Rings, fields, and modules
Exercise sheet 2

https://www.maths.tcd.ie/~mascotn/teaching/2021/MAU22102/index.html

Version: March 5, 2021

Email your answers to aylwarde@tcd.ie by Friday March 5, 4PM.

Exercise 1 *The characteristic of a ring (100 pts)*

Let R be a commutative ring. We note that that there exists one and only one ring morphism from $\mathbb{Z}$ to R: indeed, if f is such a morphism, then $f(0_\mathbb{Z}) = 0_R$, $f(1_\mathbb{Z}) = f(1_R)$, and so $f(2_\mathbb{Z}) = f(1_\mathbb{Z} + 1_\mathbb{Z}) = f(1_\mathbb{Z}) + f(1_\mathbb{Z}) = 1_R + 1_R$, and more generally $f(n) = \underbrace{1_R + \cdots + 1_R}_{n}$ for all $n \geq 0$; and finally $f(-n) = -f(n)$, so $f(n) = \underbrace{-1_R - \cdots - 1_R}_{|n|}$ for all $n < 0$, so f is completely determined; and we check easily that this f is indeed a ring morphism (you are *not* required to do this in this exercise). We denote this unique morphism from $\mathbb{Z}$ to R by f_R.

1. (10 pts) Prove that there exists a unique $n \in \mathbb{Z}$, $n \geq 0$, such that $\operatorname{Ker} f_R = n\mathbb{Z}$. You may use without proof the fact that the ring $\mathbb{Z}$ is principal.

This n is called the characteristic *of the ring R; we denote it by* $\operatorname{char} R$.

2. (15+5 pts) Let R be a ring of characteristic c. Prove that R contains a subring isomorphic to $\mathbb{Z}/c\mathbb{Z}$. What does this mean when $c = 0$?

3. Determine the characteristic of the following rings:

   (a) (5 pts) $\mathbb{C}$,

   (b) (5 pts) $\mathbb{Z}/n\mathbb{Z}$, in terms of $n \in \mathbb{Z}$,

   (c) (5 pts) $R[x]$, in terms of $\operatorname{char} R$,

   (d) (10 pts) $R \times S$, where S is another commutative ring, in terms of $\operatorname{char} R$ and $\operatorname{char} S$.

4. (10 pts) Prove that if R is a domain, then $\operatorname{char} R$ is either 0 or a prime number.

5. (10 pts) Let R and S be commutative rings. Prove that if there exists a morphism from R to S, then $\operatorname{char} R$ is a multiple of $\operatorname{char} S$.

6. (5 pts) Find all ring morphisms from $\mathbb{Z}/2021\mathbb{Z}$ to $\mathbb{C}$.

7. (15+5pts) Prove that there are no ring morphisms from $\mathbb{Q}$ to $\mathbb{Z}$; comment.

Solution 1

1. Since f_R is a morphism, its kernel is an ideal of $\mathbb{Z}$. As $\mathbb{Z}$ is principal, there exists $n \in \mathbb{Z}$ such that $\operatorname{Ker} f_R = n\mathbb{Z}$. Besides, it is clear that $(-n)\mathbb{Z} = n\mathbb{Z}$, so replacing n with $-n$ if needed, we may assume $n \geq 0$; this proves the existence part of the question.

   For uniqueness, suppose that $\operatorname{Ker} f_R = n\mathbb{Z} = m\mathbb{Z}$ for non-negative $n, m \in \mathbb{Z}$. Then $n \in n\mathbb{Z} = m\mathbb{Z}$ so n is a multiple of m, so $n \geq m$ as they are both non-negative; similarly $m \in n\mathbb{Z}$ so $m \geq n$, whence $m = n$.

   Note that we have actually proved that in general, $n\mathbb{Z} = m\mathbb{Z}$ iff. $m = \pm n$; we will generalise this observation in the lectures when we introduce the concept of associate elements in a domain.

   Also note that $\operatorname{char} R$ is the smallest $n \geq 1$ such that $\underbrace{1_R + \cdots + 1_R}_{n} = 0_R$, or 0 if no such n exists; this definition of the characteristic can be used to obtain alternative proofs to most of the next questions — exercise!

2. The isomorphism theorem applied to $f_R : \mathbb{Z} \longrightarrow R$ proves that $\operatorname{Im} f_R$ is isomorphic to $\mathbb{Z}/\operatorname{Ker} f_R$, which is $\mathbb{Z}/c\mathbb{Z}$ by definition of the characteristic. Besides, we know that $\operatorname{Im} f_R$ is a subring of R, whence the result.

   If $c = 0$, then $\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}/\{0\} \simeq \mathbb{Z}$ as can be seen from the definition of a quotient ring, or (more pedantically maybe) by applying the isomorphism theorem to the identity map from $\mathbb{Z}$ to itself, so the conclusion is that a right of characteristic 0 must contain a copy of $\mathbb{Z}$.

3. (a) The identity map from $\mathbb{Z}$ to $\mathbb{C}$ is clearly a morphism, so it must agree with $f_{\mathbb{C}}$. Besides, it is injective, so its kernel is $\{0\}$; thus $\operatorname{char} \mathbb{C} = 0$ (and indeed $\mathbb{C}$ contains a copy of $\mathbb{Z}$).

   (b) The canonical projection from $\mathbb{Z}$ to its quotient $\mathbb{Z}/n\mathbb{Z}$ us a morphism, so it must agree with $f_{\mathbb{Z}/n\mathbb{Z}}$. Therefore $\operatorname{Ker} f_{\mathbb{Z}/n\mathbb{Z}} = n\mathbb{Z}$, so $\operatorname{char} \mathbb{Z}/n\mathbb{Z} = |n|$ (and indeed $\mathbb{Z}/n\mathbb{Z}$ contains, or rather agrees with, a copy of $\mathbb{Z}/|n|\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}$).

   (c) The embedding $f : R \longrightarrow R[x]$ which views elements of R as constant polynomials is clearly a morphism, so $f_{R[x]}$ must agree with the morphism $f \circ f_R$. Thus for all $n \in \mathbb{Z}$, $f_{R[x]} = 0$ iff. $f(f_R(n)) = 0$ iff. $f_R(n) = 0$ as f is clearly injective, so $\operatorname{Ker} f_{R[x]} = \operatorname{Ker} f_R$, whence $\operatorname{char} R[x] = \operatorname{char} R$.

   (d) It is clear that $f_{R\times S}$ is given by $n \longmapsto \big(f_R(n), f_S(n)\big)$. Therefore $\operatorname{Ker} f_{R\times S} = \operatorname{Ker} f_R \cap \operatorname{Ker} f_S = (\operatorname{char} R)\mathbb{Z} \cap (\operatorname{char} S)\mathbb{Z}$, which agrees with $\operatorname{lcm}(\operatorname{char} R, \operatorname{char} S)\mathbb{Z}$ by a question in the first assignment (see also the chapter 2 lecture on gcd's and lcm's in a UFD). Thus $\operatorname{char} R \times S = \operatorname{lcm}(\operatorname{char} R, \operatorname{char} S)$.

4. We prove the contrapositive. Suppose that $\operatorname{char} R$ is neither 0 nor a prime number. If $\operatorname{char} R = 1$, $1_R = f(1_{\mathbb{Z}}) = 0_R$, so R is the zero ring, which is not considered as a domain. Else, $\operatorname{char} R \geq 2$ is not prime, so we have $\operatorname{char} R = ab$ with integers a, b such that $1 < a, b < \operatorname{char} R$. Then $f_R(a)f_R(b) = f_R(ab) = f_R(\operatorname{char} R) = 0_R$, whereas $f_R(a) \neq 0_R$ as $a \notin \operatorname{Ker} f_R$ since a cannot be a multiple of $\operatorname{char} R$ as $0 < a < \operatorname{char} R$, and similarly $f_R(b) \neq 0_R$. So in R we have two nonzero elements $f_R(a), f_R(b)$ which multiply to 0_R, which shows that R is not a domain.

5. Let $f : R \longrightarrow S$ be a morphism. Then $f \circ f_R : \mathbb{Z} \longrightarrow R \longrightarrow S$ is a morphism, so it must agree with f_S. Thus $f_S(\operatorname{char} R) = f(f_R(\operatorname{char} R)) = f(0_R) = 0_S$, whence $\operatorname{char} R \in \operatorname{Ker} f_S = (\operatorname{char} S)\mathbb{Z}$, which means that $\operatorname{char} R$ is a multiple of $\operatorname{char} S$.

6. If we had a morphism $f : \mathbb{Z}/2021\mathbb{Z} \longrightarrow \mathbb{C}$, then by the previous question $2021 = \operatorname{char} \mathbb{Z}/2021\mathbb{Z}$ would be a multiple of $0 = \operatorname{char} \mathbb{C}$, absurd. Therefore there are no such morphisms.

7. Suppose $f : \mathbb{Q} \longrightarrow \mathbb{Z}$ is a morphism. Then $2f(1/2) = f(1) = 1$, which is absurd as there are no $n \in \mathbb{Z}$ such that $2n = 1$. Therefore there are no such morphisms.

   As $\operatorname{char} \mathbb{Z} = \operatorname{char} \mathbb{Q} = 0$, this proves that the converse to the statement established in question 5 does not hold.

This was the only mandatory exercise, that you must submit before the deadline. The following exercise is not mandatory; it is not worth any points, and you do not have to submit it. However, I highly recommend that you try to solve it for practice, and you are welcome to email me if you have questions about it. The solution will be made available with the solution to the mandatory exercise.

Exercise 2 *Ideals in a quotient*

In this exercise, whenever $f : X \longrightarrow Y$ is a map between two sets, for each subset $S \subseteq X$ we define $f(S) = \{f(s), s \in S\} \subseteq Y$; and for each subset $T \subseteq Y$, we define $f^{-1}(T) = \{x \in X \mid f(x) \in T\}$.

1. Let R be a commutative nonzero ring. Prove that R is a field iff. the only ideals of R are $\{0\}$ and R.

2. Let $f : R \longrightarrow S$ be a morphism between commutative rings.

   (a) Prove that if f is surjective, then for every ideal I of R, $f(I)$ is an ideal of S.

   (b) Give a counter-example showing that this statement is no longer true if f is not surjective.

3. Let again $f : R \longrightarrow S$ be a morphism between commutative rings.

   (a) Prove that if J is an ideal of S, then $f^{-1}(J)$ is an ideal of R.

   (b) Which statement proved in class do we recover by taking $J = \{0\}$?

4. Let now R be a commutative ring, I an ideal of R, and $f : R \longrightarrow R/I$ the canonical projection.

(a) Prove that the maps

$$\begin{array}{rccc} \Phi : & \{\text{Ideals of } R \text{ containing } I\} & \longrightarrow & \{\text{Ideals of } R/I\} \\ & J & \longmapsto & f(J) \end{array}$$

and

$$\begin{array}{rccc} \Psi : & \{\text{Ideals of } R/I\} & \longrightarrow & \{\text{Ideals of } R \text{ containing } I\} \\ & J & \longmapsto & f^{-1}(J) \end{array}$$

are well-defined, i.e. that their images land where their definitions claim they land.

(b) Prove that Φ and Ψ are inclusion-preserving bijections which are inverses of each other.

5. Let R be a commutative ring, and let I be an ideal of R. We say that I is *maximal* if $I \neq R$ and if there are no ideals J of R such that $I \subsetneq J \subsetneq R$ (This definition occurs in the lecture on prime and maximal ideals, but you need not study this lecture to solve this question). By using the previous question(s), prove that R/I is a field iff. I is maximal.

   NB This statement also occurs in the lecture on prime and maximal ideals, but the proof that we give in this exercise is a different one.

Solution 2

1. If R is a field, then every nonzero element is invertible, and therefore every ideal not reduced to $\{0\}$ contains an invertible element and therefore agrees with R. Conversely, if R is not a field, then there exists $0 \neq r \in R$ which is not invertible; then the ideal (r) of R is not $\{0\}$ since it contains $r \neq 0$, and it is not R either, for else we would have $1 \in (r)$ whence $1 = rx$ for some $x \in R$, contradicting our assumption that r is not invertible.

2. (a) Let I be an ideal of R. By definition, the elements of $f(I)$ are the $f(i)$ for $i \in I$. In particular, $0 = f(0) \in f(I)$ as $0 \in I$. $f(I)$ is also closed by sum, since if $j_1, j_2 \in f(I)$, then $j_1 = f(i_1)$ and $j_2 = f(i2)$ for some $i_1, i_2 \in I$, and then $f(i_1) + f(i_2) = f(i_1 + i_2) \in f(I)$ as I is closed by sum. Finally, let $j \in f(I)$, and let $s \in S$. We have $j = f(i)$ for some $i \in I$, and also $s = f(r)$ for some $r \in R$ as f is surjective. Thus $sj = f(r)f(i) = f(ri) \in f(I)$ as I is an ideal.

   (b) Consider the identity map from $\mathbb{Z}$ to $\mathbb{Q}$ (or $\mathbb{R}$, or $\mathbb{C}$, it does not matter). $\mathbb{Z}$ is an ideal of $\mathbb{Z}$, yet the image of this ideal, which is still $\mathbb{Z}$, is not an ideal of $\mathbb{Q}$ since the only ideals of $\mathbb{Q}$ are $\{0\}$ and $\mathbb{Q}$ as $\mathbb{Q}$ is a field.

3. (a) Let $I = f^{-1}(J)$. We have $0 \in I$, because $f(0) = 0 \in J$. Let $i_1, i_2 \in I$; then $f(i_1 + i_2) = f(i_1) + f(i_2) \in J$ since $f(i_1), f(i_2) \in J$ by definition of I, so $i_1 + i_2 \in I$, and I is closed under sum. Finally, let $i \in I$¡ and let $r \in R$; then $f(ri) = f(r)f(i) \in J$ as $f(r) \in S$ and $f(i) \in J$, so $ri \in I$, which shows that I is an ideal of R.

   (b) $\{0\}$ is certainly an ideal of S, and we have

$$f^{-1}(\{0\}) = \{r \in R | f(r) \in \{0\}\} = \{r \in R | f(r) = 0\} = \operatorname{Ker} f,$$

   so we recover the fact that $\operatorname{Ker} f$ is an ideal of R.

4. (a) The canonical projection f is surjective by definition, so by question 2a, if J is an ideal of R, then $f(J)$ is an ideal of R/I.

   By question 3a, if J is an ideal of R/I, then $f^{-1}(J)$ is an ideal of R; besides, if $i \in I$, then $f(i) = \overline{0}$ by definition of f, so $f(i) \in J$ as $J \ni \overline{0}$ is an ideal, so $i \in f^{-1}(J)$; this shows that indeed $I \subseteq f^{-1}(J)$.

   (b) This is typically the kind of question where you should take a deep breath, patiently unroll the definitions, and calmly prove double-inclusions.

   Let J be an ideal of R containing I, and let $J' = \Psi\Phi(J) = f^{-1}\big(f(J)\big)$. If $j \in J$, then $f(j) \in f(J)$, so $j \in f^{-1}\big(f(J)\big) = J'$, whence $J \subseteq J'$. Conversely, let $j' \in J'$; then $f(j') \in f(J)$, so there exists $j \in J$ such that $f(j') = f(j)$. Thus $f(j'-j) = f(j') - f(j) = 0$, so $j' = j \in \operatorname{Ker} f = I$, so $j' = j + i$ for some $i \in I$. As $I \subseteq J$, this implies that $j' \in J$, whence $J' \subseteq J$. In conclusion, $J = J'$.

   Let now J be an ideal of R/I; then

$$\begin{aligned}\Phi\Psi(J) &= f\big(f^{-1}(J)\big)\\ &= f\big(\{x \in R \,|\, f(x) \in J\}\big)\\ &= \{f(x) \mid x \in R, f(x) \in J\}\end{aligned}$$

   which is clearly contained in J. Conversely, if $j \in J$, then $j \in R/I$ so is of the form $\overline{x}$ for some $x \in R$, which is such that $f(x) = \overline{x} = j \in J$, so that $x \in f^{-1}(J)$; therefore $j = f(x) \in f\big(f^{-1}(J)\big)$, which proves the reverse containment and hence the equality $J = f\big(f^{-1}(J)\big)$.

   Finally, it is clear form the definition of f and f^{-1} on subsets that these maps preserve the inclusion between subsets.

5. The previous question shows that the ideals of R/I may be identified with the ideals of R which contain I.

   If I is maximal, the only such ideals are I and R, so the only ideals of R/I are $f(I) = \{\overline{0}\}$ and $f(R) = R/I$, so R/I is a field by question 1.

   Conversely, still by question 1, if R/I is a field, then it only has 2 ideals, so there are only 2 ideals of R which contain I; as I and R are such ideals, this must be all of them, which means that I is maximal.