pdf file

0.D Polynomial rings

Let A be a ring, I be a set and $\mathbb{N}^{(I)}$ be the I-fold direct sum of the additive monoid $(\mathbb{N}, +)$, i.e. $\mathbb{N}^{(I)} := \{\nu = (\nu_i)_{i\in I} \in \mathbb{N}^I \mid \nu_i = 0 \text{ for almost all } i \in I\}$ with the componentwise addition.

For $i \in I$, let $\varepsilon_i := (\delta_{ij})_{j\in I} \in \mathbb{N}^{(I)}$, where δ_{ij} denotes the Kronecker-delta. Then every element $\nu = (\nu_i) \in \mathbb{N}^{(I)}$ can be written uniquely in the form $\nu = \sum_{i\in I} \nu_i \varepsilon_i$.

Recall that $A^{(\mathbb{N}^{(I)})}$ is a free A-module with the standard basis $\{e_\nu \mid \nu \in \mathbb{N}^{(I)}\}$, where e_ν is the map $\mathbb{N}^{(I)} \longrightarrow A$ defined by $e_\nu(\mu) = \delta_{\nu\mu}$, $\mu \in \mathbb{N}^{(I)}$.

We would like to define a multiplication on $A^{(\mathbb{N}^{(I)})}$ so that the A-module $A^{(\mathbb{N}^{(I)})}$ is an A-algebra. For this we shall make use of the addition in $\mathbb{N}^{(I)}$.

0.D.1 Definition For $f, g \in A^{(\mathbb{N}^{(I)})}$, define $fg \in A^{(\mathbb{N}^{(I)})}$ by the formula:

$$(fg)(\nu) = \sum_{\substack{\alpha \in \mathbb{N}^{(I)} \\ \nu-\alpha \in \mathbb{N}^{(I)}}} f(\alpha)\, g(\nu-\alpha).$$

Note that the sum on the right hand side is finite, since for a given $\nu \in \mathbb{N}^{(I)}$, there are only finitely many $\alpha \in \mathbb{N}^{(I)}$ with $\nu - \alpha \in \mathbb{N}^{(I)}$. Further, $fg \in A^{(\mathbb{N}^{(I)})}$, i.e. $(fg)(\nu) \neq 0$ only for finitely many $\nu \in \mathbb{N}^{(I)}$, since there are only finitely many $\alpha, \beta \in \mathbb{N}^{(I)}$ with $f(\alpha) \neq 0$ and $g(\beta) \neq 0$.

It is easy to check that with this multiplication the A-module $A^{(\mathbb{N}^{(I)})}$ is a commutative A-algebra with unity $1 : \mathbb{N}^{(I)} \longrightarrow A$ defined by $1(0) = 1_A$ and $1(\nu) = 0$ for all $\nu \in \mathbb{N}^{(I)}$, $\nu \neq 0$.

The map $A \xrightarrow{\iota} A^{(\mathbb{N}^{(I)})}$ defined by $a \longmapsto \tilde{a}$, where $\tilde{a} : \mathbb{N}^{(I)} \longrightarrow A$ is defined by $\tilde{a}(0) = a$ and $\tilde{a}(\nu) =$ for all $0 \neq \nu \in \mathbb{N}^{(I)}$, is a ring homomorphism; in fa $\tilde{a} = a \cdot 1$ and hence ι is the structure homomorphis of the A-algebra $A^{(\mathbb{N}^{(I)})}$. Further, ι is injective and hence we can identify A as a subring of $A^{(\mathbb{N}^{(I}}$ via the map ι.

For $i \in I$, we put $X_i := e_{\varepsilon_i} \in A^{(\mathbb{N}^{(I)})}$ and for $\underbrace{\nu}_{=(\nu_i)} \in \mathbb{N}^{(I}$ put $X^\nu := \prod_{i \in I} X_i^{\nu_i}$.

The elements X_i, $i \in I$ in $A^{(\mathbb{N}^{(I)})}$ are called <u>indeterminates over A</u> and the element X^ν in $A^{(\mathbb{N}^{(I)})}$ is called the <u>monomial in X_i, $i \in I$</u> <u>corresponding to $\nu \in \mathbb{N}^{(I)}$</u>.

Note that: for $\nu \in \mathbb{N}^{(I)}$, $X^\nu = e_\nu$ in $A^{(\mathbb{N}^{(I)})}$.

(<u>Proof</u> By induction on $|\nu| := \sum_{i \in I} \nu_i$. If $\nu = 0$, then each $\nu_i = 0$ and $X^\nu = 1 = 1_A$ and $e_0 = 1 = 1_A$. Now, suppose $|\nu| \geq 1$. Then choose $j \in I$ such that $\nu_j > 0$ and let $\nu' := \nu - e_j \in \mathbb{N}^{(I)}$. Then $X^\nu = \prod_{i \in I} X_i^{\nu_i} = X^{\nu'} \cdot X_j = e_{\nu'} \cdot e_j$ by induction. Now, $e_{\nu'} \cdot e_j = e_{\nu' + j} = e_\nu$, since

$$(e_{\nu'} \cdot e_j)(\mu) = \sum_{\substack{\alpha, \beta \in \mathbb{N}^{(I)} \\ \alpha + \beta = \mu}} e_{\nu'}(\alpha) \cdot e_j(\beta) = \begin{cases} e_{\nu'}(\nu') \cdot e_j(j), & \text{if } \mu = \nu' + j = \nu \\ 0, & \text{otherwise} \end{cases}$$

With this notation, $A^{(\mathbb{N}^{(I)})}$ is a free A-module with basis $\{X^\nu \mid \nu \in \mathbb{N}^{(I)}\}$ (= the set of monic monomials in X_i, $i \in I$). Therefore every element $f \in A^{(\mathbb{N}^{(I)})}$ has a unique expression of the form:

$$f = \sum_{\nu \in \mathbb{N}^{(I)}} a_\nu X^\nu \quad \text{with } a_\nu = f(\nu) \in A,\ \nu \in \mathbb{N}^{(I)} \text{ and } a_\nu = 0 \text{ for almost all } \nu \in \mathbb{N}^{(I)}$$

This A-algebra $A^{(\mathbb{N}^{(I)})}$ is called the <u>polynomial ring in the indeterminates</u> $\{X_i \mid i \in I\}$ <u>over</u> A and is denoted by $A[X_i \mid i \in I]$ or $A[X_i]_{i \in I}$. Its elements are called <u>polynomials</u> in X_i, $i \in I$ <u>with coefficients in</u> A. Therefore every polynomial in $A[X_i \mid i \in I]$ is a finite sum of the elements of the form $a_\nu X^\nu$, $\nu \in \mathbb{N}^{(I)}$, $a_\nu \in A$; these elements are called <u>monomials in</u> $\{X_i \mid i \in I\}$ <u>over</u> A. More over, this expression is unique, i.e. $\sum_{\nu \in \mathbb{N}^{(I)}} a_\nu X^\nu = \sum_{\nu \in \mathbb{N}^{(I)}} b_\nu X^\nu \iff a_\nu = b_\nu$ for all $\nu \in \mathbb{N}^{(I)}$.

Note that every polynomial $f \in A[X_i \mid i \in I]$ contains only finitely many indeterminates X_i, $i \in I$.

For two polynomials $f = \sum_{\nu \in \mathbb{N}^{(I)}} a_\nu X^\nu$, $g = \sum_{\nu \in \mathbb{N}^{(I)}} b_\nu X^\nu$ in $A[X_i]_{i \in I}$, the <u>sum</u> and <u>product</u> polynomials are respectively the polynomials

$$f + g = \sum_{\nu \in \mathbb{N}^{(I)}} (a_\nu + b_\nu) X^\nu \quad \text{and} \quad fg = \sum_\lambda c_\lambda X^\lambda, \text{ where}$$

$$c_\lambda := \sum_{\nu + \mu = \lambda} a_\nu \cdot b_\mu .$$

If $I = \{1, 2, \cdots, n\}$, then we put:

$$A[X_1, \cdots, X_n] = A[X_i \mid i \in \{1, 2, \cdots, n\}].$$

This ring is called the polynomial ring in n indeterminates

$X_1, \cdots, X_n$ over A; every polynomial f in $A[X_1, \cdots, X_n]$ can be written uniquely in the form:

$$f = \sum_{(\nu_1, \cdots, \nu_n) \in \mathbb{N}^n} a_{\nu_1 \cdots \nu_n} X_1^{\nu_1} \cdots X_n^{\nu_n} \text{ with } a_{\nu_1 \cdots \nu_n} \in A \text{ and}$$

$a_{\nu_1 \cdots \nu_n} = 0$ for almost all $(\nu_1, \cdots, \nu_n) \in \mathbb{N}^n$.

O.D.2 The polynomial ring $A[X_i \mid i \in I]$ is generated by $\{X_i \mid i \in I\}$ as an A-algebra. In particular, if I is finite, then $A[X_i \mid i \in I]$ is a finitely generated A-algebra.

O.D.2 Remarks (1) If I is not a finite set, then the polynomial ring $A[X_i \mid i \in I]$ is not a finitely generated A-algebra; this follows from the fact that every polynomial in $A[X_i \mid i \in I]$ contains only finitely many X_i, $i \in I$.

(2) The polynomial ring $A[X_1, \cdots, X_n]$ is not a finitely generated A-module; in fact $\{X_1^{\nu_1} \cdots X_n^{\nu_n} \mid \nu = (\nu_1, \cdots, \nu_n) \in \mathbb{N}^n\}$ (which is not finite) is a basis of $A[X_1, \cdots, X_n]$ and hence no finite subset of $A[X_1, \cdots, X_n]$ can generate the A-module $A[X_1, \cdots, X_n]$ since every polynomial in $A[X_1, \cdots, X_n]$ contain only finitely many $X_1^{\nu_1} \cdots X_n^{\nu_n} = X^{\nu}$, $\nu = (\nu_1, \cdots, \nu_n) \in \mathbb{N}^n$.

Now we come to the most important property called the <u>universal property of the polynomial ring</u>.

0.D.3 Universal property of the polynomial ring

Let B be an A-algebra and let x_i, $i \in I$ be a family of elements of B. Then there exists a unique A-algebra homomorphism

$$\Phi : A[X_i \mid i \in I] \longrightarrow B$$

with $\Phi(X_i) = x_i$ for every $i \in I$.

<u>Proof</u> Uniqueness of Φ is clear from the fact that Φ is A-linear and Φ is a ring homomorphism: for $\nu \in \mathbb{N}^{(I)}$, $\Phi(X^\nu) = \Phi(\prod_{i \in I} X_i^{\nu_i}) = \prod_{i \in I} \Phi(X_i^{\nu_i}) = \prod_{i \in I} \Phi(X_i)^{\nu_i}$

$= \prod_{i \in I} x_i^{\nu_i} = x^\nu$ and hence $\Phi(f) = \Phi\left(\sum_{\nu \in \mathbb{N}^{(I)}} a_\nu X^\nu\right) =$

$\sum_{\nu \in \mathbb{N}^{(I)}} a_\nu \Phi(X^\nu) = \sum_{\nu \in \mathbb{N}^{(I)}} a_\nu x^\nu =: f(x)$.

<u>Existence of Φ</u>: For a polynomial $f = \sum_{\nu \in \mathbb{N}^{(I)}} a_\nu X^\nu$ in $A[X_i \mid i \in I]$, put $f(x) := \sum_{\nu \in \mathbb{N}^{(I)}} a_\nu x^\nu \in B$ and define $\Phi : A[X_i \mid i \in I] \longrightarrow B$ by $f \longmapsto f(x)$. Then $\underbrace{}_{\Phi(X_i) = x_i \text{ for all } i \in I}$ (by using the distributive law and the compatibility of the scalar multiplication of A on B with the multiplication in B) we have

$\Phi(af + bg) = (af + bg)(x) = af(x) + bg(x) = a\Phi(f) + b\Phi(g)$,

and $\Phi(fg) = (fg)(x) = f(x)g(x) = \Phi(f) \cdot \Phi(g)$ for all $a, b \in A$, $f, g \in A[X_i \mid i \in I]$. Therefore Φ is an A-algebra homomorphism.

O.D.4 Definitions

Let B be an A-algebra and let $x := (x_i)_{i\in I} \in B^I$. The ~~unique A-algebra~~ homomorphism

$$\Phi : A[X_i \mid i\in I] \longrightarrow B \text{ with } \Phi(X_i) = x_i \text{ for all } i\in I$$

is denoted by Φ_x and is called the subsitution homomorphism by x. For a polynomial $f\in A[X_i \mid i\in I]$ the image $\Phi_x(f)$ is denoted by $f(x)$ and is called the value of f at the point $x\in B^I$. Since Φ_x is an A-algebra homomorphism, for $f, g\in A[X_i \mid i\in I]$ and $a\in A$, $x\in B^I$, we have:

$$(f+g)(x) = f(x)+g(x), \quad (fg)(x) = f(x)g(x) \text{ and } (af)(x) = af(x).$$

If $y\in B$ and $y = f(x)$, then x is called a y-place of f. In particular, $x\in B^I$ is called a 0-place or zero of f if $f(x)=0$ (equivalently, $f\in \operatorname{Ker}\Phi_x$).

O.D.5 Remarks

(1) The universal property O.D.3 determines a polynomial ring over A, $A\neq 0$ uniquely (up to a unique isomorphism of A-algebras): Suppose that P is an A-algebra and Y_i, $i\in I$ be a family of elements in P. Further, suppose that $(P; Y_i, i\in I)$ satisfies the universal property O.D.3, i.e. for every A-algebra B and every $x = (x_i)\in B^I$, there is a unique A-algebra homomorphism $\Phi : P \longrightarrow B$ such that $\Phi(Y_i) = x_i$ for all $i\in I$. Then there exists a unique isomorphism of A-algebras

$$\psi : A[X_i \mid i\in I] \longrightarrow P \text{ with } \psi(X_i) = Y_i \text{ for all } i\in I.$$

In fact $\psi = \Phi_{(Y_i)}$ is an isomorphism of A-algebras with inverse $P \longrightarrow A[X_i \mid i\in I]$, $Y_i \longmapsto X_i$, $i\in I$ (which exists by assumption on P)

(2) The universal property can be used to give simple examples of A-algebra homomorphism between polynomial rings (over A), for example: Let I, J be sets and let $\sigma : I \longrightarrow J$ be a map. Then there is a unique A-algebra homomorphism

$$\Phi_\sigma : A[Y_i \mid i \in I] \longrightarrow A[X_j \mid j \in J]$$

with $Y_i \longmapsto X_{\sigma(i)}$ for all $i \in I$.

If $A \neq 0$, then Φ_σ is injective (resp. surjective, bijective) if and only if σ is injective (resp. surjective, bijective). Further if $\tau : J \longrightarrow K$ is another map of sets and Φ_τ is the corresponding A-algebra homomorphism, then $\Phi_\tau \circ \Phi_\sigma = \Phi_{\tau\sigma}$. Therefore:

The map $\mathfrak{S}(I) \longrightarrow \mathrm{Aut}_{A\text{-alg}} A[X_i \mid i \in I]$, $\sigma \longmapsto \Phi_\sigma$ is a group homomorphism and hence:

<u>The permutation group $\mathfrak{S}(I)$ operates on the polynomial ring $A[X_i \mid i \in I]$ as a group of automorphisms of A-algebras</u>. The invariant polynomials under this operation are called <u>symmetric polynomials</u>.

(3) Let I, J be sets with $J \subseteq I$. Then we can identify $A[X_j \mid j \in J]$ as an A-subalgebra of $A[X_i \mid i \in I]$ via injective A-algebra homomorphism (see (2) above)

$$A[X_j \mid j \in J] \longrightarrow A[X_i \mid i \in I].$$

This subalgebra precisely (contain) the polynomials (in $A[X_i \mid i \in I]$) which donot contain the indeterminates X_i with $i \in I \setminus J$.

Moreover, we have the cannonical isomorphism of A-algebras (nesting of indeterminates)

$$A[X_i \mid i\in I] \xrightarrow{\approx} (A[X_j \mid j\in J])[X_i \mid i\in I\setminus J]$$

In particular, for $n\in\mathbb{N}^*$, we can identify

$$A[X_1,\dots,X_n] = A[X_1,\dots,X_{n-1}][X_n].$$

(3) For an I-tuple $a=(a_i)_{i\in I}\in A^I$, let φ_a be the A-algebra homomorphism

$$\varphi_a : A[X_i \mid i\in I] \longrightarrow A[X_i \mid i\in I]$$

with $\varphi_a(X_i) = X_i - a_i$ for all $i\in I$. For $a, b\in A^I$, we have $\varphi_a\circ\varphi_b = \varphi_{a+b}$, since $(\varphi_a\circ\varphi_b)(X_i) = \varphi_a(X_i - b_i) = (X_i - a_i) - b_i = X_i - (a_i+b_i)$ for all $i\in I$. Further, $\varphi_a = \mathrm{id}_{A[X_i \mid i\in I]}$ if and only if $a=0$. Therefore the map

$$(A^I, +) \longrightarrow \mathrm{Aut}_{A\text{-alg}}(A[X_i \mid i\in I]).$$

$a \longmapsto \varphi_a$ is an embedding (an injective group homomorphism) of the additive group $(A^I,+)$ in the multiplicative group $\mathrm{Aut}_{A\text{-alg}}(A[X_i \mid i\in I])$.

The automorphisms φ_a, $a\in A^I$ are called the <u>translation-automorphisms</u> of $A[X_i \mid i\in I]$ (with respect to the indeterminates X_i).

Further, $\varphi_a\left(\prod_{i\in I} X_i^{\nu_i}\right) = \prod_{i\in I}\varphi_a(X_i)^{\nu_i} = \prod_{i\in I}(X_i - a_i)^{\nu_i}$, therefore the monomials $(X-a)^\nu := \prod_{i\in I}(X_i - a_i)^{\nu_i}$, $\nu\in\mathbb{N}^{(I)}$ form a A-basis for the A-module $A[X_i \mid i\in I]$.

Therefore :

(<u>Taylor's expansion</u>) Let A be a commutative ring and let $a \in A^I$. Every polynomial $f \in A[X_i \mid i \in I]$ can be expressed uniquely in the form

$$f = \sum_{\nu \in \mathbb{N}^{(I)}} b_\nu (X-a)^\nu, \qquad b_\nu \in A$$

This representation is called the <u>Taylor's expansion of f at the point</u> $a \in A^I$.

The following proposition shows that a good understanding of the structure of the polynomial algebras over A is essential for the study of any A-algebra.

<u>**O.D.6 Proposition**</u> Let B be an Algebra over a commutative ring A. Then there exists a surjective A-algebra homomorphism $A[X_i \mid i \in I] \twoheadrightarrow B$, i.e. B is isomorphic to the quotient A-algebra $\dfrac{A[X_i \mid i \in I]}{\mathfrak{A}}$. Moreover, if B is a finitely generated A-algebra, then B is isomorphic to the quotient A-algebra of the polynomial algebra $A[X_1, \dots, X_n]$

<u>Proof</u> Let $x = (x_i)_{i \in I}$ be a set of generators for B as an A-algebra and let $\Phi_x : A[X_i \mid i \in I] \longrightarrow B$ be the subsitution homomorphism. Then the image of Φ_x is the smallest A-subalgebra $A[x_i \mid i \in I]$ of B containing x_i, $i \in I$ and hence Φ_x is surjective, since B is generated as an A-algebra by $\{x_i \mid i \in I\}$, i.e. $B = A[x_i \mid i \in I] = \operatorname{Im} \Phi_x$.