THE CHINESE UNIVERSITY OF HONG KONG
Department of Mathematics
MATH 2078 Honours Algebraic Structures 2023-24
Homework 8 Solutions
4th April 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. It suffices to show that there are no ring homomorphism from $\mathbb{C}$ to $\mathbb{R}$, then there would be no ring homomorphism from a ring R that contains $\mathbb{C}$ to $\mathbb{R}$ as it would restrict to one from $\mathbb{C}$ to $\mathbb{R}$.

   Let $\phi : \mathbb{C} \to \mathbb{R}$ and $\phi(i) = a \in \mathbb{R}$, then $0 = \phi(0) = \phi(i^2 + 1) = \phi(i)^2 + \phi(1) = a^2 + 1$. This implies that there is a real number whose square is -1, which is a contradiction.

2. See Tutorial 9 Q2.

3. Let $a + N \in R/N$, if it is nilpotent, then $(a + N)^k = a^k + N = 0 + N$ for some $k > 0$. This implies that $a^k \in N$, i.e. a^k is nilpotent, so there is some n so that $a^{nk} = 0$. So a is in fact also nilpotent and $a \in N$, so that $a + N = 0 + N$.

4. Let $\phi : R \to R'$ be a homomrphism so that $\phi(I) \subset I'$. Define $\phi_* : R/I \to R'/I'$ by $\phi_*(a + I) = \phi(a) + I'$. We will show that this is a well-defined ring homomorphism.

   It is well-defined because if $a, b \in R$ represents the same coset, i.e. $a + I = b + I$, then $a - b \in I$, so that $\phi(a - b) \in \phi(I) \subset I'$, in particular $\phi(a)$ and $\phi(b)$ represents the same I'-cosets, therefore $\phi_*(a + I) = \phi(a) + I' = \phi(b) + I' = \phi_*(b + I)$.

   ϕ_* is a ring homomorphism because $\phi_*((a+I)+(b+I)) = \phi_*(a+b+I) = \phi(a+b)+I' = (\phi(a) + I') + (\phi(b) + I') = \phi_*(a + I) + \phi_*(b + I)$. And similarly $\phi_*((a + I)(b + I)) = \phi_*(ab + I) = \phi(ab) + I' = (\phi(a) + I')(\phi(b) + I') = \phi_*(a + I)\phi_*(b + I)$. Finally, $\phi_*(1 + I) = \phi(1) + I' = 1 + I'$ is the multiplicative identity element in R'/I'.

5. Let $I \subset J$ be ideals of R, to show that J/I is an ideal in R/I, first note that it is an additive subgroup: if $a, b \in J$ so that $a + I, b + I$ are general elements in J/I, then $(a + I) - (b + I) = (a - b) + I \in J/I$ since $a - b \in J$ as it is an ideal. Similarly, if $r + I \in R/I$ and $a + I \in J/I$ then $(r + I)(a + I) = ra + I \in J/I$ because $ra \in J$.

   To prove the isomorphism, we will construct a surjective homomorphism

   $$\phi : R/I \to R/J,$$

   such that $\ker \phi = J/I$, then by first isomorphism theorem, we get the result.

   Here ϕ is defined by $\phi(a + I) = a + J$. It is well-defined because if $a + I = b + I$, then $a - b \in I \subset J$, so $a + J = b + J$ as well. It is clearly a ring homomorphism as $\phi((a+I)+(b+I)) = \phi(a+b+I) = a+b+J = (a+J)+(b+J) = \phi(a+I)+\phi(b+I)$; and $\phi((a+I)(b+I)) = \phi(ab+I) = ab+J = (a+J)(b+J) = \phi(a+I)\phi(b+I)$. And $\phi(1 + I) = 1 + J$ is the multiplicative identity.

The homomorphism is surjective because any $a + J \in R/J$ is the image of $a + I \in R/I$. And $\ker \phi = J/I$ because $\phi(a + I) = a + J = 0 + J$ if and only if $a \in J$, if and only if $a + J \in J/I$. This concludes the proof.

6. See the discussion in Tutorial 10 Q5. $\mathbb{Z}[i]/(a + bi) \cong \mathbb{Z}/(a^2 + b^2)\mathbb{Z}$ holds when a, b are coprime.

   For $\mathbb{Z}[i]/(2 + 2i)$, it is a commutative ring with 8 elements, but it is not isomorphic to $\mathbb{Z}_8$. Suppose there is an isomorphism $\phi : \mathbb{Z}[i]/(2 + 2i) \to \mathbb{Z}_8$, let $a \in \mathbb{Z}_8$ be the image of $\bar{i}$. Since $\bar{i}^2 = \overline{-1}$, whose image is $-1 \in \mathbb{Z}_8$. This implies that $a^2 \equiv -1 \equiv 7$ in $\mathbb{Z}_8$. However, we have $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1$ and $2^2 \equiv 6^2 \equiv 4$ and $0^2 \equiv 4^2 \equiv 0$. So such an a does not exist.

Optional Part

1. Let $\{I_i\}_{i \in J}$ be an arbitrary collection of ideals in R, the $I := \bigcap_{i \in J} I_i$ is an ideal because arbitrary intersection of additive subgroup is an additive subgroup. And if $a \in I$ and $r \in R$, then $ar, ra \in I_i$ for all $i \in J$ since each I_i is an ideal, so $ar, ra \in I$ as desired.

2. Suppose $\phi : \mathbb{Q} \to \mathbb{Z}_n$ is a ring homomorphism, then $\phi(n) = n\phi(1) = n1 = 0 \in \mathbb{Z}_n$. But $\phi(n)\phi(1/n) = \phi(n \cdot 1/n) = \phi(1) = 1$ would imply that there exists a multiplicative inverse of $\phi(n) = 0$, this is clearly absurd.

3. First note that $(a) = (b)$ is equivalent to $a \in (b)$ and $b \in (a)$. Therefore it is equivalent to the existence of $r, s \in R$ so that $a = rb$ and $b = sa$. Now this implies that $a = (rs)a$. By cancellation law (which is valid for integral domain D), we have $rs = 1$, so in fact $r, s \in D^\times$.

   Conversely, if $a = ub$ for some unit u, then $u^{-1}a = b$ and we have both $a \in (b)$ and $b \in (a)$, so the two ideals are equal.

4. If $u \in R$ is a unit, then $ru^{-1}u = r \in (u)$ for arbitrary $r \in R$. So $(u) = R$ and $R/(u) = R/R = 0$ is the zero ring.

5. (a) A quotient ring has its additive structure given by quotient group, so the order can be computed by considering quotient group. The underlying additive group of $\mathbb{Z}_{12}$ is just the additive group of integers modulo 12, so $|\mathbb{Z}_{12}| = 12$, and $(3) = \{0, 3, 6, 9\}$ is an ideal (subgroup) of order 4, so the quotient group (hence ring) has order $12/4 = 3$ by Lagrange's theorem.

   (b) $5 \in \mathbb{Z}_{12}$ is a unit since $5^2 = 25 = 1 \in \mathbb{Z}_{12}$, so by Q4 we know $\mathbb{Z}_{12}/(5)$ is the zero ring, it has 1 element.

   (c) There are as many equivalence classes as there are degree $0, 1$ and 2 polynomials in $\mathbb{Z}_2[x]$. The reason is, any equivalence class is represented by some polynomial $p(x) \in \mathbb{Z}_2[x]$, and we may perform division algorithm and write $p(x) = (x^3 + 1)q(x) + r(x)$, where $q, r \in \mathbb{Z}_2[x]$ with $\deg r(x) < \deg(x^3 + 1) = 3$. Note that $(x^3 + 1)q(x)$ is in the ideal $(x^3 + 1)$, so $p(x)$ and $r(x)$ represents the same class. This means that any class is represented by a polynomial of degree $0, 1$ or 2. And if $r_1(x)$ and $r_2(x)$ are degree $0, 1$ or 2 polynomials that represent the same class, then $r_1 - r_2 \in (x^3 + 1)$, the only possibility is that they are equal by degree consideration.

Thus the classes are represented by $0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1$ and there are 8 distinct classes.

6. (a) ϕ as defined is a ring homomorphism because complex conjugation is a ring homomorphism. Write $c : \mathbb{Z}[i] \to \mathbb{Z}[i]$ where $c(z) = \overline{z}$, then we know that $\overline{z+w} = \overline{z}+\overline{w}$ and $\overline{zw} = \overline{z} \cdot \overline{w}$ and conjugate of 1 is itself. Therefore, one can realize ϕ as the composition of the conjugation map c, followed by the canonical projection $\pi : \mathbb{Z}[i] \to \mathbb{Z}[i]/(a-bi)$ by $z \mapsto z + (a-bi)$.

   (b) This is clear because given any $z + (a-bi) \in \mathbb{Z}[i]/(a-bi)$ we have $z + (a-bi) = \phi(\overline{z})$, so ϕ is surjective.

   (c) Note that

$$
\begin{aligned}
c + di \in \ker\phi &\iff \phi(c+di) = c - di + (a-bi) = 0 + (a-bi) \\
&\iff c - di \in (a-bi) \\
&\iff c - di = k(a-bi),\ k \in \mathbb{Z}[i] \\
&\iff c + di = \overline{k}(a+bi),\ \overline{k} \in \mathbb{Z}[i] \\
&\iff c + di \in (a+bi)
\end{aligned}
$$

   So $\ker\phi = (a+bi)$.

   (d) By the first isomorphism theorem, $\mathbb{Z}[i]/(a+bi) = \mathbb{Z}[i]/\ker\phi \cong \operatorname{im}(\phi) = \mathbb{Z}[i]/(a-bi)$.

7. (a) I is an additive subgroup since if $f, g \in I$, then $(f+g)(0) = f(0)+g(0) = 0+0 = 0$. And if $f \in I$ and $h \in R$, then $(fh)(0) = f(0)h(0) = 0h(0) = 0$, so I is an ideal.

   (b) Define $\phi : R \to \mathbb{R}$ by $\phi(f) = f(0)$. Then ϕ is a ring homomorphism because $\phi(f+g) = (f+g)(0) = f(0) + g(0) = \phi(f) + \phi(g)$ and $\phi(fg) = (fg)(0) = f(0)g(0) = \phi(f)\phi(g)$, and $\phi(1) = 1$ for the constant function.

   This homomorphism is surjective since for any $a \in \mathbb{R}$, regarded a as the constant function with value a, we have $\phi(a) = a$. And $\ker\phi = I$ by definition of I.

   Therefore by first isomorphism theorem $R/I \cong \mathbb{R}$.

8. Let D be a PID and I an ideal of D, let $J \subset D/I$ be an ideal of the quotient ring. Write $\pi : D \to D/I$ the canonical projection map, then $\pi^{-1}(J)$ is an ideal of D, hence it is principal. Denote $(b) = \pi^{-1}(J)$. Clearly, $(b) = \pi^{-1}(J) \supset \pi^{-1}(0) = I$, therefore by by compulsory Q5, $(b)/I$ is an ideal of D/I. We will show that $(b)/I = J$, therefore J is generated by $b + I \in D/I$.

   Let $c + I \in J$, then $\pi(c) = c + I$, so that $c \in \pi^{-1}(J) = (b)$, therefore $c + I \in (b)/I$. Conversely, if $c + I \in (b)/I$, then $c - rb \in I$ for some $r \in R$, in particular, $c \in (b) = \pi^{-1}(J)$, so $c + I = \pi(c) \in J$.

   This concludes the claim since $(b)/I$ is a principal ideal since by definition $(b)/I := \{x + I : x \in (b)\}$, so $(b)/I = (b + I)$ (the ideal generated by $b + I$).