Formally, the definition of $\mathcal{P}_A(1)$ has nothing to do with X. The reason for using X is simply convenience. Indeed, it is more convenient to write a polynomial as $P = a_0 + a_1X + \cdots + a_nX^n$ rather than as $P = a_0e_0 + a_1e_1 + \cdots + a_ne_n$.

We have the following simple but crucial proposition.

Proposition 30.1. *Given two nonnull polynomials $P(X) = a_0 + a_1X + \cdots + a_mX^m$ of degree m and $Q(X) = b_0 + b_1X + \cdots + b_nX^n$ of degree n, if either a_m or b_n is not a zero divisor, then $a_mb_n \neq 0$, and thus, $PQ \neq 0$ and*

$$\deg(PQ) = \deg(P) + \deg(Q).$$

In particular, if A is an integral domain, then $A[X]$ is an integral domain.

Proof. Since the coefficient of X^{m+n} in PQ is a_mb_n, and since we assumed that either a_m or a_n is not a zero divisor, we have $a_mb_n \neq 0$, and thus, $PQ \neq 0$ and

$$\deg(PQ) = \deg(P) + \deg(Q).$$

Then, it is obvious that $A[X]$ is an integral domain. $\square$

It is easily verified that $A[X]$ is a commutative ring, with multiplicative identity $1X^0 = 1$. It is also easily verified that $A[X]$ satisfies all the conditions of Definition 3.1, but $A[X]$ is not a vector space, since A is not necessarily a field.

A structure satisfying the axioms of Definition 3.1 when K is a ring (and not necessarily a field) is called a *module*. Modules fail to have some of the nice properties that vector spaces have, and thus, they are harder to study. For example, there are modules that do not have a basis. We postpone the study of modules until Chapter 35.

However, when the ring A is a field, $A[X]$ is a vector space. But even when A is just a ring, the family of polynomials $(X^k)_{k\in\mathbb{N}}$ is a basis of $A[X]$, since every polynomial $P(X)$ can be written in a unique way as $P(X) = a_0 + a_1X + \cdots + a_nX^n$ (with $P(X) = 0$ when $P(X)$ is the null polynomial). Thus, $A[X]$ is a free module.

Next, we want to define the notion of evaluating a polynomial $P(X)$ at some $\alpha \in A$. For this, we need a proposition.

Proposition 30.2. *Let A, B be two rings and let $h\colon A \to B$ be a ring homomorphism. For any $\beta \in B$, there is a unique ring homomorphism $\varphi\colon A[X] \to B$ extending h such that $\varphi(X) = \beta$, as in the following diagram (where we denote by $h+\beta$ the map $h+\beta\colon A\cup\{X\} \to B$ such that $(h+\beta)(a) = h(a)$ for all $a \in A$ and $(h+\beta)(X) = \beta$):*

$$\begin{tikzcd} A \cup \{X\} \arrow[r, "\iota"] \arrow[dr, "h+\beta"'] & A[X] \arrow[d, "\varphi"] \\ & B \end{tikzcd}$$