Problem Set 2 - Thomas Boyko - 30191728

1. A group G and a subset $H \subseteq G$ is given below. Show that H is a subgroup of G.

   (a) $G = GL_n(\mathbb{R})$ and H is the subset of all diagonal matrices in G.

   Clearly the identity I is in H since the identity matrix is a diagonal matrix.

   Take $A, B \in H$. Then A, B are diagonal. Consider B^{-1}. This must be diagonal since the inverse of a diagonal matrix is also diagonal.

   And since A, B^{-1} are diagonal their product must be diagonal since the product of diagonal matrices is also diagonal. So AB^{-1} is a diagonal matrix, and $AB^{-1} \in H$. Therefore, H is a subgroup of $GL_N(\mathbb{R})$.

   (b) Fix a positive integer n. Let G be any Abelian group, and $H = \{g \in G : g^n = e\}$.

   The identity of G must be in H because $e^n = e$ for any integer n.

   Let $a, b \in H$. Then $a^n = e = b^n$. This also gives us:

$$\begin{aligned} e &= a^n b^{-n} \\ &= a^n (b^{-1})^n \\ &= (ab^{-1})^n && \text{Since G is abelian.} \end{aligned}$$

   And since $ab^{-1} \in H$, H is a subgroup of G.

   (c) G is any Abelian group, H is the subset of all elements of finite order.

   Trivially, the identity of G is in H since $o(e) = 1$ is finite.

   Then let $a, b \in H$. Both a, b have finite order. So write $o(a) = m$, $o(b) = n$. Let $l = lcm(m, n)$, so $m|l$, and $n|l$.

   Write $mc = l$ and $nd = l$, for some $c, d \in \mathbb{Z}$.

$$\begin{aligned} (ab^{-1})^l &= a^l b^{-l} && \text{Since } G \text{ is abelian} \\ &= a^{mc} b^{-nd} \\ &= (a^m)^c (b^n)^{-d} \\ &= e^c e^{-d} \\ &= e. \end{aligned}$$

   From this we can say the order of ab^{-1} must divide l, $o(ab^{-1})$ is less than or equal to l, meaning the order is finite and H is a subgroup of G.

2. For a positive integer n, recall the group n-th roots of unity, denoted by μ_n.

   (a) Show that if d—n, then μ_d is a subgroup of μ_n.

   Begin with showing $\mu_d \subseteq \mu_n$. Suppose $d|n$, so $dk = n$ for some $k \in \mathbb{Z}$.

   Suppose $z \in \mu_d$. Then $z^d = 1$. Then:

$$\begin{aligned} 1 = 1^k &= (z^d)^k \\ &= z^{dk} \\ &= z^n. \end{aligned}$$

   So $z^n = 1$, $z \in \mu_n$, and $\mu_d \subseteq \mu_n$.

   We can show easily that $1 \in \mu_d$, since $1^d = d$ for any $d \in \mathbb{Z}$.

   Now take some $a, b \in \mu_d$. We say that $a^d = b^d = 1$. This gives $a^d b^{-d} = 1$, and since multiplication in $\mathbb{C}$ is commutative, $(ab^{-1})^d = 1$, and $ab^{-1} \in \mu_d$. So μ_d is a subgroup of μ_n.

   (b) Describe all subgroups of μ_n.

   By the fundamental theorem of finite groups, we know that since μ_n is generated by $e^{\frac{2\pi i}{n}}$, any subgroup $H = \left\langle e^{\frac{2\pi i d}{n}} \right\rangle$, with $d|n$. So $n = dk$ and $H = \langle \frac{2\pi i}{k} \rangle$. So any subgroup of μ_n is μ_k for some $k|n$.

(c) If H is any finite subgroup of $(C \setminus \{0\}, \cdot)$, then show that there exists a positive integer k such that H = μ_k.

Let H be a finite subgroup of $(C \setminus \{0\})$, and write $|H| = n$.

Since all elements of H have finite order, let l be the lcm of all elements of H. Then for any $h \in H, h^l = 1$, since the order of h must divide l.

So any $h \in H$ must be an lth root of unity. Since H is a subgroup of $(\mathbb{C} \setminus \{0\}, \cdot)$, it is closed under $\cdot$, and it must be a subset of μ_l, we can say from part b that H must be μ_k for some $k|l$.

3. Let $f : G \to H$ be a group homomorphism.

(a) Show that if $G = \langle g \rangle$, then $\text{Im}(f) = \langle f(g) \rangle$.

We begin by showing $\text{Im}(f) \subseteq \langle f(g) \rangle$

Suppose $y \in \text{Im}(f)$. Then there exists some $x \in G$ so that $f(x) = y$. Since G is cyclic, we can write $g^k = x$ for some integer k and $g \in G$. Now we can apply f on both sides, giving $f(g^k) = f(x)$. Since f is a homomorphism, $f(g^k) = f(g)^k = f(x) = y$, and $y \in \langle f(g) \rangle$.

Now we show $\langle f(g) \rangle \subseteq \text{Im}(f)$.

Suppose $y \in \langle f(g) \rangle$. Then there exists some $k \in \mathbb{Z}$ so that $f(g)^k = y$. Since f is a homomorphism, $f(g)^k = f(g^k) = y$ and y is in $\text{Im}(f)$.

(b) Let $G \cong H$, show that G is cyclic, if and only if H is cyclic.

We show G is cyclic $\implies$ H is cyclic. The converse is identical.

Let G be cyclic, $\langle g \rangle = G$. And since $G \cong H$, there exists a bijection $f : G \to H$.

In order to show that H is cyclic, we will show that any $h \in H$ can be generated as some power of $f(g)$, or that $H = \langle f(g) \rangle$.

Let $h \in H$. Since f is bijective, there exists a uniques $x \in G$ so that $f(x) = h$. And since g generates G, for some $k \in \mathbb{Z}$, $g^k = x$. If we apply f to both sides of this equality, we get $f(g^k) = f(x)$.

Since f is a homomorphism, $f(g)^k = h$. So any $h \in H$ is some power of $f(g)$, and H is cyclic.

(c) Recall, N is a normal subgroup if $gNg^{-1} = N$ for all $g \in G$. Show that $\ker(f)$ is a normal subgroup of G.

$\ker(f)$ is trivially a subset of G, since by definition each element of $\ker(f)$ must be in G.

First we show $\ker(f)$ is a subgroup, then we will show that it is a normal subgroup.

Let $a, b \in \ker(f)$. Then $f(a) = e = f(b)$. Next note that $f(b^{-1}) = e = f(b)^{-1}$ since f is a homomorphism. Now we note that $f(a)f(b^{-1}) = e$, and again by homomorphism, $f(ab^{-1}) = e$, and $\ker(f)$ is a subgroup of G.

Let $g \in G$ and $h \in \ker(f)$. We want to show that $ghg^{-1} \in \ker(f)$.

Now we have

$$\begin{aligned} f(ghg^{-1}) &= f(g)f(h)f(g^{-1}) && \text{by homomorphism} \\ &= f(g)ef(g)^{-1} && \text{since } h \in \ker(f) \text{ and by homom.} \\ &= f(g)f(g)^{-1} \\ &= e. \end{aligned}$$

Therefore $ghg^{-1} \in \ker(f)$ and $\ker(f)$ is a normal subgroup of G.

4. For any two groups G_1 and G_2, consider the set of all homomorphisms: $Hom(G_1, G_2) := \{f : G_1 \to G_2 : f \text{ is a group homomorphism}\}$.

(a) Show that for any group G, there is a bijective map $\alpha : Hom(\mathbb{Z}, G) \to G$

Choose the map $\alpha : Hom(\mathbb{Z}, G) \to G$ given by $\alpha(f) = f(1)$ for any $f \in Hom(\mathbb{Z}, G)$.

First we show that α is injective. Suppose $\alpha(f) = \alpha(g)$ for some homomorphisms f, g from $\mathbb{Z} \to G$. Then:

$$\begin{aligned} \alpha(f) &= \alpha(g) \\ f(1) &= g(1) \\ f(1)^k &= g(1)^k && \text{For some } k \in \mathbb{Z} \\ f(k) &= g(k) && \text{By Homomorphism.} \end{aligned}$$

And since f, g agree on all inputs from $\mathbb{Z}$, they are equal and α is injective.

Now we show surjectivity. Let $y \in G$. We want to show that there exists some $f : \mathbb{Z} \to G$ so that f is a homomorphism, and $\alpha(f) = y$.

So we choose $f(1) = y$, and for any $k \in \mathbb{Z}$, $f(k) = y^k$ This satisifies our second condition, and we only need to show that f is a homomorphism.

For $a, b \in \mathbb{Z}$, we get $f(a+b) = y^{a+b} = y^a y^b = f(a)f(b)$. So f is a homomorphism and α is surjective

So α is bijective and we are done.

(b) List all elements of $Hom(\mathbb{Z}, S_3)$. How many elements does it have?

As we saw above, a homomorphism from a cyclic group is dependent on where we send the generator, and the image of the homomorphism is generated by the element we map the generator to. So we have our six homomorphisms (all for $x \in \mathbb{Z}$):

$$\begin{aligned}
&\phi_1 : x \mapsto e \\
&\phi_2 : x \mapsto (1\,2)^x \\
&\phi_3 : x \mapsto (1\,3)^x \\
&\phi_4 : x \mapsto (2\,3)^x \\
&\phi_5 : x \mapsto (1\,2\,3)^x \\
&\phi_6 : x \mapsto (1\,3\,2)^x.
\end{aligned}$$

5. Let $\varphi(n)$ denote the Euler's totient function. Give a group theoretic argument to show the famous identity from elementary number theory:

$$\sum_{d|n} \varphi(d) = n.$$

Hint : Let G be a cyclic group of order n. Partition G into subsets S_d of elements of order d. Then count the number of elements in each S_d.

Suppose G is a cyclic group with $|G| = n$, and that G is generated by g. Then for each divisor $d|n$, we have a unique cyclic subgroup S_d of order d. And each subgroup S_d is generated by g^d.

Stuck here :p