November 18, 2024

Problem Set 9 Solutions

Exercise 1. Let R be a ring and I, J (two-sided) ideals in R. Show that $I+J$, $I\cap J$ and IJ are ideals in R. Compute the ideals $I+J$, $I\cap J$, IJ if $I = 30\mathbb{Z}$ and $J = 24\mathbb{Z}$ in the ring of integers $\mathbb{Z}$.

Solution 1.
- $I+J$:
  - (i) I and J are non-empty sets since they are ideals, so we can take $a \in I$ and $b \in J$. Then $a+b \in I+J$, so $I+J$ is not empty. In particular $0 \in I+J$.
  - (ii) Let $a = a_1 + a_2 \in I+J$, where $a_1 \in I$, $a_2 \in J$, and let $x \in R$. Then $xa_1 \in I$ and $xa_2 \in J$ since I and J are ideals, so we have $xa = x(a_1+a_2) = xa_1 + xa_2 \in I+J$.
  - (iii) Let $a = a_1 + a_2 \in I+J$ and $b = b_1 + b_2 \in I+J$, where $a_1, b_1 \in I$ and $a_2, b_2 \in J$. Then $a_1 + b_1 \in I$ and $a_2 + b_2 \in J$ since I and J are ideals, so we have $a+b = (a_1+a_2)+(b_1+b_2) = (a_1+b_1)+(a_2+b_2) \in I+J$.
- $I\cap J$:
  - (i) We have $0 \in I$ and $0 \in J$ since I and J are ideals. Thus $0 \in I\cap J$, i.e. $I\cap J$ is not empty.
  - (ii) Let $a \in I\cap J$ and let $x \in R$. Then $xa \in I$ and $xa \in J$ since I and J are ideals, so we have $xa \in I\cap J$.
  - (iii) Let $a \in I\cap J$ and $b \in I\cap J$. Then $a+b \in I$ and $a+b \in J$ since I and J are ideals, so we have $a+b \in I\cap J$.
- IJ:
  - (i) We have $0 \in IJ$, so IJ is not empty.
  - (ii) Let $x = \sum_{i=1}^n a_i b_i \in IJ$ where $a_1, \ldots, a_n \in I$ and $b_1, \ldots, b_n \in J$. Let $y \in R$. Then $ya_1, \ldots, ya_n \in I$ as I is an ideal, so we obtain $yx = y \cdot \sum_{i=1}^n a_i b_i = \sum_{i=1}^n (ya_i) b_i \in IJ$. Similarly, $xy = \sum_{i=1}^n a_i b_i y = \sum_{i=1}^n a_i (b_i y) \in IJ$.
  - (iii) $x = \sum_{i=1}^n a_i b_i \in IJ$ and $x' = \sum_{i=1}^m a_i' b_i' \in IJ$ where $a_1, \ldots, a_n, a_1', \ldots, a_m' \in I$ and $b_1, \ldots, b_n, b_1', \ldots, b_m' \in J$. We set $a_{n+k} = a_k'$ and $b_{n+k} = b_k'$ for $1 \leq k \leq m$. Then we have $x + x' = \sum_{i=1}^n a_i b_i + \sum_{i=1}^m a_i' b_i' = \sum_{i=1}^{n+m} a_i b_i \in IJ$.
- Consider the ideals $I = 30\mathbb{Z} \subset \mathbb{Z}$ and $J = 24\mathbb{Z} \subset \mathbb{Z}$. The ideal $I+J$ contains numbers of the form $24x+30y$. We know from Bezout's theorem that the equation $24x + 30y = d$ has (infinitely many) integer solutions for x, y if and only if d is a multiple of $\gcd(24, 30)$. Therefore, the ideal $I+J$ is generated by $\gcd(24, 30) = 6$, and so $I+J = 6\mathbb{Z} \subset \mathbb{Z}$. The ideal $I\cap J$ contains the elements that belong to both ideals, meaning that they are divisible by 24 and by 30. Since $\operatorname{lcm}(24, 30) = 120$, we have $I\cap J = 120\mathbb{Z}$. Finally, the ideal IJ is spanned by sums of products of elements of I and J, therefore each element of IJ is divisible by the product $30 \cdot 24 = 720$. We have $IJ = 720\mathbb{Z}$. Note that $IJ \subset I\cap J \subset I \subset I+J$: $720\mathbb{Z} \subset 120\mathbb{Z} \subset 30\mathbb{Z} \subset 6\mathbb{Z}$.

Exercise 2. (a) Consider the ring $\mathbb{Z}[X]$ of polynomials in one variable with integer coefficients. Let $I = (2, X)$ be the ideal generated by elements 2 and X. Describe the polynomials in this ideal.

(b) Let A be a commutative ring and I, J ideals in A. Show also that the set $I \star J = \{ab \mid a \in I, b \in J\}$ is not in general an ideal in A, by providing the counter-example of the set $I \star J \subset \mathbb{Z}[X]$, where $I = J = (2, X) \subset \mathbb{Z}[X]$.

(c) Let $I = (m) \subset \mathbb{Z}$ and $J = (n) \subset \mathbb{Z}$. Is $I \star J$ an ideal in $\mathbb{Z}$?

Solution 2. (a) Consider the ring $\mathbb{Z}[X]$, and $I = (2, X)$. By definition the ideal I is spanned by the elements of the form

$$2p(X) + Xq(X),$$

where $p(X), q(X) \subset \mathbb{Z}[X]$ are arbitrary polynomials. Therefore, the elements in I have the form

$$2a_0 + a_1 X + a_2 X^2 + \cdots + a_n X^n,$$

for some $n \in \mathbb{N}$, where $a_0, a_1, \ldots a_n \in \mathbb{Z}$. This is the set of all polynomials with integer coefficients, where the constant coefficient is even.

(b) Consider the ideals $I = J = (2, X) \subseteq \mathbb{Z}[X]$. We claim that $I \star J = \{ab \mid a \in I, b \in J\}$ is not an ideal in $\mathbb{Z}[X]$. Indeed, we have $2, X \in I$ and $2, X \in J$, so $4 = 2 \cdot 2, X^2 = X \cdot X \in I \star J$. Thus, if $I \star J$ were an ideal, we would have $X^2 + 4 \in I \star J$. This would in particular mean that $X^2 + 4 = PQ$ for some $P, Q \in I = J$.

If, in such a factorization, one of P and Q is of the form aX^0 for some $a \in \mathbb{Z}$, then a must be 1 or -1 since it must divide the leading coefficient of $X^2 + 4$, i.e. 1. Note, however, that $I = J$ contains neither 1 nor -1 since every element of $I + J$ has a constant coefficient divisible by 2. The other case, i.e. that $P = X + a$ and $Q = X + b$ are linear polynomials, is also impossible since that would mean that $PQ = (X + a)(X + b) = X^2 + (a + b)X + ab = X^2 + 4$, which implies $b = -a$ and $-a^2 = 4$. This equation has no solution in $\mathbb{Z}$.

Thus we have $X^2 + 4 \notin I \star J$ and hence $I \star J$ is not an ideal.

(c) In case $I = (n) \subset \mathbb{Z}$ and $J = (m) \subset \mathbb{Z}$, we have $I \star J = \{nxmy \mid x, y \in \mathbb{Z}\}$, which is equivalent to $\{nmt \mid t \in \mathbb{Z}\} = (nm) = I \cdot J$. This is an ideal in $\mathbb{Z}$.

Exercise 3. Let I be the smallest ideal in $\mathbb{Z}$ containing $\{392, 224, 168\}$. Find $d \in \mathbb{N}$ such that $I = (d) \subset \mathbb{Z}$.

Solution 3. We know from the course that any ideal in $\mathbb{Z}$ is *principal*, meaning that it is generated by a single natural number. From the proof of this property we know that, if the ideal is nonzero, the number d such that $I = (d) \subset \mathbb{Z}$ is the smallest positive integer contained in the given ideal I. So we need to find the smallest positive integer contained in the ideal I. The numbers of the form $392a + 224b$, where a, b are integers, are the multiples of the greatest common divisor of $392 = 7^2 \cdot 2^3$ and $224 = 7 \cdot 2^5$, which is $7 \cdot 2^3 = 56$. The numbers of the form $392a + 224b + 168c = 56k + 168c$ are the multiples of the greatest common divisor of $56 = 7 \cdot 2^3$ and $168 = 7 \cdot 3 \cdot 2^3$, which is 56. Therefore, $d = 56$, and $I = (56) \subset \mathbb{Z}$.

Exercise 4. Let $I = ((x^2 + x - 6)) \subset \mathbb{R}[x]$ be the ideal of polynomials divisible by $(x^2 + x - 6)$, and $J = ((x^2 - x - 2)) \subset \mathbb{R}[x]$ the ideal of polynomials divisible by $(x^2 - x - 2)$. Describe the ideals $I, J, I \cap J, I \cdot J, I + J$.

Solution 4. Consider the ideals $I = ((x^2 + x - 6)) = ((x - 2)(x + 3))$, $J = ((x^2 - x - 2)) = ((x - 2)(x + 1))$. We have:

- $I \cap J = ((x - 2)(x + 3)(x + 1)) = I$ is the ideal of polynomials divisible by $(x - 2)(x + 3)(x + 1)$.
- $I \cdot J = ((x - 2)^2(x + 3)(x + 1))$ is the ideal of polynomials divisible by $(x - 2)^2(x + 3)(x - 1)$.
- $I + J$ is the ideal spanned by sums of polynomials divisible by polynomials of the form $(x - 2)(x + 3)f(x) + (x - 2)(x + 1)g(x)$, where $f(x), g(x) \in \mathbb{R}[x]$. Therefore, $I + J$ contains all polynomials divisible by $(x - 2)$: $I + J = ((x - 2))$.

Note that, all of the ideals we considered above are *principal*, meaning that they are generated by a single element in $\mathbb{R}[x]$. We will see later on that, similarly to the ideals in the ring $\mathbb{Z}$, any ideal in the ring $\mathbb{R}[x]$ is principal. There are other similarities between these two rings.

Exercise 5. Let A be a commutative ring and $N \subset A$ a subset of all nilpotent elements in A:

$$N = \{x \in A : \ \exists n \in \mathbb{N} : \ x^n = 0\}.$$

Show that $N \subset A$ is an ideal. This ideal is called the *nilradical* of the ring. Show that the quotient ring A/N has no nonzero nilpotent elements.

Solution 5. The set N contains zero and is closed with respect to addition: if $x, y \in N$, such that $x^n = 0$ and $y^k = 0$, then we can choose $m = \max(n, k)$ and we have $x^m = y^m = 0$. Then $(x + y)^{2m} = \sum_{k=0}^{2m} \binom{2m}{k} x^k y^{2m-k} = 0$, because every summand contains a power of x or y greater or equal to m. Here we used the Newton's binomial formula that holds in commutative rings (see Proposition 1.7 in Rings). Also, if $a \in A$ and $x \in N$, such that $x^n = 0$, then $(ax)^n = a^n x^n = a^n \cdot 0 = 0$, therefore N is an ideal in A.

Now suppose $a \in A \setminus N$. Then $a^n \neq 0$ for any $n \in \mathbb{N}$. Therefore in the quotient ring we have $(a + N)^n \neq 0$ for any $n \in \mathbb{N}$ (we can choose a as a representative of the congruence class $(a + N)$). Therefore there are no nilpotent nonzero elements in the quotient ring A/N.