Math 345-60 Abstract Algebra I

Questions for Section 19: Integral Domains

1. Let $R$ be a ring. What does it mean for an element $a \in R$ to be a zero-divisor?

2. Let $R = \mathbb{Z}_{30}$. Find all the zero-divisors in $R$.

3. Let $R = M_2(\mathbb{Z}_4)$, the ring of all $2 \times 2$ matrices with coefficients in $\mathbb{Z}_4$. Find all the zero-divisors in $R$.

4. Define integral domain.

5. Prove that $\mathbb{Z}_5$ is an integral domain.

6. Here’s a proof that $\mathbb{Z}_n$ is an integral domain if and only if $n$ is prime: Assume $\mathbb{Z}_n$ is an integral domain. We will prove that $n$ is prime. If it isn’t, then $n = ab$ for some $0 < a < n$, $0 < b < n$. Therefore $[a]_n \neq [0]_n$ and $[b]_n \neq 0$, yet $[a]_n[b]_n = [ab]_n = [n]_n = [0]_n$, which contradicts the fact that $\mathbb{Z}_n$ has no zero-divisors. Hence $n$ is prime. Conversely, suppose that $n$ is prime. Suppose that $[a]_n[b]_n = [0]_n$ in $\mathbb{Z}_n$. Then $[ab]_n = [0]_n$, therefore $ab \in [0]_n$, therefore $ab$ is a multiple of $n$, therefore $n|ab$, therefore by unique factorization into primes $n|a$ or $n|b$, therefore $a \in [0]_n$ or $b \in [0]_n$, therefore $[a]_n = [0]_n$ or $[b]_n = [0]_n$. Hence $\mathbb{Z}_n$ has no zero divisors and is an integral domain.

7. Let $n \in \mathbb{Z}$ be given. We will show that the only zero-divisors in $\mathbb{Z}_n$ are those numbers of the form $[a]_n$ where $\gcd(a, n) > 1$ and $1 \leq a < n$. First suppose $\gcd(a, n) = d > 1$, where $1 \leq a < n$. Write $n_0 = \frac{n}{d} \in \mathbb{Z}$. Then $1 < n_0 < n$, therefore $[n_0]_n \neq [0]_n$. Also, write $a_0 = \frac{a}{d} \in \mathbb{Z}$. We have $[a]_n[n_0]_n = [a_0]_n = [a]_n[n]_n = [a_0]_n[0]_n = [0]_n$, hence $[a]_n$ is a zero divisor. Now consider $r, s \in \mathbb{Z}$ such that $ra + sn = 1$. This implies $[r]_n[a]_n = [1]_n$. Now suppose $[a]_n[b]_n = [0]_n$. Then $[b]_n = [r]_n[a]_n[b]_n = [r]_n[0]_n = [0]_n$. Hence $[a]_n$ is not a zero divisor.

8. We’ll prove that $\mathbb{Z}_p$ is a field when $p$ is a prime number. All we require is that $[a]_p$ have a multiplicative inverse in $\mathbb{Z}_p$ when $1 \leq a < p$. Since $p$ is prime and $1 \leq a < p$, we must have $\gcd(a, p) = 1$. So there is a solution to $ra + sp = 1$ among the integers. This implies $[r]_p[a]_p = [1]_p$. 

1
9. The characteristic of a ring is the smallest positive integer \( n \) such that 
\[ r + r + \cdots + r = 0 \text{ (} n \text{ summands)}. \]
For example, let \( c \) be the characteristic of \( \mathbb{Z}_n \). Then 
\[ c \leq n \text{ because } [a]_n + \cdots + [a]_n = [na]_n = [0]_n \text{ (} n \text{ summands)}. \]
Also, 
\[ c \geq n \text{ because otherwise } [1]_n + [1]_n + \cdots + [1]_n = [c]_n \neq [0]_n \text{ (} c \text{ summands)}. \]
Therefore 
\[ c = n. \]

Theorem: the characteristic \( c \) of an integral domain \( D \) must be a prime number. 
Proof: first we'll prove that \( c \) is the smallest positive integer \( k \) such that 
\[ 1 + 1 + \cdots + 1 = 0 \text{ (} k \text{ summands)} \]
in \( D \). Clearly \( k \leq c \) because \( c \) summands does produce zero. Suppose 
\[ 1 + 1 + \cdots + 1 = 0 \text{ (} k \text{ summands)}. \]
Multiplying through by \( r \in R \) we get 
\[ r + r + \cdots + r = 0 \text{ (} k \text{ summands)}. \]
Therefore \( c \leq k \). Now suppose \( c \) is not a prime number. Then it factors as 
\[ c = pq \text{ for two positive integers } p, q \text{ smaller than } c. \]
Let 
\[ x = 1 + 1 + \cdots + 1 \text{ (} p \text{ summands)} \text{ and } y = 1 + 1 + \cdots + 1 \text{ (} q \text{ summands)}. \]
Then 
\[ x \neq 0 \text{ and } y \neq 0, \text{ yet } xy = 1 + 1 + \cdots + 1 = 0 \text{ (} pq \text{ summands)}. \]
Contradiction: cannot happen in an integral domain. Therefore \( c \) is prime.

**Homework for Section 19, due ??? (only the starred problems will be graded):**

1, 2*, 10*, 14*, 17, 26*

Hints:
2. If we were dealing with real numbers we would solve this via 
\[ 3^{-1}3x = 3^{-1}2, \]
therefore \( x = 3^{-1}2 \). Only now you must find \( 3^{-1} \) in \( \mathbb{Z}_7 \) and \( \mathbb{Z}_{23} \).

26(a). In parts (a) through (d) we must not assume that \( R \) is commutative. 
A division ring satisfies all the axioms of a field except one: multiplication is 
not necessarily commutative. To show that \( R \) has no zero divisors, let \( x \neq 0 \) we given. We must show that if \( xz = 0 \) then \( z = 0 \), and that if \( zx = 0 \) then \( z = 0 \). I will do one of these (do the other one). Suppose \( xz = 0 \). Since \( x \neq 0 \) there exists a unique \( y \in R \) such that \( xyx = x \). Observe that 
\[ x(y + z)x = xyx + xzx = x + 0x = x, \]
therefore by uniqueness \( y = y + z \). This implies \( z = 0 \).

26(b). Argue that \( a(bab)a = a \), then use uniqueness.

26(c). It is not assumed to begin with that \( R \) has a multiplicative identity element (acting as 1). But we are given that \( R \) has at least two elements, and one of them is 0, so call the other one \( r \). Then there exists a unique \( s \) such that 
\( rsr = r \). A logical candidate for 1 is \( sr \). So we must show 
\[ srx = x = xsr \]
for all \( x \in R \). I will prove that 
\[ xsr = x \]
for all \( x \in R \) (do the other one).
Note that we have \( r(srx - x) = rsrx - rx = rx - rx = 0 \). By part (a), this implies \( srx - x = 0 \), which implies \( srx = x \).

26(d). Let \( x \neq 0 \). We must find \( y \in R \) such that \( xy = 1 = yx \). I will prove that \( y \) can be found such that \( xy = 1 \). You will have to prove that \( yx = 1 \) using the same value of \( y \). Let \( x \neq 0 \) be given. Then there exists a unique \( y \in R \) such that \( xyx = x \). Subtracting, \( xyx - x = 0 \). Factoring, \( (xy - 1)x = 0 \). Since there are no zero-divisors, \( xy - 1 = 0 \), therefore \( xy = 1 \).