Q3) Part One : $f(e_H) = e_{G_1}$

$f(e_H) = f(e_H \cdot e_H) = f(e_H) * f(e_H)$

$f(e_H) \in G_1 \Rightarrow f(e_H)^{-1} \in G_1$ (G_1 is a group)

$f(e_H) * f(e_H)^{-1} = f(e_H) * (f(e_H) * f(e_H)^{-1})$

$e_{G_1} = f(e_H) * e_{G_1}$

Thus, $f(e_H) = e_{G_1}$

Part Two: Try One

For all $h \in H$, $h^{-1}h = e_H = hh^{-1}$.

$f(h^{-1}) = f(h^{-1} e_H) = f(h^{-1} \cdot e_H)$

$= f(h^{-1}) \cdot f(e_H) = f(h^{-1}) \cdot e_{G_1}$

Since $h \in H$, $h^{-1} \in H$ and thus $f(h^{-1}) \in G_1$.

$f(h^{-1}) = f(h^{-1}) \cdot e_{G_1}$ X

$[f(h^{-1})]^{-1} \cdot f(h^{-1}) =$ X

Part Two : Try Two

Since H is a group, $h^{-1} \in H$ for all $h \in H$. Thus,

$f(h \cdot h^{-1}) = f(h^{-1} \cdot h) = f(e_H) = e_{G_1}$

$f(h) * f(h^{-1}) = f(h^{-1}) * f(h) = e_{G_1}$

Thus, $f(h)^{-1} = f(h^{-1})$.

Q5) First consider the complex numbers under addition $= (a+bi) + (c+di)$

$= (a+c) + (b+d)i$

Then, there does exist $*$ such that $(R^2, *)$ is isomorphic to $(C, +)$.

There does exist a homomorphism from R^2 to C:

$f[(a,b)] = (a+bi)$.

$f[(a,b) + (c,d)] = f[(a,b)] + f[(c,d)]$

$= (a+bi) + (c+di) = (a+c) + (b+d)i$

$f[(a,b) + (c,d)] = f[(a+c, b+d)]$

$= (a+c) + (b+d)i = (a+bi) + (c+di)$

$= f[(a,b)] + f[(c,d)]$

Also, the function f is bijective, so f is an isomorphism between R^2 and C.

Define $*$ on R^2 to be:

- $(a,b) * (c,d) = (ac - bd, ad + bc)$

Now, $f[(a,b)] = (a + bi) \quad [R^2 \to C]$

$f[(a,b) * (c,d)] = f[(ac - bd, ad + bc)]$

$= (ac - bd) + (ad + bc)i$

$= (a + bi) \times (c + di) = f[(a,b)] \cdot f[(c,d)]$

Thus, $f[(a,b) * (c,d)] = f[(a,b)] \cdot f[(c,d)]$

Thus, there exists a homomorphism from R^2 to C under multiplication in C.

(Q13)

$\Rightarrow$ Assume that $\text{Ker}(f) = [e_H]$. We have to show that for all $h_1, h_2 \in H$, $f(h_1) = f(h_2) \Rightarrow h_1 = h_2$.

Since $f(h_1) = f(h_2)$, we have that $[f(h_1)]^{-1} = [f(h_2)]^{-1}$. Thus,

$e_G = [f(h_1)][f(h_2)]^{-1}$

$e_G = [f(h_1)][f(h_2^{-1})]$ (Problem 3)

$e_G = [f(h_1 h_2^{-1})]$ (homomorphism property)

$h_2 h_2^{-1} = e_H$ (by assumption)

$h_1 = h_2$

$\Leftarrow$ Assume that f is injective. That is, for all $h_1, h_2 \in H$ we have $f(h_1) = f(h_2) \Rightarrow h_1 = h_2$. We have to show $\text{Ker}(f) = [e_H]$.

We give a proof by contradiction. Assume there exists $e \in H$ such that $f(e) = e_{G_1}$ and $e \neq e_H$. Now,

$$f(e) = e_{G_1} = f(e_H)$$

$e = e_H$ (since f is injective).

Thus, we have that for all elements in the kernal of f, they are equal to the identity in H.

Q1)

(b) $\Rightarrow$ If H is a subgroup of G_1, then we have that for $h_1, h_2 \in H$:

$h_2^{-1} \in H$ (existance of inverse) (A2)

$(h_1 \cdot h_2^{-1}) \in H$ (closure). (A0)

$\Leftarrow$ Assume that $h_1, h_2 \in H$. We have that $(h_1 \cdot h_2^{-1}) \in H$. We have to prove that H is a (sub)group (of G_1).

(A1)• $h_1 \in H \Rightarrow [h_1 \cdot h_1^{-1}] \in H \Rightarrow e \in H$

(A2)• $h_1 \in H \Rightarrow [e \cdot h_1^{-1}] \in H \Rightarrow [h^{-1}] \in H$

(A0)• $h_1 \in H$ and $h_2 \in H \Rightarrow h_1 \in H$ and $h_2^{-1} \in H \Rightarrow [h_1 \cdot (h_2^{-1})^{-1}] \in H \Rightarrow [h_1 \cdot h_2] \in H$

(A3)• $h_1 \in H$, $h_2 \in H$ and $h_3 \in H \Rightarrow h_1, h_2, h_3 \in G_1$.

Since G_1 is a group, $(h_1 \cdot h_2) \cdot h_3 = h_1 \cdot (h_2 \cdot h_3)$

Thus H is a subgroup of G_1.

(a) (Scratch Work)

Lemma: For all $g \in G_1$ and $n, m \in \mathbb{Z}$, we have that:

1. $g^{m+n} = g^m \cdot g^n$
2. $(g \cdot h)^m = g^m \cdot h^m$
3. $g^1 = g$

Case One: $n > 0$ and $m \in \mathbb{Z}$.

We give a proof by induction.

I Base case, $n = 1$.

$(g^1)^m = (g)^m = g^m = g^{1 \times m}$ ■

II Inductive hypothesis, for $R \in \mathbb{Z}^+$, we have that

$(g^R)^m = g^{Rm}$

III Inductive step:

$(g^{R+1})^m = (g^R \cdot g^1)^m = (g^R \cdot g)^m$

$= (g^R)^m \cdot (g)^m$

$= g^{Rm} \cdot (g)^m$ (Inductive Hypothesis)

$= g^{Rm} \cdot g^m$ (Base case)

$= g^{Rm+m}$ (Lemma)

$= g^{m(R+1)}$.

Thus, $(g^{R+1})^m = g^{m(R+1)}$ ■

(a) g^{nm} = 'dotting ($\cdot$)' g with itself nm times.

$(g^n)^m$ = 'dotting g^n with itself m times.
= dotting g with itself nm times!

We are done!

(Q2) We can only find subgroups of order 1, 2, 4 and 8. (by lagranges theorem).

- Subgroups of order 1: $[e]$
- Subgroups of order 2: $[e, p^2]$, $[e, \delta]$, $[e, \delta p]$, $[e, \delta p^2]$, $[e, \delta p^3]$, (Identical upto isomophism).

Proofs

- $[e, p^2]$ is a group, since $e \in [e, p^2]$, $e^{-1} = e \in [e, p^2]$, $(p^2)^{-1} = p^2 \in [e, p^2]$ (a rotation of 180° counterclockwise is the same thing as the clockwise 180° rotations). Moreover, $(p^2)^n = p^2$ for all odd n and $(p^2)^n = e$ for all even n. Thus, the set is closed under multiplication as well.
- $[e, \delta]$, $[e, \delta p]$, $[e, \delta p^2]$, $[e, \delta p^3]$ are all groups since the inverse of a reflection is itself. Thus these sets are closed under multiplication [$(\delta p^k)^n = (\delta p^k)$ for all odd n and $(\delta p^k)^n = e$ for all even n].

Also note that:

- $[e, p^2] = \langle p^2 \rangle$ [The cyclic group generated by p^2].
- $[e, \delta] = \langle \delta \rangle$

(Q7) The inverse of (ab) is $(b^{-1}a^{-1})$. Proof:

$(ab)(b^{-1}a^{-1}) = abb^{-1}a^{-1} = a(bb^{-1})a^{-1} = a(e)a^{-1}$

$= aa^{-1} = e$

$(b^{-1}a^{-1})(ab) = b^{-1}a^{-1}ab = b^{-1}(a^{-1}a)b = b^{-1}eb$

$= b^{-1}b = e.$

The inverse of $(a_1 \cdots a_n)$ is $(a_n^{-1} \cdots a_1^{-1})$. We give a proof by induction:

- Base Case, $n = 2$ (Already proved above).
- Inductive step, assuming $n = k$, prove for $n = k+1$.

$(a_1 \cdots a_n a_{n+1})^{-1} = (a_{n+1}^{-1} a_n^{-1} \cdots a_1^{-1})$

Proof:

$(a_1 \cdots a_n a_{n+1})(a_{n+1}^{-1} a_n^{-1} \cdots a_1^{-1})$

$= a_1 \cdots a_n (a_{n+1} a_{n+1}^{-1}) a_n^{-1} \cdots a_1^{-1}$

$= a_1 \cdots a_n (e) a_n^{-1} \cdots a_1^{-1}$

$= (a_1 \cdots a_n)(a_n^{-1} \cdots a_1^{-1})$ [Since by hypothesis we have that $(a_1 \cdots a_n)^{-1} = a_n^{-1} \cdots a_1^{-1}$]

$= e.$

~~$(a_{n+1}^{-1} a_n^{-1}$~~

Q.E.D.