

where  $g_1 \in A[X]$  and  $g_1(\alpha_i) \neq 0$ , for  $1 \leq i \leq m-1$ . Since  $A$  is an integral domain and  $\alpha_i \neq \alpha_j$  for  $i \neq j$ , since  $\alpha_m$  is a root of  $f$ , we have

$$0 = (\alpha_m - \alpha_1)^{k_1} \cdots (\alpha_m - \alpha_{m-1})^{k_{m-1}} g_1(\alpha_m),$$

which implies that  $g_1(\alpha_m) = 0$ . Now, by Proposition 30.21 (2), since  $\alpha_m$  is not a root of the polynomial  $(X - \alpha_1)^{k_1} \cdots (X - \alpha_{m-1})^{k_{m-1}}$  and since  $A$  is an integral domain,  $\alpha_m$  must be a root of multiplicity  $k_m$  of  $g_1$ , which means that

$$g_1(X) = (X - \alpha_m)^{k_m} g(X),$$

with  $g(\alpha_m) \neq 0$ . Since  $g_1(\alpha_i) \neq 0$  for  $1 \leq i \leq m-1$  and  $A$  is an integral domain, we must also have  $g(\alpha_i) \neq 0$ , for  $1 \leq i \leq m-1$ . Thus, we have

$$f(X) = (X - \alpha_1)^{k_1} \cdots (X - \alpha_m)^{k_m} g(X),$$

where  $g \in A[X]$ , and  $g(\alpha_i) \neq 0$  for  $1 \leq i \leq m$ . □

As a consequence of Proposition 30.22, we get the following important result.

**Theorem 30.23.** *Let  $A$  be an integral domain. For every nonnull polynomial  $f \in A[X]$ , if the degree of  $f$  is  $n = \deg(f)$  and  $k_1, \dots, k_m$  are the multiplicities of all the distinct roots of  $f$  (where  $m \geq 0$ ), then  $k_1 + \cdots + k_m \leq n$ .*

*Proof.* Immediate from Proposition 30.22. □

Since fields are integral domains, Theorem 30.23 holds for nonnull polynomials over fields and in particular, for  $\mathbb{R}$  and  $\mathbb{C}$ . An important consequence of Theorem 30.23 is the following.

**Proposition 30.24.** *Let  $A$  be an integral domain. For any two polynomials  $f, g \in A[X]$ , if  $\deg(f) \leq n$ ,  $\deg(g) \leq n$ , and if there are  $n+1$  distinct elements  $\alpha_1, \alpha_2, \dots, \alpha_{n+1} \in A$  (with  $\alpha_i \neq \alpha_j$  for  $i \neq j$ ) such that  $f(\alpha_i) = g(\alpha_i)$  for all  $i$ ,  $1 \leq i \leq n+1$ , then  $f = g$ .*

*Proof.* Assume  $f \neq g$ , then,  $(f - g)$  is nonnull, and since  $f(\alpha_i) = g(\alpha_i)$  for all  $i$ ,  $1 \leq i \leq n+1$ , the polynomial  $(f - g)$  has  $n+1$  distinct roots. Thus,  $(f - g)$  has  $n+1$  distinct roots and is of degree at most  $n$ , which contradicts Theorem 30.23. □

Proposition 30.24 is often used to show that polynomials coincide. We will use it to show some interpolation formulae due to Lagrange and Hermite. But first, we characterize the multiplicity of a root of a polynomial. For this, we need the notion of derivative familiar in analysis. Actually, we can simply define this notion algebraically.

First, we need to rule out some undesirable behaviors. Given a field  $K$ , as we saw in Example 2.8, we can define a homomorphism  $\chi: \mathbb{Z} \rightarrow K$  given by

$$\chi(n) = n \cdot 1,$$