Some more Exercises (some worked out and some given as exercises to do)

1. Show That ~~cancellation~~ cancellation Laws may hold in a semigroup (Let $*$ be a binary operation on a non-empty set G. Then $(G, *)$ is said to be a semi-group if $*$ is associative.)

Proof: Consider G be the set of all 2×2 matrices over integers under matrix multiplication. It forms a semigroup.

Let $A = \begin{bmatrix} 2 & 0 \\ 0 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 0 & 0 \\ 0 & 5 \end{bmatrix}$ and $C = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}$

then $AB = AC = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}$ but $B \neq C$

2. If G is a group such that $(ab)^k = a^k b^k$ for three ~~consec~~ consecutive integers k, then show that G is abelian

Proof. Let $a, b \in G$. Let $n, n+1, n+2$ be the three consecutive integers such that $(ab)^n = a^n b^n$, $(ab)^{n+1} = a^{n+1} b^{n+1}$ and $(ab)^{n+2} = a^{n+2} b^{n+2}$

Now $(ab)^{n+1} = (ab)^n (ab) = (a^n b^n)(ab)$ $(\because (ab)^n = a^n b^n)$

or, $a^{n+1} b^{n+1} = a^n b^n ab$ $(\because (ab)^{n+1} = a^{n+1} b^{n+1})$

or, $ab^n = b^n a$ (by Cancellation Law) ——(1)

Again, $(ab)^{n+2} = (ab)^{n+1}(ab) = a^{n+1} b^{n+1}(ab)$ $[\because (ab)^{n+1} = a^{n+1} b^{n+1}]$

or, $a^{n+2} b^{n+2} = a^{n+1} b^{n+1} ab$ $[\because (ab)^{n+2} = a^{n+2} b^{n+2}]$

or, $ab^{n+1} = b^{n+1} a$ (by cancellation law) --- (2)

So, from (1) and (2), we have

~~$a b^{n+1} = ab^n b = b^n ab = b^n a b = a b^{n+1}$~~

Again, $b^{n+1} a = b b^n a = bab^n$

So, $bab^n = ab^{n+1} \Rightarrow ba = ab$ (by cancellation Law)

3. Let G be a group and suppose there exist two integers m and n which are relatively prime and $a^m b^m = b^m a^m$ and $a^n b^n = b^n a^n$ for all $a, b \in G$. Show that G is abelian.

Proof: Let $a, b \in G$. Now, There exist integers x and y such that $xm + yn = 1$. So,

$$a^m b^n = \left(a^m b^n\right)^{xm+yn} = (a^m b^n)(a^m b^n)\cdots(a^m b^n) \quad xm+yn \text{ times}$$

$$= a^m \left(b^n a^m\right)^{xm+yn-1} b^n$$

$$= a^m \left(b^n a^m\right)^{xm-1+yn} b^n$$

$$= a^m \left(b^n a^m\right)^{xm} \left(b^n a^m\right)^{-1} \left(b^n a^m\right)^{yn} b^n$$

$$= \left(b^n a^m\right)^{xm} a^m \left(a^{-m} b^{-n}\right) b^n \left(b^n a^m\right)^{yn} \quad \left[\begin{array}{l} a^m b^m = b^m a^m \text{ and } a^n b^n = b^n a^n \\ \text{for any } a, b \in G \text{ and also} \\ (ab)^{-1} = b^{-1} a^{-1} \end{array}\right]$$

$$= \left(b^n a^m\right)^{xm} \left(b^n a^m\right)^{yn} = \left(b^n a^m\right)^{xm+yn} = b^n a^m$$

So, $a^m b^n = b^n a^m$ for all $a, b \in G$.

Now, for $a, b \in G$,

$$ab = a^{xm+yn} b^{xm+yn} = \left(a^x\right)^m \left(a^y\right)^n \left(b^x\right)^m \left(b^y\right)^n$$

$$= \left(a^x\right)^m \left(b^z\right)^m \left(a^y\right)^n \left(b^y\right)^n = \left(b^x\right)^m \left(a^x\right)^m \left(b^y\right)^n \left(a^y\right)^n$$

$$= \left(b^x\right)^m \left(b^y\right)^n \left(a^x\right)^m \left(a^y\right)^n = b^{mx+ny} a^{mx+ny} = ba$$

[Here, also, you can start with $a^m b^n = a^m e b^n = a^m \left(a^n b^m\right)^{xm+yn-1} b^n$, e is the identity element, as $a^0 = e$ for any $a \in G$]

4. Let G be a group such that $a^2 = e$ for all $a \in G$. Show that G is abelian.

Proof: Let $a, b \in G$.

$$ab = aeb = a(ab)^2 b = a(ab)(ab)b = a^2 bab^2 = ba$$

[Here e is the identity in G, $(ab)^2 = e$, $a^2 = b^2 = e$]

5. Let G be a group such that $(ab)^2 = a^2 b^2$ for all $a, b \in G$, Show that G is abelian

Proof: Do it yourself.

6. Let G be the multiplicative group of the nth roots of unity. Prove that $G \simeq (\mathbb{Z}_n, +)$

Proof: Here $G = \{ e^{2k\pi i/n} : k = 0, 1, \ldots, n-1 \}$. Define $f : G \to \mathbb{Z}_n$ by $f(\bar{k}) = e^{2k\pi i/n}$. Then f is well defined and it is an isomorphism (Show it yourself)

Hence $G \simeq (\mathbb{Z}_n, +)$

7. Show that a group G is abelian if and only if the mapping $f : G \to G$ given by $f(x) = x^2$, is a homomorphism.

Proof: Let G be abelian. Let $x, y \in G$.

$f(xy) = (xy)^2 = x^2 y^2$ (As G is abelian)

$= f(x) f(y)$. So, f is a homomorphism.

Conversely, let f be a homomorphism. Let $x, y \in G$

Then $f(xy) = f(x) f(y)$ [As f is a homomorphism]

or, $(xy)^2 = x^2 y^2$

or, $(xy)(xy) = xxyy$

or, $x(yx)y = xxyy$

or, $yx = xy$ (by cancellation law)

So G is abelian

8. Show that there does not exist any non-trivial homomorphism of the group S_3 to the group $(\mathbb{Z}_3, +)$

Proof: If possible, let there be a homomorphism $f : S_3 \to \mathbb{Z}_3$. As f is a homomorphism, $o(f(a))$ divides $o(a)$ for any $a \in S_3$.

As $o(\rho_3) = o(\rho_4) = o(\rho_5) = 2$, so, $f(\rho_3) = f(\rho_4) = f(\rho_5) = \bar{0}$,

as $o(\bar{1}) = 3$ and $o(\bar{2}) = 3$

Now ρ_2 as ρ_5 $\rho_1 = (13)(12) = \rho_4 \rho_5$

So, $f(\rho_1) = f(\rho_4) f(\rho_5)$ (as f is a homomorphism)

$= \bar{0}$

Similarly $\rho_2 = (12)(13) = \rho_5 \rho_4$

So $f(\rho_2) = f(\rho_5) f(\rho_4)$ [as f is a homomorphism]

So $f(\rho_2) = \bar{0}$

Hence f is a trivial homomorphism. So there does not exist any non-trivial homomorphism of the group S_3 to the group $(\mathbb{Z}_3, +)$

9. Show that $o(a) = o(a^{-1})$ for any element a in a group G. Proof: Do it yourself.

10. Let G be a group and $a, b \in G$ such that $ab = ba$. If $o(a) = m$, $o(b) = n$ and $\gcd(m,n) = 1$, then $o(ab) = mn$.

Proof: $(ab)^{mn} = a^{mn} b^{mn}$ [as $ab = ba$]

$= e$ [e is the identity element in G, as $o(a) = m$, $o(b) = n$]

So, $o(ab)$ is finite. Let $o(ab) = k$ Then k divides mn

Also $(ab)^k = e \Rightarrow a^k b^k = e \Rightarrow a^k = b^{-k}$

Thus $o(a^k) = o(b^{-k}) = o(b^k)$ [as $o(a) = o(a^{-1})$ in a group]

But $a^m = e \Rightarrow (a^k)^m = e \Rightarrow o(a^k)$ divides m

Similarly $o(b^k)$ divides n. So, $o(b^k) = o(a^k)$ divides n

So, $o(a^k)$ divides $\gcd(m,n)$

As $\gcd(m,n) = 1$, so, $o(a^k) = 1$ So, $a^k = e$

But then m divides k. As $o(a^k) = o(b^k) = 1$

So, $b^k = e$, So, n divides k also. Consequently,

mn divides k as $\gcd(m,n) = 1$

As k divides mn and mn divides k. So $k = mn$. Hence $o(ab) = mn$

11. Let G be a group and H is a subgroup of G. Show that xHx^{-1} is a subgroup for any $x \in G$ and has the same cardinality as H.

Proof: Let $x \in G$, we want to show that xHx^{-1} is a subgroup. As H is a subgroup and $e \in H$, e is the identity in G, then

$xex^{-1} = e \in xHx^{-1}$; So, $xHx^{-1} \neq \phi$.

Let $a, b \in xHx^{-1} \Rightarrow a = xh_1x^{-1}$ and $b = xh_2x^{-1}$, $h_1, h_2 \in H$.

As H is a subgroup, $h_1h_2 \in H$

Now $ab = (xh_1x^{-1})(xh_2x^{-1}) = xh_1h_2x^{-1} \in xHx^{-1}$ (as $h_1h_2 \in H$)

Let $a \in H$. Then $a = xhx^{-1}$, for some $h \in H$. As H is a subgroup, $h^{-1} \in H$

Now $a^{-1} = (xhx^{-1})^{-1} = (x^{-1})^{-1}h^{-1}x^{-1} = xh^{-1}x^{-1} \in xHx^{-1}$ (as $h^{-1} \in H$)

So, xHx^{-1} is a subgroup of G.

Define $f: H \to xHx^{-1}$ by $f(h) = xhx^{-1}$, $h \in H$

Then by definition, f is surjective.

Also, $f(h_1) = f(h_2) \Rightarrow xh_1x^{-1} = xh_2x^{-1}$

$\Rightarrow h_1 = h_2$ (by cancellation law)

So, f is injective

So, f is bijective. So xHx^{-1} has the same cardinality as H.

12. If H and K are two subgroups of a group such that their orders are relatively prime, prove that $H \cap K = \{e\}$, e is the identity element in G.

Proof: Let $O(H) = m$, $O(K) = n$ and $\gcd(m,n) = 1$ Let $a \in H \cap K$

So, $O(a)$ divides m. Similarly, $o(a)$ divides n also. So $o(a)$ divides $\gcd(m,n) = 1$. So $o(a) = 1$. So, $a = e$. Hence $H \cap K = \{e\}$,