Homework 6 Solutions

<u>Section 10</u>:

35. Show that there are the same number of left cosets as right cosets of a subgroup H of a group G; that is, exhibit a one-to-one map of the collection of left cosets onto the collection of right cosets.

Proof. Let G be a group and $H \leq G$. We first show that, for $g, g' \in G$, if $gH = g'H$, then $Hg^{-1} = H(g')^{-1}$.

Fix $g, g' \in G$ such that $gH = g'H$. Given $a \in Hg^{-1}$, we have $a = hg^{-1}$ for some $h \in H$. Then $a^{-1} = (hg^{-1})^{-1} = gh^{-1} \in gH = g'H$ (since H is a group). So $a^{-1} = g'h'$ for some $h' \in H$. But then $a = (a^{-1})^{-1} = (g'h')^{-1} = (h')^{-1}(g')^{-1} \in H(g')^{-1}$ (again, since H is a group). This shows that $Hg^{-1} \subseteq H(g')^{-1}$. A similar argument shows that $H(g')^{-1} \subseteq Hg^{-1}$, so $H(g')^{-1} = Hg^{-1}$.

In light of the fact that $Hg^{-1} = H(g')^{-1}$ if $gH = g'H$, we may define a map

$$\mu : \{\text{left cosets of } H\} \to \{\text{right cosets of } H\}$$

by $\mu(gH) = Hg^{-1}$. We claim that μ is a bijection. μ is clearly surjective, since every element of G has an inverse, so

$$Hg = H(g^{-1})^{-1} = \mu(g^{-1}H).$$

Showing that μ is injective is equivalent to our work to show that μ is well-defined (just in reverse), so we omit the proof here. So μ is a bijection and hence the number of left cosets of H is the same as the number of right cosets of H (or, to be more accurate, the *cardinality* of the set of left cosets of H is the same as the *cardinality* of the set of right cosets of H) □

<u>Section 11</u>:

16. Are the groups $\mathbb{Z}_2 \times \mathbb{Z}_{12}$ and $\mathbb{Z}_4 \times \mathbb{Z}_6$ isomorphic? Why or why not?

Solution. Yes, $\mathbb{Z}_2 \times \mathbb{Z}_{12} \simeq \mathbb{Z}_4 \times \mathbb{Z}_6$.

Proof. As shown in class, $\mathbb{Z}_{12} \simeq \mathbb{Z}_3 \times \mathbb{Z}_4$ and $\mathbb{Z}_6 \simeq \mathbb{Z}_2 \times \mathbb{Z}_3$. Hence, by the Fundamental Theorem of Finitely Generated Abelian Groups,

$$\mathbb{Z}_2 \times \mathbb{Z}_{12} \simeq \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \simeq \mathbb{Z}_4 \times \mathbb{Z}_6\,.$$

□

18. Are the groups $\mathbb{Z}_8 \times \mathbb{Z}_{10} \times \mathbb{Z}_{24}$ and $\mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{40}$ isomorphic? Why or why not?

Solution. No, $\mathbb{Z}_8 \times \mathbb{Z}_{10} \times \mathbb{Z}_{24} \not\simeq \mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{40}$.

Proof. Rewriting each in the format of the Fundamental Theorem of Finitely Generated Abelian Groups, we have

$$\mathbb{Z}_8 \times \mathbb{Z}_{10} \times \mathbb{Z}_{24} \simeq \mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

and

$$\mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_{40} \simeq \mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_5\,.$$

By uniqueness in the Fundamental Theorem of Finitely Generated Abelian Groups, they are not isomorphic. □

24. Find all abelian groups, up to isomorphism, of order 720.
Solution. $720 = 2^4 3^2 5^1$

$$\mathbb{Z}_{16} \times \mathbb{Z}_9 \times \mathbb{Z}_5$$
$$\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_9 \times \mathbb{Z}_5$$
$$\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$$
$$\mathbb{Z}_{16} \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$
$$\mathbb{Z}_2 \times \mathbb{Z}_8 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$
$$\mathbb{Z}_4 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$
$$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_5$$

29. a. Let p be a prime number. Fill in the second row of the table to give the number of abelian groups of order p^n, up to isomorphism.

n	2	3	4	5	6	7	8
number of groups	2	3	5	7	11	15	22

b. Let p, q, and r be distinct prime numbers. Use the table you created to find the number of abelian groups, up to isomorphism, of the given order.

i. $p^3 q^4 r^7$

Solution. $3 \cdot 5 \cdot 15 = 225$.

ii. $(qr)^7$

Solution. $(qr)^7 = q^7 r^7$. $15 \cdot 15 = 225$.

iii. $q^5 r^4 q^3$

Solution. $q^5 r^4 q^3 = q^8 r^4$. $22 \cdot 5 = 110$.

39. Let G be an abelian group. Show that the elements of finite order in G form a subgroup. This subgroup is called the **torsion subgroup** of G.

Proof. Let T be the set of elements of G with finite order. Now, the identity element e of G has order 1, so $e \in T$. Suppose $a, b \in T$. Then a and b have finite orders, say m & n, respectively. Since G is abelian, $(ab)^{mn} = (a^m)^n (b^n)^m = e^n e^m = e$. Hence ab has finite order and so $ab \in T$. Thus T is closed under the operation of G. Finally, $(a^{-1})^m = (a^{-1})^m e = (a^{-1})^m a^m = e^m = e$, so that a^{-1} has finite order. This implies that $a^{-1} \in T$. We have shown that T is a subgroup of G. □

40. Find the order of the torsion subgroup of $\mathbb{Z}_4 \times \mathbb{Z} \times \mathbb{Z}_3$; of $\mathbb{Z}_{12} \times \mathbb{Z} \times \mathbb{Z}_{12}$.

Solution. If $(a, b, c) \in \mathbb{Z}_4 \times \mathbb{Z} \times \mathbb{Z}_3$ with $b \neq 0$ and $n \in \mathbb{Z}^+$, then $n(a, b, c) = (na, nb, nc) \neq (0, 0, 0)$. Hence, if $(a, b, c) \in \mathbb{Z}_4 \times \mathbb{Z} \times Z_3$ has finite order, then $b = 0$. Furthermore, for $(a, 0, c) \in \mathbb{Z}_4 \times \{0\} \times \mathbb{Z}_3$, $12(a, 0, c) = (12a, 0, 12c) = (0, 0, 0)$. Hence every element of $\mathbb{Z}_4 \times \{0\} \times \mathbb{Z}_3$ has finite order. Therefore the elements of finite order in $\mathbb{Z}_4 \times \mathbb{Z} \times \mathbb{Z}_3$ are exactly those elements in $\mathbb{Z}_4 \times \{0\} \times \mathbb{Z}_3$. There are 12 such elements.

Simlarly, the elements of $\mathbb{Z}_{12} \times \mathbb{Z} \times \mathbb{Z}_{12}$ with finite order are exactly those in $\mathbb{Z}_{12} \times \{0\} \times \mathbb{Z}_{12}$. There are 144 such elements.

41. Find the torsion subgroup of the multiplicative group $\mathbb{R}^*$ of nonzero real numbers.

    Solution. The identity element of the multiplicative group $\mathbb{R}^*$ is 1, so the torsion subgroup of $\mathbb{R}^*$ is the set of all real numbers x such that $x^n = 1$ for some $n \in \mathbb{Z}^+$. Therefore the torsion subgroup of $\mathbb{R}^*$ is $\{-1, 1\}$.

42. Find the torsion subgroup T of the multiplicative group $\mathbb{C}^*$ of nonzero complex numbers.

    Solution. The identity element of the multiplicative group $\mathbb{C}^*$ is 1, so then T is the set of all complex numbers z such that $z^n = 1$ for some $n \in \mathbb{Z}^+$, or in other words, the complex roots of unity.

49. Find a counterexample of Exercise 47 with the hypothesis that G is abelian omitted. [Exercise 47: Let G be an abelian group. Let H be the subset of G consisting of the identity e together with all elements of G of order 2. Show that H is a subgroup of G.]

    Solution. Consider $G = S_3$. Then the elements of order 2 are $(1,2)$, $(1,3)$, and $(2,3)$. So $H = \{\iota, (1,2), (1,3), (2,3)\}$. It is clear that H is not a subgroup of S_3, since it is not closed under permutation multiplication. For instance, $(1,2)(2,3) = (1,2,3) \notin H$.

Section 13:

2. Let $\phi : \mathbb{R} \to \mathbb{Z}$ under addition be given by $\phi(x) = \lfloor x \rfloor$. Determine whether ϕ is a homomorphism.

    Solution. No, ϕ is not a homomorphism.

    Proof. $\frac{1}{2} \in \mathbb{R}$ and $\phi(\frac{1}{2} + \frac{1}{2}) = \phi(1) = 1 \neq 0 = 0 + 0 = \phi(\frac{1}{2}) + \phi(\frac{1}{2})$. □

12. Let M_n be the additive group of all $n \times n$ matrices with real entries, and let $\mathbb{R}$ be the additive group of real numbers. Let $\phi(A) = \det(A)$, the determinant of A for $A \in M_n$. Determine whether ϕ is a homomorphism.

    Solution. No, ϕ is not a homomorphism for $n > 1$. [If $n = 1$, then ϕ actually is a homomorphism, but we omit the proof here.]

    Proof. Consider the identity matix $I_n \in M_n$. If $n > 1$, then
    $\phi(I_n + I_n) = \phi(2I_n) = \det(2I_n) = 2^n \neq 2 = 1 + 1 = \det(I_n) + \det(I_n) = \phi(I_n) + \phi(I_n)$. □

13. Let M_n and $\mathbb{R}$ be as in Exercise 12. Let $\phi(A) = \operatorname{tr}(A)$ for $A \in M_n$, where the **trace** $\operatorname{tr}(A)$ is the sum of the elements on the main diagonal of A, from the upper-left to the lower-right corner.

    Solution. Yes, ϕ is a homomorphism.

    Proof. Let $A = (a_{i,j})_{1\le i,j\le n}$ and $B = (b_{i,j})_{1\le i,j\le n}$ be $n \times n$ matrices and set $c_{i,j} = a_{i,j} + b_{i,j}$ for $1 \le i, j \le n$, so that $C := (c_{i,j})_{1\le i,j\le n} = A + B$. Then

$$\phi(A+B) = \operatorname{tr}(A+B) = \operatorname{tr}(C) = \sum_{i=1}^{n} c_{i,i} = \sum_{i=1}^{n} (a_{i,i}+b_{i,i}) = \sum_{i=1}^{n} a_{i,i} + \sum_{i=1}^{n} b_{i,i} = \operatorname{tr}(A) + \operatorname{tr}(B) = \phi(A) + \phi(B).$$

□

14. Let $\mathbb{R}$ be the additive group of real numbers and let $\phi : GL_n(\mathbb{R}) \to \mathbb{R}$ be given by $\phi(A) = \operatorname{tr}(A)$, where $\operatorname{tr}(A)$ is defined in Exercise 13.

    Solution. No, ϕ is not a homomorphism.

    Proof. Consider the identity matrix $I_n \in GL_n(\mathbb{R})$. Then

$$\phi(I_n I_n) = \phi(I_n) = \operatorname{tr}(I_n) = n \neq 2n = \operatorname{tr}(I_n) + \operatorname{tr}(I_n) = \phi(I_n) + \phi(I_n).$$

□

21. Find $\text{Ker}(\phi)$ and $\phi(14)$ for $\phi : \mathbb{Z}_{24} \to S_8$, where $\phi(1) = (2,5)(1,4,6,7)$.

Solution. $(2,5)(1,4,6,7)$ has order $\text{lcm}(2,4) = 4$, so $\text{Ker}(\phi) = \{0, 4, 8, 12, 16, 20\}$ and

$$\phi(14) = \phi(1)^{14} = [(2,5)(1,4,6,7)]^{14} = [(2,5)(1,4,6,7)]^{12}[(2,5)(1,4,6,7)]^2 = (1,6)(4,7).$$

41. Give an example of a nontrivial homomorphism $\phi : D_4 \to S_3$ or explain why no such homomorphism exists.

Solution. Noting that D_4 is a subgroup of S_4, we let $\phi(\sigma) = (1,2)$ for all odd $\sigma \in D_4$ and $\phi(\sigma) = \iota$ for all even $\sigma \in D_4$. This map mimics $\text{sgn} : S_4 \to \{-1, 1\}$, but uses $\{(1,2), \iota\}$ in place of $\{-1, 1\}$. As we did with sgn, we omit the proof that ϕ is a homomorphism. [Note: In fact, if σ is any of the 3 transpositions of S_3, we can define a homomorphism ϕ by any of the 3 following assignments:

$$\phi((2,4)) = \sigma \qquad \phi((1,2,3,4)) = \sigma \tag{1}$$
$$\phi((2,4)) = \sigma \qquad \phi((1,2,3,4)) = \iota \tag{2}$$
$$\phi((2,4)) = \iota \qquad \phi((1,2,3,4)) = \sigma \tag{3}$$

Here we use the facts that ϕ is determined by where it sends generators and that $(2,4)$ and $(1,2,3,4)$ generate D_4. Of course, you would still need to show that these maps are well-defined (since it is possible to write each element of D_4 in more than one way as a product of copies of $(2,4)$ and $(1,2,3,4)$).]

47. Show that any group homomorphism $\phi : G \to G'$ where $|G|$ is prime must either be the trivial homomorphism or a one-to-one map.

Proof. Let $\phi : G \to G'$ be a group homomorphism and suppose $|G| = p$ for some prime p. We proved in class that $\text{Ker}(\phi)$ is a subgroup of G, so by Lagrange's Theorem, $|\text{Ker}(\phi)|$ divides $|G| = p$. Hence we must have either $|\text{Ker}(\phi)| = 1$ or $|\text{Ker}(\phi)| = p$, i.e. either $\text{Ker}(\phi) = \{e\}$ or $\text{Ker}(\phi) = G$. It follows that either ϕ is one-to-one or the trivial homomorphism, respectively. $\square$

49. Show that if G, G', and G'' are groups and if $\phi : G \to G'$ and $\gamma : G' \to G''$ are homomorphisms, then the composite map $\gamma\phi : G \to G''$ is a homomorphism.

Proof. Let G, G', and G'' be groups and suppose $\phi : G \to G'$ and $\gamma : G' \to G''$ are homomorphisms. Given $g, h \in G$, we use the fact that γ and ϕ are homomorphisms:

$$\gamma\phi(gh) = \gamma(\phi(gh)) = \gamma(\phi(g)\phi(h)) = \gamma(\phi(g))\gamma(\phi(h)) = \gamma\phi(g)\gamma\phi(h).$$

Therefore $\gamma\phi$ is a homomorphism. $\square$

55. Let G be a group, $h \in G$, and $n \in \mathbb{Z}^+$. Let $\phi : \mathbb{Z}_n \to G$ be defined by $\phi(i) = h^i$ for $0 \leq i < n$. Give a necessary and sufficient condition (in terms of h and n) for ϕ to be a homomorphism. Prove your assertion.

Solution. Given a group G, some $h \in G$, and $n \in \mathbb{Z}^+$, the map $\phi : \mathbb{Z}_n \to G$ defined by $\phi(i) = h^i$ for $0 \leq i < n$ is a homomorphism if and only if $h^n = e$.

Proof. $(\Rightarrow)$ Suppose ϕ is a homomorphism. Then $h^n = \phi(1)^n = \phi(n \cdot 1) = \phi(0) = e$.

($\Leftarrow$) Suppose $h^n = e$. Then we also have $h^{-n} = e$. Now consider $0 \leq i, j < n$. Then

$$\begin{aligned}
\phi(i +_n j) &= \begin{cases} \phi(i+j) & \text{if } i+j < n \\ \phi(i+j-n) & \text{if } i+j \geq n \end{cases} \\
&= \begin{cases} h^{i+j} & \text{if } i+j < n \\ h^{i+j-n} & \text{if } i+j \geq n \end{cases} \\
&= \begin{cases} h^i h^j & \text{if } i+j < n \\ h^i h^j h^{-n} & \text{if } i+j \geq n \end{cases} \\
&= \begin{cases} \phi(i)\phi(j) & \text{if } i+j < n \\ \phi(i)\phi(j)e & \text{if } i+j \geq n \end{cases} \\
&= \phi(i)\phi(j).
\end{aligned}$$

Hence ϕ is a homomorphism. □

<u>Additional Exercises</u>:

1. Let $\phi : G \to G'$ be a homomorphism of groups and suppose $g \in G$ is an element of finite order.
   (a) Prove that $|\phi(g)|$ divides $|g|$.

   Proof. Set $n = |g|$. Then $\phi(g)^n = \phi(g^n) = \phi(e) = e'$, so $|\phi(g)| \leq n$. Set $k = |\phi(g)|$. Then $n = kq + r$ for some integers q and r such that $0 \leq r < k$ (by the division algorithm). Hence

   $$e' = \phi(g)^n = \phi(g)^{kq+r} = (\phi(g)^k)^q \phi(g)^r = (e')^q \phi(g)^r = e'\phi(g)^r = \phi(g)^r.$$

   But the minimality of $|\phi(g)|$ then implies that $r = 0$, i.e. $n = kq$ and so $|\phi(g)|$ divides $|g|$. □

   (b) Prove that $|\phi(g)| = |g|$ if ϕ is injective.

   Proof. We prove the contrapositive. Set $n = |g|$ and suppose that $|\phi(g)| \neq |g|$. By part (a), $|\phi(g)|$ divides $|g|$, so $|\phi(g)|$ is finite and we may set $k = |\phi(g)| < n$ (since $|\phi(g)| \neq |g|$). By the minimality of $|g|$, it follows that $g^k \neq e$. However, $\phi(g^k) = \phi(g)^k = e' = \phi(e)$, so ϕ is not injective. □

3. Show that $SL_n(\mathbb{R})$ is a normal subgroup of $GL_n(\mathbb{R})$ for all $n \in \mathbb{Z}^+$.

   Proof. Consider $\det : GL_n(\mathbb{R}) \to \mathbb{R}^*$, which we showed in class is a group homomorphism (where the operation on $\mathbb{R}^*$ is multiplication). Now $\mathbb{R}^*$ has identity element 1, so

   $$\operatorname{Ker}(\det) = \{A \in GL_n(\mathbb{R}) \mid \det(A) = 1\} = SL_n(\mathbb{R}).$$

   Since we showed in class that the kernel of a homomorphism is a normal subgroup of the domain, this shows that $SL_n(\mathbb{R})$ is a normal subgroup of $GL_n(\mathbb{R})$. □