Solutions

1. Let G and H be groups and let $\phi : G \to H$ be a group homomorphism.

   (a) (2 pts) State the definition of a **group homomorphism**.

   A function $\phi : G \to H$ is a group homomorphism if $\forall a,b \in G$, $\phi(ab) = \phi(a)\phi(b)$. (or, if you prefer, $\phi(a+b) = \phi(a)+\phi(b)$.

   (b) (2 pts) State the definition of the **kernel of** ϕ, ker ϕ.

   Given a group homomorphism $\phi : G \to H$, the **kernel of** ϕ, ker ϕ, is $\phi^{-1}(0_H)$ or the inverse image of the identity in H or the set of elements in G whose image is the identity in H.

   (c) (8 pts) Prove ker ϕ is a normal subgroup of G. (Note that you must show ker ϕ is a subgroup of G **and** that it is normal.)

   Proof: (ker ϕ is a subgroup of G.)
   We know that all group homomorphisms send the identity in the domain to the identity in the range. So $e_G \in$ ker ϕ which implies ker $\phi \neq \emptyset$.
   Let $a,b \in$ ker ϕ. Observe

   $$\begin{aligned} \phi(ab^{-1}) &= \phi(a)\phi(b^{-1}) && \text{b/c } \phi \text{ respects the group operation} \\ &= \phi(a)(\phi(b))^{-1} && \text{by Prop 11.4} \\ &= e_H \cdot (e_H)^{-1} && \text{b/c } a,b \in \ker\phi \\ &= e_H && \text{b/c } e_H \text{ is the identity.} \end{aligned}$$

   Thus, we have shown that $ab^{-1} \in$ ker ϕ. Thus, by Proposition 3.31, the kernel of ϕ is a subgroup of G.

   (ker ϕ is normal G.)
   By Theorem 10.3, it is sufficient to demonstrate that $gag^{-1} \in$ ker ϕ, for every $g \in G$ and $a \in$ ker ϕ.Observe

   $$\begin{aligned} \phi(gag^{-1}) &= \phi(g)\phi(a)\phi(g^{-1}) && \text{b/c } \phi \text{ respects the group operation} \\ &= \phi(g)e_H\phi(g^{-1}) && \text{b/c } a \in \ker\phi \\ &= \phi(g)\phi(g)^{-1} && \text{by Prop 11.4} \\ &= e_H. \end{aligned}$$

   Thus, we have shown that $gag^{-1} \in$ ker ϕ.

2. (18 points) Give an examples of the following, if they exist. Otherwise, briefly explain why such examples do not exist.

   (a) An infinite nonabelian group.

   $GL_2(\mathbb{R})$

(b) A nonabelian group of order $n = 11$.
none exist. All groups of prime order are cyclic and therefore abelian.

(c) An infinite group G with multiple elements of finite order.

$G = Z_6 \times Z$

(d) Three nonisomorphic groups of order 12.

D_6, $\mathbb{Z}_4 \times \mathbb{Z}_3$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$

(e) A commutative ring with unity that is not an integral domain.

$\mathbb{Z}_6$

(f) A ring R and an ideal I such that I is prime.
$R = \mathbb{Z}$ and $I = 2\mathbb{Z}$

(g) A ring R and an ideal I that is maximal in R.
$R = \mathbb{Z}$ and $I = 2\mathbb{Z}$

(h) A ring R such that $R[x]$ contains a unit of degree at least 1.
$R = \mathbb{Z}_4$ and $2x + 1$ (It is its own inverse.)

3. (12 points) Let G be an abelian group. Let $H = \{a \in G : |a| < \infty\}$. (That is, H consists of all elements of G of finite order.)

Prove that H is a subgroup of G.

Proof: Let e_G be the identity of G. Since $|e_G| = 1$, we know that $e_G \in H$. Thus, $H \neq \emptyset$.
Let $a, b \in H$. Thus, we know that $|a| = m$ and $|b| = n$ for some $m, n \in \mathbb{Z}^+$. Thus, $|a^{-1}| = n$. Since G is abelian, $(ab^{-1})^{mn} = a^{mn}b^{-mn} = e_G^m e_G^n = e_G$. Thus, $ab^{-1} \in H$. Thus, $H \leq G$.

4. (a) (4 points) State Lagrange's Theorem
Let G be a finite group and let H be a subgroup of G. Then $[G : H] = |G|/|H|$ and, thus, $|H| \,\big|\, |G|$.

(b) (10 points) Let G be a group of order pq where p and q are both primes. Prove that every proper subgroup of G is cyclic.

Proof: Let G be a group of order pq where p and q are both primes. Let $H \leq G$ and $H \neq G$. By Lagrange's Theorem, $|H| \,\big|\, |G|$. So $|H| \in \{1, p, q\}$. If $|H| = 1$, then $H = \langle e \rangle$. If H has prime order then since groups of prime order are cyclic, H is cyclic.

5. Let R be the ring of functions $f : \mathbb{R} \to \mathbb{R}$ with the usual operations of addition and multiplication. Let S be the set of differentiable functions in R. (Note: All the functions in R, and therefore S, have domain $\mathbb{R}$.)

(a) (10 points) Prove that S is a subring of R.

Proof: Since $f(x) = 1$ is differentiable, S is not empty. Let $f, g \in S$. Since g is differentiable, so is $-g$. Since the sum of two differentiable functions is differentiable, we know $f - g \in S$. Since the product of two differentiable functions is differentiable, we know $fg \in S$.

(b) (4 points) Prove that S is **not** an ideal of R.
Proof: We know $f(x) = 1$ is in S and $g(x) = |x|$ is not in S. Since $fg = |x|$, we see that S fails the absorption requirement of an ideal.

6. Let $R = \left\{ \begin{bmatrix} a & b \\ 0 & c \end{bmatrix} : a, b, c \in \mathbb{Z} \right\}$. Consider the function $\phi : R \to \mathbb{Z}$ defined by $\phi\left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}\right) = a$.

(a) (10 points) Prove that ϕ is a ring homomorphism.

Proof: (respects addition)
Let $\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}, \begin{bmatrix} a' & b' \\ 0 & c' \end{bmatrix} \in \mathbb{M}_2(\mathbb{Z})$. Observe

$$\phi\left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix} + \begin{bmatrix} a' & b' \\ 0 & c' \end{bmatrix}\right) = \phi\left(\begin{bmatrix} a+a' & b+b' \\ 0 & c+c' \end{bmatrix}\right) = a + a' = \phi\left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}\right) + \phi\left(\begin{bmatrix} a' & b' \\ 0 & c' \end{bmatrix}\right).$$

(respects multiplication)

Observe

$$\phi\left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}\begin{bmatrix} a' & b' \\ 0 & c' \end{bmatrix}\right) = \phi\left(\begin{bmatrix} aa' & bc' + ab' \\ 0 & cc' \end{bmatrix}\right) = aa' = \phi\left(\begin{bmatrix} a & b \\ 0 & c \end{bmatrix}\right)\phi\left(\begin{bmatrix} a' & b' \\ 0 & c' \end{bmatrix}\right).$$

(b) (4 points) Determine the kernel of ϕ.

$$\ker\phi = \left\{ \begin{bmatrix} 0 & b \\ 0 & c \end{bmatrix} \,\middle|\, b, c \in \mathbb{Z} \right\}.$$

7. (4 points each) Short Answer

(a) What is the order of the factor group $\mathbb{Z}_{60}/\langle 15 \rangle$?
15

(b) What is the order of the element $10 + \langle 15 \rangle$ in the factor group $\mathbb{Z}_{60}/\langle 15 \rangle$?
3

(c) Is $2x^4 + 1$ an element of $\langle x^2 + 2 \rangle$, the ideal generated by $x^2 + 2$ in $\mathbb{Z}_3[x]$? Justify your answer.
Answer: Yes. $2x^4 + 1 \in \langle x^2 + 2 \rangle$ because $(x^2 + 2)(2x^2 + 2) = 2x^4 + 6x^2 + 4 = 2x^4 + 1$.

(d) Show that the map $f(x) = 5x$ is **not** a ring homomorphism from $\mathbb{Z}_{12}$ to $\mathbb{Z}_{60}$.
Answer: $f(1) = 5$. However, $5 = f(1 \cdot 1) \neq f(1)f(1) = 25$.

5 pts Extra Credit: Suppose $f(x)$ is irreducible in $F[x]$, where F is a field. Prove that for every nonzero polynomial $g(x) \in F[x]$, either $\gcd(f(x), g(x)) = 1$ or $f(x) \,\big|\, g(x)$.

Proof: Suppose $f(x)$ is irreducible in $F[x]$, where F is a field. Thus, by the definition of **irreducible**, $\deg(f(x)) \geq 1$. Let $g(x)$ be a nonzero polynomial in $F[x]$ and let $h(x) = \gcd(f(x), g(x))$. If $h(x) = 1$, the result holds.

So, suppose $\deg(h(x)) \geq 1$. From the definition of a greatest common divisor, it follows that $f(x) = h(x) \cdot k(x)$ and $g(x) = h(x)\ell(x)$ for some $k(x), \ell(x) \in F[x]$. Since $f(x)$ is irreducible and $\deg(h(x)) \geq 1$, it must be the case that $\deg(h(x)) = \deg(f(x))$ and $k(x)$ is a unit. Since $k(x)$ is a unit, $F[x]$ contains a multiplicative inverse for $k(x)$, say $(k(x))^{-1}$. Thus, $h(x) = f(x)(k(x))^{-1}$.

Now, we can replace $h(x)$ in the equation $g(x) = h(x)\ell(x)$ to obtain the equation $g(x) = f(x)(k(x))^{-1}\ell(x)$ which demonstrates that $f(x)$ divides $g(x)$.