Rings, fields, and modules
Exercise sheet 1

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

Version: February 19, 2021

Email your answers to aylwarde@tcd.ie by Friday February 19, 4PM.

Exercise 1 *Arithmetic on ideals (100 pts)*

In this exercise, we fix a commutative ring R, and given elements $r_1, \cdots, r_m$ of R, we write $(r_1, \cdots, r_m)$ for the ideal generated by $r_1, \cdots, r_m$; this generalises the notation (r) for principal ideals.

Reminder: In order to prove an if and only if, it is often convenient to prove both implications separately. In order to prove that two subsets A and B are equal, it is often convenient to prove separately that $A \subseteq B$ and that $B \subseteq A$.

1. (10 pts) Let $I \subseteq R$ be an ideal, and let $r \in R$. Prove that $r \in I$ if and only if $(r) \subseteq I$.

2. (a) (10 pts) Let $r_1, \cdots, r_m \in R$. Prove that

$$(r_1, \cdots, r_m) = \{x_1 r_1 + \cdots + x_m r_m \mid x_1, \cdots, x_m \in R\}.$$

   (b) (5 pts) Let $r_1, \cdots, r_m \in R$. Prove that

$$(r_1, \cdots, r_m) = (r_1) + \cdots + (r_m).$$

   (c) (10 pts) Let $r, s \in R$. Prove that $(r)(s) = (rs)$.

   (d) (10 pts) More generally, prove that if $r_1, \cdots, r_m, s_1, \cdots, s_n \in R$, then

$$(r_1, \cdots, r_m)(s_1, \cdots, s_n) = (r_1 s_1, \cdots, r_1 s_n, r_2 s_1, \cdots, r_2 s_n, \cdots, r_m s_1, \cdots, r_m s_n).$$

3. (15 pts) In this question, we take $R = \mathbb{Z}[x]$, and we consider the ideal $I = \{P(x) \in \mathbb{Z}[x] \mid P(0) \text{ is even}\} \subset R$. Prove that $I = (2, x)$.

4. (15 pts) In this question, we take $R = \mathbb{Z}$, and we admit without proof the following facts:

   - *For all $n, m \in \mathbb{Z}$, $\gcd(m, n)$ divides m and n and is of the form $mu + nv$ with $u, v \in \mathbb{Z}$.*
   - *For all $n, m \in \mathbb{Z}$, every common multiple of m and n is a multiple of the lowest common multiple $\operatorname{lcm}(m, n)$.*
   - *Every ideal of $\mathbb{Z}$ is principal.*

Let $m, n \in \mathbb{Z}$. Since every ideal of $\mathbb{Z}$ is principal, there must exist $a, b, c \in \mathbb{Z}$ such that $(m) + (n) = (a)$, $(m) \cap (n) = (b)$, and $(m)(n) = (c)$. Express a, b, c in terms of m and n, and prove that your answer is correct.

5. In this question, R is a general commutative ring, and I and J are ideals of R.

   (a) (15 pts) Prove that
   $$IJ \subseteq I \cap J \subseteq I \subseteq I + J.$$

   (b) (10 pts) Find an example where all these inclusions are strict.
   Hint: Take $R = \mathbb{Z}$, and use the previous question.

Solution 1

1. We prove one implication and its converse separately.

   If $r \in I$, then since I is an ideal, we have $rx \in I$ for all $x \in R$. Since (r) is precisely the set of the rx for $x \in R$, this proves that $(r) \subseteq I$.

   Conversely, if $(r) \subseteq I$, then as $r = r1 \in (r)$, we have that $r \in I$ as well.

2. (a) Let us write $I = (r_1, \cdots, r_m)$ and $I' = \{x_1 r_1 + \cdots + x_m r_m \mid x_1, \cdots, x_m \in R\}$. We are going to prove that I and I' contain each other.

   By definition, I, which is the ideal generated by the r_i, contains all the r_i. Therefore, since it is an ideal, it contains $x_i r_i$ for all $i \leq m$ and for all $x_i \in R$, so again because it is an ideal, it contains all the elements of the form $x_1 r_1 + \cdots + x_m r_m$. This shows that $I' \subseteq I$.

   In order to show the converse inclusion, we are going to prove that I' is an ideal. Since $I' \ni r_i$ for all i (as $r_i = x_1 r_1 + \cdots + x_m r_m$ for $x_j = 0$ when $j \neq i$ and $x_i = 1$), and since I is by definition the *smallest* ideal which contains all the r_i, this will prove that $I \subseteq I'$.

   First of all, $I' \ni 0$ (take $x_i = 0$ for all i).

   Second, I' is stable by sum: if $x, x' \in I$, then by definition of I' we have $x = x_1 r_1 + \cdots + x_m r_m$, $x' = x'_1 r_1 + \cdots + x'_m r_m$ for some $x_i, x'_i \in R$, and so $x + x' = (x_1 + x'_1) r_1 + \cdots + (x_m + x'_m) r_m \in I'$ as well.

   Finally, I' is stable by multiplication by R: if $x \in I$ and $y \in R$, then writing $x = x_1 r_1 + \cdots + x_m r_m$ we see that $yx = (yx_1) r_1 + \cdots + (yx_m) r_m$ by distributivity and associativity of multiplication, so $yx \in I'$.

   In conclusion, I' is an ideal, so we are done.

   (b) Simply notice that for each i we have $(r_i) = \{x_i r_i, x_i \in R\}$, whence
   $$(r_1) + \cdots + (r_m) = \{s_1 + \cdots + s_m \mid s_1 \in (r_1), \cdots, s_m \in (r_m)\}$$
   $$= \{x_1 r_1 + \cdots + x_m r_m \mid x_1, \cdots, x_m \in R\} = (r_1, \cdots, r_m)$$
   where the last equality was proved in the previous question.

   (c) We prove the inclusions separately. We have
   $$(r)(s) = \{rx, x \in R\}\{sy, y \in R\} = \left\{ \sum_i^{\text{finite}} r x_i s y_i \mid x_i, y_i \in R \right\}$$

$$= \left\{ rs \sum_i^{\text{finite}} x_i y_i \mid x_i, y_i \in R \right\} \subseteq \{rsz \mid z \in R\} = (rs),$$

and the reverse inclusion holds since every $z \in R$ is of the form $\sum_i^{\text{finite}} x_i y_i$ with $x_i, y_i \in R$: simply take a 1-term sum with $x_1 = z$ and $y_1 = 1$. Alternatively, we could also argue that since $r = r1 \in (r)$ and $s = s1 \in (s)$, we have $rs \in (r)(s)$, whence $(rs) \subseteq (r)(s)$ by the first question of the exercise (since $(r)(s)$ is an ideal, as shown in class).

(d) We prove again both inclusions separately.

Since $(r_1s_1, \cdots, r_1s_n, r_2s_1, \cdots, r_2s_n, \cdots, r_ms_1, \cdots, r_ms_n)$ is by definition the smallest ideal containing the r_is_j and since the product of two ideals is an ideal, in order to prove that

$$(r_1s_1, \cdots, r_1s_n, r_2s_1, \cdots, r_2s_n, \cdots, r_ms_1, \cdots, r_ms_n) \subseteq (r_1, \cdots, r_m)(s_1, \cdots, s_n),$$

it is enough to prove that $r_is_j \in (r_1, \cdots, r_m)(s_1, \cdots, s_n)$ for all i and j; but this is clear since $r_i \in (r_1, \cdots, r_m)$ and $s_j \in (s_1, \cdots, s_n)$.

Conversely, let $z \in (r_1, \cdots, r_m)(s_1, \cdots, s_n)$. By definition of the product, we have $z = \sum_k^{\text{finite}} r_k s_k$ with $r_k \in (r_1, \cdots, r_m)$ and $s_k \in (s_1, \cdots, s_n)$ for all k. By Question 2a, we have $r_k = x_{k,1}r_1 + \cdots + x_{k,m}r_m = \sum_{i=1}^m x_{k,i}r_i$ and $s = y_{k,1}s_1 + \cdots + y_{k,n}s_n = \sum_{j=1}^n y_{k,j}s_j$ for some $x_{k,i}, y_{k,j} \in R$. Expanding, we find that $r_ks_k = (\sum_{i=1}^m x_{k,i}r_i)\left(\sum_{j=1}^n y_{k,j}s_j\right) = \sum_{i=1}^m \sum_{j=1}^n x_{k,i}r_iy_{k,j}s_j = \sum_{i=1}^m \sum_{j=1}^n (x_{k,i}y_{k,j})r_is_j$, whence

$$z = \sum_k^{\text{finite}} r_k s_k = \sum_k^{\text{finite}} \sum_{i=1}^m \sum_{j=1}^n (x_{k,i}y_{k,j})r_is_j = \sum_{i=1}^m \sum_{j=1}^n \left(\sum_k^{\text{finite}} x_{k,i}y_{k,j} \right) r_is_j$$

which lies in $(r_1s_1, \cdots, r_1s_n, r_2s_1, \cdots, r_2s_n, \cdots, r_ms_1, \cdots, r_ms_n)$ by Question 2a.

3. Let $J = (2, x)$; we are going to prove that I and J contain each other.

By question 2a, we have that $J = \{2P(x) + xQ(x) \mid P(x), Q(x) \in \mathbb{Z}[x]\}$. Since the expression $2P(x) + xQ(x)$ clearly evaluates to an even number at $x = 0$ for all $P(x), Q(x) \in \mathbb{Z}[x]$, we conclude that $J \subseteq I$.

Conversely, let $F(x) \in I$. We can write $F(x) = f_dx^d + \cdots + f_1x + f_0$ with the $f_i \in \mathbb{Z}$. Since $f_0 = F(0)$ is even, we can write $f_0 = 2n$ for some $n \in \mathbb{Z}$; but then $F(x) = xQ(x) + 2P(x)$ where $Q(x) = f_dx^{d-1} + \cdots + f_1 \in \mathbb{Z}[x]$ and $P(x) \in \mathbb{Z}[x]$ is the constant polynomial n, whence $F(x) \in J$; this proves that $I \subseteq J$.

4. Let $g = \gcd(m, n)$, so that we can write $m = gm'$, $n = gn'$ with $m,' n' \in \mathbb{Z}$ as this gcd is a common divisor of m and n. We have $(m) + (n) = (m, n)$ by Question 2b, and $(m, n) = \{mx + ny \mid x, y \in \mathbb{Z}$ by Question 2a. Therefore, $g \in (m) + (n)$ by the admitted fact about the gcd, so $(g) \subseteq (m) + (n)$ by Question 1. Conversely, if $z \in (m) + (n)$, then by the above $z = mx + ny$ for some $x, y \in \mathbb{Z}$; but then $z = gm'x + gn'y = g(m'x + n'y) \in \mathbb{Z}$ as $M'x + n'y \in \mathbb{Z}$ (because $\mathbb{Z}$ is a ring), which shows that $(m) + (n) \subseteq (g)$. In conclusion, we have $(m) + (n) = (g)$.

Let $l = \mathrm{lcm}(m, n)$. By definition, $(m) \cap (n)$ is the set of common multiples of m and n, whence $(m) \cap (n) \subseteq (l)$ by the admitted property of the lcm. Conversely, since l is a multiple of m and also of n, any multiple of l is also a multiple of m and of n, whence $(l) \subseteq (m) \cap (n)$. In conclusion, we have $(m) \cap (n) = (l)$.

Finally, we simply have $(m)(n) = (mn)$ by Question 3c.

5. (a) Recall that $IJ = \left\{ \sum_k^{\text{finite}} i_k j_k \mid i_k \in I, j_k \in J \right\}$. For each k, since $i_k \in I$, we have that $i_k j_k \in I$ since I is an ideal; similarly $i_k j_k \in J$ as J is an ideal and $j_k \in J$, so that $i_k j_k \in I \cap J$. As $I \cap J$ is an ideal, it is closed by sum, whence $\sum_k^{\text{finite}} i_k j_k \in I \cap J$; this proves that $IJ \subseteq I \cap J$.

   We have $I \cap J \subseteq I$ by definition of the intersection.

   Finally, since J is an ideal, $J \ni 0$, so $I + J = \{i + j \mid i \in I, j \in J\} \supseteq \{i + 0 \mid i \in I\} = I$.

   (b) Let us take $R = \mathbb{Z}$, $I = (6)$, $J = (4)$. Then by Question 4, we then have $IJ = (24)$, $I \cap J = (12)$, and $I + J = (2)$. It follows that all the inclusions are strict: 12 is in $I \cap J$ but not in IJ, 6 is in I but not $I \cap J$, and 2 is in $I + J$ but not in I.

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

Exercise 2 *Associate elements*

Let R be a commutative **domain**, and let $x, y \in R$. Recall the notation

$$(x) = \{xz \mid z \in R\} \subseteq R,$$

for the ideal generated by x, and similarly for (y).

1. Prove that $(x) \subseteq (y)$ if and only if there exists $z \in R$ such that $x = yz$ (in other words, if $x \in (y)$).

2. Deduce that $(x) = (y)$ if and only if there exists a unit $u \in R^\times$ such that $x = uy$.

Solution 2

1. We prove both implications separately.

   Suppose first $(x) \subseteq (y)$. Then in particular $x \in (y)$, so thre exists $z \in R$ such that $x = yz$.

   Conversely, suppose there exists $z \in R$ such that $x = yz$. Then every multiple of x is also a multiple of x, since for all $t \in R$, $xt = (yz)t = y(zt)$. In other words, we have $(x) \subseteq (y)$.

2. Again, we prove both implications separately.

   Suppose first $(x) = (y)$. Then $(x) \subseteq (y)$, so by the above there exists $z \in R$ such that $x = yz$; but also $(y) \subseteq (x)$, so there exists $z' \in R$ such that $y = xz'$. Thus $x = yz = xzz'$, so $x(1 - zz') = 0$. *Since R is a domain*, this forces either $x = 0$ or $1 - zz' = 0$. In the first case ($x = 0$), we have $y \in (y) = (x) = (0) = \{0\}$ so $y = 0$ as well, and we indeed have $x = uy$ for $u = 1 \in R^\times$ for instance (and for any other u as well). In the second case, we have $zz' = 1$, so z and z' are units that are inverses of each other; in particular, we have $x = yz$ with $z \in R^\times$ as desired.

   Suppose conversely that there exists $u \in R^\times$ such that $x = uy$, and let $v = u^{-1} \in R$. Then since $x = yu$ we have $(x) \subseteq (y)$ by the previous question, and since $y = 1y = vuy = vx = xv$, we have similarly $(y) \subseteq (x)$, so finally $(x) = (y)$.

Exercise 3 *Products of rings*

Let R_1 an R_2 be two rings, neither of which is the 0 ring. Consider the set of pairs

$$R_1 \times R_2 = \{(x_1, x_2) \mid x_1 \in R_1, x_2 \in R_2\}.$$

1. Let R be a ring, and suppose we have a ring isomorphism

   $$\phi : R_1 \times R_2 \xrightarrow{\sim} R$$

   between a product ring $R_1 \times R_2$ of nonzero rings and R. Prove that there exists an $e \in R$ such that $e^2 = e$ but $e \neq 0$ and $e \neq 1$. Use this to deduce that R cannot be a domain.

   Hint: Take a look at the pair $(1, 0) \in R_1 \times R_2$.

2. Prove that conversely, if there exists $e \in R$ such that $e^2 = e$ but $e \neq 0$ and $e \neq 1$, then R is isomorphic to the product of two nonzero rings.

   Hint: $R_1 = eR$, $R_2 = (1 - e)R$.

3. Prove that the ring

   $$F = \{f : \mathbb{R} \longrightarrow \mathbb{R} \mid f \text{ continuous}\}$$

   of continuous functions from $\mathbb{R}$ to $\mathbb{R}$, equipped as usual with the laws

   $$(f + g)(x) = f(x) + g(x), \quad (fg)(x) = f(x)g(x)$$

for all $f, g \in F$ and $x \in \mathbb{R}$, is NOT isomorphic to a product ring $R_1 \times R_2$.

Hint: Proceed by contradiction. You may use without proof the following consequence of the intermediate value theorem: If $f : \mathbb{R} \longrightarrow \mathbb{R}$ is continuous and satisfies $f(x) \in \{0, 1\}$ for all $x \in \mathbb{R}$, then f is constant (and thus either identically 0 or 1).

4. What happens if we drop the continuity condition, and consider instead the ring of all functions from $\mathbb{R}$ to $\mathbb{R}$?

Solution 3

1. Let $e' = (1, 0) \in R_1 \times R_2$, and $e = \phi(e') \in R$.

   First of all, observe that

   $$e'^2 = (1, 0)^2 = (1^2, 0^2) = (1, 0) = e'.$$

   As a result, we have

   $$e^2 = \phi(e')^2 = \phi(e'^2) = \phi(e') = e,$$

   where we used the fact that ϕ is a morphism at the second step.

   Besides, since neither R_1nor R_2 are the 0 ring, we have $0 \neq 1$ both in R_1 and in R_2, so e' is neither the 0 of $R_1 \times R_2$ (which is $(0, 0)$, as proved in the previous question) nor the 1 of $R_1 \times R_2$ (which is $(1, 1)$, as proved in the previous question).

   Next, ϕ is an isomorphism, it is injective, so $\phi(e') \neq \phi(0)$ and $\phi(e') \neq \phi(1)$; and since ϕ is a morphism, we have $\phi(0) = 0 \in \mathbb{R}$ and $\phi(1) = 1 \in R$. This shows that $e = \phi(e')$ is neither 0 nor 1.

   In particular, R cannot be a domain, for else

   $$0 = e^2 - e = e(e - 1)$$

   would force $e = 0$ or $e = 1$.

2. Let $e \in R$ such that $e^2 = e$, define $R_1 = eR = (e)$ and $R_2 = (1-e)R = (1-e)$. Then R_1 an R_2, equipped with the $+$ and $\times$ of R, are rings (since $re+se = (r+s)e$, $re \times se = rse^2 = rse$, and similarly for R_2 as $(1-e)^2 = 1-2e+e^2 = 1-e$), whose 1 are respectively e and $1-e$ (since $re \times e = re$, etc. In particular, they are NOT subrings since they do not have the same 1 as R). In particular, if $e \neq 0, 1$, then R_1 and R_2 are not the 0 ring since their 1 is distinct from their 0. Finally, we have the mutually inverse ring isomorphisms

   $$\begin{array}{ccc} R & \longleftrightarrow & R_1 \times R_2 \\ x & \longmapsto & \big(ex, (1-e)x\big) \\ ey + (1-e)z & \longleftarrow & \big(ey, (1-e)z\big) \end{array}$$

   (we leave it to you to check that they are morphisms).

3. It is tempting to try to conclude by showing that F is a domain, but this is not the case (F is **NOT** a domain, a seen in class).

   Instead, we are going to show that it contains no e as above. Suppose by contradiction that $e(x) \in F$ satisfies $e^2 = e$ but $e \neq 0, 1$, and let $x \in \mathbb{R}$.

   $$0 = e(x) - e(x) = e^2(x) - e(x) = e(x)^2 - e(x) = e(x)\big(e(x) - 1\big) \in \mathbb{R}$$

   where we used the definition of $\times$ on F at the third step. Since $\mathbb{R}$ is a field, it is a domain, so the above forces $e(x) = 0$ or $e(x) = 1$. Since this holds for any x, we may apply the hint and conclude that e is either the constant function 0, or the constant function 1. But these are precisely the 0 an the 1 of the ring F, so we contradict our assumption that $e \neq 0, 1$.

   In conclusion, F is not isomorphic to a product of rings, even though it is not a domain.

   Remark: The hint relies on the intermediate value theorem, and thus on continuity. If we drop the continuity assumption, then the hint becomes false: consider for instance the function $e(x)$ defined by $e(x) = 1$ if $x < 0$, and $e(x) = 0$ else.

   The ring decomposition attached to this e by the converse of the previous question (cf. remark above) is simply the restrictions map

   $$\begin{array}{ccc} \{\text{Functions } \mathbb{R} \longrightarrow \mathbb{R}\} & \xrightarrow{\sim} & \{\text{Functions } \mathbb{R}_{<0} \longrightarrow \mathbb{R}\} \times \{\text{Functions } \mathbb{R}_{\geqslant 0} \longrightarrow \mathbb{R}\} \\ f & \longmapsto & \Big(\quad f_{|\mathbb{R}_{<0}} \quad , \quad f_{|\mathbb{R}_{\geqslant 0}} \quad \Big). \end{array}$$

   In fact, a little reflexion shows that we can keep decomposing. In total, we get the ring isomorphism

   $$\{\text{Functions } \mathbb{R} \longrightarrow \mathbb{R}\} \simeq \mathbb{R}^{\mathbb{R}}$$

   assigning to a function f the "list" of its values $f(x)$ for each $x \in \mathbb{R}$. We cannot decompose further since $\mathbb{R}$, being a field, is a domain.

4. If we do not require our functions to be continuous, then we can find plenty of functions $e(x)$ such that $e(x)^2 = e(x)$ for all $x \in \mathbb{R}$. For example, we can take the function such that $e(x) = 1 is x > 0$, and $e(x) = 0$ if $x leq 0$; the corresponding ring decomposition is then

   $\{\text{Functions } \mathbb{R} \to \mathbb{R}\} \simeq \{\text{Functions } (0, +\infty) \to \mathbb{R}\} \times \{\text{Functions } (-\infty, 0] \to \mathbb{R}\}$.

   We see that we can continue to decompose; in the end, we find that

   $$\{\text{Functions } \mathbb{R} \to \mathbb{R}\} \simeq \mathbb{R}^{\mathbb{R}} = \prod_{x \in \mathbb{R}} \mathbb{R}$$

   is a product indexed by $\mathbb{R}$ of copies of $\mathbb{R}$ — for each $x \in \mathbb{R}$, we pick a value $f(x) \in \mathbb{R}$, where the $f(x)$ for different $x \in \mathbb{R}$ need noty satisfy any relation with each other since we are not imposing continuity.

   Moral of the story: the ring of all functions is quite "nice" from an algebraic point of view, whereas its subring of continuous functions is more difficult to understand, all because continuity is a rather "obscure" condition for the algebraist.