November 11, 2024

Problem Set 8 Solutions

Exercise 1. (a) Let m be an integer. Show that the ring modulo m, $\mathbb{Z}/m\mathbb{Z}$, is an integral domain if and only if m is a prime.

(b) Find all zero divisors and all invertible elements (units) in $\mathbb{Z}/30\mathbb{Z}$.

(c) Show that $[a]_m \in \mathbb{Z}/m\mathbb{Z}$ is invertible if and only if it is not a zero divisor.

Solution 1. (a) If m is not a prime, then there exist $1 < n, k < m$ such that $m = nk$. Then $[n]_m[k]_m = [0]_m \in \mathbb{Z}/m\mathbb{Z}$, so the ring $\mathbb{Z}/m\mathbb{Z}$ is not an integral domain.
If $m = p$ is a prime, then for the product of two integers ab to be congruent to 0 modulo p, either $p|a$, or $p|b$. The numbers $\{1, 2, \dots p-1\}$ are not divisible by p, and therefore $[a]_m[b]_m \neq [0]_m$ in $\mathbb{Z}/p\mathbb{Z}$, and the ring is an integral domain.

(b) Units: $[1]_{30}$, $[7]_{30}$, $[11]_{30}$, $[13]_{30}$, $[17]_{30}$, $[19]_{30}$, $[23]_{30}$, $[29]_{30}$.

Zero divisors: $[2]_{30}$, $[3]_{30}$, $[4]_{30}$, $[5]_{30}$, $[6]_{30}$, $[8]_{30}$, $[9]_{30}$, $[10]_{30}$, $[12]_{30}$, $[14]_{30}$, $[15]_{30}$, $[16]_{30}$, $[18]_{30}$, $[20]_{30}$, $[21]_{30}$, $[22]_{30}$, $[24]_{30}$, $[25]_{30}$, $[26]_{30}$, $[27]_{30}$, $[28]_{30}$.

In particular, every nonzero element of $\mathbb{Z}/30\mathbb{Z}$ is either a unit or a zero divisor.

(c) Suppose $[a]_m \in \mathbb{Z}/m\mathbb{Z}$ is not a zero divisor. This holds if and only if $\gcd(a, m) = 1$ (If $\gcd(a, m) = d > 1$, then $[a]_m \cdot [m/d]_m = [0]_m \in \mathbb{Z}/m\mathbb{Z}$. If $\gcd(a, m) = 1$, then $an = mt$ for integers n, t implies that $m|n$, and therefore $[n]_m = 0 \in \mathbb{Z}/m\mathbb{Z}$). On the other hand, Bezout's theorem tells us that $\gcd(a, m) = 1$ if and only if there are integers x, y such that $xa + ym = 1$. This is equivalent to the statement that $[a]_m[x]_m = [1]_m \in \mathbb{Z}/m\mathbb{Z}$, or that a is invertible in $\mathbb{Z}/m\mathbb{Z}$.

Exercise 2. (a) Consider the set S of all polynomials with real coefficients of degree up to 3 with the usual addition and multiplication of polynomials. Is it a ring?

(b) Consider the ring $\mathbb{Z}[X]$ of all polynomials with integer coefficients. Check that it is a ring. Is it an integral domain?

(c) Let $R = \mathbb{Z}/4\mathbb{Z}$, and consider the ring $R[X]$ of polynomials with coefficients in R. Is it an integral domain? Justify your answer.

Solution 2. (a) The set S is not a ring. For example, $x \in S$ and $x^3 + 1 \in S$, but $x(x^3 + 1)$ is a polynomial of degree 4 and therefore does not belong to S. The set S is not closed with respect to multiplication of polynomials.

(b) The set $\mathbb{Z}[X]$ is an abelian group with respect to addition (0 is the neutral element), and is closed with respect to mulitplication with the neutral element 1, and the distributivity holds. So $\mathbb{Z}[X]$ is a commutative ring. For a polynomial $f(x) \in \mathbb{Z}[x]$ let n be the leading coefficient, which is defined as the coefficient of the highest power of x in $f(x)$. Then if n is the leading coefficient of $f(x)$ and m the leading coefficient of $g(x)$, it is easy to see that the leading coefficient of $f(x)g(x)$ is nm. Suppose that $f(x)g(x) = 0$, then the leading coefficient of the right-hand side is 0. The leading coefficients of both sides should be equal, therefore we have $nm = 0$. Since $\mathbb{Z}$ has no zero divisors, this implies that either n or m is zero. Therefore, either $f = 0$ or $g = 0$. This shows that $\mathbb{Z}[x]$ is an integral domain. Note that the argument works for any ring $A[x]$, where A is an integral domain.

(c) $R[X]$ is not integral: $[2]_4X \in R[X]$ and $[2]_4 \in R[X]$ are nonzero elements, but we have $[2]_4 \cdot [2]_4X = [0]_4X = 0_{R[X]}$.

Exercise 3. Let $C[0, 1]$ denote the ring of continuous real functions on the interval $[0, 1]$.

(a) Let $f \in C[0, 1]$ be such that the set $\{x : f(x) = 0\}$ contains a closed interval $[a, b] \subset [0, 1]$ of positive length $b - a > 0$. Show that f is a zero divisor in $C[0, 1]$.

(b) What are the invertible elements in the ring $C[0, 1]$?

Solution 3. (a) Suppose that $f \in C[0, 1]$ is such that $f(x) = 0$ for all $x \in [a, b] \subset [0, 1]$. Consider the function $g : [0, 1] \to \mathbb{R}$ such that $g(x) = 0$ for all $x \in [0, 1] \backslash]a, b[$, and $g(x)$ is nonzero on $]a, b[$ (for example, $g(x) = (x-a)(b-x)$ for all $x \in]a, b[$, and $g(x) = 0$ otherwise). Then $fg(x) = 0$ for all $x \in [0, 1]$, so $f(x)$ is a zero divisor.

(b) The invertible elements of $C[0,1]$ are the functions that have no zeros on $[0,1]$. If we have $f(x)g(x) = 1$ for all $x \in [0,1]$, then the number $f(x) \in \mathbb{R}$ has to be nonzero for each $x \in [0,1]$. Conversely, if $f : [0,1] \to \mathbb{R}$ is nonzero for each $x \in [0,1]$, then $g(x) = 1/f(x),\ x \in [0,1]$ defines the inverse element with respect to the pointwise multiplication of functions.

Exercise 4. (a) Show that a finite integral domain is a field.

(b) Find an example of a commutative finite ring that is not an integral domain.

(c) Find an example of an integral domain that is not a field.

Solution 4. (a) Let A be a finite integral domain, or equivalently, a finite commutative ring with no nontrivial zero divisors. Let $|A| = n$. Consider an element $a \in A, a \neq 0$ and let $\{b_1, \dots b_{n-1}\} = A \setminus \{0\}$ be the set of all nonzero elements in A. Consider the products

$$ab_1 = c_1,\ ab_2 = c_2, \dots ab_{n-1} = c_{n-1}.$$

Suppose that $c_i = c_j$ for some i and j. Then $a(b_i - b_j) = c_i - c_j = 0$. Since A has no nontrivial zero divisors, this implies that $b_i = b_j$, which contradicts the choice of $\{b_i\}_{i=1}^{n-1}$. Therefore, all $\{c_1, \dots c_{n-1}\}$ are all distinct nonzero elements of A. Since A has exactly $n-1$ nonzero elements, there exists $1 \leq k \leq n-1$ such that $c_k = 1$, and we have $ab_k = 1$, which means that a is invertible. We have proved that an arbitrary nonzero element of A is invertible, and therefore that A is a field.

(b) For example, $\mathbb{Z}/8\mathbb{Z}$. The elements $[2]_8$ and $[4]_8$ are zero divisors: $[2]_8 \cdot [4]_8 = [0]_8$.

(c) For example, $\mathbb{Z}$ is an integral domain but is not a field, because $5 \in \mathbb{Z}$ does not have a multiplicative inverse in $\mathbb{Z}$.

Exercise 5. Let $C[0,1]$ be the ring of continuous functions on the interval $[0,1]$. Let S be a closed subset of $[0,1]$ and set $I_S = \{f \in C[0,1] \ :\ f(x) = 0 \ \text{ for all } \ x \in S\}$.

(a) Show that I_S is an ideal in $C[0,1]$.

(b) If $S_1 = [0, \frac{1}{2}]$, $S_2 = [\frac{1}{2}, 1]$, $S_3 = \{\frac{1}{3}\}$, $S_4 = \{\frac{2}{3}\}$, describe the ideals $I_{S_1} \cap I_{S_2}$, $I_{S_1} \cdot I_{S_2}$, $I_{S_1} + I_{S_2}$, $I_{S_3} \cap I_{S_4}$, $I_{S_3} \cdot I_{S_4}$, and $I_{S_3} + I_{S_4}$.

Solution 5. (a) If $g \in C[0,1]$, we have $fg(x) = 0\ \forall x \in S$. Also, if $f_1(x) = 0\ \forall x \in S$ and $f_2(x) = 0\ \forall x \in S$, then $(f_1 + f_2)(x) = 0\ \forall x \in S$. Therefore, I_S is an ideal.

(b) $I_{S_1} \cap I_{S_2} = \{f \in C[0,1] \ :\ f(x) = 0\ \forall x \in [0,1]\} = \{0\}$.
$I_{S_1} \cdot I_{S_2} = \{f \in C[0,1] \ :\ f(x) = 0\ \forall x \in [0,1]\} = \{0\}$.
$I_{S_1} + I_{S_2} = \{f \in C[0,1] \ :\ f(\frac{1}{2}) = 0\}$
$I_{S_3} \cap I_{S_4} = \{f \in C[0,1] \ :\ f(\frac{1}{3}) = f(\frac{2}{3}) = 0\}$
$I_{S_3} \cdot I_{S_4} = \{f \in C[0,1] \ :\ f(\frac{1}{3}) = f(\frac{2}{3}) = 0\}$
$I_{S_3} + I_{S_4} = C[0,1]$. This holds because the ideal $I_{S_3} + I_{S_4}$ contains the identity function $f(x) = 1$, for example:

$$f(x) = 3\left(x - \frac{1}{3}\right) - 3\left(x - \frac{2}{3}\right) = 1.$$