MATH 31 – HOMEWORK 7 SOLUTIONS!

due Wednesday, August 16

Instructions: This assignment is due at the *beginning* of class. Staple your work together (do not just fold over the corner). Please write the questions in the correct order. If I cannot read your handwriting, you won't receive full credit.

1. Let X be a set (not necessarily finite) and let $Y \subseteq X$. Recall the group $(\mathcal{P}(X), \triangle)$ from Homework 1. Prove without using any material from Chapter 14 that

$$\mathcal{P}(X)/\mathcal{P}(Y) \cong \mathcal{P}(X \setminus Y).$$

(Don't forget to make sure you verify that $\mathcal{P}(Y)$ is a subgroup!)

Proof: We actually don't need to separately verify that $\mathcal{P}(Y)$ is a subgroup. We will define a map $\varphi : \mathcal{P}(X) \to \mathcal{P}(X \setminus Y)$, show that φ is a surjective homomorphism, check the $\ker(\varphi) = \mathcal{P}(Y)$, and then Theorem 13.1 and the First Isomorphism Theorem (Theorem 13.2) do the rest—Theorem 13.1 will confirm that $\mathcal{P}(Y)$ is a normal subgroup and the First Isomorphism Theorem will give the desired isomorphism.

Before we try to come up with a φ, let's think about what $\mathcal{P}(X)/\mathcal{P}(Y)$ looks like. The elements in this groups are cosets of $\mathcal{P}(Y)$:

$$\mathcal{P}(X)/\mathcal{P}(Y) = \{\mathcal{P}(Y) + S : S \in \mathcal{P}(X)\}$$

Two elements of $\mathcal{P}(X)$ get "compressed" into the same coset of $\mathcal{P}(X)/\mathcal{P}(Y)$ if and only if they differ (with respect to the operation $\triangle$) by a subset of Y. Put another way, two elements S and T of $\mathcal{P}(X)$ get "compressed" to the same coset if $S \setminus Y = T \setminus Y$.

We don't need to realize this to find φ, but it does help.

We know that we want a map whose kernel is $\mathcal{P}(Y)$. In other words, we want $\varphi(S) = \emptyset$ for all $S \subseteq Y$. One such map is that defined by $\varphi(S) = S \setminus Y$ for all $S \in \mathcal{P}(X)$. Let's check if it works.

Is φ a homomorphism? Let $S, T \in \mathcal{P}(X)$. Then,

$$\varphi(S \triangle T) = (S \triangle T) \setminus Y$$

while

$$\varphi(S) \triangle \varphi(T) = (S \setminus Y) \triangle (T \setminus Y).$$

Are these two the same?

$$(S \triangle T) \setminus Y = \{x \in X : x \notin Y \text{ and } x \text{ is in exactly one of } S \text{ and } T\} = (S \triangle T) \cap \overline{Y}$$

and

$$\begin{aligned}(S \setminus Y) \triangle (T \setminus Y) &= \{x \in X : x \text{ is in exactly one of } S \setminus Y \text{ and } T \setminus Y\} \\ &= \overline{Y} \cap \{x \in X : x \text{ is in exactly one of } S \text{ and } T\} \\ &= (S \triangle T) \cap \overline{Y}.\end{aligned}$$

So, φ is a homomorphism.

Moreover, φ is surjective because for any $T \in \mathcal{P}(X \setminus Y)$, it's obvious that $\varphi(T) = T$.

Lastly, $\ker(\varphi) = \{T \in \mathcal{P}(X) : T \setminus Y = \emptyset\} = \{T \in \mathcal{P}(X \setminus Y) : T \subseteq Y = \emptyset\} = \mathcal{P}(Y)$.

By the Theorem 13.1 and the First Isomorphism Theorem, $\mathcal{P}(Y) \lhd \mathcal{P}(X)$ and $\mathcal{P}(X)/\mathcal{P}(Y) \cong \mathcal{P}(X \setminus Y)$.

□

---

2. (13.11) Suppose $H \lhd G$ and $K \lhd G$.

(a) Prove that $G/H \times G/K$ has a subgroup that is isomorphic to $G/(H \cap K)$.

Proof: We probably suspect we need to define a homomorphism somewhere, but where? As we're looking to show that a *subgroup* of $G/H \times G/K$ is isomorphic to all of $G/(H \cap K)$, it is hopeless to try to define a homomorphism whose domain is $G/H \times G/K$. Instead, we'll try the other direction.

There is a remark right below the First Isomorphism Theorem which says that if we find a homomorphism $\varphi : A \to B$ which is not necessarily onto, then although we can't conclude that $A/\ker(\varphi) \cong B$ we can still have that $A/\ker(\varphi) \cong \varphi(A)$. (In other words, $A/\ker(\varphi)$ is isomorphic to the range of φ—if φ is surjective, then the range is all of B, otherwise the range is just some subgroup $\varphi(A) \leq B$.) Given that we're looking for a *subgroup* of $G/H \times G/K$ that is isomorphic to something, this seems to be the way to go.

So, the game-plan is to find a homomorphism $\varphi : G \to (G/H \times G/K)$ whose kernel is $H \cap K$. The input to φ is an element g, and the output is some pair of cosets (Hx, Ky), for some $x, y \in G$. The most natural map that does this is the *natural homomorphism* on each component of the pair. Thus, define

$$\varphi(g) = (Hg, Kg).$$

This map is a homomorphism because

$$\varphi(g_1 g_2) = (H(g_1 g_2), K(g_1 g_2)) = (Hg_1 Hg_2, Kg_1 Kg_2) = (Hg_1, Kg_1)(Hg_2, Kg_2) = \varphi(g_1)\varphi(g_2).$$

The kernel of this map is

$$\begin{aligned}
\ker(\varphi) &= \{g \in G : \varphi(g) = e_{G/H \times G/K}\} \\
&= \{g \in G : \varphi(g) = (H, K)\} \\
&= \{g \in G : (Hg, Kg) = (H, K)\} \\
&= \{g \in G : g \in H \text{ and } g \in K\} \\
&= H \cap K.
\end{aligned}$$

We *did not* show that φ is surjective, and it might not be. So we can only conclude that

$$G/(H \cap K) \cong \varphi(G),$$

but since $\varphi(G)$ is a subgroup of $G/H \times G/K$ (Theorem 12.6(a)), this is enough to prove the theorem. □

(b) Prove that if $G = HK$ then $G/(H \cap K) \cong G/H \times G/K$.

Proof: If we can show that when $G = HK$ the map φ from part (a) is surjective, then we're done. Let $(Hx, Ky) \in G/H \times G/K$ be arbitrary. Our goal is to find $g \in G$ such that

$$\varphi(g) = (Hx, Ky),$$

or equivalently,

$$(Hg, Kg) = (Hx, Ky).$$

As g cannot be both x and y at the same time, we have to be more sneaky. We know we have to use the assumption that $G = HK$ somewhere. Since we've picked some element (Hx, Ky), we might as well apply it here to conclude that

$$x = h_1k_1 \qquad \text{and} \qquad y = h_2k_2$$

for some $h_1, h_2 \in H$ and $k_1, k_2 \in K$. This lets us simplify

$$Hx = H(h_1k_1) = Hk_1$$

and

$$Ky = K(h_2k_2) = (Kh_2)(Kk_2) = (Kh_2)(K) = Kh_2.$$

Hence,

$$(Hx, Ky) = (Hk_1, Kh_2).$$

Now, set $g = h_2k_1$ and see that

$$\begin{aligned}
\varphi(g) &= \varphi(h_2k_1) \\
&= (H(h_2k_1), K(h_2k_1)) \\
&= ((Hh_2)(Hk_1), (Kh_2)(Kk_1)) \\
&= ((H)(Hk_1), (Kh_2)(K) \\
&= (Hk_1, Kh_2) \\
&= (Hx, Ky).
\end{aligned}$$

The First Isomorphism Theorem now tells us that

$$G/(H \cap K) \cong G/H \times G/K.$$

□

---

3. (13.19) Let $\varphi : G \to K$ be a homomorphism. Prove that φ is injective if and only if $\ker(\varphi) = \{e_G\}$.

Proof: To prove an if and only if statement, we need to prove two separate directions.

($\Longrightarrow$) First assume that φ is injective. Let $a \in \ker(\varphi)$. We also know that $e_G \in \ker(\varphi)$. Hence, $\varphi(a) = \varphi(e_G) = e_K$, and injectivity proves that $a = e_G$. Since a was an arbitrary element of $\ker(\varphi)$, we've shown that all elements in the kernel are just e_G.

($\Longleftarrow$) Assume that $\ker(\varphi) = \{e_G\}$. To show injectivity, suppose that a and b are elements of G such that $\varphi(a) = \varphi(b)$. Then,

$$\begin{aligned}
e_K &= \varphi(a)(\varphi(b))^{-1} \\
&= \varphi(a)\varphi(b^{-1}) \\
&= \varphi(ab^{-1}).
\end{aligned}$$

Since $\varphi(ab^{-1}) = e_K$ we know $ab^{-1} \in \ker(\varphi)$. The only element in $\ker(\varphi)$ is e_G! So,

$$ab^{-1} = e_G,$$

implying that $a = b$. This proves injectivity. □

---

4. (13.22) Let $\varphi : G \to K$ be a surjective homomorphism and assume that K is abelian. Show that every subgroup of G containing $\ker(\varphi)$ is normal.

Proof, version 1: Let H be a subgroup of G that contains the kernel. By a fact from class, since φ is a homomorphism and since H contains the kernel, we have that $H = \varphi^{-1}(\varphi(H))$. Since $\varphi(H) \leq K$ and since K is abelian, we have $\varphi(H) \lhd K$. By Theorem 12.6, it follows that $\varphi^{-1}(\varphi(H)) \lhd G$, and thus $H \lhd G$. □

Proof, version 2: The first proof is quick and efficient, but not at all enlightening. It doesn't tell us anything about *why* it's true. Let's prove the statement again in a longer, but more elucidatory, manner.

Let H be a subgroup of G that contains $\ker(\varphi)$ and let $h \in H$. Let $g \in G$ be arbitrary. If H is to be normal, then we must have $ghg^{-1} \in H$. Let's imagine what it would mean for this to go wrong. That is, suppose $ghg^{-1} \notin H$. How could this happen?

We have two elements in G (h and ghg^{-1}). What does φ do to them? Notice that because K is abelian and φ is a homomorphism,

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(h).$$

Thus we have two elements in G, not both in H, but both map to the same element of K.

Let's forget the context of the problem for a moment and explore that. What does it mean to have two elements $a, b \in G$ which map to the same element $\varphi(a) = \varphi(b)$ in K? This implies that $\varphi(ab^{-1}) = e_K$, i.e., that ab^{-1} is in the kernel of φ.

For us, with $a = ghg^{-1}$ and $b = h$, this lets us conclude that $ghg^{-1}h^{-1} \in \ker(\varphi) \subseteq H$. It follows from this that $ghg^{-1} \in H$, proving that $H \lhd G$. □

---

5. (14.4) Let n be a positive integer. Show that every abelian group of order n is cyclic if and only if n is not divisible by the square of any prime.

Proof:

($\Longrightarrow$) We prove this direction by contrapositive. Assume that n is divisible by the square of some prime p, so that we can write

$$n = p^2 q.$$

where p is a prime and q is a positive integer (possibly $q = 1$). One group of order n is $\mathbb{Z}_p \times \mathbb{Z}_{pq}$ which is not cyclic by Theorem 6.1

($\Longleftarrow$) Again the contrapositive seems easier (to me, at least). Suppose that n is a number such that *not every abelian group is cyclic*. Let G be an abelian group of order n that is not cyclic. By the Fundamental Theorem of Finite Abelian Groups (Theorem 14.2), G is isomorphic to the direct product of finitely many nontrivial finite cyclic groups of prime-power order. Since every finite cyclic group is isomorphic to $\mathbb{Z}_m$ for some m, we can write

$$G \cong \mathbb{Z}_{{p_1}^{k_1}} \times \mathbb{Z}_{{p_2}^{k_2}} \times \cdots \times \mathbb{Z}_{{p_\ell}^{k_\ell}}$$

where the p_i are primes (not necessarily distinct), and the k_i are positive integers. Note that this implies

$$n = {p_1}^{k_1}{p_2}^{k_2} \cdots {p_\ell}^{k_\ell}.$$

Since we seek to show that n is divisible by the square of some prime, we only need to show that $k_i \geq 2$ for some i, or that $p_i = p_j$ for some non-equal i and j.

As G is not cyclic, Theorem 6.1 implies that there is some pair r, s such that $|\mathbb{Z}_{{p_r}^{k_r}}|$ and $|\mathbb{Z}_{{p_s}^{k_s}}|$ are *not* relatively prime. This implies that ${p_r}^{k_r}$ and ${p_s}^{k_s}$ share some non-trivial factor. Because p_r and p_s are prime, this is only possible if $p_r = p_s$.

This implies that n is divisible by ${p_r}^2$, completing the proof. □
