## Homework 4 due Wed, Sept 29th by 11am in Gradescope

**Name: Sean Eva**
**GTID: 903466156**
**Collaborators:**
**Outside resources:**

INSERT a "pagebreak" command between each problem (integer numbers). Problem subparts (letter numbered) can be on the same page.

REMOVE all comments (within "textit{}" commands) before submitting solutions.

DO NOT include any identifying information (name, GTID) except on the first/cover page.

1. Let $G$ be a group with subgroup $H$ and $N \triangleleft G$. Let $HN = \{hn \mid h \in H,\ n \in N\}$. Prove that:

   (a) $H \cap N \triangleleft H$

   Let assumptions be as above. Consider $a \in N \cap H$, and $h \in H$, we need to show that $h^{-1}ah \in N \cap H$ which is the same as $h^{-1}ah \in H$ and $h^{-1}ah \in N$. It is trivial to see that $h^{-1}ah \in H$ because each $H$ is a subgroup and is therefore closed under the operation. Alternatively, since $N \triangleleft G$ that means that any conjugation of an element in $N$ with an element of $G$ is still an element of $N$. Therefore, since $H$ is a subgroup of $G$, then $h^{-1}ah \in N$. Since $h^{-1}ah \in N$ and $h^{-1}ah \in H$ then $h^{-1}ah \in H \cap N$ and $H \cap N \triangleleft H$.

   (b) $HN$ is a subgroup of $G$

   Let assumptions be as above. Since $H$ and $N$ are subgroups of $G$, then $e \in H$ and $e \in N$, and therefore, $ee = e \in HN$ which means that $HN$ is nonempty. Consider $x, y \in HN$ such that $x = h_1n_1$ and $y = h_2n_2$. Then, $xy^{-1} = h_1n_1(h_2n_2)^{-1} = h_1n_1n_2^{-1}h_2^{-1}$. Since $N \triangleleft G$, then $n_1n_2^{-1} \in N$ and then $h_1(n_1n_2^{-1})h_2^{-1} \in h_1Nh_2^{-1}$ and $h_1Nh_2^{-1} = h_1h_2^{-1}N$. Since $h_1h_2^{-1} \in H$ then $h_1h_2^{-1} \in HN$ and $xy^{-1} \in HN$ and so $HN$ is a subgroup of $G$.

   (c) $N \subseteq HN$ and $N \triangleleft HN$

   Let assumptions be as above. Since $H$ and $N$ are subsets of $G$ we know that $e \in H$. Therefore, if we consider $hn \in HN$ where $h \in H$ and $n \in N$, and if we consider $h = e$ then $hn = en = n \in N$ which would mean that any $n \in N$ is also an element of $HN$. Therefore, $N \subseteq HN$. Since $HN$ is a subgroup of $G$ we know that all $hn \in HN$ are also in G and since $N$ is normal in G, we know that $(hn)^{-1}n(hn) \in N$ and since this apply to all $hn \in HN$, we know that $N \triangleleft HN$.

   (d) $(HN)/N \simeq H/(H \cap N)$

   Since $N \triangleleft G$, $N \subseteq HN$, and $N \triangleleft HN$ we know that $HN/N$ is a group under right coset multiplication. Let us define $\phi : H \to HN/N$ by $\phi(h) = Nh$. It is easy to see that $\phi(ab) = Nab = NaNb = \phi(a)\phi(b)$ so $\phi$ is a homomorphism. then, let $y \in HN/N$, that is to say that $y = Nhn$ for some $h \in H$ and $n \in N$. Since $N \triangleleft HN$ then all left cosets is also a right coset. This means that we can rewrite $y = Nhn = hnN$ and since $nN = N$ we can rewrite $y = hN = \phi(h)$. Finally, $\operatorname{Ker}\phi = \{h \in H : \phi(h) = N\} = \{h \in H : hN = N\} = \{h \in H : h \in N\} = H \cap N$. Therefore, $H/(H \cap N) \simeq HN/N$ by the first homomorphism theorem.

2. Let $S$ be a nonempty set and consider the group $A(S)$. Let $i$ denote the identity function so that $i(s) = s$ for all $s \in S$. Let $f \in A(S)$. Let $p$ be a prime.

Let $s \in S$. Define *the orbit of* $s$ (under $f$) as $O(s) = \{f^j(s) \mid j \in \mathbb{Z}\}$.

(a) For $s, t \in S$, prove that either $O(s) \cap O(t) = \emptyset$ or $O(s) = O(t)$.

Let assumptions be as above. Let $O(s) = \{s, f^1(s), ..., f^n(s)\}, O(t) = \{t, f^1(t), ..., f^m(t)\}$ where $n, m \in \mathbb{Z}$ such that $f^{n+1}(s) = s, f^{m+1}(t) = t$. If $s = t$ then it is trivial to see that $O(s) = O(t)$. So suppose that $s \neq t$ and let it be that $f^j(s) \neq t$. Then it would suffice then that $O(s) \neq O(t)$ and that $O(s) \cap O(t) = \emptyset$. However, consider that for some $j \in Z, f^j(s) = t$, which implies that $O(t) \subset O(s)$. Then it would follow that for some $b \in \mathbb{Z}$ that $f^{j+b}(s) = s$ as we could say that $n + 1 = j + b$ such as we defined $O(s)$. This then implies that $s \in O(t)$ which would then imply that $O(s) \subset O(t)$ which therefore means that $O(s) = O(t)$.

(b) If $f^3 = i$, show that the orbit of any element of $S$ has one or three elements.

Let assumptions be as above. If $f^3 = i$ then we know that $f^3(s) = s$ which then means that $O(s) = \{s, f^1(s), f^2(s)\}$. Suppose that $s = f^1(s)$ this would then imply also that $f^2(s) = s$ and then $O(s)$ would only have one element. Otherwise, if $s \neq f^1(s)$ and since that $f^3 = i$ we know then that $f^1(s)f^2(s) = f^3(s) = s$. We know $f^1$ cannot be it's own inverse because then that would imply that $f^1(s)f^1(s) = s = f^2(s)$ which would then imply that $f^1(s)f^2(s) = f^3(s) = f^1(s) = s$ which would contradict that $f^1(s) \neq s$ and then show that $O(s)$ has three elements.

(c) Suppose $f^p = i$ but $f \neq i$. If $f^j(s) = s$ for some $s \in S$ and $1 \leq j < p$, prove $f(s) = s$.

Let assumptions be as above. Consider that $f^p(s) = s = f^j(s)$ for $s \in S$ and $1 \leq j < p$. Since $p \nmid j$ we can say that $ap + bj = 1$ for some $a, b \in \mathbb{Z}$. Therefore $f^1(s) = f^{ap+bj}(s) = f^{ap}(f^{bj}(s)) = f^{ap}(s) = s$ which therefore implies that $f^1(s) = s$.

(d) Suppose $f$ has order $p$. Prove that for every $s \in S$, $O(s)$ has either one or $p$ elements.

Let assumptions be as above. We want to show that $O(s) = \{s, f^1(s), f^2(s), ..., f^{p-1}(s)\}$ has either $p$ elements or only one element. Suppose that $s = f(s)$ then that would imply that $s = f(s) = ... = (f^{p-1})$ which would mean that $O(s)$ has only one element. Suppose then $s \neq f(s)$ and we claim that these $p$ elements are distinct. If not then that is to say that for some $f^i(s)$ it is equal to $f^j(s)$ for $0 \leq i < j \leq p - 1$. This would then imply that $f^{j-i}(s) = s$. Let $m = j - i$, then $0 < m \leq p - 1$ and $f^m(s) = s$. However, since $p \nmid m$, we can say that $ap + bm = 1$ some some $a, b \in \mathbb{Z}$. Therefore, $f^1(s) = f^{ap+bm}(s) = f^{ap}(f^{bm}(s)) = f^{ap}(s) = s$, since $f^m(s) = f^p(s) = s$. This contradicts that $f(s) \neq s$. Therefore, $O(s)$ consists of $p$ elements.

3. Let $G$ be a group of order 42.

   (a) Prove that $G$ has a normal subgroup of order 7.

   Let assumptions be as above. Consider the prime factorization of 42, that is $42 = 7^1 * 3^1 * 2^1$. This means that for some element $a \in G$ it is true that $o(a) = 7$ by Cauchy's Theorem. Additionally, since $7 > 3 > 2$, it is true that $(a) \triangleleft G$.

   (b) Now prove that $G$ has a normal subgroup of order 21.

   Let assumptions be as above. Since we know that $G$ has a normal subgroup of order 7, and that $G$ has a subgroup of order 3 we know that. Let us say that $A \triangleleft G$ such that $|A| = 7$ and let us say that $H$ is a subgroup of $G$ such that $|H| = 3$. We know that all left cosets of $A$ are also right cosets of $A$. Then if we used the group $AH$, since $(7, 3) = 1$ and we know $ah = ha$ since all $A$ is normal in $G$. We know from homework 2 number 1 part b that $AH$ is a subgroup of $G$ order $3 * 7 = 21$.

4. Problem #24 in Section 2.5 on page 75.

   (a) Prove that $G$ is a group.

   Let assumptions be as above. In order to show that $G$ is a group, we need to show that it is nonempty, contains an identity, contains inverses, is closed under the operation, and is associative. Let $(a_1, b_1) \in G$. The identity element of $G$ would be $(e_1, e_2)$ where $e_1 \in G_1$ is the identity element in $G_1$ and $e_2 \in G_2$ is the identity element in $G_2$. This means that $(a_1, b_1)(e_1, e_2) = (a_1e_1, b_1e_2) = (a_1, b_1)$. Since $G$ has this element $(e_1, e_2)$ then $G$ is nonempty. Let $(a_1, b_1) \in G$ where $a_1 \in G_1, b_1 \in G_2$, since $G_1, G_2$ are groups, then we know that $a_1^{-1} \in G_1$ and $b_1^{-1} \in G_2$, and then $(a_1^{-1}, b_1^{-1}) \in G$. Therefore, $(a_1, b_1)(a_1^{-1}, b_1^{-1}) = (a_1a_1^{-1}, b_1b_1^{-1}) = (e_1, e_2)$ which is the identity element of $G$. Since $G_1, G_2$ are groups, we know that they are are closed under their operations, that is to say that for some $a_1a_2 = a_3 \in G_1, b_1b_2 = b_3 \in G_2$. This implies that $(a_1, b_1), (a_2, b_2) \in G$ then that $(a_1, b_1)(a_2, b_2) = (a_1a_2, b_1b_2) = (a_3, b_3) \in G$ which means that $G$ is closed under the operation. Lastly, let $(a_1, b_1), (a_2, b_2), (a_3, b_3) \in G$ then $(a_1, b_1)[(a_2, b_2)(a_3, b_3)] = (a_1, b_1)(a_2a_3, b_2b_3) = (a_1a_2a_3, b_1b_2b_3) = (a_1a_2, b_1b_2)(a_3, b_3) = [(a_1, b_1)(a_2, b_2)](a_3, b_3)$ which means that $G$ is associative under the operation. Therefore, $G$ meets all conditions and is thus a group.

   (b) Show that there is a monomorphism $\phi_1$ of $G_1$ into $G$ such that $\phi_1(G_1) \triangleleft G$, given by $\phi(a_1) = (a_1, e_2)$, where $e_2$ is the identity element of $G_2$.

   Let assumptions be as above. Then we first need to show that $\phi_1$ is a monomorphism. We will first show that $\phi_1$ is one to one, consider $a_1, a_2 \in G_2$ such that $\phi_1(a_1) = \phi_1(a_2)$. That is to say that $(a_1, e_2) = (a_2, e_2)$ that implies that $a_1 = a_2$ and therefore, $\phi_1$ is one to one. Now we need to show that $\phi_1$ is a homomorphism. Consider $a_1, a_2 \in G_1$, then $\phi_1(a_1)\phi_1(a_2) = (a_1, e_2)(a_2, e_2) = (a_1a_2, e_2) = \phi(a_1a_2)$ which then means that $\phi_1$ is a homomorhpism and similarly, $\phi_1$ is a monomorphism. Next we want to show that $\phi_1(G_1) \triangleleft G$. Consider $(a_1, e_2) \in \phi_1(G_1)$ and $(a_2, b_2), (a_2^{-1}, b_2^{-1}) \in G$. Then, $(a_2^{-1}, b_2^{-1})(a_1, e_2)(a_2, b_2) = (a_2^{-1}a_1a_2, b_2^{-1}e_2b_2) = (a_2^{-1}a_1a_2, e_2)$ and since $a_2^{-1}a_1a_2 \in G_1$ then $(a_2^{-1}a_1a_2, e_2) \in \phi_1(G_1)$ which means that $\phi_1(G_1) \triangleleft G$.

   (c) Find the similar monomorphism $\phi_2$ of $G_2$ into $G_2$.

   Let assumptions be as above. Let $\phi_2(b_1) = (e_1, b_1)$, where $e_1$ is the identity element of $G_1$.

   (d) Using the mappings $\phi_1, \phi_2$ of Parts (b) and (c), prove that $\phi_1(G_1)\phi_2(G_2) = G$ and $\phi_1(G_1) \cap \phi_2(G_2)$ is the identity element of $G$.

   Let assumptions be as above. Let $x \in \phi_1(G_1) \cap \phi_2(G_2)$, that is to say that $x \in \phi_1(G_1)$ and $x \in \phi_2(G_2)$. Then $x = (a_1, e_2)$ and $x = (e_1, b_1)$ that then means that $(a_1, e_2) = (e_1, b_1)$ and thus, $a_1 = e_1, b_1 = e_2$ which then means that $x = (e_1, e_2)$. Therefore, $\phi_1(G_1) \cap \phi_2(G_2)$ is the identity element of $G$. Now, let $x = (a_1, b_1) \in G$. Then $x = (a_1, b_1)(e_1, e_2) = (a_1e_1, b_1e_2) = (a_1, e_2)(e_1, b_1) = \phi_1(a_1)\phi_2(b_1) \in \phi_1(G_1)\phi_2(G_2)$. Since this applies to any element of $G$, then we know that $\phi_1(G_1)\phi_2(G_2) = G$.

   (e) Prove that $G_1 \times G_2 \simeq G_2 \times G_1$.

   Let assumptions be as above. Define a map $\psi : G_1 \times G_2 \to G_2 \times G_1$ such that $\psi(a_1, b_1) = (b_1, a_1)$ for $a_1 \in G_1, b_1 \in G_2$. We will first show that $\psi$ is a homomorphism. Consider $\psi((a_1, b_1)(a_2, b_2)) = \psi((a_1a_2, b_1b_2)) = (b_1b_2, a_1a_2) = (b_1, a_1)(b_2, a_1) = \psi((a_1, b_1))\psi((a_2, b_2))$ which shows that $\psi$ is a homomorphism. Next we will show that $\psi$ is one to one. Let $\psi((a_1, b_1)) = \psi((a_2, b_2))$, then $(b_1, a_1) = (b_2, a_2)$ which then implies that $b_1 = b_2, a_1 = a_2$ and therefore, $\psi$ is one to one. Lastly, we will show that $\psi$ is onto. Let $x \in G_2 \times G_1$ that is to say that $x = (b_1, a_1)$. Then $\psi((a_1, b_1)) = (b_1, a_1)$ for any $x \in G_2 \times G_1$. Since $\psi$ is an isomorphism, then $G_1 \times G_2 \simeq G_2 \times G_1$.

5. Problem #4 in Section 2.7 on page 87.

(a) $N = \{(a, e_2)|a \in G_1)\}$, where $e_2$ is the unit element of $G_2$, is a normal subgroup of $G$.

Let assumptions be as above. We want to show that $N \triangleleft G$. Consider $(a_1, e_2) \in N$ and $(a_2, b_2), (a_2^{-1}, b_2^{-1}) \in G$. Then, $(a_2^{-1}, b_2^{-1})(a_1, e_2)(a_2, b_2) = (a_2^{-1}a_1a_2, b_2^{-1}e_2b_2) = (a_2^{-1}a_1a_2, e_2)$ and since $a_2^{-1}a_1a_2 \in G_1$ then $(a_2^{-1}a_1a_2, e_2) \in N$ which means that $N \triangleleft G$.

(b) $N \simeq G_1$

Let assumptions be as above. In order for $N \simeq G_1$ we need to define an isomorphism $\phi : N \to G_1$. Consider $\phi((a, e_2)) = a$. Consider $(a, e_2), (b, e_2) \in N$, then $\phi((a, e_2)(b, e_2)) = \phi((ab, e_2)) = ab = \phi((a, e_2))\phi((b, e_2))$. Therefore, $\phi$ is a homomorphism. Now we will show that $\phi$ is one to one. Consider $(a, e_2), (b, e_2) \in N$ such that $\phi((a, e_2)) = \phi(b, e_2)$. Then that is to say that $\phi((a, e_2)) = a = \phi((b, e_2)) = b$ which implies that $\phi$ is one to one. Lastly we will show that $\phi$ is onto. Consider $a \in G_1$, then for $(a, e_2) \in N$ that $\phi((a, e_2)) = a$ which shows that $\phi$ is onto. Therefore, since $\phi$ is isomorphic, then we know that $N \simeq G_1$.

(c) $G/N \simeq G_2$

Let assumptions be as above. Then $G/N = \{[a]|a \in G\} = \{Na|a \in G\}$ and we can show that this is isomorphic to $G_2$ if we can define $\phi : G/N \simeq G_2$. Then define $a \in G/N$ that is to say that $a = (a_1, e_2)(a_2, b_1) = (a_1a_2, b_1)$ and define $\phi(a) = \phi((a_1a_2, b_1)) = b_1$. Consider $\phi((a, b)) = b$. Consider $(a_1, b_1), (a_2, b_2) \in G/N$, then $\phi((a_1, b_1)(a_2, b_2)) = \phi((a_1a_2, b_1b_2)) = b_1b_2 = \phi((a_1, b_1))\phi((a_2, b_2))$. Therefore, $\phi$ is a homomorphism. Now we will show that $\phi$ is one to one. Consider $(a_1, b_1), (a_2, b_2) \in G/N$ such that $\phi((a_1, b_1)) = \phi(a_2, b_2)$. Then that is to say that $\phi((a_1, b_1)) = b_1 = \phi((a_2, e_2)) = b_2$ which implies that $\phi$ is one to one. Lastly we will show that $\phi$ is onto. Consider $b \in G_2$, then for $(a, b) \in N$ that $\phi((a, b)) = b$ which shows that $\phi$ is onto. Therefore, since $\phi$ is isomorphic, then we know that $G/N \simeq G_2$.

6. Let $[a]_n$ denote the equivalence class of $a$ in $\mathbb{Z}_n$. Compute $G/N$ but do NOT submit:

   (a) $G = \mathbb{Z}_4 \times \mathbb{Z}_6$ and $N$ is the cyclic group generated by $([0]_4, [1]_6)$.

   (b) $G = \mathbb{Z}_4 \times \mathbb{Z}_6$ and $N$ is the cyclic group generated by $([2]_4, [3]_6)$.

   (c) $G = \mathbb{Z} \times \mathbb{Z}$ and $N$ is the cyclic group generated by $(1, 1)$.

7. Let $[a]_n$ denote the equivalence class of $a$ in $\mathbb{Z}_n$. Compute but do NOT submit:

   (a) Let $\phi : \mathbb{Z}_{12} \to \mathbb{Z}_3$ be the homomorphism with $\phi([1]_{12}) = [2]_3$. Check that all the conditions of the First Homomorphism Theorem apply, and then write down what all the conclusions are.

   (b) Do the same thing for the Second Homomorphism Theorem and the group $\mathbb{Z}_{24}$ with $H = ([4])$ and $N = ([6])$. Be sure to write down the isomorphism between $H/(H \cap N)$ and $(HN)/N$ explicitly.

   (c) Do the same thing for the Third Homomorphism Theorem and the homomorphism $\phi : \mathbb{Z}_{24} \to \mathbb{Z}_8$ with $\phi([5]_{24}) = [3]_8$ and the subgroup $H = ([4]_{24})$. Be sure to write down the isomorphism between $G/H$ and $(G/K)/(H/K)$ explicitly.