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`

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

Proof

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

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

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

$(\impliedby)$ $k \equiv m \mod n \implies \exists q \in \mathbb{Z}\ \ k = qnm$. *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 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. $g^k = g^r \iff k = m$;
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. $$g^k = g^m \iff g^{k-m} = 1 \overset{\text{by } 1}{\iff} k - m = 0 \iff k = m$$

$\square$

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

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

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*

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

$\square$

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

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

$\square$