Recall: A subgroup \( N \) of a group \( G \) is normal if 
\[ \forall g \in G, \forall x \in N, \quad g x g^{-1} \in N. \]

Notation \( N \triangleleft G \) if \( N \) is a normal subgroup of \( G \).

2) The kernel of a homomorphism \( \varphi : G \to H \) is 
\[ \ker \varphi = \{ g \in G \mid \varphi(g) = e_H \}. \]

Then \( \ker \varphi \) is a normal subgroup of \( G \).

Recall: \( n \mathbb{Z} \) is a normal subgroup of \( \mathbb{Z} \). It's used to define 
\[ \mathbb{Z}/n \mathbb{Z} = \mathbb{Z}/n\mathbb{Z}. \]

Goal: Generalization of this construction for any group \( G \) and any normal subgroup \( N \triangleleft G \).

Steps:

(Right) Cosets.

Definition: Let \( H \) be a subgroup of a group \( G \). Define a relation \( \sim \) on \( G \) by: 
\[ a \sim b \iff ab^{-1} \in H \]
(i.e. \( a \sim b \iff \exists h \in H \) with \( ab^{-1} = h \)
\[ \iff \exists h \in H \) with \( a = hb \)

Proposition: The relation \( \sim \) defined above is an equivalence relation.

Proof: \( \forall a \in G \), \( aa^{-1} = e \in H \), \( \Rightarrow a \sim a \).

1) If \( a \sim b \), then \( a = hb \) for some \( h \in H \). \( \Rightarrow b = h^{-1}a \)
Since \( h^{-1} \in H \), \( b \sim a \).

2) Suppose \( a \sim b \sim c \). Then \( \exists h_1, h_2 \in H \) s.t.
\[ a = h_1b, \ b = h_2c. \Rightarrow a = h_1(h_2c) = (h_1h_2)c. \Rightarrow a \sim c. \]

Definition: The equivalence classes of the relation \( \sim \) of proposition \( \sim \) are called right cosets of \( H \) in \( G \):

\[ aH = \{ ah \mid h \in H \}. \]
\[ \{ a \in G \mid b = a b h \text{ for some } h \in H \} = \{ a \in H \mid a \text{ for some } h \in H \} = H a \]

**Example**

\[ G = \mathbb{Z}, \quad H = n\mathbb{Z} \text{ (for some } n \in \mathbb{N}). \quad \text{For } k \in \mathbb{Z} \]

\[ \epsilon_k = \{ h \in \mathbb{Z} \mid h = n k \} = \{ n \in \mathbb{Z} \mid k \in \mathbb{Z} \} = n \mathbb{Z} + k. \]

**Remarks**

1. \( H a = H b \iff a - b \in H \iff a = h b \text{ for some } h \in H \).
2. \( H a \cap H b \neq \emptyset \quad \Rightarrow \quad H a = H b \iff a = h b \text{ for some } h \in H \)
3. Let \( \varphi : G \to K \) be a homomorphism. We proved:

   \[ \varphi(a) = \varphi(b) \iff ab^{-1} \in \ker(\varphi) \]

   Thus

   \[ \varphi(a) = \varphi(b) \iff (\ker(\varphi))a = (\ker(\varphi))b. \]

**Notation**

\[ \mathbb{H} \setminus G = \{ a \in G \mid a \in \mathbb{H} \}, \text{ the set of right cosets of } H \]

**Example**

\[ G = \mathbb{Z}, \quad H = n\mathbb{Z} \quad n\mathbb{Z} \setminus \mathbb{Z} = \{ 10, 11, \ldots, n-1 \} \]

**Example**

\( \varphi : G \to K \) homomorphism.

Remark above says: \( \forall b \in (\ker(\varphi))a \iff \varphi(b) = \varphi(a) \).

Hence \( (\ker(\varphi)) \setminus G = \{ \varphi^{-1}(c) \mid c \in K \} \)

the set of "level sets" of \( \varphi \)

**Left cosets**

If \( H \) is a subgroup of \( G \) then the relation

\[ a \ast b \iff a^{-1}b \in H \]

\[ \iff b = ah \text{ for some } h \in H \]

is an equivalence relation. "Same proof as 12.1"
The corresponding equivalence classes are called
left cosets. They are of the form
\[ [a] = \{ ah | h \in H \} = ah. \]

\[ G/H = \text{set of left cosets of } H \text{ in } G. \]

Remarks. For a subgroup \( H \) of a group \( G \),
left cosets are different from right cosets, unless
\( H \) is normal. We'll prove this later.

**Lemma 12.2.** Let \( H \) be a subgroup of a group \( G \). All
left cosets of \( H \) are of the "same size": \( \forall a \in G \) There is
a bijection \( H \to \{ aH \} \).

**Proof.** Consider \( La: G \to G, \ La(g) = ag \) (left
multiplication by \( a \)). \( La \) is invertible: the inverse
is \( La^{-1}. \ (La^{-1} \circ La)(g) = a^{-1}ag = g \ \forall g \in G \)
\( (La \circ La^{-1})(g) = a a^{-1}g = g \ \forall g \in G \).

\[ La(H) = \{ ah | h \in H \} \]
\[ \Rightarrow La: H \to \{ aH \} \text{ is a bijection.} \]

**Theorem (Lagrange).** Let \( G \) be a finite group. Then
\[ |G| = |G/H| \cdot |H| = |H/G| \cdot |H|. \]

**Proof.** Since \( G \) is finite, so is \( H \leq G \). Also
the map \( G \to G/H, \ a \mapsto aH \) is onto,
\[ \Rightarrow G/H \text{ is finite. } \Rightarrow a_1 \cdots a_k \in G \text{ for } \]
\[ \Rightarrow G/H = a_1H \cup a_2H \cup \cdots \cup a_kH; \ x = |G/H| \]
with \( a_i H \cap a_j H = \emptyset \) for \( i \neq j \).

\[
\Rightarrow |G| = |a_1 H| + |a_2 H| + \cdots + |a_k H| \\
= \left| H \right| + \left| H \right| + \cdots + \left| H \right| \quad \text{(since } \left| a_i H \right| = H \text{ for } a_i \text{)} \\
= |G/H| \cdot |H|.
\]

Similarly \( |G| = |H \setminus G| \cdot |H| \).

\[\square\]

**Corollary 12.3** Let \( G \) be a finite group. Then, \( \forall g \in G \)

\[|\langle g \rangle| \mid |G|\].

**Proof** \( |G| = |G/\langle g \rangle| \cdot |\langle g \rangle| \) by Lagrange's theorem.

**Ex** \( G = \mathbb{Z}/p \) where \( p \) is prime.

\[\Rightarrow \forall k \in \mathbb{Z}/p, \; |k| \neq \text{loj}, \; \text{[k]} \text{ has order } p.\]

**Ex** \( G = S_3, \quad |S_3| = 6.\)

\[\Rightarrow \] if \( \sigma \in S_3 \) then \( \sigma \) has order 1, 2, 3 or 6.

Easy to see: (12), (13), (23) have order 2

(123), (132) have order 3

no elements of order 6.

\( G = \mathbb{Z}/6. \) \[|D_3| \text{ has order 6 since } \langle [12] \rangle = \mathbb{Z}/6\]

**Corollary 12.4** Suppose \( G \) is a finite group and \( |G| = p \)

is prime. Then

1) the only subgroups of \( G \) are \( G \) and \( \{e\}. \)

2) \( \forall g, \in G, \; g \neq e, \; \langle g \rangle = G \)

3) \( \forall \text{ homomorphism } \varphi : G \rightarrow H, \) either \( \varphi (g) = e_H + g \)

or \( \varphi \) is 1-1.
Proof: 1) If $H \leq G$ is a subgroup, then

$|H| \mid |G| = p. \Rightarrow |H| = 1$ or $p. \Rightarrow H = \{e\}$ or $G$.

2) $\langle g \rangle$ is a subgroup. If $g \neq e$, $\langle g \rangle \neq \{e\}$.

$\Rightarrow$ (by (1)) $\langle g \rangle = G$.

3) $\ker \phi$ is a subgroup. By (1) either $\ker \phi = G$ (and then $\phi(g) = e_H \forall g \in G$)

or $\ker \phi = \{e\}$ (and then $\phi$ is 1-1). $\square$