Alert! In $\mathbb{Z}_n$, I use m to refer to $[m]$, and since our operations are well-defined on them, I use them as integers at times. Also, I sometimes use $[g]_H$ or simply $[g]$ refer to cosets in G/H.

Lastly, I know you don't need problem 1, but I use it later to show $\text{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}$. It was also a mistake to do it this way, I thought it would be fun but it wasn't. It also isn't fun to read... sorry about that.

Problem 1. If p is a prime number, prove that the nonzero elements of $\mathbb{Z}_p$ form a multiplicative group of order $p-1$. Show that this statement is false if p is not a prime.

Proof. Consider $\mathbb{Z}_4 \setminus \{0\} = \{1,2,3\}$. $2(2) = 0 \notin \mathbb{Z}_4 \setminus \{0\}$, so closure doesn't hold and it can't be a group under multiplication at all. Therefore, the statement is false if p is not prime. Now consider the statement for a prime p.

$\mathbb{Z}_2 = \{0,1\}$ and so $\mathbb{Z}_2^* = \{1\}$ is clearly a group under multiplication of order $2-1=1$. Now consider any prime $p > 2$, which must be odd. $p = 2k+1$ for some $k \in \mathbb{Z}^+$. Observe.

$\langle 2 \rangle_p^* = \{2,4,\ldots,2k\} \sqcup \{2(2k),\ldots\}$. Well, since $p = 2k+1$, $2(2k) = 4k = 2k+2k = (2k+1)+(2k-1) = p+2k-1 = 2k-1 = p-2$. So note that the elements following $2k$ must be odd since p is odd. Additionally, $2q(p-2) = -4q = p-4q$ for $q = 1,\ldots,k-1$ and finally note that $2(k-1)(p-2) = 2(k-1)p - 2(k-1)(2) = p-2k = 1$. Therefore,

$\langle 2 \rangle_p^* = \{2,4,\ldots,2k\} \sqcup \{2(2k),\ldots\} = \{2,4,\ldots,2k\} \sqcup \{p-2, p-4\ldots, p-2k,\ldots\} = \{2,4,\ldots,p-1\} \sqcup \{p-2, p-4,\ldots,1,2,\ldots\}$ and continuing in this fashion loops us back around to the evens.

So, $\langle 2 \rangle_p^* = (\mathcal{E}_p \setminus \{0\}) \sqcup (\mathcal{O}_p) = \mathbb{Z}_p^*$ must therefore be a cyclic multiplicative group of order $p-1$.

$\square$

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.

$(\mathbf{a})$: Recall that two functions are equal if they share the same domain, codomain, and if they map each element from the domain to the same element in the codomain. Also let $e : G \to G$ denote the identity mapping $e := e(x) = x, \forall x \in G$. Observe. $\forall f, g, h \in \mathrm{Aut}(G),$ and all x

$[\mathbf{e}]$: $(e \circ f)(x) = e(f(x)) = f(x) = f(e(x)) = (f \circ e)(x).$

[Associativity]: $(f \circ (g \circ h))(x) = f((g \circ h)(x)) = f(g(h(x))) = (f \circ g)(h(x)) = (f \circ (g \circ h))(x).$

[Inverses]: Since f is a bijection, it has an inverse function f^{-1} such that$(f \circ f^{-1})(x) = (f^{-1} \circ f)(x).$

We simply show that this bijection is a group homomorphism. For any $\alpha, \beta \in G, \exists a, b \in G$ such that

$f(a) = \alpha$ and $f(b) = \beta$ and $f(ab) = f(a)f(b) = \alpha\beta,$ since f is a group automorphism. Therefore,

since $f^{-1}(\alpha) = a, f^{-1}(\beta) = b,$ and $f^{-1}(\alpha\beta) = ab,$ we have$f^{-1}(\alpha\beta) = (f^{-1}(\alpha))(f^{-1}(\beta)) = ab = e(ab).$

So in fact the bijective inverse of any automorphism in $\mathrm{Aut}(G)$ is also an automorphism in $\mathrm{Aut}(G)$.

So $\mathrm{Aut}(G)$ is a group under function composition.

$\square$

We now prove a lemma about automorphisms of cyclic groups on the next page before proving (b).

Lemma.

1. *If G is a cyclic group generated by g, then an endomorphism $\phi \in \mathrm{Aut}(G)$ if and only if $\phi(g)$ is a generator of G.*
2. *The set of all endomorphisms of $\mathbb{Z}_n$ is $\mathrm{End}(\mathbb{Z}_n) = \{\phi_m := m(x) = \sum_{i=1}^{m} x \mid m \in \mathbb{Z}_n,\ \phi_m : \mathbb{Z}_n \to \mathbb{Z}_n\}$.*
3. *An endomorphism of $\mathbb{Z}_n$ is in $\mathrm{Aut}(\mathbb{Z}_n)$ if and only if it is of the form $\phi_k(x) = kx = \sum_{i=1}^{k} x$ where $\gcd(n,k) = 1$.*

Proof.
If $\phi \in \mathrm{Aut}(G)$, then

$$G = \phi(G) = \phi(\langle g \rangle) = \phi(\{g^i \mid i \in \mathbb{Z}\}) = \{\phi(g^i) \mid i \in \mathbb{Z}\} = \{(\phi(g))^i \mid i \in \mathbb{Z}\} = \langle \phi(g) \rangle.$$

On the other hand, if ϕ is an endomorphism such that $\phi(g)$ is a generator of G such that $x = g^k$ and $y = g^c$, then $\phi(x) = \phi(y) \implies \phi(g^k) = \phi((g)^c) \implies (\phi(g))^k = (\phi(g))^c \implies (\phi(g))^k(\phi(g))^{-c} = e \implies \phi(g^k)\phi(g^{-c}) = e \implies \phi(g^k g^{-c}) = e \implies xy^{-1} = e \implies x = y$. Next, for any $\alpha \in G$, $\alpha = (\phi(g))^m$ for some integer m since $\phi(g)$ is a generator of G. So then $\phi(g^m) = \alpha$. So $\phi \in \mathrm{Aut}(G)$. So we have proven 1. and move onto 2.

Throughout, we denote $\sum_{i=1}^{m} x = m(x)$ to make things cleaner. Any endomorphism of $\mathbb{Z}_n$ must abide by $\phi(xy) = \phi(x)\phi(y)$ by definition. Therefore, since 1 generates $\mathbb{Z}_n$, any $x \in \mathbb{Z}_n$ is of the form $x(1)$. So then if ϕ is an endomorphism of $\mathbb{Z}_n$, $\phi(x) = \phi(x(1)) = x(\phi(1))$, and is uniquely determined by $\phi(1)$, for which there are n total options, since the codomain of ϕ is G. More specifically, $1 \mapsto \mathbb{Z}_n$ gives us that

$$\mathrm{End}(\mathbb{Z}_n) = \{\phi(1)(x) \mid \phi(1) \in \mathbb{Z}_n\} = \{mx \mid m \in \mathbb{Z}_n\}.$$

We move onto 3. By 1., any endomorphism is an automorphism of $\mathbb{Z}_n = \langle 1 \rangle$ if and only if $\phi(1)$ generates G. Consider some automorphism ϕ_k such that $\phi_k(1) = k$. Well, any $x \in \mathbb{Z}_n$ is of the form $x = x(1) = \sum_{i=1}^{x} 1$. So then $\phi_k(x) = \phi_k(x(1)) = x(\phi(1)) = xk = kx$. Since k generates $\mathbb{Z}_n$, we know that $|k| = n$. So then since $1 \leq k < n$, we know that $\mathrm{lcm}(n,k) = n(k)$, otherwise there exists some $m(k) = n$ where $m < n$, and $|k| = m < n$, a contradiction. Therefore, $nk = \mathrm{lcm}(n,k) = \frac{nk}{\gcd(n,k)} \implies \gcd(n,k)$.

On the other hand, if $\phi_k = kx$ is an endomorphism of $\mathbb{Z}_n$ and $\gcd(n,k) = 1$, then $|k| = \mathrm{lcm}(n,k) = \frac{nk}{\gcd(n,k)} = n(k)$ and so $|k| = n$. Therefore, since ϕ_k is an endomorphism such that $\phi(1) = k$ generates $\mathbb{Z}_n = \langle 1 \rangle$, by 1., $\phi_k \in \mathrm{Aut}(\mathbb{Z}_n)$.

So we have proven all statements.

□

We now prove (b) on the next page.

Proof. We prove all but $\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_{p-1}$, which is found on the next page.

Trivially, $1, -1$ both generate $\mathbb{Z}$. However, any $n \in \mathbb{N}$ with $n > 1$ is such that

$$\langle n \rangle = \langle -n \rangle = \{\ldots, -2n, -n, 0, n, 2n, \ldots\} = n\mathbb{Z} \neq \mathbb{Z}$$

since any non-zero integer k with $|k| < n$ doesn't belong to $n\mathbb{Z}$. Trivially, since $|0| = 1$ it can't generate $\mathbb{Z}$. So then $-1, 1$ are the only generators of $\mathbb{Z}$ and $\mathrm{Aut}(G) = \{\phi_1, \phi_{-1}\}$. Notice that $\phi_1(x) = x(\phi(1)) = x$. So ϕ_1 is actually the identity automorphism. Therefore, since the identity is unique, ϕ_{-1} must have order 2 and $\mathrm{Aut}(\mathbb{Z})$ must be cyclic which means $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$

.

By our **Lemma**, The set of all endomorphisms of $\mathbb{Z}_n$ is

$$\mathrm{End}(\mathbb{Z}_n) = \{\phi_m := m(x) = \sum_{i=1}^{m} x \mid m \in \mathbb{Z}_n,\, \phi_m : \mathbb{Z}_n \to \mathbb{Z}_n\}.$$
$$\implies \mathrm{Aut}(\mathbb{Z}_n) = \{\mathrm{End}(\mathbb{Z}_n) \ni \phi_k := x \mapsto kx \mid \gcd(n,k) = 1\}.$$

We use this result for the remainder of the problem. Since $0, 1, 2, 3, 4$ all share divisors greater than 1 with 6, they cannot give us an endomorphism in $\mathrm{Aut}(\mathbb{Z}_6)$. So, $\mathrm{Aut}(\mathbb{Z}_6) = \{\phi_1, \phi_5\}$. Then, since $\phi_1(x) = x$ it's the identity, and by definition the only element in the group of order 1. So ϕ_5 must have order 2 and $\mathrm{Aut}(\mathbb{Z}_6) \cong \mathbb{Z}_2$.

Notice that since all of these automorphisms are defined via addition, which is commutative that the isomorphisms themselves are commutative under composition: $\phi_a \circ \phi_b(x) = \phi_a(\phi_b(x)) = \phi_a(b(x)) = abx = bax = \phi_b(\phi_a(x)) = (\phi_b \circ \phi_a)(x)$. Now once again, $1, 2, 4, 6, 8$ all share non-trivial divisors with 8, and so $\mathrm{Aut}(\mathbb{Z}_8) = \{\phi_1, \phi_3, \phi_5, \phi_7\}$. Finally, $(\phi_3 \circ \phi_3)(x) = 9x = x = 25x = (\phi_5 \circ \phi_5)(x)$. So then $\langle \phi_3 \rangle, \langle \phi_5 \rangle$ are both subgroups of order 2, and therefore since this is a non-cyclic abelian group it must be isomorphic to $\mathbb{Z}_2 \oplus \mathbb{Z}_2$ by the fundamental theorem of finite Abelian groups. $\square$

We complete (b) here.

Proof. By our lemma,

$$\mathrm{Aut}(\mathbb{Z}_n) = \{\mathrm{End}(\mathbb{Z}_n) \ni \phi_k := x \mapsto kx \mid \gcd(n,k) = 1\}.$$

Well, all elements in $x \in \mathbb{Z}_p$ where p is prime have $\gcd(x, p) = 1$, except 0. So then

$$\mathrm{Aut}(\mathbb{Z}_p) = \{\phi_i \mid i \in \mathbb{Z}_p^*\}.$$

Recall that we proved that automorphisms of cyclic groups are Abelian under composition of functions. Also notice that the composition of two automorphisms of this group exactly corresponds with the product of two units in $\mathbb{Z}_p^* \equiv \mathbb{Z}_{p-1}$; $(\phi_a \circ \phi_b)(x) = a(b(x)) = ab(x) = \phi_{ab}x$ and we know that this is a group and therefore $\phi_{ab} \in \mathrm{Aut}(\mathbb{Z}_p)$. Well then we just define the trivial isomorphism $\phi_x \mapsto x \in \mathbb{Z}_p^*$. To cover our bases, we show that $f : \mathrm{Aut}(\mathbb{Z}_p) \to \mathbb{Z}_p^*$ is an isomorphism briefly:

$[Injective]: \ f(\phi_x) = f(\phi_y) \implies x = y \in \mathbb{Z}_p \implies \phi_x = \phi_y$

$[Surjective]: \ \forall x \in \mathbb{Z}_p^*, \exists \phi_x \in \mathrm{Aut}(\mathbb{Z}_p)$ such that $f(\phi_x) = x$ by our lemma, since units mod n are exactly all elements in $\mathbb{Z}_n$ coprime with n.

$[Homomorphic]: \ $ As established previously, $f(\phi_{ab}) = f(\phi_a)f(\phi_b) = ab,$ essentially by definition.

Refer to problem 1 for the isomorphism from $\mathbb{Z}_p$ to $\mathbb{Z}_{p-1}$. We simply show that 2 generates all of $\mathbb{Z}_p^*$ for $p \geq 3$. If $p = 2$, $\mathbb{Z}_p^*$ is the trivial group, which is trivially cyclic.

Thus,

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

$\square$

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.

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

$$B^2 = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \implies B^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I \tag{2}$$

$$AB = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \tag{3}$$

$$(AB)^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \tag{4}$$

Above, by (1) and (2), we see A and B have finite order. Now consider non-trivial powers $n \geq 2$ of (AB).

It is shown in (4) that $(AB)^2 = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$. Now suppose $(AB)^k = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix}$ for some $k \geq 2$. Then we have:

$$(AB)^{k+1} = (AB)(AB)^k = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & k+1 \\ 0 & 1 \end{pmatrix}.$$

So we see that $(AB)^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$ for all $n \geq 2$ and so in fact it holds for all $n \in \mathbb{N}$ when combined with (3) and the fact that $(AB)^0 = I$. So by definition, AB has infinite order since $(AB)^k \neq I$ for all $k \in \mathbb{Z}^+$.

Thus,

$$A \text{ and } B \text{ have finite order but } AB \text{ has infinite order.}$$

$\square$

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 $(H\cap K) \le H,K \le G$.

[1-Step]: $\forall a,b \in (H\cap K)$, $ab^{-1}\in H$ and $ab^{-1}\in K \implies ab^{-1}\in (H\cap K) \implies (H\cap K)\le H,K\le G$.

Since $(H\cap K)\le H,K\le G$, 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.

$(H_K \subseteq G/K) \iff (|H_k|\le [G:K])$ and then $(|H_k|\le [G:K])$ 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,

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

$\square$

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 $kN = h_k N$ 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.

□

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,

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

□

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

$$|HK| = \frac{|H||K|}{|H \cap K|} \leq |G| \tag{5}$$

$$[G : H] = \frac{|G|}{|H|} \tag{6}$$

$$[G : K] = \frac{|G|}{|K|} \tag{7}$$

$$\implies [G : H][G : K] = \frac{|G|^2}{|H||K|} \tag{8}$$

$$[G : H \cap K] = \frac{|G|}{|H \cap K|} \tag{9}$$

Observe.

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

$\square$

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,

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

$\square$