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) (12 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. (20 points) Give an examples of the following, if they exist. Otherwise briefly explain why such examples do not exist.

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

   $\mathbb{Z}_6$ (Note any $\mathbb{Z}_n$ where n is composite would suffice.)

(b) A ring that is an integral domain but is not a field.

$\mathbb{Z}$ or $\mathbb{R}[x]$

(c) A ring R and a nontrivial subring I such that I is an ideal of R

$R = \mathbb{Z}$ and $I = 6\mathbb{Z}$

(d) A ring R and a nontrivial subring S such that S is **not** an ideal of R

$R = \mathbb{Z}[x]$ and $S = \mathbb{Z}$ or $R = \mathbb{R}$ and $S = \mathbb{Z}$

(e) A ring R and an ideal I that is prime.

$R = \mathbb{Z}$ and $I = 2\mathbb{Z}$

3. (16 points)

(a) (4 pts) State the First Isomorphism Theorem (for groups) Let $f : G \to H$ be a group homomorphism with kernel K. Let $g : G \to G/K$ be the canonical homomorphism. Then there is a unique isomorphism $h : G/K \to f(G)$ such that $f = h \circ g$.

(b) (12 pts) Let $\psi : G \to H$ be a group homomorphism. Prove that ψ is one-to-one if and only if $\psi^{-1}(e_H) = \{e_G\}$.

Proof: ($\Longrightarrow$:) Suppose that ψ is one-to-one. Since ψ is a homomorphism, $\psi(e_G) = e_H$. Since ψ is one-to-one, ψ can map no other element of G to e_H. Thus, $\phi^{-1}(e_H) = \{e_G\}$.

($\Longleftarrow$:) Suppose $\psi^{-1}(e_H) = \{e_G\}$. Thus, by the definition of kernel, $\ker\psi = \{e_G\}$. Since $\ker\psi = \{e_G\}$, it follows that $G \cong G/(\ker\psi)$. The First Isomorphism Theorem states that $G/(\ker\psi) \cong \psi(G)$. Thus, $G \cong \psi(G)$. Thus, ψ must be one-to-one.

4. (12 points) Prove that if R is a field, the only ideals of R are $\{0\}$ and R itself.

Proof: Let R be a field and let I be an ideal in R such that $I \neq \{0\}$. Since $I \neq \{0\}$, it follows that there exists some $r \in R \backslash \{0\}$ such that $r \in I$. Since R is a field and $r \neq 0$, there exists a multiplicative inverse, r^{-1}, in R. Since I is an ideal, $r^{-1}r = 1 \in I$. Since $1 \in I$, for every $a \in R$, $a = a \cdot 1 \in I$. Thus, $I = R$.

5. (12 points) Let R be a ring and let $a \in R$. Prove that the set $S = \{r \in R : ra = 0\}$ is a subring of R. Note that you should not assume R is commutative.

   Proof: (Note that I am using Prop 16.10)
   (Show $S \neq \emptyset$.) We know that $0 \cdot a = 0$. Thus, $0 \in S$.
   (Show S is closed under multiplication.) Let $x, y \in S$. Observe

$$\begin{aligned}(xy)a &= x(ya) && \text{b/c mult is associative in } R\\ &= x \cdot 0 && \text{b/c } y \in S\\ &= 0.\end{aligned}$$

   Thus $xy \in S$.
   (Show $x - y \in S$, $\forall x, y \in S$.) Let $x, y \in S$. Observe that

$$0 = 0 \cdot a = (y + (-y))a = ya + (-y)a = 0 + (-y)a = (-y)a.$$

   Thus,

$$(x - y)a = xa + (-y)a = 0 + 0 = 0.$$

   Thus, $x - y \in S$.

6. (24 points)

   (a) List all nonisomorphic abelian groups of order 24.

   answer: $\mathbb{Z}_8 \times \mathbb{Z}_3$, $\mathbb{Z}_2 \times \mathbb{Z}_4 \times \mathbb{Z}_3$, $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$

   (b) Let $\mathbb{R}$ be the ring of real numbers under the usual operations of addition and multiplication. Explain why the function $f : \mathbb{R} \to \mathbb{R}$ defined as $f(x) = 2x + 1$ is not ring homomorphism.

   answer: Observe that for real numbers 1 and 2, $f(1 + 2) = f(3) = 2 \cdot 3 + 1 = 7$, but $f(1) + f(2) = 2 \cdot 1 + 1 + 2 \cdot 2 + 1 = 8$. Thus f does not respect addition.

   (c) Find all group homomorphisms from $\mathbb{Z}_{16}$ to $\mathbb{Z}_{18}$. Your answer(s) must be stated as functions.

   answer: Since $gcd(16, 18) = 2$, we know there are two homomorphisms because there are only two divisors of 2, namely 1 and 2. So,
   option 1: $f(x) = 0$ (always a homomorphism)
   and
   option 2: $f(x) = 9x$ (b/c 2 is the only number that divides the orders of both groups, the image of f must have order 2)

   (d) Give a maximal ideal in the ring $\mathbb{Z}_{20}$
   answer: $\langle 2 \rangle$ or $\langle 5 \rangle$

Extra Credit: (5 points) Prove that every finite integral domain is a field.

Proof: Let R be a finite integral domain. We must show that for every $r \in R \backslash \{0\}$ there exists an element $r^{-1} \in R$ such that $rr^{-1} = 1$. Observe that 1 is its own inverse.
So let $r \in R \backslash \{0,1\}$ and consider the set $S = \{r^n : n \in \mathbb{Z}^+\}$. Observe that while $\mathbb{Z}^+$ is infinite, the set S must be finite since $S \subset R$ and R is finite. Thus, there exists some $m, n \in \mathbb{Z}^+$ such that $m < n$ and $r^m = r^n$.
Since R is an integral domain, the cancellation law applies. Thus, we can conclude $1 = r^{n-m}$. Since $r \neq 1$, we know $n - m \geq 2$. Thus, we see that $1 = r^{n-m} = r \cdot r^{n-m-1}$ where $n - m - 1 \geq 1$. So it follows that r^{n-m-1} is the multiplicative inverse of r.