Foreword

Usage

- Notes are presented in two columns: main notes on the left, and sidenotes on the right. Main notes will have a larger margin.
- The following is the color code for the notes:

Blue	Definitions
Red	Important points
Yellow	Points to watch out for / comment for incompletion
Green	External definitions, theorems, etc.
Light Blue	Regular highlighting
Brown	Secondary highlighting

- The following is the color code for boxes, that begin and end with a line of the same color:

Blue	Definitions
Red	Warning
Yellow	Notes, remarks, etc.
Brown	Proofs
Magenta	Theorems, Propositions, Lemmas, etc.

- Hyperlinks are underlined in magenta. If your PDF reader supports it, you can follow the links to either be redirected to an external website, or a theorem, definition, etc., in the same document. Note that this is only reliable if you have the full set of notes as a single document, which you can find on: `https://japorized.github.io/TeX_notes`

3 Lecture 3 May 07th 2018

3.1 Groups

3.1.1 Groups

Definition 6 (Groups)
*Let G be a set and $*$ an operation on $G \times G$. We say that $G = (G, *)$ is a **group** if it satisfies*[1]

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

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

Definition 7 (Abelian Group)
A group G is said to be abelian if $\forall a, b \in G$, we have $a * b = b * a$.

Proposition 4 (Group Identity and Group Element Inverse)
Let G be a group and $a \in G$.

1. *The identity of G is unique.*
2. *The inverse of a is unique.*

Proof

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

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

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

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

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

where (1) is by associativity.

Example 3.1.1

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

Note

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

Example 3.1.2

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

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

Example 3.1.3

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

[3] Let us make this an exercise.

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

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

Example 3.1.5
Let G and H be groups. Their direct product is the set $G \times H$ with the component-wise operation defined by

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

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

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

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

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

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

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

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

and

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

With the above notations,

Proposition 5
Let G be a group and $g, h \in G$. We have

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

Exercise 3.1.2
Prove Proposition 5 as an exercise.

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

Warning

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

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

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