Solutions of exercise sheet 8

The content of the marked exercises **(*)** should be known for the exam.

1. **(*)** [Formal construction of the polynomial ring] Let A be a commutative ring and consider the set

$$V = \{(a_i) \mid i \in \mathbb{Z}_{\geq 0}, a_i \in A, a_i = 0 \text{ for } i \text{ large enough}\}.$$

Endowing V with componentwise sum and with the scalar multiplication $a \cdot (a_i) = (a \cdot a_i)$, we have that V is an A-module. Define a multiplication

$$V \times V \to V$$
$$((a_i), (b_i)) \mapsto (a_i) \cdot (b_i) = (c_i), c_i = \sum_{\substack{j,k \geq 0 \\ j+k=i}} a_j b_k$$

1. Show that this product is well defined.
2. Show that $(1_A, 0_A, 0_A, \dots)$ is a neutral element for this product, and that the product is associative, commutative and distributive with respect to addition. This allows us to conclude that V is a ring.
3. Let $Y := (\alpha_i)$, with $\alpha_1 = 1_A$ and $\alpha_i = 0_A$ for $i \neq 1$. For $j \geq 0$, find the sequence of elements β_i for which $Y^j = (\beta_i)$. Deduce that $(Y^j)_{j \geq 0}$ is a basis of V as an A-module.
4. Let B be a commutative ring, $f_0 : A \to B$ a ring homomorphism and $b \in B$. Prove that there exists a unique ring homomorphism $f : V \to B$ sending $f(Y) = b$ and $f(a \cdot 1_V) = f_0(a)$ for each $a \in A$.
5. Let M be an A-module and $T : M \to M$ an A-linear map. Show that there exists a unique V-module structure $\cdot_V$ on M such that $Y \cdot_V m = T(m)$ and $(a \cdot 1_V) \cdot_V m = a \cdot_A m$. Moreover, show that if M is finitely generated as an A-module, then so it is as a V-module. Is the converse true?
6. Prove that V and $A[X]$ are isomorphic rings.

Solution:

1. We have that $(a_i) \cdot (b_i)$ defined as above is a uniquely determined sequence (c_i) of elements in A_i, for every $(a_i), (b_i) \in$. The product is well-defined if this sequence belongs to V, that is, if $c_i = 0$ for $i \gg 0$. By hypothesis, there exists positive

numbers $n, m \geq 0$ such that $a_i = 0$ for $i \geq n$ and $b_i = 0$ for $i \geq m$. Then one has for every $N \geq n + m$ that

$$c_N = \sum_{i=0}^{N} a_i b_{n+m-i} = \sum_{i=0}^{m} a_i b_{n+m-i} + \sum_{i=m+1}^{N} a_i b_{n+m-i} = 0 + 0 = 0,$$

since for $i \in \{0, \dots, m\}$ we have $n + m - i \geq m$, so that $b_{n+m-i} = 0$, and for $i \in \{m+1, \dots, m+n0\}$ we have $a_i = 0$.

2. First, notice that the product is commutative, as we can interchange the indexes j and k in the sum appearing in the definition. Then we just need to check that $(e_i) = (1, 0, 0, \dots)$ is neutral on one side, and we have

$$(1, 0, 0, \dots) \cdot (a_i) = \Big(\sum_{\substack{j,k \geq 0 \\ j+k=i}} e_j a_k \Big) = (a_i)\,,$$

since for $j \neq 0$ we have $e_j = 0$. Hence $1_V := (1, 0, 0, \dots)$ is a neutral element for the multiplication.
As concerns associativity, for every $(a_i), (b_i), (c_i) \in V$ applying the definition we have

$$((a_i) \cdot (b_i)) \cdot (c_i) = \Big(\sum_{j=0}^{i} a_j b_{i-j} \Big) \cdot (c_i) = \Big(\sum_{k=0}^{i} \Big(\sum_{j=0}^{k} a_j b_{k-j} \Big) c_{i-k} \Big) =$$
$$= \Big(\sum_{k=0}^{i} \sum_{j=0}^{k} a_j b_{k-j} c_{i-k} \Big) = \Big(\sum_{\substack{\alpha,\beta,\gamma \geq 0 \\ \alpha+\beta+\gamma=i}} a_\alpha b_\beta c_\gamma \Big)$$

and

$$(a_i) \cdot ((b_i) \cdot (c_i)) = (a_i) \cdot \Big(\sum_{k=0}^{i} b_k c_{i-k} \Big) = \Big(\sum_{j=0}^{i} a_j \Big(\sum_{k=0}^{i-j} b_k c_{(i-j)-k} \Big) \Big) =$$
$$= \Big(\sum_{j=0}^{i} \Big(\sum_{k=0}^{i-j} a_j b_k c_{i-j-k} \Big) \Big) = \Big(\sum_{\substack{\alpha,\beta,\gamma \geq 0 \\ \alpha+\beta+\gamma=i}} a_\alpha b_\beta c_\gamma \Big)$$

so that the product is associative. Finally, we check distributivity with respect to addition (only one side, being the product commutative): for every $(a_i), (b_i), (c_i) \in V$ we have

$$((a_i) + (b_i)) \cdot (c_i) = (a_i + b_i) \cdot (c_i) = \Big(\sum_{j=0}^{i} (a_j + b_j) c_i \Big) = \Big(\sum_{j=0}^{i} (a_j c_{i-j} + b_j c_{i-j}) \Big) =$$
$$= \Big(\sum_{j=0}^{i} (a_j c_{i-j}) \Big) + \Big(\sum_{j=0}^{i} (b_j c_{i-j}) \Big) = (a_i) \cdot (c_i) + (b_i) \cdot (c_i).$$

So V is a ring with componentwise sum, multiplication defined as above, $0_V = (0, \dots)$ and $1_V = (1, 0, \dots)$.

See next page!

3. For $i, j \in \mathbb{Z}_{\geq 0}$ we denote with $\delta_{i,j} \in A$ the Kronecher's delta of i and j, which is 1 if $i = j$, and 0 otherwise. Then $Y = (\delta_{i1})_i$. We claim that $Y^j = (\delta_{i,j})_i$ for all $j \geq 0$. This is easily proven by induction. For $j = 0, 1$ this is clear. Now suppose that $Y^k = (\delta_{i,k})_i$ (inductive hypothesis) and let us prove that $Y^{k+1} = (\delta_{i,(k+1)})_i$. Write $Y^{k+1} = (\vartheta_i)$. Then $\vartheta_{k+1} = \sum_{\substack{j,l \geq 0 \\ j+l=k+1}} \delta_{j,k}\delta_{l,1} = 1$, because we can make both δ's non-zero only when we choose $j = k$ and $l = 1$, in which case we obtain 1 as summand. On the other hand, for $h \neq k+1$ we see that $\vartheta_h = \sum_{\substack{j,l \geq 0 \\ j+l=h}} \delta_{j,k}\delta_{l,1} = 0$, because the couple of indexes $(j, l) = (k, 1)$, which is the only one making both δ's non-zero, is not considered in the sum. In conclusion, $Y^k = (\delta_{i,k})_i$, that is, Y^k is the sequence with 1 in the k-th position and 0 everywhere else.

   Then for every $a = (a_i) \in V$ we have that $a = \sum_{i:a_i \neq 0} a_i Y^i$, which is a finite sum by definition of V, so that $(Y^i)_{i \in \mathbb{Z}_{\geq 0}}$ spans all V over A. Moreover a finite linear combination $\sum_{j=0}^m a_{i_j} \cdot Y^{i_j}$, where the i_j's are distinct indexes in $\mathbb{Z}_{\geq 0}$ is zero if and only if all the a_{i_j} are zero, so that we can conclude that $(Y^i)_{i \in \mathbb{Z}_{\geq 0}}$ is an R-basis for V. As the set of indexes i such that $a_i \neq 0$ is finite, there exists $d \in \mathbb{Z}$ bigger or equal than all those i's, and we can rewrite $a = \sum_{i \leq d} a_i Y^i$. Notice that since the Y^j are R-linear independent, this decomposition is unique up to choosing a different d, in which case we can just have fewer/more zero summand.

4. We first prove uniqueness and then existence. Also, by abuse of notation, for $r \in A$ we write $r = r \cdot 1_V \in V$. It is the sequence with r in the 0-th position and 0 everywhere else.

   Suppose that $f : V \to B$ is a ring homomorphism sending $A \ni a \mapsto f_0(a)$ and $Y \mapsto b$. Then by applying previous point, for $s \in V$ we can write $s = \sum_{i=0}^d s_i Y^i$ for some $s_i \in A$ and $d \in \mathbb{Z}_{\geq 0}$, giving

$$f(s) = f\Big(\sum_{i=0}^d s_i Y^i\Big) = \sum_{i=0}^d f(s_i) f(Y^i) = \sum_{i=0}^d f_0(s_i) f(Y^i) = \sum_{i=0}^d f_0(s_i) b^i,$$

   which means that f has a prescribed behavior on all V, that is, if f exists it is unique.

   To prove existence, we just check that the definition for f on s that we found while proving uniqueness, that is,

$$f\Big(\sum_{i=0}^d s_i Y^i\Big) = \sum_{i=0}^d f_0(s_i) b^i$$

   gives indeed a ring homomorphism. First, notice that this is a good definition because the decomposition $s = \sum_{i=0}^d s_i Y^i$ is unique up to extra zero-summand, and $f_0(0) = 0$ being f_0 a ring homomorphism. Then we have $f(0) = f(0 \cdot Y^0) = f_0(0) b^0 = 0$, and $f(1) = f(1 \cdot Y^0) = f_0(1) b^0 = 1$ being f_0 a ring homomorphism. To conclude, we prove that f respects sums and multiplications. For every $s, t \in V$, we let d be big enough so that we can write $s = \sum_{i=0}^d s_i Y^i$ and $t = \sum_{i=0}^d t_i Y^i$.

Now

$$
\begin{aligned}
f(s+t) =& f\Big(\sum_{i=0}^{d}(s_i+t_i)Y^i\Big) = \sum_{i=0}^{d} f_0(s_i+t_i)b^i = \\
&= \sum_{i=0}^{d}(f_0(s_i)+f_0(t_i))b^i = \sum_{i=0}^{d} f_0(s_i)b^i + \sum_{i=0}^{d} f_0(s_i)b^i = \\
&= f\Big(\sum_{i=0}^{d} s_iY^i\Big) + f\Big(\sum_{i=0}^{d} t_iY^i\Big) = f(s)+f(t),
\end{aligned}
$$

and

$$
\begin{aligned}
f(s\cdot t) =& f\Big(\sum_{i=0}^{2d}\Big(\sum_{j=0}^{i} s_jt_{i-j}\Big)Y^i\Big) = f\Big(\sum_{i=0}^{2d} f_0\Big(\sum_{j=0}^{i} s_jt_{i-j}\Big)b^i\Big) = \\
&= \sum_{i=0}^{2d}\Big(\sum_{j=0}^{i} f_0(s_j)f_0(t_{i-j})\Big)b^i = \sum_{i=0}^{d} f_0(s_i)b^i \cdot \sum_{i=0}^{d} f_0(t_i)b^i = f(s)\cdot f(t),
\end{aligned}
$$

and $f : V \to B$ is a ring homomorphism which maps $Y \mapsto b$ and $A \ni a \mapsto f_0(a)$.

5. Similarly as in previous point, we first prove uniqueness, and then existence. By hypothesis, we have an A-module structure on M, and an A-linear map $T : M \to M$.

   Suppose we have that M has also a V-module structure with $Y \cdot m = T(m)$ and with $a \in A$ acting on $m \in M$ as it does with respect to the given A-module structure. Then for every $s = \sum_{i=0}^{d} s_iY^i \in V$ and $m \in M$ we have

$$
s\cdot m = \Big(\sum_{i=0}^{d} s_iY^i\Big)\cdot m = \sum_{i=0}^{d} s_i \cdot T^i(m) = \sum_{i=0}^{d} T^i(s_i\cdot m),
$$

   so that $s \cdot m$ is uniquely determined, and the V-module structure is unique, if it exists.

   Disclaimer: Notice that by T^i we denote the multiplication of T with itself in the ring of additive endomorphisms $\mathrm{End}(M)$, which is just the i-th iteration of the endomorphism T.

   Now we prove existence, by checking that the definition we found,

$$
\Big(\sum_{i=0}^{d} s_iY^i\Big)\cdot m = \sum_{i=0}^{d} T^i(s_i\cdot m),
$$

   gives indeed a V-module structure on M coinciding with the one of A-module on elements $a \in A$ and satisfies $Y \cdot m = T(m)$. Those properties are clear from the definition, which is well-given as the decomposition $s = \sum_{i=0}^{d} s_iY^i$ is unique up to adding zero summands, and $0_A \cdot m = 0$ by hypothesis. Clearly, for every $m \in M$

See next page!

we have $1_V \cdot m = (1 \cdot Y^0) \cdot m = T^0(1 \cdot m) = m$. Now we check that $s\cdot$ is additive for every $s = \sum_{i=0}^d s_i Y^i \in V$: for every $m, n \in M$, we have indeed:

$$s \cdot (m+n) = \Big(\sum_{i=0}^d s_i Y^i\Big) \cdot (m+n) = \sum_{i=0}^d T^i(s_i \cdot (m+n)) =$$
$$= \sum_{i=0}^d T^i(s_i \cdot (m)) + \sum_{i=0}^d T^i(s_i \cdot (n)) = s \cdot m + s \cdot n.$$

Now we check compatibility with operations in V. For every $m \in M$ and $s, t \in V$, with $s = \sum_{i=0}^d s_i Y^i$ and $t = \sum_{i=0}^d t_i Y^i$, we have

$$(s+t) \cdot m = \sum_{i=0}^d T^i((s_i + t_i) \cdot m) = \sum_{i=0}^d T^i(s_i \cdot m) + = \sum_{i=0}^d T^i(t_i \cdot m) = s \cdot m + t \cdot m$$

and

$$(s \cdot t) \cdot m = \Big(\sum_{i=0}^{2d} \Big(\sum_{j=0}^{i} s_j t_{i-j}\Big) Y^i\Big) \cdot m = \sum_{i=0}^{2d} \sum_{j=0}^{i} s_j t_{i-j} \cdot T^i(m) =$$
$$= \sum_{k=0}^d \sum_{h=0}^d s_k t_h \cdot T^{k+h}(m) = \sum_{k=0}^d s_k \cdot T^k\Big(\sum_{h=0}^d t_h \cdot T^h(m)\Big) = s \cdot (t \cdot m)$$

The proof is finished, since we have also proven that the axioms of V-modules are satisfied.

6. Define a map

$$\phi : V \to R[X]$$
$$\sum_{i=0}^d s_i Y^i \mapsto \sum_{i=0}^d s_i X^i.$$

It is well-defined because of Point 3, and it is clearly surjective. The operations defined in V makes ϕ a ring homomorphism, whose kernel is trivial since a polynomial is zero if it only has zero coefficients. Hence this is an isomorphism of rings.

2. Let A be a commutative ring

1. Show that there exists a unique A-linear map

$$D : A[X] \to A[X]$$

such that

$$D(X^i) = iX^{i-1}, \quad i \geq 1$$
$$D(1) = 0.$$

Is D a ring homomorphism?

Please turn over!

2. Prove that for all $P, Q \in A[X]$ one has

$$D(PQ) = PD(Q) + QD(P)$$

3. (Factorization Theorem) Now let $A = K$ be a field, and $P \in K[X]$. Prove that for every $\alpha \in K$ one has $P(\alpha) = 0$ if and only if P is divisible by $X - \alpha$, that is, there is a polynomial $Q \in K[X]$ such that $P(X) = (X - \alpha)Q(X)$ [*Hint:* One implication is immediate. For the other, divide P by $X - \alpha$.]

4. We say that $\alpha \in K$ is a multiple root of $P \in K[X]$ if P is divisible by $(X - \alpha)^2$. Prove: α is a multiple root of P if and only if $P(\alpha) = D(P)(\alpha) = 0$.

Solution:

1. First, notice that such a map D cannot be a ring homomorphism, since it sends $1 \mapsto 0 \neq 1$.

   Since the X^i, $i \geq 0$, form a basis of $A[X]$ as an A-module (as the isomorphism in Exercise 1.6 is easily seen to be an isomorphism of A-modules as well), for every map $f : \{X^i\} \to A[X]$ there exists a unique R-linear map $R[X] \to R[X]$ which behaves as f on the X^i. In this case, we can take $f : X^i \mapsto iX^{i-1}$. This is because of the Universal Property of free modules:

Theorem Let M be a free R-module $M = \bigoplus_{i \in I} R \cdot m_i$, and denote $B = \{m_i | i \in I\}$. Let N be another R-module. Then for every map $f : B \to N$ there exists a unique R-linear map $\alpha : M \to N$ such that $\alpha|_M = f$

Proof: Suppose that $m \in M$, then by hypothesis we have a unique decomposition $m = \sum_{i \in I} r_i \circ m_i$, with $r_i = 0$ for almost every $i \in I$. If $\alpha : M \to N$ is R-linear and $\alpha|_M = f$, then we have that $\alpha(m) = \sum_{i \in I} r_i \alpha(m_i) = \sum_{i \in I} r_i f(m_i)$ is uniquely determined, proving uniqueness of α. To conclude, we need to check that

$$\alpha(\sum_{i \in I} r_i \circ m_i) = \sum_{i \in I} r_i f(m_i)$$

defines indeed an R-linear map. Uniqueness of the linear combination expressing $m \in M$ proves that α is well-defined, and linearity follows easily from the fact that linear combinations of linear combinations of the m_i's are still linear combinations of the m_i. □

2. The identity can be directly checked by writing $P = \sum_{i=0}^{m} a_i X^i$ and $Q = \sum_{j=0}^{n} b_j X^j$ and computing both sides. An equivalent (but faster) way to do this is to observe that both sides of the identity $D(PQ) = PD(Q) + QD(P)$ are linear in P and in Q. Then it is enough to check the equality for an arbitrary P and $Q = X^k$, $k \geq 0$, and this is then equivalent to check the equality for $P = X^j$ and $Q = X^k$, with $j, k \geq 0$, which is immediate:

$$D(X^j X^k) = D(X^{j+k}) = (j+k)D^{j+k-1} = X^j \cdot kX^{k-1} + X^k \cdot jX^{j-1}.$$

See next page!

3. Suppose that $P \in K[X]$ is divisible by $(X-\alpha)$, that is, there is a polynomial $Q \in K[X]$ such that $P(X) = (X-\alpha)Q(X)$. Then clearly $P(\alpha) = 0 \cdot Q(0)$, so that α is a root of P.

   Conversely, assume that $P(\alpha) = 0$. As seen in class, we can use Euclidean division to obtain polynomials $Q(X), R(X)$ such that $P(X) = (X-\alpha)Q(X) + R(X)$ and $\deg(R) < \deg(X-\alpha) = 1$. Then $R(X) = r \in K$, and

$$0 = P(\alpha) = 0 \cdot Q(\alpha) + r = r,$$

   so that $P(X)$ is divisible by $X - \alpha$.

4. Suppose that $\alpha \in K$ is a multiple root of P, that is, $P(X) = (X-\alpha)^2 Q(X)$. Clearly, $P(\alpha) = 0$. Moreover, by Point 2 we have

$$D(P) = (X-\alpha)^2 D(Q) + QD((X-\alpha)^2) = (X-\alpha^2)D(Q) + 2(X-\alpha)Q,$$

   from which $D(P)(\alpha) = 0$ just by substitution.

   Conversely, assume that $P(\alpha) = D(P)(\alpha) = 0$. By previous point we can write $P = (X-\alpha)S$ for some polynomial $S \in K[X]$. Then by Point 2

$$D(P) = D((X-\alpha)S) = (X-\alpha)D(S) + S,$$

   and the condition $D(P)(\alpha) = 0$ gives $S(\alpha) = 0$, so that S is again divisible by $X-\alpha$, and we can conclude that P is divisible by $(X-\alpha)^2$, so that α is a multiple root of P.

3. Let A be an integral domain. Show that $A[X]^\times = A^\times$.

Solution:

Of course, $A^\times \subseteq A[X]^\times$ because $A \subseteq A[X]$. To conclude, we just need to prove that any invertible $f \in A[X]$ is indeed in $A^\times$. Suppose that $f \in A[X]^\times$, and that $fg = 1$ for some $g \in A[X]$. Of course f and g cannot be 0, so that we have well-defined $\deg(f), \deg(g) \geq 0$. Being A a domain, we have that $\deg(fg) = \deg(f) + \deg(g)$ (because the product of the leading coefficients is the leading coefficient of the product, as it cannot vanish). Hence $0 = \deg(1) = \deg(f) + \deg(g)$, and the only possibility is that $\deg(f) = \deg(g) = 0$. Hence $f, g \in A$, giving $f \in A^\times$.

4. Let K be a field, and consider the ideal I generated by X and Y in $K[X,Y]$. Show:

1. I is not principal;
2. I is maximal.

Solution:

Please turn over!

1. By contradiction, suppose that $I = (P)$ for some $P \in K[X,Y]$. Then there must exist $Q, R \in K[X,Y]$ such that $X = P \cdot Q$ and $Y = P \cdot R$. Notice that both $K[X]$ and $K[Y]$ are integral domains, so that regarding $K[X,Y]$ as $K[X][Y]$ or as $K[Y][X]$ we have that both the degree in X and the degree in Y of a product of polynomials are the sum of the degrees of the polynomials. As P, Q, R cannot be zero, they have a well-defined degree. In particular, we have $0 = \deg_Y(X) = \deg_Y(P) + \deg_Y(Q)$, which implies $\deg_Y(P) = 0$, and $0 = \deg_X(Y) = \deg_X(P) + \deg_X(R)$, which implies $\deg_X(P) = 0$. Then $P \in K$, since it is constant in both variables. In particular, $P \in K^\times$, so that $1 \in (P)$ and $P = K[X,Y]$. This means in particular that for some $A, B \in K[X,Y]$ we can write $X \cdot A + Y \cdot B = 1$, which is a contradiction (as evaluating the two sides of the equality at $X = Y = 0$ we obtain $0 = 1$, which is not true in a field. Hence I is a not a principal ideal.
2. We can do this by proving that $K[X,Y]/(X,Y)$ is a field. Since we are adding to K two variables which then we set equal to zero (by quotienting over I), intuition suggests that $K[X,Y]/(X,Y) \cong K$, which is a field by hypothesis. This is true: consider the map

$$\begin{aligned} \phi : K[X,Y] &\to K \\ P(X,Y) &\mapsto P(0.0). \end{aligned}$$

   It is a ring homomorphism (as it is the composition of evaluation maps $K[X][Y] \to K[X] \to K$), and it is clearly surjective, as every element in K is its own counterimage. We claim that $\ker(\phi) = (X,Y)$. The inclusion "$\supseteq$" is immediate. For the other inclusion, take $P \in \ker(\phi)$. Dividing P by X and its remainder by Y, we obtain a constant $c \in K[X,Y]$ and polynomials $A \in K[X,Y]$, $B \in K[Y]$ such that $P = XA + YB + c$, and then evaluating the two sides at $(0,0)$ we obtain $0 = P(0,0) = c$, so that $P = XA + YB \in (X,Y)$.

   To conclude, we apply First Isomorphism Theorem for rings, which gives an isomorphism $K[X,Y]/(X,Y) \cong K$ as desired.