DT8248 Stage 4 Group Theory Problem Set 5

Name: Jason Borland

Student Number: D17129310

Question 1:

If $(A, *_A), (B, *_B)$ are two groups, the direct product $A \times B$ is defined to be the group with underlying set $\{(a,b) : a \in A, b \in B\}$ with componentwise operation; i.e. $(a_1, b_1) * (a_2, b_2) = (a_1 *_A a_2, b_1 *_B b_2)$.

a. Verify that the direct product $A \times B$ is really a group.

b. Show that A is isomorphic to a subgroup of $A \times B$.

c. For any prime number p, what are the possible subgroups (up to isomorphism) of $\mathbb{Z}_p \times \mathbb{Z}_p$? Explain your answer.

Q1a:

Definition Let G be a non-empty set together with a binary operation *, that assigns to each ordered pair (a,b) of elements of G an element of G denoted ab.

$$(a,b) \rightarrow ab$$

We say $(G, *)$ is a group under the operation * if:

1. Associativity. $(ab)c = a(bc) \forall a, b, c \in G$
2. Identity. $\exists e \in G$ s.t. $ae = ea = a, \forall a \in G$
3. Inverse. $\forall a \in G, \exists b \in G$ s.t. $ab = ba = e$. b is the inverse of a and denoted a^{-1}.

To verify that the direct product is a group we need to check 1, 2, and 3 and that $A \times B$ is closed under the operation (direct product).

Clearly $A \times B$ is closed under the direct product. Note $(a_1, b_1)(a_2, b_2) = (a_1 a_2, b_1 b_2) \in A \times B$ as $a_1 a_2 \in A$ and $b_1 b_2 \in B$.

1: Consider elements $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in A \times B$ Also note associativity holds in the componentwise operations of $A \times B$ as A and B are both groups.

$$\begin{aligned} ((a_1, b_1)(a_2, b_2))(a_3, b_3) &= (a_1, b_1)[(a_2, b_2)(a_3, b_3)] \\ (a_1 a_2, b_1 b_2)(a_3, b_3) &= (a_1, b_1)(a_2 a_3, b_2 b_3) \\ (a_1 a_2 a_3, b_1 b_2 b_3) &= (a_1 a_2 a_3, b_1 b_2 b_3) \end{aligned}$$

So associativity holds for $A \times B$

2: Both A and B are groups so each contains an identity element e_A and e_B respectively. Consider $(e_A, e_B) \in A \times B$.

$$\begin{aligned} (e_A, e_B)(a, b) &= (e_A a, e_B b) \\ &= (a, b) \\ (a, b)(e_A, e_B) &= (a e_A, b e_B) \\ &= (a, b) \end{aligned}$$

$A \times B$ contains the identity element (e_A, e_B).

3: Both A and B are groups, so every element $a \in A$ and $b \in B$ contains an inverse $a^{-1} \in A$ and $b^{-1} \in B$. So for an element $(a, b) \in A \times B$, the inverse is (a^{-1}, b^{-1}).

$$\begin{aligned} (a, b)(a^{-1}, b^{-1}) &= (aa^{-1}, bb^{-1}) \\ &= (e_A, e_B) \\ (a^{-1}, b^{-1})(a, b) &= (a^{-1}a, b^{-1}b) \\ &= (e_A, e_B) \end{aligned}$$

Every element $(a, b) \in A \times B$ contains the an inverse element $(a^{-1}, b^{-1}) \in A \times B$.

So $A \times B$ is a group ■.

Q1b:

Definition An isomorphism $\phi : G \rightarrow H$ is a bijection (one-to-one and onto mapping) which preserves the group operation.

$$\phi(a *_G b) = \phi(a) \diamond_H \phi(b), \quad \forall a, b \in G$$

If there is an isomorphism from G to H we say G and H are isomorphic groups and denote: $G \cong H$.

We need to consider a subgroup of $A \times B$. I propose the subgroup $K = \{(a, e_B) : a \in A, e_B \text{ is identity in } B\}$. Firstly we need to show this is a subgroup of $A \times B$. To do this we are going to use the 'one-step' subgroup test:

1. The elements of K are all elements of $A \times B$ where the b component is fixed to e_B (the identity in B).
2. The identity is in K, as $e_A \in A$ and b is fixed to e_B. The identity being $(e_A, e_B) \in K$. So $K \neq \emptyset$.
3. Lets consider two elements in K, say $k_1 = (a_1, e_B)$ and $k_2 = (a_2, e_B)$.
4. If $k_2 = (a_2, e_B)$, then $k_2^{-1} = (a_2^{-1}, e_B)$. Note $e_B^{-1} = e_B$ as, e_B is the identity.
$$\begin{aligned} k_1 k_2^{-1} &= (a_1, e_B)(a_2^{-1}, e_B) \\ &= (a_1 a_2^{-1}, e_B e_B) \\ &= (a_1 a_2^{-1}, e_B) \in K \end{aligned}$$
By the one-step subgroup test $K \leq G$

To show that A is isomorphic to K, consider the mapping $\phi : A \rightarrow K$, where ϕ maps $(a_i \in A) \rightarrow ((a_i, e_B) \in K)$.

1. We first need to show if ϕ is a homomorphism (i.e. it preserves the group operation):
$$\begin{aligned} \phi(a_p *_A a_q) &= (a_p a_q, e_B) \\ &= (a_p a_q, e_B e_B) \\ &= (a_p, e_B) *_K (a_q, e_B) \\ &= \phi(a_p) *_K \phi(a_q) \end{aligned}$$
So A is homomorphic K.
2. We now need to show ϕ is one-to-one. This is trivial from the definition: ϕ maps $(a_i \in A) \rightarrow ((a_i, e_B) \in K)$.
$$\begin{aligned} Consider\ \phi(a_p) &= \phi(a_q) \\ (a_p, e_B) &= (a_q, e_B) \\ \therefore a_p &= a_q \end{aligned}$$
3. Showing that ϕ is onto (surjective). This is trivial from the definition.

So $A \cong K$ ■.

1c:

Lagrange's Theorem If G is a finite group and $H \leq G$ then $|H|\big||G|$. Moreover, the number of distinct left (or right) cosets of H in G is $\frac{|G|}{|H|}$.

Corollary Any group of prime order is cyclic.

Corollary In a finite group G, $\forall a \in G$, then $o(a)\big||G|$.

$$\mathbb{Z}_p = \{0, 1, 2, \ldots, p-1\}$$

The order of $\mathbb{Z}_p = p$, thus the order of $\mathbb{Z}_p \times \mathbb{Z}_p$ is p^2.

A subgroup of $\mathbb{Z}_p \times \mathbb{Z}_p$ must have order that divides p^2, as per Lagrange's theorem.
As p is prime, the possible orders of the subgroups of $\mathbb{Z}_p \times \mathbb{Z}_p$ are $1, p, p^2$. For 1 and p^2 there are only two subgroups of $\mathbb{Z}_p \times \mathbb{Z}_p$ which are $\{(e, e)\}$ and $\mathbb{Z}_p \times \mathbb{Z}_p$ respectively. Note e is the identity element in $\mathbb{Z}_p$.

So now suppose we have $A \leq \mathbb{Z}_p \times \mathbb{Z}_p$ with $|A| = p$. From corollary, since p is prime then A must be cyclic. So there exists some element $(x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p$ s.t. $A =< (x, y) >$, with $o((x, y)) = p$.

So we need to find size of the set of subgroups of $\mathbb{Z}_p \times \mathbb{Z}_p$ of order p.
i.e. $\Big|\{< (x, y) > : (x, y) \in \mathbb{Z}_p \times \mathbb{Z}_p \text{ has order p}\}\Big|$.

From corollary the number of elements of order p of $\mathbb{Z}_p \times \mathbb{Z}_p$ is all of the elements of form (x, y) except (e, e). This is $p^2 - 1$.

Now each subgroup of order p consists of the identity and p-1 elements of order p. So the number of subgroups of order p is $\frac{p^2-1}{p-1} = p + 1$.

Thus the total number of subgroups of $\mathbb{Z}_p \times \mathbb{Z}_p$ is $p + 3$.

Question 2:

a. The exponent of a group is defined to be the smallest positive integer m such that $x^m = e$ for all x in the group.

i. Prove that every finite group has exponent that divides the order of the group.

ii. What is the exponent of D_4, the dihedral group of degree 4.

b. Suppose that $\varphi : G \rightarrow G'$ is a group isomorphism:

i. Prove that the inverse function $\varphi^{-1} : G' \rightarrow G$ is also an isomorphism.

ii. Prove that for any element $a \in G$, the order $o(a) = o(\varphi(a))$.

iii. Prove that the group of integers under addition is not isomorphic to the group of non-0 rationals under multiplication.

Q2a,i:

Definition The order of an element g in a group G is the smallest positive integer n such that $g^n = e$.

Corollary In a finite group G, $\forall a \in G, o(a)\big||G|$.

Corollary Let G be a finite group, and let $a \in G$, then $a^{|G|} = e$

Since the exponent of a finite group G is the smallest positive integer m, s.t. $x^m = e$ for all $x \in G$. This is the defintion of the order of an element. From the corollary the $o(x)\big||G|$. So the exponent of a group divides the order of the group ■.

Q2a,ii:

$D_4 = \{I, R, R^2, R^3, H, V, D, D'\}$

Element	o(a)
I	1
R	4
R^2	2
R^3	4
H	2
V	2
D	2
D'	2

The exponent of $D_4 = 2$.

Q2b i:

Let $\varphi : G \rightarrow G'$ be a group isomorphism. Because $\varphi : G \rightarrow G'$ is an is isomorphism, φ is a bijection. This means the inverse mapping $\varphi^{-1} : G' \rightarrow G$ is also a bijection. So it is only necessary to show that the mapping φ^{-1} is a group homomorphism (i.e the group operation is preserved).

If we consider elements $g_1', g_2' \in G'$. We know since φ is bijective that $g_1, g_2 \in G$, where $\varphi(g_1) = g_1'$ and $\varphi(g_2) = g_2'$. Also because φ^{-1} exists and is bijective $\varphi^{-1}(g_1') = g_1$ and $\varphi^{-1}(g_2') = g_2$.

$$\begin{aligned} \varphi^{-1}(g_1' g_2') &= \varphi^{-1}(\varphi(g_1)\varphi(g_2)) \\ &= \varphi^{-1}(\varphi(g_1 g_2)) \quad As,\ \varphi\ is\ isomorphic \\ &= g_1 g_2 \quad Follows\ from\ definition\ of\ inverse\ mapping \\ &= \varphi^{-1}(g_1')\varphi^{-1}(g_2') \end{aligned}$$

This proves $\varphi^{-1} : G' \rightarrow G$ is also an isomorphism ■.

Q2b ii:

Consider any element $a \in G$, the order of $o(a) = n$.

$$\begin{aligned} o(a) &= n \\ \therefore a^n &= e \\ \therefore \varphi(a^n) &= \varphi(aa......a) \quad note\ a\ n\ times. \\ \therefore &= \varphi(a)\varphi(a)\ldots\varphi(a) \quad Because\ \varphi\ is\ isomorphic \\ \therefore &= (\varphi(a))^n \\ We\ know\ \varphi(a^n) &= \varphi(e) = e' \quad where\ e'\ identity\ in\ G' \\ \therefore (\varphi(a))^n &= e' \\ \therefore o(\varphi(a)) &= n \quad ■ \end{aligned}$$

Q2b iii:

Goal is to prove that $(\mathbb{Z}, +) \ncong (\mathbb{Q}, *)$. Since the function is not defined, I am going to aim for a contradiction. Suppose that $\phi : (\mathbb{Z}, +) \rightarrow (\mathbb{Q}, *)$ is an isomorphism.

This means ϕ is onto (surjective). Now consider an element $2r \in \mathbb{Z}$ (i.e. an even integer), such that $\phi(2r) = 2$.

$$\begin{aligned} 2 &= \phi(2r) \\ &= \phi(r + r) \quad as\ r \in \mathbb{Z} \\ &= \phi(r) * \phi(r) \quad properties\ of\ isomorphism \\ &= (\phi(r))^2 \\ \therefore \phi(r) &= \pm\sqrt{2} \end{aligned}$$

However this is a contradiction since $\phi(r)$ must be a rational number, note $\sqrt{2} \notin \mathbb{Q}$.
We can conclude that $(\mathbb{Z}, +) \ncong (\mathbb{Q}, *)$ ■.

Question 3:

1. If G is a group and $H < G$ with $[G : H] = 2$, prove that $H \lhd G$.
2. If $N \lhd G$ and $H < G$, prove that $NH < G$.
3. Show that the intersection of two normal subgroups of a group G is also a normal subgroup of G.
4. If $H < G$ and $N \lhd G$, show that $H \cap N \lhd H$.
5. Suppose H is the only subgroup of order $|H|$ in a finite group G. Prove that $H \lhd G$.

Q3a:

Definition Let G be a group and H a subset of G. $\forall a \in G$, the set

$aH = \{ah : h \in H\}$ and $Ha = \{ha : h \in H\}$

when H is a subgroup of G, the set aH is called the left coset of H by a (or containing a) and Ha is called the right coset of H by a. (a is called the coset representative of aH (or Ha). Note $a \in aH$ since $e \in H \leq G$; so $a = ae \in aH$ (likewise $a \in Ha$).

Definition The index of a subgroup H in G is the number of distinct left cosets of H in G; denoted by [G:H].

*Properties of Cosets:*Lemma* Let $H \leq G$ and let $a, b \in G$ Then:

1. $a \in aH$
2. $aH = H$ iff $a \in H$
3. $aH = bH\ or\ aH \cap bH = \emptyset$
4. $aH = bH\ iff\ a^{-1}b \in H$
5. $|aH| = |bH|$

Definition A subgroup H of a group G is called a normal subgroup of G if :

$$aH = Ha\ for\ all\ a \in G;$$

Denoted $H \trianglelefteq G\ or\ H \lhd G$ or equivalently $aHa^{-1} = H$.

Proof: Since $[G : H] = 2$, then H has two left (and two right) cosets. Since H is a subgroup it contains the identity so one of those cosets is H (as $eH = H$). If we consider $g \notin H$. Then gH is the other coset. (Hg is the other right coset).

$$H \cup gH = G = H \cup Hg$$

Since these are disjoint unions, we have $gH = Hg$ or equivalently $gHg^{-1} = H$.
As the equation $gHg^{-1} = H$ holds for any $g \in gH$, and clearly holds for any element in the trivial coset H. The equation holds for all elements in G. Which is the definition of a normal subgroup. Therefore $H \lhd G$ ■.

Q3b:

Consider a group G, and a normal subgroup $N \lhd G$. Prove that if $H < G$, then $NH < G$. Where $NH = \{nh : n \in N, h \in H\}$.

To show NH is a subgroup we have are going to use the onestep subgroup method.

1. The property that defines NH is that it is the product nh, where $n \in N$ and $h \in H$.
2. The identity is in NH (and therefore the group is not empty). Since N is a subgroup so $e \in N$, and similarly H is a subgroup so $e \in H$.
$$e = ee \in NH$$
3. If we consider two elements say $a = n_1 h_1 \in NH$ and $b = n_2 h_2 \in NH$.
4. Now $b^{-1} = (n_2 h_2)^{-1} = h_2^{-1} n_2^{-1}$. We need to see if $ab^{-1} \in NH$:
$$\begin{aligned} ab^{-1} &= n_1 h_1 (h_2^{-1} n_2^{-1}) \\ &= n_1 (h_1 h_2^{-1}) n_2^{-1} \\ &= n_1 n_2^{-1} (h_1 h_2^{-1}) \quad As\ gN = Ng \\ \therefore ab^{-1} &= n_1 n_2^{-1} (h_1 h_2^{-1}) \in NH \end{aligned}$$
So $NH \lhd G$■

Q3c:

Let N_1 and N_2 be normal subgroups of G. Consider an element $n \in N_1 \cap N_2$. Note that $n \in N_1$ and $n \in N_2$ since $N_1 \cap N_2 \subseteq N_1, N_2$). We can say $gng^{-1} \in N_1$ and $gng^{-1} \in N_2\ \forall g \in G$. Therefore $gng^{-1} \in N_1 \cap N_2\ \forall g \in G$. So we have:

$$g(N_1 \cap N_2)g^{-1} \subseteq (N_1 \cap N_2)$$

So $(N_1 \cap N_2) \lhd G$■

Q3d:

We are trying to show: $h(H \cap N) = (H \cap N)h$ or equivalently $h(H \cap N)h^{-1} = (H \cap N)$.

We know $gN = Ng$ and $gNg^{-1} = N$ for all $g \in G$. We also know $H < G$, therefore $hN = Nh$ and $hNh^{-1} = N$ for all $h \in H$.

Consider $x \in (H \cap N)$ therefore $x \in H$ and $x \in N$. Since $x \in N$ and $h \in H < G$, then $hxh^{-1} \in (H \cap N)$. Since $x \in (H \cap N) \subseteq H, N$. Therefore we can say:

$$(H \cap N) \lhd H■$$

Q3e:

We know $H < G$ and order of H is $|H| = n$. In particular it is the only subgroup of order $|H| = n$ in finite group G.

From Lagrange's Theorem we know $|H|\big||G|$.

I need to show $gH = Hg\ or\ gHg^{-1} = H$:

Consider the set gHg^{-1}, where $g \in G$. If we can show firstly that gHg^{-1} is a group and secondly it has order n, then we will have shown $gHg^{-1} = H$.

To show $gHg^{-1} < G$ I will use the one-step subgroup test:

1. The property that defines gHg^{-1} is ghg^{-1} where $h \in H$.
2. The identity is in gHg^{-1}, as $e \in H$, therefore $geg^{-1} = gg^{-1} = e$. So clearly the group is not empty.
3. Consider two elements $a = gh_1g^{-1}$ and $b = gh_2g^{-1}$.
4. Now $b^{-1} = (gh_2g^{-1})^{-1} = gh_2^{-1}g^{-1}$. We need to show $ab^{-1} \in gHg^{-1}$:
$$\begin{aligned} ab^{-1} &= gh_1g^{-1}(gh_2^{-1}g^{-1}) \\ &= gh_1(g^{-1}g)h_2^{-1}g^{-1}) \\ &= g(h_1h_2^{-1})g^{-1} \\ \therefore ab^{-1} &= g(h_1h_2^{-1})g^{-1} \in gHg^{-1} \end{aligned}$$
So gHg^{-1} < G.

So what is the order of gHg^{-1}. Clearly there is a one-to-one mapping $H \rightarrow gHg^{-1}$, so the order is n. So we can say $gHg^{-1} \lhd G$■

In [ ]: