TRANSCENDENTAL EXTENSIONS

Let E be an extension field of F. let S be a subset of E. By a function $\nu : S \to \mathbb{N}$ of finite support, we mean for all but a finite number of x, $\nu(x) = 0$. For a function $\nu : S \to \mathbb{N}$ of finite support, we set

$$M_{(\nu)}(S) := \prod_{x \in S} x^{\nu(x)}.$$

We denote the set of all functions $S \to \mathbb{N}$ of finite support by $\mathbb{N}^{(S)}$. S is said to be algebraically independent over F, if whenever we have a relation

$$0 = \sum_{\nu \in \mathbb{N}^{(S)}} a_{(\nu)} M_{(\nu)}(S)$$

with coefficients $a_{(\nu)} \in F$, almost all $a_{(\nu)} = 0$, then we must necessarily have all $a_{(\nu)} = 0$.

We can introduce an ordering among algebraically independent subset of E, by inclusion. These subsets are inductively ordered, and thus there exist maximal elements. A subset S of E which is algebraically independent over F and is maximal with respect to the inclusion will be called a transcendence base of E over F. Note that an algebraically independent subset S of E is a transcendence base of E over F if and only if E is algebraic over $F(S)$.

Algebraic independence may be viewed as an extension

of the concept of linear independence. For a set S is linearly dependent over F provided that for some positive integer n there is a nonzero polynomial f of degree one in $F[x_1,\ldots,x_n]$ such that $f(s_1,\ldots,s_n)=0$ for some distinct $s_i \in S$. Consequently, every algebraically independent set is also linearly independent, but not vice versa as the following example shows.

Example. If $f/g = f(x)/g(x) \in F(x)$ with $f, g \neq 0$, then the nonzero polynomial $h(y_1,y_2) = g(y_1)y_2 - f(y_1) \in F[y_1,y_2]$ is such that $h(x, f/g) = g(x)[f(x)/g(x)] - f(x) = 0$. Thus $\{x, f/g\}$ is algebraically dependent in $F(x)$ over F. This shows that $\{x\}$ is a transcendence base of $F(x)$ over F. The set $\{x\}$ is not a basis since $\{1_F, x, x^2, x^3, \ldots\}$ is linearly independent in $F(x)$.

THEOREM. Let E be an extension of a field F. Suppose there is a finite transcendence base of E over F. Then any two transcendence bases of E over F have the same cardinality.

PROOF. We shall prove that if there is one finite transcendence base, say $\{u_1,\ldots,u_n\}$, $n \geq 1$, n minimal, then any other transcendence base must also have n elements. For

this it will suffice to prove: If $w_1, \dots, w_n$ are elements of E which are algebraically independent over F, then $n \leq m$. Suppose on the contrary that $n > m$. By assumption, there exists a nonzero irreducible polynomial f_1 in $m+1$ variables with coefficients in F such that $f_1(w_1, u_1, \dots, u_m) = 0$. After renumbering $u_1, \dots, u_m$ we may write

$$f_1 = \sum g_j(w_1, u_2, \dots, u_n) u_1^j$$

with $g_N(w_1, u_2, \dots, u_n) \neq 0$ for some $N \geq 1$, otherwise w_1 would be algebraic over F, a contradiction. Thus u_1 is algebraic over $F(w_1, u_2, \dots, u_m)$. Also $w_1, u_2, \dots, u_m$ are algebraically independent over F since otherwise w_1 would be a root of two distinct irreducible polynomials over $F(u_1, \dots, u_m)$ one of which is known to be $f_1(X, u_1, \dots, u_m) \in F(u_1, \dots, u_m)[X]$. Since $\{u_1, \dots, u_m\}$ is a transcendence base of E over F, E is algebraic over $F(u_1, \dots, u_m)$. It follows that E is algebraic over $F(w_1, u_1, \dots, u_m)$ and $F(w_1, u_1, \dots, u_m)$ is algebraic over $F(w_1, u_2, \dots, u_m)$, which gives that E is algebraic over $F(w_1, u_2, \dots, u_m)$. Therefore $\{w_1, u_2, \dots, u_m\}$ is a trans. base of E over F. Suppose inductively that after a suitable renumbering of $u_2, \dots, u_m$ we have found $w_1, \dots, w_r$ $(r < n)$ such that $\{w_1, \dots, w_r, u_{r+1}, \dots, u_m\}$ is a trans. base of E over F. Then there exists a nonzero polynomial f in $m+1$ variables with coefficients in F such that

$$f(w_{r+1}, w_1, \ldots, w_r, u_{r+1}, \ldots, u_m) = 0.$$

Since the w's are algebraically independent over F, it follows by the same argument as in the first step that some u_j, say u_{r+1}, is algebraic over $F(w_1, \ldots, w_{r+1}, u_{r+2}, \ldots, u_m)$ and $w_1, \ldots, w_{r+1}, u_{r+2}, \ldots, u_m$ are algebraically independent over F. It follows that E is algebraic over $F(w_1, \ldots, w_{r+1}, u_{r+2}, \ldots, u_m)$, which shows that $\{w_1, \ldots, w_{r+1}, u_{r+2}, \ldots, u_m\}$ is a trans. base of E over F. We can repeat the procedure and replace all the u's by w's, to see that $\{w_1, \ldots, w_m\}$ is a transcendence base of E over F, which is a contradiction since $\{u_1, \ldots, u_m\} \subsetneq \{u_1, \ldots, u_n\}$ and $u_1, \ldots, u_n$ are algebraically independent. This completes the proof.

THEOREM. Let E be an extension field of F. If S is an infinite transcendence base of E over F, then every transcendental base of E over F has the same cardinality as S.

PROOF. If T is another transcendence base of E over F, then T must be finite by the above theorem. If $s \in S$, then s is algebraic over $F(T)$. The coefficients of the minimal polynomial f of s over $F(T)$ all lie in $F(T_s)$ for some finite subset T_s of T. Consequently, $f \in F[T_s][x]$ and s is algebraic over $F[T_s]$. Choose such a finite subset T_s of T for each $s \in S$.

We shall show that $\bigcup_{s\in S} T_s$ is a transcendence base of E over F. Since $\bigcup_{s\in S} T_s \subseteq T$, this will imply that $\bigcup_{s\in S} T_s = T$. As a subset of T, the set $\bigcup_s T_s$ is algebraically independent. Furthermore, any element of S is algebraic over $F(\bigcup_s T_s)$. Consequently, $F(\bigcup_s T_s)(S)$ is algebraic over $F(\bigcup_s T_s)$. Since $F(S) \subseteq F(\bigcup_s T_s)(S)$, every element of $F(S)$ is algebraic over $F(\bigcup_s T_s)$. Since E is algebraic over $F(S)$, E is also algebraic over $F(\bigcup_s T_s)$. Therefore, $\bigcup_s T_s$ is a trancendence base, whence $\bigcup_s T_s = T$.

Finally we shall show that $|T| \leq |S|$. The sets T_s need not be mutually disjoint and we remedy this as follows. Well order the set S and denote its first element by 1. Let $T_1' = T_1$ and for each $1 < s \in S$, define $T_s' = T_s - \bigcup_{i<s} T_i$. Clearly each T_s' is finite. Verify that $\bigcup_s T_s = \bigcup_s T_s'$ and that the T_s' are mutually disjoint. For each $s \in S$, if T_s' is non-empty, choose a fixed ordering of the elements of T_s': $t_1 < t_2 < \ldots < t_{k_s}$. The assignment $t_i \longmapsto (s,i)$ defines an injective map $\bigcup_s T_s' \longrightarrow S \times \mathbb{N}$. Therefore we have

$$|T| = |\bigcup_s T_s| = |\bigcup_s T_s'| \leq |S \times \mathbb{N}| = |S|\,|\mathbb{N}| = |S|\aleph_0 = |S|.$$

Reversing the roles of S and T in the preceding argument shows that $|S| \leq |T|$, whence $|S| = |T|$ by the Schroeder-Bernstein Theorem.

DEFINITION. Let E be an extension field of F. The transcendence degree of E over F (denoted $\text{tr.d. } E/F$) is the cardinal number $|S|$, where S is any transcendence base of E over F.

We remark that $\text{tr.d. } E/F \leq [E:F]$ and that $\text{tr.d. } E/F = 0$ if and only if E is algebraic over F.

THEOREM. If E is an extension field of F and K is an extension field of E, then

$$\text{tr.d. } K/F = (\text{tr.d. } K/E) + (\text{tr.d. } E/F).$$

PROOF. Let S be a transcendence base of E over F and T a transcendence base of K over E. Since $S \subseteq E$, S is algebraically dependent over E and so $S \cap T = \phi$. It suffices to show that $S \cup T$ is a transcendence base of K over F. First of all every element of E is algebraic over $F(S)$ and hence over $F(S \cup T)$. Thus $F(S \cup T)(E)$ is algebraic over $F(S \cup T)$. Since $F(S \cup T) = F(S)(T) \subseteq E(T) \subseteq F(S \cup T)(E)$, $E(T)$ is algebraic over $F(S \cup T)$. But K is algebraic over $E(T)$ and therefore algebraic over $F(S \cup T)$. Consequently, it suffices to show that $S \cup T$ is algebraically independent over F.

$$\begin{array}{c} K \\ | \; \} T \\ E \\ | \; \} S \\ F \end{array}$$

Let f be a polynomial over F in $n+m$ variables (denoted

$x_1, \ldots, x_n, y_1, \ldots, y_m$) such that $f(s_1, \ldots, s_n, t_1, \ldots, t_m) = 0$ for some distinct $s_1, \ldots, s_n \in S$, $t_1, \ldots, t_m \in T$. Let $g = g(y_1, \ldots, y_m) = f(s_1, \ldots, s_n, y_1, \ldots, y_m) \in F(S)[y_1, \ldots, y_m] \subseteq E[y_1, \ldots, y_m]$. Since $g(t_1, \ldots, t_m) = 0$, the algebraic independence of T over E implies that $g = 0$. Now

$$f = f(x_1, \ldots, x_n, y_1, \ldots, y_m) = \sum_{i=1}^{r} h_i(x_1, \ldots, x_n) k_i(y_1, \ldots, y_m)$$

with $h_i \in F[x_1, \ldots, x_n]$, $k_i \in F[y_1, \ldots, y_m]$. Hence $0 = g(y_1, \ldots, y_m) = f(s_1, \ldots, s_n, y_1, \ldots, y_m)$ implies that $h_i(s_1, \ldots, s_n) = 0$ for every i. The algebraic independence of S over F implies that $h_i = 0$ for all i, whence

$$f(x_1, \ldots, x_n, y_1, \ldots, y_m) = 0.$$

Therefore SUT is algebraically independent over F.

TRANSCENDENCE BASES FOR DOMAINS AND AFFINE ALGEBRAS

Let D be a commutative domain D that is an algebra over a field F, E the field of fractions of D, so $F \subseteq D \subseteq E$. Evidently, since $F(D)$ is a subfield of E containing D, $F(D) = E$ and hence D contains a transcendence base of E/F. We call $\text{tr.d. } E/F$ the transcendence degree of D/F.

THEOREM. **(i)** Let D/F and D'/F be domains and suppose there exists a surjective homomorphism η of D/F onto D'/F. Then $\text{tr.d. } D/F \geq \text{tr.d. } D'/F$. **(ii)** Moreover, if $\text{tr.d. } D/F = \text{tr.d. } D'/F = m < \infty$, then η is an isomorphism.

PROOF. **(i)** Let $\mathcal{B}'$ be a transcendence base for D'/F. For each $x' \in \mathcal{B}'$ choose an $x \in D$ such that $\eta x = x'$. Then $\mathcal{C} = \{x\}$ is an algebraically independent subset of D. Thus $\mathcal{C}$ can be extended to a base $\mathcal{B}$ for E/F, E the field of fractions of D. Hence

$$\text{tr.d. } D/F = |\mathcal{B}| \geq |\mathcal{C}| = |\mathcal{B}'| = \text{tr.d. } D'/F.$$

(ii) Now let $\mathcal{B}' = \{x_1', \ldots, x_m'\}$, $\mathcal{C} = \{x_1, \ldots, x_m\}$ where $\eta x_i = x_i'$. Since $\mathcal{C}$ is an algebraically independent set of cardinality $\text{tr.d. } E/F$, $\mathcal{B} = \mathcal{C}$ is a transcendence base of E/F. Let $0 \neq a \in D$. Then a is algebraic over $F(x_1, \ldots, x_m)$. Let $f(X) = X^n - \alpha_1 X^{n-1} + \cdots + \alpha_n$, $\alpha_i \in F(x_1, \ldots, x_m)$ be the minimal polynomial of a over $F(x_1, \ldots, x_m)$. Since $a \neq 0$, $\alpha_n \neq 0$. We can write

$a_i = g_i(x_1,\ldots,x_m)g_0(x_1,\ldots,x_m)^{-1}$ where $g_i(x_1,\ldots,x_m), g_0(x_1,\ldots,x_m) \in F[x_1,\ldots,x_m]$. Then we have

$$g_0(x_1,\ldots,x_m)a^n + g_1(x_1,\ldots,x_m)a^{n-1} + \cdots + g_n(x_1,\ldots,x_m) = 0$$

and hence

$$g_0(x_1',\ldots,x_m')(\eta a)^n + \cdots + g_n(x_1',\ldots,x_m') = 0. \qquad (*)$$

Since $a_n \neq 0$, $g_n(x_1,\ldots,x_m) \neq 0$ and since the x_i's are algebraically independent $g_n(x_1',\ldots,x_m') \neq 0$. Then by $(*)$, $\eta a \neq 0$. Thus $a \neq 0$ implies $\eta a \neq 0$ and so η is an isomorphism. □

DEFINITION. If E is a commutative ring and R is a subring, then an element $u \in E$ is called R-integral (or integral over R) if there exists a monic polynomial $f(x) \in R[x]$, x an indeterminate, such that $f(u) = 0$.

The subset R' of E consisting of all elements that are integral over R is a subring containing R. The subring R' is called the integral closure of R in E. If $R' = E$, that is, every element of E is integral over R, then we say that E is integral over R (or E is an integral extension of R). If $R' = R$, then we say that R is integrally closed in E. A domain is said to be integrally closed if it is integrally closed in its field of fractions.

NOETHER NORMALIZATION THEOREM. Let D be a domain which is finitely generated over a field F, say, $D = F[u_1,\ldots,u_m]$. Let $\text{tr.d. } D/F = r \leq m$. Then there exists a transcendence base $\{v_i\}$ such that D is integral over $F[v_1,\ldots,v_r]$.

PROOF. The result is trivial if $m = r$ so suppose $m > r$. Then the u_i

are algebraically dependent. Hence there exists a nonzero polynomial

$$f(X_1,\dots,X_m)=\sum a_{j_1\dots j_m}X_1^{j_1}\dots X_m^{j_m}$$

in indeterminates X_i with coefficients in F such that $f(u_1,\dots,u_m)=0$. Let X be the set of monomials $X_1^{j_1}\dots X_m^{j_m}$ occuring in f (with nonzero coefficients). With each such monomial $X_1^{j_1}\dots X_m^{j_m}$ we associate the polynomial $j_1+j_2t+\dots+j_mt^{m-1}\in\mathbb{Z}[t]$, t an indeterminate. The polynomials obtained in this way from the monomials in X are distinct. Since a polynomial of degree n in one indeterminate with coefficients in a field has at most n zeros in the field, it follows that there exists an integer $d\geq 0$ such that the integers $j_1+j_2d+\dots+j_md^{m-1}$ obtained from the monomials in X are distinct. Now consider the polynomial

$$f(X_1,X_1^d+Y_2,\dots,X_1^{d^{m-1}}+Y_m)$$

where $Y_2,\dots,Y_m$ are indeterminates. We have

$$\begin{aligned}f(X_1,X_1^d+Y_2,\dots,X_1^{d^{m-1}}+Y_m)&=\sum a_{j_1\dots j_m}X_1^{j_1}(X_1^d+Y_2)^{j_2}\dots(X_1^{d^{m-1}}+Y_m)^{j_m}\\&=\sum a_{j_1\dots j_m}X_1^{j_1+j_2d+\dots+j_md^{m-1}}+g(X_1,Y_2,\dots,Y_m)\end{aligned}$$

where the degree of g in X_1 is less than that of

$$\sum a_{j_1\dots j_m}X_1^{j_1+j_2d+\dots+j_md^{m-1}}.$$

Hence for a suitable $\beta\in F^*$, $\beta f(X_1,X_1^d+Y_2,\dots,X_1^{d^{m-1}}+Y_m)$ is monic as a polynomial in X_1 with coefficients in $F[Y_2,\dots,Y_m]$. If we put

$$w_i=u_i-u_1^{d^{i-1}},\quad 2\leq i\leq m,$$

we have $\beta f(u_1,u_1^d+w_2,\dots,u_1^{d^{m-1}}+w_n)=0$ which implies that u_1 is integral over $D'=F[w_2,\dots,w_n]$. By induction on the numbes of generators, D' has a transcendence base $\{v_i\}_{i=1}^s$ such that D' is integral

over $F[v_1,\ldots,v_s]$. Then D is integral over $F[v_1,\ldots,v_s]$ by the transitivity of integral dependence. Thus it remains only to show that $s=r$ and $\{v_1,\ldots,v_s\}$ is also a transcendence base of D/F. Let E and E' be fields of fractions of D and D', respectively. Since $D=D'[u_1]$, we have $E=E'(u_1)$. We know that E' is algebraic over $F(v_1,\ldots,v_s)$ and E is algebraic over E' (since u_1 is integral over $D'\subseteq E'$). Thus E is algebraic over $F(v_1,\ldots,v_s)$ and so $s=r$ and $\{v_1,\ldots,v_s\}$ is also transcendence base of D/F.

Let E be a commutative ring and R a subring of E. For any (prime) ideal I of R, we denote $I\cap R$, which is a (prime) ideal of R, by I^c. It is easy to see that if E is integral over R, then E/I is integral over R/I^c for any ideal I of E. One can also easily show that if E is a domain that is integral over the subdomain R, then E is a field if and only if R is a field. Moreover, for any multiplicatively closed subset S of R, $S^{-1}E$ is integral over $S^{-1}R$ when E is integral over R. Combining these results, we can deduce that if E is integral over R, then

(1) for a prime ideal P of E, P^c is maximal in R if and only if P is maximal in E, and

(2) for prime ideals P_1 and P_2 in E, if $P_1\supsetneq P_2$, then $P_1^c\supsetneq P_2^c$.

THEOREM. ("LYING-OVER" THEOREM) Let E be a commutative ring, R a subring such that E is integral over R. Then any

prime ideal p of R is the contraction P^c of a prime ideal P of E. □

THEOREM ("GOING-DOWN" THEOREM) Let D be an integrally closed subdomain of a domain E that is integral over D. Let p_1 and p_2 be prime ideals of D such that $p_1 \supset p_2$ and suppose P_1 is a prime ideal of E such that $P_1^c = p_1$. Then there exists a prime ideal P_2 of E such that $P_2^c = p_2$ and $P_1 \supset P_2$.

A commutative ring that is a finitely generated algebra over a field is called an affine algebra. Such an algebra is Noetherian (by the famous Hilbert basis theorem). We recall that the Krull dimension of a Noetherian ring is defined to be $\sup S$ for chains of prime ideals $P_0 \supsetneq P_1 \supsetneq \dots \supsetneq P_s$ in R.

THEOREM. Let D be an affine domain of transcendence degree r over F. Then the Krull dimension $\dim D \geq r$ and $\dim D = r$ if F is algebraically closed.

PROOF. By Noether's normalization theorem, we may write $D = F[u_1, \dots, u_r, u_{r+1}, \dots, u_m]$ where u_i, $1 \leq i \leq r$, constitute a transcendence base and the remaining u_j are integral over $F[u_1, \dots, u_r]$. Then $F[u_1, \dots, u_r]$ is a UFD and hence is integrally closed. Under these circumstances, we can apply the "going-down" theorem to show that $\dim D = \dim F[u_1, \dots, u_r]$: First, let

$$P_0 \supsetneq P_1 \supsetneq \dots \supsetneq P_s$$

be a strictly descending chain of prime ideals in $F[u_1,\dots,u_r]$. By the "lying-over" theorem, there exists a prime ideal P_0 in D such that $P_0^c = P_0 \cap F[u_1,\dots,u_r] = p_0$. By the "going-down" theorem, there exists a prime ideal P_1 in D such that $P_1^c = p_1$ and $P_0 \supseteq P_1$. Then $P_0 \neq P_1$. By induction, we obtain a chain of prime ideals $P_0 \supsetneq P_1 \supsetneq \dots \supsetneq P_s$ such that $P_i \cap F[u_1,\dots,u_r] = p_i$, $0 \leq i < s$. This implies that $\dim D \geq \dim F[u_1,\dots,u_r]$. Next let $P_0 \supsetneq P_1 \supsetneq \dots \supsetneq P_s$ for prime ideals P_i in D. Then $p_0 \supsetneq p_1 \supsetneq \dots \supsetneq p_s$, where $p_i = P_i^c$ is a properly descending chain of prime ideals in $F[u_1,\dots,u_r]$ (since D is integral over $F[u_1,\dots,u_r]$). It follows that $\dim F[u_1,\dots,u_r] \geq \dim D$. Hence $\dim D = \dim F[u_1,\dots,u_r]$. Now we have the chain of prime ideals

$$(u_1,\dots,u_r) \supsetneq (u_1,\dots,u_{r-1}) \supsetneq \dots \supsetneq (u_1) \supsetneq (0)$$

in $F[u_1,\dots,u_r]$. Hence $\dim D = \dim F[u_1,\dots,u_r] \geq r = \text{tr.d. } D/F$. On the other hand, it is known that if F is algebraically closed, then $\dim F[u_1,\dots,u_r]$, for algebraically independent u_i, is r. This concludes the proof. □

LINEARLY DISJOINT EXTENSIONS

In this section, we assume that all the fields involved are contained in one field Ω, assumed algebraically closed. Let K and L be two extensions of a field F.

K is said to be <u>linearly disjoint from</u> L over F if every finite set of elements of K that is linearly independent over F is still such over L.

The definition is unsymmetric, but we prove that the property of being linearly disjoint is actually symmetric for K and L. Assume K is linearly disjoint from L over F. Let $y_1, \dots, y_n$ be elements of L linearly independent over F. Suppose there is a non-trivial relation of linear dependence over K,

$$x_1 y_1 + x_2 y_2 + \cdots + x_n y_n = 0. \quad (1)$$

Say $x_1, \dots, x_r$ are linearly independent over F and $x_{r+1}, \dots, x_n$ are linear combinations $x_i = \sum_{j=1}^{r} a_{ij} x_j$, $i = r+1, \dots, n$. We can write the relation (1) as follows:

$$\sum_{j=1}^{r} x_j y_j + \sum_{i=r+1}^{n} \left(\sum_{j=1}^{r} a_{ij} x_j \right) y_i = 0$$

and collecting terms, after inverting the second sum, we get

$$\sum_{j=1}^{r} \left(y_j + \sum_{i=r+1}^{n} (a_{ij} y_j) \right) x_j = 0.$$

The y's are linearly independent over F, so the coefficients of x_j are $\neq 0$. This contradicts the linear disjointness of K and L over F.

We now give two criteria for linear disjointness.

Criterion 1. Suppose that K is the quotient field of a ring R and L the quotient field of a ring S. To test whether L and K are linearly disjoint, it suffices to show that if elements $y_1, \dots, y_n$ of S are linearly independent over F, then there is no linear relation among the y's with coefficients in R. Indeed, if elements $y_1, \dots, y_n$ of L are

linearly independent over F, and if there is a relation

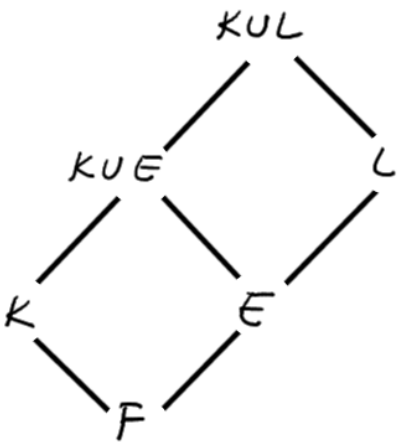
$$x_1 y_1 + \cdots + x_n y_n = 0$$

with $x_i \in K$, then we can select $y \in S$ and $x \in R$ such that $xy \neq 0$, $yy_i \in S$ for all i, and $xx_j \in R$ for all j. Multiplying the relation by xy gives a linear dependence between elements of R and S. However, yy_i are obviously linearly independent over F, and this proves our criterion.

Criterion 2. Again let R be a subring of K such that K is its quotient field and R is a vector space over F. Let $\{u_\alpha\}$ be a basis of R considered as a vector space over F. To prove K and L are linearly disjoint over F, it suffices to show that the elements $\{u_\alpha\}$ of this basis remain linearly independent over L. Indeed, suppose this is the case. Let $x_1, \ldots, x_m$ be elements of R linearly independent over F. They lie in a finite-dimensional vector space generated by some of the u_α, say $u_1, \ldots, u_s$. They can be completed to a basis for this subspace over F. Lifting this vector space of dimension n over L, it must conserve its dimension because the u's remain linearly independent by hypothesis, and hence the x's must also remain linearly independent over L.

PROPOSITION. Let K be a field containing another field F, and let $L \supseteq E$ be two other extensions of F. Then K and L are

linearly disjoint over F if and only if K and E are linearly disjoint over F and KUE, L are linearly disjoint over E.



PROOF. Assume first that K, E are linearly disjoint over F, and KUE, L are linearly disjoint over E. Let $\{\kappa\}$ be a basis of K as a vectorspace over F, and let $\{\alpha\}$ be a basis of E over F. Let $\{\lambda\}$ be a basis of L over E. Then $\{\alpha\lambda\}$ is a basis of L over F. If K and L are not linearly disjoint over F, there exists a relation

$$\sum_{\lambda,\alpha}\left(\sum_{\kappa} c_{\kappa\lambda\alpha}\kappa\right)\lambda\alpha = 0$$

with some $c_{\kappa\lambda\alpha} \neq 0$, $c_{\kappa\lambda\alpha} \in F$. Changing the order of summation gives

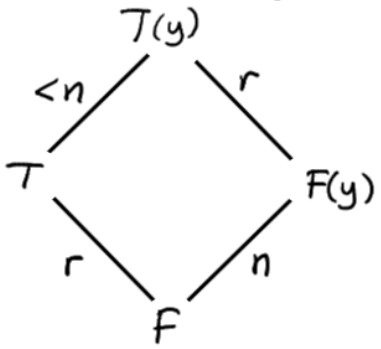
$$\sum_{\lambda}\left(\sum_{\kappa,\alpha} c_{\kappa\lambda\alpha}\kappa\alpha\right)\lambda = 0$$

contradicting the linear disjointness of L and KUE over E.

Conversely, assume that K and L are linearly disjoint over F, and the field KUE is the quotient field of the ring $E[K]$ generated over E by all elements of K. This ring is a vector space over E, and a basis for K over F is also a basis for this ring $E[K]$ over E. With this remark and the criteria for linear disjointness, we see that it suffices to prove that the elements of such a basis remain linearly independent over L. Since K and L are linearly disjoint, we are done.

Let K and L be two extensions of a field F. We shall say that K is free from L over F if every finite set of elements of K algebraically independent over F remains such over L. If (x) and (y) are two sets of elements in Ω, we say that they are free over F (or independent over F) if $F(x)$ and $F(y)$ are free over F.

The property of being free from a field is symmetric: Assume that K is free from L over F. Let $y_1, \ldots, y_n \in L$ be algebraically independent over F. Suppose they become dependent over K. They become so in a subfield T of K finitely generated over F, say of transcendence degree r over F. Computing the transcendence degree of $T(y)$ over F in two ways gives a contradiction. (See the figure below.)



PROPOSITION. If K and L are linearly disjoint over F, then they are free over F.

PROOF. Let $x_1, \ldots, x_n$ be elements of K algebraically independent over F. Suppose they become algebraically dependent over L. We get a relation

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

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 F. 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 finite-dimensional 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 F be a field of characteristic $p \neq 0$, and K an extension of F. We embed K into its algebraic closure $\overline{K}$. If m is a positive integer, then we denote the subset of $\overline{K}$ 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 $\overline{K}$ containing F for every $m > 0$, and that we have an ascending chain

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

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 $\overline{K}$ (and also $\overline{F}$, 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 $m > 0$.