Rings
Tim Smits

We assume that rings have a multiplicative identity.

1. An element $a \in R$ is called **nilpotent** if $a^n = 0$ for some integer $n \geq 0$. Prove that if a is nilpotent, then $1 - a$ is a unit in R (Hint: think about a certain power series).

2. A ring R is called a **Boolean ring** if $a^2 = a$ for all $a \in R$.

   (a) Prove that every Boolean ring is commutative and $2a = 0$ for all $a \in R$.

   Let X be any non-empty set and let $\mathcal{P}(X)$ be the set of all subsets of X. Define addition and multiplication on $\mathcal{P}(X)$ by $A + B = (A \setminus B) \cup (B \setminus A)$ and $A \cdot B = A \cap B$.

   (b) Prove that the operations above make $\mathcal{P}(X)$ into a boolean ring.

3. An element $e \in R$ is called **idempotent** if $e^2 = e$.

   (a) Prove that if $f : R \to S$ is a ring homomorphism and e is an idempotent in R, then $f(e)$ is idempotent in S.

   (b) Compute the units and idempotents in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

   (c) Prove that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ are not isomorphic rings.

4. Let R be a finite, non-zero ring with no zero divisors. Show that R is a division ring, i.e. r is a unit for all $r \neq 0 \in R$.

5. Let $S = \left\{ \begin{pmatrix} m & n \\ 2n & m \end{pmatrix} : m, n \in \mathbb{Z} \right\}$. Prove that S is a subring of $M_2(\mathbb{Z})$, and that $\mathbb{Z}[\sqrt{2}] \cong S$.

6. Find all the possible ring homomorphisms $f : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$.

Solutions

1. First we prove the identity that $(1-x)(1+x+\ldots+x^N) = 1-x^{N+1}$ for any $x \in R$ and $N \geq 1$. This is obvious for $N = 1$, so suppose it's true for some integer k. Then $(1-x)(1+x+\ldots+x^k+x^{k+1}) = (1-x^{k+1})+(x^{k+1}-x^{k+2}) = 1-x^{k+2}$. By induction, it's therefore true for all $N \geq 1$. If $a^n = 0$, then using the above says that $(1-a)(1+a+\ldots+a^{n-1}) = 1-a^n = 1$. Similarly, we find $(1+a+\ldots+a^{n-1})(1-a) = 1-a^n = 1$, so $1-a$ is a unit with $(1-a)^{-1} = 1+a+\ldots+a^{n-1}$.

2. (a) Let $a \in R$. First, we show that $2a = 0$. We have $4a = 4a^2 = (2a)^2 = 2a$, so $2a = 0$. Now for any $a, b \in R$ we have $a+b = (a+b)^2 = a^2+ab+ba+b^2 = a+ab+ba+b$, so $ab+ba = 0$. This says $ab = ab+(ab+ba) = 2ab+ba = ba$ as desired.

   (b) It's pretty clear that if $A \in \mathcal{P}(X)$ that $A \cdot A = A$, so once we prove $\mathcal{P}(X)$ is a ring, we've proven it's a Boolean ring. To that end, we just need to verify the 6 ring axioms.

   The additive identity is the empty set, and the multiplicative identity is X. The additive inverse of a set A must be itself (by part a), this is the only candidate and it's obvious that it does work). Addition being commutative is clear. Distributivity and associativity follow from basic facts about sets (it's quite easy to see if you draw a picture, but I leave the details to you if you want to formally check this).

3. (a) We have $f(e)^2 = f(e^2) = f(e)$ since e is idempotent and f is a homomorphism.

   (b) $(\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z})^\times = \{([1],[1]),([1],[5])\}$.
   Idempotents: $\{([0],[0]),([0],[1]),([0],[3]),([0],[4]),([1],[0]),([1],[1]),([1],[3]),([1],[4])\}$.

   $(\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z})^\times = \{([1],[1]),([1],[3]),([2],[1]),([2],[3])\}$.
   Idempotents: $\{([0],[0]),([0],[1]),(([1],[0]),([1],[1])\}$.

   (c) Suppose there was an isomorphism $f : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z} \to \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. Then part a) says this would induce a bijection on the idempotents of these rings. However the first ring has 8 idempotents while the latter ring has 4 idempotents, a contradiction. Alternatively, one could run the same argument but with units instead.

4. For $r \neq 0 \in R$, consider the map $f : R \to R$ given by $f(x) = rx$. Then I claim f is injective: if $f(x) = f(y)$ for some $x, y \in R$, we have $r(x-y) = 0$. Since r is not a zero divisor, this says $x = y$. Since R is finite and f is injective, it's surjective, so there exists $b \neq 0 \in R$ with $rb = 1$. This says $brb = b$, so $(br-1)b = 0$. Again using that R has no zero divisors, this says $br - 1 = 0$, so that $br = 1$, i.e. r is a unit.

5. It's clear that $0, I_2 \in S$. For $A, B \in S$, we need to check that $AB \in S$ and $A - B \in S$. For the first, write $A = \begin{pmatrix} m & n \\ 2n & m \end{pmatrix}$ and $B = \begin{pmatrix} m' & n' \\ 2n' & m' \end{pmatrix}$ for some $n, m, n', m' \in \mathbb{Z}$. Then $A+B = \begin{pmatrix} m+m' & n+n' \\ 2(n+n') & m+m' \end{pmatrix}$ and $AB = \begin{pmatrix} mm'+2nn' & mn'+nm' \\ 2(m'n+mn') & 2nn'+mm' \end{pmatrix}$, both of which are clearly elements of S. By the subring test, S is a subring of $M_2(\mathbb{Z})$.

   Now, define a map $f : \mathbb{Z}[\sqrt{2}] \to M_2(\mathbb{Z})$ by $f(a+b\sqrt{2}) = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$. Note that $f(1) = I_2$. For $x, y \in \mathbb{Z}[\sqrt{2}]$, we may write $x = a+b\sqrt{2}$ and $y = a'+b'\sqrt{2}$ for some $a, b, a', b' \in \mathbb{Z}$. We have $x+y = (a+b)+(a'+b')\sqrt{2}$ by definition, so $f(x+y) = \begin{pmatrix} a+b & a'+b' \\ 2(a'+b') & a+b \end{pmatrix} = \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} + \begin{pmatrix} a' & b' \\ 2b' & a' \end{pmatrix} = f(x)+f(y)$. Similarly, one can check that $f(xy) = f(x)f(y)$. This says that f is a ring homomorphism. It's clear from the definition that f is surjective. To check that f is injective, we show that $\ker(f) = \{0\}$. If $x = a+b\sqrt{2} \in \ker(f)$, this says $\begin{pmatrix} a & b \\ 2b & a \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$, so $a = b = 0$ says $x = 0$. Therefore, f is bijective, and so is an isomorphism.

6. Let $f : \mathbb{Z}\times\mathbb{Z} \to \mathbb{Z}$ be a ring homomorphism. We can write any $(a,b) \in \mathbb{Z}\times\mathbb{Z}$ as $a(1,0)+b(0,1)$, so $f((a,b)) = af((1,0)) + bf((0,1))$ because f is a ring homomorphism. Therefore, we need only to determine the possible images of $(1,0)$ and $(0,1)$. Since $(1,0)$ and $(0,1)$ are both idempotent, they must map to idempotents in $\mathbb{Z}$, i.e. 0 or 1. This says there are at most 4 possible maps. Since f is a ring homomorphism, we must have that $f((1,1)) = 1$, so in particular, $(1,0)$ and $(0,1)$ cannot both simultaneously map to 0. This also says that they cannot both map to 1 simultaneously, because otherwise this would say $f((1,1)) = 1+1 = 2 \neq 1$. This leaves two possibilities: $f((a,b)) = a$ or $f((a,b)) = b$. It's hopefully quite clear that both of these maps *are* ring homomorphisms, so these are the only two possibilities.