Solutions for Exercise sheet 1, Algebra I (Commutative Algebra) – Week 1

The first two exercise sheets will only use material you should be familiar with already. Some of it is covered and recalled by the first three lectures. These two sheets are not compulsory but the points can be counted towards your final score of the necessary 50% to get admitted to the exams.

Exercise 1. (Examples of rings)

1. Using material from the lecture, one could consider $A = M(n \times n, \mathbb{F}_q)$ for $n \geq 2$, or $A = \mathbb{F}_q[G]$ for G a finte non-commutative group such as S_3... That those are rings, is stated in the lecture; their finiteness comes from that fact that they are finite dimensional $\mathbb{F}_q$-vector spaces (and as such have cardinality respectively q^{n^2} and $q^{|G|}$) and it is sufficient to exhibit an example of a pair of elements that do not commute.
   For $M(2 \times 2, \mathbb{F}_q)$, we can take:
   $$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} \neq \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$
   For $\mathbb{F}_q[S_3]$, we can take:
   $$(1\ 3) \cdot (1\ 2) = (1\ 3) \circ (1\ 2) \neq (1\ 2) \circ (1\ 3) = (1\ 2) \cdot (1\ 3)$$
   as we see, for example, by looking at the image of 1.

2. For $f, g \in A^X$, define $f +_{A^X} g : X \to A$ by $x \mapsto f(x) + g(x)$ and $f \cdot_{A^X} g : X \to A$ by $x \mapsto f(x)g(x)$. Define 0_{A^X} by $x \mapsto 0 \in A$ and $1_{A^X} : x \mapsto 1 \in A$. For a $f \in A^X$, define $-f \in A^X$ by $x \mapsto -f(x)$. The associativity of $+_{A^X}$ and $\cdot_{A^X}$ come from the associativity of the corresponding operation on A. To prove the associativity of $+_{A^X}$, take $f, g, h \in A^X$. Then
   $$[f +_{A^X} (g +_{A^X} h)](a) = f(a) + (g(a) + h(a)) \underset{\text{in } A}{=} (f(a) + g(a)) + h(a) = [(f +_{A^X} g) +_{A^X} h](a)$$
   for any $a \in A$; in other words $f +_{A^X} (g +_{A^X} h) = (f +_{A^X} g) +_{A^X} h$.
   To prove the associativity of $\cdot_{A^X}$, take $f, g, h \in A^X$. Then
   $$[f \cdot_{A^X} (g \cdot_{A^X} h)](a) = f(a)(g(a)h(a)) \underset{\text{in } A}{=} (f(a)g(a))h(a) = [(f \cdot_{A^X} g) \cdot_{A^X} h](a)$$
   for any $a \in A$; in other words $f \cdot_{A^X} (g \cdot_{A^X} h) = (f \cdot_{A^X} g) \cdot_{A^X} h$.
   That $\cdot_{A^X}$ is distributive over $+_{A^X}$ also follows from the fact that $\cdot$ is distributive over $+$ in A. To prove it, take $f, g, h \in A^X$. Then
   $$\begin{aligned}[f \cdot_{A^X} (g +_{A^X} h)](a) = f(a)(g(a) + h(a)) \underset{\text{in } A}{=} f(a)g(a) + f(a)h(a) &= f \cdot_{A^X} g(a) + f \cdot_{A^X} h(a) \\ &= [f \cdot_{A^X} g + f \cdot_{A^X} h](a)\end{aligned}$$
   for any $a \in A$. Thus $\cdot_{A^X}$ is distributive over $+_{A^X}$.
   The commutativity of $+_{A^X}$ is proven in similar manner.
   For $f \in A^X$, we have $(f +_{A^X} 0_{A^X})(a) = f(a) + 0 = f(a)$ and $(f \cdot_{A^X} 1_{A^X})(a) = f(a) \cdot 1 = f(a)$ for any a; in other words $f +_{A^X} 0_{A^X} = f$ and $f \cdot_{A^X} 1_{A^X} = f$ respectively.
   Finally, for $f \in A^X$, $(-f +_{A^X} f)(a) = -f(a) + f(a) = 0$ for any $a \in A$ i.e. $-f +_{A^X} f = 0_{A^X}$.

3. Likewise, we can define for a commutative group $(G,+)$, on the set $\mathrm{End}(G)$, an addition $+_{\mathrm{End}(G)}$ by the following rule: for $f,g\in\mathrm{End}(G)$, $f+_{\mathrm{End}(G)}g : x\mapsto f(x)+g(x)$. We can check, by pointwise computations (as in the previous question), that $(\mathrm{End}(G),+_{\mathrm{End}(G)})$ is a commutative group with $0_{\mathrm{End}(G)} : x\mapsto 0$ as its zero element and for $f\in\mathrm{End}(G)$, $-f\in\mathrm{End}(G)$ defined by $x\mapsto -f(x)$. We take for $\cdot_{\mathrm{End}(G)}$, the composition $\circ$, which is always associative and has $\mathrm{Id}_G\in\mathrm{End}(G)$ as unit. We can check that $\cdot_{\mathrm{End}(G)}$ is distributive over $+_{\mathrm{End}(G)}$: for $f,g,h\in\mathrm{End}(G)$, for any $x\in G$,

$$\begin{aligned} h\circ(f+_{\mathrm{End}(G)}g)(x) &= h(f(x)+g(x)) = h(f(x))\ +\ h(g(x)) \text{ because } h \text{ is a group homomorphism}\\ &= h\circ f(x)+h\circ g(x).\end{aligned}$$

Endowed with this ring structure, $\mathrm{End}(G)$ is not always commutative as the following example shows: take $G=\mathbb{Z}\times\mathbb{Z}$ ($0_G=(0,0)$) endowed with the component-wise sum and $f,g\in\mathrm{End}(G)$ defined respectively by $f:(a,b)\mapsto(b,a)$ $(f((a,b)+(c,d))=f(a+c,b+d)=(b+d,a+c)=(b,a)+(d,c)=f(a,b)+f(c,d))$ and $g:(a,b)\mapsto(0,b)$. Then $f\circ g(1,0)=f(g(1,0))=f(0,0)=(0,0)$ but $g\circ f(1,0)=g(0,1)=(0,1)$.

It is commutative for example when $(G,+)=(\mathbb{Z},+)$ (or more generally, when the group $(G,+)$ is cyclic). Indeed, in this case $\mathrm{End}(\mathbb{Z})\simeq\mathbb{Z}$ where the isomorphism of rings is given by $f\mapsto f(1)$. That this is a ring homomorphism follows from

$$\begin{aligned} f\circ(g+h)(1) &= f(g(1)+h(1)) = f(g(1))+f(h(1))\\ &= \underbrace{f(1)+\cdots+f(1)}_{g(1)-\text{times}}+\underbrace{f(1)+\cdots+f(1)}_{g(1)-\text{times}}\\ &= f(1)g(1)+f(1)h(1)\end{aligned}$$

and $0_{\mathrm{End}(G)}(1)=0$, $Id_G(1)=1$. The injectivity follows from the fact that $(\mathbb{Z},+)$ is cyclic: if $f(1)=0$ for $f\in\mathrm{End}(G)$ then, $f(-1)=-f(1)=0$ and for any $n\geq 0$,

$$f(n)=f(\underbrace{1+\cdots+1}_{n-\text{times}})=\underbrace{f(1)+\cdots+f(1)}_{n-\text{times}}=0$$

and $n<0$, since $f(-1)=0$, we have by similar computations $f(n)=0$ so that $f=0_{\mathrm{End}(G)}$. The surjectivity is immediate: for any $n\in\mathbb{Z}$, $a\mapsto na$ is a homomorphism of $(\mathbb{Z},+)$.

Exercise 2. (Examples of ring homomorphisms)

1. The ring structure on $\mathrm{Maps}(k,k)$ is induced, as in item (ii) of the previous exercise, by the structure of k. Let us denote the map ϕ. We have to check that $\phi(P(Q-R))=\phi(P)\cdot(\phi(Q)+\phi(R))$. Let $a\in k$, we have:

$$\begin{aligned} \phi(P(Q+R))(a) &= P(Q+R)(a)\\ &= P(a)(Q(a)+R(a)) \text{ usual rules of evaluation of polynomials}\\ &\quad\text{(for example writing down the polynomials in the basis}\\ &\quad ((x-a)^i)_{i\in\mathbb{N}}\text{) the evaluation is just theconstant term}\\ &= \phi(P)(a)(\phi(Q)(a)+\phi(R)(a))\end{aligned}$$

hence the equality. Moreover $\phi(1)=[a\mapsto 1]=1_{\mathrm{Maps}(k,k)}$.
Let us prove that I_{a_0} is a subgroup of $\mathrm{Maps}(k,k)$ (for a fixed $a_0\in k$). Pick $f,g\in I_{a_0}$ and evaluate $(f-g)(a_0)=f(a_0)-g(a_0)=0$; which means $f-g\in I_{a_0}$. So $(I_{a_0},+)$ is a subgroup of $\mathrm{Maps}(k,k)$. Now, for $f\in I_{a_0}$ and $g\in\mathrm{Maps}(k,k)$, we have $(fg)(a_0)=f(a_0)g(a_0)=0g(a_0)=0$ so I_{a_0} is an ideal of $\mathrm{Maps}(k,k)$.
We have $\phi^{-1}(I_{a_0})=\{P\in k[x],\ P(a_0)=0\}=\{P\in k[x],\ (x-a_0)|P\}=(x-a_0)$ the principal ideal of $k[x]$ generated by the polynomial $x-a_0$.

2. Again the ring structure is the one induced, as in item (ii) of the previous exercise, by the structure of A. Let us denote the map ϕ. We have:

$$\phi(f \cdot (g+h)) = (f \cdot (g+h))(x) = f(x)(g(x)+h(x)) = \phi(f)(\phi(g)+\phi(h))$$

and $\phi(1_{A^X}) = 1_{A^X}(x) = 1$ so ϕ is a ring homomorphism.

3. For $n \geq 1$, let $\phi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}$ be a ring homomorphism. Then $\phi(1) = 1$ and since ϕ is homomorphism of commutative groups

$$\mathbb{Z} \ni n = \underbrace{1 + \cdots + 1}_{n-\text{times}} = \underbrace{\phi(1) + \cdots + \phi(1)}_{n-\text{times}} = \phi(\underbrace{1 + \cdots + 1}_{n-\text{times}}) = \phi(\overline{n}) = \phi(\overline{0}) = 0 \in \mathbb{Z}$$

so there is no such ring homomorphism.

Exercise 3. (Kernel of ring homomorphism)

We recall (by Euclidean division) that a polynomial $P \in k[x]$ admits $a \in k$ as a root (i.e. $P(a) = 0$) if and only if $(x-a)|P$. Moreover if $a \neq b$ are distinct elements of k, then $x-a$ and $x-b$ are coprime (as shown by $(a-b)^{-1}(x-b) - (a-b)^{-1}(x-a) = 1$) so that if a and b are roots of a polynomial P, then $(x-a)(x-b)|P$ (or writing down the Euclidean division $P = (x-a)Q$ we have $0 = P(b) = (b-a)Q(b)$ so $Q(b) = 0$ i.e. Euclidean division gives $Q = (x-b)Q'$). As a consequence, a non-zero polynomial P of degree d can have at most d distinct roots.
Now if k is infinite, let us consider $P \in ker(\phi)$; we have $P(a) = 0$ for any $a \in k$ i.e. a is a root of P for any $a \in k$. Since k is infinite, by the previous reminder, P has to be zero. So ϕ is injective.
Conversely, if ϕ is not injective, pick $P \in ker(\phi)\backslash\{0\}$. Since any $a \in k$ is a root of P and P has at most $\deg(P)$ distinct roots, k has at most $\deg(P) < \infty$ elements.
If $k = \mathbb{F}_q$, set $F = \prod_{a \in k}(x-a)$. It is a non-zero polynomial since $k[x]$ is a domain (or as shown by its expansion $x^{|k|} - x$ by Lagrange's theorem) and for any $a \in k$, $F(a) = 0$ so $F \in ker(\phi)$. Moreover for any $P \in k[x]$, $\phi(PF) = [x \mapsto P(x)F(x)] = [x \mapsto 0] = 0$. Thus the principal ideal $(F) = \{FP,\ P \in k[x]\}$ is contained in $ker(\phi)$.
Now, for $P \in k[x]$, $\phi(P) = 0$ if and only if for any $a \in k$, a is a root of P. Since for $a \neq b$ in k, $x-a$ and $x-b$ are coprime, we have $F|P$ i.e. $P \in (F)$. As a consequence $ker(\phi) = (F)$.

Notice that even when k is infinite, $ker(\phi) = \{0\}$ is a principal ideal.

Exercise 4. (Rings with few ideals)

(1) The two distinct ideals that exist in any (non-zero) ring A are the principal ideals (0) and $(1) = A$. Assume A has no other ideal. Then pick $a \in A\backslash\{0\}$ and consider the principal ideal $(a) = \{ab,\ b \in A\} \subset A$. Since as a set $(0) = \{0\}$ and $a \neq 0$, $(a) \neq (0)$ and since there are exactly two distinct ideals, we have $(a) = (1) = A$. In particular $1 \in (a)$ i.e. $\exists b \in A$, such that $ab = 1$. So any non-zero element of A has an inverse. So such A is a field.

Now when A is not a field, there exists $a \in A\backslash\{0\}$ such that $ab \neq 1$ for any $b \in A$; in other words, $1 \notin (a)$. In particular $(1) \neq (a)$ and since $a \neq 0$, $(a) \neq (0)$. So A contains at least three distinct principal ideals.

(2) As $char(k) = 0$, we have a natural inclusion (injective ring homomorphism) of $\mathbb{Q} \subset k$. Define $R : k[x] \to k[x]$ to be the linear endomorphism whose action on the natural basis of $k[x]$ is given by $x^\ell \mapsto \frac{x^{\ell+1}}{\ell+1}$, $\ell \geq 0$. Then for a polynomial $P = a_0 + a_1x + \cdots + a_dx^d$, with $a_i \in k$, we have

$$(D \circ R)(P) = D(\sum_{i=0}^{d} a_i \frac{x^{i+1}}{i+1}) = \sum_{i=0}^{d} a_i x^i = P$$

so R is a right inverse to D.
If D had a left inverse $L \in \mathrm{End}_k(k[x])$ then we would have $P = L \circ D(P)$ for any $P \in k[x]$ in particular D would be injective. But we know that D is not injective as shown by $D(1) = 0$ (and $1 \neq 0$) so D does not admit a left inverse.

The purpose of the question was to emphasize that when dealing with non-commutative rings (such as $\mathrm{End}_k(k[x])$, $D \circ R(1) = 1 \neq 0 = R(0) = R \circ D(1)$), there is a distinction (a priori) between left ideals (i.e. subgroup $(I, +) \subset (A, +)$ such that $fg \in I$ as soon as $g \in I$) right ideals (i.e. subgroup $(I, +) \subset (A, +)$ such that $fg \in I$ as soon as $f \in I$) and two-sided ideals (i.e. subgroup $(I, +) \subset (A, +)$ such that $fg \in I$ as soon as $g \in I$ or $f \in I$).