 Algebra I HS17

Solution 2

Category theory, first definitions on Rings

1. Prove that a morphism in the category of sets is an isomorphism if and only if it is a bijective map.

   Solution: A morphism in the category of sets is a map $f : X \longrightarrow Y$. The identity morphism $\mathrm{id}_Z : Z \longrightarrow Z$ is the identity map.

   Suppose that f is an isomorphism. Then there exists a map $g : Y \longrightarrow X$ such that $g \circ f = \mathrm{id}_X$ and $f \circ g = \mathrm{id}_Y$. Let $x_1, x_2 \in X$ be such that $f(x_1) = f(x_2)$. Then

   $$x_1 = \mathrm{id}_X(x_1) = g(f(x_1)) = g(f(x_2)) = \mathrm{id}_X(x_2) = x_2.$$

   This means that f is injective. Moreover, for every $y \in Y$ we can write

   $$y = \mathrm{id}_Y(y) = f(g(y)),$$

   so that f is surjective. Hence f is a bijective map.

   Conversely, assume that f is a bijective map. For each $y \in Y$, the set

   $$f^{-1}(y) := \{x \in X : f(x) = y\}$$

   is non-empty because f is surjective. For each $x, x' \in f^{-1}(y)$, we notice that $f(x) = y = f(x')$, so that injectivity of f implies $x = x'$. This means that for each $y \in Y$ there exists $x_y \in X$ such that $f^{-1}(y) = \{x_y\}$. Define $g : Y \longrightarrow X$ as $g(y) := x_y$. Then $\forall x \in X,\ (g \circ f)(x) = g(f(x)) = x_{f(x)} = x$ because $f : x \mapsto f(x)$. On the other hand, $\forall y \in Y,\ (f \circ g)(y) = f(x_y) = y$. This means that g is an inverse of the morphism f, so that f is an isomorphism of sets.

2. Let $\mathcal{C}$ be a category and A an object of $\mathcal{C}$. Define F_A from $\mathcal{C}$ to sets by

   $$\begin{aligned} \forall B \text{ object of } \mathcal{C},\ & F_A(B) := \mathrm{Hom}_{\mathcal{C}}(A, B) \\ \forall f \in \mathrm{Hom}_{\mathcal{C}}(B, C),\ & F_A(f) := \left(\begin{array}{c} \mathrm{Hom}_{\mathcal{C}}(A, B) \longrightarrow \mathrm{Hom}_{\mathcal{C}}(A, C) \\ g \mapsto f \circ g \end{array} \right). \end{aligned}$$

   Prove that F_A is a functor (it is called the *functor represented by* A).

   Solution: First, notice that F_A is well-defined. Indeed $\mathrm{Hom}_{\mathcal{C}}(A, B)$ is defined to be a set for all objects A and B in $\mathcal{C}$. Moreover, for each $f \in \mathrm{Hom}_{\mathcal{C}}(B, C)$ and $g \in \mathrm{Hom}_{\mathcal{C}}(A, B)$, composition in $\mathcal{C}$ gives $f \circ g \in \mathrm{Hom}_{\mathcal{C}}(A, C)$.

   In order to prove that F_A is a functor, we need to check that it maps identity morphisms to identity morphisms and that it respects compositions.

- Let B be an object of $\mathcal{C}$. Then $\mathrm{id}_B \circ g = g$ for each morphism $g \in \mathrm{Hom}_{\mathcal{C}}(A, B)$ by definition of identity morphism. This implies that the map

$$\begin{aligned} F_A(\mathrm{id}_B) : \mathrm{Hom}_{\mathcal{C}}(A, B) &\longrightarrow \mathrm{Hom}_{\mathcal{C}}(A, B) \\ g &\longmapsto \mathrm{id}_B \circ g \end{aligned}$$

  is the identity of $\mathrm{Hom}_{\mathcal{C}}(A, B)$. Hence $F_A(\mathrm{id}_B) = \mathrm{id}_{F_A(B)}$ for each object B of $\mathcal{C}$.

- Let B, C and D be three objects in $\mathcal{C}$ and take morphisms $f_1 \in \mathrm{Hom}_{\mathcal{C}}(C, D)$ and $f_2 \in \mathrm{Hom}_{\mathcal{C}}(B, C)$. Then $F_A(f_1 \circ f_2)$ and $F_A(f_1) \circ F_A(f_2)$ are both maps $\mathrm{Hom}_{\mathcal{C}}(A, B) \longrightarrow \mathrm{Hom}_{\mathcal{C}}(A, D)$. For $g \in \mathrm{Hom}_{\mathcal{C}}(A, B)$, we notice that

$$\begin{aligned} F_A(f_1 \circ f_2)(g) = (f_1 \circ f_2) \circ g = f_1 \circ (f_2 \circ g) &= f_1 \circ (F_A(f_2)(g)) \\ &= F_A(f_1)\big(F_A(f_2)(g)\big), \end{aligned}$$

  so that $F_A(f_1 \circ f_2) = F_A(f_1) \circ F_A(f_2)$ for each pair of composable morphisms f_1 and f_2 in $\mathcal{C}$.

3. We want to define a category $\mathcal{C}$ as follows:

   - An object (X, Y, f) of $\mathcal{C}$ is given by two sets X and Y and a map $f : X \longrightarrow Y$.
   - A morphism $(u, v) \in \mathrm{Hom}_{\mathcal{C}}((X, Y, f), (X', Y', f'))$ is given by maps $u : X \longrightarrow X'$ and $v : Y \longrightarrow Y'$ such that the following diagram commutes:

$$\begin{tikzcd} X \arrow[r, "f"] \arrow[d, "u"'] & Y \arrow[d, "v"] \\ X' \arrow[r, "f'"] & Y' \end{tikzcd}$$

   (a) Define composition of morphisms so that $\mathcal{C}$ is indeed a category.

   (b) Prove that F from $\mathcal{C}$ to sets defined by $F((X, Y, f)) = X$ and $F((u, v)) = u$ is a functor.

Solution:

(a) Notice that the morphisms between two objects (X, Y, f) and (X', Y', f') in $\mathcal{C}$ form a set, as they form a subclass of the set $\mathrm{Hom}_{\mathcal{C}}((X, Y, f), (X', Y', f'))$. Given three objects (X, Y, f), (X', Y', f') and (X'', Y'', f'') in $\mathcal{C}$ and morphisms $(u, v) : (X, Y, f) \longrightarrow (X', Y', f')$ and $(u', v') : (X', Y', f') \longrightarrow (X'', Y'', f'')$, that is, maps

$$u : X \longrightarrow X', \ v : Y \longrightarrow Y', \ u' : X' \longrightarrow X'', \ v' : Y' \longrightarrow Y''$$

such that

$$f' \circ u = v \circ f \tag{1}$$
$$f'' \circ u' = v' \circ f', \tag{2}$$

we define

$$(u', v') \circ (u, v) := (u' \circ u, v' \circ v).$$

This definition is well-given because

$$\begin{aligned} f'' \circ (u' \circ u) &= (f'' \circ u') \circ u \overset{(2)}{=} (v' \circ f') \circ u \\ &= v' \circ (f' \circ u) \overset{(1)}{=} v' \circ (v \circ f) = (v' \circ v) \circ f. \end{aligned}$$

In order to conclude that $\mathcal{C}$ is a category, we need to check existence of identities and associativity of composition. Those properties follow immediately from the same property in the category of sets, since we have defined composition *coordinate-wise*. Let us see this very explicitly:

- For each object (U, V, g) of $\mathcal{C}$, consider the morphism $e_{(U,V,g)} := (\mathrm{id}_U, \mathrm{id}_V) \in \mathrm{Hom}_{\mathcal{C}}((U, V, g), (U, V, g))$. This is an identity of (U, V, g). Indeed, for each object (X, Y, f) of $\mathcal{C}$ and morphism (u, v) from (X, Y, f) to (U, V, g), one has

  $$e_{(U,V,g)} \circ (u, v) = (\mathrm{id}_U, \mathrm{id}_V) \circ (u, v) = (\mathrm{id}_U \circ u, \mathrm{id}_V \circ v) = (u, v),$$

  so that $e_{(U,V,g)}$ is a left unit. Similarly, one can prove that $e_{(U,V,g)}$ is a right unit.
- Let (X, Y, f), (X', Y', f'), (X'', Y'', f''), $(u, v) : (X, Y, f) \longrightarrow (X', Y', f')$ and $(u', v') : (X', Y', f') \longrightarrow (X'', Y'', f'')$ be as above, and take a fourth object (X''', Y''', f''') and a morphism $(u'', v'') : (X'', Y'', f'') \longrightarrow (X''', Y''', f''')$. Then

  $$\begin{aligned} ((u'', v'') \circ (u', v')) \circ (u, v) &= (u'' \circ u', v'' \circ v') \circ (u, v) \\ &= ((u'' \circ u') \circ u, (v'' \circ v') \circ v) = (u'' \circ (u' \circ u), v'' \circ (v' \circ v)) \\ &= (u'', v'') \circ ((u' \circ u, v' \circ v)) = (u'', v'') \circ ((u', v') \circ (u, v)) \end{aligned}$$

  and by arbitrarity of all objects and morphisms involved we can conclude that the composition law we defined is associative.

4. Let R and S be two rings and $f : R \longrightarrow S$ a map between them. Prove that f is a ring isomorphism if and only if it is ring homomorphism and it is bijective.

   Solution: Suppose that $f : R \longrightarrow S$ is a ring isomorphism. Then, by definition, it is a ring homomorphism and there exists an inverse ring homomorphism $g : S \longrightarrow R$.

In particular, at level of sets, g is an inverse map, so that, by exercise 1., f is bijective.

Now suppose that $f : R \longrightarrow S$ is a bijective ring homomorphism. Then, by Exercise 1., there exists a map of sets $g : S \longrightarrow R$ such that $f \circ g = \mathrm{id}_S$ and $g \circ f = \mathrm{id}_R$. We need to check that g is itself a ring homomorphism. First, notice that

$$g(1_S) = g(f(1_R)) = 1_R,$$

because f is a ring homomorphism so that $f(1_R) = 1_S$. Now, for $s_1, s_2 \in S$, let $r_1, r_2 \in R$ be such that $f(r_1) = s_1$ and $f(r_2) = s_2$. Notice that $g(s_1) = r_1$ and $g(s_2) = r_2$. Then

$$g(s_1 + s_2) = g(f(r_1) + f(r_2)) \overset{(*)}{=} g(f(r_1 + r_2)) = r_1 + r_2 = g(s_1) + g(s_2)$$
$$g(s_1 \cdot s_2) = g(f(r_1) \cdot f(r_2)) \overset{(*)}{=} g(f(r_1 \cdot r_2)) = r_1 \cdot r_2 = g(s_1) \cdot g(s_2)$$

which allows us to conclude that g is a ring homomorphism. (In the equalities $(*)$ above we used the fact that f is a ring homomorphism).

5. (a) Compute the units of $\mathbb{Z}[i]$.
   (b) (*Euclidean division in* $\mathbb{Z}[i]$) Let $z, w \in \mathbb{Z}[i] \smallsetminus \{0\}$. Prove that there exist $q, r \in \mathbb{Z}[i]$ such that $z = q \cdot w + r$ and $|r| < |w|$. [*Hint:* Define $q \in \mathbb{Z}[i]$ such that it is a good approximation of $\frac{z}{w} \in \mathbb{C}$.]

Solution: We will make use of the complex norm $N : \mathbb{C} \longrightarrow \mathbb{R}_{\geqslant 0}$ defined by $N(z) = z\overline{z}$. For $a + ib \in \mathbb{Z}[i]$, this gives $N(a + ib) = a^2 + b^2 \in \mathbb{N}$. Notice that for each $x, y \in \mathbb{C}$

$$N(xy) = xy\overline{xy} = x\overline{x}y\overline{y} = N(x)N(y). \tag{3}$$

(a) Let $x = a + ib \in \mathbb{Z}[i]$. If x is a unit, then $xy = 1$ for some $y \in \mathbb{Z}$. Then, by (3),

$$1 = N(1) = N(x)N(y),$$

and since $N(x), N(y) \in \mathbb{N}$ we deduce that $N(x) = 1$. This means that $a^2 + b^2 = 1$. This implies that $a^2 \leqslant 1$ and $b^2 \leqslant 1$, so that $a, b \in \{-1, 0, 1\}$. The only possibilities are $(a, b) = (\pm 1, 0)$ and $(a, b) = (0, \pm 1)$, which implies that $\mathbb{Z}[i]^\times \subseteq \{\pm 1, \pm i\}$. Since those four elements are all units since $1^2 = (-1)^2 = i \cdot (-i) = 1$, which allows us to conclude that $\mathbb{Z} = \{\pm 1, \pm i\}$.

(b) Let $u, v \in \mathbb{R}$ be such that

$$\frac{z}{w} = u + iv.$$

There exist $u_0, v_0 \in \mathbb{Z}$ such that $|u - u_0| \leqslant \frac{1}{2}$ and $|v - v_0| \leqslant \frac{1}{2}$. Define $q := u_0 + iv_0$ and $r := z - qw$. In order to conclude, we need to check that $|r| < |w|$, or, equivalently, that $|\frac{r}{w}| < 1$. This is done by noticing that

$$\frac{r}{w} = \frac{z - qw}{w} = (u - u_0) + i(v - v_0)$$

which implies, by definition of complex absolute value, that

$$\left|\frac{r}{w}\right|^2 = |u - u_0|^2 + |v - v_0|^2 \leqslant \frac{1}{4} + \frac{1}{4} = \frac{1}{2} < 1.$$

6. Let $F(\mathbb{R}, \mathbb{C})$ the set of functions $\mathbb{R} \longrightarrow \mathbb{C}$. Denote by $C(\mathbb{R}, \mathbb{C})$ the subset of continuous functions and by $C_0(\mathbb{R}, \mathbb{C})$ the subset of continuous bounded functions.

   (a) Check that $F(\mathbb{R}, \mathbb{C})$, endowed with pointwise sum and multiplication, is a commutative ring. Find $F(\mathbb{R}, \mathbb{C})^\times$.

   (b) Prove that $C_0(\mathbb{R}, \mathbb{C})$ and $C(\mathbb{R}, \mathbb{C})$ are subrings of $F(\mathbb{R}, \mathbb{C})$.

   (c) Determine $C(\mathbb{R}, \mathbb{C})^\times$ and $C_0(\mathbb{R}, \mathbb{C})^\times$.

   (d) Is $C_0(\mathbb{R}, \mathbb{C})$ an integral domain?

   (e) Which of the following maps are ring homomorphisms?

      i. $\varphi : C_0(\mathbb{R}, \mathbb{C}) \longrightarrow \mathbb{C}$, sending $f \mapsto f(1)$;

      ii. $\psi : C_0(\mathbb{R}, \mathbb{C}) \longrightarrow \mathbb{R}$, sending $f \mapsto \sup_{x \in \mathbb{R}} |f(x)|$;

      iii. $\eta : C(\mathbb{R}, \mathbb{C}) \longrightarrow \mathbb{R}$, sending $f \mapsto \mathrm{Re}(f(0))$;

      iv. $\theta : \mathbb{Z} \longrightarrow F(\mathbb{R}, \mathbb{C})$ sending $n \in \mathbb{Z}$ to the constant function with value n.

Solution:

(a) The operations $+$ and $\cdot$ on $F(\mathbb{R}, \mathbb{C})$ are defined pointwise, that is,

$$(f + g)(x) := f(x) + g(x)$$
$$(f \cdot g)(x) := f(x)g(x).$$

With a notation abuse, we denote by 0 and 1 the functions $\mathbb{R} \longrightarrow \mathbb{C}$ with constant value 0 and 1 respectively. Let $- : F(\mathbb{R}, \mathbb{C}) \longrightarrow F(\mathbb{R}, \mathbb{C})$ be defined by $(-f)(x) := -f(x)$. Then the $(F(\mathbb{R}, \mathbb{C}), +, -, \cdot, 0, 1)$ satisfies all the axioms for a commutative. Indeed, for all $a, b, c \in F(\mathbb{R}, \mathbb{C})$ the following hold:

- $\forall x \in \mathbb{R}$, $(a + (b + c))(x) = a(x) + (b + c)(x) = a(x) + b(x) + c(x) = (a + b)(x) + c(x) = ((a + b) + c)(x)$, so that $a + (b + c) = (a + b) + c$ (sum is associative);
- $\forall x \in \mathbb{R}$, $(a + b)(x) = a(x) + b(x) = b(x) + a(x) = (b + a)(x)$, so that $a + b = b + a$ (sum is commutative);

- $\forall x \in \mathbb{R}$, $(0+a)(x) = 0(x) + a(x) = 0 + a(x) = a(x)$, so that $0 + a = a$ (0 is neutral for the sum on the left);
- $\forall x \in \mathbb{R}$, $(a + (-a))(x) = a(x) + (-a)(x) = a(x) + (-a(x)) = 0 = 0(x)$, so that $a + (-a) = 0$ (the map "$-$" is an inversion for the sum);
- $\forall x \in \mathbb{R}$, $(a \cdot (b \cdot c))(x) = a(x)(b \cdot c)(x) = a(x)b(x)c(x) = (a \cdot b)(x)c(x) = ((a \cdot b) \cdot c)(x)$, so that $a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (product is associative);
- $\forall x \in \mathbb{R}$, $(a \cdot b)(x) = a(x)b(x) = b(x)a(x) = (b \cdot a)(x)$, so that $a \cdot b = b \cdot a$ (product is commutative);
- $\forall x \in \mathbb{R}$, $(1 \cdot a)(x) = 1(x) \cdot a(x) = 1 \cdot a(x) = a(x)$, so that $1 + a = a$ (1 is neutral for the product on the left);
- $\forall x \in \mathbb{R}$, $(a \cdot (b+c))(x) = a(x)(b+c)(x) = a(x)(b(x)+c(x)) = a(x)b(x) + a(x)c(x) = (a \cdot b)(x) + (a \cdot c)(x)$, so that $a \cdot (b+c) = a \cdot b + a \cdot c$ (distributivity).

Let $f \in F(\mathbb{R}, \mathbb{C})^\times$, with inverse g. This means that

$$\forall x \in \mathbb{R},\ f(x)g(x) = 1.$$

Then $f(x) \neq 0$ for every $x \in \mathbb{R}$. On the other hand, every non-zero complex number $z \in \mathbb{C} \setminus \{0\}$ is invertible, so that if $f \in F(\mathbb{R}, \mathbb{C})$ is nowhere zero, then we can define

$$g(x) := \frac{1}{f(x)}$$

and this is an inverse of f in $F(\mathbb{R}, \mathbb{C})$. Hence

$$F(\mathbb{R}, \mathbb{C})^\times = \{f : \mathbb{R} \longrightarrow \mathbb{C} : \forall x \in \mathbb{R},\ f(x) \neq 0\}.$$

(b) Given a subset R of a ring S, we say that R is a *subring* of S if the ring operations on S restrict to R, and R is a ring when endowed with those restrictions, with $0_R = 0_S$ and $1_R = 1_S$. Clearly, if R is closed under the operations $+, -$ and $\cdot$ of S and it contains 0_S and 1_S, then the ring axioms hold for R, since they hold for the whole superset S.

First, notice that $C_0(\mathbb{R}, \mathbb{C}) \subseteq C(\mathbb{R}, \mathbb{C})$ by definition. The constant functions 0 and 1 are continuous and bounded, hence they both belong to $C_0(\mathbb{R}, \mathbb{C})$ and $C(\mathbb{R}, \mathbb{C})$. Basic calculus tells us moreover that for f, g continuous functions the functions $f + g$, $-f$ and fg are continuous. Hence $C(\mathbb{R}, \mathbb{C})$ is a subring of $F(\mathbb{R}, \mathbb{C})$.

Let f, g be bounded functions, that is, suppose there are numbers $M_f, M_g \in \mathbb{R}_{>0}$ such that $|f(x)| < M_f$ and $|g(x)| < M_g$ for each $x \in \mathbb{R}$. Then for each $x \in \mathbb{R}$

$$\begin{aligned} |(f+g)(x)| &\leqslant |f(x)| + |g(x)| < M_f + M_g \\ |(-f)(x)| &= |-f(x)| = |f(x)| < M_f \\ |(f \cdot g)(x)| &= |f(x)g(x)| = |f(x)| \cdot |g(x)| < M_f M_g \end{aligned}$$

which means that $f+g$, $-f$ and $f \cdot g$ are bounded functions. This means that the ring operations on $F(\mathbb{R}, \mathbb{C})$ restrict to continuous functions and to bounded functions and hence to $C_0(\mathbb{R}, \mathbb{C})$, which is a subring of $F(\mathbb{R}, \mathbb{C})$.

(c) If $f \in C(\mathbb{R}, \mathbb{C})^\times$ or $f \in C_0(\mathbb{R}, \mathbb{C})^\times$, then there exists an inverse in the relevant subring and hence in $F(\mathbb{R}, \mathbb{C})$. This implies that

$$C(\mathbb{R}, \mathbb{C})^\times \subseteq C(\mathbb{R}, \mathbb{C}) \cap F(\mathbb{R}, \mathbb{C})^\times, \quad C_0(\mathbb{R}, \mathbb{C})^\times \subseteq C_0(\mathbb{R}, \mathbb{C}) \cap F(\mathbb{R}, \mathbb{C})^\times,$$

so that by part a) we can restrict our attention to functions f such that $f(x) \neq 0$ for all $x \in \mathbb{R}$. By basic calculus, when such a function is continuous, so is the function $\frac{1}{f}$. This means that

$$\begin{aligned} C(\mathbb{R}, \mathbb{C})^\times &= C(\mathbb{R}, \mathbb{C}) \cap F(\mathbb{R}, \mathbb{C})^\times \\ &= \{f : \mathbb{R} \longrightarrow \mathbb{C} | \forall x \in \mathbb{R}\ f(x) \neq 0 \text{ and } f \text{ is continuous}\}. \end{aligned}$$

Now let $f \in C_0(\mathbb{R}, \mathbb{C}) \cap F(\mathbb{R}, \mathbb{C})^\times$. Since the inverse of an element is unique, f is invertible in $C_0(\mathbb{R}, \mathbb{C})$ if and only if $\frac{1}{f}$ is in $C_0(\mathbb{R}, \mathbb{C})$, which is the case if and only if $\frac{1}{f}$ is bounded (since it is always continuous, as we have just noticed). Notice that, for all $x \in \mathbb{R}$

$$\left|\frac{1}{f}(x)\right| < N_f \iff |f(x)| > \frac{1}{N_f},$$

so that f is invertible if and only if there exists $\varepsilon > 0$ such that $|f(x)| > \varepsilon$ for all $x \in X$. Hence

$$C_0(\mathbb{R}, \mathbb{C})^\times = \left\{ f : \mathbb{R} \longrightarrow \mathbb{C} \;\middle|\; \begin{array}{c} \exists \varepsilon > 0, \exists N > 0 \in \forall x \in X \varepsilon < |f(x)| < N \\ \text{and } f \text{ is continuous} \end{array} \right\}.$$

(d) $C_0(\mathbb{R}, \mathbb{C})$ is not an integral domain. Indeed, considering the functions $f_1, f_2 : \mathbb{R} \longrightarrow \mathbb{C}$

$$f_1(x) := \begin{cases} 0 & \text{if } x < 0 \text{ or } x > 1 \\ x - x^2 & \text{if } x \in [0,1] \end{cases}$$
$$f_2(x) := \begin{cases} 0 & \text{if } x < -1 \text{ or } x > 0 \\ -x - x^2 & \text{if } x \in [-1,0], \end{cases}$$

we see that they are continuous (since $f_1(0) = f_1(1) = 0$ and $f_2(-1) = f_2(0) = 0$) and bounded, since they both have image in $\mathbb{R}_{\geqslant 0}$ and maximum value $\frac{1}{4} = f_1(\frac{1}{2}) = f_2(-\frac{1}{2})$, which shows moreover that $f_1 \neq 0 \neq f_2$. But $f_1 \cdot f_2 = 0$ because $f_1(x) = 0$ for $x \leqslant 0$ and $f_2(x) = 0$ for $x > 0$, so that $f_1(x)f_2(x) = 0$ for all $x \in \mathbb{R}$. Hence f_1 and f_2 are zero-divisors and $C_0(\mathbb{R}, \mathbb{C})$ is not an integral domain.

(e) i. φ is a ring homomorphism. Indeed $\varphi(1) = 1(1) = 1$, whereas for $f, g \in C_0(\mathbb{R}, \mathbb{C})$ we observe that

$$\begin{aligned} \varphi(f+g) &= (f+g)(1) = f(1) + g(1) = \varphi(f) + \varphi(g) \\ \varphi(f \cdot g) &= (f \cdot g)(1) = f(1)g(1) = \varphi(f)\varphi(g). \end{aligned}$$

ii. ψ is not a ring homomorphism, because it does not respect the sum. For example, let $f, g : \mathbb{R} \longrightarrow \mathbb{C}$ be defined by

$$f(x) = \sin(x), \;\; g(x) = -\sin(x).$$

Then $|f(x)| = |g(x)| = |\sin(x)| \leqslant 1$ for all $x \in \mathbb{R}$ (so that $f, g \in C_0(\mathbb{R}, \mathbb{C})$, and since $|f(\pi/2)| = |g(\pi/2)| = 1$ we see that $\sup|f| = \sup|g| = 1$. This means that $\psi(f) = \psi(g) = 1$. Clearly, $f + g = 0$, so that

$$\psi(f+g) = 0 \neq 2 = \psi(f) + \psi(g)$$

and ψ is not a ring homomorphism.

iii. η is not a ring homomorphism, because it does not respect the product. For example, let $f = g : \mathbb{R} \longrightarrow \mathbb{C}$ be the constant function with value i. Then $f \cdot g = -1$, the constant function with value -1. Then, since $\mathrm{Re}(i) = 0$ and $\mathrm{Re}(-1) = -1$,

$$\eta(fg) = -1 \neq 0 = 0 \cdot 0 = \eta(f)\eta(g)$$

and η is not a ring homomorphism.

iv. θ is a ring homomorphism. Indeed, $1_{\mathbb{Z}}$ is mapped to the constant function of value 1, and for each $n, m \in \mathbb{Z}$, the sum (resp., the product) of the function of constant value n with the function of constant value m is the function of constant value $n + m$ (resp., nm).

7. Let $\mathbb{F}_2 \cong \mathbb{Z}/2\mathbb{Z}$ be the field with two elements $0, 1$. Define

$$R := \left\{ \begin{pmatrix} a & b \\ b & a+b \end{pmatrix} : a, b \in \mathbb{F}_2 \right\}.$$

(a) Prove that R is a commutative ring under the usual matrix sum and multiplication.

(b) Prove that R is a field with exactly four elements.

Solution:

(a) As usual, the matrices $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ and $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ (obtained for $(a, b) = (0, 0)$ and for $(a, b) = (1, 0)$ respectively) are seen to be neutral elements for $+$ and

· respectively. Moreover, for each $a, b, a', b' \in \mathbb{F}_2$, we see that

$$\begin{pmatrix} a & b \\ b & a+b \end{pmatrix} + \begin{pmatrix} a' & b' \\ b' & a'+b' \end{pmatrix} = \begin{pmatrix} a+a' & b+b' \\ b+b' & (a+a')+(b+b') \end{pmatrix}$$
$$\begin{pmatrix} a & b \\ b & a+b \end{pmatrix} \begin{pmatrix} a' & b' \\ b' & a'+b' \end{pmatrix} = \begin{pmatrix} aa'+bb' & ab'+a'b+bb' \\ a'b+ab'+bb' & bb'+aa'+ab'+ba'+bb' \end{pmatrix}$$

and both results still belong to R. As can be proven in general, sum of matrices is commutative and associative, whereas multiplication is associative. This proves that R is a ring. Moreover, one can check the commutativity from the above equation by noticing that the result of the multiplication does not change after switching a with a' and b with b'.

(b) There are four choices of parameters $(a, b) \in \mathbb{F}_2^2$. Since the first row of the matrix is (a, b), each choice gives a different matrix. Hence $|R| = 4$. Those matrices are 0_R, 1_R, $\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}$ and $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Notice that $1 \cdot 1 = 1$ and

$$\begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = 1_R,$$

so that each non-zero matrix is invertible in the commutative ring R. Hence R is a field with 4 elements.

8. Let R be a finite integral domain. Prove that R is a field. [*Hint:* For each $x \in R \setminus \{0\}$, consider the map $R \longrightarrow R$ sending $a \mapsto ax$. Is it injective/surjective?]

Solution: Let $x \in R \setminus \{0\}$. Call $f_x : R \longrightarrow R$ the map $a \mapsto ax$. Suppose that $f_x(a) = f_x(b)$ for $a, b \in R$. Then $(a-b)x = ax - bx = f_x(a) - f_x(b) = 0$ and since R is an integral domain and $x \neq 0$ we deduce that $a - b = 0$, so that $a = b$. This implies that f_x is injective. Since R is a finite set, f_x is also surjective. In particular, there exists $y \in R$ such that $yx = f_x(y) = 1_R$, meaning that x has a left inverse. Being R commutative, x has a right inverse as well. By arbitrarity of $x \in R \setminus \{0\}$, we can conclude that R is a field.