College of the Holy Cross, Fall Semester, 2018
MATH 351, Solutions for Midterm 2
Friday, November 16

I. Let $G = U(20)$ (where the operation is multiplication mod 20), and $N = \langle 9 \rangle$ in G.

(A) (5) How do you know is N a normal subgroup of G?

Solution: G is an abelian group, so *every* subgroup H in G is normal. This follows since if $g \in G$, $h \in H$, then by commutativity $ghg^{-1} = (gg^{-1})h = eh = h \in H$. Therefore H is normal.

(B) (20) Construct a group table for the factor (quotient) group G/N. To which "standard" group is this isomorphic?

Solution: The subgroup $N = \{1, 9\}$. The distinct left cosets are N, $3N = \{3, 27\}$, $11N = \{11, 9\}$, and $13N = \{13, 17\}$. The group table is

	N	$3N$	$11N$	$13N$
N	N	$3N$	$11N$	$13N$
$3N$	$3N$	N	$13N$	$11N$
$11N$	$11N$	$13N$	N	$3N$
$13N$	$13N$	$11N$	$3N$	N

For instance, by the definition of the coset product, $13N \cdot 13N = 169N = 9N$ since $169 \equiv 9 \bmod 20$. However, $9 \in N$, so $9N = N$.

From the form of the table, the group $G/N = U(20)/\langle 9 \rangle$ is non-cyclic of order 4, hence isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$. This relies on Lemma 4.1, or the Fundamental Theorem for finite abelian groups.

II. (A) (10) Let $\alpha : G \to H$ be a group homomorphism. Show that $\ker(\alpha)$ is a normal subgroup of G.

Solution: By definition, $\ker(\alpha) = \{g \in G \mid \alpha(g) = e\}$ (the identity in H). We always have $\alpha(e) = e$ for a group homomorphism, so $e \in \ker(\alpha)$. Moreover, if $a, b \in \ker(\alpha)$, then

$$\alpha(a^{-1}b) = (\alpha(a))^{-1}\alpha(b) = e^{-1}e = e.$$

Hence $a^{-1}b \in \ker(\alpha)$. Since this is true for all $a, b \in \ker(\alpha)$, we have shown $\ker(\alpha)$ is a subgroup of G. Finally, to show that $\ker(\alpha)$ is normal in G, let $g \in G$ and $a \in \ker(\alpha)$. Then

$$\alpha(gag^{-1}) = \alpha(g)\alpha(a)(\alpha(g))^{-1} = \alpha(g)e(\alpha(g))^{-1} = e.$$

Hence $gag^{-1} \in \ker(\alpha)$ whenever $g \in G$ and $a \in \ker(a)$. By part 2 of Theorem 4.3, this shows $\ker(\alpha)$ is normal in G.

(B) (10) State the First Isomorphism Theorem for groups.

Solution: Let $\alpha : G \to H$ be a group homomorphism. Then $G/\ker(\alpha) \cong \alpha(G)$. In words, the image of α (that is, the subgroup $\alpha(G) \subseteq H$) is isomorphic as a group to the factor group $G/\ker(\alpha)$).

(C) (10) Let $G = \mathbb{Z} \times \mathbb{Z}$ and $N = \{(a, 2a) \mid a \in \mathbb{Z}\}$. Using the First Isomorphism Theorem, determine a group isomorphic to G/N.

Solution: Consider the mapping $\alpha : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$ defined by $\alpha(x, y) = y - 2x$. Then α is a group homomorphism since

$$\alpha(x + x', y + y') = y + y' - 2(x + x') = (y - 2x) + (y' - 2x') = \alpha(x, y) + \alpha(x', y').$$

The subgroup N is the kernel of this α since $y - 2x = 0$ if and only if $(x, y) = (x, 2x) \in N$. Moreover α is clearly surjective since given any $z \in \mathbb{Z}$, $\alpha(0, z) = z - 2 \cdot 0 = z$. Therefore, the First Isomorphism Theorem says

$$(\mathbb{Z} \times \mathbb{Z})/N \cong \alpha(\mathbb{Z} \times \mathbb{Z}) = \mathbb{Z}.$$

III. Let G be a group of order 14.

(A) (15) Show that G contains elements of order 2 and elements of order 7. You may use without proof any general facts we know that apply here.

Solution 1: If you recall Theorem 4.15 in the text, then you can use the fact that every group of order 14 is isomorphic to either $\mathbb{Z}_{14}$ or D_{14} (the symmetries of a regular heptagon). In $\mathbb{Z}_{14}$, $|2| = 7$ and $|7| = 2$, so we have elements of both order 2 and order 7. In D_{14}, the rotation $R_{370/7}$ has order 7 and the "flip" across any symmetry line has order 2.

Solution 2: If you didn't recall Theorem 4.15, you could still derive this, essentially by repeating a portion of the proof of that theorem in this special case (possibly taking things we showed later into account). If G is cyclic of order 14 with generator a and $|a| = 14$, then G also has elements of both order 2 and order 7, since $|a^7| = 2$ and $|a^2| = 7$. If G is not cyclic, then by Lagrange's theorem, the orders of the non-identity elements of G can only be 2 or 7. If G has only elements of order 1 and 2, then G must be abelian (Exercise 3.32, which we did earlier). But then G would be an abelian 2-group and the order would be a power of 2. Since 14 is not a power of 2, this case is impossible. Similarly, if G has only elements of order 1 and 7, then since 7 is prime, any element of order 7 generates a subgroup of order 7 which contains the identity and 6 elements of order 7. The intersection of any two distinct subgroups of order 7 can contain only the identity. Therefore, $|G|$ would be congruent to 1 modulo 6. But 14 is not congruent to 1 mod 6. So this case also is impossible. G must contain both elements of order 2 and order 7.

(B) (10) Still assuming G has order 14, any element a of order 7 generates a normal subgroup. If b has order 2, determine all possibilities for $bab = bab^{-1}$.

Solution: (This is one of the steps in the proof of Theorem 4.15 mentioned in Solution 1 of the previous part.) We have $\langle a \rangle$ is normal in G since it has order equal to half the order of G (Theorem 4.1). Hence $bab = bab^{-1}$ must be an element of $\langle a \rangle$, hence $bab = a^i$ for some i. Now we "do it" (i.e. conjugate by b) again. Since b has order 2 in G,

$$a = b^2ab^2 = b(bab)b = ba^ib = (bab)(bab)\cdots(bab) = (bab)^i = a^{i^2}.$$

This implies $i^2 \equiv 1 \bmod 7$, so $i = 1$ or $i = 6$.

IV. (A) (10) Using the Fundamental Theorem, give a complete list of abelian groups of order 72 up to isomorphism.

Solution: We have $72 = 2^3 \cdot 3^2$. Every abelian group of order 72 is isomorphic to one of the following:

$$\begin{gathered}\mathbb{Z}_8 \times \mathbb{Z}_9, \quad \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3,\\ \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_9, \quad \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3\\ \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3.\end{gathered}$$

(B) (5) Let $G = \mathbb{Z}_4 \times \mathbb{Z}_{18}$. To which group in your list from part (A) is G isomorphic?

Solution: Since $18 = 2 \cdot 9$ with $\gcd(2, 9) = 1$, $\mathbb{Z}_{18} \cong \mathbb{Z}_2 \times \mathbb{Z}_9$. This says

$$\mathbb{Z}_4 \times \mathbb{Z}_{18} \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_9.$$

(C) (5) Let $G = \langle a \rangle$ be a cyclic group of order 72. Write $a = b \cdot c$, where b is a 2-element of G and c is a 3-element of G.

Solution: a has order $72 = 8 \cdot 9$, so a^9 has order 8 and a^8 has order 9. The 2-subgroup is generated by a^9 and the 3-subgroup is generated by a^8. We get $a = (a^9)^k \cdot (a^8)^\ell$ when $9k + 8\ell \equiv 1 \bmod 72$. This holds when $k = 1$ and $\ell = 8$. So $b = a^9$ and $c = a^{64} = (a^8)^8$.