

is a basis of $A[X_1, \dots, X_n]$, since every polynomial $P(X_1, \dots, X_n)$ can be written in a unique way as

$$P(X_1, \dots, X_n) = \sum_{(k_1, \dots, k_n) \in \mathbb{N}^{(n)}} a_{(k_1, \dots, k_n)} X_1^{k_1} \cdots X_n^{k_n}.$$

Thus, $A[X_1, \dots, X_n]$ is a free module.

Remark: The construction of Definition 30.3 can be immediately extended to an arbitrary set I , and not just $I = \{1, \dots, n\}$. It can also be applied to monoids more general than $\mathbb{N}^{(I)}$.

Proposition 30.2 is generalized as follows.

Proposition 30.3. *Let A, B be two rings and let $h: A \rightarrow B$ be a ring homomorphism. For any $\beta = (\beta_1, \dots, \beta_n) \in B^n$, there is a unique ring homomorphism $\varphi: A[X_1, \dots, X_n] \rightarrow B$ extending h such that $\varphi(X_i) = \beta_i$, $1 \leq i \leq n$, as in the following diagram (where we denote by $h + \beta$ the map $h + \beta: A \cup \{X_1, \dots, X_n\} \rightarrow B$ such that $(h + \beta)(a) = h(a)$ for all $a \in A$ and $(h + \beta)(X_i) = \beta_i$, $1 \leq i \leq n$):*

$$\begin{array}{ccc} A \cup \{X_1, \dots, X_n\} & \xrightarrow{\iota} & A[X_1, \dots, X_n] \\ & \searrow h + \beta & \downarrow \varphi \\ & & B \end{array}$$

Proof. Let $\varphi(0) = 0$, and for every nonnull polynomial

$$P(X_1, \dots, X_n) = \sum_{(k_1, \dots, k_n) \in \mathbb{N}^{(n)}} a_{(k_1, \dots, k_n)} X_1^{k_1} \cdots X_n^{k_n},$$

let

$$\varphi(P(X_1, \dots, X_n)) = \sum h(a_{(k_1, \dots, k_n)}) \beta_1^{k_1} \cdots \beta_n^{k_n}.$$

It is easily verified that φ is the unique homomorphism $\varphi: A[X_1, \dots, X_n] \rightarrow B$ extending h such that $\varphi(X_i) = \beta_i$. \square

Taking $A = B$ in Proposition 30.3 and $h: A \rightarrow A$ the identity, for every $\beta_1, \dots, \beta_n \in A$, there is a unique homomorphism $\varphi: A[X_1, \dots, X_n] \rightarrow A$ such that $\varphi(X_i) = \beta_i$, and for every polynomial $P(X_1, \dots, X_n)$, we write $\varphi(P(X_1, \dots, X_n))$ as $P(\beta_1, \dots, \beta_n)$ and we call $P(\beta_1, \dots, \beta_n)$ the *value of $P(X_1, \dots, X_n)$ at $X_1 = \beta_1, \dots, X_n = \beta_n$* . Thus, we can define a function $P_A: A^n \rightarrow A$ such that $P_A(\beta_1, \dots, \beta_n) = P(\beta_1, \dots, \beta_n)$, for all $\beta_1, \dots, \beta_n \in A$. This function is called the *polynomial function induced by P* .

More generally, P_B can be defined for any (commutative) ring B such that $A \subseteq B$. As in the case of a single variable, it is possible that $P_A = Q_A$ for distinct polynomials P, Q . We will see shortly that the map $P \mapsto P_A$ is injective when $A = \mathbb{R}$ (in general, any infinite integral domain).