1 Two groups are equivalent if they are isomorphic. In the list below, find all the equivalence classes, with explanations as to why the equivalence classes are distinct:

a. $\mathbb{Z}/4\mathbb{Z}$

b. $\mathbb{Z}/24\mathbb{Z}$

c. $\mathbb{Z}/4Z \times \mathbb{Z}/6\mathbb{Z}$

d. $\mathbb{Z}/2Z \times \mathbb{Z}/4\mathbb{Z}$

e. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$

f. $(\mathbb{Z}/10\mathbb{Z})^\times$

g. $(\mathbb{Z}/9\mathbb{Z})^\times$

h. $(\mathbb{Z}/5\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times$

i. D_6

j. The subgroup of rotations in D_6

Solution We'll group the classes by cardinality, and then determine which groups are isomorphic to it.

$|G| = 4$:

The groups here are (a) and (f).

We map the elements as follows: $\varphi(0) = 1$, $\varphi(1) = 7$, $\varphi(2) = 9$, and $\varphi(3) = 3$. Notice that both sets are abelian, so we only need to check the following:

$$\begin{aligned}\varphi(1+2) &= 7 = 1 \times 7 = \varphi(0) \times \varphi(1)\\ \varphi(1+3) &= 1 \equiv 7 \times 3 \mod 10 = \varphi(1) \times \varphi(3)\\ \varphi(2+3) &= 7 \equiv 9 \times 3 \mod 10 = \varphi(2) \times \varphi(3),\end{aligned}$$

so $\mathbb{Z}/4\mathbb{Z} \simeq (\mathbb{Z}/10\mathbb{Z})^\times$.

$|G| = 6$:

The groups here are (g) and (j).

Notice that 2 has order 6, so (g) is cyclic. (j) is also cyclic, so we can simply take the map $2^n \mapsto r^n$, where r is a rotation by $\pi/6$, which is clearly an isomorphism. Hence, $(\mathbb{Z}/9\mathbb{Z})^\times \simeq$ rotations in D_6.

$|G| = 8$:

The groups here are (d) and (h).

Notice that $(\mathbb{Z}/5\mathbb{Z})^\times = \langle 2\rangle$ and $(\mathbb{Z}/3\mathbb{Z})^\times = \langle 2\rangle$, so they are cyclic, which means that they are isomorphic to $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/2\mathbb{Z}$, respectively. Thus, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \simeq (\mathbb{Z}/5\mathbb{Z})^\times \times (\mathbb{Z}/3\mathbb{Z})^\times$.

$|G| = 12$:

The only group here is (i), so there is nothing to be said.

$|G| = 24$:

The groups here are (b), (c), and (e).

By the Chinese remainder theorem, $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, so $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

The order of elements in $\mathbb{Z}/4\mathbb{Z}$ and $\mathbb{Z}/6\mathbb{Z}$ must lie in $\{1, 2, 4\}$ and $\{1, 2, 3, 6\}$, respectively. Then the order of $\mathbb{Z}/4\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}$ is given by the largest least common multiple of any of these, which is 12.

Thus, $Z/24\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ cannot be isomorphic, since $Z/24\mathbb{Z}$ has an element of order 24, namely 1. Since $\mathbb{Z}/6\mathbb{Z} \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, we know that $\mathbb{Z}/24\mathbb{Z}$ is not isomorphic to either of them.

2 Give examples of each of the following with justification:

a. A non-abelian group with a proper non-abelian subgroup.

b. A non-abelian group of order 10.

c. A group of order 8 so that every element has order 2 or 1.

d. A group so that the only element that commutes with every element of the group is the identity.

e. A homomorphism of groups which is surjective but not injective.

Solution a. The symmetries of D_6 where we keep 1 fixed, which we'll call D_6^1. D_6 is non-abelian, and D_6^1 is clearly a proper subset of D_6. D_6^1 is also a group since composing these permutations and inverting permutations keep 1 fixed.

b. D_5, the symmetries of a pentagon. We have 5 choices for $D_5(i)$, 2 choices for $D_5(i+1)$, and the rest of the map is fixed, so it has order 10. It is also abelian since a flip and a rotation don't commute in general.

c. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, and the proof is in problem (5).

d. $\{e\}$, the trivial group.

e. $\varphi\colon \mathbb{Z}/4\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$, $[n]_4 \mapsto [n]_2$. This is clearly surjective, but not injective, since $\varphi([0]_4) = \varphi([2]_4) = [0]_2$.

3** Suppose G is a finite group and that H and H' are conjugate subgroups. Show that

$$|H| = |H'|,$$

where $|H|$ is the number of elements in H.

Solution Since H and H' are conjugate, we know that there exists $g \in G$ such that $H' = gHg^{-1}$.

If $g = e$, then it follows that $H = H'$, so they clearly have the same number of elements.

Otherwise, we can define a bijection as follows: $\varphi\colon H \to H'$, $\varphi(h) = ghg^{-1}$. It is one-to-one since

$$ghg^{-1} = gh'g^{-1} \implies h = g^{-1}ghg^{-1}g = h'.$$

Moreover, it is onto, since if $h' \in H'$, then by definition, there exists $h \in H$ such that $h' = ghg^{-1} = \varphi(h)$, so φ is a bijection. Hence, $|H| = |H'|$.

---

4 Suppose G is a finite group and $H \subseteq G$ is a subgroup of index 2. Show for any $g \in G$, that $gHg^{-1} = H$. *Hint*: Look at the left and right cosets of H.

Solution Since H is a subgroup of index 2, it has one distinct left coset aH. Similarly, it has a distinct right coset Hb. Since H together with its cosets partition G, we must have that $aH = Hb$, i.e., the left coset and right coset of H are the same.

Let $g \in H$. Then $gH = H$ and $Hg = H$, since H is a subgroup, so $gH = Hg \implies H = g^{-1}Hg$.

If $g \in G \setminus H$, then $gH \neq H$ and $Hg \neq H$, so $gH = Hg \implies H = g^{-1}Hg$.

5 Classify all groups of order 8 up to isomorphism. You should show that any group show that any group of order 8 is one of the groups you know and love. *Hint*: Look at Elman 8.5.3.

Solution Let G be a group with order 8.

Since G is a group, by Lagrange's theorem, the order of any element must be among $\{1, 2, 4, 8\}$.

$\underline{\exists\, a \in G \text{ such that } \operatorname{ord}(a) = 8}$:

In this case, $\langle a \rangle = G$, so G is cyclic. Thus, $G \simeq \mathbb{Z}/8\mathbb{Z}$.

$\underline{\exists\, a \in G \text{ such that } \operatorname{ord}(a) = 4}$:

$\underline{\exists\, b \in G \setminus \langle a \rangle \text{ with } \operatorname{ord}(b) = 2}$:

In this case, $|\langle a \rangle| = 4$, and if $a^n \in \langle a \rangle$, then $ba^n \notin \langle a \rangle$. Indeed, if $ba^n = a^m$, then $b = a^m a^{-n} \in \langle a \rangle$.

Moreover, bab^{-1} is a permutation of $\langle a \rangle$. There are only two isomorphisms from $\langle a \rangle$ to itself: the identity permutation and the permutation $a \mapsto a^3$. $a \mapsto a^2$ doesn't work because a has order 4 whereas a has order 2.

$\underline{bab^{-1} \text{ is the identity permutation}}$:

In this case, we see that $b^2 a = ab^2 = bab = a$. Thus, the elements can be written in the form $a^n b^m$, with $n \in \{0, 1, 2, 3\}$ and $m \in \{0, 1\}$, so we see that $G \simeq \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

$\underline{bab^{-1} \text{ is the permutation } a \mapsto a^3}$:

Then $bab^{-1} = a^3$, so we see that

$$G = \langle a, b \mid a^4 = 1,\ b^2 = 1,\ bab^{-1} = a^3 \rangle = D_4,$$

so in this case, $G \simeq D_4$.

$\underline{\exists\, b \in G \setminus \langle a \rangle \text{ with } \operatorname{ord}(b) = 4}$:

The same argument as above holds here, but with $b^4 = 1$. Hence, $G \simeq Q_8$.

<u>All elements of G have order 2</u>:

In this case, G is abelian, indeed, for all $a, b \in G$, we have $abba = e = ab(ab)$, so we see $ba = ab$.

Pick $a \in G$. Then $|\langle a \rangle| = 2$.

Pick $b \in G \setminus \langle a \rangle$. Then $|\langle a, b \rangle| = 4$. Indeed, $\langle a, b \rangle = \{e, a, b, ab\}$ because G is abelian.

Pick $c \in G \setminus \langle a, b \rangle$. Then $|\langle a, b, c \rangle| = 8$ for the same reason above. Since G is abelian, given $a^\ell b^m c^n$ and $a^x b^y c^z$,

$$(a^\ell b^m c^n)(a^x b^y c^z) = a^{\ell+x} b^{m+y} c^{n+z},$$

which is the same thing as addition in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. The representation of an element in $\langle a, b, c \rangle$ gives a natural bijection to the group, so we get $G \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

---

6 In D_6, let r be a rotation. Let H be the subgroup $\{e, r^2, r^4\}$. List all the left cosets in G/H.

Solution The left cosets are the following:

$$\begin{aligned} H &= \{e, r^2, r^4\} \\ rH &= \{r, r^3, r^5\} \\ fH &= \{f, fr^2, fr^4\} \\ rfH &= \{rf, rfr^2, rfr^4\}. \end{aligned}$$

We know that these are all the cosets since the left cosets of H partition D_6, so since $|D_6| = 12$, H has $|D_6|/|H| = 4$ cosets.

10.16.2** Let G be a group of order p^n where p is a prime and $n \geq 1$. Prove that there exists an element of order p in G.

Solution We will prove this by strong induction.

Base step:

Let G be a group of order p. By a corollary of Lagrange's theorem, $g^{|G|} = g^p = e$ for any $g \in G$. Thus, given an element g, its order must divide p. Since p is prime, g has either 1 or p. Since g has more than one element, we pick an element that is not the identity, and that element has order p.

Inductive step:

Suppose that the conclusion is true for groups of order $p, p^2, \dots, p^n$. We wish to show that these imply that it holds for groups of order p^{n+1}.

Let G be a group of order p^{n+1}. By a corollary of Lagrange's theorem, for all $g \in G$, $g^{p^{n+1}} = e$. Since p is prime, $\operatorname{ord}(g) \mid p^n \implies \operatorname{ord}(g) \in \{1, p, \dots, p^{n+1}\}$.

Pick any element g other than the identity element.

If $\operatorname{ord}(g) = p$, then we're done.

If $\operatorname{ord}(g) = p^{n+1}$, then g^{p^n} has order p, indeed, $(g^{p^n})^p = g^{p^{n+1}} = e$. Its order cannot be less than p because otherwise, it would have order 1, which is a contradiction since we assumed $p \neq e$.

Otherwise, if $\operatorname{ord}(g) = p^\ell$ for some $2 \leq \ell \leq n$, consider $\langle g \rangle \subseteq G$, which has order p^ℓ, so it has an element g' of order p in $\langle g \rangle$, by the inductive hypothesis. This means that it has order p in G also, so the inductive step holds.

By induction, a group of order p^n has an element of order p.

10.16.4 Let H and K be subgroups of the group G.

Let $HK := \{hk \mid h \in H,\ k \in K\}$. Then (clearly) $H/(H \cap K)$ is a subset of $G/(H \cap K)$ and HK/K is a subset of G/K. Show that $f\colon H/(H \cap K) \to HK/K$ by $h(H \cap K) \mapsto hK$ is a well-defined bijection.

Solution Let $h, h' \in H$ so that $hH = h'H$. Then $h(H \cap K) \mapsto hK$ and $h'(H \cap K) \mapsto h'K$. We want to show that $hK = h'K$.

Since $h(H \cap K) = h'(H \cap K)$, there exists $g, g' \in H \cap K$ such that $hg = h'g' \implies h = h'g'g^{-1}$. Then if $k \in K$,

$$hK \ni hk = h'\big(g'g^{-1}k\big) \in h'K,$$

since $g, g' \in K$. So, $hK \subseteq h'K$, and similarly, $h'K \subseteq hK$. Thus, $hK = h'K$, so the map is well-defined.

We'll now show injectivity:

Let $hK, h'K \in HK/K$ with $hK = h'K$. Since $H \cap K \subseteq K$, $h(H \cap K) = h'(H \cap K)$, so injectivity holds.

Surjecitivity is clear: for every $hK \in HK/K$, $h(H \cap K) \mapsto hK$.

Thus, the map is a well-defined bijection.

10.16.6** Let H and K be subgroups of the group G.

If $K \subseteq H \subseteq G$, show that $[G : K] = [G : H][H : K]$ (even if any are infinite if read correctly).

Solution Assume that G is finite.

By Lagrange's theorem, $|G| = |K|[G : K]$ and $|G| = |H|[G : H]$.

Similarly, $K \subseteq H$, so K is a subgroup of H. Hence, $|K| = |H|[K : H]$. Thus,

$$|H|[G : H] = |K|[G : K] = |H|[K : H][G : K] \implies [G : H] = [K : H][G : K],$$

by cancelling out $|H|$.

10.16.11 Prove that a group of order 30 can have at most 7 subgroups of order 5.

Solution We first prove the following fact: If K and H are subgroups of G with order 5, then $K \cap H = \{e\}$ or they are the same.

Suppose $K \neq H$, but$K \cap H$ contains an element $g \neq e$. Then g has either order 5 or order 1, by Lagrange's theorem. $g \neq e$, so g must have order 5, but this implies that $|\langle g \rangle| = |H| = |K| = 5$, which means that $\langle g \rangle = H = K$. This is a contradiction, as we assumed $H \neq K$, so their intersection must be $\{e\}$.

This fact tells us that a subgroup contains e and 4 other elements that are not in any other subgroup.

If the group G has 8 subgroups of order 5, then this implies that G has $1+8\cdot 4 > 30$ elements, so 8 subgroups is not possible.

On the other hand, if G has 7 subgroups, then they make up $1 + 7 \cdot 4 = 29 < 30$ elements, which is possible. Any smaller number of subgroups is possible.