Given any nonnull polynomial $P(X_1, \ldots, X_n) = \sum_{(k_1,\ldots,k_n)\in\mathbb{N}^{(n)}} a_{(k_1,\ldots,k_n)} X_1^{k_1} \cdots X_n^{k_n}$ in $A[X_1, \ldots, X_n]$, where $n \geq 2$, $P(X_1, \ldots, X_n)$ can be uniquely written as

$$P(X_1, \ldots, X_n) = \sum Q_{k_n}(X_1, \ldots, X_{n-1}) X_n^{k_n},$$

where each polynomial $Q_{k_n}(X_1, \ldots, X_{n-1})$ is in $A[X_1, \ldots, X_{n-1}]$. Even if A is a field, $A[X_1, \ldots, X_{n-1}]$ is not a field, which confirms that it is useful (and necessary!) to consider polynomials over rings that are not necessarily fields.

It is not difficult to show that $A[X_1, \ldots, X_n]$ and $A[X_1, \ldots, X_{n-1}][X_n]$ are isomorphic rings. This way, it is often possible to prove properties of polynomials in several variables $X_1, \ldots, X_n$, by induction on the number n of variables. For example, given two nonnull polynomials $P(X_1, \ldots, X_n)$ of total degree p and $Q(X_1, \ldots, X_n)$ of total degree q, since we assumed that A is an integral domain, we can prove that

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

and that $A[X_1, \ldots, X_n]$ is an integral domain.

Next, we will consider the division of polynomials (in one variable).

30.3 Euclidean Division of Polynomials

We know that every natural number $n \geq 2$ can be written uniquely as a product of powers of prime numbers and that prime numbers play a very important role in arithmetic. It would be nice if every polynomial could be expressed (uniquely) as a product of "irreducible" factors. This is indeed the case for polynomials over a field. The fact that there is a division algorithm for the natural numbers is essential for obtaining many of the arithmetical properties of the natural numbers. As we shall see next, there is also a division algorithm for polynomials in $A[X]$, when A is a field.

Proposition 30.4. *Let A be a ring, let $f(X), g(X) \in A[X]$ be two polynomials of degree $m = \deg(f)$ and $n = \deg(g)$ with $f(X) \neq 0$, and assume that the leading coefficient a_m of $f(X)$ is invertible. Then, there exist unique polynomials $q(X)$ and $r(X)$ in $A[X]$ such that*

$$g = fq + r \quad \textit{and} \quad \deg(r) < \deg(f) = m.$$

Proof. We first prove the existence of q and r. Let

$$f = a_m X^m + a_{m-1} X^{m-1} + \cdots + a_0,$$

and

$$g = b_n X^n + b_{n-1} X^{n-1} + \cdots + b_0.$$

If $n < m$, then let $q = 0$ and $r = g$. Since $\deg(g) < \deg(f)$ and $r = g$, we have $\deg(r) < \deg(f)$.