Homework 3 due Wed, Sept 22nd 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 and $N \triangleleft G$. Suppose G is cyclic.

   (a) Prove that G/N is cyclic directly (i.e. from the definition).

   Proof. Let G be a group and $N \triangleleft G$. Suppose that G is cyclic. Since N is normal to G and G is cyclic, we know that G is abelian. Consider $G/N = \{[a] | a \in G\} = \{Na | a \in G\}$ under the relation $ba^{-1} \in N$ and is a group under the operation $[a][b] = [ab]$. Since G is cyclic we can write any element $a \in G$ as $g^i = a \in G$ for some $i \in \mathbb{Z}$. Therefore, we can write $Na = Ng^i \forall a \in G$. Similarly, we then know that $Na = Ng^i = (Ng)^i$ which implies that G/N is cyclic and is generated by Ng. $\square$

   (b) Prove that G/N is cyclic using a homomorphism.

   Proof. $\square$

2. Let G be a group and $N \lhd G$.

(a) Suppose G/N is abelian. Prove $aba^{-1}b^{-1} \in N$ for all $a, b \in G$.

Proof. Let G be a group and $N \lhd G$, and that G/N is abelian. Consider $a, b \in G$, then we have that $(aN)(bN) = (bN)(aN)$. Therefore, $Nab = Nba$, $Naba^{-1}b^{-1} = N$ which then implies that $aba^{-1}b^{-1} \in N$. □

(b) Suppose $aba^{-1}b^{-1} \in N$ for all $a, b \in G$. Prove G/N is abelian.

Proof. Let G be a group and $N \lhd G$. Suppose that $aba^{-1}b^{-1} \in N$ for all $a, b \in G$. In order to show that G/N is abelian, we need to show that $Nab = Nba$ for all $a, b \in G$. Then $(Nb)(Na) = Nba = (eba)N = (Ne)(Nba) = N(Nba) = (Naba^{-1}b^{-1})(Nba) = (Naba^{-1}b^{-1}ba) = Nab = (Na)(Nb)$ which implies that G/N is abelian since $(Nb)(Na) = (Na)(Nb)$. □

3. Let G be a cyclic group of order n. Prove that G has $\phi(n)$ distinct generators (where $\phi(n)$ is the Euler ϕ-function). Specify their form explicitly.

Proof. Let G be a cyclic group of order n. We will prove that the generators for G will be of the form $\{g^s | 0 \leq s < n, gcd(s, n) = 1\}$. In order for this to be a generator, the order of g^s be equal to n. Let us say that the order of g^s is equal to k where $0 < k \leq n$. Because of Lagrange's Theorem, we know that k divides n, so we now need to show that n divides k. From Euclid's lemma, we know that we can rewrite $k = qn + r$ for $qr \in \mathbb{N}$ where $0 \leq r < n$. Then, $e = (g^s)^k = (g^s)^{qn+r} = (g^s)^{qn}(g^s)^r = (g^s)^r = g^{sr}$. If the order of g is n, then we know that $n|sr$, but since the $\gcd(s, n) = 1$, we know that $n|r$. This would then mean that $n \leq r$ or that $r = 0$. Because $0 \leq r < n$ we know that $r = 0$ and that $k = qn$, so then $n|k$ and therefore, we know that $k = n$ since $0 < k \leq n$. Therefore, g^s is a generator of G for $\gcd(s, n) = 1$ which means that the group G has $\phi(n)$ generators. □

4. Let G be a finite group of **even** order with identity e. Prove that there must be an element $a \in G$ with $a \neq e$ and $a^2 = e$.

Proof. Let G be a finite group of even order with identity e. Suppose that $g \in G$ such that $g^2 \neq e$ which would mean that $g \neq g^{-1}$, if we counted these pairs of g, g^{-1}, and we then have the identity elements e. This would mean that we have an odd number of elements. This would then mean that we have one more element $a \in G$ that doesn't have a pairing implying that $a = a^{-1}$ and $a^2 = e$. $\square$

5. Assuming Problem 7 is true, prove that $U_n = \{[a] \in \mathbb{Z}_n \mid (a, n) = 1\}$ is a group under the product $[a][b] = [ab]$.

Proof. In order to prove that U_n is congruent under multiplication modulo n we need to show that it is nonempty, contains an identity, contains inverses, is closed under the operation, and is associative. However, given that problem 7 is true, we only need to prove that the set U_n is closed under the operation and that the operation is associative. Luckily, multiplication modulo n is associative, so then we know that the operation of U_n is associative. Consider $a, b \in U_n$, that means that $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$ which implies that $\gcd(ab, n) = 1$ which therefore means that $ab \in U_n$ and the operation is closed. Therefore, U_n is a group. $\square$

6. Disprove Problem 7 if G is an infinite set with the same properties.

   Consider G is the set of natural numbers under addition. It would be true that $ax = ay$ forces $x = y$ and $ua = wa$ forces $u = w$ for every $a, x, y, u, w \in G$. However, there is no identity element for the natural numbers under the operation of addition and therefore, G is not a group.

7. Let G be a finite nonempty set closed under an associative operation such that $ax = ay$ forces $x = y$ and $ua = wa$ forces $u = w$ for every $a, x, y, u, w \in G$. Prove that G is a group.