Alert! In $\mathbb{Z}_n$, I use m to refer to $[m]$. Also, I sometimes use $[g]_H$ or simply $[g]$ refer to cosets in G/H.

Problem 2.

(a) Prove that the relation given by $a \sim b \iff a - b \in \mathbb{Z}$ is an equivalence relation on the additive group $\mathbb{Q}$.

(b) Prove that $\mathbb{Q}/\mathbb{Z}$ is an infinite abelian group.

Proof.

(a) For any $a, b, c \in \mathbb{Q}$

$$[\mathbf{a} \sim \mathbf{a}]: \quad a - a = 0 \in \mathbb{Z} \implies a \sim a.$$

$$[\mathbf{a} \sim \mathbf{b} \implies \mathbf{b} \sim \mathbf{a}]: \quad a \sim b \implies a - b \in \mathbb{Z} \implies -(a-b) = b - a \in \mathbb{Z} \implies b \sim a.$$

$$[\mathbf{a} \sim \mathbf{b}, \mathbf{b} \sim \mathbf{c} \implies \mathbf{a} \sim \mathbf{c}]: \quad a \sim b, b \sim c \implies c \sim b \implies (a-b)-(c-b) = a - c \in \mathbb{Z} \implies a \sim c.$$

So $\sim$ is an equivalence relation on $(\mathbb{Q}, +)$.

(b) $\mathbb{Q}/\mathbb{Z} = \{[q] = q + \mathbb{Z} \mid q \in \mathbb{Q}\}$. Consider any $q_1, q_2 \in (0,1) \cap \mathbb{Q}$. If $[q_1] = [q_2]$, then $[q_1] - [q_2] = \mathbb{Z}$ and $q_1 - q_1 \in \mathbb{Z}$. Well, $q_1, q_2 \in (0,1)$, so $q_1 - q_2 \in (-1,1) \cap \mathbb{Z} \implies q_1 - q_2 = 0$. So $[q_1] = [q_2] \implies q_1 = q_2$. On the other hand, $q_1 = q_2 \implies [q_1] = [q_2]$ by definition. So then

$$q_1 = q_2 \iff [q_1] = [q_2], \forall q_1, q_2 \in (0,1) \cap \mathbb{Q}.$$

Since the rationals are dense in $\mathbb{R}$, there are infinitely many distinct rationals in $(0,1)$ and infinitely many distinct cosets of the form $[q]$ where $q \in (0,1) \cap \mathbb{Q}$. Therefore, $\mathbb{Q}/\mathbb{Z}$ is infinite. Lastly, since $(\mathbb{Q}, +)$ is Abelian, so is $\mathbb{Q}/\mathbb{Z}$ since $[q_1] + [q_2] = [q_1 + q_2] = [q_2 + q_1] = [q_2] + [q_1]$.

Thus,

$$\mathbb{Q}/\mathbb{Z} \text{ is an infinite Abelian group.}$$

$\square$

Problem 3. Let p be a prime number and let $Z(p^\infty)$ be the following subset of the group $\mathbb{Q}/\mathbb{Z}$:

$$\mathbb{Z}(p^\infty) = \left\{ \left[\frac{a}{b}\right] \in \mathbb{Q}/\mathbb{Z} \,\middle|\, a,b \in \mathbb{Z},\ b = p^i \text{ for some } i \geq 0 \right\}.$$

Prove that $\mathbb{Z}(p^\infty)$ is an infinite subgroup of $\mathbb{Q}/\mathbb{Z}$.

Proof. Clearly, $\mathbb{Z}(p^\infty) \subset \mathbb{Q}/\mathbb{Z}$. Consider any integers $i, j \geq 0$ and let $a_i, a_j \in \mathbb{Z}$.

$$\textbf{[Closure]:} \quad \left[\frac{a_i}{p^i}\right] + \left[\frac{a_j}{p^i}\right] = \left[\frac{p^j(a_i) + p^i(a_j)}{p^{i+j}}\right] \in \mathbb{Z}(p^\infty).$$

$$\textbf{[Inverses]:} \quad \left[\frac{-a_i}{p^i}\right] + \left[\frac{a_i}{p^i}\right] = [0] \implies -\left[\frac{a_i}{p^i}\right] = \left[\frac{-a_i}{p^i}\right].$$

So $\mathbb{Z}(p^\infty) \leq \mathbb{Q}/\mathbb{Z}$. Next, for any $i, j \in \mathbb{Z}^+$, notice that $\frac{1}{p^i}, \frac{1}{p^j} \in (0,1)$. We showed in **Problem 3** that $[q_1] = [q_2] \iff q_1 = q_2, \forall q_1, q_2 \in (0,1)$. Well, if $i \neq j$, then $\frac{1}{p^i} \neq \frac{1}{p^j}$. Therefore, since there are infinitely many distinct positive integers $k \in \mathbb{Z}^+$, there are infinitely many distinct cosets of the form $\left[\frac{1}{p^k}\right]$ in $\mathbb{Z}(p^\infty)$. Thus,

$$\mathbb{Z}(p^\infty) \text{ is an infinite subgroup of } \mathbb{Q}/\mathbb{Z}.$$

$\square$

Problem 5. Let Q_8 be the multiplicative group generated by the complex matrices

$$A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}.$$

Observe that $A^4 = B^4 = I_2$ and $BA = AB^3$. Prove that Q_8 is a group of order 8.

Proof. We will use the notation $-M$ to denote $(-m_{ij})$ where $M = (m_{ij})$. To begin, notice that

$$A^2 = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I \implies A^3 = A(-I) = -A.$$

We are given that $A^4 = I$, the identity. So $|A| = 4$. Similarly, notice that

$$B^2 = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = A^2 = -I,$$

and then obviously $B^{-1} = B^3 = -B$ and we are given that $B^4 = I$, so $|B| = 4$.

So $\langle A \rangle, \langle B \rangle \leq Q_8$ are both cyclic subgroups of order 4. Observe.

$$\langle A \rangle \cap \langle B \rangle = \{I, -I\} \implies |\langle A \rangle \langle B \rangle| = \frac{|\langle A \rangle||\langle B \rangle|}{|\langle A \rangle \cap \langle B \rangle|} = \frac{(4)(4)}{(2)} = 8.$$

Well, we are given that A and B generate all of Q_8, which means $Q_8 = \langle A, B \rangle = \langle A \rangle \langle B \rangle$.

Thus,

$$|Q_8| = |\langle A, B \rangle| = |\langle A \rangle \langle B \rangle| = \frac{|\langle A \rangle||\langle B \rangle|}{|\langle A \rangle \cap \langle B \rangle|} = 8.$$

$\square$

Problem 6. Let G be a group and let $\mathrm{Aut}(G)$ denote the set of all automorphisms of G.

(a) Prove that $\mathrm{Aut}(G)$ is a group with composition of functions as the binary operation.

(b) Prove that $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2,\ \mathrm{Aut}(\mathbb{Z}_6) \cong \mathbb{Z}_2,\ \mathrm{Aut}(\mathbb{Z}_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2,\ \mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$ (p prime).

Proof. Let *meow* □

Problem 8. Let G be the multiplicative group of 2×2 invertible matrices with rational entries. Show that

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}, \qquad B = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

have finite orders but AB has infinite order.

Proof. Note the following products.

$$A^2 = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2 = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = -I \implies A^4 = (-I)^2 = I$$
$$B^2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \implies B^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I$$
$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} = (AB)^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$$

Above it is shown A and B have finite order. Now consider non-trivial powers of (AB). $\square$

Problem 10. Let H, K be subgroups of a group G. Prove that HK is a subgroup of G if and only if $HK = KH$.

Proof.
($\Rightarrow$) $HK \leq G \implies$ For all $hk \in HK$, $(hk)^{-1} = k^{-1}h^{-1} \in HK$. Therefore, $HK = \{hk \mid h \in H, k \in K\} = \{k^{-1}h^{-1} \mid k \in K, h \in H\} = KH$.

($\Leftarrow$) Note $HK = KH \implies \forall hk \in HK, \exists (h_k, k_h) \in H \times K,$ such that $hk = k_h h_k \in KH = HK$. The same logic holds for 'flipped' elements $kh \in KH = HK$. Observe.

> **[Closure]:** $(h_1k_1)(h_2k_2) = (h_1k_1)(k_{h_2}h_{k_2}) = h_1(k_1k_{h_2})h_{k_2} = (k_1k_{h_2})_{h_1} h_{k_1k_{h_2}} h_{k_2} \in KH = HK$.
>
> **[Inverses]:** For any $hk \in HK$, $(hk)^{-1} = k^{-1}h^{-1} \in KH = HK$.

So $HK \leq G$.

Thus,

$$HK \leq G \iff HK = KH.$$

$\square$

Problem 11. Let H, K be subgroups of finite index of a group G such that $[G : H]$ and $[G : K]$ are relatively prime. Prove that $G = HK$.

Proof. We begin by proving $(H \cap K) \leq H, K \leq G$.
[1-Step]: $\forall a, b \in (H \cap K)$, $ab^{-1} \in H$ and $ab^{-1} \in K \implies ab^{-1} \in (H \cap K) \implies (H \cap K) \leq H, K \leq G$.

Since $(H \cap K) \leq H, K \leq G$, by the Tower Rule for groups,

$$[G : (H \cap K)] = [G : H][H : H \cap K] = [G : K][K : H \cap K] \implies [K : H \cap K] = \tfrac{[G:H][H:H\cap K]}{[G:K]}$$
$$\text{and } \gcd([G : H], [G : K]) = 1 \implies [G : K] \mid [H : H \cap K].$$

Now consider $H_K = \{hK \mid h \in H\} \subseteq G/K$ and $H/(H \cap K) = \{h(H \cap K) \mid h \in H\}$. Well,

$H \ni h_2 \in [h_1]_K \iff h_1K = h_2K \iff h_2^{-1}h_1 \in K \iff h_2^{-1}h_1 \in (H \cap K) \iff h_2 \in [h_1]_{(H \cap K)}$

$H \ni h_2 \in [h_1]_{(H \cap K)} \iff h_1(H \cap K) = h_2(H \cap K) \iff h_2^{-1}h_1 \in (H \cap K) \iff h_2^{-1}h_1 \in K \iff h_2 \in [h_1]_K$

So $h_2 \in [h_1]_K \iff h_2 \in [h_1]_{(H \cap K)}$ and clearly $[h]_K \leftrightarrow [h]_{(H \cap K)}$ is a bijection from H_K to $H/(H \cap K)$. Observe.

$(H_K \subseteq G/K) \iff (|H_k| \leq [G : K])$ and then $(|H_k| \leq [G : K])$ with $([G : K] \mid [H : H \cap K] = |H_K|)$ implies that $|H_K| = [G : K]$. Therefore, $H_k \not\subset G/K$ and we must have that $H_K = G/K$. Therefore, $\forall g \in G, \exists h_g \in H$ such that $gK = h_gK$. Finally, $h_g^{-1}g \in K \implies \exists k_g \in K$ such that $h_g^{-1}g = k_g \implies g = h_gk_g$. So we see that $\forall g \in G$, $\exists (h_g, k_g) \in H \times K$ such that $g = h_gk_g$.

Thus,

$$H, K \leq G \text{ and } \gcd([G : H], [G : K]) = 1 \implies G = HK.$$

$\square$

Problem 12. Let H,K,N be subgroups of G such that $H \subseteq N$. Prove that $HK \cap N = H(K \cap N)$.

Proof. Notice that since $H \subseteq N$, $HN = N$. Therefore, we show $H(K \cap N) = HK \cap HN = HK \cap N$.
$[\subseteq]: \forall a \in H(K \cap N)$, $a = hg$ where $h \in H$ and $g \in (K \cap N)$. Well, $g \in K \implies a = hg \in HK$. Similarly, $g \in N \implies a = hg \in HN$. Therefore, $a \in HK \cap HN \implies H(K \cap N) \subseteq (HK \cap HN) = (HK \cap N)$.

$[\supseteq]: \forall a \in HK \cap HN$, $a = hg$ where $hg \in HK$ and $hg \in HN$. So then $g \in K$ and $g \in N$ and we have $a = hg$ where $h \in H$ and $g \in K \cap N$. Therefore, $a \in H(K \cap N) \implies H(K \cap N) \subseteq HK \cap HN = HK \cap N$.

Thus,

$$H,K,N \leq G \text{ and } H \subseteq N \implies HK \cap N = HK \cap HN = H(K \cap N).$$

$\square$

Problem 13. Let H,K,N be subgroups of G such that $H \subseteq K$, $H \cap N = K \cap N$, $HN = KN$. Prove that $H = K$.

Proof. $H \subseteq K$ is given. We show $K \subseteq H$ to prove the statement.
$[\supseteq]$: $\forall k \in K$, $\exists h_k \in H$ such that $kN = h_kN$ and so $h_k^{-1}k \in N$. Well, $h_k^{-1} \in H \subseteq K$ and therefore by closure $h_k^{-1}k \in K \implies h_k^{-1}k \in (K \cap N) = (H \cap N)$. Finally, $h_k^{-1}k \in H$ and so $\exists h_* \in H$ such that $h_k k = h_* \implies k = h_k h_* \in H$. Therefore, $K \subseteq H$.

Thus,
$$H,K,N \leq G \text{ with } H \subseteq K, H \cap N = K \cap N, \text{ and } HN = KN \implies H = K.$$
$\square$

We prove the following lemma to be used for **Problem 16.**

Lemma. *Any subgroup H of a cyclic group G is cyclic, and if G has order $N \in \mathbb{Z}^+$ there exists exactly one subgroup $H_d \leq G$ of order d for each divisor d of $|G| = N$.*

Proof. Let $G = \langle g \rangle$. If $H = \{g^0\} = \{e\}$ it is cyclic. If H is non-trivial, then it contains some $h \neq e$. Well, since $h \in H \leq G$, we have that $h = g^k$ for some $k \in \mathbb{Z} \setminus \{0\}$. So then there exists some minimal positive power $n = \min\{i \in \mathbb{Z}^+ \mid g^i \in H \setminus \{e\}\}$ of g present in $H \setminus \{e\}$. Observe.

By the division algorithm and since $n \leq m$, $\forall m \in \{i \in \mathbb{Z}^+ \mid g^i \in H\}$, $\exists (q,r) \in (\mathbb{Z}^+)^2$ with $0 \leq r < n$ such that

$$m = nq + r \implies g^m = g^{nq+r} = g^{nq}g^r \implies g^{m-nq} = g^r \in H.$$

But since n is the minimal positive power of g in H, $r = 0$ otherwise we get a contradiction via $0 < r < n$. So then for any $m \in \mathbb{Z}^+$, such that $g^m \in H$, by the division algorithm we have that $g^m = g^{nq+(0)} = (g^n)^q$ for some $q \in \mathbb{Z}^+$. Note that this accounts for all elements of H, since all negative powers of g in H are inverses of positive powers of g in H, which are multiples of n, and since $g^0 = e \in H \leq G$ by definition.

Next, if G is finite and of order N, consider any divisor d of $|G| = N$. Since $G = \langle g \rangle$, $|g| = N$. Well, since $d|N$, $\exists! q \in \mathbb{Z}^+$ such that $dq = N$. So we see $g^{dq} = g^N \implies (g^q)^d = e$. Such a d is necessarily a minimal power that gives identity here since $0 < q, d$ and otherwise $N = d'q < dq = N$, which is nonsense. So $|g^q| = d$. So then there is only one power q of g that has order $|g^q| = d$ (otherwise the existence of $q' \neq q$ such that $|g^{q'}| = d \implies N = q'd \neq qd = N$... nonsense.) Since any $d-$ordered subgroup H_d of G is cyclic, it must be generated by some power of G, of which there is only one and so $H_d = \langle g^d \rangle$ is the only subgroup of order d which divides N.

$\square$

Now we present the solution to 16 on the following page.

Problem 16. If H is a cyclic normal subgroup of a group G, then every subgroup of H is normal in G.

Proof. Suppose $|H| = n$. Since $K \leq H = \langle h \rangle$ where $|h| = n$, K is cyclic by our lemma and there exists some minimal positive power $d \in \mathbb{Z}^+$ of h such that $K = \langle h^d \rangle$. So any $k \in K$ is of the form $k = (h^d)^q$ for some minimal power $q \in \mathbb{Z}^+$. Since $H \trianglelefteq G$,

$$\forall g \in G, gHg^{-1} = H \iff \forall (g, h^q) \in G \times H, \exists h^p \in H, \text{ such that } gh^q g^{-1} = h^p. \text{ for any powers } p, q \in \mathbb{Z}^+$$

Observe.

$$(gh^q g^{-1})^m = \overbrace{(gh^q g^{-1})(gh^q g^{-1}) \cdots (gh^q g^{-1})}^{m} = \overbrace{g(h^{2q} g^{-1})(gh^q g^{-1}) \cdots (gh^q g^{-1})}^{m-1} = \cdots = gh^{mq} g^{-1} = h^{mp}.$$

So then for any $k \in K = \langle h^d \rangle$, where $k = (h^d)^q = (h^q)^d$ and any $g \in G$, $\exists h^p \in H$ such that

$$gh^q g^{-1} = h^p \implies gkg^{-1} = g(h^q)^d g^{-1} = (g(h^q)g^{-1})^d = (h^p)^d = (h^d)^p \in \langle h^d \rangle = K.$$

Note that since $gkg^{-1} = h^{dp}$ implies $gk = h^{dp} g$, there is only one power $(h^d)^p \in K$ for which the equality holds otherwise we get a contradiction. So for each $k_l \in K$, $\exists! k_r \in K$ such that $gk_l g^{-1} = k_r$. To avoid further nightmare indexing, note that we are taking the union of all conjugates $gk_l g^{-1} \in gKg$ on the left side and showing that since each conjugate is paired with some unique $k_r \in K$ on the right side. The union of all conjugates $gk_l g^{-1}$ is equal to the union of all their unique partners k_r and since there are $|K|$ conjugates and $|K|$ unique partners, of course the right side must be all of K.

$$\bigcup_{k_l \in K} gk_l g^{-1} = gKg^{-1} = \bigcup_{gk_l g^{-1} = k_r \in K} k_r = K.$$

Thus,

$$K \leq H = \langle h \rangle \trianglelefteq G \implies K \trianglelefteq G.$$

$\square$

Problem 21. If G is a finite group and H,K are subgroups of G, then

$$[G : H \cap K] \leq [G : H][G : K].$$

Proof. Since G is finite and $H,K \leq G$, we have the following

$$|HK| = \frac{|H||K|}{|H \cap K|} \leq |G| \tag{1}$$

$$[G : H] = \frac{|G|}{|H|} \tag{2}$$

$$[G : K] = \frac{|G|}{|K|} \tag{3}$$

$$\implies [G : H][G : K] = \frac{|G|^2}{|H||K|} \tag{4}$$

$$[G : H \cap K] = \frac{|G|}{|H \cap K|} \tag{5}$$

Observe.

$$|HK| = \tfrac{|H||K|}{|H\cap K|} \leq |G| \implies (|G|)\tfrac{|H||K|}{|H\cap K|} \leq |G|^2 \implies (\tfrac{|G|}{|H||K|})\tfrac{|H||K|}{|H\cap K|} = \tfrac{|G|}{|H\cap K|} = [G : K] \leq \tfrac{|G|^2}{|H||K|} = [G : H][G : K]$$

□

Problem 22. If H,K,L are subgroups of a finite group G such that $H \subseteq K$, then

$$[K:H] \geq [L\cap K : L\cap H].$$

Proof.
Consider elements in $K/H = \{kH \mid k \in K\}$ and $(L\cap K)/(L\cap H) = \{k(L\cap H) \mid k \in (L\cap K)\}$. Well,

$$k_2 \in [k_1]_{(L\cap H)} \implies k_1(L\cap H) = k_2(L\cap H) \implies k_2^{-1}k_1 \in (L\cap H) \implies k_2^{-1}k_1 \in H \implies k_2 \in [k_1]_H$$

Therefore $f : (L\cap K)/(L\cap H) \to K/H$ where $f([k]_{L\cap H}) = [k]_H$ is well-defined. Observe.

$\forall [k_1]_{(L\cap H)}, [k_2]_{(L\cap H)} \in (L\cap K)/(L\cap H)$, if $f([k_1]_{(L\cap H)}) = f([k_2]_{(L\cap H)})$, then $[k_1]_H = [k_2]_H$ by definition. So then $k_2^{-1}k_1 \in H$ and since $[k_1]_{(L\cap K)}, [k_2]_{(L\cap K)} \in (L\cap K)/(L\cap H)$, obviously $k_1, k_2 \in L$. So $k_2^{-1}k_1 \in L$ by closure and finally $k_2^{-1}k_1 \in (L\cap H) \implies [k_1]_{(L\cap H)} = [k_2]_{(L\cap H)}$. So f is injective.

Therefore, since G is finite and f is an injection from $(L\cap K)/(L\cap H)$ to K/H it must be the case that $|(L\cap K)/(L\cap H)| = [L\cap K : L\cap H] \leq [K:H] = |K/H|$. Otherwise, the mapping either wouldn't be well-defined or wouldn't be injective by the Pigeonhole Principle, both contradictions.

Thus,

If H,K,L are subgroups of a finite group G such that $H \subseteq K$, then $[K:H] \geq [L\cap K : L\cap H]$.

□

Problem 23. Let H,K be subgroups of a group G. Assume that $H \cup K$ is a subgroup of G. Prove that either $H \subseteq K$ or $K \subseteq H$.

Proof. $H \cup K \leq G \implies \forall (h,k) \in H \times K,$ we have $hk \in H \cup K$ by closure. Therefore,

$$H \cup K = \{g \mid g \in H \text{ or } g \in K\} \text{ so for each product } hk \in H \cup K \text{ either } hk = g \in H \text{ or } hk = g \in K \text{ or both.}$$

So in fact the only certainty here is that $H \cup K \neq H \sqcup K$ otherwise $hk \notin H \cup K$ which is a subgroup of G. Therefore, necessarily $K \subset H$ or $H \subset K$ or $H = K$.

Thus,

$$H,K,H \cup K \leq G \implies H \subseteq K \text{ or } K \subseteq H.$$

□