

Theorem 1. *Let E be a finite extension of a field F with prime characteristic $p > 0$. Then E is separable over F iff $E = F(E^p)$.¹*

Proof. Assume first that E is separable over F and let $a \in E$. Then $\mu_{a|F}$ is separable. Let $g = \mu_{a|F(a^p)}$. Clearly then $g|\mu_{a|F}$ in $F(a^p)$, so f is separable. Consider the polynomial $x^p - a^p \in F(a^p)[x]$. By Lemma 3.4.9 a, $x^p - a^p = (x - a)^p$. Then since g is separable, we conclude that $g = x - a$, and hence $a \in F(a^p) \subset F(E^p)$. Conclude $E \subset F(E^p)$. Since $F(E^p) \subset E$, we have equality, i.e., $E = F(E^p)$.

Conversely, assume that $E = F(E^p)$, and let $a \in E$. Wish to show that $f = \mu_{a|F}$ is separable. Suppose f is inseparable. Then by Corollary 3.4.6 c, $f = g(x^p)$ for some $g \in F[x]$. Write $g = \sum_{i=0}^k c_i x^i$. Since $\sum_{i=0}^k c_i a^{pi} = 0$, the field elements $1, a^p, \dots, a^{kp}$ are linearly dependent over F . On the other hand, $k < kp = \deg(f) = [F(a) : F]$, so that the field elements $1, a, \dots, a^k$ must be linearly independent over F . Extend the set $\{1, a, \dots, a^k\}$ to an F -basis of E , say $\{y_1, \dots, y_n\}$, with $y_i = a^i$ for $0 \leq i \leq k$ and $n = [E : F]$. Now $E = Fy_1 + Fy_2 + \dots + Fy_n$. Then by Lemma 3.4.9 a, $E^p \subset Fy_1^p + Fy_2^p + \dots + Fy_n^p$. Therefore $E = F(E^p) = Fy_1^p + Fy_2^p + \dots + Fy_n^p$. Then the n elements y_1^p, \dots, y_n^p span $E \Rightarrow$ the n elements y_1^p, \dots, y_n^p form a basis for E since $n = [E : F]$. Now we conclude that $y_1^p, \dots, y_n^p = 1, a^p, \dots, a^{kp}$ are linearly independent over F , a contradiction. Hence $f = \mu_{a|F}$ must be separable, and $E|F$ is a separable extension. \square

Corollary 1 (Remark 3.4.15 a). *Let F be a field of characteristic $p > 0$. If a_i is separable over K for each $1 \leq i \leq n$, then $E = F(a_1, \dots, a_n)$ is separable over F .²*

Proof. Since a_i is separable over F , we have that $a_i \in F(a_i^p)$ as in the first paragraph of the preceding proof. Then $a_i \in F(E^p)$ and $E = F(a_1, \dots, a_n) = F(a_1^p, \dots, a_n^p) \subset F(E^p)$. Hence $E = F(E^p)$, and $E|F$ is separable by the previous theorem. \square

Corollary 2. *Let K be a field of characteristic $p > 0$, and let $M|L$ and $L|K$ be field extensions of finite degrees. Suppose that $M|L$ is separable and $L|K$ is separable. Then $M|K$ is separable.³*

Proof. By the above theorem, we have that $M = L(M^p)$ and $L = K(L^p)$. Clearly $K(M^p) \subset M$. But also $M = L(M^p) = K(L^p)(M^p) = K(M^p)$ since $L^p \subset M^p$. Then $M = K(M^p)$, so $M|K$ is separable by the above theorem. \square

Corollary 3 (Remark 3.4.15 b). *Let $M|L$ and $L|K$ be algebraic field extensions. Suppose that $M|L$ and $L|K$ are each separable. Then $M|K$ is separable.*

Proof. Let $a \in M$. We wish to show that a is separable over K . Write $\mu_{a|L} = \sum_{i=0}^n c_i x^i$, $c_i \in L$. By assumption, $\mu_{a|L}$ is separable. Consider the field $F = K(c_1, \dots, c_n)$. Then $\mu_{a|F} = \mu_{a|L}$, so a is separable over F . But $L|K$ separable $\Rightarrow c_i$ is separable over K for each $1 \leq i \leq n \Rightarrow F|K$ is separable by Corollary 1. Then $F(a)|K$ is separable by Corollary 2. In particular, a is separable over K . Conclude that $M|K$ is separable. \square

¹Theorem and Proof from *An Introduction to Abstract Algebra* by Derek J.S. Robinson, Page 211-212.

²Robinson, Page 212.

³Robinson, Page 213, Exercise 11.1.6