Algebra I - Homework 5

Pablo Sánchez Ocal

October 21st, 2016

Exercise 1

Consider the direct non empty product $\prod_{i\in I} R_i$ of rings. We want to see that it is a ring with coordinate wise addition and multiplication. We will use the notation $\{a_i\}_{i\in I}$ for an element in $\prod_{i\in I} R_i$. First, we clearly have that it is an abelian group:

1. Associativity: for $\{a_i\}_{i\in I}, \{b_i\}_{i\in I}, \{c_i\}_{i\in I} \in \prod_{i\in I} R_i$ we have:

$$\{a_i\}_{i\in I} + (\{b_i\}_{i\in I} + \{c_i\}_{i\in I}) = \{a_i\}_{i\in I} + \{b_i + c_i\}_{i\in I} = \{a_i + b_i + c_i\}_{i\in I}$$
$$(\{a_i\}_{i\in I} + \{b_i\}_{i\in I}) + \{c_i\}_{i\in I} = \{a_i + b_i\}_{i\in I} + \{c_i\}_{i\in I} = \{a_i + b_i + c_i\}_{i\in I}$$

2. Identity element: consider $\{0_i\}_{i\in I} \in \prod_{i\in I} R_i$, for every $\{a_i\}_{i\in I} \in \prod_{i\in I} R_i$ we have:

$$\{a_i\}_{i\in I} + \{0_i\}_{i\in I} = \{a_i + 0_i\}_{i\in I} = \{a_i\}_{i\in I}$$
$$\{0_i\}_{i\in I} + \{a_i\}_{i\in I} = \{0_i + a_i\}_{i\in I} = \{a_i\}_{i\in I}$$

3. Inverse: for every $\{a_i\}_{i\in I} \in \prod_{i\in I} R_i$ consider $\{-a_i\}_{i\in I}, \in \prod_{i\in I} R_i$, we have:

$$\{a_i\}_{i\in I} + \{-a_i\}_{i\in I} = \{a_i - a_i\}_{i\in I} = \{0_i\}_{i\in I} = \{-a_i + a_i\}_{i\in I} = \{-a_i\}_{i\in I} + \{a_i\}_{i\in I}$$

4. Commutativity: for $\{a_i\}_{i\in I}, \{b_i\}_{i\in I} \in \prod_{i\in I} R_i$ we have:

$$\{a_i\}_{i\in I} + \{b_i\}_{i\in I} = \{a_i + b_i\}_{i\in I} = \{b_i + a_i\}_{i\in I} = \{b_i\}_{i\in I} + \{a_i\}_{i\in I}$$

where we have used that every R_i for $i \in I$ is an abelian group, hence satisfy the four properties above elementwise. Moreover, the multiplication is associative: for $\{a_i\}_{i\in I}, \{b_i\}_{i\in I}, \{c_i\}_{i\in I} \in \prod_{i\in I} R_i$ we have:

$$\{a_i\}_{i\in I} \cdot (\{b_i\}_{i\in I} \cdot \{c_i\}_{i\in I}) = \{a_i\}_{i\in I} \cdot \{b_i \cdot c_i\}_{i\in I} = \{a_i \cdot b_i \cdot c_i\}_{i\in I}$$
$$(\{a_i\}_{i\in I} \cdot \{b_i\}_{i\in I}) \cdot \{c_i\}_{i\in I} = \{a_i \cdot b_i\}_{i\in I} \cdot \{c_i\}_{i\in I} = \{a_i \cdot b_i \cdot c_i\}_{i\in I}$$

where again we use that multiplication in every R_i for $i \in I$ is associative. Finally, we have the distributive law: for $\{a_i\}_{i\in I}, \{b_i\}_{i\in I}, \{c_i\}_{i\in I} \in \prod_{i\in I} R_i$ we have:

$$\{a_i\}_{i\in I} \cdot (\{b_i\}_{i\in I} + \{c_i\}_{i\in I}) = \{a_i\}_{i\in I} \cdot \{b_i + c_i\}_{i\in I} = \{a_i \cdot b_i + a_i \cdot c_i\}_{i\in I}$$
$$\{a_i\}_{i\in I} \cdot \{b_i\}_{i\in I} + \{a_i\}_{i\in I} \cdot \{c_i\}_{i\in I} = \{a_i \cdot b_i\}_{i\in I} + \{a_i \cdot c_i\}_{i\in I} = \{a_i \cdot b_i + a_i \cdot c_i\}_{i\in I}$$
$$(\{a_i\}_{i\in I} + \{b_i\}_{i\in I}) \cdot \{c_i\}_{i\in I} = \{a_i + b_i\}_{i\in I} \cdot \{c_i\}_{i\in I} = \{a_i \cdot c_i + b_i \cdot c_i\}_{i\in I}$$
$$\{a_i\}_{i\in I} \cdot \{c_i\}_{i\in I} + \{b_i\}_{i\in I} \cdot \{c_i\}_{i\in I} = \{a_i \cdot c_i\}_{i\in I} + \{b_i \cdot c_i\}_{i\in I} = \{a_i \cdot c_i + b_i \cdot c_i\}_{i\in I}$$

since we have the distributive law in every R_i for $i \in I$. Hence, $\prod_{i\in I} R_i$ is a ring.

Letting $\sum_{i\in I} R_i \subset \prod_{i\in I} R_i$ be with only finitely many components non zero, note that the reasoning above still holds, and we just have to check that the operations are closed. This is clear since when $(a_{i_1}, \dots, a_{i_n}), (b_{j_1}, \dots, a_{j_m}) \in \sum_{i\in I} R_i$ with $n, m \in \mathbb{N}$ then both $(a_{i_1}, \dots, a_{i_n}) + (b_{j_1}, \dots, a_{j_m})$ and $(a_{i_1}, \dots, a_{i_n}) \cdot (b_{j_1}, \dots, a_{j_m})$ have at most $i_1, \dots, i_n, j_1, \dots, j_m$ components non zero, $n + m \in \mathbb{N}$. Hence, $\sum_{i\in I} R_i$ is a ring.

Let all R_i for $i \in I$ have identities. Clearly $\{1_{R_i}\}_{i\in I}$ is the identity element in $\prod_{i\in I} R_i$ since for every $\{a_i\}_{i\in I}, \in \prod_{i\in I} R_i$ we have:

$$\{a_i\}_{i\in I} \cdot \{1_{R_i}\}_{i\in I} = \{a_i \cdot 1_{R_i}\}_{i\in I} = \{a_i\}_{i\in I} = \{1_{R_i} \cdot a_i\}_{i\in I} = \{1_{R_i}\}_{i\in I} \cdot \{a_i\}_{i\in I}$$

However, we have that $\{1_{R_i}\}_{i\in I} \in \sum_{i\in I} R_i$ if and only if I is finite. In this case, $\sum_{i\in I} R_i$ has an identity. However, if I is not finite, then no element of $\sum_{i\in I} R_i$ can behave like an identity: suppose $(a_{i_1}, \ldots, a_{i_n})$ is the identity, since I is not finite, there exists $j \in I$ with $j \neq i_k$ for $k \in \{1, \ldots, n\}$, thus considering the element (1_{R_j}) we have that $(1_{R_j}) \cdot (a_{i_1}, \ldots, a_{i_n}) = \{0_i\}_{R_i} \neq (1_{R_j})$, a contradiction. Hence, $\sum_{i\in I} R_i$ has an identity if and only if I is finite, and in such case it coincides with the one in $\prod_{i\in I} R_i$ (note that this must true because $\prod_{i\in I} R_i$ already had an identity and when I finite we have $\prod_{i\in I} R_i = \sum_{i\in I} R_i$).

Exercise 2

Let G be an abelian group, $\text{End}(G) = \{f : G \longrightarrow G : f \text{ homomorphism}\}$ with pointwise addition and composition as operations. We prove that this is a ring. First, we clearly have that it is an abelian group:

1. Associativity: for $f, g, h \in \text{End}(G)$ and $a \in G$ we have:

$$\begin{aligned}(f + (g + h))(a) &= f(a) + (g + h)(a) = f(a) + g(a) + h(a)\\ ((f + g) + h)(a) &= (f + g)(a) + h(a) = f(a) + g(a) + h(a)\end{aligned}$$

2. Identity element: consider $0 \in \text{End}(G)$ as the homomorphism constant to $0 \in G$, for every $f \in \text{End}(G)$ and $a \in G$ we have:

$$(f + 0)(a) = f(a) + 0(a) = f(a) = 0(a) + f(a) = (0 + f)(a)$$

3. Inverse: for every $f \in \text{End}(G)$ consider $\tilde{f} \in \text{End}(G)$ defined as $\tilde{f}(b) = -f(b)$ for every $b \in G$. Now for every $a \in G$ we have:

$$\begin{aligned}(f + \tilde{f})(a) &= f(a) + \tilde{f}(a) = f(a) - f(a) = 0 = 0(a)\\ (\tilde{f} + f)(a) &= \tilde{f}(a) + f(a) = -f(a) + f(a) = 0 = 0(a)\end{aligned}$$

   thus $-f = \tilde{f} \in \text{End}(G)$.

4. Commutativity: for $f, g \in \text{End}(G)$ and every $a \in G$ we have:

$$(f + g)(a) = f(a) + g(a) = g(a) + f(a) = (g + f)(a)$$

where for manipulating the images of the homomorphisms we have used that G is an abelian group. Moreover, composition is associative: for $f, g, h \in \text{End}(G)$ we have:

$$\begin{aligned}(f \circ (g \circ h))(a) &= f((g \circ h)(a)) = f(g(h(a)))\\ ((f \circ g) \circ h)(a) &= (f \circ g)(h(a)) = f(g(h(a)))\end{aligned}$$

Finally, we have the distributive law: for $f, g, h \in \text{End}(G)$ we have:

$$\begin{aligned}(f \circ (g + h))(a) &= f((g + h)(a)) = f(g(a) + h(a)) = f(g(a)) + f(h(a))\\ ((f \circ g) + (f \circ h))(a) &= (f \circ g)(a) + (f \circ h)(a) = f(g(a)) + f(h(a))\\ ((f + g) \circ h))(a) &= (f + g)(h(a)) = f(h(a)) + g(h(a))\\ ((f \circ h) + (g \circ h))(a) &= (f \circ h)(a) + (g \circ h)(a) = f(h(a)) + g(h(a))\end{aligned}$$

where we used the fact that f is a homomorphism in the first equality. Hence, $\text{End}(G)$ is a ring.

However, $\text{End}(\mathbb{Z} \oplus \mathbb{Z})$ is not commutative. Consider the homomorphisms given by:

$$\begin{array}{rccc} f : & \mathbb{Z} \oplus \mathbb{Z} & \longrightarrow & \mathbb{Z} \oplus \mathbb{Z} \\ & (n, m) & \longmapsto & (n + m, 0) \end{array}, \quad \begin{array}{rccc} g : & \mathbb{Z} \oplus \mathbb{Z} & \longrightarrow & \mathbb{Z} \oplus \mathbb{Z} \\ & (n, m) & \longmapsto & (n, 2m) \end{array}$$

we clearly have that $f, g \in \text{End}(\mathbb{Z} \oplus \mathbb{Z})$ since for any $(n, m), (a, b) \in \mathbb{Z} \oplus \mathbb{Z}$ we have:

$$\begin{aligned} f((n,m)+(a,b)) = f(n+a, m+b) = (n+a+m+b, 0) &= (n+m+a+b, 0) \\ f(n,m)+f(a,b) = (n+m,0)+(a+b,0) &= (n+m+a+b,0) \\ g((n,m)+(a,b)) = g(n+a,m+b) = (n+a, 2(m+b)) &= (n+a, 2m+2b) \\ g(n,m)+g(a,b) = (n,2m)+(a,2b) &= (n+a,2m+2b) \end{aligned}$$

but now we have that:

$$\begin{aligned} (f \circ g)(n,m) = f(g(n,m)) = f(n,2m) = (n+2m,0) \\ (g \circ f)(n,m) = g(f(n,m)) = g(n+m,0) = (n+m,0) \end{aligned}$$

and since $2m \neq m$ in general (except when $m = 0$), we have $f \circ g \neq g \circ f$, as desired.

Exercise 3

1. Let R be a commutative ring, $a, b \in R$ nilpotent elements, say $a^n = 0$ and $b^m = 0$ with $n, m \in \mathbb{N}$, suppose $1 < n \leq m$. Prove that $a + b$ is nilpotent. Consider:

$$(a+b)^{nm} = \sum_{k=0}^{nm} \binom{nm}{k} a^{nm-k} b^k$$

by [1, Theorem 1.6 (p. 118)] (remark that although this result requires R to have an identity element to say that $r^0 = 1$ for $r \in R$, the formal statement by getting a^{nm} and b^{nm} out of the sum thus avoiding the cases a^0 and b^0 is still true. That is what we are really using). We have two options:

   (a) $0 \leq k \leq m$: then $k = m - j$ for $0 \leq j \leq m$, thus $a^{nm-k} = a^{(n-1)m+j} = (a^m)^{n-1} a^j$, but $a^m = 0$ and $n - 1 > 0$, $j \geq 0$ meaning that $a^{nm-k} = 0$.

   (b) $m \leq k \leq nm$: then $k = m + j$ for $0 \leq j \leq (n-1)m$, thus $b^k = b^{m+j} = b^m b^j$, but $b^m = 0$ and $j \geq 0$ meaning that $a^k = 0$.

2. If R is not commutative, the above is not true in general, that is, the sum of nilpotent elements may not be nilpotent. Consider $M_2(\mathbb{R})$ the ring of 2×2 matrices with real entries. Now:

$$A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$

are both nilpotent since $A^2 = 0$, $B^2 = 0$. However:

$$A + B = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad (A+B)^2 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

so that $(A + B)^n$ for $n \in \mathbb{N}$ is two periodic, alternating between $A + B$ when n is odd and the identity matrix when n is even. Since none of those is the matrix with all zero entries, $A + B$ is not nilpotent, as desired.

Exercise 4

We consider R the ring of linear maps $L : \mathbb{R}[x] \longrightarrow \mathbb{R}[x]$ with addition and composition as the operations. Obviously the identity element is $\mathrm{id}_{\mathbb{R}[x]}(f) = f$ for every $f \in \mathbb{R}[x]$.

1. We want to see that the linear transformation $D(f) = f'$ is right invertible in R, but not invertible. Consider the linear operator G that acts on the basis $\{1, x, \dots, x^n, \dots\}$ of $\mathbb{R}[x]$ as $G(x^m) = x^{m+1}/m + 1$ for $m \in \mathbb{N}$ (in particular, $G(1) = x$). If we let $f(x) = a_0 + a_1 x + \cdots + a_n x^n$ be a generic element of $\mathbb{R}[x]$, we have:

   $$(D \circ G)(f) = D(a_0 x + a_1 x^2/2 + \cdots + a_n x^{n+1}/n+1) = a_0 + a_1 z + a_n x^n = f = \mathrm{id}_{\mathbb{R}[x]}(f).$$

   Hence, D is right invertible, having G as a right inverse. Moreover, notice that it cannot be left invertible, since for f as above we have $D(f) = a_1 + 2a_2 x + \cdots + n a_n x^{n-1}$ and there is no way of recovering the constant a_0: fix f, suppose there exists $H \in R$ with $H \circ D = \mathrm{id}_{\mathbb{R}[x]}$, then:

   $$f = (H \circ D)(f) = H(a_1 + 2a_2 x + \cdots + n a_n x^{n-1}) = a_0 + a_1 x + \cdots + a_n x^n$$

   this means that for $g(x) = b_0 + a_1 x + \cdots + a_n x^n$ with $b_0 \neq a_0$ (which exists, we have the coefficients in $\mathbb{R}$) we have:

   $$(H \circ D)(g) = H(a_1 + 2a_2 x + \cdots + n a_n x^{n-1}) = a_0 + a_1 x + \cdots + a_n x^n \neq g$$

   a contradiction with $H \circ D = \mathrm{id}_{\mathbb{R}[x]}$. Hence, D is not invertible.

2. We will now see that D cannot be a (two sided) zero divisor. Remark first that it cannot be a right zero divisor: suppose H is such that $H \circ D = 0$, applying D to the basis $\{1, x, \dots, x^n/n, \dots\}$ we must have for every $m \in \mathbb{N}$ that:

   $$H(x^m) = H(D(x^{m+1}/m + 1)) = (H \circ D)(x^{m+1}/m + 1) = 0$$

   hence $H = 0$ since it is zero in every element of the basis. However, D is a left zero divisor: define H with $H(a) = a$ when $a \in \mathbb{R}$ and $H(x^n) = 0$ for every $n > 0$ and extend by linearity (in particular, we have by definition that H is linear), now:

   $$(D \circ H)(f) = D(H(f)) = D(a_0) = 0$$

   for a generic polynomial $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, as desired.

Exercise 5

Let R be a commutative ring with identity of prime characteristic $p \in \mathbb{N}$.

1. We show that for any $a, b \in R$ we have $(a+b)^p = a^p + b^p$. Again by [1, Theorem 1.6 (p. 118)] we have that:

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^{p-k} b^k,$$

notice that for $k = 0$ we obtain the term a^p, for $k = p$ we obtain the term b^p, and for $0 < k < p$ we have that:

$$\binom{p}{k} = \frac{p!}{k!(p-k)!} = \frac{p(p-1)\cdots(p-k+1)}{k(k-1)\cdots 2} = p\frac{(p-1)\cdots(p-k+1)}{k(k-1)\cdots 2}$$

and since $k < p$, we have that p cannot divide $k(k-1)\cdots 2$, that is, $\binom{p}{k}$ is always divisible by p in those cases. Since R has characteristic p, this means that $\binom{p}{k} = 0$ when $0 < k < p$. Thus $(a+b)^p = a^p + b^p$ as desired.

2. We show that the map $\varphi : R \longrightarrow R$ defined by $\varphi(a) = a^p$ for $a \in R$ is an endomorphism of rings. Let $a, b \in R$, we have:

$$\varphi(ab) = (ab)^p = a^p b^p = \varphi(a)\varphi(b),$$
$$\varphi(a+b) = (a+b)^p = a^p + b^p = \varphi(a) + \varphi(b),$$

where we have used the commutativity of R as well as the equality proven above. This yields the desired result.

References

[1] T. W. Hungerford, *Algebra*.