MIDTERM SOLUTIONS

(1) (20 pts) Let $Z_n = \langle x \mid x^n = 1 \rangle$.
   (a) Describe all homomorphisms $\varphi : Z_n \to Z_n$.
   (b) Which of these homomorphisms are bijective?
   (c) Show that the set
   
   \[ A = \{ \varphi \mid \varphi : Z_n \to Z_n \text{ is a bijective homomorphism} \} \]

   is a group under function composition, and describe its isomorphism type. (Hint: reviewing your modular arithmetic is advisable)

   **Answer.** (a) A homomorphism between two cyclic groups is determined by the image of the generator. So the viable homomorphisms are generated by
   
   \[ f_a : x \to x^a. \]

   Since $|x^a||x|$, the resulting homomorphism is well-defined. So
   
   \[ H = \{ f_a \mid a = 0, \ldots, n-1 \}. \]

   (b) The map $f_a$ is bijective if and only if $x^a$ is a generator of $Z_n$, which is true if and only if $\gcd(a, n) = 1$.

   (c) Function composition is associative. Given two homomorphisms $f_a, f_b : Z_n \to Z_n$, their composition is the homomorphism
   
   \[ (f_a \circ f_b)(x) = f_a(f_b(x)) = f_a(x^b) = (x^b)^a = x^{ba}. \]

   We showed that if $a$ and $b$ are relatively prime to $n$, then so is $ab$, so $A$ is closed. This also shows that $f_1$ serves as the identity. However, $f_a$ has an inverse exactly when there is some $0 \leq b < n$ such that $ba \equiv 1 \pmod{n}$. As we saw, this is true exactly when $\gcd(n,a) = 1$. So $A$ is closed under inverses. Therefore $A$ is a group, idomorphic to $(\mathbb{Z}/n\mathbb{Z})^\times$.

(2) (10 pts) Recall (from exercises 3.1.40-41) that the **commutator subgroup** of $G$ is

   \[ [G, G] = \{ [x, y] \mid x, y \in G \} \quad \text{where} \quad [x, y] = x^{-1}y^{-1}xy. \]

   You showed that if $N \trianglelefteq G$, then $G/N$ is abelian if and only if $[G, G] \leq N$. Prove that if $[G, G] < H < G$, then $H \leq G$.

   **Proof.** Let $N = [G, G]$. Since $\bar{G} = G/N$ is abelian, every subgroup of $\bar{G}$ is normal. In particular, $\bar{H} = H/N$ is normal in $\bar{G}$. By the lattice isomorphism theorem, this implies that $H \leq G$. \qed

(3) (10 pts) If $G$ and $H$ are finite groups with $\gcd(|G|, |H|) = 1$, show that the only homomorphism $\varphi : G \to H$ is the trivial one.

   **Proof.** Let $\varphi : G \to H$ be a homomorphism. Since $\varphi(G) \cong G/\ker(\varphi)$, we must have $|\varphi(G)|||G|$. But $\varphi(G) \leq H$, and so $|\varphi(G)|||H|$, so $|\varphi(G)| = 1$, so the only homomorphism is the trivial one. \qed
(4) (25 pts) We call a subgroup \( H \leq G \) characteristic in \( G \) if for every automorphism (i.e. bijective homomorphism) \( \varphi : G \to G \), we have \( \varphi(H) = H \) (set-wise mapping, not necessarily identity mapping).

(a) Show that \([G,G]\) is characteristic in \( G \).

(b) Show that if \( H \) is characteristic in \( K \), and \( K \) is normal in \( G \), then \( H \) is normal in \( G \). (Note that this implies that characteristic subgroups are all normal.)

(c) Is every normal subgroup of a finite cyclic group characteristic?

(d) Find an example of a group \( G \) with a normal subgroup \( N \) which is not characteristic in \( G \) (find some automorphism of \( G \) which moves some normal subgroup off of itself).

**Proof.** (a) Let \( \varphi : G \to G \) be an automorphism. Let \( g \) be a generator of \([G,G]\), so that 
\[
g = x^{-1}y^{-1}xy \text{ for some } x, y \in G.
\]
Then 
\[
\varphi(g) = \varphi(x^{-1}y^{-1}xy) = \varphi(x^{-1})\varphi(y^{-1})\varphi(x)\varphi(y) \in [G,G].
\]
So \( \varphi(g) \in [G,G] \) for every generator, so \( \varphi([G,G]) \leq [G,G] \). Similarly, since \( \varphi \) is a bijection, there are some \( a, b \in G \) with \( \varphi(a) = x \) and \( \varphi(b) = y \), so 
\[
g = x^{-1}y^{-1}xy = \varphi(a)^{-1}\varphi(b)^{-1}\varphi(a)\varphi(b) = \varphi(a^{-1})\varphi(b^{-1})\varphi(a)\varphi(b) = \varphi(a^{-1}b^{-1}ab) \in [G,G].
\]
So \( g \in \varphi([G,G]) \) for every generator, so \( \varphi([G,G]) = [G,G] \). Therefore \([G,G]\) is characteristic.

(b) Let \( g \in G \). Since \( gKg^{-1} \leq gKg^{-1} = K \), the conjugation automorphism \( \sigma_g : G \to G \) by \( x \mapsto gxg^{-1} \) (from the homework) is also an automorphism of \( K \). Since \( H \) is setwise fixed by every automorphism of \( K \), \( H = \sigma_g(H) = gKg^{-1} \) and so \( H \) is normal in \( G \).

(c) Yes. If \( \varphi : Z_n \to Z_n \) is a bijective homomorphism and \( H \leq Z_n \), then \( \varphi(H) \leq Z_n \) and \( |\varphi(H)| = |H| \). But in finite cyclic groups, there is exactly one subgroup of every size, so it must be that \( \varphi(H) = H \). So \( H \) is characteristic.

(d) Consider \( D_8 \), and the automorphism \( \varphi : s \mapsto sr \) and \( \varphi : r \mapsto r \). Since \( |\varphi(s)| = |sr| = 2 \), \( |\varphi(r)| = |r| = 4 \) and \( \varphi(r)\varphi(s) = rsr = sr^{-1}r = srr^{-1} = \varphi(s)(\varphi(r))^{-1} \), this is a well-defined bijective homomorphism. However, this automorphism takes the normal subgroup \( \langle s, r^2 \rangle \) to the normal subgroup \( \langle sr, r^2 \rangle \). So \( \langle s, r^2 \rangle \) is normal but not characteristic in \( D_8 \).

\( \square \)

(5) (10 pts) Let \( G \) be a finite group, and recall that a subgroup \( H \leq G \) is maximal if \( H \neq G \), and \( H \) is not contained in any other proper subgroup. Let \( \Phi(G) \) be the set of elements \( g \in G \) satisfying
\[
\text{if } K \leq G \text{ then } \langle K, g \rangle < G
\]
(if \( K \) is a proper subgroup then so is \( \langle K, g \rangle \)). Show that
\[
\Phi(G) = \bigcap_{\text{maximal } H \leq G} H.
\]

**Proof.** Suppose \( g \in \Phi(G) \) and \( H \) is any maximal subgroup of \( G \). Then since \( H < G \), we have \( H \leq \langle H, g \rangle < G \) and so \( \langle H, g \rangle = H \). Therefore \( g \in H \). So \( \Phi(G) \leq \bigcap_{\text{maximal } H \leq G} H \).

Now suppose \( g \in \Phi(G) = \bigcap_{\text{maximal } H \leq G} H \), and let \( K < G \). Since \( K \) is contained in some maximal \( H \), and \( g \in H \), we have \( \langle K, g \rangle \leq H < G \). So \( g \in \Phi(G) \).

So we have equality. \( \square \)
(6) (15 pts) Let $N$ be a normal subgroup of $G$ and suppose $\varphi : G \to H$ is a surjective homomorphism with $\ker(\varphi) \cap N = 1$. Show that for any $x \in N$, we have

(a) $\varphi(C_G(x)) \leq C_H(\varphi(x))$, and
(b) $\varphi(C_G(x)) \geq C_H(\varphi(x))$.

(Hint: For part (b), a return to commutators may be helpful. Namely $[a, b] = 1$ if and only if $a$ and $b$ commute.)

Proof. (a) First, if $g \in C_G(x)$ then

$$\varphi(x) = \varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1},$$

so $\varphi(C_G(x)) \leq C_H(\varphi(x))$. Now suppose $h \in C_H(\varphi(x))$.

(b) Suppose $h \in C_H(\varphi(x))$, and let $g \in G$ with $\varphi(g) = h$. Then

$$\varphi(x) = h\varphi(x)h^{-1} = \varphi(gxg^{-1}).$$

So $gxg^{-1} \in xK$ where $K = \ker(\varphi)$. So $x^{-1}gx^{-1} \in K$. But $gxg^{-1} \in N$ (because $N$ is normal) and so $x^{-1}gxg^{-1} \in N$. But $N \cap K = 1$, so $[x, g] = [x, g^{-1}] = 1$, so $g \in C_G(x)$.

(7) (10 pts) Characterize all finite groups with exactly two conjugacy classes.

Proof. The identity is always in its own conjugacy class, so the other class must contain all other elements. But the class equation tells us that the size of a conjugacy class divides the order of the group. So if $n$ is the order of the group, we need $n = k(n - 1)$ for some integer $k$. The only positive integer solutions to this is when $n = k = 2$. So up to isomorphism, $Z_2$ is the only finite group with exactly two conjugacy classes.