PMATH347S18 - Groups & Rings

Johnson Ng

May 16, 2018

Table of Contents

List of Definitions

List of Theorems

1 Lecture 1 May 02nd 2018

1.1 Introduction

1.1.1 Numbers

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

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

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

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

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

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

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

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

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

- (**closure**) $r_1 + r_2 \in R$
- (**associativity**) $r_1 + (r_2 + r_3) = (r_1 + r_2) + r_3$

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

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

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

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

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

- (**closure**) $r_1 r_2 \in R$
- (**associativity**) $r_1(r_2 r_3) = (r_1 r_2) r_3$

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

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

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

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

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

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

1.1.2 *Matrices*

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

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

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

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 $M_n(\mathbb{R})$.

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 that the operation is **commutative**, i.e.

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

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

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

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

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

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

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

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

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

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

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 2.1.1 (Injectivity)
*Let $f : X \to Y$ 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 2.1.2 (Surjectivity)
*Let $f : X \to Y$ be a function. We say that f is **surjective** (or **onto**) if $\forall y \in Y \ \exists x \in X \ \ f(x) = y$.*

Definition 2.1.3 (Bijectivity)
*Let $f : X \to Y$ be a function. We say that f is **bijective** if it is both **injective** and **surjective**.*

Definition 2.1.4 (Permutations)
Given a non-empty set L, a permutation of L is a bijection from L to L. The set of all permutations of L is denoted by S_L.

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

tions:

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

Note

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

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

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

Definition 2.1.5 (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 2.1.1

$|S_n| = n!$

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

It is important to note that $\because$ σ, τ are **both bijective**, $\sigma\tau$ is also bijective. Thus, together with the fact that $\sigma\tau : \{1,\ldots,n\} \to \{1,\ldots,n\}$, 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

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

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

Solution

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

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

[1] This is proven in A1

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

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

[2]

Exercise 2.1.1
Prove this as an exercise.

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

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

[3]

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

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

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

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

It follows, immediately, that

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

$\therefore$ 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:

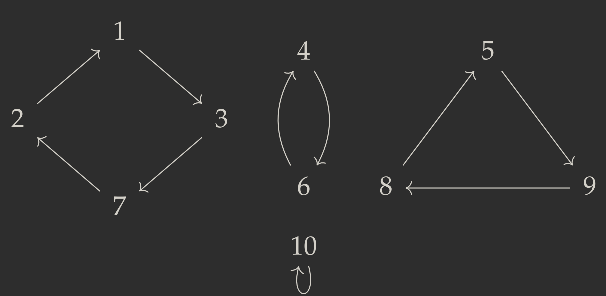
Proposition 2.1.2 (Properties of S_n)
We have

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

Consider

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

If we represent the action of σ geometrically, we get



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

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

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

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

Note that we may also write

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

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

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

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

[5] See bonus question of A1. Proof will be included in the notes once the assignment is over.

Theorem 2.1.1 (Cycle Decomposition Theorem)
If $\sigma \in S_n$, $\sigma \neq \varepsilon$, then σ is a product of (one or more) disjoint cycles of length at least 2. This factorization is unique up to the order of the factors.

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

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

3 Lecture 3 May 07th 2018

3.1 Groups

3.1.1 Groups

Definition 3.1.1 (Groups)
Let G be a set and $*$ an operation on $G \times G$. We say that $G = (G, *)$ is a ***group*** *if it satisfies*[1]

1. ***Closure***: $\forall a, b \in G \quad a * b \in G$
2. ***Associativity***: $\forall a, b, c \in G \quad a * (b * c) = (a * b) * c$
3. ***Identity***: $\exists e \in G \;\; \forall a \in G \quad a * e = a = e * a$
4. ***Inverse***: $\forall a \in G \;\; \exists b \in G \quad a * b = e = b * a$

[1] If you wonder why the uniqueness is not specified for **Identity** and **Inverse**, see Proposition 3.1.1.

Definition 3.1.2 (Abelian Group)
A group G is said to be abelian if $\forall a, b \in G$, we have $a * b = b * a$.

Proposition 3.1.1 (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, wehre the additive identity is 0, and the additive inverse of an element r is $(-r)$.

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

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

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

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

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

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

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

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

But 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. Define the set

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

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, and is in fact called the **general linear group of degree n over $\mathbb{R}$**.

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 2.1.2, we know that S_n is a group. We call S_n the ***symmetry group of degree n****. For $n \geq 3$, the group S_n is not abelian*[3].

[3] Let us make this an exercise.

Exercise 3.1.1

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

Now that we have a fairly good idea of the basic concept of a group, we will now proceed to look into handling multiple groups. One such operation is known as the **direct product**.

Example 3.1.5

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

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

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

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

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

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

Notation

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

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

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

and

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

With the above notations,

Proposition 3.1.2

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 3.1.2 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,

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

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 4.1.1 (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 $y = ba^{-1}$.

$\square$

4.1.2 Cayley Tables

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

Definition 4.1.1 (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 Cancellation Laws 4.1.1, the entries in each row (and respectively, column) of a Cayley Table are all distinct.

Example 4.1.1
Consider the group $(\mathbb{Z}_2, +)$. Its Cayley Table is

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

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

Example 4.1.2
Consider the group $\mathbb{Z}^* = \{1. -1\}$. Its Cayley Table (under multiplication) is

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

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

Example 4.1.3

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

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

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

C_n	1	a	a^2	$\dots$	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 4.1.2

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

1. *if $|G| = 1$, then $G \cong \{1\}$.*
2. *if $|G| = 2$, then $G \cong C_2$.*
3. *if $|G| = 3$, then $G \cong C_3$.*
4. *if $|G| = 4$, then either $G \cong C_4$ or $G \cong K_4 \cong C_2 \times C_2$.*

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

Proof

1. *If $|G| = 1$, then it can only be $G = \{1\}$ where 1 is the identity element.*
2. *$|G| = 2 \implies G = \{1, g\}$ with $g \neq 1$. The Cayley Table of G is thus*

G	1	g
1	1	g
g	g	1

where we note that $g^2 = 1$; otherwise if $g^2 = g$, then we would have $g = 1$ by Cancellation Laws 4.1.1, 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 Cancellation Laws 4.1.1, $gh \neq g$ 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 Cancellation Laws 4.1.1, we have that $h = g$, which is a contradiction.*

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

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

Recall that the Cayley Table for C_3 is:

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

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

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

4.2 Subgroups

4.2.1 Subgroups

Definition 4.2.1 (Subgroup)
Let G be a group and $H \subseteq G$. If H itself is a group, then we say that H is a subgroup of G

5 Lecture 5 May 11th 2018

5.1 Subgroups (Continued)

5.1.1 Subgroups (Continued)

Note (Recall: definition of a subgroup)
Let G be a group and $H \subseteq G$. If H itself is a group, then we say that H is a subgroup of G.

Note
Since G is a group, $\forall h_1, h_2, h_3 \in H \subseteq G$, we have $h_1(h_2h_3) = (h_1h_2)h_3$. 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 5.1.1 (Special Linear Group)
*The **special linear group** of order n of $\mathbb{R}$ is defined as*

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

Example 5.1.3
Clearly, $SL_n(\mathbb{R}) \subseteq GL_n(\mathbb{R})$. Note that the identity matrix I must be in $SL_n(\mathbb{R})$ since $\det I = 1$. Also, $\forall A, B \in SL_n(\mathbb{R})$, we have that

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

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

Definition 5.1.2 (Center of a Group)
*Given a group G, the **the center of a group** G is defined as*

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

Example 5.1.4
For a group G, $Z(G)$ is an abelian subgroup of G.

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

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

Therefore $yz \in Z(G)$ and so $Z(G)$ is closed under its operation. Also, $\forall hinG$, 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 5.1.1 (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 5.1.2 (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*

$$h, h^2, h^3, \ldots$$

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 Finite Subgroup Test 4.1.1,* $h^m = 1$ *and so* $1 \in H$. *Also, because* $1 = h^{m-1}h$, *we have that* $h^{-1} = h^{m-1}$, *and thus the inverse of* h *is also in* H. *Therefore,* H *is a subgroup of* G *as requried.* $\square$

6 Lecture 6 May 14th 2018

6.1 Subgroups (Continued 2)

6.1.1 Alternating Groups

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

Definition 6.1.1 (Transposition)
*A **transposition** $\sigma \in S_n$ is a cycle of length 2, i.e. $\sigma = \begin{pmatrix} a & b \end{pmatrix}$, where $a, b \in \{1, ..., n\}$ and a neqb.*

Example 6.1.1
We have that[1]

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

Also, we can show that[2]

$$\begin{pmatrix} 1 & 2 & 4 & 5 \end{pmatrix} = \begin{pmatrix} 2 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 2 & 5 \end{pmatrix} \begin{pmatrix} 1 & 3 \end{pmatrix} \begin{pmatrix} 2 & 4 \end{pmatrix} \tag{6.1}$$

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

Theorem 6.1.1 (Parity Theorem)
If a permutations σ has 2 factorizations

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

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

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

[2]

Exercise 6.1.1
Show that Equation 6.1 is true.

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

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

Proof

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

Definition 6.1.2 (Odd and Even Permutations)

A permutation σ is even (or odd) if it can be written as a product of an even (or odd) number of transpositions. By Parity Theorem 6.1.1, a permutation must either be even or odd, but not both.

Theorem 6.1.2 (Alternating Group)

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

1. $\varepsilon \in A_n$
2. $\forall \sigma, \tau \in A_n \;\; \sigma\tau \in A_n$ *and* $\exists \sigma^{-1} \in A_n$ *such that* $\sigma\sigma^{-1} = \varepsilon = \sigma^{-1}\sigma$
3. $|A_n| = \frac{1}{2} n!$

Note

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

Proof

1. *We have that* $\varepsilon = \begin{pmatrix} 1 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 \end{pmatrix}$. *Thus ε is even and so $\varepsilon \in A_n$.*
2. $\forall \sigma, \tau \in A_n$, *we may write*

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

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

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

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

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

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

which is an even permutation and

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

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

3. *Let O_n denote the set of odd permutations in S_n. Then we have $S_n = A_n \cup O_n$, and by the Parity Theorem, we have that $A_n \cap O_n = \emptyset$. 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 $f : A_n \to O_n$ such that $f(\sigma) = \gamma\sigma$. Since σ is even, $\gamma\sigma$ is odd, and so f is well-defined.

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

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

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

   Therefore, f is surjective.

   It follows that $|A_n| = |O_n|$. □

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

Also, note that the set of all odd permutations of S_n is not a group, since
- there is no identity element in this set; and
- this set is not closed under map composition.

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

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 6.1.1 (Cyclic Group as A Subgroup)
If G *is a group and* $g \in G$, *then* $\langle\, g \,\rangle$ *is a subgroup of* G.

Definition 6.1.3 (Cyclic Groups)
Let G *be a group and* $g \in G$. *Then we call* $\langle\, g \,\rangle$ *the* ***cyclic subgroup*** *of* G *generated by* g. *If* $G = \langle\, g \,\rangle$ *for some* $g \in G$, *then we say that* G *is a* ***cyclic group***, *and* g *is a* ***generator*** *of* G.

7 Lecture 7 May 16th 2018

7.1 Subgroups (Continued 3)

7.1.1 Order of Elements (Continued)

Example 7.1.1
Consider $(\mathbb{Z}, +)$ *. Note that* $\forall k \in \mathbb{Z}$*, we can write* $k = k \cdot 1 = \underbrace{1 + 1 + \ldots + 1}_{k times}$*.*

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

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

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

With that, we may have the following definition:

Definition 7.1.1 (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 7.1.1 (Properties of Elements of Finite Order)
Let G *be a group with* $g \in G$ *where* $o(g) = n \in \mathbb{N}$*. Then*

1. $g^k = 1 \iff n|k$;
2. $g^k = g^m \iff k \equiv m \mod n$; and
3. $\langle\, g \,\rangle = \{1, g, g^2, ..., g^{n-1}\}$ *where each* g^i *is distinct from others.*

Proof

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

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

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

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

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

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

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

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

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

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

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

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

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

$\square$

Proposition 7.1.2 (Property of Elements of Infinite Order)
Let G be a group, and $g \in G$ such that $o(g) = \infty$. Then

1. $g^k = 1 \iff k = 0$;
2. $g^k = g^r \iff k = m$;
3. $\langle g \rangle = \{..., g^{-2}, g^{-1} 1, g, g^2, ...\}$ *where each* g^i *is distinct from others.*

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

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

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

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

□

Proposition 7.1.3 (Orders of Powers of the Element)
Let G be a group, and $g \in G$ with $o(g) = n \in \mathbb{N}$. We have that

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

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

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

□

7.1.2 *Cyclic Groups*

Recall the definition of a cyclic groups.

Definition 7.1.2 (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 7.1.4 (Cyclic Groups are Abelian)
All cyclic groups are abelian.

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

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

$\square$

8 Index

9 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
$n \mid d$	n divides d