Seperable polynomials and extensions

Definitions

- A polynomial is *separable* if it has no multiple roots in the splitting filed.
- An extension $L : K$ is *seperable* if the minimal polynomial over K of any element in L is separable.
- A field K is called *perfect* if every irreducible polynomial over K is separable.

(We didn't have time to go over the following exercises. They will be on the homework.)

1. Prove that an irreducible polynomial whose derivative is not zero is separable.
2. Let K be a field of characteristic p (prime). Let $f(x) \in K[x]$ be a polynomial whose derivative is the zero polynomial.
   (a) Prove that $f(x)$ can be written as $f(x) = a_0 + a_1 x^p + \cdots + a_n x^{np}$ for $a_0, \ldots, a_n \in K$.
   (b) Prove that if K is finite, then $f(x) = (g(x))^p$ for some $g(x) \in K[x]$.
3. Prove that finite fields are perfect.
4. Give an example of a field that is not perfect.
5. (Primitive elements) Let $K = \mathbb{Z}_p(x, y)$ and $L = K[a, b]/\langle a^p - x, b^p - y \rangle$.
   (a) Show that L is a field and that $[L : K] = p^2$.
   (b) Show that for any element $\alpha \in L$, $\alpha^p \in K$. It follows that $L \neq K(\alpha)$ for any $\alpha \in L$.

We've proven the following last week:
Lemma Let $\sigma : K \to K'$ be an isomorphism of fields that sends a separable polynomial $f(x) \in K[x]$ to $f'(x) \in K'[x]$. Let L and L' be splitting fields of $f(x)$ and $f'(x)$ over K and K' respectively. Then there are exactly $[L : K]$ ways to extend σ to an isomorphism $L \to L'$.

Theorem 1 Let L be the splitting field of a polynomial $f(x)$ over K. Then for every $\alpha \in L$, its minimal polynomial $p(x)$ splits over L.

Proof. Suppose not. Let α' be another root of $p(x)$ in some field extension. Then there is an isomorphism $\varphi : K(\alpha) \to K(\alpha')$ fixing K because

The field $L(\alpha')$ is the splitting field of ____________over ____________.
By the Lemma bove, φ can be extended to an isomorphism $L \to L(\alpha')$. Complete the proof:

Theorem 2 Let L be the splitting field of a **separable** polynomial $f(x)$ over K (i.e. $L : K$ is Galois). Then for every $\alpha \in L$, its minimal polynomial $p(x)$ is separable.

Proof. Let $B = \{\sigma(\alpha) \mid \sigma \in \mathrm{Gal}(L : K)\}$ and consider $q(x) = \prod_{\beta \in B}(x - \beta)$. Compelete the proof: