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`

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 $y = ba^{-1}$.

$\square$

4.1.2 Cayley Tables

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

Definition 9 (Cayley Table)
Let G be a group. Given $x, y \in G$, let the product xy be an entry of a table in the row corresponding to x and column corresponding to y. Such a table is called a ***Cayley Table****.*

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

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

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

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

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

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

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

Example 4.1.3
Given $n \in \mathbb{N}$, the **Cyclic Group** *of order n is defined by*

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

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

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

Proposition 7
Let G be a group. Up to isomorphism, we have

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

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

Proof

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

G	1	g
1	1	g
g	g	1

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

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

start with the following Cayley Table:

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

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

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

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

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

Recall that the Cayley Table for C_3 is:

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

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

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

4.2 Subgroups

4.2.1 Subgroups

Definition 10 (Subgroup)

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