Chapter 7

Notation: For a group G, $S \subseteq G$, and $a \in G$ define

$aS = \{as : s \in S\}$	$a+S$
$Sa = \{sa : s \in S\}$	$S+a$
$aSa^{-1} = \{asa^{-1} : s \in S\}$	in additive notation
$\lvert S\rvert$ = number of elements in S	

Defn: 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.A: Let G be a group; $H \leq G$ a subgroup, and $a, b \in G$.
Then either $aH = bH$ or $aH \cap bH = \emptyset$.
Moreover, $aH \overset{①}{=} bH \iff a \overset{②}{\in} bH \iff b^{-1}a \overset{③}{\in} H$
(Similarly, either $Ha = Hb$ or $Ha \cap Hb = \emptyset$.
Moreover, $Ha = Hb \iff a \in Hb \iff ab^{-1} \in H$)

Pf: We prove "Moreover..." first by showing ① ⇒ ② ⇒ ③ ⇒ ①.

(① ⇒ ②) Assume $aH = bH$. Since $e \in H$,
$$a = ae \in aH = bH.$$

(② ⇒ ③) Assume $a \in bH$. Then there is $h \in H$ with
$$a = bh. \text{ Then } b^{-1}a = b^{-1}bh = eh = h \in H.$$

(③ ⇒ ①) Assume $b^{-1}a \in H$. Set $h_0 = b^{-1}a \in H$. Note $h_0^{-1} = a^{-1}b$

($aH \subseteq bH$) For any $h \in H$ we have $ah = (bb^{-1})ah = b(b^{-1}a)h = bh_0h \in bH$ (since $h_0 h \in H$)

($bH \subseteq aH$) For any $h \in H$ we have $bh = (aa^{-1})bh = a(a^{-1}b)h = ah_0^{-1}h \in aH$

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 $aH = bH$. $\square$

Lemma 7.B: 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 $a \in G$)

Pf: Since $e \in H$, we have $a = ae \in aH$. So the union of the sets aH $(a \in G)$ is equal to G. By Lem 6.A, 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 $h \in H \mapsto ah \in aH$ is one-to-one and onto. $\square$

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

Lem 7.C: $aH = Ha \iff aHa^{-1} = H$

Pf: Multiplication on the right by a^{-1} is a one-to-one operation that sends
aH to aHa^{-1} and Ha to H. $\square$

$\{\alpha \in S_3 : \alpha(1) = 1\}$

Ex: Set $H = \{\varepsilon, (23)\} \subseteq S_3$. ($H$ is a subgroup of S_3).

The left-cosets of H are

$(12)H = \{(12), (123)\} = (123)H = \{\alpha \in S_3 : \alpha(1) = 2\}$

$(13)H = \{(13), (132)\} = (132)H = \{\alpha \in S_3 : \alpha(1) = 3\}$

$\varepsilon H = \{\varepsilon, (23)\} = (23)H = \{\alpha \in S_3 : \alpha(1) = 1\}$

The right cosets of H are

$H(12) = \{(12), (132)\} = H(132) = \{\alpha \in S_3 : \alpha(2) = 1\}$

$H(13) = \{(13), (123)\} = H(123) = \{\alpha \in S_3 : \alpha(3) = 1\}$

$H\varepsilon = \{\varepsilon, (23)\} = H(23) = \{\alpha \in S_3 : \alpha(1) = 1\}$

Lagrange's Thm 7.1:

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 $|G|/|H|$.

Called the index of H in G

Pf: Let $a_1H, a_2H, \cdots, a_rH$ 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

$$|G| = |a_1H| + |a_2H| + \cdots + |a_rH| \overset{\text{Lem. 6.B}}{=} r|H|.$$

Therefore $r = |G|/|H|$ and $|H| \mid |G|$. $\square$

Warning: $k \mid |G|$ does not imply G has a subgroup of order k.

Let G be a finite group.

<u>CorA</u> For every $a \in G$, the order of a divides $|G|$.

<u>Pf</u>: By Lagrange Thm $|\langle a\rangle|$ divides $|G|$.
Now recall (order of a) $= |\langle a \rangle|$. $\square$

<u>CorB</u> Let G be a finite group. Then
$a^{|G|} = e$ for all $a \in G$

<u>Pf</u>: Set $n =$ (order of a). By Cor A, $n \mid |G|$.
Say $k = |G|/n$. Then $a^{|G|} = a^{nk} = (a^n)^k = e^k = e$. $\square$

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

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

<u>Cor (Fermat's Little Theorem)</u>:
For every integer a and prime p, $a^p \bmod p = a \bmod p$.

<u>Pf</u>: Set $r = a \bmod p$. Then $a^p \bmod p = r^p \bmod p$ (Lem. 0.B).
If $r = 0$ the result is trivial. So assume $r \neq 0$.
Then $r \in U(p)$ since p is prime. So by Cor. B

$r^{|U(p)|} \bmod p = 1$. Since $|U(p)| = p-1$, this gives
$r^p \bmod p = r \cdot r^{p-1} \bmod p = r \cdot r^{|U(p)|} \bmod p$
$= r \cdot 1 \bmod p = r$
Therefore $a^p \bmod p = r^p \bmod p = r = a \bmod p$ $\square$