$$\sum y_\alpha M_\alpha(x) = 0$$

between monomials $M_\alpha(x)$ with coefficients $y_\alpha \in L$. This gives a linear relation among the $M_\alpha(x)$. But these are linearly independent over F because the x's are assumed algebraically independent over F. This is a contradiction.

PROPOSITION. Let L be an extension of F, and let $(u)=(u_1,\dots,u_r)$ be a set of quantities algebraically independent over L. Then the field $F(u)$ is linearly disjoint from L over F.

PROOF. According to the criteria for linear disjointness, it suffices to prove that the elements of a basis for the ring $F[u]$ that are linearly independent over F remains so over L. In fact the monomials $M(u)$ give a basis of $F[u]$ over F. They must remain linearly independent over L, because as we have seen, a linear relation gives an algebraic relation.

SEPARABLE AND REGULAR EXTENSIONS

Let K be a finitely generated extension of F. We shall say that it is <u>separably generated</u> over F if we can find a transcendence base $\{t_1,\dots,t_r\}$ of K/F such that K is a separable algebraic extension of $F(t_1,\dots,t_r)$. Such a transcendence base is called a <u>separating transcendence base</u> for K over F.

Let $E = F(x)$, x transcendental over F, $\operatorname{char} F = p \neq 0$. Let $\mathcal{B} = \{x^p\}$. We know that $\text{tr.d. } E/F = 1$, and so $\{x^p\}$ is a transcendence base of E/F. However; E is not separable over $F(x^p)$ since the polynomial $X^p - x^p \in F(x^p)[X]$ has all roots equal (to x). This example shows that even if E is separably generated over F, not every transcendence base $\mathcal{B}$ has the property that E is separable algebraic over $F(\mathcal{B})$.

Let F be a field of characteristic $p \neq 0$, and K an extension of F. We embed K into its algebraic closure $\bar{K}$. If m is a positive integer, then we denote the subset of $\bar{K}$ of elements u such that $u^{p^m} \in F$ by F^{1/p^m}. It can be readily checked that F^{1/p^m} is a subfield of $\bar{K}$ containing F for every $m > 0$, and that we have an ascending chain

$$F^{1/p} \subseteq F^{1/p^2} \subseteq \dots \subseteq F^{1/p^m} \subseteq \dots$$

of subfields. Indeed, F^{1/p^m} is the splitting field of $\{x^{p^m} - a : a \in F\}$ over F. We also set $F^{1/p^\infty} := \bigcup_{m>0} F^{1/p^m}$, the smallest subfield of $\bar{K}$ (and also $\bar{F}$, indeed) containing all the F^{1/p^m}'s. It is easy to see that K is linearly disjoint from F^{1/p^∞} if and only if it is linearly disjoint from F^{1/p^m} for all $m > 0$.

LEMMA. If E/F is separable algebraic where F has characteristic $p \neq 0$, then E and F^{1/p^∞} are linearly disjoint.

PROOF. It suffices to show that if $a_1, \dots, a_k$ are F-linearly independent elements of E, then these are linearly independent over F^{1/p^m} for every $m > 0$. This is equivalent to the following:

$a_1^{p^m}, \ldots, a_k^{p^m}$ are F-independent. Let $L = F[a_1, \ldots, a_k]$. Since $a_1, \ldots, a_k$ are all algebraic over F, $[L:F] < \infty$. Say $[L:F] = n$. Since $a_1, \ldots, a_k$ are F-linearly independent, they can be extended to a basis for L/F. Let $\{x_1, \ldots, x_n\}$ be a basis of L/F such that $x_i = a_i$ for all $1 \le i \le k \le n$. Write

$$x_i x_j = \sum_{t=1}^{n} c_{ijt} x_t$$

where $c_{ijt} \in F$. Then

$$y_i y_j = \sum_{t=1}^{n} d_{ijt} y_t$$

for $y_i = x_i^{p^m}$, $d_{ijt} = c_{ijt}^{p^m}$. The multiplication table for the y_i shows that $\sum_{i=1}^{n} F y_i$ is an F-algebra. Now let $a \in L$ and write $a = \sum_{i=1}^{n} a_i x_i$, $a_i \in F$. Then $a^{p^m} = \sum_{i=1}^{n} a_i^{p^m} y_i \in \sum_{i=1}^{n} F y_i$. Since $F(a)$ is separable over F, we have $a \in F(a) = F(a)^{p^m} \cap F = F(a^{p^m}) = F[a^{p^m}] \subseteq \sum_{i=1}^{n} F y_i$. So the y_i generate L as vector space over F. Since the number of y_i is $n = [L:F]$, these form a base for L/F. It follows that $y_1 = x_1^{p^m} = a_1^{p^m}, \ldots, y_k = x_k^{p^m} = a_k^{p^m}$ are F-independent. This completes the proof. ∎

Let E/F be an extension of fields. E is called purely transcendental over F if it has a transcendence base $\mathcal{B}$ such that $E = F(\mathcal{B})$.

LEMMA. If E is purely transcendental over F (char $F = p \neq 0$), then E and F^{1/p^∞} are linearly disjoint over F.

PROOF. It suffices to prove the result for $E=F(x_1,\dots,x_n)$ where the x_i are algebraically independent. Moreover; the result will follow if we can show that a base for $F[x_1,\dots,x_n]$ over F remains linearly independent over F^{1/p^m} for every $m>0$. We have a base for $F[x_1,\dots,x_n]/F$ consisting of all monomials $x_1^{k_1}\dots x_n^{k_n}$, $k_i\geq 0$. Let $\{m_\alpha\}$ be the base of monomials. Then the set $\{m_\alpha^{p^m}\}$ is linearly independent as $\{m_\alpha^{p^m}\}\subseteq\{m_\alpha\}$. It follows that $\{m_\alpha\}$ is linearly independent over F^{1/p^m}. ∎

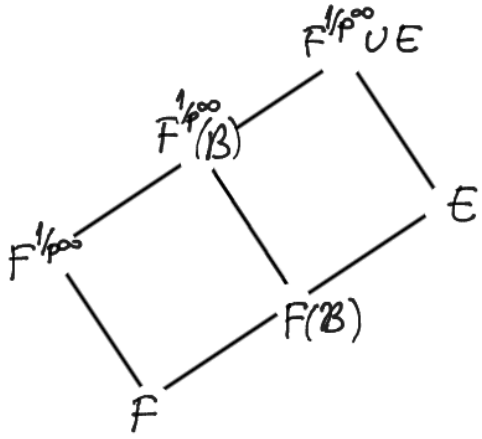
THEOREM. Let E be an extension field of a field F of characteristic $p\neq 0$. Then the following properties of E/F are equivalent:

(1) Every finitely generated subfield of E/F is separably generated.

(2) E and F^{1/p^∞} are linearly disjoint over F.

(3) E and $F^{1/p}$ are linearly disjoint over F.

PROOF. (1) $\Rightarrow$ (2): Let $\mathfrak{B}$ be a transcendence base of E/F and let E be separable algebraic over $F(\mathfrak{B})$. By above lemma, F^{1/p^∞} and $F(\mathfrak{B})$ are linearly disjoint over F. On the other hand, E and $F(\mathfrak{B})^{1/p^\infty}$ are linearly disjoint over $F(\mathfrak{B})$. Since $F(\mathfrak{B})^{1/p^\infty}\geq F^{1/p^\infty}(\mathfrak{B})\supseteq F(\mathfrak{B})$, it follows that $F^{1/p^\infty}(\mathfrak{B})$ and E are linearly disjoint over $F(\mathfrak{B})$. Now consider the following diagram.



Therefore, F^{1/p^∞} and E are linearly disjoint over F.

(2) $\Rightarrow$ (3) : Obvious.

(3) $\Rightarrow$ (1) : Assume that E and $F^{1/p}$ are linearly disjoint over F and let $K = F(a_1, \ldots, a_n)$ be a finitely generated subfield of E/F. We prove by induction on n that we can extract from the given set of generated of generators a transcendence base $a_{i_1}, \ldots, a_{i_r}$ (where r is 0 if all the a_i are algebraic over F) such that K is separable algebraic over $F(a_{i_1}, \ldots, a_{i_r})$. The result is clear if $n=0$, so we assume $n>0$. The result is clear also if $a_1, \ldots, a_n$ are algebraically independent. Hence we assume that $a_1, \ldots, a_r$, $0 \leq r < n$, is a transcendence base for K/F. Then $a_1, \ldots, a_{r+1}$ are algebraically dependent over F, so we can choose a polynomial $f(x_1, \ldots, x_{r+1}) \in F[x_1, \ldots, x_{r+1}] - \{0_F\}$ of least degree such that $f(a_1, \ldots, a_{r+1}) = 0$. Then $f(x_1, \ldots, x_{r+1})$ is irreducible. We claim that f does not have the form $g(x_1^p, \ldots, x_{r+1}^p)$, $g \in F[x_1, \ldots, x_r]$. For $g(x_1^p, \ldots, x_{r+1}^p) = h(x_1, \ldots, x_{r+1})^p$ in $F^{1/p}[x_1, \ldots, x_{r+1}]$ and if $f(x_1, \ldots, x_{r+1}) = g(x_1^p, \ldots, x_{r+1}^p)$, then $h(a_1, \ldots, a_{r+1}) = 0$. Let $m_i(x_1, \ldots, x_{r+1})$, $1 \leq i \leq u$, be the monomials occuring in h. Then the elements $m_i(a_1, \ldots, a_{r+1})$ are linearly depen-

dent over $F^{1/p}$, so by our hypothesis, these are linearly dependent over F. This gives a non-trivial polynomial relation in $a_1, \ldots, a_{r+1}$ with coefficients in F of lower degree than f, contrary to the choice of f. We have therefore shown that for some i, $1 \le i \le r+1$, $f(x_1, \ldots, x_{r+1})$ is not a polynomial in x_i^p (and the other x's). Then a_i is algebraic over $F(a_1, \ldots, \hat{a}_i, \ldots, a_{r+1})$ where $\hat{a}_i$ denotes omission of a_i. This shows that $F(a_1, \ldots, a_{r+1})$ is algebraic over $F(a_1, \ldots, \hat{a}_i, \ldots, a_{r+1})$. Since $\{a_1, \ldots, a_r\}$ is a transcendence base for $F(a_1, \ldots, a_n)$, we also have $F(a_1, \ldots, a_n)$ is algebraic over $F(a_1, \ldots, a_{r+1})$. By transitivity property of being algebraic, $F(a_1, \ldots, a_n)$ is algebraic over $F(a_1, \ldots, \hat{a}_i, \ldots, a_{r+1})$, and hence $\{a_1, \ldots, \hat{a}_i, \ldots, a_{r+1}\}$ is a transcendence base for $F(a_1, \ldots, a_n)$. Then $F[a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_{r+1}] \cong F[x_1, \ldots, x_{r+1}]$ in the obvious way and so $f(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_{r+1})$ is irreducible in $F[a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_{r+1}]$. Then this polynomial is irreducible in $F(a_1, \ldots, \hat{a}_i, \ldots, a_{r+1})[x]$. Since a_i is a root of $f(a_1, \ldots, a_{i-1}, x, a_{i+1}, \ldots, a_{r+1})$ and this is not a polynomial in x^p, we see that a_i is separable over $F(a_1, \ldots, \hat{a}_i, \ldots, a_{r+1})$ and hence over $L = F(a_1, \ldots, \hat{a}_i, \ldots, a_n)$. The induction hypothesis applies to L and gives us a subset $\{a_{i_1}, \ldots, a_{i_r}\}$ of $\{a_1, \ldots, \hat{a}_i, \ldots, a_n\}$ that is a separating transcendence base for L over F. (Notice that tr. d. L/F = tr. d. $F(a_1, \ldots, a_n)/F$.) Since a_i is separable algebraic over L, it follows that a_i is

separable algebraic over $F(a_{i_1},\ldots,a_{i_r})$. Hence $\{a_{i_1},\ldots,a_{i_r}\}$ is a separating transcendence base for $F(a_1,\ldots,a_n)$. ☑

We remark that the result is applicable in particular to an algebraic extension E/F. In this case it states that if E and $F^{1/p}$ are linearly disjoint over F, then E is separable over F and if E is separable over F, then E and F^{1/p^∞} are linearly disjoint (which was given as a lemma above). This makes it natural to extend the concept of separability for arbitrary extension fields in the following manner.

DEFINITION. An extension field E/F is called separable if either the characteristic is 0 or the characteristic is $p\neq 0$, and the equivalent conditions of the above theorem hold.

COROLLARY. If F is perfect, then every extension E/F is separable.

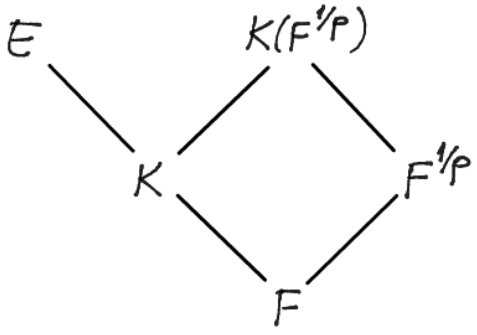
PROOF. This is clear since F is perfect if and only if $F^{1/p}=F$ where $\operatorname{char} F=p$. ☑

THEOREM. Let E be an extension field of F, K an intermediate field. Then (1) If E is separable over F, then K is separable over F. (2) If E is separable over K and K is separable

over F, then E is separable over F. (3) If E is separable over F, then E need not be separable over K. (4) If E is separable over F, it need not have a separating transcendence base over F.

PROOF. We may assume that the characteristic is $p \neq 0$.

(1) This is clear since the linear disjointness of E and $F^{1/p}$ over F implies that of K and $F^{1/p}$ over F. (2) The hypothesis is that E and $K^{1/p}$ are linearly disjoint over K and that K and $F^{1/p}$ are linearly disjoint over F. Then E and $K(F^{1/p})$ are linearly disjoint over K since $K(F^{1/p}) \subseteq K^{1/p}$.



By the diagram on the left, it can bee seen that E and $F^{1/p}$ are linearly disjoint over F and so E is separable over F.

(3) Take $E = F(x)$, x transcendental, and $K = F(x^p)$.

(4) Take $E = F(x, x^{1/p}, x^{1/p^2}, \ldots)$ where x is transcendental over F. Then E has transcendence degree one over F and E is not separably generated over F.

$\square$