Chapter 7

Notation: For a group \( G \), \( S \leq G \), and \( a \in G \) define
\[
\begin{align*}
    aS &= \{ as : s \in S \} & \text{left coset of } S \\
    Sa &= \{ sa : s \in S \} & \text{right coset of } S \\
    aS^{-1} &= \{ asa^{-1} : s \in S \} & \text{in additive notation}
\end{align*}
\]
\( |S| = \) number of elements in \( S \)

Definition: Let \( G \) be a group, \( H \leq G \) a subgroup, and \( a \in G \)
- \( aH \) is the left coset of \( H \) containing \( a \)
- \( a \) is called a coset representative of \( aH \)
- \( Ha \) is the right coset of \( H \) containing \( a \)
- \( a \) is called a coset representative of \( Ha \)

Lemma 7.4: Let \( G \) be a group, \( H \leq G \) a subgroup, and \( a, b \in G \).
Then \( aH = bH \) or \( aH \cap bH = \emptyset \).
Moreover, \( aH = bH \iff a \in bH \iff b^{-1}a \in H \)
(Similarly, either \( Ha = Hb \) or \( Ha \cap Hb = \emptyset \).
Moreover, \( Ha = Hb \iff a \in Hb \iff a^{-1}b \in H \)

Proof: We prove "Moreover..." first by showing \( 1 \Rightarrow 2 \Rightarrow 3 \Rightarrow 0 \).
- \( 1 \Rightarrow 2 \): Assume \( aH = bH \). Since \( e \in H \),
  \[ a = ae \in aH = bH. \]
- \( 2 \Rightarrow 3 \): Assume \( a \in bH \). Then there is \( h \in H \) with
  \[ a = bh. \] Then \( b^{-1}a = b^{-1}bh = eh = h \in H. \]
- \( 3 \Rightarrow 0 \): Assume \( b^{-1}a \in H \). Set \( h_0 = b^{-1}a \in H \).
  Note \( b^{-1}a = \) since \( h \in H \)
  \( ah \in bH \) For any \( h \) we have \( ah = (bh^{-1})ah = b(h^{-1}a)h = bh_0h \in bH. \)
  \( bh \in aH \) For any \( h \) we have \( bh = (a^{-1}b)h = a(a^{-1}bh) = ah_0h \in aH. \)
Lastly, we prove $ah = bh$ or $ah \cap bh = \emptyset$.

Case 1: $ah \cap bh = \emptyset$. Done.

Case 2: $ah \cap bh \neq \emptyset$. Pick any $c \in ah \cap bh$.

By the "Moreover..." part, we have $cH = ah$ and $cH = bh$. Therefore $ah = bh$. □

Lemma 7.8: The collection of left cosets $\{ah : a \in G\}$
partition $G$. Also $|ah| = |H|$ for all $a \in G$
(Similarly, the right cosets $\{Ha : a \in G\}$ partition $G$)
and $|Ha| = |H|$ for all $a \in G$.

Proof: Since $e \in H$, we have $a = ae = aH$. So the union of the
sets $ah (a \in G)$ is equal to $G$. By Lem 7.6a, the sets
$ah (a \in G)$ are disjoint when they are not equal. This
proves that $\{ah : a \in G\}$ is a partition of $G$.
Lastly, $|H| = |ah|$ because the map $h \in H \mapsto ah \in H$
is one-to-one and onto. □

Warning: Generally $ah \neq Ha$. However...

Lemma 7.9: $aH = Ha \iff aHa^{-1} = H$

Proof: Multiplication on the right by $a^{-1}$ is a
one-to-one operation that sends
$ah$ to $aHa^{-1}$ and $Ha$ to $H$. □
Ex: Set \( H = \{ e, (23) \} \leq S_3 \). (\( H \) is a subgroup of \( S_3 \)).

The left cosets of \( H \) are

\[
(12)H = \{ (12), (123) \} = (123)
\]
\[
(13)H = \{ (13), (132) \} = (132)
\]
\[
(2)H = \{ (2), (23) \} = (23)
\]

The right cosets of \( H \) are

\[
H(12) = \{ (12), (132) \} = H(132) = \{ (13), (13) \} = (132)
\]
\[
H(13) = \{ (13), (123) \} = H(123) = \{ (2), (23) \} = (23)
\]

Lagrange's Theorem:

If \( G \) is a finite group and \( H \) is a subgroup then \( |H| \) divides \( |G| \). Moreover, the number of left (or right) cosets of \( H \) in \( G \) is denoted \( |G:H| \) and is equal to \( \frac{|G|}{|H|} \).

Proof: Let \( a_1H, a_2H, \ldots, a_rH \) be the distinct left cosets of \( H \) in \( G \), where \( r = |G:H| \) (by definition of \( |G:H| \)). Since these cosets are disjoint and have union \( G \), we have

\[
|G| = |a_1H| + |a_2H| + \cdots + |a_rH| = r|H|
\]

Therefore, \( r = \frac{|G|}{|H|} \) and \( |H| |G| \).

Warning: \( |G| \) does not imply \( G \) has a subgroup of order \( k \).
Let $G$ be a finite group.

**Cor A** For every $a \in G$, the order of $a$ divides $|G|$.  

**Proof:** By Lagrange Thm. $|a| | |G|$.  
Now recall $(\text{order of } a) = |<a>|$.  

**Cor B** Let $G$ be a finite group. Then  
\[ a^{\frac{|G|}{n}} = e \text{ for all } a \in G \]

**Proof:** Set $n = (\text{order of } a)$. By Cor A, $n | |G|$.  
Say $k = \frac{|G|}{n}$. Then  
\[ a^{\frac{|G|}{n}} = a^k = (a^n)^k = e^k = e. \]

**Cor C:** If $G$ is any group and $|G| = p$ is prime, then $G$ is cyclic and $G \cong \mathbb{Z}/p\mathbb{Z}$.  

**Proof:** Pick any $a \in G \setminus \{e\}$. Then the order of  
$a$ is greater than 1 and divides $p$, so it must be equal to $p$. So $|<a>| = p = |G|$ and we must have $G = <a>$. Finally,  
every cyclic group of order $p$ must be isomorphic to $\mathbb{Z}/p\mathbb{Z}$.  

**Cor (Fermat's Little Theorem):**  
For every integer $a$ and prime $p$, $a^p \text{ mod } p = a \text{ mod } p$.  

**Proof:** Set $r = a \text{ mod } p$. Then $a^p \text{ mod } p = r^p \text{ mod } p$ (lem. 0.8).  
If $r = 0$ the result is trivial. So assume $r \neq 0$.  
Then $r \in \mathbb{U}(p)$ since $p$ is prime. So by Cor. B
\[ r^{\omega(p)} \mod p = 1. \] Since \[ |\omega(p)| = p-1, \] this gives
\[ r^{\omega(p)} \mod p = r \cdot r^{p-1} \mod p = r \cdot r^{\omega(p)} \mod p = r \cdot 1 \mod p = r \]

Therefore, \[ a^p \mod p = r^p \mod p = r = a \mod p \] \[ \square \]