MATH 521A: Abstract Algebra
Homework 6 Solutions

1. Let R, S be rings. Consider the *embedding* map $f : R \to R \times S$ given by $f : r \mapsto (r, 0_S)$. Prove that f is a homomorphism.

   We have $f(r + r') = (r + r', 0_S) = (r + r', 0_S + 0_S) = (r, 0_S) + (r', 0_S) = f(r) + f(r')$. We also have $f(rr') = (rr', 0_S) = (rr', 0_S 0_S) = (r, 0_S)(r', 0_S)$.

2. Let R, S be rings. Consider the *projection* map $f : R \times S \to R$ given by $f : (r, s) \mapsto r$. Prove that f is a homomorphism.

   We have $f((r, s) + (r', s')) = f((r + r', s + s')) = r + r' = f((r, s)) + f((r', s'))$, and $f((r, s)(r', s')) = f((rr', ss')) = rr' = f((r, s))f((r', s'))$.

3. We call a ring element x *idempotent* if $x^2 = x$. Let R, S be rings, and $f : R \to S$ a homomorphism. Suppose $x \in R$ is idempotent. Prove that $f(x)$ is idempotent.

   Suppose that x is idempotent, i.e. $x = x^2$. We have $f(x) = f(x^2) = f(xx) = f(x)f(x)$, so $f(x)^2 = f(x)$.

4. We call a ring element x *nilpotent* if there is some $n \in \mathbb{N}$ such that $x^n = 0$. Let R, S be rings, and $f : R \to S$ a homomorphism. Suppose $x \in R$ is nilpotent. Prove that $f(x)$ is nilpotent.

   Recall that $f(0_R) = 0_S$. Let $x \in R$ be nilpotent, i.e. $x^n = 0_R$. We have $f(x)^n = f(x)f(x)\cdots f(x) = f(xx\cdots x) = f(x^n) = f(0_R) = 0_S$.

5. Let R, S be rings, and $f : R \to S$ a homomorphism. Define the kernel of f, $Kerf = \{r \in R : f(r) = 0_S\}$. Prove that $Kerf$ is a subring of R.

   Because $f(0_R) = 0_S$, we have $0_R \in Kerf$. Suppose that $a, b \in Kerf$. Then $f(a) = 0_S, f(b) = 0_S$. We have $f(a + b) = f(a) + f(b) = 0_S + 0_S = 0_S$, so $a + b \in Kerf$; this proves additive closure. We also have $f(ab) = f(a)f(b) = 0_S 0_S = 0_S$, so $ab \in Kerf$; this proves multiplicative closure. By a theorem, $-f(a) = f(-a)$, so $0_S = f(a) + f(-a)$. But $f(a) = 0_S$ since $a \in Kerf$, so $0_S = 0_S + f(-a) = f(-a)$. Hence $(-a) \in Kerf$.

6. Let R, S be rings, and $f : R \to S$ a homomorphism. Prove that f is injective (one-to-one) if and only if $Kerf = \{0_R\}$.

   First, suppose that $Kerf = \{0_R\}$. Let $a, b \in R$ such that $f(a) = f(b)$. But then $f(a - b) = f(a) - f(b) = 0_S$, so $a - b \in Kerf$. Since $Kerf = \{0_R\}$, in fact $a - b = 0_R$, so $a - b + b = 0_R + b$, so $a = b$.
   Next, suppose that $c \in Kerf$ with $c \neq 0_R$. Then $f(c) = f(0_R) = 0_S$, so f is not injective.

7. Let R, S be rings, and $f : R \to S$ a homomorphism. Suppose that S_1 is a subring of S. Prove that $f^{-1}(S_1) = \{r \in R : f(r) \in S_1\}$ is a subring of R.

   First, $0_S \in S_1$ since every subring contains zero. Since $f(0_R) = 0_S$, we have $0_R \in f^{-1}(S_1)$. Next, suppose $a, b \in f^{-1}(S_1)$. Then $f(a), f(b) \in S_1$. Since S_1 is a subring, it is closed so $f(a + b) = f(a) + f(b) \in S_1$, and $f(ab) = f(a)f(b) \in S_1$. Hence $a + b, ab \in f^{-1}(S_1)$. Since S_1 is a subring, it contains additive inverses, so $-f(a) \in S_1$. By a theorem $f(-a) = -f(a)$, so $-a \in f^{-1}(S_1)$.

8. Let R, S, T be rings, and $f : R \to S$, $g : S \to T$ two homomorphisms. Prove that $g \circ f : R \to T$ is a homomorphism.

Let $a, b \in R$. We have $g(f(a+b)) = g(f(a) + f(b) = g(f(a)) + g((f(b))$, because f, g are homomorphisms (respectively). Similarly, $g(f(ab)) = g(f(a)f(b)) = g(f(a))g(f(b))$.

9. Let R, S be rings, and $f : R \to S$ an isomorphism. Let $g = f^{-1}$, i.e. for all $r \in R$, $g(f(r)) = r$ and for all $s \in S$, $f(g(s)) = s$. Prove that $g : S \to R$ is an isomorphism.

First, g is a bijection because the inverse of a bijection is a bijection (or we can prove it if we like). We have $g(a+b) = g(f(g(a)) + f(g(b))) = g(f(g(a) + g(b))) = g(a) + g(b)$, where we use the homomorphism property of f for the second equality. Similarly, we have $g(ab) = g(f(g(a))f(g(b))) = g(f(g(a)g(b))) = g(a)g(b)$.

10. Let $S = \{\left(\begin{smallmatrix} a & 2b \\ b & a \end{smallmatrix}\right) : a, b \in \mathbb{Z}\}$, which is a subring of $M_{2,2}(\mathbb{Z})$ (two-by-two matrices with integer entries). Prove that S is isomorphic to $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$, a subring of $\mathbb{R}$.

The notation gives a big hint; define $f : S \to \mathbb{Z}[\sqrt{2}]$ via $f : \left(\begin{smallmatrix} a & 2b \\ b & a \end{smallmatrix}\right) \mapsto a + b\sqrt{2}$. We check $f\left(\left(\begin{smallmatrix} a & 2b \\ b & a \end{smallmatrix}\right) + \left(\begin{smallmatrix} a' & 2b' \\ b' & a' \end{smallmatrix}\right)\right) = f\left(\left(\begin{smallmatrix} a+a' & 2(b+b') \\ b+b' & a+a' \end{smallmatrix}\right)\right) = (a + a') + (b + b')\sqrt{2} = (a + b\sqrt{2}) + (a' + b'\sqrt{2}) = f\left(\left(\begin{smallmatrix} a & 2b \\ b & a \end{smallmatrix}\right)\right) + f\left(\left(\begin{smallmatrix} a' & 2b' \\ b' & a' \end{smallmatrix}\right)\right)$. We also have $f\left(\left(\begin{smallmatrix} a & 2b \\ b & a \end{smallmatrix}\right)\left(\begin{smallmatrix} a' & 2b' \\ b' & a' \end{smallmatrix}\right)\right) = f\left(\left(\begin{smallmatrix} aa'+2bb' & 2ab'+2a'b \\ a'b+b'a & 2bb'+aa' \end{smallmatrix}\right)\right) = (aa' + 2bb') + (ab' + ba')\sqrt{2} = (a + b\sqrt{2})(a' + b'\sqrt{2}) = f\left(\left(\begin{smallmatrix} a & 2b \\ b & a \end{smallmatrix}\right)\right) f\left(\left(\begin{smallmatrix} a' & 2b' \\ b' & a' \end{smallmatrix}\right)\right)$. To prove injection, suppose $f\left(\left(\begin{smallmatrix} a & 2b \\ b & a \end{smallmatrix}\right)\right) = f\left(\left(\begin{smallmatrix} a' & 2b' \\ b' & a' \end{smallmatrix}\right)\right)$. Then $a + b\sqrt{2} = a' + b'\sqrt{2}$, which rearranges as $a - a' = (b' - b)\sqrt{2}$. If $b' = b$, then $a = a'$ and $\left(\begin{smallmatrix} a & 2b \\ b & a \end{smallmatrix}\right) = \left(\begin{smallmatrix} a' & 2b' \\ b' & a' \end{smallmatrix}\right)$. If $b' \neq b$, then we divide by $b' - b$ and discover that $\sqrt{2}$ is rational, a contradiction. Surjection is "obvious" due to the definitions: let $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, then $f\left(\left(\begin{smallmatrix} a & 2b \\ b & a \end{smallmatrix}\right)\right) = a + b\sqrt{2}$.

11. Recall the ring from HW4 #6: R has ground set $\mathbb{Z}$ and operations $\oplus, \odot$ defined as:

$$a \oplus b = a + b - 1, \quad a \odot b = a + b - ab$$

Prove that R is isomorphic to $\mathbb{Z}$.

The hard part of this problem is finding the isomorphsim, which is $f : R \to \mathbb{Z}$ via $f(x) = 1 - x$. We first prove a bijection; if $f(x) = f(x')$ then $1 - x = 1 - x'$ so $x = x'$. Also, for $a \in \mathbb{Z}$ we have $f(1 - a) = 1 - (1 - a) = a$.
Now, $f(a \oplus b) = f(a + b - 1) = 1 - (a + b - 1) = 2 - a - b = (1 - a) + (1 - b) = f(a) + f(b)$, and $f(a \odot b) = f(a + b - ab) = 1 - (a + b - ab) = 1 - a - b + ab = (1 - a)(1 - b) = f(a)f(b)$.

12. Recall the ring from HW4 #7: R has ground set $\mathbb{Z}$ and operations $\oplus, \odot$ defined as:

$$a \oplus b = a + b - 1, \quad a \odot b = ab - a - b + 2$$

Prove that R is isomorphic to $\mathbb{Z}$.

The hard part of this problem is finding the isomorphsim, which is $f : R \to \mathbb{Z}$ via $f(x) = x - 1$. We first prove a bijection; if $f(x) = f(x')$ then $x - 1 = x' - 1$ so $x = x'$. Also, for $a \in \mathbb{Z}$ we have $f(a + 1) = (a + 1) - 1 = a$.
Now, $f(a \oplus b) = f(a + b - 1) = a + b - 2 = (a - 1) + (b - 1) = f(a) + f(b)$, and $f(a \odot b) = f(ab - a - b + 2) = ab - a - b + 2 - 1 = ab - a - b + 1 = (a - 1)(b - 1) = f(a)f(b)$.