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`

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.

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

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

$$\begin{aligned}
g^m \in H &\implies \langle\, g^m \,\rangle \subseteq H \\
\because H \subseteq G = \langle\, g \,\rangle \quad & \forall h \in H\ \exists k \in \mathbb{Z}\ h = g^k \\
\textit{Division Algorithm} : & \exists q, r \in \mathbb{Z}\ 0 \leq r < m \quad k = mq + r \\
h = g^k \implies & g^r = g^{k-mq} = g^k (g^m)^{-q} = g^k(1) \in H \\
r \neq 0 \implies & \exists 0 < r < m \quad g^r \in H \quad ↯ \quad m \text{ is the smallest +ve integer} \\
\implies & g^k \in \langle\, g^m \,\rangle \implies H \subseteq \langle\, g^m \,\rangle
\end{aligned}$$

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 ($\implies$),

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

Then

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

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

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

□

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.

Theorem 19 (Fundamental Theorem of Finite Cyclic Groups)
Let $G = \langle g \rangle$ with $o(g) = n \in \mathbb{N}$.

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

Proof

1. *Note*

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

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

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

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

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

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

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

□