Homework Assignment 4

Homework 4. Due day: 10/25/06

(1.3) A ring $R$ such that $\forall a \in R, a^2 = a$ is called a Boolean ring. Prove that every Boolean ring is commutative and $a + a = 0, \forall a \in R$.

(1.6) A finite ring with more than one element and no zero divisors is a division ring.

(2.2) Let $I$ be an ideal in a commutative ring $R$ and let $\text{Rad } I = \{r \in R : r^n \in I \text{ for some integer } n \in \mathbb{Z}\}$. Show that $\text{Rad } I$ is an ideal.

(2.10) (a) Show that $\mathbb{Z}$ is a principal ideal ring.
(b) Every homomorphic image of a principal ideal ring is also a principal ideal ring.
(c) $\mathbb{Z}_m$ is a principal ideal ring for every $m > 0$.

(2.19) The ring of even integers contains a maximal ideal $M$ such that $E/M$ is not a field.
Solutions

(1.3) A ring \( R \) such that \( \forall a \in R, a^2 = a \) is called a \textbf{Boolean ring}. Prove that every Boolean ring is commutative and \( a + a = 0, \forall a \in R \).

\textbf{Proof} Let \( R \) be a Boolean ring, and \( a, b \in R \). Since \( R \) is Boolean,
\[
  a + b = (a + b)^2 = a^2 + ab + ba + b^2 = a + ab + ba + b,
\]
and so \( ab + ba = 0 \), implying \( ab = -ba \). Since \( a, b \) are arbitrary, setting \( b = a \), we have \( a = a^2 = -a^2 = -a \). Therefore, for any \( a \in R \), \( a + a = 0 \), and for any \( a, b \in R \), \( ab = -ba = b(-a) = ba \).

(1.6) A finite ring with more than one element and no zero divisors is a division ring.

\textbf{Proof} Let \( R \) be such a ring. It suffices to show that \( R \) has a multiplicative identity (unity) and that every nonzero element of \( R \) has a multiplicative inverse.

Since \( R \) is finite, denote \( R^* := R \setminus \{0\} = \{r_1, r_2, \cdots, r_n\} \). Since \( R \) has no zero divisor, the map \( f : R^* \to R^* \) by \( f(r_x) = r_1r_x \) is bijection, and so \( r_1R^* = R^* = R^*r_1 \). Therefore, there must be some \( i \), such that \( r_1r_i = r_1 \).

Fix \( i \). For any \( x \) with \( 1 \leq x \leq n \), \( r_1r_i = r_1r_x \). Since \( R \) has no zero divisor, \( r_1r_x = r_x \).

Since \( R \) has no zero divisor, for any \( x \) with \( 1 \leq x \leq n \), \( r_xr_i \in R^* \), and \( R^r_x = R^* \). Therefore, there must be a \( j \) with \( 1 \leq j \leq n \), such that \( r_xr_i = r_jr_x \). Multiply \( r_x \) both sides from right, and apply \( r_xr_x = r_x \) to get \( r_x^2 = r_jr_x^2 \). It follows that \( r_1r_x = r_x = r_jr_x = r_xr_i \). Hence, \( r_i \) is the multiplicative identity of \( R \). We denote \( r_i = 1 \).

Now pick an arbitrary \( r_x \in R^* \). By \( r_xR^* = R^* \), there must be a \( r_y \in R^* \) such that \( r_xr_y = r_i = 1 \). Let \( r_t = r_yr_x \). Then as \( r_xr_y = 1 \), \( r_x = (r_xr_y)r_x = r_x(r_yr_x) = r_xr_t \). Since \( R \) has no zero divisor, and since \( R \) has 1, we have \( r_t = 1 \), and so \( r_yr_x = 1 = r_xr_y \). Thus every \( r_x \in R^* \) has an inverse.

(2.2) Let \( I \) be an ideal in a commutative ring \( R \) and let \( \text{Rad} \, I = \{ r \in R : r^n \in I \text{ for some integer } n \in \mathbb{Z} \} \). Show that \( \text{Rad} \, I \) is an ideal.

\textbf{Proof:} Let \( a, b \in \text{Rad} \, I \). Then for some integers \( m, n \), we have \( a^m \in I \) and \( b^n \in I \). Since \( R \) is commutative,
\[
(a - b)^{m+n} = \sum_{k=0}^{m+n} (-1)^k \binom{m+n}{k} a^kb^{m+n-k}.
\]
Note that \( k < m \) if and only if \( m + n - k \geq n \). Since \( I \) is an ideal and since \( a^m, b^n \in I \), it follows that for each \( k \) with \( 0 \leq k \leq m + n \), \( a^kb^{m+n-k} \in I \), and so \( a + b \in \text{Rad} \, I \).

Now let \( a \in \text{Rad} \, I \) and \( r \in R \). As \( a^m \in I \) and as \( I \) is an ideal, \( (ra)^m = r^ma^m \in I \), and so \( ra \in \text{Rad} \, I \), which implies that \( \text{Rad} \, I \) is an ideal.

(2.10) (a) Show that \( \mathbb{Z} \) is a principal ideal ring.
(b) Every homomorphic image of a principal ideal ring is also a principal ideal ring.
(c) \( \mathbb{Z}_m \) is a principal ideal ring for every \( m > 0 \).
Proof: (a) Let $I \subseteq \mathbb{Z}$ be an ideal of $\mathbb{Z}$. Since $\mathbb{Z} = \langle 1 \rangle$, and $\{0\} = \langle 0 \rangle$, we may assume that $I$ is proper. Then since $I$ is a proper ideal, $I$ contains at least one positive integer. Pick $a \in I$ be the smallest positive integer in $I$, and we claim that $I = \langle a \rangle$.

Since $a \in I$, it suffices to show that $I \subseteq \langle a \rangle$. Let $x \in I - \{0\}$. By division algorithm, we can find integers $q$ and $r$ such that $x = qa + r$ and such that $0 \leq r < a$. Since $a \in I$ and since $I$ is an ideal, $qa \in I$ and so $r = x - qa \in I$. It follows by the choice of $a$ that $r = 0$. Hence $\forall x \in I$, $x = qa$ for some $q \in \mathbb{Z}$. Thus $I \subseteq \langle a \rangle$.

(b) Let $R, R'$ be rings, such that $R$ is a principal ideal ring, and $f : R \rightarrow R'$ be a ring homomorphism such that $R' = f(R)$. We want to show that $R'$ is also a principal ideal ring.

Let $I'$ be an ideal of $R'$ and let $I = f^{-1}(I')$. Then since $f(0_R) = 0_{R'} \in I'$, $0_R \in I$. If $a, b \in I$, then $f(a), f(b) \in I'$. Since $f$ is a homomorphism, and since $I'$ is an ideal, $f(a - b) = f(a) - f(b) \in I'$, and so $a - b \in I$. For any $r \in R$ and $a \in I$, since $I'$ is an ideal in $R'$, and since $f$ is a ring homomorphism, $f(ra) = f(r)f(a) \in I'$, and so by the definition of $I$, $ra \in I$. This shows that $I$ is an ideal of $R$. (You may also quote Exercise 13(a) of Chapter III, Section 2 on Page 134. But it is better to prove it yourself as it is also a good exercise for us to get familiar with the skill).

Hence $I$ is an ideal of $R$. Since $R$ is a principal ideal ring, $\exists a \in R$ such that $I = \langle a \rangle$. Thus $a \in I$ and so $f(a) \in I'$. Since $I'$ is an ideal, $\langle f(a) \rangle \subseteq I'$. For any $x' \in I'$, $\exists x \in I$ such that $f(x) = x'$. Note that (by Theorem 2.5(i)),

$$I = \langle a \rangle = \{ra + as + na + \sum_{i=1}^{m} r_i a s_i : r, s, r_i, s_i \in R; \text{ and } m, n \in \mathbb{Z} \}.$$  

Thus $x = ra + as + na + \sum_{i=1}^{m} r_i a s_i$. Since $f$ is a homomorphism, $x' = f(x) = f(r)f(a) + f(a)f(s) + nf(a) + \sum_{i=1}^{m} f(r_i)f(a)f(s_i) \in \langle f(a) \rangle$ and so $\langle f(a) \rangle \subseteq I'$. Thus $I' = \langle f(a) \rangle$, and so $R'$ is a principal ideal ring.

(c) Since $\mathbb{Z}$ is a principal ideal ring (by (a)), and since the map $f(n) = \pi \in \mathbb{Z}_m$ is a ring epimorphism, it follows from (b) that $\mathbb{Z}_m$ is a principal ideal ring.

(2.19) The ring of even integers contains a maximal ideal $M$ such that $E/M$ is not a field.

Proof: Note that $E = (2)$ is a principal ideal in $\mathbb{Z}$. Let $p > 2$ be a prime and let $M = \langle 2p \rangle$. Then $M$ is a principal ideal of $E$. Let $I$ be an ideal in $E$. Then $\exists 2a \in E$ with $a > 0$ such that $I = \langle 2a \rangle$ (One can imitate the proof that $\mathbb{Z}$ is a principal ideal to show that $E$ is also a principal ideal ring). If $M \subset I$, then $2a|2p$ or $a|p$. Hence either $a = p$ or $a = 1$, and so $M$ is a maximal ideal.

To see that $E/M$ is no an integral domain, we observe that $E/M = \{0, 2, \cdots, 2p - 2\}$. Since $p > 2$ is a prime, $\forall a, b \in E/M - \{0\}$, $ab \neq a$ and $ab \neq b$ (in $E/M$). Therefore $E/M$ does not have an identity and so $E/M$ cannot be a field.