Fields, rings, and modules
Exercise sheet 1

`https://www.maths.tcd.ie/~mascotn/teaching/2020/MAU22102/index.html`

Version: February 12, 2020

Answers are due for Thursday February 13rd, 4PM.

Exercise 1 *Associate elements (40 pts)*

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. (20 pts) 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. (20 pts) Deduce that $(x) = (y)$ if and only if there exists a unit $u \in R^\times$ such that $x = uy$.

Solution 1

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 $(x) = (y)$.

Remark: All in all, this exercise was as much about rings as about logic (to prove an equivalence, prove both implication; to prove two subsets are equal, prove that they contain each other, etc.)

Exercise 2 *Products of rings (60 pts)*

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. (20 pts) Show that the operations

   $$(x_1, x_2) + (y_1, y_2) = (x_1 + y_1, x_2 + y_2), \quad (x_1, x_2) \times (y_1, y_2) = (x_1 \times y_1, x_2 \times y_2)$$

   for all $x_1, y_1 \in R_1$ an $x_2, y_2 \in R_2$ define a ring structure on $R_1 \times R_2$. What are the 0 and the 1 of $R_1 \times R_2$?

   We call $R_1 \times R_2$ equipped with the above operations the product ring *of R_1 and R_2.*

2. (20 pts) Let R be another ring, and suppose we have a ring isomorphism

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

   between a product ring $R_1 \times R_2$ and R. Prove that there exists an $e \in R$ such that $e^2 = e$ but $e \neq 0$ and $e \neq 1$. Deduce that R cannot be a domain.

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

3. (20 pts) Using the previous question, 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*).*

Solution 2

1. First of all, we show that the addition thus defined on $R_1 \times R_2$ gives it the structure of an Abelian group. This follows from the fact that we have just put the product operation on $R_1 \times R_2$, and that the product of two Abelian groups is an Abeian group. Alternatively, we can (re)prove it as follows:

   - Associativity: for all $x_1, y_1, z_1 \in R_1$ and $x_2, y_2, z_2 \in R_2$, we have
   $$\begin{aligned} &\big((x_1, x_2) + (y_1, y_2)\big) + (z_1, z_2) \\ =&(x_1 + y_1, x_2 + y_2) + (z_1 + z_2) \\ =&\big((x_1 + y_1) + z_1, (x_2 + y_2) + z_2\big) \\ =&\big(x_1 + (y_1 + z_1), x_2 + (y_2 + z_2)\big) \\ =&(x_1, x_2) + (y_1 + z_1, y_2 + z_2) \\ =&(x_1, x_2) + \big((y_1, y_2) + (z_1, z_2)\big) \end{aligned}$$
   where we have successively used the definition of $+$ on $R_1 \times R_2$ (twice), the associativity of the $+$ of R_1 and of that of R_2, and the definition of $+$ on $R_1 \times R_2$ (twice more).
   - Identity: $(0, 0) \in R_1 \times R_2$ is the identity for $+$ since for all $x_1 \in R_1$ and $x_2 \in R_2$,
   $$(0, 0)+(x_1, x_2) = (0+x_1, 0+x_2) = (x_1, x_2) = (x_1+0, x_2+0) = (x_1, x_2)+(0, 0).$$
   - Inverses: For all $x_1 \in R_1$ and $x_2 \in R_2$, the inverse of $(x_1, x_2) \in R$ is
   $$-(x_1, x_2) = (-x_1, -x_2) \in R$$
   since
   $$(x_1, x_2) + (-x_1, -x_2) = (x_1 - x_1, x_2 - x_2) = (0, 0)$$
   is the identity as shown just above.
   - Commutativity: for all $x_1, y_1 \in R_1$ and $x_2, y_2 \in R_2$, we have
   $$(x_1, x_2)+(y_1, y_2) = (x_1+y_1, x_2+y_2) = (y_1+x_1, y_2+x_2) = (y_1, y_2)+(x_1, x_2)$$
   using the commutativity of $+$ on R_1 and R_2 at the second step.

   To show that $R_1 \times R_2$ is actually a ring, we still need to prove:

   - Associativity of $\times$: this is proved as for the associativity of $+$ above;
   - identity of $\times$: one checks that it is $(1, 1)$ by the same logic as when e proved that $(0, 0)$ was the identity of $+$ above;
   - distributivity on the left: for all $x_1, y_1, z_1 \in R_1$ and $x_2, y_2, z_2 \in R_2$, we have
   $$\begin{aligned} &(x_1, x_2)\big((y_1, y_2) + (z_1, z_2)\big) \\ =&(x_1, x_2)(y_1 + z_1, y_2 + z_2) \\ =&\big(x_1(y_1 + z_1), x_2(y_2 + z_2)\big) \\ =&(x_1y_1 + x_1z_1, x_2y_2 + x_2z_2) \\ =&(x_1y_1, x_2y_2) + (x_1z_1, x_2z_2) \\ =&(x_1, x_2)(y_1, y_2) + (x_1, x_2)(z_1, z_2), \end{aligned}$$

using successively the definition of $+$, that of $\times$, distributivity in R_1 and in R_2, the definition of $+$ again, and that of $\times$ again.

- And finally, distributivity on the right (i.e. $\big((x_1,x_2)+(y_1,y_2)\big)(z_1,z_2) = (x_1,x_2)(z_1,z_2)+(y_1,y_2)(z_1,z_2)$) is proved similarly.

2. 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 $e = 1$.

   Remark: The converse holds! Indeed, given $e \in R$ satisfying $e^2 = e$, 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, whose identities for $\times$ are respectively e and $1-e$ (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

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

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

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

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.