Homework Assignment 5

Homework 5. Due day: 11/6/06

(5A) Do each of the following.
(i) Compute the multiplication: \((12)(16)\) in \(\mathbb{Z}_{24}\).
(ii) Determine the set of units in \(\mathbb{Z}_5\). Can we extend our conclusion on \(\mathbb{Z}_5\) to \(\mathbb{Z}_p\), for an arbitrary prime integer \(p\)?
(iii) Determine the set of units in \(\mathbb{Z}_6\). Can we extend our conclusion on \(\mathbb{Z}_6\) to \(\mathbb{Z}_n\), for an arbitrary integer \(n\)?
(iv) Determine if \(2x - 10\) is a prime element in \(\mathbb{R}[x]\), the ring of all real coefficient polynomials.
(v) Determine if \(2x - 10\) is a prime element in \(\mathbb{Z}[x]\), the ring of all integral coefficient polynomials.

Solution:  
(i) \((12)(16) = (12)(2)(8) ≡ 0 (\text{mod} \ 24)\).

Some students misunderstood is as the product of two principal ideals. In that case,
\[\langle 12 \rangle \langle 16 \rangle = \langle (12)(16) \rangle = \langle 0 \rangle.\]

(ii) If \(a \in U(\mathbb{Z}_5)\), then for some \(u \in \mathbb{Z}\), \(ua \equiv 1 (\text{mod} \ 5)\), and so for some \(v \in \mathbb{Z}\), \(ua + 5v = 1\). Therefore, \(a\) and \(5\) are relatively prime. On the other hand, if \(a\) and \(5\) are relatively prime, then for some integers \(u\) and \(v\), \(au + 5v = 1\), and so \(au \equiv 1 (\text{mod} \ 5)\). Thus \(a \in U(\mathbb{Z}_5)\). Hence \(U(\mathbb{Z}_5) = \{a : a \text{ and } 5 \text{ are relatively prime}\} = \mathbb{Z}_5 - \{0\}\).

(iii) The same argument in (ii) indicates that \(U(\mathbb{Z}_6) = \{a : a \text{ and } 6 \text{ are relatively prime}\} = \{1, 5\} \subseteq \mathbb{Z}_6\).

In general, we have \(U(\mathbb{Z}_n) = \{a : a \text{ and } n \text{ are relatively prime}\}\).

(iv) Let \(f(x) = 2x - 10\). Since \(\mathbb{R}[x]\) is a PID, an element is prime if and only if it is irreducible. If \(f(x) = a(x)b(x)\), then compare the degree both sides we may assume that \(a(x)\) has degree 1 and \(b(x)\) has degree zero. Thus \(a(x) = b \in \mathbb{R} - \{0\}\). Since \(\mathbb{R}\) is a field, every non zero element in a field is a unit of \(\mathbb{R}\), which is also is a unit of \(\mathbb{R}[x]\). Hence \(f(x)\) is irreducible, and so \(f(x)\) is prime in \(\mathbb{R}[x]\).

(iv) Let \(f(x) = 2x - 10\). Then \(f(x) = 2(x - 5)\), where 2 and \(x - 5\) are nonzero nonunit elements in \(\mathbb{Z}[x]\). It follows that \(f(x)\) is not an irreducible element in \(\mathbb{Z}[x]\). But \(\mathbb{Z}[x]\) is a commutative ring with identity, an element in \(\mathbb{Z}[x]\) is prime only if it is irreducible. Since \(f(x)\) is not irreducible in \(\mathbb{Z}[x]\), \(f(x)\) is not a prime in \(\mathbb{Z}[x]\).

(5B) = (3.3) Let \(R = \{a + b\sqrt{10} : a, b \in \mathbb{Z}\}\) be a subring of the field of the reals.
(a) The map \(N : R \mapsto \mathbb{Z}\) given by \(N(a + b\sqrt{10}) = a^2 - 10b^2\) is multiplicative (that is, \(\forall u, v \in R, N(uv) = N(u)N(v)\)) and \(N(u) = 0\) if and only if \(u = 0\).
(b) $u$ is a unit if and only if $N(u) = \pm 1$.
(c) $2, 3, 4 + \sqrt{10}$ and $4 - \sqrt{10}$ are irreducibles in $R$.
(d) $2, 3, 4 + \sqrt{10}$ and $4 - \sqrt{10}$ are not primes of $R$.
(e) Explain why this ring is an integral domain. Obtain two different factorizations of 6, and conclude that the factorization in this integral domain is not unique.

**Proof:**
(a) Let $u = a + b\sqrt{10}$ and $v = c + d\sqrt{10}$. Then
\[
N(uv) = N((a + b\sqrt{10})(c + d\sqrt{10})) = N(ac + 10bd + (ad + bc)\sqrt{10}) \\
= (ac + 10bd)^2 - 10(ad + bc)^2 = a^2c^2 + 20abcd + 100b^2d^2 - (10a^2d^2 + 20abcd + 10b^2c^2) \\
= a^2c^2 + 100b^2d^2 - 10a^2d^2 - 10b^2c^2 \\
= a^2(c^2 - 10d^2) - 10b^2(c^2 - 10d^2) = (a^2 - 10b^2)(c^2 - 10d^2) = N(u)N(v).
\]

Note that if for some positive $d$, $a = da_1$ and $b = db_1$, then $N(u) = N(a + b\sqrt{10}) = a^2 - 10b^2 = d^2(N(a_1 + b_1\sqrt{10})$. Therefore, if $0 = N(u) = a^2 - 10b^2$, for some non zero $a$ and $b$, then we may assume that $(a, b) = 1$, (that is, $a$ and $b$ are relatively prime).

Suppose that for some non zero $a$ and $b$ such that $N(a + b\sqrt{10}) = 0$, and such that $(a, b) = 1$. Now $a^2 = 10b^2$. Then $2a^2$ implies that $2|a$. Therefore, we can write $a = 2a_1$. Thus $4a_1^2 = 10b^2$, and so $2a_1^2 = 5b^2$. Then $2|b$ and so 2 is a common factor of $a$ and $b$, contrary to the assumption that $(a, b) = 1$. Therefore, we must have $a = b = 0$.

(b) Let $u = a + b\sqrt{10}$. Suppose that $u$ is a unit. Then there must be a $v \in R$, such that $uv = 1$. Since $N$ is multiplicative, $N(u)N(v) = N(1) = 1$. Since $N(u)$ and $N(v)$ are both integers, we must have $N(u) = \pm 1$.

Conversely, we assume that $N(u) = \pm 1$. Then $u(a - b\sqrt{10}) = a^2 - 10b^2 = \pm 1$. Therefore, $\pm(a - b\sqrt{10})$ is the inverse of $u$.

(c) To prove the statements in (c), we first note that the following fact holds in number theory.

(3c-1) For any $n \in \mathbb{Z}$, both $n^2 \not\equiv 2 \pmod{5}$ and $n^2 \not\equiv 2 \pmod{5}$.

In fact, we can write $n = 5k + r$ with $0 \leq r \leq 4$. Then $n^2 \equiv r^2 \pmod{5}$. But $0^2 = 0$, $2^2 \equiv 3^2 \equiv 4 \pmod{5}$ and $1^2 \equiv 4^2 \equiv 1 \pmod{5}$. This proves (3c-1).

Suppose that $u \neq 0$ is not an irreducible element. The for some non unit nonzero $x$ and $y \in R$, $u = xy$. It follows that $N(u) = N(x)N(y)$, where both $N(x)$ and $N(y)$ are integers other than ±1.

Now consider $u = 2$. Note that $N(2) = 4$, and that $4 = (2)(2) = (-2)(-2)$ are the only factorizations. If $u = xy$, for some non units $x$ and $y$, then we must have $N(x) = N(y) = \pm 2$.

Let $u = a + b\sqrt{10}$. Then $2 = N(u) = a^2 - 10b^2$. Then we have $2 \equiv a^2 - 10b^2 = a^2 \pmod{5}$, contrary to (3c-1). Therefore, 2 must be irreducible. Similarly, 3 must be irreducible.
Now suppose that \( u = 4 + \sqrt{10} = xy \) is a product of two non unit nonzero elements. Then \( 6 = N(u) = N(x)N(y) \). Therefore, \( N(x) \in \{ \pm 2, \pm 3 \} \). This contradicts to (3c-1), as shown above. Therefore, \( 4 + \sqrt{10} \) must be irreducible. Similarly, \( 4 - \sqrt{10} \) is also irreducible.

(d) As \((2)(3) = 6 = (4 + \sqrt{10})(4 - \sqrt{10})\), we have \( 2|(4 + \sqrt{10})(4 - \sqrt{10}) \). As \( N(2) = 4 \) and \( N(4 \pm \sqrt{10}) = 6 \), if for some \( x \in R \), \( 2x = 4 + \sqrt{10} \), then \( 4N(x) = N(2)N(x) = N(4 \pm \sqrt{10}) = 6 \), forcing \( N(x) = 2/3 \) which is not an integer. Therefore, \( 2 \nmid 4 \pm \sqrt{10} \), and so \( 2 \) is not a prime in \( R \). Similarly, the other three elements are not primes in \( R \).

(e) Since \( R \) is a subring of the real number field, and since a field does not have zero divisors, \( R \) has 1, is commutative, and has no zero divisors. Therefore, \( R \) is an integral domain. Note that
\[
6 = (2)(3) = (4 - \sqrt{10})(4 + \sqrt{10}).
\]
To see that \( 4 - \sqrt{10} \) is not associate with either \( 2 \) or \( 3 \), we use the function \( N \). Suppose that \( 4 - \sqrt{10} = 2u \) for some unit \( u \in R \). Then by (a) and (b) of this problem,
\[
6 = N(4 - \sqrt{10}) = N(2)N(u) = 4 \cdot 1 = 4,
\]
a contradiction. Similarly, \( 4 - \sqrt{10} \) is not associate with 3, and so the factorization of 6 in \( R \) is not unique.

(5C) Consider this solution of the equation \( X^2 = I \) in \( M_3(R) \), the ring of all \( 3 \times 3 \) real matrices with matrix addition and multiplication:
As \( X^2 = I \) implies \( X^2 - I = 0 \), the zero matrix, so factorization shows that \( (X - I)(X + I) = 0 \).
It follows that either \( X = I \) or \( X = -I \).
Is this reasoning correct? If your answer is not, point out the error and present an counterexample.

Solution: The reasoning is incorrect. The error is that it ignores the fact that zero divisors may exist and so \( AB = 0 \) does not always imply \( A = 0 \) or \( B = 0 \). In fact, if \( X = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \),
then \( X^2 = I \) but \( X \neq I \) and \( X \neq -I \).

(5D) Mark each of the following true or false.
True a. Every field is also a ring. (Definition)
False b. Every ring with identity has at least two elements. (The subring \( \{0\} \) of \( Z \) has multiplicative identity 0).
True c. Addition in every ring is commutative. (Definition)
False d. As a ring, \( nZ \) is isomorphic to \( Z \). (When \( n \geq 2 \), \( nZ \) has no multiplicative identity).
False e. \( Z \) is a subfield of \( R \), the field of the real numbers. (Lack of multiplicative inverses for nonzero nonunit elements).
True f. A ring homomorphism \( f \) is 1-1 if and only if the kernel of \( f \) is \( \{0\} \). (A ring homomorphism
is also a group homomorphism for the additive groups. This holds for group homomorphisms).

True: Every subring of a ring $R$ is also an ideal of $R$. (The center of $M_2$, the ring of all 2 by 2 real matrices, is not an ideal).

True: A quotient ring of an integral domain can be a field. ($\mathbb{Z}/(5) \cong \mathbb{Z}_5$ is a field.)

True: Every ideal of a ring $R$ has an identity and contains a subring isomorphic to $\mathbb{Z}$.

True: A quotient ring of an integral domain can have zero divisor. ($\mathbb{Z}/(6) \cong \mathbb{Z}/6$ has zero divisors.)

(5E) = (2.12) Let $R$ be a ring without identity and with no zero divisors. Let $S$ be the ring whose additive group is $R \times \mathbb{Z}$ (with multiplication defined by $(r_1, k_1)(r_2, k_2) = (r_1 r_2 + k_2 r_1 + k_1 r_2, k_1 k_2)$, for any $r_1, r_2 \in R$ and $k_1, k_2 \in \mathbb{Z}$). Let $A = \{(r, n) : r x + n x = 0, \forall x \in R\}$.

(a) $A$ is an idea in $S$.

(b) $S/A$ has an identity and contains a subring isomorphic to $R$.

(c) If $R$ is commutative, then $S/A$ has no zero divisor.

(d) What is $A$ if $R = 2\mathbb{Z}$?

Proof: (a) Firstly, $(0, 0) \in A$ and so $A \neq \emptyset$.

Let $(r', n')(r, n) \in S$ and $(r, n) \in A$. Then $(r', n') - (r, n) = (r' - r, n' - n)$. If both $(r', n') \in A$ and $(r, n) \in A$, then $\forall x \in R$, $(r' x + n' x = 0$ and $r x + n x = 0$. It follows that $(r' - r)x + (n' - n)x = 0$ and so $(r', n') - (r, n) = (r' - r, n' - n) \in A$.

By definition of multiplication, $(r', n')(r, n) = (r'r + n'r + nr', n'n)$. For any $x \in R$, $(r' r + n'r + nr')x + n'n x = r'(rx + nx) + n'(rx + n x) = 0$, and so $(r', n')(r, n) \in A$. Similarly, $(r, n)(r', n') = (r'r + n'r + nr', n'n) \in A$. Thus $A$ is an idea of $S$.

(b) Note that for any $(r, n) \in S$, $(0, 1)(r, n) = (r, n)(0, 1)$ and so $(0, 1)$ is the identity of $S$. It follows that the element $(0, 1) + A$ is the identity of $S/A$.

Define $f : R \mapsto S$ by $f(r) = (r, 0) + A$. Then

$$f(r_1 + r_2) = (r_1 + r_2, 0) + A = (r_1, 0) + A + (r_2, 0) + A = f(r_1) + f(r_2),$$

and

$$f(r_1 r_2) = (r_1 r_2, 0) + A = (r_1, 0)(r_2, 0) + A = f(r_1)f(r_2).$$

Thus $f$ is a ring homomorphism. Suppose that for some $r, r' \in R$, $f(r) = f(r')$. Then $f(r - r') \in A$, and so $\forall x \in R$, $(r - r')x = 0$. Since $R$ does not have zero divisors, we must have $r - r' = 0$ and so $r = r'$. This implies that $f$ is a monomorphism. By the First Isomorphism Theorem, $f(R)$ is isomorphic to $R$.

(c) Since in $S$, $(a, m)(x, 0) = (ax + mx, 0)$ and $(0, 0)$ is the additive identity of $S$, the subset $A$ of $S$ can be defined as

$$A = \{(r, n) : r x + n x = 0, \forall x \in R\} = \{(r, n) : (r, n)(x, 0) = (0, 0), \forall x \in R\}.$$

Let $(a, m) + A$ and $(b, n) + A$ be two non zero elements in $S/A$. We assume that $(a, m)(b, n) + A = ((a, m) + B)((b, n) + A) = A$ (or $(a, m)(b, n) \in A$) to derive a contradiction. Since $(a, m) + A$ and
$(b, n) + A$ are nonzero elements in $S/A$, $(a, m), (b, n) \notin A$. Now suppose

$$(ab + mb + na, mn) = (a, m)(b, n) \in A.$$ 

Since $(a, m) \notin A$, $\exists y \in R$, such that $(ay + my \neq 0$ in $R$. Note that $(y, 0)(a, m)(b, n) \in A$ since $A$ is an ideal. By the definition of $A$, $\forall x \in R$,

$$(ay + my)(bx + nx), 0) = (y, 0)(a, m)(b, n)(x, 0) = (0, 0),$$

where the first equality holds as $R$ is commutative. It follows by the assumption that $R$ has no zero divisor that $bx + nx = 0$ in $R$, $\forall x \in R$, and so $(b, n) \in A$, contrary to the assumption that $(b, n) + A \neq A$. 
