Roots of Irreducible Polynomials

In this series of exercises we will prove the following. This is a stronger version of the corollary to Theorem 20.9.

Theorem 1. *Let F be a field of characteristic $p > 0$, $f(x) \in F[x]$ an irreducible polynomial. If E is a splitting field for $f(x)$ over F and $a_1, a_2, \ldots, a_m$ are the (distinct) roots of $f(x)$ in E, then there is an integer $n \geq 0$ so that*

$$f(x) = c(x - a_1)^{p^n}(x - a_2)^{p^n} \cdots (x - a_m)^{p^n}.$$

for some $c \in F$. In particular, all the zeros of $f(x)$ have the same multiplicity.

Throughout what follows, F is a field of characteristic $p > 0$, $f(x) \in F[x]$ is an irreducible polynomial, and E is a splitting field for $f(x)$ over F.

Exercise 1. Prove that there exists an integer $n \geq 0$ and an irreducible polynomial $g(x) \in F[x]$, all of whose roots have multiplicity 1, so that $f(x) = g(x^{p^n})$. [*Suggestion 1:* If $f(x)$ has multiple roots, repeatedly apply Theorem 20.6. *Suggestion 2:* Let $n \geq 0$ be the largest integer so that p^n divides all the exponents of the powers of x appearing in $f(x)$.]

Exercise 2. Let $g(x)$ be the polynomial of exercise 1 and let K be an extension of E containing the distinct roots $b_1, b_2, \ldots, b_m$ of $g(x)$.

a. Show that
$$f(x) = c(x^{p^n} - b_1)(x^{p^n} - b_2) \cdots (x^{p^n} - b_m)$$
for some $c \in F$.

b. Let $a \in E$ be a root of $f(x)$. Show that $a^{p^n} = b_i$ for some i.

c. Show that $f(x)$ has exactly m distinct roots in E.

Exercise 3. Let $a_1, a_2, \ldots, a_m \in E$ be the distinct roots of $f(x)$. Show that

$$f(x) = c(x - a_1)^{p^n}(x - a_2)^{p^n} \cdots (x - a_m)^{p^n},$$

completing the proof of the theorem.