Adjunction of a root of a polynomial

PROPOSITION. *Let R be a commutative ring and $f \in R[X]$ a monic polynomial of degree $n > 0$:*

$$f = X^n + r_1 X^{n-1} + r_2 X^{n-2} + \cdots + r_{n-1} X + r_n \quad (r_i \in R).$$

Then there exists an R-algebra T and a root $t \in T$ of f (i.e., $f(t) = 0$) such that for any (U, u) with U an R-algebra and $u \in U$ a root of f there is a unique R-homomorphism (i.e., R-algebra homomorphism) $\theta\colon T \to U$ with $\theta(t) = u$.

Moreover, the structure map $\alpha\colon R \to T$ is injective, and every element of T is uniquely of the form

$$a_0 + a_1 t + \cdots + a_{n-1} t^{n-1} \ (a_i \in R).$$

Proof. With (f) the $R[X]$-ideal generated by f, set $T := R[X]/(f)$—an R-algebra via the natural composition $\alpha\colon R \to R[X] \xrightarrow{\pi} T$—and $t := \pi(X)$. Then $f(t) = \pi f = 0$. Given (U, u) as above, there is a unique R-homomorphism $\phi\colon R[X] \to U$ with $\phi(X) = u$. Then f is in the kernel of ϕ (as $\phi(f) = f(u) = 0$); and hence there is a unique homomorphism $\theta\colon T \to U$ such that $\theta \circ \pi = \phi$. This θ has the asserted properties.

The kernel of α is $(f) \cap R$, which is clearly (0) (since any nonzero multiple of f has degree $\geq n$).

Every element $z \in T$ is of the form $g(t) = \pi g$ for some $g \in R[X]$. Then $z = a_0 + a_1 t + \cdots + a_{n-1} t^{n-1} =: h(t)$ iff $g \equiv h \pmod f$, i.e., $g = qf + h$ for some $q \in R[X]$. There can only be one such h of degree $< n$, since the difference of any two would be a polynomial of degree $< n$ divisible by f, hence 0. Thus z is uniquely of the indicated form. Q.E.D.

Remarks. (a) The universal property of the pair (T, t) characterizes it up to canonical isomorphism. This property can be thought of as saying that "t is the mother of all roots of f."

(b) Since α is injective, a standard argument shows that there is an R-algebra S isomorphic to T and containing R (the structure map $R \to S$ being the inclusion).

(c) If R is a field then T is an n-dimensional vector space, with basis $(1, t, t^2, \ldots, t^{n-1})$.

COROLLARY. *There exists a ring S containing R such that in $S[X]$, f factors as*

$$f = (X - s_1)(X - s_2) \cdots (X - s_n),$$

and $S = R[s_1, \ldots s_n]$ (i.e., the R-subalgebra of S generated by the s_i is S itself).

Proof. Proceed by induction on n, the case $n = 1$ being trivial. With $T \supset R$ and $s_n := t$ as above, since the remainder $f(s_n)$ when f is divided by $X - s_n$ vanishes, therefore in $T[X]$ we have a factorization $f = f_1(s - x_n)$, where f_1 has degree $n - 1$. By the inductive hypothesis, there is a ring $S \supset T$ such that in $S[X]$, $f_1 = (X - s_1) \cdots (X - x_{n-1})$, whence the desired conclusion.