Homework 8
Solutions

(1) If $a \in R$ then
$$-a = (-a)^2 = a^2 = a$$
so that $a + a = 0$. For $a, b \in R$ we have
$$a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b.$$
Hence it follows that $ab = (-ba) = ba$ so that R is commutative.

(2) (a) Set $I = \{x \in R \mid x^n = 0 \text{ for some } n\}$. First we show that I is a subgroup of R. Certainly, $I \neq \emptyset$ since $0 \in I$. Assume that $x, y \in I$ so that $x^n = y^m = 0$ for some $n, m \in \mathbb{N}$. Then the binomial theorem implies that
$$(x - y)^{n+m} = \sum_{k=0}^{n+m} \binom{n+m}{k} x^k (-y)^{n+m-k}.$$
If $0 \leq k \leq n$, then $n + m - k \geq m$ so that $(-y)^{n+m-k} = 0$. If $n \leq k \leq n + m$, then $x^k = 0$. Together these results imply that $(x - y)^{n+m} = 0$, so that $x - y \in I$. This shows that I is a subgroup. Now let $r \in R$ and $x \in I$. We claim that $rx \in I$. Since $x \in I$ there is some n such that $x^n = 0$. Hence $(rx)^n = r^n x^n = r^n 0 = 0$ since R is commutative. Hence I is an ideal.
Assume that there exists an $r+I \in R/I$ such that $(r+I)^n = 0 + I$ for some $n \in \mathbb{N}$. Then $(r + I)^n = r^n + I = 0 + I$ so that $r^n \in I$. Hence there exists some $m \in \mathbb{N}$ such that $(r^n)^m = r^{nm} = 0$ which implies that $r \in I$. Therefore there are no nilpotent elements in R/I besides $0 + I$.

(b) Let $R = M_2(\mathbb{R})$. Then $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$ is nilpotent since $A^2 = 0$. But $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 1 \end{pmatrix} = B$ is not nilpotent since $B^2 = B$.

(3) Let $n \in \mathbb{Z}$, $n \neq 0$. Then we have
$$f\left(\frac{1}{n}\right) g(n) = f\left(\frac{1}{n}\right) f(n) = f\left(\frac{1}{n} \cdot n\right) = f(1) = g(1).$$

Therefore we find

$$f\left(\frac{1}{n}\right)=f\left(\frac{1}{n}\right)f(1)=f\left(\frac{1}{n}\right)g(n)g\left(\frac{1}{n}\right)=g(1)g\left(\frac{1}{n}\right)=g\left(\frac{1}{n}\right).$$

Finally, if $a/b\in\mathbb{Q}$ we compute

$$f\left(\frac{a}{b}\right)=f(a)f\left(\frac{1}{b}\right)=g(a)g\left(\frac{1}{b}\right)=g\left(\frac{a}{b}\right)$$

so that $f=g$.

(4) Let $a,b\in \mathrm{Rad}I$ so that $a^n,b^m\in I$ for some $n,m\in\mathbb{N}$. Since $(-a)^n=(-1)^n a^n\in I$ also $-a\in\mathrm{Rad}I$. By the binomial theorem we have

$$(a+b)^{n+m}=\sum_{k=0}^{n+m}a^k b^{n+m-k}.$$

If $0\le k\le n$, then $n+m-k\ge m$ so that $b^{n+m-k}\in I$ and therefore $a^k b^{n+m-k}\in I$. If $n\le k\le n+m$, then $a^k\in I$ so that again $a^k b^{n+m-k}\in I$. Therefore $(a+b)^{n+m}\in I$ which in turn implies that $a+b\in\mathrm{Rad}I$ so that $\mathrm{Rad}I$ is a subgroup. Since R is commutative it suffices to show that $\mathrm{Rad}I$ is a left ideal. If $r\in R$ and $a\in\mathrm{Rad}I$, then $(ra)^n=r^n a^n\in I$ since $a^n\in I$. Therefore $ra\in\mathrm{Rad}I$ and hence $\mathrm{Rad}I$ is an ideal.

(5) (a) Take $R=M_2(\mathbb{R})$ and $I=\{A\in M_2(\mathbb{R})\mid A=\begin{pmatrix}a&0\\b&0\end{pmatrix}\}$. It is easy to check that I is a left ideal, but not a right ideal.

(b) Take $R=\mathbb{Z}/323\mathbb{Z}$. R has zero divisors since $[17]\cdot[19]=[0]$ in R. Let $I=\{k[17]\mid k\in\mathbb{Z}\}$. I is an ideal in R and $R/I\cong\mathbb{Z}/17\mathbb{Z}$. Hence R/I has no zero divisors and has 17 elements.

(6) (a) Every ideal I in $\mathbb{Z}$ is a subgroup of $(\mathbb{Z},+)$ and is therefore of the form $I=\langle n\rangle=(n)$ for some n.

(b) If $\varphi:R\to S$ is a surjective ring homomorphism, the correspondence theorem implies that every ideal J of S has the form $J=\varphi(I)$ for some ideal I in R. But R is a principal ideal ring so that $I=(a)$ for some $a\in R$ and hence $J=\varphi(I)=(\varphi(a))$.

(c) Apply the previous part to the canoncial map $\mathbb{Z}\to\mathbb{Z}_m$.