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`

10 Lecture 10 May 23rd 2018

10.1 Normal Subgroup (Continued)

10.1.1 Cosets and Lagrange's Theorem (Continued)

Theorem 23 (Lagrange's Theorem)
Let H be a subgroup of a ***finite*** *group G. Then*

$$|H| \,\Big|\, |G| \text{ and } [G:H] = \frac{|G|}{|H|}$$

Proof
Since G is finite, there can only be finitely many cosets of H. Let $k = [G:H]$ and $Ha_1, Ha_2, \ldots, Ha_k$ be the distinct right cosets of H in G. By Proposition 22, we have that these cosets partition G, i.e.

$$G = \bigcup_{i=1}^{k} Ha_i.$$

Note that by the definition of a right coset, the map

$$H \to Hb \text{ defined by } h \mapsto hb$$

is a surjection from H to Hb. By Cancellation Laws, the map is injective, since if $hb_1 = hb_2$, then $b_1 = b_2$. Therefore, for $i = 1, \ldots, k$,

$$|H| = |Ha_i|.$$

Then we have

$$|G| = k\,|H| \implies |H| \;\Big|\; |G| \wedge [G:H] = k = \frac{|G|}{|H|}$$

□

Corollary 24

1. *If G is a finite group and $g \in G$, then $o(g) \;\Big|\; G$.*
2. *If G is a finite group and $|G| = n$, then $g^n = 1$.*

Proof

1. *Let $H = \langle\, g \,\rangle$. Then by Lagrange's Theorem 23, $o(g) = |H| \;\Big|\; |G|$.*
2. *For some $g \in G$, let $o(g) = m \in \mathbb{Z} \setminus \{0\}$. Then by 1, $m \mid n$ and so $g^n = (g^m)^{\frac{n}{m}} = 1$.*

□

Note

Let $n \in \mathbb{N} \setminus \{1\}$. ***Euler's Totient Function****, or more generally written as* ***Euler's ϕ-function*** *is defined as*

$$\phi(n) \equiv \Big|\{k \in \{1, ..., n-1\} \,:\, \gcd(k, n) = 1\}\Big|. \tag{10.1}$$

Note that the set $\mathbb{Z}_n^*$ under multiplication has a similar definition to the set on the RHS, since the only numbers from 1 to n that has an inverse are those that are coprime with n. Thus $\phi(n) = |\mathbb{Z}_n^*|$.

With Corollary 24, we have ***Euler's Theorem*** *that states that*

$$\forall a \in \mathbb{Z} \;\; \gcd(a, n) = 1 \implies a^{\phi(n)} \equiv 1 \mod n. \tag{10.2}$$

If $n = p$ where p is some prime number, then Euler's Theorem implies ***Fermat's Little Theorem****, i.e. $a^{p-1} \equiv 1 \mod p$.*

Corollary 25

If p is prime, then every group G of order p is cyclic. In fact, $g = \langle g \rangle$ fpr $g \neq 1 \in G$. Hence, the only subgroup of G are $\{1\}$ and G itself.

Proof

Let $g \in G$ such that $g \neq 1$. By Corollary 24, $o(g) \mid p$. Since $g \neq 1$ and p is prime, by ***uniqueness of prime factorization****, it must be that $o(g) = p$. Thus we can write $G = \langle g \rangle$. If H is a subgroup of G, then by Lagrange's Theorem, we have $|H| \mid p$. Since p is prime, we either have $|H| = 1$ or p. In other words, we either have that $H = \{1\}$ or $H = G$, respectively.* $\square$

Corollary 26

Let H and K be finite subgroups of G. If $\gcd(|H|, |K|) = 1$, then $H \cap K = \{1\}$.

Proof

Since $H \cap K$ is a subgroup of H and of K, by Lagrange's Theorem 23, $|H \cap K| \,\Big|\, |H| \wedge |H \cap K| \,\Big|\, |K|$. By assumption that $\gcd(|H|, |K|) = 1$, we have[1] that $|H \cap K| = 1$, and hence $|H \cap K| = \{1\}$. $\square$

[1] $|H \cap K|$ is a common divisor for $|H|$ and $|K|$. But $\gcd(|H|, |K|) = 1$

10.1.2 Normal Subgroup

We have seen that given H is a subgroup of a group G and $g \in G$, gH and Hg are generally not the same.

Definition 23 (Normal Subgroup)

Let H be a subgroup of a group G. If $\forall g \in G$, we have $Hg = gH$, then we say that H is a ***normal subgroup*** *of G, and write*

$$H \triangleleft G$$

Example 10.1.1
$\{1\} \lhd G$ and $G \lhd G$.

Example 10.1.2
The center, $Z(G)$, of a group G is an abelian group. By Definition 23,

$$Z(G) \lhd G.$$

Example 10.1.3
If G is abelian, then every subgroup of G is normal in G.

Proposition (Normality Test)
Let H be a subgroup of G. The following are equivalent:

1. $H \lhd G$;
2. $\forall g \in G \quad gHg^{-1} \subseteq H$;
3. $\forall g \in G \quad gHg^{-1} = H$ [2]

[2] This means that

$$H \lhd G \iff H \text{ is the only conjugate of } H$$