Math 581 Problem Set 8 Solutions

1. Prove that a group G is abelian if and only if the function $\varphi : G \to G$ given by $\varphi(g) = g^{-1}$ is a homomorphism of groups. In this case, show that φ is an isomorphism.

Proof: First suppose that G is abelian. Let $g, h \in G$. Then we have $\varphi(gh) = (gh)^{-1} = h^{-1}g^{-1} = g^{-1}h^{-1} = \varphi(g)\varphi(h)$ where we used G is abelian to conclude $h^{-1}g^{-1} = g^{-1}h^{-1}$. Thus, φ is a homomorphism.
Now suppose φ is a homomorphism. Let $g, h \in G$. Then we have $\varphi(g^{-1}h^{-1}) = \varphi(g^{-1})\varphi(h^{-1})$, i.e., $(g^{-1}h^{-1})^{-1} = gh$. Thus, we have $hg = gh$. Since g and h were arbitrary, this shows G is abelian.
To see φ is an isomorphism, we just need to show it is bijective. Let $g \in G$. Then $\varphi(g^{-1}) = g$ and so φ is surjective. Suppose $\varphi(g) = e_G$. Then $g^{-1} = e_G$, i.e., $g = e_G$. Thus φ is injective as well. ■

2. Let $\varphi : G \to H$ be a homomorphism of groups.
(a) Let G_1 be a subgroup of G. Prove that $\varphi(G_1)$ is a subgroup of H. In particular, this shows that $\varphi(G)$ is a subgroup of H.

Proof: Recall that $\varphi(e_G) = e_H$. Since G_1 is a subgroup, $e_G \in G_1$ and thus $e_H \in \varphi(G_1)$ so it is a nonempty set. Let $h_1, h_2 \in \varphi(G_1)$. There exists g_1 and g_2 in G_1 such that $\varphi(g_i) = h_i$ for $i = 1, 2$. We have $h_1h_2 = \varphi(g_1)\varphi(g_2) = \varphi(g_1g_2)$. Thus, $h_1h_2 \in \varphi(G_1)$ and so it the set is closed under multiplication. Finally, recall that $\varphi(g_1^{-1}) = \varphi(g_1)^{-1}$, and so $h_1^{-1} \in \varphi(G_1)$. Hence, $\varphi(G_1)$ is a subgroup of H. ■

(b) Let H_1 be a subgroup of H. Prove that the set $\varphi^{-1}(H_1) = \{g \in G : \varphi(g) \in H_1\}$ is a subgroup of G. In particular, this shows that $\varphi^{-1}(H)$ is a subgroup of G.

Proof: Note that since H_1 is a subgroup of H we have $e_H \in H_1$. We know that $\varphi(e_G) = e_H$, so $e_G \in \varphi^{-1}(H_1)$ and thus it is a nonempty set. Let $a, b \in \varphi^{-1}(H_1)$, i.e., $\varphi(a), \varphi(b) \in H_1$. Since H_1 is a subgroup, we know $\varphi(a)\varphi(b)$ and $\varphi(a)^{-1}$ are both in H_1. Using that φ is a homormophism we get that $\varphi(ab)$ and $\varphi(a^{-1})$ are both in H_1, i.e., $ab \in \varphi^{-1}(H_1)$ and $a^{-1} \in \varphi^{-1}(H_1)$. Thus, it is a subgroup. ■

3. (a) Prove that $H = \left\{ \begin{pmatrix} 1-n & -n \\ n & 1+n \end{pmatrix} \mid n \in \mathbb{Z} \right\}$ is a group under matrix

multiplication.

Proof: Observe that any matrix in H has determinant 1 and hence is an element of $\mathrm{GL}_2(\mathbb{Z})$. Since we have seen $\mathrm{GL}_2(\mathbb{Z})$ is a group, we need only check that H is a subgroup of this group to see it is a group. It is clear that H is nonempty as $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \in H$. Let $\begin{pmatrix} 1-m & -m \\ m & 1+m \end{pmatrix}$ and $\begin{pmatrix} 1-n & -n \\ n & 1+n \end{pmatrix}$ be in H. Observe that

$$\begin{pmatrix} 1-m & -m \\ m & 1+m \end{pmatrix} \begin{pmatrix} 1-n & -n \\ n & 1+n \end{pmatrix} = \begin{pmatrix} 1-(m+n) & -(m+n) \\ m+n & 1+(m+n) \end{pmatrix} \in H$$

and

$$\begin{pmatrix} 1-n & -n \\ n & 1+n \end{pmatrix}^{-1} = \begin{pmatrix} 1+n & n \\ -n & 1-n \end{pmatrix} = \begin{pmatrix} 1-(-n) & -(-n) \\ -n & 1+(-n) \end{pmatrix} \in H.$$

Thus H is a subgroup of $\mathrm{GL}_2(\mathbb{Z})$ and hence is a group itself. ■

(b) Prove that $H \cong \mathbb{Z}$.

Proof: Define $\varphi : H \to \mathbb{Z}$ by $\begin{pmatrix} 1-n & -n \\ n & 1+n \end{pmatrix} \mapsto n$. The fact that we have

$$\begin{pmatrix} 1-m & -m \\ m & 1+m \end{pmatrix} \begin{pmatrix} 1-n & -n \\ n & 1+n \end{pmatrix} = \begin{pmatrix} 1-(m+n) & -(m+n) \\ m+n & 1+(m+n) \end{pmatrix} \in H$$

makes it clear that φ is in fact a homomorphism. It is also clear that φ is a surjective map. To see it is injective, suppose $\begin{pmatrix} 1-n & -n \\ n & 1+n \end{pmatrix}$ maps to 0. Then we must have $n = 0$ and so $\begin{pmatrix} 1-n & -n \\ n & 1+n \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = e_H$. Thus the kernel is just the identity element and hence the map is injective. ■

4. List all the distinct left cosets of $H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\}$ in S_3. What is $[S_3 : H]$? Is H a normal subgroup of S_3?

There are 3 distinct cosets of H, they are

$$\begin{aligned} eH &= \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} H = \left\{ \begin{pmatrix}1&2&3\\1&2&3\end{pmatrix}, \begin{pmatrix}1&2&3\\2&1&3\end{pmatrix} \right\} \\ \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} H &= \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} H = \left\{ \begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}, \begin{pmatrix}1&2&3\\2&3&1\end{pmatrix} \right\} \\ \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} H &= \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} H = \left\{ \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix}, \begin{pmatrix}1&2&3\\3&1&2\end{pmatrix} \right\}. \end{aligned}$$

Since there are 3 distinct cosets, we know $[S_3 : H] = 3$. To see that H is in fact not a normal subgroup, just observe that

$$\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix} = \begin{pmatrix}1&2&3\\1&3&2\end{pmatrix} \notin H.$$

5. This is a series of finite group questions. They are not necessarily related. **(a)** A group has fewer then 100 elements and subgroups of orders 10 and 25. What is the order of G?

We know by Lagrange's theorem that $10 \mid |G|$ and $25 \mid |G|$. Thus, the least common multiple of 10 and 25, namely 50 divides $|G|$. However, since $|G| < 100$, there are no other common multiples of 10 and 25 that could be $|G|$. Thus, $|G| = 50$.

(b) If H and K are subgroups of a finite group G, prove that $|H \cap K|$ is a common divisor of $|H|$ and $|K|$.

Recall we proved in class that $H \cap K$ is a subgroup of H and K. Therefore, Lagrange's theorem gives $|H \cap K| \mid |H|$ and $|H \cap K| \mid |K|$.

(c) If G is a group with more then 1 element and G has no proper subgroups, prove that G is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ for some prime p.

Proof: Let $a \in G$ be such that $a \neq e_G$ (since we know $|G| > 1$ we can choose such an a). Consider the subgroup $\langle a \rangle$. Since G has no proper subgroups it must be that $G = \langle a \rangle$. Thus G is a cyclic group and hence isomorphic to $\mathbb{Z}/n\mathbb{Z}$ for some positive integer n. However, we proved in class that for any proper divisor m of n the set $\langle a^m \rangle$ is a proper subgroup of $\langle a \rangle$. Since there can be no such subgroups, there can be no such proper divisor. Thus n is

prime and so $G \cong \mathbb{Z}/p\mathbb{Z}$ for some prime p. ■

(d) If p and q are primes, show that every proper subgroup of a group of order pq is cyclic.

Proof: By Lagrange's theorem every proper subgroup must be of order 1, p, or q. If it is of order 1 then clearly it is just $\langle e_G \rangle$. Otherwise, it is a group of prime order and hence is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ or $\mathbb{Z}/q\mathbb{Z}$, both of which are cyclic. ■

6. Let $a \in G$ be fixed, and define $\varphi : G \to G$ by $\varphi(x) = axa^{-1}$. Prove that φ is a homomorphism. Under what conditions is φ an isomorphism?

Proof: Let $g, h \in G$. Observe that

$$\begin{aligned} \varphi(gh) &= agha^{-1} \\ &= age_Gha^{-1} \\ &= aga^{-1}aha^{-1} \\ &= \varphi(g)\varphi(h). \end{aligned}$$

Thus, φ is a homomorphism. To see that φ is surjective, observe that $\varphi(a^{-1}ga) = g$. Suppose that $g \in \ker \varphi$. Thus, $\varphi(g) = e_G$, i.e., $aga^{-1} = e_G$. However, solving this for g we obtain $g = e_G$. Thus, φ is injective. Hence, φ is always an isomorphism. ■

7. Show that $\varphi : \mathbb{R} \to \mathbb{C}^\times$, $\varphi(t) = \cos(2\pi t) + i \sin(2\pi t)$ is a homomorphism. What are its kernel and image?

Proof: Observe we can write $\varphi(t) = e^{2\pi i t}$. Let $s, t \in \mathbb{R}$. Then we have

$$\begin{aligned} \varphi(s+t) &= e^{2\pi i(s+t)} \\ &= e^{2\pi is}e^{2\pi it} \\ &= \varphi(s)\varphi(t). \end{aligned}$$

Thus, φ is a homomorphism. The image of φ is precisely the set of complex numbers that can be written in the form $e^{2\pi it}$ for some $t \in \mathbb{R}$. In Math 580 we saw this is the circle of radius 1 in the complex plane. The kernel consists of those t such that $e^{2\pi it} = 1$. This is the set of real numbers so that $\cos(2\pi t) = 1$ but $\sin(2\pi t) = 0$, i.e., it is the integers. Thus, $\ker \varphi = \mathbb{Z}$.

■

8. Consider the subgroup $N = \mathbb{Z}$ of the additive group $\mathbb{Q}$.
(a) What does it mean for $r \equiv s (\mathrm{mod}\, N)$, i.e., for the cosets $r+N = s+N$?

It means that $r - s \in \mathbb{Z}$.

(b) Show that for $m, n \in \mathbb{Z}$, one has $m + N = n + N$.

This is clear since $m - n \in \mathbb{Z}$.

(c) $\frac{1}{2} + N =$?

$$\frac{1}{2} + N = \{r \in \mathbb{Q} : r - \frac{1}{2} \in \mathbb{Z}\} = \{0, \pm\frac{1}{2}, \pm 1, \pm\frac{3}{2}, \pm 2, \pm\frac{5}{2}, \dots\}$$

(d) How many distinct cosets are there?

There are infinitely many distinct cosets. For example, the cosets $\frac{1}{p} + \mathbb{Z}$ are all distinct for each prime p. To see this, suppose $\frac{1}{p} + \mathbb{Z} = \frac{1}{q} + \mathbb{Z}$ where p and q are primes. This means that $\frac{1}{p} - \frac{1}{q} \in \mathbb{Z}$, i.e., $\frac{q-p}{qp} \in \mathbb{Z}$. However, since $p \neq q$ this is not 0 and we have $pq > p - q$ so this is not an integer. Since there are infinitely many primes, there are infinitely many cosets.

9. Consider the additive group $G = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$. Set $N = \langle (1, 2) \rangle$.
(a) What is $|N|$? What about $[G : N]$?

Note that $N = \{(1, 2), (2, 4), (3, 6) = (0, 0)\}$. Thus, $|N| = 3$. Since $|G| = 18$, we have $[G : N] = 18/3 = 6$.

(b) Compute the distinct left cosets that comprise G/N.

Note that since we know there are 6 left cosets, once we find 6 distinct cosets we are done. Any other left coset must then be one of the 6 we've found.

Thus, we have

$$\begin{aligned}
(0,0)+N &= \{(0,0),(1,2),(2,4)\}\\
(1,0)+N &= \{(1,0),(2,2),(0,4)\}\\
(2,0)+N &= \{(2,0),(0,2),(1,4)\}\\
(0,1)+N &= \{(0,1),(1,3),(2,5)\}\\
(0,3)+N &= \{(0,3),(1,5),(2,1)\}\\
(0,5)+N &= \{(0,5),(1,1),(2,3)\}
\end{aligned}$$

(c) Prove that N is a normal subgroup of G.

Proof: Since G is an abelian group all the subgroups are normal. ■

(d) Write out an addition table for G/N.

Recall that $[(a,b)+N]+[(c,d)+N] = (a+c,b+d)+N$. Using this we have:

+	(0,0) + N	(1,0) + N	(2,0) + N	(0,1) + N	(0,3) + N	(0,5) + N
(0,0) + N	(0,0) + N	(1,0) + N	(2,0) + N	(0,1) + N	(0,3) + N	(0,5) + N
(1,0) + N	(1,0) + N	(2,0) + N	(0,0) + N	(0,5) + N	(0,1) + N	(0,3) + N
(2,0) + N	(2,0) + N	(0,0) + N	(1,0) + N	(0,3) + N	(0,5) + N	(0,1) + N
(0,1) + N	(0,1) + N	(0,5) + N	(0,3) + N	(0,5) + N	(1,0) + N	(0,0) + N
(0,3) + N	(0,3) + N	(0,1) + N	(0,5) + N	(1,0) + N	(0,0) + N	(2,0) + N
(0,5) + N	(0,5) + N	(0,3) + N	(0,1) + N	(0,0) + N	(2,0) + N	(1,0) + N

Note we have used for example that $(1,4)+N = (2,0)+N$ when filling out the table. It is important to only have elements of the group G/N in the table.

(e) What familiar group is G/N?

We stated in class (but did not prove) that any group of order 6 is either $\mathbb{Z}/6\mathbb{Z}$ or S_3. Since our group has order 6 and is abelian, it must be isomorphic to $\mathbb{Z}/6\mathbb{Z}$.