Some Problems.

1. G is a commutative group and $a \in G$, $b \in G$ with $o(a) = m$ and $o(b) = n$. Show that $\exists$ an element $c \in G$ such that $o(c) = [m,n]$ where $[m,n]$ is the l.c.m of m, n.

Proof: Case 1. Let $\gcd(m,n) = 1$ Then $[m,n] = mn$. As G is commutative and $\gcd(m,n) = 1$ then $o(ab) = o(a) \cdot o(b) = mn$

So $\exists\ c = ab$ such that $o(c) = [m,n]$

Case 2 Let $\gcd(m,n) > 1$

Let $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} p_{k+1}^{\alpha_{k+1}} \cdots p_r^{\alpha_r}$ and $n = p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k} p_{k+1}^{\beta_{k+1}} \cdots p_r^{\beta_r}$

where $p_1, p_2, \ldots p_r$ are prime numbers and $\alpha_1, \alpha_2, \ldots \alpha_r$ and $\beta_1, \beta_2, \ldots \beta_r$ are non-negative integral powers of $p_1, \ldots, p_r$ in m and n such that $0 \le \beta_1 \le \alpha_1, 0 \le \beta_2 \le \alpha_2, \ldots 0 \le \beta_k \le \alpha_k$ and

$0 \le \alpha_{k+1} < \beta_{k+1}, 0 \le \alpha_{k+2} < \beta_{k+2}, \ldots, 0 \le \alpha_r < \beta_r$

So, $[m,n] = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} p_{k+1}^{\beta_{k+1}} \cdots p_r^{\beta_r}$

Let $p = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, $q = p_{k+1}^{\beta_{k+1}} \cdots p_r^{\beta_r}$

Then $\gcd(p,q) = 1$ and $pq = [m,n]$

Let $u = a^{p_{k+1}^{\beta_{k+1}} p_{k+2}^{\beta_{k+2}} \cdots p_r^{\beta_r}}$, $v = b^{p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}}$. Then $u, v \in G$.

and $o(u) = \dfrac{m}{\gcd(m, p_{k+1}^{\beta_{k+1}} \cdots p_r^{\beta_r})} = \dfrac{m}{p_{k+1}^{\alpha_{k+1}} \cdots p_r^{\alpha_r}} = p$

and $o(v) = \dfrac{n}{\gcd(n, p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k})} = \dfrac{n}{p_1^{\beta_1} p_2^{\beta_2} \cdots p_k^{\beta_k}} = q$

$o(u)$ and $o(v)$ are relatively prime and G is commutative

So, $o(uv) = pq = [m,n]$. So Here $c = uv$ is such that

$o(c) = [m,n]$

2. Give an example of a proper commutative sub-group of a non-commutative group.

Solution: S_3 is a non-commutative group. A_3 is a proper commutative subgroup of S_3.

---

8. Definition: In a finite group G, each element is of finite order. The highest possible order of an element in G is called the exponent of G.

Examples 1. S_3 has exponent 3

2. Klein's 4-group has exponent 2

3. $(\mathbb{Z}_6, +)$ has exponent 6.

Problem 4 Prove that the order of every element of a finite abelian group is a divisor of the exponent of G.

Proof: Let the exponent of G be n. Let $a \in G$ and $o(a) = m$. Then $m \leq n$. If m is not a divisor of n then the l.c.m of m, n is greater than n. Since G is a commutative group, $\exists$ an element c in G such $o(c) =$ l.c.m of m, n. This implies $o(c) > n$, a contradiction. So m is a divisor of n.

Note: The order of an element of a finite non-abelian group G may not be a divisor of the exponent of G. Consider the group S_3. It is non-abelian and its exponent is 3 and $o((23)) = 2$ and 2 is not a divisor of 3.

Problem 5 Let G be a finite abelian group in which the number of solutions in G of the equation $x^n = e$ is at most n for every positive integer n, e is the identity element in G. Prove that G is cyclic.

Proof: Let $o(G) = m$ and let m_1 be the exponent of G.

Then $m_1 \leq m$ —(i)

As m_1 is the exponent of G, the order of every element of G is a divisor of m_1. So, for each $x \in G$, $x^{m_1} = e$ as if $o(x) = k$, then $m_1 = k.d$ for some positive integer d

So, $x^{m_1} = x^{kd} = (x^k)^d = e^d = e$

So, every $x \in G$ is a solution of $x^{m_1} = e$. As by the given condition, $x^{m_1} = e$ has at most m_1 solution,

So $m \leq m_1$ ---(ii). So, by (i) & (ii), $m = m_1$

As m_1 is the exponent, $\exists\ c \in G$ s.t $o(c) = m_1 = m = o(G)$. As $\exists$ an element $c \in G$ s.t $o(c) = o(G)$, G is cyclic.

Problem 6 Prove that all proper subgroups of order 6 are commutative.

Proof: As order of the subgroup divides the order of the group, so the proper subgroup of this group of order 6 may of order 1, 2, 3 and 4. As every group of order less than 6 are commutative. So, all the proper subgroups would be commutative.

Problem 7 Prove that a group of order 27 must have a subgroup of order 3.

Proof: Let G be a group of order 27.

Case 1 Let G be cyclic. Then $G = \langle a \rangle$ and $o(a) = 27$

or now $o(a^9) = \frac{27}{\gcd(9,27)} = 3$ So $\langle a^9 \rangle$ is the required cyclic subgroup.

Case 2. G is not cyclic. As order of each element

is a divisor of the order of the group. So, order the elements of G it may be 1, 3, 9 and 9. Since G is not cyclic $\exists$ no element of order 27. Identity element is the only element of order 1. So all the other non-identity element has either order 3 or 9. If $\exists$ an element a such that $o(a) = 3$ then $\langle a \rangle$ is the required subgroup of G. If $\exists$ no element of order 3, then each non-identity element a has order 9. Let $a \in G$ and $o(a) = 9$

Then $o(a^3) = \frac{9}{\gcd(3,9)} = \frac{9}{3} = 3$. So, it is not possible, that all non-identity element has order 9, So, $\exists$ always an element a of order 3 and $\langle a \rangle$ is the required subgroup.

Problem 7 Give an example of an infinite group in which every element is of finite order.

Solution: Let $(\mathbb{Q}, +)$ and $(\mathbb{Z}, +)$ be the groups of rationals and integers under addition. Then the quotient group

$\mathbb{Q}/\mathbb{Z} = \left\{ \mathbb{Z} + \frac{m}{n} : \frac{m}{n} \in \mathbb{Q} \right\}$ is an infinite group

Consider any member $\mathbb{Z} + \frac{m}{n}$ of $\mathbb{Q}/\mathbb{Z}$, $n > 0$ as every rational can be written as $\frac{m}{n}$ where $m \in \mathbb{Z}$ and $n > 0$. Now $n\left(\mathbb{Z} + \frac{m}{n}\right) = \mathbb{Z} + n \cdot \frac{m}{n} = \mathbb{Z} + m = \mathbb{Z}$ = zero of $\mathbb{Q}/\mathbb{Z}$

So we find $\mathbb{Z} + \frac{m}{n}$ has order $\leq n$. So, every element of $\mathbb{Q}/\mathbb{Z}$ is of finite order.

Problem 8 Find all the homomorphism from $\mathbb{Z}_{20}$ to $\mathbb{Z}_8$. How many of these are onto?

Solution Let $f : \mathbb{Z}_{20} \to \mathbb{Z}_8$ be any homomorphism.

Suppose $f(\bar{1}) = a$, then for any $\bar{x} \in \mathbb{Z}_{20}$

$$f(\bar{x}) = f(\underbrace{\bar{1}+\bar{1}+\cdots+\bar{1}}_{x \text{ times}}) = x f(\bar{1}) = xa$$

i.e., all homomorphism are determined if we know a

Since $a \in \mathbb{Z}_8$ $\quad o(a)$ divides $o(\mathbb{Z}_8) = 8$

Again as f is a homomorphism $o(f(\bar{1}))$ divides $o(\bar{1}) = 20$

So, $o(x)$ divides 20 also.

Hence possible values of $o(a)$ are $1, 2, 4$

Now if $o(a) = 1$ then a is the identity in $\mathbb{Z}_8$

i.e $\quad a = \bar{0}$

If $o(a) = 2$, then $2a = \bar{0} \Rightarrow a = \bar{4}$ as $\bar{4} + \bar{4} = \bar{0}$

If $o(a) = 4$ then $4a = \bar{0} \Rightarrow a = \bar{2}$ as $\bar{2}+\bar{2}+\bar{2}+\bar{2} = \bar{0}$

or, $a = \bar{6}$ as $\bar{6}+\bar{6}+\bar{6}+\bar{6} = \bar{0}$

Hence possible values of a is $\bar{0}, \bar{4}, \bar{2}, \bar{6}$

Hence $\exists$ 4 homomorphisms from $\mathbb{Z}_{20}$ to $\mathbb{Z}_8$

If $f: \mathbb{Z}_{20} \to \mathbb{Z}_8$ is an onto homomorphism, then by fundamental Theorem (first Isomorphism Theorem) $\mathbb{Z}_8 \simeq \frac{\mathbb{Z}_{20}}{\ker f} \Rightarrow o(\mathbb{Z}_8) = \frac{o(\mathbb{Z}_{20})}{o(\ker f)}$

$\Rightarrow o(\ker f) = \frac{20}{8} = \frac{5}{2}$ which is impossible. Hence $\exists$ no onto homomorphism.

Problem Prove that if $G/H \simeq G/K$ and G is cyclic then $H = K$

Solution: Let $G = \langle a \rangle$ and suppose $H = \langle a^n \rangle$ and $K = \langle a^m \rangle$. Then n is the smallest positive integer such that $a^n \in H$. So, $H, Ha, \ldots Ha^{n-1}$ are distinct right cosets of H in G. So $[G:H] = n$ Similarly $[G:K] = m$ Now $G/H \simeq G/K \Rightarrow [G:H] = [G:K] \Rightarrow m = n$

So, $\quad H = K$.