THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 2078 Honours Algebraic Structures 2023-24
Homework 7 Solutions
28th March 2024

- If you have any questions, please contact Eddie Lam via echlam@math.cuhk.edu.hk or in person during office hours.

Compulsory Part

1. By definition, a ring homomorphism $\varphi : S \to R$ has to satisfy $\varphi(1_S) = 1_R$ and $\varphi(0_S) = 0_R$. If S is the zero ring, then $1_S = 0_S$, and if $\varphi : 0 \to R$ is a ring homomorphism, then $1_R = \varphi(1_S) = \varphi(0_S) = 0_R$, and $1_R = 0_R$ holds true only if R is also the zero ring.

2. We will consider $\mathbb{Z}_{mn} \cong \mathbb{Z}/mn\mathbb{Z}$ as the quotient ring. In that case, $\phi : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ is a well-defined ring homomorphism requires checking that $\phi(a + mn) = \phi(a)$ for any $a \in \mathbb{Z}$, since a and $a + mn$ represents the same element in the quotient ring $\mathbb{Z}_{mn}$. Indeed, $\phi(a + mn) = ((a + mn)_m, (a + mn)_n) = (a_m, a_n) = \phi(a)$, therefore proving that ϕ is well-defined. The fact that ϕ is a ring homomorphism follows from the definition of addition and multiplication in $\mathbb{Z}_m$ and $\mathbb{Z}_n$, i.e. $a +_m b$ is defined as the remainder of $a + b$ modulo m, therefore $\phi(a + b) = ((a + b)_m, (a + b)_n) = (a_m + b_m, a_n + b_n)$. The case for multiplication is similar. Finally $\phi(1) = (1, 1)$ is clearly the multiplicative identity in $\mathbb{Z}_m \times \mathbb{Z}_n$.

   To show that this is an isomorphism, first note that $|\mathbb{Z}_{mn}| = |\mathbb{Z}_m \times \mathbb{Z}_n| = mn$, therefore to show that ϕ is bijective, it suffices to show that it is injective. Note that if $\phi(a) = (a_m, a_n) = (0, 0)$, then a is divisible by both m and n, and thus a is a multiple of $mn = \text{lcm}(m, n)\gcd(m, n) = \text{lcm}(m, n)$. So $a = 0 \in \mathbb{Z}_{mn}$.

   Remark: More ideally, one should prove this by invoking first isomorphism theorem on the homomorphism $\psi : \mathbb{Z} \to \mathbb{Z}_m \times \mathbb{Z}_n$ since such a homomorphism is necessarily well-defined and canonical.

3. $Z(R) := \{r \in R | rs = sr, \forall s \in R\}$. It suffices to show that $Z(R)$ is closed under addition, additive inverse and multiplication, and that $1_R \in Z(R)$. The last property is clear since $1_R r = r 1_R = r$ by definition of multiplicative identity. For closedness, note that if $r, s \in Z(R)$, then $(r - s)t = rt - st = tr - ts = t(r - s)$, so $r - s \in Z(R)$ and it is a subgroup. Finally for closedness under multiplication, if $r, s \in Z(R)$, then $rst = rts = trs$, so $rs \in Z(R)$.

4. Let $x \in I_a$, then $ax = 0$, so if $r \in R$, we also have $a(rx) = r(ax) = r0 = 0$, so that $rx \in I_a$. It is also clear that I_a is an additive subgroup, since $ax = 0$ if and only if $-ax = 0$, and if $x, y \in I_a$, we have $a(x - y) = ax - ay = 0 - 0 = 0$, so that $x - y \in I_a$. The ideal I_a is called the annihilator of a.

5. (a) See Tutorial 9 Q1.

   (b) See Tutorial 9 Q1.

(c) IJ is clearly closed under addition since sum of two elements of the form $r = \sum_{i=1}^n a_i b_i$ is still an element of the same form. If $r = \sum_{i=1}^n a_i b_i \in IJ$ then its additive inverse $-r = \sum_{i=1}^n (-a_i) b_i \in IJ$ since $-a_i \in I$. Therefore IJ is an additive subgroup. Now pick $r \in IJ$ and $x \in R$ be any element, then $xr = \sum_{i=1}^n (xa_i) b_i \in IJ$ since $xa_i \in I$ as I is an ideal. Similarly, $rx = \sum_{i=1}^n a_i (b_i x) \in IJ$ as $b_i x \in J$.

6. See Tutorial 9 Q7.

Optional Part

1. Consider the map $\phi : \mathbb{R}[x] \to M_2(\mathbb{R})$ defined by $\phi(a) = \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ for any $a \in \mathbb{R}$ and $\phi(x) = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. We will show that ϕ is a ring homomorphism such that $\mathrm{im}(\phi) = R$ and $\ker(\phi) = (x^2+1)$, therefore by first isomorphism theorem $\mathbb{R}[x]/(x^2+1) \cong R$. On the other hand, $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$ according to results from the lectures.

   Given any $f(x) = \sum_{i=0}^n a_i x^i$, from the definition we have $\phi(f(x)) = \sum_{i=0}^n a_i \phi(x)^i = f(\phi(x))$, i.e. the same polynomial expression evaluating at the matrix $\phi(x)$. From this, it is clear that $\phi(f(x)+g(x)) = f(\phi(x))+g(\phi(x)) = \phi(f(x))+\phi(g(x))$ and $\phi(f(x)g(x)) = f(\phi(x))g(\phi(x)) = \phi(f(x))\phi(g(x))$. Finally, $\phi(1) = I$ is the identity matrix. So ϕ is indeed a ring homomorphism.

   It is also clear that $\phi(x)^2 = I = \phi(1))$ and so $\phi(x^2-1) = 0$. So $(x^2-1) \subset \ker\phi$. Conversely if $\phi(f(x)) = f(\phi(x)) = 0$ then by linear algebra $f(x)$ is a multiple of the minimal polynomial of $\phi(x)$, which can be easily seen to be x^2+1 (it has distinct eigenvalues, so the minimal and characteristic polynomials coincide). This implies that $\ker\phi \subset (x^2+1)$, as claimed.

   Therefore, given a general $f(x) \in \mathbb{R}[x]$, we may write $f(x) = (x^2+1)p(x) + q(x)$ where $p(x), q(x) \in \mathbb{R}[x]$ with $\deg q < \deg(x^2+1) = 2$. Writing $q(x) = bx + a$, then $\phi(f(x)) = \phi(x^2+1)\phi(p(x)) + \phi(bx+a) = b\phi(x) + \phi(a) = \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$. Therefore the image of ϕ is precisely R. This completes the proof.

2. (a) No, it is not a group homomorphism on the underlying additive groups. For example, $\phi(n+m) = (n+m)^2 \neq n^2 + m^2 = \phi(n) + \phi(m)$ for general m, n.

   (b) Yes. It suffices to prove that it is well-defined. Then it is a ring homomorphism for the same reason as described in Q2 of compulsory part. For well-definedness it suffices to check $\phi(s+6) = \phi(s)$, which is true as 6 has remainder 0 modulo 3.

   (c) No, it is not a well-defined group homomorphism. For example, $3\mathbb{Z} = \phi(0) = \phi(3+4) = \phi(3) + \phi(4) = (3+3\mathbb{Z}) + (4+3\mathbb{Z}) = 7+3\mathbb{Z} = 1+3\mathbb{Z}$, which is clearly a contradiction.

3. No, a ring homomorphism $\phi : \mathbb{Z}_7 \to \mathbb{Z}_5$ (if exists), would satisfy $\phi(1) = 1$. Therefore $0 = \phi(0) = \phi(7 \cdot 1) = 7\phi(1) = 2 \in \mathbb{Z}_5$, which is clearly a contradiction.

4. (a) It is possible, for example the one exhibited in optional Q2b.

(b) It is also possible, for any ring S, we always have a (unique) homomorphism $\mathbb{Z} \to S$ by sending $1 \mapsto 1_S$, regardless whether S is an integral domain. For example, one may consider the quotient map $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ for n a composite number.

5. (a) No, if $f \in I$, then $2f \notin I$ since $2a_0$ is no longer odd.

   (b) No, it is not an additive subgroup. For example, $2x^2 + x, -2x^2 \in I$ but $(2x^2 + x) - 2x^2 = x \notin I$.

   (c) Yes, clearly I is additive as sum/difference of even numbers is still even. And if $r + 6\mathbb{Z} \in I$ and $k + 6\mathbb{Z} \in \mathbb{Z}/6\mathbb{Z}$, we have r is even and $(r + 6\mathbb{Z})(k + 6\mathbb{Z}) = rk + 6\mathbb{Z}$ with rk even, so the product is in I, so it forms an ideal.

6. By tutorial 9 Q4, the ideal $(m) \cap (n)$ is principal and is given by (k) where k is the smallest positive integer in $(m) \cap (n)$. Without loss of generality we may assume m, n are positive integers as well, otherwise simply replace m by $-m$.

   Therefore, it suffices to show that the smallest positive integer in $(m) \cap (n)$ is mn. This is clear since (m) and (n) consist of all multiples of m and n respectively, so $(m) \cap (n)$ consists of all common multiples of m and n, thus the smallest such positive integer is the least common multiple, i.e. $k = \text{lcm}(m, n) = mn/\gcd(m, n) = mn$.