November 25, 2024

Problem Set 10 Solutions

Exercise 1. Recall that a ring homomorphism between two commutative rings $f : A \to B$ is a map that satisfies the conditions: (1) $f(x+y) = f(x) + f(y)$, (2) $f(xy) = f(x)f(y)$ for any $x, y \in A$, and (3) $f(1_A) = 1_B$.

(a) Show that the map $F : \mathbb{C} \to M_2(\mathbb{R})$ from complex numbers to 2×2 real matrices defined by

$$F(a+ib) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$$

is a ring homomorphism. Find its image and kernel.

(b) Let A be a commutative ring and $I \subset A$ an ideal. Prove that the map $\psi : A \to A/I$ sending $\psi(a) = a + I$ is a ring homomorphism. Find its image and kernel.

Solution 1. (a) We check the conditions. Let $a, b \in \mathbb{R}$.

$$F(a+ib+c+id) = F((a+c)+i(b+d)) = \begin{pmatrix} a+c & b+d \\ -b-d & a+c \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = F(a+ib)+F(c+id).$$

$$F((a+ib)(c+id)) = F(ac-bd+i(ad+bc)) = \begin{pmatrix} ac-bd & ad+bc \\ -ad-bc & ac-bd \end{pmatrix} = \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = F(a+ib)F(c+id).$$

We also have $F(1) = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Therefore F is a ring homomorphism. The kernel is $\{0\}$ and the image is the set of all real 2×2 matrices of the form $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ with $a, b \in \mathbb{R}$. In particular, this set of matrices is a field (since it is isomorphic to $\mathbb{C}$): the multiplication is commutative, as the computation above of $F(a+ib)F(c+id)$ shows, and any nonzero element is invertible. If $a + ib \neq 0 \in \mathbb{C}$, then we have

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix}^{-1} = \frac{1}{a^2+b^2} \begin{pmatrix} a & -b \\ b & a \end{pmatrix}.$$

(b) We check the conditions of a ring homomorphism. We have $\psi(a+b) = a + I + b + I = (a+b) + I = \psi(a+b)$, $\psi(ab) = (a+I)(b+I) = ab + I = \psi(a)\psi(b)$, where we used the ideal property $aI = I$ and $Ib = I$. We also have $\psi(1) = 1 + I = 1_{A/I}$. The kernel is by construction $\ker(\psi) = I$, and the image is $\mathrm{im}(\psi) = A/I$.

Exercise 2. Find the characteristic of the following rings :

(a) $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$.

(b) $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$.

(c) $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$.

(d) Let A and B be rings and c_A, c_B their characteristics. What is the characteristic of the ring $A \times B$?

(e) $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$

Solution 2. First we check that the map $\phi : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ defined by $\phi(a) = ([a]_n, [a]_m)$ is a ring homomorphism. Note that ϕ is well defined. Meaning that if $a = b \in \mathbb{Z}$ then $\phi(a) = ([a]_n, [a]_m) = ([b]_n, [b]_m) = \phi(b)$. It is easy to check that $\phi(a+b) = \phi(a) + \phi(b)$ and $\phi(ab) = \phi(a)\phi(b)$, for any $a, b \in \mathbb{Z}$. We have $\phi(1_{\mathbb{Z}}) = ([1]_n, [1]_m) = 1_{\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}}$. Therefore ϕ is the unique ring homomorphism $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$. To find the characteristic of the given rings, we need to find the kernel of ϕ in each case.

(a) We compute:

$$\phi(n) = ([n]_4, [n]_7) = 0 \in \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$$

if and only if both 4 and 7 divide n, or equivalently, n is a multiple of $\mathrm{lcm}(4, 7) = 28$. Therefore $(28) = \ker\phi$ and the characteristic of this ring is 28.

(b) By the same argument, $\phi(n) = ([n]_3, [n]_9) = 0 \in \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$ if and only if n is a multiple of $\text{lcm}(3,9) = 9$. Therefore $(9) = \ker\phi$ and the characteristic of this ring is 9.

(c) By the same argument, $\phi(n) = ([n]_2, n)$ is never zero in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}$, therefore $\ker\phi = 0$ and the characteristic of this ring is 0.

(d) We have $1_{A\times B} = (1_A, 1_B)$. Let $n \in \mathbb{Z}$. We have

$$n \cdot 1_{A\times B} = (n \cdot 1_A, n \cdot 1_B),$$

and so $n \cdot 1_{A\times B} = 0$ if and only if $n \cdot 1_A = 0$ and $n \cdot 1_B = 0$, if and only if $n \in c_A\mathbb{Z}$ and $n \in c_B\mathbb{Z}$. Therefore if $c_A = 0$ or $c_B = 0$, then $c_{A\times B} = 0$. On the other hand, if $c_A \neq 0$ and $c_B \neq 0$, then the characteristic of $A \times B$ equals to the smallest positive integer $\geqslant 1$ in the intersection $c_A\mathbb{Z} \cap c_B\mathbb{Z}$, therefore to the least common multiple of c_A et c_B: $c_{A\times B} = \text{lcm}(c_A, c_B)$.

(e) The same argument generalizes to a direct product of multiple rings. Let $R = \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/9\mathbb{Z}$. In this case, we have $c_R = \text{lcm}(6,3,8,9) = 72$.

Exercise 3.
Solve the system of congruences:

$$\begin{cases} x \equiv 2 \pmod 3 \\ x \equiv 4 \pmod 5 \\ x \equiv 3 \pmod 7. \end{cases}$$

Use the Chinese remainder theorem to show that a solution exists. Then find the complete set of solutions by solving the congruences consecutively. Solve the congruences (mod 3) and (mod 5) first, then use the obtained solution (mod 15) together with the last congruence (mod 7).

Solution 3.
Since the numbers $3, 5$ and 7 divide 105, we have a well defined homomorphism of rings:

$$\begin{aligned} \psi : \mathbb{Z}/105\mathbb{Z} &\longrightarrow \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z} \\ [n]_{105} &\mapsto ([n]_3, [n]_5, [n]_7). \end{aligned}$$

Since $105 = 3 \cdot 5 \cdot 7$ and $3, 5$ et 7 are pairwise mutually prime, by the Chinese remainder theorem we know that ψ is an isomorphism.

Therefore for each choice of $u, v, w \in \mathbb{Z}$ there exists $n \in \mathbb{Z}$ such that $([n]_3, [n]_5, [n]_7) = ([u]_3, [v]_5, [w]_7)$, and if another $n' \in \mathbb{Z}$ satisfies the same condition, then $[n]_{105} = [n']_{105}$.

We start by solving the first two congruences. Since 3 and 5 are mutually prime, by the Chinese remainder theorem we know that there exists a unique solution modulo $3 \cdot 5 = 15$. An integer x is a solution if and only if s and t are such that $x = 2 + 3s = 4 + 5t$. Then we have $3s - 5t = 2$. We can take $s = -1$ and $t = -1$, which gives $x = -1$. If we cannot guess a solution for (s, t), we could find it by using Euclidean algorithm and Bezout's identity.

So the original system is equivalent to the system of two congruences

$$\begin{cases} x \equiv -1 \pmod{15} \\ x \equiv 3 \pmod 7. \end{cases}$$

Again, since 15 and 7 are mutually prime, we know by the Chinese remainder theorem that there exists a unique solution modulo $15 \cdot 7 = 105$. An integer x is a solution if and only if the integers u and v are such that $x = -1 + 15u = 3 + 7v$. We obtain $15u - 7v = 4$. Note that $15 - 2 \cdot 7 = 1$, and we obtain $u = 4$ and $v = 8$, which gives $x = 59$.

The set of all solutions of the given system of congruences is the set of integers congruent to 59 modulo 105. Equivalently, this is the set $\{59 + 105k, k \in \mathbb{Z}\}$.

Another method

1. Using Bezout's identity for 3 and $35 = 5 \cdot 7$, we can find an explicit solution a for the system of congruences:

$$\begin{cases} x \equiv 1 \pmod 3 \\ x \equiv 0 \pmod 5 \\ x \equiv 0 \pmod 7. \end{cases}$$

Euclidean division gives $35 = 11 \cdot 3 + 2$ and $3 = 1 \cdot 2 + 1$, and we get $1 = 3 - 2 = 3 + 3 \cdot 11 - 35 = 12 \cdot 3 - 35$. Therefore $a := 1 - 12 \cdot 3 = -35$ satisfies the system.

2. We can proceed similarly to find a solution b for the following system of congruences:

$$\begin{cases} x \equiv 0 \pmod 3 \\ x \equiv 1 \pmod 5 \\ x \equiv 0 \pmod 7). \end{cases}$$

We see that $b := 21 = 4 \cdot 5 + 1$ satisfies the system of congruences $b \equiv 0 \mod 3$, $b \equiv 1 \mod 5$ and $b \equiv 0 \mod 7$.

3. In a similar way, we find a solution c for the following system of congruences:

$$\begin{cases} x \equiv 0 \pmod 3 \\ x \equiv 0 \pmod 5 \\ x \equiv 1 \pmod 7). \end{cases}$$

Finally the eucllidean division gives $15 = 2 \cdot 7 + 1$, and we have that $c := 15$ is a solution of the system of congruences $x \equiv 0 \mod 3$, $x \equiv 0 \mod 5$, et $x \equiv 1 \mod 7$.

4. Now we can find an explicit solution for the original system of congruences as a linear combination of a, b et c. We have to find $x_a, x_b, x_c \in \mathbb{Z}$ such that $\psi(x_a \cdot [a]_{105} + x_b \cdot [b]_{105} + x_c \cdot [c]_{105}) = ([2]_3, [4]_5, [3]_7)$. Set $n = 2(-35) + 4(21) + 3(15) = 59$. Then by the construction, n satisfies the original congruences. The set of solutions is $\{n' \in \mathbb{Z} \mid [n] = [n'] \bmod 105\} = \{59 + 105k \mid k \in \mathbb{Z}\}$.

Exercise 4. Is the ring $\mathbb{Z}/180\mathbb{Z}$ isomorphic to

$$\begin{array}{ll} (a) & \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3Z \times \mathbb{Z}/15\mathbb{Z}, \\ (b) & \mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/4Z \times \mathbb{Z}/5\mathbb{Z}, \\ (c) & \mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6Z \times \mathbb{Z}/5\mathbb{Z}? \end{array}$$

Hint: To prove that two rings are not isomorphic you can compare the number of invertible elements or the characteristic of the rings.

Solution 4. We have $180 = 2^2 \cdot 3^2 \cdot 5$. By the Chinese remainder theorem, the ring $\mathbb{Z}/180\mathbb{Z}$ is isomorphic to the ring $\mathbb{Z}/9\mathbb{Z} \times \mathbb{Z}/4Z \times \mathbb{Z}/5\mathbb{Z}$ as $9, 4, 5$ are pairwise mutually prime.

For the other rings, let us consider the number of invertible elements. For a ring $\mathbb{Z}/d\mathbb{Z}$ it is equal to the Euler's totient function $\varphi(d)$. We have $\varphi(180) = \varphi(9) \cdot \varphi(4) \cdot \varphi(5) = (9-3) \cdot (4-2) \cdot 4 = 48$.

Suppose $A \times B$ is a direct product of rings. If (a, b) is a unit in $A \times B$, then there exist $a^{-1} \in A$ and $b^{-1} \in B$ such that $(a, b) \cdot (a^{-1}, b^{-1}) = (1_A, 1_B)$. Therefore the number of invertible elements in $A \times B$ equals to the product of the numbers of invertible elements in A and in B. This generalizes by induction to multiple direct product.

The number of invertible elements in $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3Z \times \mathbb{Z}/15\mathbb{Z}$ is $\varphi(4) \cdot \varphi(3) \cdot \varphi(15) = 2 \times 2 \times 8 = 32$, and the number of invertible elements in $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6Z \times \mathbb{Z}/5\mathbb{Z}$ is $2 \times 2 \times 4 = 16$. Also, the characteristic of $\mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3Z \times \mathbb{Z}/15\mathbb{Z}$ is $\operatorname{lcm}(4, 3, 15) = 60$, the characteristic of $\mathbb{Z}/6\mathbb{Z} \times \mathbb{Z}/6Z \times \mathbb{Z}/5\mathbb{Z}$ is $\operatorname{lcm}(6, 6, 5) = 30$, but the characteristic of $\mathbb{Z}/180\mathbb{Z}$ is 180. Therefore $\mathbb{Z}/180\mathbb{Z}$ is not isomorphic to either of the rings (a) or (c).