Submit the following from the problem list: 2, 3, 5, 6, 8, 10, 11, 12, 13, 16, 23.

Submit two of the following : 19, 20, 21, 22, 24.

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) $\mathbb{Q}/\mathbb{Z} = \{[\frac{a}{b}] = \frac{a}{b} + \mathbb{Z} \mid a, b \in \mathbb{Z} \text{ and } b \nmid a\}$. Consider any $q_1, q_2 \in (0,1)$. If $[q_1] = [q_2]$, then $[q_1] - [q_2] = \mathbb{Z}$ and so $q_1 - q_1 \in \mathbb{Z}$. Well, $q_1, q_2 \in (0,1)$, so $q_1 - q_2 \in (-1, 1)$ and therefore $q_1 - q_2 = 0$. 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

$$q_1 = q_2 \iff [q_1] = [q_2], \forall q_1, q_2 \in (0,1).$$

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 $q \in (0,1)$. 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 $\mathbb{Q}/\mathbb{Z}$:

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

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 some integers $i, j \geq 0$ and $a_i, a_j \in \mathbb{Z}$.

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

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

So $\mathbb{Z}(p^\infty) \leq \mathbb{Q}/\mathbb{Z}$. Now once more consider some integers $i, j \in \mathbb{Z}^+$ but set $a = 1$. Notice that $\frac{1}{p^i}, \frac{1}{p^j} \in (0,1)$.

<u>Observe.</u>

This result essentially follows from **Problem 2**. $[\frac{1}{p^i}] = [\frac{1}{p^j}] \implies [\frac{1}{p^i}] - [\frac{1}{p^j}] = \mathbb{Z} \implies \frac{1}{p^i} - \frac{1}{p^j} \in \mathbb{Z}$. Well, $\frac{1}{p^i}, \frac{1}{p^j} \in (0,1) \implies \frac{1}{p^i} - \frac{1}{p^j} \in (-1,1) \implies \frac{1}{p^i} - \frac{1}{p^j} = 0 \implies \frac{1}{p^i} = \frac{1}{p^i} \implies i = j$. On the other hand, $i = j \implies \frac{1}{p^i} = \frac{1}{p^j} \implies [\frac{1}{p^i}] = [\frac{1}{p^j}]$ by definition. So then,

$$i = j \iff [\frac{1}{p^i}] = [\frac{1}{p^j}],\ \forall i, j \in \mathbb{Z}^+.$$

There are infinitely many distinct positive integers so there must be infinitely many distinct cosets in $\mathbb{Z}(p^\infty)$.

Thus,

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

$\square$

Problem 4. If G is a finite group of even order, prove that G has an element of order two.

Proof. If G is a finite group of even order, then $|G| = 2k$ and $|G \setminus \{e\}| = 2k-1$ for some $k \in \mathbb{Z}^+$. Suppose there doesn't exist an element of order 2 in G. Then, $\forall g \in G \setminus e$, $g \neq g^{-1}$. **Observe.**

If all non-identity elements are not equal to their inverse, then non-identity elements come two at a time. But then $|G \setminus \{e\}| = 2k-1$ is even, a contradiction.

Thus,

If G is a finite group of even order, then it contains an element of order 2.

□

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. Well, □

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).

Problem 7. Let G be an infinite group that is isomorphic to each of its proper subgroups. Prove that $G \cong \mathbb{Z}$.

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.

Problem 9. Let G be an abelian group containing elements a and b of orders m and n, respectively. Prove that G contains an element of order $\text{lcm}(m,n)$.

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 $HK = KH \implies \forall hk \in HK, \exists (h_{k_1}, k_{h_1}) \in H \times K,$ such that $hk = k_{h_1}h_{k_1} \in KH = HK$. 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. By **Class notes - 08/29** we have that $|G| = [G:M]|M| \implies [G:M] = \frac{|G|}{|M|}$ for all $M \leq G$. Therefore, we have that $[G:H] = \frac{|G|}{|H|} = n$, $[G:K] = \frac{|G|}{|K|} = m$ where $gcd(m,n) = 1$. **Observe.**

If G is finite, so are H and K. So, $|G| = |H|n = |K|m \implies |H| = \frac{m|K|}{n}$. Since $n \nmid m$, n must divide $|K|$. Similarly, $|G| = |H|n = |K|m \implies |H| = \frac{n|K|}{m}$. So m divides $|H|$ by the same logic. Therefore, $|K| = nx$ and $|H| = my$ for some $x, y \in \mathbb{Z}^+$. $\square$

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

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 $H = K$.

Problem 14. Let H be a subgroup of G. For $a \in G$, prove that aHa^{-1} is a subgroup of G that is isomorphic to H.

Problem 15. Let G be a finite group and H a subgroup of G of order n. If H is the only subgroup of G of order n, prove that H is normal in G.

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

Problem 17. What is $Z(S_n)$ for $n \geq 2$?

Problem 18. If H is a normal subgroup of G such that H and G/H are finitely generated, then G is finitely generated.

Problem 19. If N is a normal subgroup of G, $[G:N]$ is finite, H is a subgroup of G, $|H|$ is finite, and $[G:N]$ and $|H|$ are relatively prime, then H is a subgroup of N.

Problem 20. If N is a normal subgroup of G, $|N|$ is finite, H is a subgroup of G, $[G:H]$ is finite, and $[G:H]$ and $|N|$ are relatively prime, then N is a subgroup of H.

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

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

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

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

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 $K \subseteq H$.

Problem 24. Let G be an abelian group, H a subgroup of G such that G/H is an infinite cyclic group. Prove that $G \cong H \times G/H$.