1. Let G be a finite set with an associative law of composition, and $e \in G$ an element with $xe = ex = x$ for all $x \in G$. If G has the property that

$$xa = ya \quad \text{implies} \quad x = y,$$

prove that G is a group.

Solution: Let $|G| = n$, and $G = \{g_1, \ldots, g_n\}$. Let $a \in G$ be an arbitrary element; we need to show it has an inverse. The elements $g_1a, \ldots, g_na$ must be distinct since $g_ia = g_ja$ implies $g_i = g_j$. Since $g_1a, \ldots, g_na$ are n distinct elements, and hence all of the group elements, we must have $g_ia = e$ for some i. But then $ag_ia = ae = ea$, and so $ag_i = e$, and g_i is an inverse for a.

2. Let n be a positive integer, and consider the set G of positive integers less than or equal to n, which are relatively prime to n. The number of elements of G is called the *Euler phi-function*, denoted $\varphi(n)$. For example, $\varphi(1) = 1$, $\varphi(2) = 1$, $\varphi(3) = 2$, $\varphi(4) = 2$, etc.

   (a) Show that G is a group under multiplication mod n.

   (b) If m and n are relatively prime positive integers, show that

$$m^{\varphi(n)} \equiv 1 \mod n.$$

Solution: (a) Let $x, y \in G$. Since they are relatively prime to n, so is their product. Consequently $xy \equiv z \mod n$ for some $z \in G$. The element 1 serves as the identity and since G is finite, we may use Problem 1 above. Suppose $x, y, a \in G$ with $xa \equiv ya \mod n$. Then n divides $xa - ya = (x - y)a$. Since a is relatively prime to n, we must have $n|(x - y)$. But then x and y are both positive integers less than or equal to n, so they must be equal.

(b) Since m is relatively prime to n, there exists $x \in G$ with $x \equiv m \mod n$. The order of x divides $|G| = \varphi(n)$, and so $x^{\varphi(n)} \equiv 1 \mod n$. This implies $m^{\varphi(n)} \equiv 1 \mod n$.

3. Let n be a positive integer. Show that

$$n = \sum_{d|n} \varphi(d),$$

where the sum is taken over all positive integers d which divide n.

(Hint: Recall that a cyclic group of order n has a unique subgroup of order d for each integer d which divides n.)

Solution: Let $G = \mathbb{Z}/\langle n \rangle$. Note that if $x \in G$, then the order of x divides n.

$$\begin{aligned} n = |G| &= \sum_{d|n} \text{number of elements of } G \text{ which have order } d \\ &= \sum_{d|n} \text{number of generators for the unique subgroup of } G \text{ of order } d \\ &= \sum_{d|n} \varphi(d). \end{aligned}$$

4. Let G be a finite group with identity e, which has the property that for every positive integer d, the number of elements x of G with $x^d = e$ is at most d. Show that G must be cyclic.

   Solution: Let $|G| = n$, and $a \in G$ be an element of order d. Then the cyclic group $\langle a \rangle = \{a, a^2, \ldots, a^d\}$ has d distinct elements satisfying $x^d = e$, and so these must be the only elements x with $x^d = e$. Consequently if G has at least one element of order d, then it has precisely $\varphi(d)$ elements of order d. But

$$n \;=\; \sum_{d|n} \text{number of elements of } G \text{ which have order } d \;\leq\; \sum_{d|n} \varphi(d) \;=\; n,$$

   and so for each d dividing n, the number of elements of G which have order d must be precisely $\varphi(d)$. In particular, G has $\varphi(n)$ elements of order n, and therefore is a cyclic group.

5. Let G be a group, and H be a subgroup of finite index. Prove that the number of right cosets of H is equal to the number of left cosets of H.

   Solution: Consider the map

$$f : \{\text{left cosets of } G\} \longrightarrow \{\text{right cosets of } G\}, \quad \text{where} \quad f(xH) = Hx^{-1}.$$

   Now $xH = yH$ if and only if $y^{-1}x \in H$, and this occurs if and only if $Hy^{-1} = Hx^{-1}$. Therefore f is a well defined injective map. It is clearly also surjective, and so gives a bijection between the left cosets and right cosets.

6. If a subgroup of a group G has index 2, show that it must be a normal subgroup.

   Solution: Let H be a subgroup of G of index 2. If $g \in H$ then $gH = Hg$. Next let $g \in G \setminus H$. Since there are only two cosets and $gH \neq H$, we must have $gH = G \setminus H$. By the previous problem, H also has two right cosets, and so similarly $Hg = G \setminus H$. Hence $gH = Hg$ for every $g \in G$.

7. Let G be a finite group in which $x^2 = e$ for all elements $x \in G$. Prove that the order of G is a power of 2.

   Solution: Let $a, b \in G$. Then $(ab)^2 = abab = e$, and so $ab = b^{-1}a^{-1}$. But $b^2 = e$ implies $b = b^{-1}$, and similarly $a = a^{-1}$. Hence $ab = ba$, and so G is abelian.

   We proceed by induction on $|G|$. If $|G| = 1 = 2^0$ there is nothing to be proved, so assume $|G| > 1$. Pick $x \in G$ with $x \neq e$. Then $H = \{e, x\}$ is a normal subgroup, and G/H is also a group which satisfies the hypothesis that the square of every element is the identity. Since

$$|G/H| = |G|/2 < |G|,$$

   the induction hypothesis implies that $|G/H|$ is a power of 2. But then $|G| = |H||G/H| = 2|G/H|$ is a power of 2 as well.

8. Let G be a group such that for a fixed integer $n > 1$, $(xy)^n = x^n y^n$ for all $x, y \in G$. Let $G^{(n)} = \{x^n | x \in G\}$ and $G_{(n)} = \{x \in G | x^n = e\}$.

   (a) Prove that $G^{(n)}$ and $G_{(n)}$ are normal subgroups of G.

   (b) If G is finite, show that the order of $G^{(n)}$ is equal to the index of $G_{(n)}$.

(c) Show that for all $x, y \in G$, we have $x^{1-n}y^{1-n} = (xy)^{1-n}$. Use this to deduce that $x^{n-1}y^n = y^n x^{n-1}$.

(d) Conclude from the above that the set of elements of G of the form $x^{n(n-1)}$ generates a commutative subgroup of G.

Solution: (a) Consider the map $f : G \to G$ with $f(x) = x^n$ for all $x \in G$. The condition $(xy)^n = x^n y^n$ tells us that f is a homomorphism. The kernel of f is precisely $G_{(n)}$, and it follows that $G_{(n)}$ is a normal subgroup. Since $G^{(n)}$ is the image of f, it must be a subgroup. Let $g \in G$ and $x^n \in G^{(n)}$. Then

$$gx^n g^{-1} = (gxg^{-1})^n \in G^{(n)},$$

and so $G^{(n)}$ is a normal subgroup.

(b) The homomorphism f induces an isomorphism $G/G_{(n)} \approx G^{(n)}$ and so, if G is finite, we get

$$(G : G_{(n)}) = |G|/|G_{(n)}| = |G^{(n)}|.$$

(c)

$$\begin{aligned} x^{1-n}y^{1-n} &= xx^{-n}y^{-n}y = x(x^{-1}y^{-1})^n y \\ &= x(x^{-1}y^{-1})\cdots(x^{-1}y^{-1})y \\ &= (y^{-1}x^{-1})\cdots(y^{-1}x^{-1}) = (y^{-1}x^{-1})^{n-1} = (xy)^{1-n}. \end{aligned}$$

Next, taking inverses, we get

$$(xy)^{n-1} = y^{n-1}x^{n-1}.$$

Consequently

$$x^n y^n = (xy)^n = xy(xy)^{n-1} = xyy^{n-1}x^{n-1} = xy^n x^{n-1},$$

and so $x^{n-1}y^n = y^n x^{n-1}$.

(d) For $a, b \in G$,

$$\begin{aligned} a^{n(n-1)}b^{n(n-1)} &= (a^n)^{n-1}(b^{n-1})^n \\ &= (b^{n-1})^n(a^n)^{n-1} = b^{n(n-1)}a^{n(n-1)}. \end{aligned}$$

Consequently elements of G of the form $a^{n(n-1)}$ commute with each other, and hence generate a commutative subgroup.

9. Let G be a group such that

(a) the map $x \mapsto x^3$ permutes elements of G, and

(b) $(xy)^3 = x^3y^3$ for all $x, y \in G$.

Prove that G is abelian.

Solution: Using the previous problem, elements of the form x^6 commute with each other, i.e.,

$$x^6y^6 = y^6x^6 \quad \text{for all} \quad x, y \in G. \qquad (*)$$

For arbitrary elements $a, b \in G$, condition (a) implies that there exist $x, y \in G$ with $a = x^3$ and $b = y^3$, and $(*)$ then implies that $a^2b^2 = b^2a^2$. Now

$$(ab)(ab)(ab) = a^3b^3 = a(a^2b^2)b = a(b^2a^2)b = ab(ba)ab,$$

using which we get $ab = ba$.

10. Let G be a group. If S is a simple group, S is said to *occur* in G if there exist two subgroups H and H' of G, with $H \lhd H'$, such that $H'/H \approx S$. Let $\mathrm{In}(G)$ be the set of isomorphism classes of simple groups occurring in G.

    (a) Prove that
    $$\mathrm{In}(G) = \emptyset \Leftrightarrow G = \{e\}.$$

    (b) If H is a subgroup of G, show that $\mathrm{In}(H) \subset \mathrm{In}(G)$; if H is normal, show that
    $$\mathrm{In}(G) = \mathrm{In}(H) \cup \mathrm{In}(G/H).$$

    (c) Let G_1, G_2 be two groups. Show that the following two properties are equivalent:

    (i)
    $$\mathrm{In}(G_1) \cap \mathrm{In}(G_2) = \emptyset,$$

    (ii) Every subgroup of $G_1 \times G_2$ is of the form $H_1 \times H_2$ with $H_1 \subset G_1$ and $H_2 \subset G_2$.

Solution: (a) Clearly if $G = \{e\}$ then $\mathrm{In}(G) = \emptyset$. If $G \neq \{e\}$, pick $g \in G$ with $g \neq e$. If $\langle g \rangle \approx \mathbb{Z}$, then we have $\langle g^2 \rangle \lhd \langle g \rangle$, and so

$$\langle g \rangle / \langle g^2 \rangle \approx \mathbb{Z}/\langle 2 \rangle$$

is a simple group which occurs in G. If $\langle g \rangle$ is finite, then it is simple if $|\langle g \rangle|$ is prime. Otherwise, let H be a maximal proper subgroup of $\langle g \rangle$. Then $\langle g \rangle / H$ must be simple and occurs in G.

(b) If S occurs in H, then $S \approx H_1/H_2$ where H_i are subgroups of H with $H_2 \lhd H_1$. But then H_i are subgroups of G as well, so S occurs in G.

If $H \lhd G$ and S occurs in G/H, then $S \approx (H_1/H)/(H_2/H)$ where H_i/H are subgroups of G/H with $H_2/H \lhd H_1/H$. But then $H_2 \lhd H_1$, and so

$$S \approx \frac{H_1/H}{H_2/H} \approx H_1/H_2$$

occurs in G. Consequently we have $\mathrm{In}(H) \cup \mathrm{In}(G/H) \subseteq \mathrm{In}(G)$.

Now suppose S occurs in G. Then there exist two subgroups H_1, H_2 of G where $H_2 \lhd H_1$ and $H_1/H_2 \cong S$ is a simple group. Then $H_1 \cap H \lhd H_1$, and hence $H_2 \lhd H_2(H_1 \cap H) \lhd H_1$. Since H_1/H_2 is simple, either $H_2(H_1 \cap H) = H_1$ or $H_2(H_1 \cap H) = H_2$.

In the first case,

$$S \approx H_1/H_2 = H_2(H_1 \cap H)/H_2 \approx (H_1 \cap H)/(H_1 \cap H \cap H_2) = (H_1 \cap H)/(H_2 \cap H),$$

and so S occurs in H.

In the second case, $H_1 \cap H \subset H_2$, and it is easily checked that $H_1 \cap H \lhd H_2$. Note that

$$H_1/H_2 \approx \frac{H_1/(H_1 \cap H)}{H_2/(H_1 \cap H)},$$

which implies that S occurs in $H_1/(H_1 \cap H) \approx H_1H/H$. But H_1H/H is a subgroup of G/H, and so S occurs in G/H.

(c) (i) $\Rightarrow$ (ii) Let H be a subgroup of $G_1 \times G_2$, and set $H_1 = p_1(H)$ and $H_2 = p_2(H)$, where p_1, p_2 are the projection homomorphisms. Let

$$H_1' = \{x \in H_1 : (x, e_2) \in H\} \qquad \text{and} \qquad H_2' = \{y \in H_2 : (e_1, y) \in H\}.$$

It is easily verified that $H_1' \lhd H_1$ and $H_2' \lhd H_2$. Consider the homomorphism

$$\phi : H \longrightarrow H_1/H_1' \qquad \text{where} \qquad \phi((x, y)) = xH_1'.$$

Then

$$\begin{aligned}\operatorname{Ker}\phi &= \{(x, y) \in H : x \in H_1'\} \\ &= \{(x, y) \in H : (x, e_2) \in H\} \\ &= \{(x, y) \in H_1 \times H_2 : (x, e_2) \in H, (e_1, y) \in H\} = H_1' \times H_2'.\end{aligned}$$

Consequently $H/(H_1' \times H_2') \approx H_1/H_1'$ and so, by symmetry,

$$H_1/H_1' \approx H/(H_1' \times H_2') \approx H_2/H_2'.$$

If H is not a direct product of a subgroup of G_1 with a subgroup of G_2, then $H/(H_1' \times H_2') \neq \{e\}$, and so we have a nonempty set

$$\operatorname{In}(H_1/H_1') = \operatorname{In}(H/(H_1' \times H_2')) = \operatorname{In}(H_2/H_2')$$

contained in the intersection $\operatorname{In}(G_1) \cap \operatorname{In}(G_2)$.

(ii) $\Rightarrow$ (i) Suppose there exists $S \in \operatorname{In}(G_1) \cap \operatorname{In}(G_2)$, then there exist subgroups $H_1' \lhd H_1$ of G_1 and $H_2' \lhd H_2$ of G_2, such that $S \approx H_1/H_1' \approx H_2/H_2'$. Let ϕ_i be the composition

$$H_i \longrightarrow H_i/H_i' \xrightarrow{\approx} S, \qquad \text{for} \qquad i = 1, 2.$$

Then $(\phi_1, \phi_2) : H_1 \times H_2 \to S \times S$. Consider the subgroup $\Delta = \{(s, s) \in S \times S\}$ and its inverse image $H = (\phi_1, \phi_2)^{-1}(\Delta)$. Then H is a subgroup of $H_1 \times H_2$, and we claim it is not the direct product of a subgroup of G_1 with a subgroup of G_2.

It is easy to check that $p_1(H) = H_1$ and $p_2(H) = H_2$, and so it suffices to show that $H \neq H_1 \times H_2$. Let $h_1 \in H_1 \setminus H_1'$ and $h_2 \in H_2'$. Then $(\phi_1, \phi_2)((h_1, h_2)) = (\phi_1(h_1), e)$ where $\phi_1(h_1) \neq e$, and so $(h_1, h_2) \in (H_1 \times H_2) \setminus H$.