where 1 is the multiplicative identity of K. Recall that we define $n \cdot a$ by

$$n \cdot a = \underbrace{a + \cdots + a}_{n}$$

if $n \geq 0$ (with $0 \cdot a = 0$) and

$$n \cdot a = -(-n) \cdot a$$

if $n < 0$. We say that the field K is of *characteristic zero* if the homomorphism χ is injective. Then, for any $a \in K$ with $a \neq 0$, we have $n \cdot a \neq 0$ for all $n \neq 0$

The fields $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are of characteristic zero. In fact, it is easy to see that every field of characteristic zero contains a subfield isomorphic to $\mathbb{Q}$. Thus, finite fields can't be of characteristic zero.

Remark: If a field is not of characteristic zero, it is not hard to show that its characteristic, that is, the smallest $n \geq 2$ such that $n \cdot 1 = 0$, is a prime number p. The characteristic p of K is the generator of the principal ideal $p\mathbb{Z}$, the kernel of the homomorphism $\chi\colon \mathbb{Z} \to K$. Thus, every finite field is of characteristic some prime p. Infinite fields of nonzero characteristic also exist.

Definition 30.13. Let A be a ring. The *derivative f', or $\mathrm{D}f$, or $\mathrm{D}^1 f$, of a polynomial* $f \in A[X]$ is defined inductively as follows:

$$\begin{aligned}
f' &= 0, \quad \text{if } f = 0, \text{ the null polynomial,} \\
f' &= 0, \quad \text{if } f = a,\ a \neq 0,\ a \in A, \\
f' &= na_n X^{n-1} + (n-1)a_{n-1}X^{n-2} + \cdots + 2a_2 X + a_1, \\
&\qquad \text{if } f = a_n X^n + a_{n-1}X^{n-1} + \cdots + a_0,\ \text{ with } n = \deg(f) \geq 1.
\end{aligned}$$

If $A = K$ is a field of characteristic zero, if $\deg(f) \geq 1$, the leading coefficient na_n of f' is nonzero, and thus, f' is not the null polynomial. Thus, if $A = K$ is a field of characteristic zero, when $n = \deg(f) \geq 1$, we have $\deg(f') = n - 1$.

For rings or for fields of characteristic $p \geq 2$, we could have $f' = 0$, for a polynomial f of degree ≥ 1.

The following standard properties of derivatives are recalled without proof (prove them as an exercise).

Given any two polynomials, $f, g \in A[X]$, we have

$$\begin{aligned}
(f+g)' &= f' + g', \\
(fg)' &= f'g + fg'.
\end{aligned}$$

For example, if $f = (X - \alpha)^k g$ and $k \geq 1$, we have

$$f' = k(X-\alpha)^{k-1}g + (X-\alpha)^k g'.$$

We can now give a criterion for the existence of simple roots. The first proposition holds for any ring.