MTH3121 Assignment 5 : Saral 30 618 428

Question 3 b

$G = D_4 = \{e, r_1, r_2, r_3, m_1, m_2, m_3, m_4\}$

$H = \{r_2, e\}$

Left Cosets of H in G : $\{r_2, e\}, \{r_1, r_3\}, \{m_1, m_3\}, \{m_2, m_4\}$

Right Cosets of H in G : $\{r_2, e\}, \{r_1, r_3\}, \{m_1, m_3\}, \{m_2, m_4\}$

Order of H = 2

Index of H in G = 4

Since the left cosets of H in G are the same as the right cosets of H in G,
H is a normal subgroup of G.

To make the cayley table for the quotient group, G/H,
easier to read, let ' s give names to the cosets. Let :

$A = \{r_2, e\}$

$B = \{r_1, r_3\}$

$C = \{m_1, m_3\}$

$D = \{m_2, m_4\}$

Now put all the entries into the cayley table below :

□	A	B	C	D
A	A	B	C	D
B	B	A	D	C
C	C	D	A	B
D	D	C	B	A

The cayley table above is the same as the cayley table for $Z_2 \times Z_2$.

Therefore G/H is isomorphic to $Z_2 \times Z_2$.

Question 4 d

$G = R \times R$

$H = \{(x, y) \mid x = y\}$

To be able to describe what the left cosets of H in
G would look like lets gives some names to relevant things.

Let $(a, b) \in G$. To get the left coset for this one
element we get our (a, b) and stick on the left of everything in H.

This gives the coset :

$\{(a * c, b * c)\}$ where a and b remain constant for all $c \in R$.

The index of H in G would be infinite since there are an infinite number of left cosets.

The binary operation on the quotient group G / H could be addition,
since it allows for the quotient group to be closed under a binary operation,
closed under inversion and associative.

Question 9

a) To show that $H \cap K$ is a subgroup of H and a subgroup of K, $H \cap K$ must be :

1) Non – empty.

2) Closed under inversion

3) Closed under the binary operation.

So is $H \cap K$ non – empty ?

Well we know that H and K are subgroups of a group G.

This means that H and K are non – empty and that they are closed under inversion.

By definition if you are even closed under inversion that means that you have an identity.

So for any $h \in H$ and $k \in K$:

$h * h^{-1} = e_h$ (Equation 9.0)

$k * k^{-1} = e_k$ (Equation 9.1)

Where e_h and e_k are the identities in H and K.

But wait e_h and e_k the same ?

Since h, h^{-1}, k, k^{-1} are all elements of G ,
that means that Equations 9.0 and 9.1 are the same as doing :

(something in G) * (inverse of that something) (Equation 9.2)

And since we know G to be a group this means
that Equation 9.2 must evaluate to the inverse of G. Thus :

(something in G) * (inverse of that something) = e

Where e is the identitiy of G.

This means that :

$h * h^{-1} = e_h = e$ (Equation 9.4)

$k * k^{-1} = e_k = e$ (Equation 9.5)

Therefore $e_h = e_k = e$

So we have found that both H and K contain the identity of G.

This means that $H \cap K$ will at least contain the identity of G.

Therefore $H \cap K$ is non – empty.

So is $H \cap K$ closed under the binary operation?

For any $a, b \in H \cap K$, we know that a and b are in both the subgroups H and K.

By definition, the subgroups H and K are closed under the binary operation.

So if we take our a and b we know that:

$a * b$ = something in H = something in K (Equation 9.6)

Thus $a * b$ returns a value that is in both the subgroups H and K.

Therefore $H \cap K$ is closed under the binary operation.

Now is $H \cap K$ closed under inversion?

Again using a similar argument we know that for any $a \in H \cap K$, that a is an element of both H and K.

Since H and K are subgroups of some group G, we know that they are closed under inversion.

Therfore:

a^{-1} = something in H = something in K (Equation 9.7)

Thus a^{-1} is an element of both H and K.

Therfore $H \cap K$ is closed under inversion.

So we have shown that $H \cap K$ is non – empty,
closed under the binary operation and closed under inversion.

Since the elements of $H \cap K$ come from both H and K, $H \cap K$ is a subgroup of H and a subgroup of K.

b) Since G is finite this means the subgroups H and K are also finite.

We showed in part a) that $H \cap K$ is a subgroup of H and K.

By Lagrange ' s theorem we know that the order of any
subgroup of a finite group is a divsor of the order of the finite group.

Since $H \cap K$ is a subgroup of the two finite groups H and K.

This means that $|H \cap K|$ is a divisor of $|H|$ and a divisor of $|K|$

c) Lets write out the prime factorisation of $|H|$ and $|K|$ since this will be relevant.

$|H| = 13 \times 2^2$

$|K| = 13 \times 7$

From part b) we know that $|H \cap K|$ is a divisor of both $|H|$ and $|K|$.

This means that $|H \cap K| = 13$.

Since $|H \cap K|$ has a prime order it must be a cyclic group.

Question 14 b

The elements of G/H come from the cosets of H in G.

The question states that each element in G/H has a finite order.

That means for any $g \in G$:

gH = a set of elements that have a finite order. (Equation 14.0)

Thus for any $g \in G$, $h \in H$ and $c \in G/H$:

$g * h = c$ (Equation 14.1)

Now we know that h has a finite order. Lets denote the order of with n.

c has a finite order. Lets denote its order with a d.

If we raise both sides of Equation 14.1 to the power of the order of h we have that :

$(g * h)^n = c^n$

$g^n * h^n = c^n$

$g^n * e = c^n$ (Since n is the order of h)

$g^n = c^n$ (Since $g^n * e = g^n$)

Thus :

$g = c$

And this make sense since every element of G appears in G/H which we know c to be an element of.

Since we know that c has a finite order this means that g also has a finite order since $g = c$.

Therefore every element of G has a finite order.

Question 18

a) To prove that S^* is a subgroup of G it must be :

1) Non - empty.

2) Closed under the binary operation.

3) Closed under inversion.

So is S^* non - empty ?

First let ' s write what S^* even is :

$S^* = \{g \in G \mid f(g) \in S\}$ (Equation 18.0)

Equation 18.0 can be better read as
"S* is the stuff in g that maps to S under the homomorphism", this will help later on.

Now for the actual proving part :

Since S is a subgroup of H we know that S is non - empty, which means that H is also non - empty.

Why is this important ?

The question tells us that there is a homomorphism,
$f : G \longrightarrow H$, between G and H that is surjective.

This means that everything in H gets mapped to by elements of G and we know that H is non - empty.

So for there to even be this homomorphism between G and H :

G must also be non -
empty because you cannot have an empty domain mapping to a non - empty codomain.

Furthermore, since the homomorphism is surjective,
G maps to all of H so you also know that it maps to all of S, since S is a subgroup of H.

So we have shown that G is non -
empty and that its elements map to S (as well as H) under the homomorphism.

Now coming back to our informal definition of S^* ,
S^* was precisely the stuff in G that mapped to S under the homomorphism.

And we now know that G is non - empty and that its elements map to S (as well as H).

Therfore S^* is non - empty.

Now is S^* closed under the binary operation ?

For any $a, b \in S^*$, let ' s see what happens if we do the binary operation on them.

$a * b$ = something, and we cannot conclude anything from trying to compute $a * b$.

But what we do know is that $f : G \longrightarrow H$, is a homomorphism between G and H. Thus :

$f(a * b) = f(a) * f(b)$ (Equation 18.1)

We also know that $f(a) \in S$ and $f(b) \in S$.

From the question we know that S is a subgroup
of H which means it is closed under the binary operation.

This means that :

$f(a) * f(b) \in S$

Which subsequently means that :

$f(a * b) \in S$

Since a and b are also elements of G which we
know to be closed under the binary operation, we have that :

$a * b \in G$ and $f(a * b) \in S$ (Statement 18.2)

Statement 18.2 is precisely what it means to be in S^*.

Thus S^* is closed under the binary operation.

Now is S^* closed under inversion?

For any $a \in S^*$, a is also an element of G, which we know to be a group.

This means that a^{-1} is in G.

Additionally since f is a homomorphism:

$f(a^{-1}) = (f(a))^{-1}$ (Equation 18.3)

We know that $f(a)$ is in S and since S is closed under inversion (since it is a subgroup), $(f(a))^{-1}$ will also be in S.

Thus we can rewrite Equation 18.3 more informally as:

$f(a^{-1}) = (f(a))^{-1}$ = something in S.

Therefore $a^{-1} \in G$ and $f(a^{-1}) \in S$, and this is precisely what it means to be an element of S^*.

Which means that S^* is closed under inversion.

So we have shown that S^* is non – empty,
closed under the binary operation and closed under inversion.

Thus S^* is a subgroup of G.

Now for the final part of the question we have to show that the kernel of f, K, is in S^*.

But first what even is K?

K contains the elements of G that map to the identity of H.

So for any $k \in K$:

$f(k) = e_H$ (Equation 18.4)

Where e_H is the identity in H.

Since S is a subgroup of H, we know that the identity of S, let's call it e_S, is equal to e_H:

$e_S = e_H$ (Equation 18.5)

Thus:

$f(k) = e_S$ (Equation 18.6)

Or in easier to understand terms, for any k e K:

$f(k)$ = something in S (Equation 18.7)

So we have found that $f(k) \in S$ and we know that k is also an element of G.

So summarising this fact:

For any $k \in K$, $k \in G$ and $f(k) \in S$. This is precisely what it means to be an element of S^*.

Thus S^* contains K.

b) For $f^* : S^* \longrightarrow H$, to be a homomorphism, for any a and $b \in S^*$:

$f^*(a * b) = f^*(a) * f^*(b)$ (Equation 18.8)

So does this hold?

$f^*(a * b) = f(a * b)$ (Since $f^*(g) = f(g)$ and we can set $g = a * b$)

$f(a * b) = f(a) * f(b)$ (Since we are told from the question that S is a homomorphism)

$f(a) * f(b) = f^*(a) * f^*(b)$ (Since $f^*(g) = f(g)$ for all $g \in S^*$)

Thus:

$f^*(a * b) = f^*(a) * f^*(b)$

So f^* is a homomorphism.

So what would be the image of f^*?

Let's think of f^* as f but with a restricted domain.

We know that f is surjective, so it maps the elements of its domain, G, to all of H.

Since S is a subgroup of H, f also maps the elements of its domain to all of S.

So what would be these elements of f's domain that map to all of S?

It would be everything in G that maps to S. Or rather:

$\{g \in G \mid f(g) \in S\}$

And we can see that this set is the same as S^*.

So what we just found was that in the domain S^*, the image of f is S.

And f is the same as f^* under this domain.

Thus the image of f^* is S.

So what would be the kernel of f^*?

First let's call the kernel of f^*, F and let's define F below:

F is all $g \in S^*$, such that $f(g) = e_H$. (Definition 1)

Let's again think of f^* as another version of f but with a restricted domain.

Now let's recap what K is:

K is all $g \in G$ such that $f(g) = e_H$, where e_H is the identity of H. (Definition 2)

Now since S is a subgroup of H, the identity of S is the same as the identity of H. Thus:

$e_S = e_H$ (Equation 18.9)

Where e_S is the identity of S.

So another definition for K is:

K is all $g \in G$ such that $f(g) = e_S$. (Definition 3)

The domain of f^* is all $g \in G$ that maps to S. e_S is within S.

So we could again make another definition for K :

K is all $g \in S^*$, such that $f(g) = e_s$. (Definition 4)

Now again replacing e_s with e_H is Definition 4, we can make one more defitition for K :

K is all $g \in S^*$, such that $f(g) = e_H$. (Definition 5)

And now we see that from Definition 5 and Definition 1 that F and K have the same definition.

Therefore F = K.

Thus the kernel of f^* is K.

c) So we have shown that $f^* : S^* \longrightarrow H$ is a homomorphism and its image is S and its kernel is K.

From the first isomorphism theory we therefore know that :

$$S \cong \frac{S^*}{K}$$