First, one more fact about monoids:

THM A Let M be a monoid, and let $\mathcal{S}(M)$ be the set of all subsets $A \subset M$. For $A, B \in \mathcal{S}(M)$, i.e. $A, B \subset M$, the product AB is the subset of M defined by

$$\boxed{AB = \{ab : a \in A, b \in B\}}$$

This multiplication makes $\mathcal{S}(M)$ into a monoid in which $\{1\}$ is the identity element.

Proof. For A, B, C in $\mathcal{S}(M)$,

$$\begin{aligned} AB \cdot C &= \{xc : x \in AB, c \in C\} \\ &= \{ab \cdot c : a \in A, b \in B, c \in C\} \\ &= \{a \cdot bc : a \in A, b \in B, c \in C\} \\ &= \{ay : a \in A, y \in BC\} \\ &= A \cdot BC. \end{aligned}$$

Thus our multiplication in $\mathcal{S}(M)$ is associative. Finally, for $A \in \mathcal{S}(M)$,

$$\{1\}A = \{1 \cdot a : a \in A\} = \{a : a \in A\} = A,$$

and similarly $A\{1\} = A$. Thus $\{1\}$ is an (the!) identity element for $\mathcal{S}(M)$.

EXERCISE 1 Show that $MM = M$, for each monoid M.

THM B Let G be a group. For each $g \in G$, define maps l_g & $r_g : G \to G$ by

$$l_g(x) = gx \quad (l_g \text{ is } \underline{\text{left-translation}} \text{ by } g)$$
$$r_g(x) = xg \quad (r_g \text{ is } \underline{\text{right-translation}} \text{ by } g)$$

Then

(1) $l_g l_{g'} = l_{gg'}$, $r_g r_{g'} = r_{g'g}$, $l_g r_{g'} = r_{g'} l_g$ $\forall g, g' \in G$.

(2) Each of the maps l_g & r_g is a bijection, i.e. a permutation of G.

(3) If $f : G \to G$ is any map satisfying $l_g f = f l_g$ for all $g \in G$, then $f = r_{g'}$ for some $g' \in G$: "Only right translations commute with all left translations."

Proof. There is less here than meets the eye:

(1) $g \cdot g'x = gg' \cdot x$, $xg' \cdot g = x \cdot g'g$, $g \cdot xg' = gx \cdot g'$ $\forall g, g', x \in G$.

(2) Taking $g' = g^{-1}$ in the first equation in (1) gives $l_g l_{g'} = l_1 = 1_G$, which is bijective, so l_g is surjective and $l_{g^{-1}}$ is injective, $\forall g \in G$. Replacing g by g^{-1} in this shows that $l_{g^{-1}}$ is surjective and l_g is injective. In particular l_g is both surjective and injective, i.e. bijective. Similarly for r_g.

EXERCISE 2. Prove (3).

COR Let G be a finite group, and let $A \subset G$, $g \in G$. Then *)

$$|gA| = |A| \;\&\; |Ag| = |A|.$$

Proof Since $l_g : G \to G$ is injective, $gA = l_g A$ has the same size as A. Similarly for $Ag = r_g A$.

DEF Let G be a group. A subgroup of G is any subset H of G satisfying: $a, b \in H \Rightarrow ab \in H$; $1 \in H$; $a \in H \Rightarrow a^{-1} \in H$.

Observe that each subgroup of a group is itself a group, with the same multiplication **), same 1, same inverses.

EXERCISE 3. Prove that for each $d \in \mathbb{N}$, the set of all $n \in \mathbb{Z}$ with $d \mid n$ is a subgroup of $\mathbb{Z}^+$.

EXERCISE 4. Let G be a group and let H be a subset of G. Prove that H is a subgroup of $G \iff$ (i) $H \neq \emptyset$; and (ii) $a, b \in H \Rightarrow ab^{-1} \in H$.

DEF Let G be a group, and let H be a subgroup of G. A left H-coset of G is a subset of G of the form gH for some $g \in G$.

Right H-cosets similarly. Observe that the concepts coincide if G is abelian. Thus one may speak of the H-cosets of G, if G is abelian.

*) gA abbreviates $\{g\}A = \{ga : a \in A\}$. Similarly, $Ag = \{ag : a \in A\}$.

**) (but restricted to the elements of H).

LEMMA For each subgroup H of a group G, distinct left cosets are disjoint, i.e.

$$\forall g, g' \in G, \quad \text{if } gH \neq g'H, \text{ then } gH \cap g'H = \phi.$$

Proof. It suffices to show that

$$\forall g, g' \in G \quad \text{if } (gH \cap g'H \neq \phi) \text{ then } \boxed{gH = g'H}.$$

Assuming ◯, there are elements $h, h' \in H$ with $gh = g'h'$, so

$$gH \overset{(=)}{=} g.hH = gh.H = g'h'.H = g'.h'H \overset{(=)}{=} g'H,$$

showing that ◯ implies □. The two (=) follow from the fact that translation of H by an element of H is a permutation of H, in particular a surjective map from H to H, so $hH = H$ and $h'H = H$.

DEF For each subgroup H of a group G, the left H-coset space G/H is the set of all left H-cosets of G, i.e. $G/H = \{gH : g \in G\}$

THM C For each subgroup H of a group G, G/H is a partition of G

Proof. Here the parts are the left H-cosets. Disjoint parts are disjoint by the Lemma. Since $g = g.1 \in gH$ for each $g \in G$, no part is empty, and the parts cover G.

THM D Let G be a finite group. For each subgroup H of G,

$$\boxed{|G| = |G/H|\,|H|}, \text{ i.e. } |G/H| = |G|/|H|. \text{ *)}$$

Proof. The $|G/H|$ parts each have size $|H|$, by the Cor on 8.2, with $A = H$.

DEF If G is a finite group, $|G|$ is the order of G, and for each subgroup H of G, $|G/H|$ is the index of H in G.

THM E (Lagrange) For each subgroup H of a finite group G, the order and index of H divide the order of G.

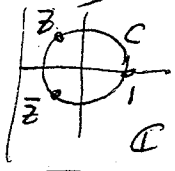
Proof. This follows from THM D.

*) This equation is behind the choice of G/H as the notation for coset space.

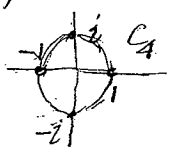
APPLICATION A group of order 6 can have no subgroup of order or index 4, or 5.

EXAMPLES of groups and subgroups

(1) In $\mathbb{C}^* = \mathbb{C} - \{0\}$, the multiplicative group of nonzero complex numbers, the set $C = \{z \in \mathbb{C} : |z| = 1\}$ is a subgroup, the circle group. In C, $z^{-1} = \bar{z}$ the complex conjugate of z.



(2) For each $n \in \mathbb{N}$, $C_n = \{z \in \mathbb{C} : z^n = 1\}$ is a subgroup of C of order n. The elements of C_n are the nth roots of unity. They are the vertices of the regular n-gon inscribed in C one of whose vertices is 1. Observe that C_d is a subgroup of C_n for each $d \mid n$.



(3) Let $G = S_X$, with $X = \{1,2,3\}$. Let's call it S_3 (the symmetric group on $\{1,2,3\}$)
We know that $|S_3| = 3! = 6$. Here are its six elements: Besides 1_X,
three transpositions $(12), (13), (23)$; (12) sends 1 to 2, 2 to 1, 3 to 3; etc., etc.
two 3-cycles $(123), (132)$; (123) sends 1 to 2, 2 to 3, 3 to 1; etc.
The reader should verify that

$$(12)(23) = (123) \quad \& \quad (23)(12) = (132),$$

so S_3 is a nonabelian group. Check also that

$$(12)(12) = 1_X, \quad \text{and} \quad (123)(132) = 1_X.$$

EXERCISE 5 Let a & b be elements in a group G. Prove that if either $ab = 1$ or $ba = 1$, then $b = a^{-1}$.

EXERCISE 6 Let t_3, t_2, t_1 be the three transpositions and r, r^{-1} the two 3-cycles in S_3, in the order in which they were introduced above, so $t_3 t_1 = r$, etc. Prove $\{1\}, \{1, t_1\}, \{1, t_2\}, \{1, t_3\}, \{1, r, r^{-1}\}, S_3$ are all of the subgroups of S_3. (Thus S_3, of order 6, does have subgroups of orders 1, 2, 3, 6 as is not forbidden by Lagrange's Theorem.)