Recall from MTH 182, that an equivalence relation R on a set S is a *relation* on S such that the following properties hold:

1. *Reflexive Property*: sRs for all $s \in S$.
2. *Symmetric Property*: If $s_1 R s_2$, then $s_2 R s_1$ of all $s_1,\ s_2 \in S$.
3. *Transitive Property*: If $s_1 R s_2$ and $s_2 R s_3$ then $s_1 R s_3$ for all $s_1,\ s_2,\ s_3 \in S$.

The equivalence relation R corresponds to a *partition* $S/\sim_R = \left\{ [s]_R \middle| s \in S \right\}$ of S *into* disjoint sets called *equivalence classes,* where

$$[s]_R = \{x \in S \,|\, x \sim_R s\} = \text{subset of the elements of } S \text{ related to } s \in S \text{ by } R.$$

Example 1: If $n > 1$ is an integer and

$$n\mathbf{Z} = \{0, \pm n, \pm 2n, \pm 3n, \cdots\} = \text{the subset of fall integer multiples of } n.$$

and R is the equivalence relation m modulo n on the integers $\mathbf{Z}$ defined by

$$aRb \iff a \equiv b (\mathbf{mod}\ n) \iff a - b \in n\mathbf{Z}$$

then the equivalence class $[a]_R = [a]_n$ since

$$\begin{aligned} [a]_R &= \{x \in \mathbf{Z} \,|\, xRa\} = \{x \in \mathbf{Z} \,|\, x \equiv a (\mathbf{mod}\ n)\} \\ &= \{x \in \mathbf{Z} \,|\, x - a \in n\mathbf{Z}\} = \{x \in \mathbf{Z} \,|\, x \in a + n\mathbf{Z}\} \\ &= \left\{ x = a + nk \middle| k \in \mathbf{Z} \right\} = [a]_n \end{aligned}$$

Because of the *Division Algorithm*, we know that $a = nq + r$ where $0 \le r < n$;hence,

$$\begin{aligned} [a]_n &= \left\{ x = a + nk \middle| k \in \mathbf{Z} \right\} = \left\{ x = (aq + r) + nk \middle| k \in \mathbf{Z} \right\} = \left\{ x = r + n(q + k) \middle| k \in \mathbf{Z} \right\} \\ &= \left\{ x = r + nj \middle| j \in \mathbf{Z} \right\} \text{ where } j = q + k \in \mathbf{Z} \text{ and } 0 \le r < n \\ &= [r]_n \end{aligned}$$

Now, since $[a]_n = \left\{ x = r + nj \middle| j \in \mathbf{Z} \right\}$ where $0 \le r < n$, we can express the equivalence of class a as

$$[a]_n = \left\{ x = r + nj \middle| j \in \mathbf{Z} \right\} = r + n\mathbf{Z}\,.$$

Thus, if $n = 5$, the set $\mathbf{Z}_5$ can be expressed as either

$$\mathbf{Z}_5 = \{[0]_5,\ [1]_5,\ [2]_5,\ [3]_5,\ [4]_5\}$$

or

$$\mathbf{Z}_5 = \{0 + 5\mathbf{Z},\ 1 + 5\mathbf{Z},\ 2 + 5\mathbf{Z},\ 3 + 5\mathbf{Z},\ 4 + 5\mathbf{Z}\}.$$

The properties of $n\mathbf{Z}$ used to show that $\equiv (\mathbf{mod}\, n)$ is an equivalence relation can be reduced to just the following two:

A. $0 \in n\mathbf{Z}$, and
B. For any $a,\ b \in \mathbf{Z},\ a - b \in n\mathbf{Z}$

These properties imply that $n\mathbf{Z}$ is a *subgroup* of the additive group $\mathbf{Z}$; that is a subset of $\mathbf{Z}$ that is, has 0 as its *identity* and is closed under *subtraction,* contains *additive inverses* of its elements, and is closed under *addition*. To see this, first note that (B) shows closure under *subtraction*. Next, by that by setting $a = 0$ and $b = c$ in (B), we find

$$\text{For any } c \in n\mathbf{Z},\ -c = 0 - c \in n\mathbf{Z},$$

which means that $n\mathbf{Z}$ contains *additive inverses* of its elements. Finally, by setting $b = -c$ in (B), we see that

$$\text{For any } a, c \in n\mathbf{Z},\ a + c = a - (-c) \in n\mathbf{Z},$$

which means that $n\mathbf{Z}$ is closed under *addition.*

Remark: For a general group G with a subset $H \subseteq G$ we express these properties by

A'. $e \in H$ (instead of $0 \in n\mathbf{Z}$), and
B'. For any $a,\ b \in H$, then $ab^{-1} \in H$ (instead of $a,\ b \in \mathbf{Z},\ a - b \in n\mathbf{Z}$)

where e is the identity element of G , the *inverse* of b in G denoted by b^{-1} and the group operation is represented by the *juxtaposition* of elements of G. Just as above these two properties imply that H is a subgroup of G.

Proposition 1: Let G be a group and a subgroup $H \subseteq G$.

(i) The relation ${}_H\sim$ on G by

$$a\ {}_H\sim \iff ab^{-1} \in H \text{ for all } a,\ b \in G.$$

is an *equivalence* relation on G.

(ii) The relation $\sim_H$ on G by

$$a \sim_H b \Leftrightarrow a^{-1}b \in H \text{ for all } a, b \in G\,.$$

is an *equivalence* relation on G.

Proof.

(i) To show that ${}_H\sim$ is an equivalence relation, I show that it is *reflexive*, *symmetric* and *transitive*:

Reflexive: Let $a \in G$, then $aa^{-1} \in H \iff a\ {}_H\sim a$.

Symmetric: Let $a,\ b \in G$ and assume $a\ {}_H\sim b$. Then $ab^{-1} \in H$ but since H is a subgroup it contains inverses of its elements. Thus, $ba^{-1} = (b^{-1})^{-1}a^{-1} = \left(ab^{-1}\right)^{-1} \in H$ which means $b\ {}_H\sim a$.

Transitive: Let $a,\ b,\ c \in G$. Assume $a\ {}_H\sim b$ and $b\ {}_H\sim c$. Then $ab^{-1} \in H$ and $bc^{-1} \in H$.
Thus, $ac^{-1} = aec^{-1} = a(b^{-1}b)c^{-1} = (ab^{-1})(bc^{-1}) \in H$ which means $a\ {}_H\sim c$.

(ii) The proof that $\sim_H$ is an equivalence relation is similar and is left to the student.

∎

Let G be a group and a subgroup $H \subseteq G$. Similar to the notation of **Example 1** above, the equivalence class of an element a under the relation ${}_H\sim$ on G is denoted by

$$\begin{aligned}{}_H[a] &= \{x \in G \mid x\ {}_H\sim a\} = \{x \in G \mid xa^{-1} \in H\} = \{x \in G \mid xa^{-1} = h \in H\} \\ &= \{x \in G \mid x = ha \in Ha\} = \{x \in G \mid x \in Ha\} = Ha\end{aligned}$$

Similarly, the equivalence class of the element a under relation $\sim_H$ on G is denoted by

$$\begin{aligned}[a]_H &= \{x \in G \mid x\ \sim_H a\} = \{x \in G \mid a^{-1}x \in H\} = \{x \in G \mid a^{-1}x = h \in H\} \\ &= \{x \in G \mid x = ah \in aH\} = \{x \in G \mid x \in aH\} = aH\end{aligned}$$

Definition: The equivalence class $[a]_H = aH$ is called a *left-coset* of H in G and ${}_H[a] = Ha$ is called a *right-coset* of H in G. The sets $G/\sim_H = \{aH \mid a \in G\}$ and $G/_H\sim = \{Ha \mid a \in G\}$ both form partitions of G; that is,

$$G = \bigcup_{a\in G} aH \text{ where either } (aH) \cap (bH) = \phi \text{ or } aH = bH \text{ for all } a, b \in G$$

and similarly

$$G = \bigcup_{a\in G} Ha \text{ where either } (Ha) \cap (Hb) = \phi \text{ or } Ha = Hb \text{ for all } a, b \in G.$$

Proposition 2: Let G be a group and a subgroup $H \subseteq G$.

(i) For each $a \in G$, the function $\varphi_a : H \to Ha$ defined by $\varphi_a(h) = ha$ is a *bijection*; hence, $|H| = |Ha|$.

(ii) For each $a \in G$, the function ${}_a\varphi : H \to aH$ defined by ${}_a\varphi(h) = ah$ is a *bijection*; hence, $|H| = |aH|$.

(iii) If G is *commutative*, then $Ha = aH$ for all $a \in G$; hence, $G/\sim_H = G/_H\sim = G/H$.

(iv) If G is a *finite* group, then the order (size) $|H|$ of H is a divisor of the order (size) $|G|$ of G. The quotient $[G : H] = |G|/|H| = |G/\sim_H| = |G/_H\sim| = |G/H|$ is called *the index of H in G.* Consequently, the number of l*eft-cosets* is the same as the number of *right-cosets*.

Proof. Let G be a group and a subgroup$H \subseteq G$.

(i) Since $Ha = \{y \in G \mid y = ha, h \in H\}$ the function $\varphi_a : H \to Ha$ is *surjective* (onto). Next assume $\varphi_a(h_1) = \varphi_a(h_2)$ for some $h_1, h_2 \in H$. Then $h_1a = h_2a$; hence,

$$h_1 = h_1e = h_1(aa^{-1}) = (h_1a)a^{-1} = (h_2a)a^{-1} = h_2(aa^{-1}) = h_2e = h_2$$

Therefore, φ_a is also *injective (one to one*). Consequently, $\varphi_a : H \to Ha$ is a *bijection* and $|H| = |Ha|$.

(ii) The proof is similar and is left to the student.

(iii) Assume G is commutative. Then $ha = ah$ for all $a \in G$ and $h \in H$. Therefore,

$$Ha = \{y \in G \mid g = ha, h \in H\} = \{g \in G \mid g = ah, h \in H\} = aH$$

(iv) Assume G is *finite*. Then there are only a *finite* number of left-cosets; that is, for some integer $k > 0$, and elements $a_1, a_2, a_3, \cdots, a_k$ of G,

$$G/\sim_H = \{aH \mid a \in G\} = \{a_1H, a_2H, a_3H, \cdots, a_kH\}.$$

where

$$G = a_1H \cup a_2H \cup a_3H \cup \cdots \cup a_kH \text{ and } (a_iH) \cap (a_jH) = \varnothing \text{ for } i \neq j, 1 \le i, j \le k.$$

But by (i), $|H| = |a_iH|$ for $i = 1, \ldots, k$. Therefore,

$$|G| = |a_1H| + |a_2H| + |a_3H| + \cdots + |a_kH| = k|H|.$$

The unique integer $k = [G : H] = |G|/|H| = |G/\sim_H|$ is just the index of H in G. In a similar fashion, it can also be proved that $k = [G : H] = |G|/|H| = |G/_H\sim|$; hence, the number of left-cosets and the number of right-cosets are equal!

∎

Notes: 1. If G is *noncommutative* and $a \in G$, then $Ha \neq aH$ in general.
2. If G is *noncommutative*, $Ha = aH$ and for all $a \in G$, then H is called a *normal subgroup* of G.
3. *Normal* subgroups are used to study the structure of *noncommutative* groups.

Definition: Let G be a group and let $a \in G$. The set $\langle a \rangle = \{e, a^{\pm 1}, a^{\pm 2}, a^{\pm 3}, \cdots\}$ of all positive and negative powers of a is called the *cyclic subgroup* of G generated by a. If then $\langle a \rangle = G$ is called a *cyclic* group generated by a. If $\langle a \rangle$ is a *finite* group , then it is called a *finite cyclic group;* otherwise it is called an *infinite cyclic* group.

Notes: 1. The reader should check that $\langle a \rangle$ is, in fact, a *commutative* group!
2. A cyclic group can also be expressed additively as $\langle a \rangle = \{0, \ \pm 1a, \pm 2a, \pm 3a, \ \cdots\}$
3. The *additive* group of the integers $\mathbf{Z}$ is an infinite cyclic group and then *additive* group $\mathbf{Z}_n$ has order n.
4. Cyclic subgroups are used to study the structure of *Abelian* (*commutative*) groups.

Corollary 3:. Let G be a group and let $a \in G$.

(i) If either G is a finite group (or $\langle a \rangle$ itself is finite), then

$$\langle a \rangle = \{e, a^1, a^2, a^3, \ \cdots \ a^{n-1}\} \text{ or } \langle a \rangle = \{0, a, 2a, 3a, \ \cdots \ (n-1)a\}$$

for a *unique* integer $n \geq 1$ called the *order of* $\langle a \rangle = O(a) = \left| \langle a \rangle \right|$.

(ii) If G is finite, then $O(a)$ is a divisor of $|G|$.

Proof: The proof is left to the reader.
∎

Problems:

1. Let $S_3 = \{(1), (1,2), (1,3), (2,3), (1,2,3), (1,3,2)\}$
   (a) Find the cyclic subgroup $\langle (1,2) \rangle \subseteq S_3$.
   (b) Find all the left-cosets and all the right-cosets of $\langle (1,2) \rangle$ in S_3. How many are there?
   (c) Find the cyclic subgroup $\langle (1,2,3) \rangle \subseteq S_3$.
   (d) Find the left-cosets and all the right-cosets $\langle (1,2,3) \rangle$ in S_3. How many are there?
2. Find all the subgroups of $\mathbf{Z}_6$ as a group under addition.
3. Find all the subgroups of $\mathbf{Z}_7^{\times}$.
4. Find all the subgroups of S_4.