 May 16th 2018</b>	<b>43</b>
7.1	Subgroups (Continued 3) . . . . .	43
7.1.1	Order of Elements (Continued) . . . . .	43

7.1.2	Cyclic Groups . . . . .	46
<b>8</b>	<b>Lecture 8 May 18th 2018</b>	<b>47</b>
8.1	Subgroups (Continued 4) . . . . .	47
8.1.1	Cyclic Groups (Continued) . . . . .	47
<b>9</b>	<b>Lecture 9 May 22nd 2018</b>	<b>51</b>
9.1	Subgroups (Continued 5) . . . . .	51
9.1.1	Examples of Non-Cyclic Groups . . . . .	51
9.2	Normal Subgroup . . . . .	52
9.2.1	Homomorphism and Isomorphism . . . . .	52
9.2.2	Cosets and Lagrange's Theorem . . . . .	55
<b>10</b>	<b>Lecture 10 May 23rd 2018</b>	<b>59</b>
10.1	Normal Subgroup (Continued) . . . . .	59
10.1.1	Cosets and Lagrange's Theorem (Continued) . . . . .	59
10.1.2	Normal Subgroup . . . . .	61
<b>11</b>	<b>Lecture 11 May 25th 2018</b>	<b>63</b>
11.1	Normal Subgroup (Continued 2) . . . . .	63
11.1.1	Normal Subgroup (Continued) . . . . .	63
<b>12</b>	<b>Lecture 12 May 28th 2018</b>	<b>69</b>
12.1	Normal Subgroup (Continued 3) . . . . .	69
12.1.1	Normal Subgroup (Continued 2) . . . . .	69
12.2	Isomorphism Theorems . . . . .	70
12.2.1	Quotient Groups . . . . .	71
<b>13</b>	<b>Lecture 13 May 30th 2018</b>	<b>73</b>
13.1	Isomorphism Theorems (Continued) . . . . .	73
13.1.1	Quotient Groups (Continued) . . . . .	73
13.1.2	Isomorphism Theorems . . . . .	74
<b>14</b>	<b>Lecture 14 Jun 01st 2018</b>	<b>79</b>
14.1	Isomorphism Theorems (Continued 2) . . . . .	79
14.1.1	Isomorphism Theorems (Continued) . . . . .	79
<b>15</b>	<b>Lecture 15 Jun 04th 2018</b>	<b>85</b>
15.1	Group Action . . . . .	85
15.1.1	Cayley's Theorem . . . . .	85
15.1.2	Group Action . . . . .	87
<b>16</b>	<b>Lecture 16 Jun 06th 2018</b>	<b>89</b>

16.1	Group Action (Continued) . . . . .	89
16.1.1	Group Action (Continued) . . . . .	89
<b>17</b>	<b>Lecture 17 Jun 08th 2018</b>	<b>93</b>
17.1	Group Action (Continued 2) . . . . .	93
17.1.1	Group Action (Continued 2) . . . . .	93
<b>18</b>	<b>Lecture 18 Jun 13th 2018</b>	<b>97</b>
18.1	Finite Abelian Groups . . . . .	97
18.1.1	Primary Decomposition . . . . .	97
18.1.2	p-Groups . . . . .	99
<b>19</b>	<b>Lecture 19 Jun 15th 2018</b>	<b>101</b>
19.1	Finite Abelian Groups (Continued) . . . . .	101
19.1.1	p-Groups (Continued) . . . . .	101
<b>20</b>	<b>Lecture 20 Jun 18th 2018</b>	<b>105</b>
20.1	Finite Abelian Groups (Continued 2) . . . . .	105
20.1.1	p-Groups (Continued 2) . . . . .	105
20.2	Rings . . . . .	107
20.2.1	Rings . . . . .	107
<b>21</b>	<b>Lecture 21 Jun 20th 2018</b>	<b>109</b>
21.1	Rings (Continued) . . . . .	109
21.1.1	Rings (Continued) . . . . .	109
21.1.2	Subring . . . . .	112
<b>22</b>	<b>Lecture 22 Jun 22nd 2018</b>	<b>115</b>
22.1	Ring (Continued 2) . . . . .	115
22.1.1	Ideals . . . . .	115
<b>23</b>	<b>Lecture 23 Jun 25th 2018</b>	<b>121</b>
23.1	Ring (Continued 3) . . . . .	121
23.1.1	Ideals (Continued) . . . . .	121
23.1.2	Isomorphism Theorems for Rings . . . . .	121
<b>24</b>	<b>Lecture 24 Jun 27th 2018</b>	<b>127</b>
24.1	Rings (Continued 4) . . . . .	127
24.1.1	Isomorphism Theorems for Rings (Continued) . .	127
24.2	Commutative Rings . . . . .	130
24.2.1	Integral Domain and Fields . . . . .	130
<b>25</b>	<b>Index</b>	<b>133</b>

















# 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:

$$\begin{aligned}\mathbb{N} &= \{1, 2, 3, \dots\} & \mathbb{Z} &= \{\dots, -2, -1, 0, 1, 2, \dots\} \\ \mathbb{Q} &= \left\{ \frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{N} \right\} & \mathbb{R} &= \text{set of real numbers} \\ \mathbb{C} &= \{a + bi : a, b \in \mathbb{R}, i = \sqrt{-1}\} = \text{set of complex numbers}\end{aligned}$$

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

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

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

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

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 **multiplicative 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 multiplicative inverse. For example, for  $[2] \in \mathbb{Z}_4$ , there is no  $[x] \in \mathbb{Z}_4$  such that  $[2][x] = [1]$ .<sup>1</sup>

<sup>1</sup> 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  $\mathbb{R}$ <sup>2</sup> is an  $n \times n$  array that can be expressed as follows:

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

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  $M_n(\mathbb{R})$ .

<sup>2</sup>  $\mathbb{R}$  can be replaced by  $\mathbb{Q}$  or  $\mathbb{C}$ .

*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

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

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 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

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

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

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

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

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

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 permutations:

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

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

**Note**

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

indicates the bijection  $\sigma : \{1, 2, 3\} \rightarrow \{1, 2, 3\}$  with  $\sigma(1) = 1$ ,  $\sigma(2) = 3$  and  $\sigma(3) = 2$ .

For  $n \in \mathbb{N}$ , we denote  $S_n := S_{\{1, 2, \dots, n\}}$ , the set of all permutations of  $\{1, 2, \dots, n\}$ . 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  $\sigma(n)$ .  $\square$

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  $\sigma\tau : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$  is given by  $\forall x \in \{1, \dots, n\}, x \mapsto \sigma(\tau(x))$ .

It is important to note that  $\because \sigma, \tau$  are **both bijective**,  $\sigma\tau$  is also bijective. Thus, together with the fact that  $\sigma\tau : \{1, \dots, n\} \rightarrow \{1, \dots, n\}$ , 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  $\sigma$  and  $\tau$  have support sets that are disjoint<sup>1</sup>.

<sup>1</sup> This is proven in A1

On the other hand, the associative property holds<sup>2</sup>, i.e.

<sup>2</sup>

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

#### Exercise 2.1.1

Prove this as an exercise.

The set  $S_n$  also has an identity element<sup>3</sup>, namely

<sup>3</sup>

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

#### Exercise 2.1.2

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

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

Finally,  $\forall \sigma \in S_n$ , since  $\sigma$  is a bijection, we have that its inverse function,  $\sigma^{-1}$  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  $\sigma$ , 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<sup>4</sup>

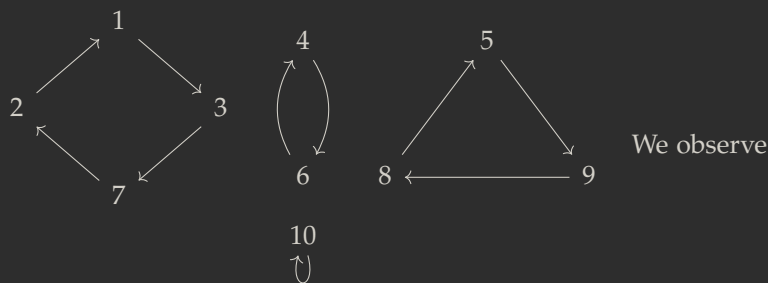
1.  $\forall \sigma, \tau \in S_n \quad \sigma\tau, \tau\sigma \in S_n.$
  2.  $\forall \sigma, \tau, \mu \in S_n \quad \sigma(\tau\mu) = (\sigma\tau)\mu.$
  3.  $\exists \varepsilon \in S_n \quad \forall \sigma \in S_n \quad \sigma\varepsilon = \sigma = \varepsilon\sigma.$
  4.  $\forall \sigma \in S_n \quad \exists! \sigma^{-1} \in S_n \quad \sigma\sigma^{-1} = \varepsilon = \sigma^{-1}\sigma.$
- 

<sup>4</sup> These properties show that  $S_n$  is a group, which will be defined later.

**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  $\sigma$  geometrically, we get



that  $\sigma$  can be **decomposed** into one 4-cycle,  $(1 \ 3 \ 7 \ 2)$ , one 2-cycle,  $(4 \ 6)$ , one 3-cycle,  $(5 \ 9 \ 8)$ , and one 1-cycle,  $(10)$ .

Note that these cycles are (pairwise) **disjoint**, and we can write<sup>5</sup>

$$\sigma = (1 \ 3 \ 7 \ 2) (4 \ 6) (5 \ 9 \ 8)$$

Note that we may also write

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

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

$$(1 \ 3 \ 7 \ 2) = (7 \ 2 \ 1 \ 3) \neq (1 \ 2 \ 7 \ 3).$$

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<sup>6</sup>.

<sup>5</sup> 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.

<sup>6</sup> See bonus question of A1. Proof will be included in the notes once the assignment is over.

---

### Theorem 3 (Cycle Decomposition Theorem)

If  $\sigma \in S_n$ ,  $\sigma \neq \varepsilon$ , then  $\sigma$  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

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



## 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<sup>1</sup>

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

<sup>1</sup> 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

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

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

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

where (1) is by associativity.

**Example 3.1.1**

The sets  $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ , and  $(\mathbb{C}, +)$  are all abelian, where 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 multiplication 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<sup>2</sup>,  $(M_n(\mathbb{R}), \cdot)$  is not a group.

<sup>2</sup> 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  $\{1, 2, \dots, n\}$ . 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<sup>3</sup>.

<sup>3</sup> 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  $G_1, G_2, \dots, G_n$  are groups, then so is  $G_1 \times G_2 \times \dots \times G_n$ .

To facilitate our writing, we 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  $g_1 *_G g_2 = g_1 g_2$ . 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

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

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.  $(gh)^{-1} = h^{-1}g^{-1}$
3.  $g^n g^m = g^{n+m}$  for all  $n, m \in \mathbb{Z}$
4.  $(g^n)^m = g^{nm}$  for all  $n, m \in \mathbb{Z}$

**Exercise 3.1.2**

Prove Proposition 5 as an exercise.

---

**Warning**

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

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

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

---



## 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

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

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

**Example 4.1.3**

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

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

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

**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

$g \neq 1$  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







## 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  $h_1(h_2h_3) = (h_1h_2)h_3$ . 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.  $h_1h_2 \in H$
2.  $1_G \in H$
3.  $\exists h_1^{-1} \in H$  such that  $h_1h_1^{-1} = 1_G$

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  $h_1h_1^{-1} = 1_H$ , but  $h_1, h_1^{-1} \in G$  as well, and so  $h_1h_1^{-1} = 1_G$ . 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  $A^{-1} \in SL_n(\mathbb{R})$ . 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 **center of a group**  $G$  is defined as

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

---

### 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  $\forall g \in G$ ,

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

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

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

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 *Cancellation Laws*,  $h^m = 1$  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 required.  $\square$

---

## 6 Lecture 6 May 14th 2018

### 6.1 Subgroups (Continued 2)

#### 6.1.1 Alternating Groups

Recall that  $\forall \sigma \in S_n$ , with  $\sigma \neq \varepsilon$ ,  $\sigma$  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.  $\sigma = (a \ b)$ , where  $a, b \in \{1, \dots, n\}$  and  $a \neq b$ .

---

#### Example 6.1.1

We have that<sup>1</sup>

$$(1 \ 2 \ 4 \ 5) = (1 \ 2)(2 \ 4)(4 \ 5)$$

Also, we can show that<sup>2</sup>

$$(1 \ 2 \ 4 \ 5) = (2 \ 3)(1 \ 2)(2 \ 5)(1 \ 3)(2 \ 4) \quad (6.1)$$

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

---

#### Theorem 10 (Parity Theorem)

<sup>1</sup> If we apply the permutations on the right hand side, we have that

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

<sup>2</sup>

#### 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 transpositions (why?).

If a permutations  $\sigma$  has 2 factorizations

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

where each  $\gamma_i$  and  $\mu_j$  are transpositions, then  $r \equiv s \pmod{2}$ .

### 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  $\sigma$  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.  $\forall \sigma, \tau \in A_n \quad \sigma\tau \in A_n$  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  $A_n$  is 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  $\varepsilon$  is even and so  $\varepsilon \in A_n$ .



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

$$\sigma = \sigma_1 \sigma_2 \dots \sigma_r \quad \text{and}$$

$$\tau = \tau_1 \tau_2 \dots \tau_s,$$

where  $\sigma_i, \tau_j$  are transpositions, and  $r, s$  are even integers. Then

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

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  $\sigma_i$  is a transposition, we have that  $\sigma_i^2 = \varepsilon$  and thus  $\sigma_i^{-1} = \sigma_i$ . It follows that

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

which is an even permutation and

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

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

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  $A_n \cap O_n = \emptyset$ . 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  $f : A_n \rightarrow O_n$  such that  $f(\sigma) = \gamma\sigma$ . Since  $\sigma$  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  $|A_n| = |O_n|$ . □

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  $\varepsilon$  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.

## 6.1.2 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  $k = k \cdot 1 = \underbrace{1 + 1 + \dots + 1}_{k \text{ times}}$ .

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,  $\pm 1$  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.  $g^k = g^m \iff k \equiv m \pmod{n}$ ; and
3.  $\langle g \rangle = \{1, g, g^2, \dots, g^{n-1}\}$  where each  $g^i$  is distinct from others.<sup>1</sup>

<sup>1</sup> This also means that the order of the group is the same as the order of the generator.

### Proof

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

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

( $\Rightarrow$ ) 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. ( $\Rightarrow$ )  $g^k = g^m \implies g^{k-m} = 1 \xrightarrow{\text{by 1}} n|(k-m) \iff k \equiv m \pmod{n}$

( $\Leftarrow$ )  $k \equiv m \pmod{n} \implies \exists q \in \mathbb{Z} \ k = qn + m$ . 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

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

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

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  $k \equiv m \pmod{n}$ . Therefore,  $k = m$ .

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

□

---

**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.  $g^k = g^r \iff k = r$ ;
  3.  $\langle g \rangle = \{\dots, g^{-2}, g^{-1}, 1, g, g^2, \dots\}$  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.  $(\iff) g^0 = 1$

$(\implies)$  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.

$$g^k = g^m \iff g^{k-m} = 1 \xrightarrow{\text{by 1}} k - m = 0 \iff k = m$$

□

---

**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

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


---

**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  $\exists r \in \mathbb{N} \quad (g^d)^r = 1$ . Since  $o(g) = n$ , then  $n \mid dr$ . Then  $\exists q \in \mathbb{Z} \quad dr = nq$  by definition of divisibility.  $\therefore n = dk$  and  $d \neq 0$ , we have

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

□

### 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

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

□

## 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  $G$ .

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

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  $H = \langle g^m \rangle$ .

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

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

**Division Algorithm** :  $\exists q, r \in \mathbb{Z} \ 0 \leq r < m \quad k = mq + r$

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

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

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

Finally,

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

□

### 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  $(\implies)$ ,

$$\begin{aligned} G = \langle g^k \rangle &\implies g \in \langle g^k \rangle \implies \exists x \in \mathbb{Z} \quad g = g^{kx} \\ &\implies 1 = g^{kx-1} \implies n \mid (kx-1) \quad (\because \text{Proposition 13}) \\ &\implies \exists y \in \mathbb{Z} \quad kx-1 = ny \quad (\because \text{Division Algorithm}) \\ &\implies 1 = kx + ny \end{aligned}$$

Then

$$\begin{aligned} &\because 1 \mid kx \wedge 1 \mid ny \wedge 1 = kx + ny \\ &\gcd(k, n) = 1 \quad (\because \text{gcd Characterization}) \end{aligned}$$

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.  $g \in \langle g^k \rangle$ .

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

□

### 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  $G \implies \exists d \in \mathbb{N} \quad d \mid n \quad H = \langle g^d \rangle \implies |H| \mid n$ .
2.  $k \mid n \implies \langle g^{\frac{n}{k}} \rangle$  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

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

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

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

$$\text{Note: } d = \gcd(m, n) \implies d \mid n \implies |H| = o(g^d) = \frac{n}{d}$$

$\therefore$  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

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

where (1) is by Proposition 13 and (2) is by Proposition 15. Thus

$$d = \frac{n}{k} \text{ and } K = \langle g^{\frac{n}{k}} \rangle$$

□



## 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

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

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.

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

### 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 (Group Homomorphism)

Let  $G, H$  be groups. A mapping

$$\alpha : G \rightarrow H$$

is called a group **homomorphism** if  $\forall a, b \in G$ ,<sup>1</sup>

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

<sup>1</sup> 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:

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

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

1.  $\alpha(1_G) = 1_H$
  2.  $\forall g \in G \quad \alpha(g^{-1}) = \alpha(g)^{-1}$
  3.  $\forall g \in G \quad \forall k \in \mathbb{Z} \quad \alpha(g^k) = \alpha(g)^k$
- 

**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.  $\square$
- 

**Definition 20 (Isomorphism)**

Let  $G, H$  be groups. Consider a mapping

$$\alpha : G \rightarrow H$$

We say that  $\alpha$  is an **isomorphism** if it is a homomorphism and bijective.

If  $\alpha$  is an isomorphism, we say that  $G$  is **isomorphic 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  $G \rightarrow G$  is an isomorphism.
  2. **(Symmetric)** If  $\sigma : G \rightarrow H$  is an isomorphism, then the inverse map  $\sigma^{-1} : H \rightarrow G$  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

$$\alpha(g_1g_2) = g_1g_2 = \alpha(g_1)\alpha(g_2).$$

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

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

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

Note that since  $\sigma$  has a bijective inverse, we also have

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

Then since  $\sigma$  is a homomorphism,

$$\begin{aligned} \sigma^{-1}(h_1h_2) &= \sigma^{-1}(\sigma(g_1)\sigma(g_2)) = \sigma^{-1}(\sigma(g_1g_2)) \\ &= g_1g_2 = \sigma^{-1}(h_1)\sigma^{-1}(h_2). \end{aligned}$$

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

$$\tau\sigma(g_1g_2) = \tau(\sigma(g_1)\sigma(g_2)) = \tau\sigma(g_1)\tau\sigma(g_2),$$

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

□

**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<sup>2</sup>. Also,  $\forall r, s \in \mathbb{R}$  we have that

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

<sup>2</sup> The image of the map covers all positive real numbers while taking all real numbers, which is the perfect candidate as a map here.

Therefore,  $\alpha$  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  $\tau : (\mathbb{Q}, +) \rightarrow (\mathbb{Q}^*, \cdot)$  is an isomorphism.

In particular, we have that  $\tau$  is onto. Then  $\exists q \in \mathbb{Q}$  such that  $\tau(q) = 2$ . Let  $\tau(\frac{q}{2}) = \alpha$ . Since  $\tau$  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  $\tau$  and

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

as required. □

## 9.2.2 Cosets and Lagrange's Theorem

**Definition 21 (Coset)**

Let  $H$  be a subgroup of a group  $G$ .

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

and

$\forall a \in G \quad aH = \{ah : h \in H\}$  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  $G$ . For example, we know that  $A_n$  is a subgroup of  $S_n$ . But if  $\sigma$  is an odd permutation, then  $\sigma A_n$  and  $A_n \sigma$  are sets of odd permutations since  $A_n$  is the set of even permutations. As proven before,  $O_n$ , the set of odd permutations is not a subgroup of  $S_n$ .

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.  $Ha = Hb \vee Ha \cap Hb = \emptyset$ .<sup>3</sup> Then the distinct right cosets of  $H$  forms a partition of  $G$ .<sup>4</sup>

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

<sup>3</sup>  $\vee \equiv \text{XOR}$

<sup>4</sup> 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  $(\implies)$ ,

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



For ( $\Leftarrow$ ),

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

Let  $b = 1$ . Then

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

2. Note

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

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

$$\begin{aligned}
 Ha \cap Hb &\neq \emptyset \\
 &\implies \exists x \in Ha \cap Hb \\
 &\implies (x \in Ha \xrightarrow{\text{by 1}} Hx = Hb) \wedge (x \in Hb \xrightarrow{\text{by 1}} Hx = Hb) \\
 &\implies Ha = Hb
 \end{aligned}$$

□

---

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

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

---

#### Proof

Since  $G$  is finite, there can only be finitely many cosets of  $H$ . Let  $k = [G : H]$  and  $Ha_1, Ha_2, \dots, Ha_k$  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

$$H \rightarrow Ha_i \text{ defined by } h \mapsto ha_i$$

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

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

Then we have

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

□

### Corollary 24

1. If  $G$  is a finite group and  $g \in G$ , then  $o(g) \mid |G|$ .
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*,  $o(g) = |H| \mid |G|$ .
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  $\phi$ -function* is defined as

$$\phi(n) \equiv \left| \{k \in \{1, \dots, n-1\} : \gcd(k, n) = 1\} \right|. \quad (10.1)$$

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

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

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

### Corollary 25

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

---

### Proof

Let  $g \in G$  such that  $g \neq 1$ . By Corollary 24,  $o(g) \mid p$ . 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  $|H| \mid p$ . Since  $p$  is prime, we either have  $|H| = 1$  or  $p$ . In other words, we either have that  $H = \{1\}$  or  $H = G$ , respectively.  $\square$

---

### 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,  $|H \cap K| \mid |H| \wedge |H \cap K| \mid |K|$ . By assumption that  $\gcd(|H|, |K|) = 1$ , we have<sup>1</sup> that  $|H \cap K| = 1$ , and hence  $H \cap K = \{1\}$ .  $\square$

<sup>1</sup>  $|H \cap K|$  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.  $\forall g \in G \quad gHg^{-1} = H$  <sup>2</sup>

<sup>2</sup> 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.  $\forall g \in G \quad gHg^{-1} \subseteq H$
3.  $\forall g \in G \quad gHg^{-1} = H$

---

### Note

Note that item 3 is indeed a stronger statement than 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):

$$\begin{aligned}
x \in gHg^{-1} &\implies \exists h \in H \ x = ghg^{-1} \\
&\implies \exists h_1 \in H \ gh = h_1g \quad \because gh \in gH = Hg \\
&\implies x = ghg^{-1} = h_1gg^{-1} = h_1 \in H \\
&\implies gHg^{-1} \subseteq H
\end{aligned}$$

(2)  $\implies$  (3):

$$\begin{aligned}
(2) &\implies \forall g \in G \ gHg^{-1} \subseteq H \\
&\implies \exists g^{-1} \in G \ g^{-1}Hg \subseteq H \\
&\implies H \subseteq gHg^{-1} \\
&\stackrel{(2)}{\implies} gHg^{-1} = H
\end{aligned}$$

(3)  $\implies$  (1):

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

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

**Example 11.1.1**

Let  $G = GL_n(\mathbb{R})$  and  $H = SL_n(\mathbb{R})$ .<sup>1</sup> 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.  $SL_n(\mathbb{R}) \triangleleft GL_n(\mathbb{R})$ .<sup>2</sup>

<sup>1</sup> Recall Definition 8 and Definition 11.

<sup>2</sup>

**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  $a \in G$ .

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

$$a \notin H \implies G = H \cup Ha \implies Ha = G \setminus H \quad \therefore \text{Proposition 22}$$

$$a \notin H \implies G = H \cup aH \implies aH = G \setminus H \quad \therefore \text{Proposition 22}$$

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

### Example 11.1.2

Let  $A_n$  be the **Alternating Group** contained by  $S_n$ .<sup>3</sup> 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

$$A_n \triangleleft S_n.$$

<sup>3</sup> Recall the definition of alternating group from Theorem 11 and  $S_n$  from Definition 4

### Example 11.1.3

Let

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

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

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

<sup>4</sup> 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.  $HK = KH$  <sup>5</sup>
3.  $KH$  is a subgroup of  $G$

<sup>5</sup> 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

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

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  $1 = 1 \cdot 1 \in HK$ .  $\forall hk \in HK$ ,  $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$ . 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  $G$ . □

---

**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

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

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  $HK \triangleleft G$ .

□

---

**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  $G$ .

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

---

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  $G$ .<sup>1</sup> Define  $\sigma : H \times K \rightarrow HK$  by

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

Claim 2:  $\sigma$  is an isomorphism.

<sup>1</sup> We do not need the more powerful statement that says that  $HK$  is a normal subgroup.

Let  $(h, k), (h_1, k_1) \in H \times K$ . By Claim 1, note that  $h_1k = kh_1$ . Therefore,

$$\begin{aligned}\sigma((h, k) \cdot (h_1, k_1)) &= \sigma((hh_1, kk_1)) = hh_1kk_1 \\ &= hkh_1k_1 = \sigma((h, k))\sigma((h_1, k_1))\end{aligned}$$

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

$$\begin{aligned}hk = h_1k_1 &\implies h_1^{-1}h = k_1k^{-1} \in H \cap K = \{1\} \\ &\implies h_1^{-1}h = 1 = k_1k^{-1} \implies h_1 = h \wedge k_1 = k.\end{aligned}$$

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

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  $G \cong C_{mn} \cong C_m \times C_n$ .

### 12.2.1 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

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

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

$$Ka = Ka_1 \wedge Kb = Kb_1 \implies Kab = Ka_1b_1.$$

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.  $\forall a, b \in G \quad KaKb = Kab$  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  $Kab = Ka_1b_1$ , it suffices to show that  $(ab)(a_1b_1)^{-1} \in K$ . Note that since  $K \triangleleft G$ , we have that  $aKa^{-1} = K$ . Therefore,

$$\begin{aligned} ab(a_1b_1)^{-1} &= ab(b_1^{-1}a_1^{-1}) = a(bb_1^{-1})a_1^{-1} \\ &= (a(bb_1^{-1})a^{-1})(aa_1^{-1}) \in K. \end{aligned}$$

Therefore  $Kab = Ka_1b_1$  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  $Kk = K(1)$ <sup>2</sup>, by (2), we have that  $Kak = Ka(1)$ , i.e.

<sup>2</sup> This is cause 1 is in the same coset.





## 13 Lecture 13 May 30th 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  $\phi : G \rightarrow G/K$  given by  $\phi(a) = Ka$  is a surjective homomorphism.<sup>1</sup>
3. If  $[G : K]$  is finite, then  $|G/K| = [G : K]$ . In particular, if  $|G|$  is finite, then  $|G/K| = \frac{|G|}{|K|}$ .

1

##### Exercise 13.1.1

Is  $\phi$  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,  $\phi$  is surjective. For  $a, b \in G$ ,

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

Thus  $\phi$  is a surjective homomorphism.

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

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

□

---

### 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

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

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

---

## 13.1.2 Isomorphism Theorems

---

### Definition 27 (Kernel and Image)

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

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

and the **image** of  $\alpha$  is defined by

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


---

### Proposition 36

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

1.  $\text{im } \alpha$  is a subgroup of  $H$
2.  $\ker \alpha \triangleleft G$

**Proof**

1. Note that  $1_H = \alpha(1_G) \in \alpha(G)$  (i.e. the identity is in  $\text{im } \alpha$ ). 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.  $\text{im } \alpha$  is 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  $\text{im } \alpha$ ). Thus by the **Subgroup Test**, we have that  $\text{im } \alpha$  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,  $\ker \alpha \triangleleft G$ .

□

**Example 13.1.1**

Consider the determinant map

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

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

**Example 13.1.2**

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

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

Then the sign mapping,  $\text{sgn} : S_n \rightarrow \{\pm 1\}$  defined by  $\sigma \mapsto \text{sgn}(\sigma)$  is a homomorphism.<sup>2</sup> Also,  $\ker \text{sgn} = A_n$ . Thus, we have  $A_n \triangleleft S_n$ , as proven before.

<sup>2</sup> Think about why. It's quite straightforward using the definition.

### Proposition 37 (Normal Subgroup as the Kernel)

If  $K \triangleleft G$ , then  $K = \ker \phi$  where  $\phi : G \rightarrow G/K$  is the coset map.

#### Proof

Recall that  $\phi : G \rightarrow G/K$  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  $\alpha : G \rightarrow H$  be a group homomorphism. We have

$$G/\ker \alpha \cong \text{im } \alpha$$

#### Proof

Let  $K = \ker \alpha$ . Since  $K \triangleleft G$  (by Proposition 36),  $G/K$  is a group. Let<sup>3</sup>

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

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

<sup>3</sup> 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 01st 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  $\alpha : G \rightarrow H$  where  $G$  and  $H$  are groups,

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

Now let  $\alpha : G \rightarrow H$  be a group homomorphism,  $K = \ker \alpha$ ,  $\phi : G \rightarrow G/K$  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.

$$\begin{array}{ccc} G & \xrightarrow{\alpha} & H \\ \phi \downarrow & \nearrow \bar{\alpha} & \\ G/K & & \end{array}$$

---

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

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

Suppose  $\alpha = \beta\phi$  where  $\beta : G/K \rightarrow H$ . Then

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

where (1) is because  $\phi$  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  $G/K \rightarrow H$  satisfying  $\alpha = \bar{\alpha}\phi$ .  $\square$

---

With that, we have the following proposition.

---

### Proposition 39

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

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

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

In such a scenario, we also say that  $\alpha$  **factors through**  $\phi$ .<sup>1</sup>

<sup>1</sup> 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  $\alpha : \mathbb{Z} \rightarrow G$ , defined as

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

which is a group homomorphism. By definition,  $\alpha$  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<sup>2</sup>

<sup>2</sup> 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  $\alpha$  would not be a group homomorphism.



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

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  $n$ .<sup>3</sup> Therefore,

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

Therefore, we have that

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

<sup>3</sup> This is why we often see texts from various authors using  $\mathbb{Z}/n\mathbb{Z}$  to represent the set of integers modulo  $n$ .

---

### 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  $\alpha : H \rightarrow HK/K$ , defined by<sup>4</sup>

$$\alpha(h) = Kh$$

<sup>4</sup>Note that  $Kh \in HK/K$  since  $h \in H \subseteq HK$ .

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

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

Therefore, we have that  $\alpha$  is surjective. Now by Proposition 22, observe that

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

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

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

#### Proof

Define  $\alpha : G/K \rightarrow G/H$  by  $\alpha(Kg) = Hg$  for all  $g \in G$ . Clearly,  $\alpha$  is surjective. Now if  $Kg = Kg_1$ , for any  $g, g_1 \in G$ , then  $gg_1^{-1} \in K \subseteq H$ . Therefore,  $Hg = Hg_1$ . Thus  $\alpha$  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

$$(G/K) / (H/K)$$

as required. □

---

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 Lecture 15 Jun 04th 2018

## 15.1 Group Action

### 15.1.1 Cayley's Theorem

---

#### Theorem 42 (Cayley's Theorem)

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

---

#### Proof

Since  $G$  is finite, let  $G = \{g_1, g_2, \dots, g_n\}$  and let  $S_G$  be the permutation group of  $G$ . By identifying  $g_i$  with  $i$ , where  $1 \leq i \leq n$ , we see that  $S_G \cong S_n$ <sup>1</sup>. Therefore, it suffices to find an injective homomorphism<sup>2</sup>  $\sigma : G \rightarrow S_G$ .

Consider the function  $\mu_a : G \rightarrow G$ , where  $a \in G$ , such that  $\mu_a(g) = ag$  for all  $g \in G$ . Clearly,  $\mu_a$  is surjective. Suppose  $\mu_a = \mu_b$ , where  $b \in G$ . Then  $a = \mu_a(1) = \mu_b(1) = b$ . Thus  $\mu_a$  is also injective. It follows that  $\mu_a \in S_G$  by definition.

Now define the function  $\sigma : G \rightarrow S_G$  such that  $\sigma(a) = \mu_a$ . Clearly,  $\sigma$  is injective, since  $\sigma(a) = \sigma(b) \implies \mu_a = \mu_b$ . Observe that  $\sigma(ab) = \mu_{ab} = ab = \mu_a \mu_b$ . Thus  $\sigma$  is a group homomorphism. Note that  $\ker \sigma = \{1\}$ , the trivial group. It follows from the First Isomorphism Theorem that  $G \cong \text{Im } \sigma \leq S_G \cong S_n$ .<sup>3</sup> <sup>4</sup>  $\square$

<sup>1</sup>  $S_G$  is the permutation group of  $G$ .

We can think of  $S_G$  as a group of permutations that permutes the index of the elements of  $G$ . Since there are  $n$  indices, there are  $n!$  ways to permute the indices, and so  $|S_G| = n! = |S_n|$ . Then we can certainly find some isomorphism from  $S_G$  to  $S_n$ , and so  $S_G \cong S_n$ .

<sup>2</sup> **Why do we need injectivity?** We need homomorphicity in order to invoke the First Isomorphism Theorem so that we can get  $G \cong \text{Im } \sigma \leq S_G \cong S_n$ .

<sup>3</sup> We shall use  $H \leq G$  to denote that  $H$  is a subgroup of  $G$  from here on.

<sup>4</sup> This is a result from Proposition 36

---

Cayley's Theorem is, however, too strong at times. We can certainly find a smaller integer  $m$  such that  $G$  is contained in  $S_m$ . Con-

sider the following example.

### Example 15.1.1

Let  $H \leq G$  with  $[G : H] = m < \infty$ . Let  $X = \{g_1H, g_2H, \dots, g_mH\}$  be the set of all distinct left cosets of  $H$  in  $G$ <sup>5</sup>. For  $a \in G$ , define  $\lambda_a : X \rightarrow X$  by  $\lambda_a(gH) = agH, gH \in X$ .

<sup>5</sup> This is simply a consequence of  $[G : H] = m$ .

Note that  $\lambda_a$  is a bijection<sup>6</sup>, and so  $\lambda_a \in S_X$ , the permutation group of  $X$ . Consider the mapping  $\tau : G \rightarrow S_X$  defined by  $\tau(a) = \lambda_a$  for  $a \in G$ . Note that  $\forall a, b \in G, \lambda_{ab} = \lambda_a \lambda_b$ . Thus  $\tau$  is a homomorphism. Note that if  $a \in \ker \tau$ , then  $aH = H$  which implies  $a \in H$  by Proposition 22. Thus  $\ker \tau \subseteq H$ .

<sup>6</sup> This is true as shown in the proof above, but it can also serve as a tiny exercise.

From the example above, if we apply the First Isomorphism Theorem, then

$$G/\ker \tau \cong \text{im } \tau \leq S_X \cong S_m \leq S_n.$$

This is the result that we desired.

---

### Theorem 43 (Extended Cayley's Theorem)

Let  $H \leq G$  with  $[G : H] = m < \infty$ . If  $G$  has no normal subgroup contained in  $H$  except for the trivial subgroup  $\{1\}$ , then  $G$  is isomorphic to a subgroup of  $S_m$ .

---

#### Proof

By our assumption, let  $X$  be the set of all distinct left cosets of  $H$  in  $G$ . Then we have that  $|X| = m$  and so  $S_X \cong S_m$ <sup>7</sup>. From Example 15.1.1, we have that there exists a group homomorphism  $\tau : G \rightarrow S_X$  with  $K := \ker \tau \subseteq H$ . So by the First Isomorphism Theorem, we have that

<sup>7</sup> This is as argued in the proof of Cayley's Theorem.

$$G/K \cong \text{im } \tau.$$

Since  $K \subseteq H$  and  $K \triangleleft G$ , we have, by assumption, that  $K = \{1\}$ . It follows that

$$G \cong \text{im } \tau \leq S_X \cong S_m.$$

□

---

**Corollary 44**

Let  $|G| = m \in \mathbb{N}$  and  $p$  the smallest prime such that  $p|m$ . If  $H \leq G$  with  $[G : H] = p$ , then  $H \triangleleft G$ .

**Proof**

Let  $X$  be the set of all distinct left cosets of  $H$  in  $G$ . We have  $|X| = p$  and so  $S_X \cong S_p$ . Let  $\tau : G \rightarrow S_X \cong S_p$  be as defined in Example 15.1.1, with  $K := \ker \tau \subseteq H$ . By the First Isomorphism Theorem, we have that

$$G/K \cong \text{im } \tau \leq S_X \cong S_p,$$

i.e.  $G/K$  is isomorphic to a subgroup of  $S_p$ . Therefore, by Lagrange's Theorem, we have that  $|G/K| \mid p!$ .

Also, since  $K \subseteq H$ , if  $[H : K] = k \in \mathbb{N}$ , then

$$|G/K| \stackrel{(1)}{=} \frac{|G|}{|K|} = \frac{|G|}{|H|} \cdot \frac{|H|}{|K|} = pk,$$

where (1) is by Proposition 35. Therefore we have that  $pk \mid p!$  and so  $k \mid (p-1)!$ .

Note that  $k \mid |H|$ <sup>8</sup>, which divides  $|G|$ , and  $p$  is the smallest prime dividing  $|G|$ . Thus every prime divisor of  $k$  must be  $\geq p$ .<sup>9</sup> Thus  $k = 1$ , which implies that  $K = H$ . Therefore,  $H \triangleleft G$  as desired.  $\square$

<sup>8</sup> This is clear since  $|H| = k|K|$ .

<sup>9</sup> By the **Fundamental Theorem of Arithmetic**, and since  $k$  is finite, let  $k = p_1^{a_1} p_2^{a_2} \dots p_m^{a_m}$ , where  $p_i$ 's are distinct primes and  $a_i \in \mathbb{N}$  are the multiplicities of the  $i^{\text{th}}$ , and by the **Well-Ordering Principle**, let  $p_i < p_{i+1}$ . Then we have, for some  $b = b_1^{c_1} b_2^{c_2} \dots b_j^{c_j} \in \mathbb{N}$  where the  $b_i$ 's are distinct primes,  $b_i < b_{i+1}$ , and  $c_i \in \mathbb{N} \cup \{0\}$ ,

$$m = kb = p_1^{a_1} p_2^{a_2} \dots p_m^{a_m} b_1^{c_1} b_2^{c_2} \dots b_j^{c_j}.$$

Since  $p$  is the smallest prime that divides  $m$ , we have

$$\begin{aligned} p &= \min\{p_1, p_2, \dots, p_m, b_1, b_2, \dots, b_j\} \\ &= \min\{p_1, b_1\} \end{aligned}$$

**15.1.2 Group Action****Definition 28 (Group Action)**

Let  $G$  be a group,  $X$  a non-empty set. A **group action** of  $G$  on  $X$  is a mapping  $G \times X \rightarrow X$  denoted as  $(a, x) \rightarrow ax$  such that

1.  $1 \cdot x = x, x \in X$
2.  $a \cdot (b \cdot x) = (ab) \cdot x, a, b \in G, x \in X$

In this case, we say  $G$  **acts on**  $X$ .





## 16 Lecture 16 Jun 06th 2018

### 16.1 Group Action (Continued)

#### 16.1.1 Group Action (Continued)

##### Remark

Let  $G$  be a group acting on a set  $X$ . For  $a, b \in G$ , and  $x, y \in X$ , we have that

$$a \cdot x = b \cdot y \iff (b^{-1}a) \cdot x = y.$$

In particular, we have

$$a \cdot x = a \cdot y \iff x = y.$$

For  $a \in G$ , define  $\sigma_a : X \rightarrow X$  by  $\sigma_a(x) = a \cdot x$  for all  $x \in X$ . In A3, we will be showing that<sup>1</sup>:

1.  $\sigma_a \in S_X$ , the permutation group of  $X$ ; and
2. The function  $\Theta : G \rightarrow S_X$  given by  $\Theta(a) = \sigma_a$  is a group homomorphism with

$$\ker \Theta = \{a \in G : a \cdot x = x, x \in X\}.$$

Note that the group homomorphism  $\Theta : G \rightarrow S_X$  gives an **equivalent definition** of a **Group Action** of  $G$  on  $X$ . If  $X = G$ ,  $|G| = n$  and  $\ker \Theta = \{1\}$ <sup>2</sup>, then the map  $\Theta : G \rightarrow S_G \cong S_n$  shows that  $G$  is isomorphic to a subgroup of  $S_n$ <sup>3</sup>, which is the equivalent statement of Cayley's Theorem.

##### Example 16.1.1

If  $G$  is a group, let  $G$  act on itself by  $a \cdot x = a \cdot x \cdot a^{-1}$ , for all  $a, x \in G$ . Note that the axioms of a group action is satisfied:

<sup>1</sup> This will be added after the assignment.

<sup>2</sup> This is also called a **faithful group action**.  
<sup>3</sup>

##### Exercise 16.1.1

Verify that  $G$  is indeed isomorphic to a subgroup of  $S_n$  using the given information and the equivalent definition of a group action.

1.  $1 \cdot x = 1 \cdot x \cdot 1^{-1} = x$ ; and
2.  $a \cdot (b \cdot x) = a \cdot (b \cdot x \cdot b^{-1}) \cdot a = ab \cdot x \cdot (ab)^{-1} = (ab) \cdot x$ .

In this case, we say that  $G$  **acts on itself by conjugation**.

### Definition 29 (Orbit & Stabilizer)

Let  $G$  be a group acting on a set  $X$ , and  $x \in X$ . We denote by

$$G \cdot x = \{g \cdot x : \forall g \in G\}$$

the **orbit** of  $x$  and

$$S(x) = \{g \in G : g \cdot x = x\} \subseteq G$$

the **stabilizer** of  $x$ .

There is no standardized way of expressing the orbit and the stabilizer, i.e. the notation for orbit and stabilizers will be different across many references.

### Proposition 45

Let  $G$  be a group acting on a set  $X$  and  $x \in X$ . Let  $G \cdot x$  and  $S(x)$  be the orbit and stabilizer of  $x$  respectively. Then

1.  $S(x) \leq G$
2. there is a bijection from  $G \cdot x$  to  $\{gS(x) : g \in G\}$  and thus  $|G \cdot x| = [G : S(x)]$ .

### Proof

1. Since  $1 \cdot x = x$ , we have  $1 \in S(x)$ . If  $g, h \in S(x)$ , then

$$gh \cdot x = g \cdot (h \cdot x) = g \cdot x = x$$

i.e.  $S(x)$  is closed under “composition of group action”. Also note that

$$g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = 1 \cdot x = x.$$

Thus the inverse of each element is also in  $S(x)$ . Therefore, by the **Subgroup Test**,  $S(x) \leq G$ .

2. For the sake of simplicity, let us write  $S = S(x)$ . Consider the map

$$\phi : G \cdot x \rightarrow \{gS(x) : g \in G\}$$

defined by  $\phi(g \cdot x) = gS$ <sup>4</sup>. To verify that the map is well-defined, note that

<sup>4</sup> We go with the most simplistic and rather naive kind of function here.

$$\begin{aligned} g \cdot x = h \cdot x &\iff (h^{-1}g) \cdot x = x = 1 \cdot x \\ &\iff \phi(h^{-1}g \cdot x) = \phi(1 \cdot x) \\ &\iff h^{-1}gS = 1 \cdot S = S \\ &\iff gS = hS \end{aligned}$$

We also observe that  $\phi$  is injective. It is also clear that  $\phi$  is onto, and therefore we have that  $\phi$  is a bijection. It follows that

$$|G \cdot x| = |\{gS : g \in G\}| = [G : S]$$

□

### Theorem 46 (Orbit Decomposition Theorem)

Let  $G$  be a group acting on a non-empty finite set  $X$ . Let

$$X_f = \{x \in X : a \cdot x = x, \forall a \in G\}$$

(Note that  $x \in X_f \iff |G \cdot x| = 1$ )<sup>5</sup>

<sup>5</sup> Notice that

Let  $G \cdot x_1, G \cdot x_2, \dots, G \cdot x_n$  denote the distinct nonsingleton orbits (i.e.  $|G \cdot x_i| > 1$  for all  $1 \leq i \leq n$ ). Then

$$\begin{aligned} x \in X_f &\iff \forall a \in G \quad a \cdot x = x \\ &\iff \forall g \cdot x \in G \cdot x \quad g \cdot x = x \\ &\iff |G \cdot x| = 1 \end{aligned}$$

$$|X| = |X_f| + \sum_{i=1}^n [G : S(x_i)].$$

### Proof

Note that for  $a, b \in G$  and  $x, y \in X$ ,

$$\begin{aligned} a \cdot x = b \cdot y &\stackrel{\text{WLOG}}{\iff} (b^{-1}a) \cdot x = y \\ &\iff y \in G \cdot x \\ &\stackrel{(1)}{\iff} G \cdot x = G \cdot y \end{aligned}$$

where (1) is the conclusion after consider the other case where  $(a^{-1}b) \cdot y = x$ .

Thus, we see that the two orbits are either disjoint or the same, but not both. It follows that the orbits form a disjoint union of  $X$ . Since  $x \in X_f \iff |G \cdot x| = 1$ , the set  $X \setminus X_f$  contains all nonsingleton orbits, which are disjoint. It follows that

$$|X| = |X_f| + \sum_{i=1}^n |G \cdot x_i| \stackrel{(2)}{=} |X_f| + \sum_{i=1}^n [G : S(x_i)]$$

where (2) is by [Proposition 45](#). □

---

# 17 Lecture 17 Jun 08th 2018

## 17.1 Group Action (Continued 2)

### 17.1.1 Group Action (Continued 2)

---

#### Note (Recall Theorem 46)

Let  $G$  act on a finite set  $X \neq \emptyset$ . Let<sup>1</sup>

$$X_f = \{x \in X : a \cdot x = x, a \in G\}$$

Let  $G \cdot x_1, G \cdot x_2, \dots, G \cdot x_n$  be distinct nonsingleton orbits (ie.  $|G \cdot x_i| > 1$ ). Then

$$|X| = |X_f| + \sum_{i=1}^n [G : S(x_i)].$$

<sup>1</sup>  $X_f$  is also called the set of elements of  $X$  that are fixed by the action of  $G$ .

---

#### Example 17.1.1 (Conjugacy Class & Centralizer)

Let  $G$  be a finite group acting on itself by **conjugation**. In the context of Theorem 46, we have that

$$\begin{aligned} X &= G \\ G_f &= \{x \in G : gxg^{-1} = x, g \in G\} \\ &= \{x \in G : gx = xg, g \in G\} = Z(G), \end{aligned}$$

where we recall that  $Z(G)$  is the center of  $G$ . Now for any  $x \in G$ , we have

$$G \cdot x = \{gxg^{-1} : g \in G\},$$

which is known as the **conjugacy class** of  $x$ . We also have

$$S(x) = \{g \in G : gxg^{-1} = x\} = \{g \in G : gx = xg\} = C_G(x),$$

which is called the **centralizer** of  $x$ .

Putting the above example with **Theorem 46**, we have the following corollary.

---

### Corollary 47 (Class Equation)

Let  $G$  be a finite group and  $\{gx_1g^{-1} : g \in G\}, \dots, \{gx_ng^{-1} : g \in G\}$  denote the distinct nonsingleton conjugacy classes. Then

$$|G| = |Z(G)| + \sum_{i=1}^n [G : C_G(x_i)].$$


---

### Lemma 48

Let  $G$  be a group of order  $o^m$ , where  $p$  prime and  $m \in \mathbb{N}$ , which acts on a finite set  $X$ . Let

$$X_f = \{x \in X : a \cdot x = x, a \in G\}.$$

Then we have

$$|X| \equiv |X_f| \pmod{p}$$


---

### Proof

By the Orbit Decomposition Theorem, we have that

$$|X| = |X_f| + \sum_{i=1}^n [G : S(x_i)],$$

where  $[G : S(x_i)] > 1$  for  $1 \leq i \leq n$ . For any  $x_i$ , by Lagrange's Theorem,  $[G : S(x_i)] \mid |G| = p^m$ . Since  $[G : S(x_i)] > 1$ , we have, by the **Fundamental Theorem of Arithmetic**, that  $[G : S(x_i)]$  must be a multiple of  $p$ , i.e.  $p$  divides  $[G : S(x_i)]$ , for all  $i$ . Therefore,  $p \mid (|X| - |X_f|)$ , i.e.

$$|X| \equiv |X_f| \pmod{p},$$

as required. □

---

RECALL **Lagrange's Theorem**: If  $G$  is finite and  $g \in G$ , then

$$o(g) \mid |G|.$$

An interesting question to ask here is: Is the converse true? I.e., given a group  $G$  with an integer  $m$  such that  $m \mid |G|$ , does  $G$  contain an element of order  $m$ ?

Consider  $K_4$ , the Klein 4-group. Note that all elements of  $K_4$  have order at most 2, but  $4 \mid |K_4| = 4$ .

Now if  $m$  is some prime, is the converse still true?

---

### Theorem 49 (Cauchy's Theorem)

Let  $p$  be a prime,  $G$  be a finite group. If  $p \mid |G|$ , then  $G$  contains an element of order  $p$ .

---

### Proof (McKay)

Let  $|G| = n$ . Suppose  $p \mid n$ . Let

$$X = \{(a_1, \dots, a_p) : a_i \in G, a_1 \dots a_p = 1\}.$$

Note that  $X \neq \emptyset$ , since  $(1, \dots, 1) \in X$  (so the proof is not vacuous). Take any  $a_1, \dots, a_{p-1} \in G$ , then  $a_p$  is uniquely determined, i.e.

$$a_p = (a_1 \dots a_{p-1})^{-1}.$$

Now for each  $a_i$ , we have  $n$  choices, thus  $|X| = n^{p-1}$ .<sup>2</sup>

<sup>2</sup> Convince yourself why this is true.

Let  $\mathbb{Z}_p = (\mathbb{Z}_p, +)$  act on  $X$  by "cycling", i.e.  $\forall k \in \mathbb{Z}_p$ ,

$$k \cdot (a_1, a_2, \dots, a_p) = (a_{k+1}, a_{k+2}, \dots, a_p, a_1, \dots, a_k).$$

<sup>3</sup> Note that

<sup>3</sup> We want to use Theorem 46 from here.

$(a_1, \dots, a_p) \in X_f \iff$  every cycled shift of  $(a_1, \dots, a_p)$  is itself i.e. all  
 $\iff a_1 = a_2 = \dots = a_p$  and  $a_1 a_2 \dots a_p = 1$   
 of the components of the  $p$ -tuple are the same. Now if  $(a_1, \dots, a_p)$  has at least 2 distinct components, then its orbits must have  $p$  elements. In other words, for some  $r \in \mathbb{N}$ , for each  $1 \leq i \leq r$ , we have that  $[G : S(x_i)] = p$ .

Then, by the Orbit Decomposition Theorem,

$$n^{p-1} = |X| = |X_f| + \sum_{i=1}^r [G : S(x_i)]$$

$$|X_f| = n^{p-1} - rp.$$

We observe that  $|X_f|$  is indeed divisible by  $p$  and is non-zero, since  $(1, \dots, 1) \in X_f$ . Therefore, there exists some  $a \neq 1 \in G$ , such that  $(a, \dots, a) \in X_f$ , i.e.  $a^p = 1$ . We know that  $p$  is the smallest power by construction, and therefore  $\text{o}(a) = p$  as required.  $\square$

---



# 18 Lecture 18 Jun 13th 2018

## 18.1 Finite Abelian Groups

### 18.1.1 Primary Decomposition

---

#### Note (Notation)

Let  $G$  be an abelian group and  $m \in \mathbb{Z}$ . We define

$$G^{(m)} := \{g \in G : g^m = 1\}$$

---

#### Proposition 50 (Group of Elements of the Same Order is a Subgroup)

Let  $G$  be an abelian group. Then  $G^{(m)} \leq G$ .

---

#### Proof

Note that  $1^m = 1 \in G^{(m)}$ .  $\forall g, h \in G^{(m)}$ , since  $G$  is abelian, we have that<sup>1</sup>

$$(gh)^m = g^m h^m = 1 \cdot 1 = 1.$$

Therefore  $gh \in G^{(m)}$ . Also, for  $g \in G^{(m)}$ , we have

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

Thus  $g^{-1} \in G^{(m)}$ . By the **Subgroup Test**, we have that  $G^{(m)} \leq G$ .  $\square$

<sup>1</sup> Pay attention that this is only true if  $G$  is abelian.

---

**Proposition 51 (Decomposition of a Finite Abelian Group)**

Let  $G$  be a finite abelian group with  $|G| = mk$  such that  $\gcd(m, k) = 1$ .  
Then

1.  $G \cong G^{(m)} \times G^{(k)}$ ; and
2.  $|G^{(m)}| = m$  and  $|G^{(k)}| = k$ .

**Proof**

1. Since  $G$  is abelian,  $G^{(m)} \triangleleft G$  and  $G^{(k)} \triangleleft G$ .

Claim 1:  $G^{(m)} \cap G^{(k)} = \{1\}$

**Proof of Claim 1:**  $\forall g \in G^{(m)} \cap G^{(k)}, g^m = 1 = g^k$

$\therefore \gcd(m, k) = 1$ , by **Bezout's Lemma**,  $\exists x, y \in \mathbb{Z} \quad 1 = mx + ky$

$$\implies g = g^1 = g^{mx+ky} = (g^m)^x (g^k)^y = 1 \cdot 1 = 1$$

$\implies G^{(m)} \cap G^{(k)} = \{1\}$  as claimed.

Claim 2:  $G = G^{(m)} G^{(k)}$  <sup>2</sup>

<sup>2</sup> Recall that this is the Product

$$\forall g \in G \quad \therefore o(g) = mk \quad 1 = g^{mk} = (g^k)^m = (g^m)^k$$

It follows that  $g^k \in G^{(m)}$  and  $g^m \in G^{(k)}$ . From **Claim 1** and by abelianness, we have that

$$g = g^{mx+ky} = (g^k)^y (g^m)^x \in G^{(m)} G^{(k)}$$

Thus  $G \subseteq G^{(m)} G^{(k)}$ . On the other hand, since  $G^{(m)} \triangleleft G$  and  $G^{(k)} \triangleleft G$ , by **Lemma 29**, we have that  $G^{(m)} G^{(k)} \leq G$  and hence  $G^{(m)} G^{(k)} \subseteq G$ .

Thus  $G = G^{(m)} G^{(k)}$  as claimed.

From **Claims 1 and 2**, we can conclude by **Corollary 33**<sup>3</sup>, that  $G \cong G^{(m)} \times G^{(k)}$  as required.

<sup>3</sup> Should this not be **Theorem 32**?

2. Write  $|G^{(m)}| = m'$  and  $|G^{(k)}| = k'$ . By part (1), we have that  $mk = |G| = m'k'$ .

Claim 3:  $\gcd(m, k') = 1$

Suppose not

$$\implies \exists p \text{ prime} \quad p \mid m \text{ and } p \mid k'$$

$$\implies \exists g \in G^{(k)} \quad o(g) = p \quad \therefore \text{Cauchy's Theorem}$$

$$\text{Now } p \mid m \implies \exists q \in \mathbb{Z} \quad m = pq$$

$$\implies g^m = g^{pq} = 1 \quad \therefore o(g) = p$$

$$\implies g \in G^{(m)}.$$

By part (1), we have that  $g \in G^{(m)} \cap G^{(k)} = \{1\} \implies g = 1$ , which

contradicts the fact that  $o(g) = p$ . Thus  $\gcd(m, k') = 1$  as claimed. Similarly, we can get that  $\gcd(m', k) = 1$ .

Notice that  $mk = m'k' \implies m \mid m'k'$   
 $\implies m \mid m' \quad \because \gcd(m, k') = 1$  and similarly  $k \mid k'$ . But then  $mk = m'k'$  would imply that  $m' = m$  and  $k' = k$ .

□

---

As a direct consequence of Proposition 51, we have the following:

---

### Theorem 52 (Primary Decomposition)

Let  $G$  be a finite abelian group with  $|G| = p_1^{n_1} \dots p_k^{n_k}$ , where  $p_1, \dots, p_k$  are distinct primes, and  $n_1, \dots, n_k \in \mathbb{N}$ . Then

1.  $G \cong G^{(p_1^{n_1})} \times \dots \times G^{(p_k^{n_k})}$ ; and
  2.  $\forall i \ 1 \leq i \leq k \quad \left| G^{(p_i^{n_i})} \right| = p_i^{n_i}$ .
- 

## 18.1.2 $p$ -Groups

On a related note of the groups  $G^{(p_i^{n_i})}$ , we define the following:

### Definition 30 (p-Group)

Let  $p$  be a prime. A  **$p$ -group** is a group in which every element has an order that is a non-negative power of  $p$ .

---

### Proposition 53 (p-Groups are Finite)

A finite group  $G$  is a  $p$ -group  $\iff |G|$  is a power of  $p$  (including  $p^0$ ).

---

### Proof

( $\Leftarrow$ ) If  $|G| = p^\alpha$  for some  $\alpha \in \mathbb{N} \cup \{0\}$  and  $g \in G$ , by Corollary 24,  $o(g) \mid p^\alpha$

$\implies G$  is a  $p$ -group.

( $\implies$ ) Consider the contrapositive and let  $|G| = p^n p_2^{n_2} \dots p_k^{n_k}$  where  $p, p_2, \dots, p_k$  are distinct primes,  $n \in \mathbb{N} \cup \{0\}$ , and  $n_2, \dots, n_k \in \mathbb{N}$ . For  $k \geq 2$ , by *Cauchy's Theorem*,  $p_2 \mid |G|$

$\implies \exists g_1 \in G \quad o(g_1) = p_2$

$\implies G$  is not a  $p$ -group.

Therefore, our desired result follows.  $\square$

OUR END GOAL here is to prove to ourselves that all finite abelian groups can be written as cross products of cyclic groups, i.e. if  $G$  is an abelian group, then

$$G \cong C_1 \times C_2 \times \dots \times C_n.$$

With *Theorem 52*, we have that

$$G \cong G_1 \times G_2 \times \dots \times G_n.$$

The following proposition will enable us to get to our goal from our current position:

**Proposition (Finite Abelian  $p$ -Groups of order  $p$  are Cyclic)**

If  $G$  is a finite abelian  $p$ -group that contains only one subgroup of order  $p$ , where  $p$  is prime, then  $G$  is cyclic. In other words, if a finite abelian  $p$ -group is not cyclic, then it must have at least 2 subgroups of order  $p$ .

# 19 Lecture 19 Jun 15th 2018

## 19.1 Finite Abelian Groups (Continued)

### 19.1.1 $p$ -Groups (Continued)

---

#### Note (Recall)

Recall the definition of a  $p$ -group:

$G$  is a  $p$ -group if the order of all of its elements is a non-negative power of  $p \iff |G| = p^k$  for some  $k \in \mathbb{N} \cup \{0\}$ .

---

We shall now proceed to prove the proposition mentioned by the end of last class.

---

#### Proposition 54 (Finite Abelian $p$ -Groups of Order $p$ are Cyclic)

If  $G$  is a finite abelian  $p$ -group that contains only 1 subgroup of order  $p$ , then  $G$  is cyclic. In other words, if a finite abelian  $p$ -group is not cyclic, then  $G$  has at least 2 subgroups of order  $p$ .

---

#### Proof

Since  $G$  is finite, let  $y \in G$  have maximal order.

Claim:  $G = \langle y \rangle$

**Proof of Claim:** Suppose not. Since  $\langle y \rangle \triangleleft G$ <sup>1</sup>, consider the quotient group  $G/\langle y \rangle$ , which is, therefore, a nontrivial  $p$ -group, since  $|\langle y \rangle| = p$ .

By Cauchy's Theorem, we know that  $\exists z \in G/\langle y \rangle$  such that  $o(z) = p$ <sup>2</sup>. In particular, we have that  $z \neq 1$ <sup>3</sup>. Consider the coset map

<sup>1</sup> We have  $\langle y \rangle \leq G$  and  $G$  is abelian.

<sup>2</sup> Note that we have  $G/\langle y \rangle$  is a  $p$ -group  $\iff |G/\langle y \rangle| = p^k$  for some  $k \in \mathbb{N} \cup \{0\}$ . The existence of our chosen  $z$  follows from there by Cauchy's Theorem.

<sup>3</sup> If  $z = 1$ , then its order would not be  $p$ .

$$\pi : G \rightarrow G/\langle y \rangle.$$

Let  $x \in G$  such that  $\pi(x) = z$ <sup>4</sup>. Since

$$\pi(x^p) = \pi(x)^p = z^p = 1,$$

we have that  $x^p$  gets mapped to 1 by  $\pi$ , i.e.  $x^p \in \langle y \rangle$ .

$\implies \exists m \in \mathbb{Z}$  such that  $x^p = y^m$ . We shall consider two cases:

**Case 1:**  $p \nmid m$ .

$\because p \nmid m$ , we have that  $\gcd(m, |\langle y \rangle|) = 1$ , and hence by *Proposition 18*<sup>5</sup>, we have that  $o(y^m) = o(y)$ . Because  $y$  has maximal order, we have

$$o(x^p) \stackrel{(1)}{<} o(x) \leq o(y) = o(y^m) = o(x^p)$$

where note that (1) is true because  $x$  would need to take more powers of  $p$  than  $x^p$  to get back to 1. We observe that we have arrived at a contradiction.

**Case 2:**  $p \mid m$ .

$$p \mid m \implies \exists k \in \mathbb{Z} \ m = pk \implies x^p = y^m = y^{pk}$$

$$\because G \text{ is abelian, we have that } (xy^{-k})^p = 1.$$

By assumption, there is only one subgroup of  $G$  of order  $p$ , call it  $H$ .

Thus  $xy^k \in H$ . On the other hand, by the *Fundamental Theorem of Finite Cyclic Groups*<sup>6</sup>,  $\langle y \rangle$  has only one subgroup of order  $p$ , which must be  $H$ . Therefore, in particular, we have  $xy^{-k} \in \langle y \rangle$  which implies  $x \in \langle y \rangle$ . It follows that  $z = \pi(x) = 1$  since  $\langle y \rangle$  is the identity in the quotient group  $G/\langle y \rangle$ , which contradicts our choice of  $z \neq 1$ .

Therefore, by combining the two cases, we have that  $G = \langle y \rangle$ . □

<sup>4</sup> Recall that  $\pi$  is surjective by *Proposition 35*.

<sup>5</sup>

**Proposition (Proposition 18)**

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

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

<sup>6</sup>

**Theorem (Theorem 19)**

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

1.  $H$  is a subgroup of  $G \implies \exists d \in \mathbb{N} \ d \mid n \quad H = \langle g^d \rangle \implies |H| \mid n$ .
2.  $k \mid n \implies \langle g^{\frac{k}{n}} \rangle$  is the unique subgroup of  $G$  of order  $k$ .

**Proposition 55**

Let  $G \neq \{1\}$  be a finite abelian  $p$ -group that contains one subgroup of order  $p$ . Let  $C$  be the cyclic subgroup of  $G$  of maximal order. Then  $\exists B \leq G$  such that  $G = CB$  and  $C \cap B = \{1\}$ . By *Corollary 33*, we have  $G \cong C \times B$ .

**Proof**

We shall prove this result by induction. If  $|G| = p$ , then  $C = G$  by definition and we can choose  $B = \{1\}$ . The result follows from there.

Suppose that the result holds for all groups of order  $p^{n-1}$  with  $n \in \mathbb{N}$  and  $n \geq 2$ . Consider the case for  $|G| = p^n$ . There are two cases to consider from here.

**Case 1:** If  $C = G$ , then we can pick  $B = \{1\}$  so that the result follows.

**Case 2:** If  $C \neq G$ , then  $G$  is not cyclic. By Proposition 54, there exists at least 2 subgroups of  $G$  that are of order  $p$ . Since  $C$  is cyclic, by the Fundamental Theorem for Finite Cyclic Groups, we have that  $C$  contains exactly one subgroup of order  $p$ . Then  $\exists D \leq G$  such that  $|D| = p$  and  $D \not\subseteq C$ , and consequently  $C \cap D = \{1\}$ . Now since  $G$  is abelian,  $D \triangleleft G$  and hence we may consider its coset map:

$$\pi : G \rightarrow G/D.$$

If we consider  $\pi|_C$ , called the **restriction** of  $\pi$  on  $C$ <sup>7</sup>, then  $\ker \pi|_C = C \cap D = \{1\}$ . Then by the First Isomorphism Theorem, we have

$$C \cong C / \ker \pi|_C \cong \text{im } \pi|_C = \pi(C).$$

Now let  $y$  be the generator of the cyclic group  $C$ . Then since  $\pi(C) \cong C$ , we have  $\pi(C) = \langle \pi(y) \rangle$ . By assumption on  $C$ ,  $\pi(C)$  is the cyclic subgroup of  $G/D$  of maximal order<sup>8</sup>. Since  $|G/D| = p^{n-1}$  by Lagrange's Theorem, and by the induction hypothesis,  $G/D$  has a subgroup  $E$  such that  $\pi(C)E = G/D$  and  $\pi(C) \cap E = \{1\}$ .

Therefore, choose  $B = \pi^{-1}(E)$ , i.e.  $\pi(B) = E$ .

**Claim 1:**  $G = CB$

Note that  $D \subseteq B$ <sup>9</sup>. If  $x \in G$ ,  $\therefore \pi(x) \in \pi(C)\pi(B) = \pi(C)E = G/D$ , we have that  $\exists u \in C$ ,  $\exists v \in B$  such that

$$\pi(x) = \pi(u)\pi(v).$$

By homomorphism, we have  $\pi(xu^{-1}v^{-1}) = 1$  which implies  $xu^{-1}v^{-1} \in D \subseteq B$ . Then because  $v \in B$ , we have that  $xu^{-1} \in B$  since  $B$  is a group. Then since  $G$  is abelian, we have

$$x = uxu^{-1} \in CB.$$

**Claim 2:**  $C \cap B = \{1\}$ .

Let  $x \in C \cap B$ . Then  $\pi(x) \in \pi(C) \cap \pi(B) = \pi(C) \cap E = \{1\}$ . Then,  $\therefore \pi(x) = 1 \in C/D$ , we have that  $x \in D$ . Therefore,  $x \in C \cap D = \{1\}$  which then  $x = 1$ .

<sup>7</sup> The restriction of  $\pi$  on  $C$  simply means that we restrict the domain of  $\pi$  to work solely for the subset  $C$ . In plain words, we are only considering the case where  $\pi$  is applied onto elements of  $C$ .

<sup>8</sup> Since  $C \cong \pi(C)$ , this is a clear result. Otherwise, if there is some other  $\pi(K)$  that has a larger order than  $\pi(C)$ , then by  $\pi^{-1}(K)$ , we will get some cyclic subgroup that has an order that is larger than  $C$ , which is a clear contradiction to our assumption.

<sup>9</sup> Note that  $E$  is a subgroup of  $G/D$ , so the identity of  $G/D$ ,  $D$  must be in  $E$ . Therefore, we clearly have  $D \subseteq B$ .





## 20 Lecture 20 Jun 18th 2018

### 20.1 Finite Abelian Groups (Continued 2)

#### 20.1.1 $p$ -Groups (Continued 2)

Recall that we had the following subgroup of a group  $G$ .

$$G^{(m)} = \{g \in G : g^m = 1\}.$$

We discussed about the Primary Decomposition, Theorem 52, and then arrived at Proposition 55. With these, we can have the following theorem:

---

#### Theorem 56 (Finite Abelian Groups are Isomorphic to a Direct Product of Cyclic Groups)

*Let  $G \neq \{1\}$  be a finite abelian  $p$ -group. Then  $G$  is isomorphic to a direct product of cyclic groups.*

---

#### Proof

By Proposition 55, there is a cyclic group  $C_1$  and a subgroup  $B_1$  of  $G$ , such that  $G \cong C_1 \times B_1$ . Since  $B_1 \leq G$ , we have that  $|B_1| \mid |G|$ , and so by Theorem 23,  $B_1$  is also a  $p$ -group. If  $B_1 \neq \{1\}$ , then by Proposition 55, there exists a cyclic group  $C_2$  and a  $B_2 \leq B_1$  such that  $B_1 \cong C_2 \times B_2$ .

By continuing this line of argument, we can get  $C_1, C_2, \dots$  until we get to some  $C_k$  with  $B_k = \{1\}$ , for some  $k \in \mathbb{N}$ . Then

$$G \cong C_1 \times C_2 \times \dots \times C_k$$

as required. □

### Remark

We can verify that the decomposition of a finite abelian  $p$ -group into a direct product of cyclic groups is in fact unique up to their orders.<sup>1</sup>

<sup>1</sup> This is the bonus question on A4. It will be included once the assignment is over.

Combining the above remark, Theorem 52 and Theorem 56, we have the following theorem.

### Theorem 57 (Finite Abelian Group Structure)

If  $G$  is a finite abelian group, then

$$G \cong C_{p_1^{n_1}} \times \dots \times C_{p_k^{n_k}}$$

where  $C_{p_i^{n_i}}$  is a cyclic group of order  $p_i^{n_i}$ , where  $1 \leq i \leq k$ . The numbers  $p_i^{n_i}$  are uniquely determined up to their order.<sup>2</sup>

<sup>2</sup> Note that the  $p_i$ 's do not have to be unique.

### Remark

Note that if  $p_1$  and  $p_2$  are distinct primes, then

$$C_{p_1^{n_1}} \times C_{p_2^{n_2}} \cong C_{p_1^{n_1} p_2^{n_2}},$$

the cyclic group of order  $p_1^{n_1} p_2^{n_2}$ . Thus, by combining suitable prime factors together, for a finite abelian group  $G$ , we can also write

$$G \cong \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \dots \times \mathbb{Z}_{m_r},$$

where  $m_i \in \mathbb{N}$ ,  $i \leq 1 \leq r$ ,  $m_1 > 1$  and

$$m_1 \mid m_2 \mid \dots \mid m_r$$

### Example 20.1.1

Consider an abelian group  $G$  with order 48. Since  $48 = 2^4 \cdot 3$ , an abelian group of order 48 is isomorphic to  $H \times \mathbb{Z}_3$ , where  $H$  is an abelian group of order  $2^4$ . The options for  $H$  are:

$$\begin{array}{ccc} \mathbb{Z}_{2^4} & \mathbb{Z}_{2^3} \times \mathbb{Z}_2 & \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \\ \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2 & \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 & \end{array}$$

Therefore, we have the following possible decompositions of  $G$ :

$$G \cong \mathbb{Z}_{2^4} \times \mathbb{Z}_3 \cong \mathbb{Z}_{48}$$

$$G \cong \mathbb{Z}_{2^3} \times \mathbb{Z}_2 \times \mathbb{Z}_3 = \mathbb{Z}_2 \times \mathbb{Z}_{24}$$

$$G \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_{2^2} \times \mathbb{Z}_3 = \mathbb{Z}_4 \times \mathbb{Z}_{12}$$

$$G \cong \mathbb{Z}_{2^2} \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{12}$$

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_6$$

## 20.2 Rings

### 20.2.1 Rings

#### Definition 31 (Ring)

A set  $R$  is a ring if  $\forall a, b, c \in R$ ,

1.  $a + b \in R$
2.  $a + b = b + a$
3.  $a + (b + c) = (a + b) + c$
4.  $\exists 0 \in R \ a + 0 = a = 0 + a$
5.  $\exists (-a) \in R \ a + (-a) = 0 = (-a) + a$
6.  $ab \in R$
7.  $a(bc) = (ab)c$
8.  $\exists 1 \in R \ 1 \cdot a = a = a \cdot 1$
9.  $a(b + c) = ab + ac$  and  $(b + c)a = ba + ca$

We call  $1$  as the **Unity** of  $R$ ,  $0$  as the **Zero** of  $R$ , and  $-a$  as the **negative** of  $a$ .

The ring  $R$  is called a **Commutative Ring** if it also satisfies the following:

10.  $ab = ba$ .

As daunting as this definition seems, it is much easier to remember if we think of  $R$  being an **abelian group under addition**, “almost” a group under **multiplication**, save the fact that the **multiplicative inverse of an element does not necessarily exist**, and with the **distributive law**.

#### Example 20.2.1

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}$  and  $\mathbb{C}$  are commutative rings with the zero being 0, and unity being 1.

**Example 20.2.2**

For  $n \in \mathbb{N}$ ,  $n \geq 2$ ,  $\mathbb{Z}_n$  is a commutative ring with the zero being  $[0]$ , and unity being  $[1]$ .

**Example 20.2.3**

The set  $M_n(\mathbb{R})$  is a ring using matrix addition and matrix multiplication, with zero being the zero matrix  $0$ , and unity being the identity matrix  $I$ . We also know that  $M_n(\mathbb{R})$  is not commutative.

---

**Warning**

Note that since  $(R, \cdot)$  is not a group, we no longer have the liberty of using *Proposition 6*, i.e. we do not have left or right cancellation. For example, in  $\mathbb{Z}$ ,  $0 \cdot x = 0 \cdot y \not\Rightarrow x = y$ .

---

## 21 Lecture 21 Jun 20th 2018

### 21.1 Rings (Continued)

#### 21.1.1 Rings (Continued)

---

##### Note (Notation)

Given a ring  $R$ , to distinguish the difference between multiples in addition and in multiplication, for  $n \in \mathbb{N} \wedge a \in R$ , we write

$$na = \underbrace{a + a + \dots + a}_{n \text{ times}}$$

and

$$a^n = \underbrace{a \cdot a \cdot \dots \cdot a}_{n \text{ times}}$$

respectively. Also, we will define

$$(-n)a = \underbrace{(-a) + (-a) + \dots + (-a)}_{n \text{ times}}$$

and

$$a^{-n} = \left(a^{-1}\right)^n$$

if  $a^{-1}$  exists.

---

##### Note

Recall that for a group  $G$  and  $g \in G$ , we have  $g^0 = 1$ ,  $g^1 = g$ , and

$(g^{-1})^{-1} = g$ . Thus for addition, we have

$$\begin{array}{c}
 \text{integer} \\
 \uparrow \\
 0 \cdot a = 0 \quad 1 \cdot a = a \\
 \downarrow \\
 \text{zero in } R \\
 -(-a) = a
 \end{array}$$

Also, by Proposition 5, if  $n, m \in \mathbb{Z}$ , we have

$$\begin{aligned}
 m \cdot a + n \cdot a &= (m + n) \cdot a \\
 n(ma) &= (nm)a \\
 n(a + b) &= na + nb
 \end{aligned}$$

---

### Proposition 58 (More Properties of Rings)

Let  $R$  be a ring and  $r, s \in R$ .

1. If  $0$  is the zero of  $R$ , then  $0 \cdot r = 0 = r \cdot 0$ ; <sup>1</sup>
2.  $-r(s) = -(rs) = r(-s)$ ;
3.  $(-r)(-s) = rs$ ;
4.  $\forall m, n \in \mathbb{Z}, (mr)(ns) = (mn)(rs)$ .

This is a problem in A4.

<sup>1</sup> i.e. all the  $0$ 's are zeros of  $R$ .

---

### Definition 32 (Trivial Ring)

A **trivial ring** is a ring of only one element. In this case, we have  $1 = 0$ , i.e. the unity is the zero and vice versa.

---

### Remark

If  $R$  is a ring with  $R \neq \{0\}$ , since  $r = r \cdot 1$  for all  $r \in R$ , we have  $1 \neq 0$ . Otherwise, if  $1 = 0$ , then  $r = r \cdot 1 = r \cdot 0 = 0$ , i.e.  $R = \{0\}$ .

### Example 21.1.1

Let  $R_1, R_2, \dots, R_n$  be rings. We define component-wise operation on the

product

$$R_1 \times R_2 \times \dots \times R_n$$

as follows:

$$(r_1, r_2, \dots, r_n) + (s_1, s_2, \dots, s_n) = (r_1 + s_1, r_2 + s_2, \dots, r_n + s_n)$$

$$(r_1, r_2, \dots, r_n)(s_1, s_2, \dots, s_n) = (r_1 s_1, r_2 s_2, \dots, r_n s_n)$$

We can check that  $R_1 \times R_2 \times \dots \times R_n$  is a ring with the zero being  $(0, 0, \dots, 0)$  and the unity being  $(1, 1, \dots, 1)$ . This set

$$R_1 \times R_2 \times \dots \times R_n$$

is called the **direct product** of  $R_1, R_2, \dots, R_n$ .

### Definition 33 (Characteristic of a Ring)

If  $R$  is a ring, we define the **characteristic** of  $R$ , denoted by  $\text{ch}(R)$ , in terms of the order of  $1_R$  in the additive group  $(R, +)$ , by

$$\text{ch}(R) = \begin{cases} n & \text{if } o(1_R) = n \in \mathbb{N} \text{ in } (R, +) \\ 0 & \text{if } o(1_R) = \infty \text{ in } (R, +) \end{cases}$$

For  $k \in \mathbb{Z}$ , we write  $kR = 0$  to mean that  $\forall r \in R, kr = 0$ .

By Proposition 58, we have

$$kr = k(1_R \cdot r) = (k1_R) \cdot r$$

and so  $kR = 0$  if and only if  $k1_R = 0$ . Then, since  $(R, +)$  is a group, by Proposition 13 and Proposition 14, it follows that:

### Proposition 59 (Implications of the Characteristic)

Let  $R$  be a ring and  $k \in \mathbb{Z}$ .<sup>2</sup>

1.  $\text{ch}(R) = n \in \mathbb{N} \implies (kR = 0 \iff n \mid k)$
2.  $\text{ch}(R) = 0 \implies (kR = 0 \iff k = 0)$

<sup>2</sup> This is why we defined  $\text{ch}(R) = 0$  if  $o(1_R) = \infty$

### Example 21.1.2

Each of  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$  and  $\mathbb{C}$  has characteristic 0. For  $n \in \mathbb{N}$  with  $n \geq 2$ , the ring  $\mathbb{Z}_n$  has characteristic  $n$ .

### 21.1.2 Subring

#### Definition 34 (Subring)

A subset  $S$  of a ring  $R$  is a subring if  $S$  is a ring itself (under the same operations: addition and multiplication).

Note that properties (2), (3), (7) and (9) from Definition 31 are automatically satisfied. Thus, to show that  $S$  is a subring, it suffices to show the following:

#### Subring Test

1.  $0, 1 \in S$ <sup>3</sup>
2.  $s, t \in S \implies (s - t), st \in S$

#### Example 21.1.3

We have the following chain of commutative rings:

$$\mathbb{Z} \leq_r \mathbb{Q} \leq_r \mathbb{R} \leq_r \mathbb{C}$$

#### Example 21.1.4

If  $R$  is a ring, the center  $Z(R)$  of  $R$  is defined as

$$Z(R) = \{z \in R : zr = rz, r \in R\}.$$

Note that  $0, 1 \in Z(R)$ . Also, if  $s, t \in Z(R)$ , then  $\forall r \in R$ ,

$$(s - t)r = sr - tr = rs - rt = r(s - t)$$

and so  $(s - t) \in Z(R)$ . Also,

$$(st)r = s(tr) = s(rt) = (sr)t = (rs)t = r(st)$$

and so  $st \in Z(R)$ . By the **Subring Test**,  $Z(R) \leq_r R$ .

#### Example 21.1.5

Unlike subgroups, since there is no proper suggestion of a symbolic representation, I shall use  $S \leq_r R$  to denote that  $S$  is a subring of  $R$ , in comparison to  $\leq$  for subgroups, which has no subscript. Note that this is purely for keeping my writing succinct, and so the subscript  $r$  is used simply to indicate that the  $\leq$  symbol is for denoting a subring and should not be confused with other  $r$ 's that may be used in a proof. This notation is also not used in class, and should be avoided during materials outside of this set of notes.

<sup>3</sup> The  $0 \in S$  is certainly not necessary to be shown, since from part (2) we would have  $s \in S \implies 0 \in (s - s) \in S$ .







## 22 Lecture 22 Jun 22nd 2018

### 22.1 Ring (Continued 2)

#### 22.1.1 Ideals

Let  $R$  be a ring and  $A$  an additive subgroup of  $R$ . Since  $(R, +)$  is abelian, we have that  $A \triangleleft R$ . Thus, we can talk about the additive quotient group

$$\begin{aligned} R/A &= \{r + a : r \in R\} \text{ with} \\ r + A &= \{r + a : a \in A\} \end{aligned}$$

Using the properties that we know about cosets and quotient groups, we have the following proposition.

---

#### Proposition 60 (Properties of the Additive Quotient Group)

Let  $R$  be a ring and  $A$  an additive subgroup of  $R$ . For  $r, s \in R$ , we have

1.  $r + A = s + A \iff (r - s) \in A$
2.  $(r + A) + (s + A) = (r + s) + A$
3.  $0 + A = A$  is the additive identity of  $R/A$
4.  $-(r + A) = (-r) + A$  is the additive inverse of  $r + A$
5.  $\forall k \in \mathbb{Z} \quad k(r + A) = kr + A$

This is just a translation of the properties of cosets and quotient groups, that we are familiar with, into the language of addition. You can (read: should) prove this as an exercise for yourself (read: myself).

---

Since  $R$  is a ring, it is natural to ask if we could make  $R/A$  into a ring<sup>1</sup>. A natural way to define “multiplication” in  $R/A$  is

<sup>1</sup> Ideally (see what I did there?), we would want  $R/A$  as a ring, just as we had  $R/A$  as a group.

$$(r + A)(s + A) = rs + A \quad \forall r, s \in R \quad (\dagger)$$

Note, however, that we would have

$$r + A = r_1 + A \quad s + A = s_1 + A$$

with  $r \neq r_1$  and  $s \neq s_1$ . In order for  $(\dagger)$  to make sense, it is necessary that

$$r + A = r_1 + A \wedge s + A = s_1 + A \implies rs + A = r_1s_1 + A$$

so that this “multiplication” is **well-defined**.

### Proposition 61

Let  $A$  be an additive subgroup of a ring  $R$ . Then  $\forall a \in A$ , define

$$Ra = \{ra : r \in R\} \quad aR = \{ar : r \in R\}.$$

The following are equivalent (TFAE):

1.  $Ra \subseteq A$  and  $aR \subseteq A, \forall a \in A$ ;
2.  $\forall r, s \in R, (r + A)(s + A) = rs + A$  is well-defined in  $R/A$ .

### Proof

(1)  $\implies$  (2): If  $r + A = r_1 + A$  and  $s + A = s_1 + A$ , for  $r, r_1, s, s_1 \in R$ , we need to show that

$$rs + A = r_1s_1 + A.$$

By Proposition 60, we have that  $(r - r_1), (s - s_1) \in A$ , and so by (1), we have

$$\begin{aligned} rs - r_1s_1 &= rs - r_1s + r_1s - r_1s_1 \\ &= (r - r_1)s + r_1(s - s_1) \\ &\in (r - r_1)R + R(s - s_1) \subseteq A \end{aligned}$$

Therefore, by Proposition 60 again, we have  $rs + A = r_1s_1 + A$ .

(2)  $\implies$  (1): Let  $r \in R$  and  $a \in A$ . We have that

$$\begin{aligned}
 ra + A &= (r + A)(a + A) && \because (2) \\
 &= (r + A)(0 + A) && \because a, 0 \in A \\
 &\quad \downarrow \\
 &\quad \text{zero of } R \\
 &= (r \cdot 0) + A && \because (2) \\
 &= 0 + A && \because \text{Proposition 58} \\
 &= A && \because \text{Proposition 60}
 \end{aligned}$$

Thus  $ra \in A$  and so  $Ra \subseteq A$ . Similarly, we can show that  $aR \subseteq A$ .  $\square$

### Definition 35 (Ideal)

An additive subgroup  $A$  of a ring  $R$  is called an **ideal** of  $R$  if  $Ra, aR \subseteq A, \forall a \in A$ .

### Example 22.1.1

If  $R$  is a ring,  $\{0\}$  and  $R$  are both ideals of  $R$ .

### Proposition 62 (The Only Ideal with the Multiplicative Identity is the Ring Itself)

Let  $A$  be an ideal of a ring  $R$ . If  $1 \in A$ , then  $A = R$ .

This also shows that if we want a non-trivial ideal, then the ideal should not have 1.

### Proof

$\forall r \in R, \because A$  is an ideal and  $1 \in A$ , we have  $r = r \cdot 1 \in A$ . It follows that  $R \subseteq A \subseteq R$  and so  $R = A$ .  $\square$

### Proposition 63 (Construction of the Quotient Ring)

Let  $A$  be an ideal of a ring  $R$ . Then the additive quotient group  $R/A$  is a ring with the multiplication  $(r + A)(s + A) = rs + A, \forall r, s \in R$ . The unity of  $R/A$  is  $1 + A$ .

**Proof**

$\therefore A$  is an additive subgroup of a ring  $R$ ,  $R/A$  is an additive abelian group. By Proposition 61, the multiplication on  $R/A$  is well-defined. The multiplication is associative, since  $\forall r, s, q \in R$ ,

$$\begin{aligned}(r + A)((s + A)(q + A)) &= (r + A)(sq + A) = (rsq + A) \\ &= (rs + A)(q + A) \\ &= ((r + A)(s + A))(q + A).\end{aligned}$$

We also have

$$(r + A)(1 + A) = r + A = (1 + A)(r + A)$$

and so the unity of  $R/A$  is  $1 + A$ . The distributive property is inherited from  $R$ .  $\square$

**Definition 36 (Quotient Ring)**

Let  $A$  be an ideal of a ring  $R$ . Then the ring  $R/A$  is called the **quotient ring** of  $R$  by  $A$ .

**Definition 37 (Principal Ideal)**

Let  $R$  be a commutative ring and  $A$  an ideal of  $R$ . If  $A = aR = \{ar : r \in R\} = Ra$  for some  $a \in A$ , we say that  $A$  is a **principal ideal** generated by  $a$ , and denote  $A = \langle a \rangle$ .

**Example 22.1.2**

If  $n \in \mathbb{Z}$ , then  $\langle n \rangle = n\mathbb{Z}$  is a(n) (principal) ideal of  $\mathbb{Z}$ , since  $\mathbb{Z}$  is commutative.

**Proposition (Ideals of  $\mathbb{Z}$  are Principal Ideals)**

All ideals of  $\mathbb{Z}$  are of the form  $\langle a \rangle$  for some  $n \in \mathbb{Z}$ .

---

We shall prove this in the next lecture.





## 23 Lecture 23 Jun 25th 2018

### 23.1 Ring (Continued 3)

#### 23.1.1 Ideals (Continued)

---

##### Proposition 64 (Ideals of $\mathbb{Z}$ are Principal Ideals)

All ideals of  $\mathbb{Z}$  are of the form  $\langle n \rangle$  for some  $n \in \mathbb{Z}$ .

---

##### Proof

Let  $A$  be an ideal of  $\mathbb{Z}$ . If  $A = \{0\}$ , then  $A = \langle 0 \rangle$ . Otherwise, let  $a \in A$  with  $a \neq 0$ , and  $|a|$  be the minimum. Clearly,  $\langle a \rangle = a\mathbb{Z} \subseteq A$ . To prove the other inclusion, let  $b \in A$ . By the **Division Algorithm**,  $\exists q, r \in \mathbb{Z}$  with  $0 \leq r < |a|$  such that  $b = qa + r$ . Because  $A$  is an ideal, we have  $r = b - qa \in A$ . Since  $|r| < |a|$  which is the minimal case, it must be that  $r = 0$ . Therefore  $b = qa \in \langle a \rangle$  and so  $A \subseteq \langle a \rangle$ .  $\square$

---

#### 23.1.2 Isomorphism Theorems for Rings

---

##### Definition 38 (Ring Homomorphism)

Let  $R$  and  $S$  be rings. A mapping

$$\Theta : R \rightarrow S$$

is a ring **homomorphism** if  $\forall a, b \in R$ , we have

1.  $\Theta(a + b) = \Theta(a) + \Theta(b)$
2.  $\Theta(ab) = \Theta(a)\Theta(b)$
3.  $\Theta(1_R) = 1_S$

**Note (Remark)**

(2)  $\not\Rightarrow$  (3) because  $\Theta(1_R) \in S$  does not necessarily have a multiplicative inverse, since  $S$  is a ring.

**Example 23.1.1**

The mapping  $k \mapsto [k]$  from  $\mathbb{Z} \rightarrow \mathbb{Z}_n$  is a surjective ring homomorphism.

**Example 23.1.2 (Direct Product of Rings)**

If  $R_1, R_2$  are rings, the projection

$$\pi_1 : R_1 \times R_2 \rightarrow R_1 \text{ defined by } \pi_1(r_1, r_2) = r_1$$

is a surjective ring homomorphism, since

1.  $\pi_1(r_1 + r_2, q_1 + q_2) = r_1 + r_2 = \pi_1(r_1, q_1) + \pi_1(r_2, q_2);$
2.  $\pi_1(r_1 r_2, q_1 q_2) = r_1 r_2 = \pi_1(r_1, q_1) \pi_1(r_2, q_2);$  and
3.  $\pi(1, 1) = 1.$

We can a similar  $\pi_2 : R_1 \times R_2 \rightarrow R_2$  such that  $(r_1, r_2) \mapsto r_2$ , and we will get that  $\pi_2$  is also a surjective ring homomorphism.

**Proposition 65 (Properties of Ring Homomorphisms)**

Let  $\Theta : R \rightarrow S$  be a ring homomorphism and let  $r \in R$ . Then

1.  $\Theta(0_R) = 0_S$
2.  $\Theta(-r) = -\Theta(r)$
3.  $\Theta(kr) = k\Theta(r)$
4.  $\forall n \in \mathbb{N} \cup \{0\} \quad \Theta(r^n) = \Theta(r)^n$
5.  $u \in R^* \implies \forall k \in \mathbb{Z} \quad \Theta(u^k) = \Theta(u)^k$

---

**Proof**

1. Note that

$$\Theta(r) = \Theta(0_R + r) = \Theta(0_R) + \Theta(r).$$

Therefore,

$$\Theta(0_R) = 0_S$$

as required.

2. Note that

$$0_S = \Theta(0_R) = \Theta(r - r) = \Theta(r) + \Theta(-r),$$

so

$$\Theta(-r) = -\Theta(r).$$

3. Observe that

$$\Theta(kr) = \Theta(\underbrace{r + r + \dots + r}_{k \text{ times}}) = \underbrace{\Theta(r) + \Theta(r) + \dots + \Theta(r)}_{k \text{ times}} = k\Theta(r)$$

Item 4 follows by induction on the definition of a ring homomorphism, and Item 5 follows as a result from Item 4 because if  $u \in R^*$ , then  $u^{-1} \in R^*$  such that  $uu^{-1} = 1_R$ .  $\square$

---

**Definition 39 (Ring Isomorphism)**

A mapping of rings  $\Theta : R \rightarrow S$  is a ring **isomorphism** if  $\Theta$  is a bijective ring homomorphism. In this case, we say that  $R$  and  $S$  are **isomorphic** and denote that by  $R \cong S$ .

---

**Definition 40 (Kernel and Image)**

Let  $\Theta : R \rightarrow S$  be a ring homomorphism. The **kernel** of  $\Theta$  is defined by

$$\ker \Theta = \{r \in R : \Theta(r) = 0_S\}$$

and the **image** of  $\Theta$  is defined by

$$\text{im } \Theta := \Theta(R) = \{\Theta(r) : r \in R\}.$$

**Proposition 66**

Let  $\Theta : R \rightarrow S$  be a ring homomorphism. Then

1.  $\text{im } \Theta \leq_r S$
2.  $\ker \Theta$  is an ideal of  $R$

**Proof**

1.  $\Theta(1_R) = 1_S$  by definition of a homomorphism so  $\Theta(1_R) \in \text{im } \Theta$ .

Suppose  $s_1 = \Theta(r_1)$  and  $s_2 = \Theta(r_2)$ , then

$$s_1 - s_2 = \Theta(r_1) - \Theta(r_2) = \Theta(r_1 - r_2)$$

$$s_1 s_2 = \Theta(r_1) \Theta(r_2) = \Theta(r_1 r_2)$$

are both in  $\text{im } \Theta$ . By the Subring Test,  $\text{im } \Theta \leq_r S$ .

2. Since  $\ker \Theta$  is an additive subgroup of  $R$ , it suffices to show that  $ra, ar \in \ker \Theta$  for all  $r \in R$  and  $a \in \ker \Theta$ . Let  $r \in R$  and  $a \in \ker \Theta$ . Then

$$\Theta(ra) = \Theta(r) \Theta(a) = \Theta(r) \cdot 0 = 0$$

So  $ra \in \ker \Theta$ . Similarly so,

$$\Theta(ar) = \Theta(a) \Theta(r) = 0 \cdot \Theta(r) = 0$$

and so  $ar \in \ker \Theta$ . Therefore,  $\ker \Theta$  is an ideal of  $R$ .

□

**Theorem 67 (First Isomorphism Theorem for Rings)**

Let  $\Theta : R \rightarrow S$  be a ring homomorphism. Then

$$R / \ker \Theta \cong \text{im } \Theta.$$

**Proof**

Let  $A = \ker \Theta$ . Since  $A$  is an ideal of  $R$ , we have that  $R/A$  is a ring.

Define

$$\bar{\Theta} : R/A \rightarrow \text{im } \Theta \text{ by } (r + A) \mapsto \theta(a).$$

Note that

$$r + A = s + A \iff (r - s) \in A \iff \Theta(r - s) = 0 \iff \Theta(r) = \Theta(s).$$

Therefore  $\bar{\Theta}$  is well-defined and injective. Also, it is clear that  $\bar{\Theta}$  is surjective. To show that  $\bar{\Theta}$  is a homomorphism, note that  $\forall r, s \in R$ , we have

$$\begin{aligned} \bar{\Theta}(r + A + s + A) &= \bar{\Theta}(r + s + A) = \Theta(r + s) \\ &= \Theta(r) + \Theta(s) = \bar{\Theta}(r + A) + \bar{\Theta}(s + A). \end{aligned}$$

It follows that  $\bar{\Theta}$  is a ring isomorphism and so

$$R/\ker \Theta \cong \text{im } \Theta$$

as required. □

### Exercise 23.1.1

Let  $A, B \leq_r R$ , where  $R$  is a ring. Prove that

1.  $A \cap B$  is the largest subring of  $R$  contained in both  $A$  and  $B$ .
2. If either  $A$  or  $B$  is an ideal of  $R$ , the sum

$$A + B = \{a + b : a \in A, b \in B\}$$

is a subring of  $R$ , and is the smallest subring of  $R$  that contains both  $A$  and  $B$ .

### Theorem 68 (Second Isomorphism Theorem for Rings)

Let  $A$  be a subring and  $B$  an ideal of a ring  $R$ . Then

1.  $A + B \leq_r R$ ;
2.  $B$  is an ideal of  $A + B$ ;
3.  $A \cap B$  is an ideal of  $A$ ; and
- 4.

$$(A + B)/_B \cong A/(A \cap B)$$

---

**Theorem 69 (Third Isomorphism Theorem for Rings)**

Let  $A$  and  $B$  be ideals of  $R$  with  $A \subseteq B$ , then  $B/A$  is an ideal of  $R/A$  and

$$(R/A) / (B/A) \cong R/B.$$

---

## 24 Lecture 24 Jun 27th 2018

### 24.1 Rings (Continued 4)

#### 24.1.1 Isomorphism Theorems for Rings (Continued)

---

##### Theorem 70 (Chinese Remainder Theorem)

Let  $A$  and  $B$  be ideals of  $R$ .

1.  $A + B = R \implies R/(A \cap B) \cong R/A \times R/B$
2.  $A + B = R \wedge A \cap B = \{0\} \implies R \cong R/A \times R/B$

---

##### Proof

It suffices to prove (1) since if (1) is true and  $A \cap B = \{0\}$ , then (2) immediately follows.

Define

$$\Theta : R \rightarrow R/A \times R/B \quad r \mapsto (r + A, r + B)$$

Then  $\Theta$  is a ring homomorphism<sup>1</sup>.

<sup>1</sup>

---

##### Proof ( $\Theta$ is a ring homomorphism)

$\forall r, s \in R$ , we have

$$\begin{aligned} \Theta(rs) &= (rs + A, rs + B) \\ &\stackrel{(*)}{=} (r + A, r + B)(s + A, s + B) \\ &= \Theta(r)\Theta(s) \end{aligned}$$

##### Exercise 24.1.1

Prove that  $\Theta$  is a ring homomorphism.





Also,  $m\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$  since  $1 = ma + nb$  for some  $a, b \in \mathbb{Z}$  by **Bezout's Lemma**. And so:

---

**Corollary 71**

1. If  $m, n \in \mathbb{N}$  with  $\gcd(m, n) = 1$ , then

$$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$

i.e.

$$\mathbb{Z}_{mn} \cong \mathbb{Z}_m \times \mathbb{Z}_n$$

2. If  $m, n \in \mathbb{N}$  with  $m, n \geq 2$  and  $\gcd(m, n) = 1$ , then

$$\phi(mn) = \phi(m)\phi(n)$$

where  $\phi(m) = |\mathbb{Z}_m^*|$  is **Euler's  $\phi$ -function**.

---

LET  $p$  be a prime. Recall that one consequence of Lagrange's Theorem is that every group  $G$  of order  $p$  is cyclic, i.e.  $G \cong C_p$ .

An analogous notion in rings is the following:

---

**Proposition 72 (Ring With Prime Order Is Isomorphic to Integer Modulo Prime)**

If  $R$  is a non-trivial ring with  $|R| = p$  where  $p$  is prime, then  $R \cong \mathbb{Z}_p$ .

---

**Proof**

Define

$$\Theta : \mathbb{Z}_p \rightarrow R \quad [k] \mapsto k \cdot 1_R.$$

Note that since  $R$  is an additive group with  $|R| = p$ , by Lagrange's Theorem,  $o(1_R) = 1$  or  $p$ . Since  $R$  is non-trivial, we have that  $1_R \neq 0$  by the remark on the definition of a trivial ring, and so  $o(1_R) \neq 1$ . Thus  $o(1_R) = p$ . Then, by Proposition 59, we have

$$[k] = [m] \iff p \mid (k - m) \iff (k - m)1_R = 0 \iff k \cdot 1_R = m \cdot 1_R$$

in  $R$ . Thus,  $\Theta$  is well-defined and injective.  $\Theta$  is also a ring homomorphism <sup>2</sup>.

2

**Exercise 24.1.2**

Prove that  $\Theta$  is a ring homomorphism.

**Proof ( $\Theta$  is a ring homomorphism)**

$\forall [a], [b] \in \mathbb{Z}$ , we have

$$\begin{aligned}\Theta([a][b]) &= \Theta([ab]) = ab \cdot 1_R \\ &= (a \cdot 1_R)(b \cdot 1_R) = \Theta([a])\Theta([b]).\end{aligned}$$

$$\Theta([1]) = 1 \cdot 1_R = 1_R$$

and

$$\begin{aligned}\Theta([a] + [b]) &= \Theta([a + b]) = (a + b) \cdot 1_R \\ &= a \cdot 1_R + b \cdot 1_R = \Theta([a]) + \Theta([b]).\end{aligned}$$

So  $\Theta$  is a ring homomorphism.

Now because  $|\mathbb{Z}_p| = p = |R|$  and  $\Theta$  is injective,  $\Theta$  must be surjective.

Therefore  $\Theta$  is a ring isomorphism and hence  $R \cong \mathbb{Z}_p$  as required.  $\square$

## 24.2 Commutative Rings

### 24.2.1 Integral Domain and Fields

**Definition 41 (Units)**

Let  $R$  be a ring. We say that  $u \in R$  is a **unit** if  $u$  has a multiplicative inverse in  $R$ , and denote it by  $u^{-1}$ . We have

$$uu^{-1} = 1 = u^{-1}u$$

**Note**

If  $u$  is a unit in  $R$ , and  $r, s \in R$ , we have

$$ur = us \implies r = s \quad (\text{Right Cancellation})$$

$$ru = su \implies r = s \quad (\text{Left Cancellation})$$

Let  $R^*$  denote the set of all units in  $R$ . We know that the definition of a ring is that  $R$  is “almost” a group under multiplication except that its elements do not necessarily have multiplicative inverses. Since  $R^*R$  is the set that contains all units, i.e. all elements with multiplicative inverses in  $R$ , we have that  $(R^*, \cdot)$  is a group. This is called the **Group of Units** of  $R$ .

**Example 24.2.1**

Note that 2 is a unit in  $\mathbb{Q}$ , but it is not a unit in  $\mathbb{Z}$ . We have that

$$\mathbb{Q}^* = \mathbb{Q} \setminus \{0\} \text{ and } \mathbb{Z}^* = \{\pm 1\}$$

**Example 24.2.2**

Consider the ring of **Gaussian Integers**,

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}, i^2 = -1\} \subseteq \mathbb{C}.$$

Then<sup>3</sup>

$$\mathbb{Z}[i]^* = \{\pm 1, \pm i\}.$$

<sup>3</sup> Proof to be added once A4 is over.

**Definition 42 (Division Ring and Field)**

A non-trivial ring  $R$  is a **division ring** if

$$R^* = R \setminus \{0\}.$$

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

**Example 24.2.3**

$\mathbb{Q}$ ,  $\mathbb{R}$ ,  $\mathbb{C}$  are fields but  $\mathbb{Z}$  is not.

**Example 24.2.4**

$\mathbb{Z}_n$  is a field  $\iff n$  is prime.

**Remark**

If  $R$  is a division ring or a field, then its only ideals are  $\{0\}$  or  $R$ , since if  $A \neq \{0\}$  is an ideal of  $R$ , then  $\exists a \in A, a \neq 0$ , such that  $1 = aa^{-1} \in A$ , which implies that  $A = R$  by [Proposition 62](#).

**Remark**

It can be shown that every finite division ring is a field, and this is known as [Wedderburn's Theorem](#).

This remark is not as useful or spectacular within this course, but it will be once we go into PMATH348 contents.

NOTE THAT if  $n = ab$  for some integer  $n$  with  $0 < a, b < n$ , then in  $\mathbb{Z}$  we have

$$[a][b] = [n] = [0]$$

but  $[a] \neq [0] \neq [b]$  by our definition of  $a, b$ .

---

**Definition 43 (Zero Divisor)**

Let  $R$  be a non-trivial ring. If  $0 \neq a \in R$ , then  $a$  is called a **zero divisor** if  $\exists 0 \neq b \in R$  such that  $ab = 0$ .

---

## 25 Index

- Abelian Group, 23
- acts on, 87
- additive identity, 14
- Alternating Group, 40, 65
- associativity, 13
  
- Bijectivity, 17
  
- Cauchy's Theorem, 95
- Cayley Table, 30
- Cayley's Theorem, 85, 89
- Center of a Group, 36
- Center of a Ring, 112
- centralizer, 94
- Characteristic, 111
- Chinese Remainder Theorem, 127
- Class Equation, 94
- closure, 13
- Commutative Ring, 107
- conjugacy class, 93
- conjugation, 90
- Coset, 55
- Coset Map, 74
- Cycle Decomposition Theorem, 21
- Cyclic Group, 31, 42, 46
  
- Dihedral Group, 51, 65
- direct product, 26, 111
- Division Ring, 131
  
- Equivalence Relation, 54
- Euler's  $\phi$ -function, 60, 129
- Euler's Theorem, 60
- Euler's Totient Function, 60, 129
- Even Permutations, 40
  
- Extended Cayley's Theorem, 86
- factors through, 80
- faithful group action, 89
- Fermat's Little Theorem, 60
- Field, 131
- Finite Abelian Group Structure, 106
- Finite Subgroup Test, 37
- First Isomorphism Theorem, 76, 124
  
- Gaussian Integers, 131
- Gaussian integers, 113
- General Linear Group, 25, 64
- generator, 42, 46, 118
- Group Action, 87, 89
- Group Homomorphism, 52
- Group of Units, 131
- Groups, 23
  
- Homomorphism, 52, 121
  
- Ideal, 117
- Image, 123
- Image of a Homomorphism, 74
- Index, 57
- Injectivity, 17
- inverse permutation, 19
- isomorphic, 53
- isomorphic to, 53
- Isomorphism, 53
  
- Kernel, 74, 123
- Klein  $n$ -group, 31
- Lagrange's Theorem, 59
  
- multiplicative identity, 14
  
- Normal Subgroup, 61
- Normality Test, 63
- Normalizer, 67
  
- Odd Permutations, 40
- one-to-one, 17
- onto, 17
- Orbit, 90
- Orbit Decomposition Theorem, 91
- Order, 18
- Order of an Element, 43
  
- $p$ -Group, 99
- $p$ -Groups are Finite, 99
- Parity Theorem, 39
- Permutations, 17
- Primary Decomposition, 99
- Principal Ideal, 118
- Product of Groups, 66
  
- Quotient Group, 74
- Quotient Map, 74
- Quotient Ring, 118
  
- restriction, 103
- Ring, 107
- Ring Homomorphism, 121
- Ring Isomorphism, 123
  
- Second Isomorphism Theorem, 81, 125
- sign of a permutation, 76
- Special Linear Group, 36, 64

Stabilizer, 90  
Subgroup, 33  
Subgroup Test, 35  
Subring, 112  
Subring Test, 112

Surjectivity, 17  
symmetry group, 26  
  
Third Isomorphism Theorem, 82, 126  
Transposition, 39  
Trivial Ring, 110

Units, 130  
Unity, 107  
  
Zero Divisor, 132  
Zero of a Ring, 107

## 26 List of Symbols

$M_n(\mathbb{R})$	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 $g$ ; principal ideal with generator $g$
$n \mid d$	$n$ divides $d$
$H \leq G$	$H$ is a subgroup of $G$ (used sparsely in this notebook)
$H \triangleleft G$	$H$ is a normal subgroup of $G$
$G/H$	quotient group of $G$ by $H \triangleleft G$
$\ker \alpha$	kernel of $\alpha$
$\text{im } \alpha$	image of $\alpha$
$G^{(m)}$	group of elements of $G$ with order $m$
$\text{ch}(R)$	characteristic of the ring $R$