Section 6
Homework Assignment

#12. Find the number of automorphisms of the group $\mathbb{Z}_2$.

<u>Answer</u>: a general fact is that an isomorphism φ between two cyclic groups G and G' is determined by the image of any generator of G. Namely, if $\varphi: G = \langle g \rangle \longrightarrow G'$ is an isomorphism then φ is determined by $\varphi(g)$. Indeed if $x = g^n$ then $\varphi(x) = [\varphi(g)]^n$. <u>Note</u> that $\varphi(g)$ must be a generator of G'.

In the case of $\mathbb{Z}_2$ there is only one generator: $\bar{1}$. Thus there is only one automorphism of $\mathbb{Z}_2$

#13 Find the number of automorphisms of the group $\mathbb{Z}_6$.

<u>Ans</u>: In this case $\bar{1}$ and $\bar{5}$ are the only generators of $\mathbb{Z}_6$. Thus we have two distinct automorphisms: φ_1 and φ_2 defined by

$\varphi_1(\bar{1}) = \bar{1}$ and $\varphi_2(\bar{1}) = \bar{5}$.

#14. Find the number of automorphisms of the group $\mathbb{Z}_8$.

<u>Ans.</u>: In this case $\bar{1}, \bar{3}, \bar{5}$, and $\bar{7}$ are the only generators of $\mathbb{Z}_8$. Thus we have four distinct automorphisms: $\varphi_1, \varphi_2, \varphi_3, \varphi_4$ defined by

$\varphi_1(\bar{1}) = \bar{1}$ $\quad\varphi_2(\bar{1}) = \bar{3}$ $\quad\varphi_3(\bar{1}) = \bar{5}$

$\varphi_4(\bar{1}) = \bar{7}$.

#19. Find the number of elements of the cyclic subgroup $\langle i \rangle$ of the group $\mathbb{C}^*$ of non-zero complex numbers under multiplication.

<u>Ans</u>: $\langle i \rangle = \{1, i, i^2 = -1, i^3 = -i\}$

Thus $|\langle i \rangle| = 4 =$ order of i.

#15. Find the number of automorphisms of the group $\mathbb{Z}$.

<u>Ans</u>: In this case 1 and -1 are the only generators of $\mathbb{Z}$. Thus we have two distinct automorphisms: φ_1 and φ_2 defined by

$\varphi_1(1) = 1$ and $\varphi_2(1) = -1$

#16. Find the number of automorphisms of the group $\mathbb{Z}_{12}$.

Ans: In this case $\bar{1}, \bar{5}, \bar{7}, \overline{11}$ are the only generators of $\mathbb{Z}_{12}$. Thus we have two distinct automorphisms: $\varphi_1, \varphi_2, \varphi_3, \varphi_4$ defined by

$\varphi_1(\bar{1}) = \bar{1}$ $\quad \varphi_2(\bar{1}) = \bar{5}$ $\quad \varphi_3(\bar{1}) = \bar{7}$

$\varphi_4(\bar{1}) = \overline{11}$.

#33. Either give an example of a finite group that is not cyclic, or explain why no example exists.

Ans: The Klein 4-group $\cong \mathbb{Z}_2 \times \mathbb{Z}_2 \cong$ units of $\mathbb{Z}_8$ under multiplication.

#34. Either give an example of an infinite group that is not cyclic, or explain why no example exists.

Ans: For example, $(\mathbb{R}, +)$ is not cyclic.

#37. Either give an example of a finite cyclic group having four generators, or explain why no example exists.

Ans: For example $\mathbb{Z}_8$, which has $\bar{1}, \bar{3}, \bar{5}, \bar{7}$ as generators.

#45. Let r, s be positive integers. Show that $\{nr + ms \mid n, m \in \mathbb{Z}\}$ is a subgroup of $\mathbb{Z}$.

Ans: The equation $(n_1 r + m_1 s) + (n_2 r + m_2 s) = (n_1 + n_2) r + (m_1 + m_2) s$ shows that the set is closed under addition.
Because $0r + 0s = 0$, we see that 0 is in the set. Because $[(-n) r + (-m) s] + [nr + ms] = 0$, we see that the set contains the inverse ($\equiv$ opposite) of each element.
Thus it is a subgroup of $\mathbb{Z}$. Note:

$$\{nr + ms \mid n, m \in \mathbb{Z}\} = d\mathbb{Z}$$

when $d = \gcd(r, s)$. ▩

#46 Let a and b be elements of a group G. Show that if ab has finite order n, then ba has also order n.

Ans: Let n be the order of ab so that

$$(ab)^n = e.$$

Multiplying this equation on the left by b and on the right by a, we find that

$$b\,(ab)^n a = (ba)^{n+1} = b\,e\,a = b\,a\,.$$

Cancellation of the first factor ba from both sides shows that $(ba)^n = e$, so the order of ba is $\leq n$.
If the order of ba were less than n, a symmetric argument would show that the order of ab is less than n, contrary to our choice of n.
Thus ba has order n also. ∎

\# 47 Let r and s be positive integers.

(a.) Define the least common multiple of r and s as a generator of a certain cyclic group.

(b.) Under what conditions is the least common multiple of r and s their product, rs?

(c.) Generalizing part (b.), show that the product of the greatest common divisor and of the least common multiple of r and s is rs.

Ans: (a.) As a subgroup of the cyclic group $(\mathbb{Z}, +)$, the subgroup

$G = r\mathbb{Z} \cap s\mathbb{Z}$ is cyclic. The positive generator of G is the <u>least common multiple</u> of r and s.

(b.) The least common multiple of r and s is rs if and only if r and s are relative prime, so that they have no common prime factor.

(c.) Let $d = ur + vs$ be the gcd of r and s, where $u, v \in \mathbb{Z}$. Write $m = kr = qs$ be the lcm of r and s. Then

$$md = mur + mvs = (qs)ur + (kr)vs$$
$$= (qu + kv)rs,$$

so rs is a divisor of md.

Now, let $r = \alpha d$ and let $s = \beta d$. Then:

$$rs = (\alpha d)(\beta d) = (\alpha\beta d)\, d,$$

and $\alpha\beta d = \beta r = \alpha s$ is a multiple of r and s, and hence

$$\alpha\beta d = m \cdot t \qquad \text{for } t \in \mathbb{Z}.$$

Thus $rs = (mt)d = (md)t$, so

md is a divisor of rs.

Hence $\boxed{md = rs.}$ ∎

#49. Show by a counterexample that the following "converse" of Theorem 6.6. is not a theorem:

"If a group G is such that every proper subgroup is cyclic, then G is cyclic."

<u>Ans</u>: The Klein 4-group V is a counterexample.

The group S_3 is also a counterexample

#50. Let G be a group and suppose $a \in G$ generates a cyclic subgroup of order 2 and is the <u>unique</u> such element. Show that $ax = xa$ for all $x \in G$.

<u>Ans</u>: Note that $xax^{-1} \neq e$ because

$$xax^{-1} = e \Longrightarrow a = e,$$

and we are given that a has order 2.

We have that:

$$(xax^{-1})^2 = (xax^{-1})(xax^{-1}) = xa^2x^{-1} =$$

$$= xex^{-1} = e$$

$\therefore$ xax^{-1} has order 2.

Because a is given to be the unique element of G of order 2, we see that

$$xax^{-1} = a \quad \text{for all } x \in G.$$

Thus $xa = ax$ for all $x \in G$. ∎

#51. Let p and q be distinct prime numbers. Find the number of generators of the cyclic group $\mathbb{Z}_{pq}$.

Answer: The positive integers less than pq and relatively prime to pq are those that are not multiples of p and are not multiples of q. There are $p-1$ multiples of q and $q-1$ multiples of p that are less than pq. Thus there are

$$(pq-1) - (p-1) - (q-1) = (p-1)(q-1)$$

positive integers less than pq and relatively prime to pq.