CHAPTER VIII

Transcendental Extensions

Both for their own sake and for applications to the case of finite extensions of the rational numbers, one is led to deal with ground fields which are function fields, i.e. finitely generated over some field k, possibly by elements which are not algebraic. This chapter gives some basic properties of such fields.

§1. TRANSCENDENCE BASES

Let K be an extension field of a field k. Let S be a subset of K. We recall that S (or the elements of S) is said to be algebraically independent over k, if whenever we have a relation

$$0 = \sum a_{(\nu)} M_{(\nu)}(S) = \sum a_{(\nu)} \prod_{x \in S} x^{\nu(x)}$$

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

We can introduce an ordering among algebraically independent subsets of K, by ascending inclusion. These subsets are obviously inductively ordered, and thus there exist maximal elements. If S is a subset of K which is algebraically independent over k, and if the cardinality of S is greatest among all such subsets, then we call this cardinality the **transcendence degree or dimension** of K over k. Actually, we shall need to distinguish only between finite transcendence degree or infinite transcendence degree. We observe that

the notion of transcendence degree bears to the notion of algebraic independence the same relation as the notion of dimension bears to the notion of linear independence.

We frequently deal with families of elements of K, say a family $\{x_i\}_{i \in I}$, and say that such a family is algebraically independent over k if its elements are distinct (in other words, $x_i \neq x_j$ if $i \neq j$) and if the set consisting of the elements in this family is algebraically independent over k.

A subset S of K which is algebraically independent over k and is maximal with respect to the inclusion ordering will be called a **transcendence base** of K over k. From the maximality, it is clear that if S is a transcendence base of K over k, then K is algebraic over $k(S)$.

Theorem 1.1. *Let K be an extension of a field k. Any two transcendence bases of K over k have the same cardinality. If Γ is a subset of K such that K is algebraic over $k(\Gamma)$, and S is a subset of Γ which is algebraically independent over k, then there exists a transcendence base $\mathfrak{B}$ of K over k such that $S \subset \mathfrak{B} \subset \Gamma$.*

Proof. We shall prove that if there exists one finite transcendence base, say $\{x_1, \ldots, x_m\}$, $m \geqq 1$, m minimal, then any other transcendence base must also have m elements. For this it will suffice to prove: If $w_1, \ldots, w_n$ are elements of K which are algebraically independent over k then $n \leqq m$ (for we can then use symmetry). By assumption, there exists a non-zero irreducible polynomial f_1 in $m + 1$ variables with coefficients in k such that

$$f_1(w_1, x_1, \ldots, x_m) = 0.$$

After renumbering $x_1, \ldots, x_m$ we may write $f_1 = \sum g_j(w_1, x_2, \ldots, x_m) x_1^j$ with some $g_N \neq 0$ with some $N \geqq 1$. No irreducible factor of g_N vanishes on $(w_1, x_2, \ldots, x_n)$, otherwise w_1 would be a root of two distinct irreducible polynomials over $k(x_1, \ldots, x_m)$. Hence x_1 is algebraic over $k(w_1, x_2, \ldots, x_m)$ and $w_1, x_2, \ldots, x_m$ are algebraically independent over k, otherwise the minimality of m would be contradicted. Suppose inductively that after a suitable renumbering of $x_2, \ldots, x_m$ we have found $w_1, \ldots, w_r$ $(r < n)$ such that K is algebraic over $k(w_1, \ldots, w_r, x_{r+1}, \ldots, x_m)$. Then there exists a non-zero polynomial f in $m + 1$ variables with coefficients in k such that

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

Since the w's are algebraically independent over k, it follows by the same argument as in the first step that some x_j, say x_{r+1}, is algebraic over $k(w_1, \ldots, w_{r+1}, x_{r+2}, \ldots, x_m)$. Since a tower of algebraic extensions is algebraic, it follows that K is algebraic over $k(w_1, \ldots, w_{r+1}, x_{r+2}, \ldots, x_m)$. We can repeat the procedure, and if $n \geqq m$ we can replace all the x's by w's, to see that K is algebraic over $k(w_1, \ldots, w_m)$. This shows that $n \geqq m$ implies $n = m$, as desired.

We have now proved: Either the transcendence degree is finite, and is equal to the cardinality of any transcendence base, or it is infinite, and every transcendence base is infinite. The cardinality statement in the infinite case will be left as an exercise. We shall also leave as an exercise the statement that a set of algebraically independent elements can be completed to a transcendence base, selected from a given set Γ such that K is algebraic over $k(\Gamma)$. (The reader will note the complete analogy of our statements with those concerning linear bases.)

Note. *The preceding section is the only one used in the next chapter. The remaining sections are more technical, especially §3 and §4 which will not be used in the rest of the book. Even §2 and §5 will only be mentioned a couple of times, and so the reader may omit them until they are referred to again.*

§2. NOETHER NORMALIZATION THEOREM

Theorem 2.1. *Let $k[x_1, \ldots, x_n] = k[x]$ be a finitely generated entire ring over a field k, and assume that $k(x)$ has transcendence degree r. Then there exist elements $y_1, \ldots, y_r$ in $k[x]$ such that $k[x]$ is integral over*

$$k[y] = k[y_1, \ldots, y_r].$$

Proof. If $(x_1, \ldots, x_n)$ are already algebraically independent over k, we are done. If not, there is a non-trivial relation

$$\sum a_{(j)} x_1^{j_1} \cdots x_n^{j_n} = 0$$

with each coefficient $a_{(j)} \in k$ and $a_{(j)} \neq 0$. The sum is taken over a finite number of distinct n-tuples of integers $(j_1, \ldots, j_n)$, $j_\nu \geqq 0$. Let $m_2, \ldots, m_n$ be positive integers, and put

$$y_2 = x_2 - x_1^{m_2}, \ldots, y_n = x_n - x_1^{m_n}.$$

Substitute $x_i = y_i + x_1^{m_i}$ $(i = 2, \ldots, n)$ in the above equation. Using vector notation, we put $(m) = (1, m_2, \ldots, m_n)$ and use the dot product $(j) \cdot (m)$ to denote $j_1 + m_2 j_2 + \cdots + m_n j_n$. If we expand the relation after making the above substitution, we get

$$\sum c_{(j)} x_1^{(j)\cdot(m)} + f(x_1, y_2, \ldots, y_n) = 0$$

where f is a polynomial in which no pure power of x_1 appears. We now select d to be a large integer [say greater than any component of a vector (j) such that $c_{(j)} \neq 0$] and take

$$(m) = (1, d, d^2, \ldots, d^n).$$

Then all $(j)\cdot(m)$ are distinct for those (j) such that $c_{(j)} \neq 0$. In this way we obtain an integral equation for x_1 over $k[y_2, \ldots, y_n]$. Since each x_i $(i > 1)$ is integral over $k[x_1, y_2, \ldots, y_n]$, it follows that $k[x]$ is integral over $k[y_2, \ldots, y_n]$. We can now proceed inductively, using the transitivity of integral extensions to shrink the number of y's until we reach an algebraically independent set of y's.

The advantage of the proof of Theorem 2.1 is that it is applicable when k is a finite field. The disadvantage is that it is not linear in $x_1, \ldots, x_n$. We now deal with another technique which leads into certain aspects of algebraic geometry on which we shall comment after the next theorem.

We start again with $k[x_1, \ldots, x_n]$ finitely generated over k and entire. Let (u_{ij}) $(i, j = 1, \ldots, n)$ be algebraically independent elements over $k(x)$, and let $k_u = k(u) = k(u_{ij})_{\text{all } i,j}$. Put

$$y_i = \sum_{j=1}^{n} u_{ij} x_j.$$

This amounts to a generic linear change of coordinates in n-space, to use geometric terminology. Again we let r be the transcendence degree of $k(x)$ over k.

Theorem 2.2. *With the above notation, $k_u[x]$ is integral over $k_u[y_1, \ldots, y_r]$.*

Proof. Suppose some x_i is not integral over $k_u[y_1, \ldots, y_r]$. Then there exists a place φ of $k_u(y)$ finite on $k_u[y_1, \ldots, y_r]$ but taking the value ∞ on some x_i. Using Proposition 3.4 of Chapter VII, and renumbering the indices if necessary, say $\varphi(x_j/x_n)$ is finite for all i. Let $z'_j = \varphi(x_j/x_n)$ for $j = 1, \ldots, n$. Then dividing the equations $y_i = \sum u_{ij} x_j$ by x_n (for $i = 1, \ldots, r$) and applying the place, we get

$$\begin{aligned} 0 &= u_{11} z'_1 + u_{12} z'_2 + \cdots + u_{1n}, \\ &\vdots \\ 0 &= u_{r1} z'_1 + u_{r2} z'_2 + \cdots + u_{rn}. \end{aligned}$$

The transcendence degree of $k(z')$ over k cannot be r, for otherwise, the place φ would be an isomorphism of $k(x)$ on its image. [Indeed, if, say, $z'_1, \ldots, z'_r$ are algebraically independent and $z_i = x_i/x_n$, then $z_1, \ldots, z_r$ are also algebraically independent, and so form a transcendence base for $k(x)$ over k. Then the place is an isomorphism from $k(z_1, \ldots, z_r)$ to $k(z'_1, \ldots, z'_r)$, and hence is an isomorphism from $k(x)$ to its image.] We then conclude that

$$u_{1n}, \ldots, u_{rn} \in k(u_{ij}, z') \qquad \text{with} \quad i = 1, \ldots, r; \quad j = 1, \ldots, n-1.$$

Hence the transcendence degree of $k(u)$ over k would be $\leqq rn - 1$, which is a contradiction, proving the theorem.

Corollary 2.3. *Let k be a field, and let $k(x)$ be a finitely generated extension of transcendence degree r. There exists a polynomial $P(u) = P(u_{ij}) \in k[u]$ such that if $(c) = (c_{ij})$ is a family of elements $c_{ij} \in k$ satisfying $P(c) \neq 0$, and we let $y_i' = \sum c_{ij}x_j$, then $k[x]$ is integral over $k[y_1', \ldots, y_r']$.*

Proof. By Theorem 2.2, each x_i is integral over $k_u[y_1, \ldots, y_r]$. The coefficients of an integral equation are rational functions in k_u. We let $P(u)$ be a common denominator for these rational functions. If $P(c) \neq 0$, then there is a homomorphism

$$\varphi: k(x)[u, P(u)^{-1}] \to k(x)$$

such that $\varphi(u) = (c)$, and such that φ is the identity on $k(x)$. We can apply φ to an integral equation for x_i over $k_u[y]$ to get an integral equation for x_i over $k[y']$, thus concluding the proof.

Remark. After Corollary 2.3, there remains the problem of finding explicitly integral equations for $x_1, \ldots, x_n$ (or $y_{r+1}, \ldots, y_n$) over $k_u[y_1, \ldots, y_r]$. This is an elimination problem, and I have decided to refrain from further involvement in algebraic geometry at this point. But it may be useful to describe the geometric language used to interpret Theorem 2.2 and further results in that line. After the generic change of coordinates, the map

$$(y_1, \ldots, y_n) \mapsto (y_1, \ldots, y_r)$$

is the generic projection of the variety whose coordinate ring is $k[x]$ on affine r-space. This projection is finite, and in particular, the inverse image of a point on affine r-space is finite. Furthermore, if $k(x)$ is separable over k (a notion which will be defined in §4), then the extension $k_u(y)$ is finite separable over $k_u(y_1, \ldots, y_r)$ (in the sense of Chapter V). To determine the degree of this finite extension is essentially Bezout's theorem. Cf. [La 58], Chapter VIII, §6.

The above techniques were created by van der Waerden and Zariski, cf., for instance, also Exercises 5 and 6. These techniques have unfortunately not been completely absorbed in some more recent expositions of algebraic geometry. To give a concrete example: When Hartshorne considers the intersection of a variety and a sufficiently general hyperplane, he does not discuss the "generic" hyperplane (that is, with algebraically independent coefficients over a given ground field), and he assumes that the variety is non-singular from the start (see his Theorem 8.18 of Chapter 8, [Ha 77]). But the description of the intersection can be done without simplicity assumptions, as in Theorem 7 of [La 58], Chapter VII, §6, and the corresponding lemma. Something was lost in discarding the technique of the algebraically independent (u_{ij}).

After two decades when the methods illustrated in Chapter X have been prevalent, there is a return to the more explicit methods of generic constructions using the algebraically independent (u_{ij}) and similar ones for some

applications because part of algebraic geometry and number theory are returning to some problems asking for explicit or effective constructions, with bounds on the degrees of solutions of algebraic equations. See, for instance, [Ph 91–95], [So 90], and the bibliography at the end of Chapter X, §6. Returning to some techniques, however, does not mean abandoning others; it means only expanding available tools.

Bibliography

[Ha 77] R. HARTSHORNE, *Algebraic Geometry*, Springer-Verlag, New York, 1977

[La 58] S. LANG, *Introduction to Algebraic Geometry*, Wiley–Interscience, New York, 1958

[Ph 91–95] P. PHILIPPON, Sur des hauteurs alternatives, I *Math. Ann.* 289 (1991) pp. 255–283; II *Ann. Inst. Fourier* 44 (1994) pp. 1043–1065; III *J. Math. Pures Appl.* 74 (1995) pp. 345–365

[So 90] C. SOULÉ, Géometrie d'Arakelov et théorie des nombres transcendants, Asterisque 198–200 (1991) pp. 355–371

§3. LINEARLY DISJOINT EXTENSIONS

In this section we discuss the way in which two extensions K and L of a field k behave with respect to each other. We assume that all the fields involved are contained in one field Ω, assumed algebraically closed.

K is said to be **linearly disjoint from L over k** if every finite set of elements of K that is linearly independent over k is still such over L.

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

$$x_1 y_1 + x_2 y_2 + \cdots + x_n y_n = 0. \tag{1}$$

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

$$\sum_{\mu=1}^{r} x_\mu y_\mu + \sum_{i=r+1}^{n} \left(\sum_{\mu=1}^{r} a_{i\mu} x_\mu \right) y_i = 0$$

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

$$\sum_{\mu=1}^{r} \left(y_\mu + \sum_{i=r+1}^{n} (a_{i\mu} y_i) \right) x_\mu = 0.$$

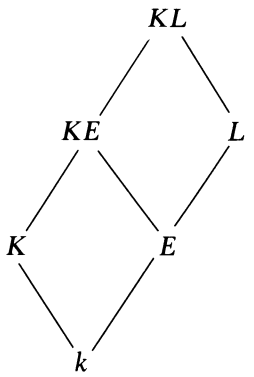
The y's are linearly independent over k, so the coefficients of x_μ are $\neq 0$. This contradicts the linear disjointness of K and L over k.

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 $y_1, \ldots, y_n$ of S are linearly independent over k, then there is no linear relation among the y's with coefficients in R. Indeed, if elements $y_1, \ldots, y_n$ of L are linearly independent over k, 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 $xx_i \in R$ for all i. Multiplying the relation by xy gives a linear dependence between elements of R and S. However, the yy_i are obviously linearly independent over k, 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 k. Let $\{u_\alpha\}$ be a basis of R considered as a vector space over k. To prove K and L linearly disjoint over k, 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 k. They lie in a finite dimension vector space generated by some of the u_α, say $u_1, \ldots, u_n$. They can be completed to a basis for this space over k. 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.

Proposition 3.1. *Let K be a field containing another field k, and let $L \supset E$ be two other extensions of k. Then K and L are linearly disjoint over k if and only if K and E are linearly disjoint over k and KE, L are linearly disjoint over E.*



Proof. Assume first that K, E are linearly disjoint over k, and KE, L are linearly disjoint over E. Let $\{\kappa\}$ be a basis of K as vector space over k (we use the elements of this basis as their own indexing set), and let $\{\alpha\}$ be a basis of E over k. Let $\{\lambda\}$ be a basis of L over E. Then $\{\alpha\lambda\}$ is a basis of L over k. If K and L are not linearly disjoint over k, then there exists a relation

$$\sum_{\lambda,\alpha}\left(\sum_{\kappa} c_{\kappa\lambda\alpha}\kappa\right)\lambda\alpha = 0 \qquad \text{with some } c_{\kappa\lambda\alpha} \neq 0,\ c_{\kappa\lambda\alpha} \in k.$$

Changing the order of summation gives

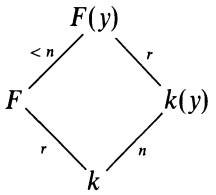
$$\sum_{\lambda}\left(\sum_{\kappa,\lambda} c_{\kappa\lambda\alpha}\kappa\alpha\right)\lambda = 0$$

contradicting the linear disjointness of L and KE over E.

Conversely, assume that K and L are linearly disjoint over k. Then *a fortiori*, K and E are also linearly disjoint over k, and the field KE 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 k 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. At this point we see that the arguments given in the first part of the proof are reversible. We leave the formalism to the reader.

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

Just as with linear disjointness, our definition is unsymmetric, and we prove that the relationship expressed therein is actually symmetric. Assume therefore that K is free from L over k. Let $y_1, \ldots, y_n$ be elements of L, algebraically independent over k. Suppose they become dependent over K. They become so in a subfield F of K finitely generated over k, say of transcendence degree r over k. Computing the transcendence degree of $F(y)$ over k in two ways gives a contradiction (cf. Exercise 5).



Proposition 3.2. *If K and L are linearly disjoint over k, then they are free over k.*

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

$$\sum y_a M_a(x) = 0$$

between monomials $M_a(x)$ with coefficients y_a in L. This gives a linear relation among the $M_a(x)$. But these are linearly independent over k because the x's are assumed algebraically independent over k. This is a contradiction.

Proposition 3.3. *Let L be an extension of k, and let $(u) = (u_1, \ldots, u_r)$ be a set of quantities algebraically independent over L. Then the field $k(u)$ is linearly disjoint from L over k.*

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

Note finally that the property that two extensions K and L of a field k are linearly disjoint or free is of finite type. To prove that they have either property, it suffices to do it for all subfields K_0 and L_0 of K and L respectively which are finitely generated over k. This comes from the fact that the definitions involve only a finite number of quantities at a time.

§4. SEPARABLE AND REGULAR EXTENSIONS

Let K be a finitely generated extension of k, $K = k(x)$. We shall say that it is **separably generated** if we can find a transcendence basis $(t_1, \ldots, t_r)$ of K/k such that K is separably algebraic over $k(t)$. Such a transcendence base is said to be a **separating transcendence base** for K over k.

We always denote by p the characteristic if it is not 0. The field obtained from k by adjoining all p^m-th roots of all elements of k will be denoted by k^{1/p^m}. The compositum of all such fields for $m = 1, 2, \ldots$, is denoted by k^{1/p^∞}.

Proposition 4.1. *The following conditions concerning an extension field K of k are equivalent:*

(i) *K is linearly disjoint from k^{1/p^∞}.*
(ii) *K is linearly disjoint from k^{1/p^m} for some m.*

(iii) *Every subfield of K containing k and finitely generated over k is separably generated.*

Proof. It is obvious that (i) implies (ii). In order to prove that (ii) implies (iii), we may clearly assume that K is finitely generated over k, say

$$K = k(x) = k(x_1, \ldots, x_n).$$

Let the transcendence degree of this extension be r. If $r = n$, the proof is complete. Otherwise, say $x_1, \ldots, x_r$ is a transcendence base. Then x_{r+1} is algebraic over $k(x_1, \ldots, x_r)$. Let $f(X_1, \ldots, X_{r+1})$ be a polynomial of lowest degree such that

$$f(x_1, \ldots, x_{r+1}) = 0.$$

Then f is irreducible. We contend that not all x_i $(i = 1, \ldots, r+1)$ appear to the p-th power throughout. If they did, we could write $f(X) = \sum c_\alpha M_\alpha(X)^p$ where $M_\alpha(X)$ are monomials in $X_1, \ldots, X_{r+1}$ and $c_\alpha \in k$. This would imply that the $M_\alpha(x)$ are linearly dependent over $k^{1/p}$ (taking the p-th root of the equation $\sum c_\alpha M_\alpha(x)^p = 0$). However, the $M_\alpha(x)$ are linearly independent over k (otherwise we would get an equation for $x_1, \ldots, x_{r+1}$ of lower degree) and we thus get a contradiction to the linear disjointness of $k(x)$ and $k^{1/p}$. Say X_1 does not appear to the p-th power throughout, but actually appears in $f(X)$. We know that $f(X)$ is irreducible in $k[X_1, \ldots, X_{r+1}]$ and hence $f(x) = 0$ is an irreducible equation for x_1 over $k(x_2, \ldots, x_{r+1})$. Since X_1 does not appear to the p-th power throughout, this equation is a separable equation for x_1 over $k(x_2, \ldots, x_{r+1})$, in other words, x_1 is separable algebraic over $k(x_2, \ldots, x_{r+1})$. From this it follows that it is separable algebraic over $k(x_2, \ldots, x_n)$. If $(x_2, \ldots, x_n)$ is a transcendence base, the proof is complete. If not, say that x_2 is separable over $k(x_3, \ldots, x_n)$. Then $k(x)$ is separable over $k(x_3, \ldots, x_n)$. Proceeding inductively, we see that the procedure can be continued until we get down to a transcendence base. This proves that (ii) implies (iii). It also proves that a separating transcendence base for $k(x)$ over k can be selected from the given set of generators (x).

To prove that (iii) implies (i) we may assume that K is finitely generated over k. Let (u) be a transcendence base for K over k. Then K is separably algebraic over $k(u)$. By Proposition 3.3, $k(u)$ and k^{1/p^∞} are linearly disjoint. Let $L = k^{1/p^\infty}$. Then $k(u)L$ is purely inseparable over $k(u)$, and hence is linearly disjoint from K over $k(u)$ by the elementary theory of finite algebraic extensions. Using Proposition 3.1, we conclude that K is linearly disjoint from L over k, thereby proving our theorem.

An extension K of k satisfying the conditions of Proposition 4.1 is called **separable**. This definition is compatible with the use of the word for algebraic extensions.

The first condition of our theorem is known as **MacLane's criterion**. It has the following immediate corollaries.

Corollary 4.2. *If K is separable over k, and E is a subfield of K containing k, then E is separable over k.*

Corollary 4.3. *Let E be a separable extension of k, and K a separable extension of E. Then K is a separable extension of k.*

Proof. Apply Proposition 3.1 and the definition of separability.

Corollary 4.4. *If k is perfect, every extension of k is separable.*

Corollary 4.5. *Let K be a separable extension of k, and free from an extension L of k. Then KL is a separable extension of L.*

Proof. An element of KL has an expression in terms of a finite number of elements of K and L. Hence any finitely generated subfield of KL containing L is contained in a composite field FL, where F is a subfield of K finitely generated over k. By Corollary 4.2, we may assume that K is finitely generated over k. Let (t) be a transcendence base of K over k, so K is separable algebraic over $k(t)$. By hypothesis, (t) is a transcendence base of KL over L, and since every element of K is separable algebraic over $k(t)$, it is also separable over $L(t)$. Hence KL is separably generated over L. This proves the corollary.

Corollary 4.6. *Let K and L be two separable extensions of k, free from each other over k. Then KL is separable over k.*

Proof. Use Corollaries 4.5 and 4.3.

Corollary 4.7. *Let K, L be two extensions of k, linearly disjoint over k. Then K is separable over k if and only if KL is separable over L.*

Proof. If K is not separable over k, it is not linearly disjoint from $k^{1/p}$ over k, and hence *a fortiori* it is not linearly disjoint from $Lk^{1/p}$ over k. By Proposition 4.1, this implies that KL is not linearly disjoint from $Lk^{1/p}$ over L, and hence that KL is not separable over L. The converse is a special case of Corollary 4.5, taking into account that linearly disjoint fields are free.

We conclude our discussion of separability with two results. The first one has already been proved in the first part of Proposition 4.1, but we state it here explicitly.

Proposition 4.8. *If K is a separable extension of k, and is finitely generated, then a separating transcendence base can be selected from a given set of generators.*

To state the second result we denote by K^{p^m} the field obtained from K by raising all elements of K to the p^m-th power.

Proposition 4.9. *Let K be a finitely generated extension of a field k. If $K^{p^m}k = K$ for some m, then K is separably algebraic over k. Conversely, if K is separably algebraic over k, then $K^{p^m}k = K$ for all m.*

Proof. If K/k is separably algebraic, then the conclusion follows from the elementary theory of finite algebraic extensions. Conversely, if K/k is finite algebraic but not separable, then the maximal separable extension of k in K cannot be all of K, and hence K^pk cannot be equal to K. Finally, if there exists an element t of K transcendental over k, then $k(t^{1/p^m})$ has degree p^m over $k(t)$, and hence there exists a t such that t^{1/p^m} does not lie in K. This proves our proposition.

There is a class of extensions which behave particularly well from the point of view of changing the ground field, and are especially useful in algebraic geometry. We put some results together to deal with such extensions. Let K be an extension of a field k, with algebraic closure K^a. We claim that the following two conditions are equivalent:

REG 1. k is algebraically closed in K (i.e. every element of K algebraic over k lies in k), and K is separable over k.

REG 2. K is linearly disjoint from k^a over k.

We show the equivalence. Assume **REG 2**. By Proposition 4.1, we know that K is separably generated over k. It is obvious that k must be algebraically closed in K. Hence **REG 2** implies **REG 1**. To prove the converse we need a lemma.

Lemma 4.10. *Let k be algebraically closed in extension K. Let x be some element of an extension of K, but algebraic over k. Then $k(x)$ and K are linearly disjoint over k, and $[k(x):k] = [K(x):K]$.*

Proof. Let $f(X)$ be the irreducible polynomial for x over k. Then f remains irreducible over K; otherwise, its factors would have coefficients algebraic over k, hence in k. Powers of x form a basis of $k(x)$ over k, hence the same powers form a basis of $K(x)$ over K. This proves the lemma.

To prove **REG 2** from **REG 1**, we may assume without loss of generality that K is finitely generated over k, and it suffices to prove that K is linearly disjoint from an arbitrary finite algebraic extension L of k. If L is separable algebraic over k, then it can be generated by one primitive element, and we can apply Lemma 4.10.

More generally, let E be the maximal separable subfield of L containing k. By Proposition 3.1, we see that it suffices to prove that KE and L are linearly disjoint over E. Let (t) be a separating transcendence base for K over k. Then K is separably algebraic over $k(t)$. Furthermore, (t) is also a separating transcendence base for KE over E, and KE is separable algebraic

over $E(t)$. Thus KE is separable over E, and by definition KE is linearly disjoint from L over K because L is purely inseparable over E. This proves that **REG 1** implies **REG 2**.

Thus we can define an extension K of k to be **regular** if it satisfies either one of the equivalent conditions **REG 1** or **REG 2**.

Proposition 4.11.

(a) *Let K be a regular extension of k, and let E be a subfield of K containing k. Then E is regular over k.*
(b) *Let E be a regular extension of k, and K a regular extension of E. Then K is a regular extension of k.*
(c) *If k is algebraically closed, then every extension of k is regular.*

Proof. Each assertion is immediate from the definition conditions **REG 1** and **REG 2**.

Theorem 4.12. *Let K be a regular extension of k, let L be an arbitrary extension of k, both contained in some larger field, and assume that K, L are free over k. Then K, L are linearly disjoint over k.*

Proof (Artin). Without loss of generality, we may assume that K is finitely generated over k. Let $x_1, \ldots, x_n$ be elements of K linearly independent over k. Suppose we have a relation of linear dependence

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

with $y_i \in L$. Let φ be a k^a-valued place of L over k. Let (t) be a transcendence base of K over k. By hypothesis, the elements of (t) remain algebraically independent over L, and hence φ can be extended to a place of KL which is identity on $k(t)$. This place must then be an isomorphism of K on its image, because K is a finite algebraic extension of $k(t)$ (remark at the end of Chapter VII, §3). After a suitable isomorphism, we may take a place equivalent to φ which is the identity on K. Say $\varphi(y_i/y_n)$ is finite for all i (use Proposition 3.4 of Chapter VII). We divide the relation of linear dependence by y_n and apply φ to get $\sum x_i \varphi(y_i/y_n) = 0$, which gives a linear relation among the x_i with coefficients in k^a, contradicting the linear disjointness. This proves the theorem.

Theorem 4.13. *Let K be a regular extension of k, free from an extension L of k over k. Then KL is a regular extension of L.*

Proof. From the hypothesis, we deduce that K is free from the algebraic closure L^a of L over k. By Theorem 4.12, K is linearly disjoint from L^a over k. By Proposition 3.1, KL is linearly disjoint from L^a over L, and hence KL is regular over L.

Corollary 4.14. *Let K, L be regular extensions of k, free from each other over k. Then KL is a regular extension of k.*

Proof. Use Corollary 4.13 and Proposition 4.11(b).

Theorem 4.13 is one of the main reasons for emphasizing the class of regular extensions: they remain regular under arbitrary base change of the ground field k. Furthermore, Theorem 4.12 in the background is important in the study of polynomial ideals as in the next section, and we add some remarks here on its implications. We now assume that the reader is acquainted with the most basic properties of the tensor product (Chapter XVI, §1 and §2).

Corollary 4.15. *Let $K = k(x)$ be a finitely generated regular extension, free from an extension L of k, and both contained in some larger field. Then the natural k-algebra homomorphism*

$$L \otimes_k k[x] \to L[x]$$

is an isomorphism.

Proof. By Theorem 4.12 the homomorphism is injective, and it is obviously surjective, whence the corollary follows.

Corollary 4.16. *Let $k(x)$ be a finitely generated regular extension, and let $\mathfrak{p}$ be the prime ideal in $k[X]$ vanishing on (x), that is, consisting of all polynomials $f(X) \in k[X]$ such that $f(x) = 0$. Let L be an extension of k, free from $k(x)$ over k. Let $\mathfrak{p}_L$ be the prime ideal in $L[X]$ vanishing on (x). Then $\mathfrak{p}_L = \mathfrak{p}L[X]$, that is $\mathfrak{p}_L$ is the ideal generated by $\mathfrak{p}$ in $L[X]$, and in particular, this ideal is prime.*

Proof. Consider the exact sequence

$$0 \to \mathfrak{p} \to k[X] \to k[x] \to 0.$$

Since we are dealing with vector spaces over a field, the sequence remains exact when tensored with any k-space, so we get an exact sequence

$$0 \to L \otimes_k \mathfrak{p} \to L[X] \to L \otimes_k k[x] \to 0.$$

By Corollary 4.15, we know that $L \otimes_k k[x] \approx L[x]$, and the image of $L \otimes_k \mathfrak{p}$ in $L[X]$ is $\mathfrak{p}L[X]$, so the lemma is proved.

Corollary 4.16 shows another aspect whereby regular extensions behave well under extension of the base field, namely the way the prime ideal $\mathfrak{p}$ remains prime under such extensions.

§5. DERIVATIONS

A **derivation** D of a ring R is a mapping $D: R \to R$ of R into itself which is linear and satisfies the ordinary rule for derivatives, i.e.,

$$D(x + y) = Dx + Dy \qquad \text{and} \qquad D(xy) = xDy + yDx.$$

As an example of derivations, consider the polynomial ring $k[X]$ over a field k. For each variable X_i, the partial derivative $\partial/\partial X_i$ taken in the usual manner is a derivation of $k[X]$.

Let R be an entire ring and let K be its quotient field. Let $D: R \to R$ be a derivation. Then D extends uniquely to a derivation of K, by defining

$$D(u/v) = \frac{vDu - uDv}{v^2}.$$

It is immediately verified that the expression on the right-hand side is independent of the way we represent an element of K as u/v $(u, v \in R)$, and satisfies the conditions defining a derivation.

Note. In this section, we shall discuss derivations of fields. For derivations in the context of rings and modules, see Chapter XIX, §3.

A derivation of a field K is **trivial** if $Dx = 0$ for all $x \in K$. It is trivial **over a subfield** k of K if $Dx = 0$ for all $x \in k$. A derivation is always trivial over the prime field: One sees that

$$D(1) = D(1 \cdot 1) = 2D(1),$$

whence $D(1) = 0$.

We now consider the problem of extending derivations. Let

$$L = K(x) = K(x_1, \ldots, x_n)$$

be a finitely generated extension. If $f \in K[X]$, we denote by $\partial f/\partial x_i$ the polynomials $\partial f/\partial X_i$ evaluated at (x). Given a derivation D on K, does there exist a derivation D^* on L coinciding with D on K? If $f(X) \in K[X]$ is a polynomial vanishing on (x), then any such D^* must satisfy

$$0 = D^*f(x) = f^D(x) + \sum (\partial f/\partial x_i) D^*x_i, \tag{1}$$

where f^D denotes the polynomial obtained by applying D to all coefficients of f. Note that if relation (1) is satisfied for every element in a finite set of generators of the ideal in $K[X]$ vanishing on (x), then (1) is satisfied by every polynomial of this ideal. This is an immediate consequence of the rules for derivations. The preceding ideal will also be called the ideal determined by (x) in $K[X]$.

The above necessary condition for the existence of a D^* turns out to be sufficient.

Theorem 5.1. *Let D be a derivation of a field K. Let*

$$(x) = (x_1, \ldots, x_n)$$

be a finite family of elements in an extension of K. Let $\{f_\alpha(X)\}$ be a set of generators for the ideal determined by (x) in $K[X]$. Then, if (u) is any set of elements of $K(x)$ satisfying the equations

$$0 = f_\alpha^D(x) + \sum (\partial f_\alpha/\partial x_i)u_i,$$

there is one and only one derivation D^* of $K(x)$ coinciding with D on K, and such that $D^*x_i = u_i$ for every i.

Proof. The necessity has been shown above. Conversely, if $g(x)$, $h(x)$ are in $K[x]$, and $h(x) \neq 0$, one verifies immediately that the mapping D^* defined by the formulas

$$D^*g(x) = g^D(x) + \sum \frac{\partial g}{\partial x_i} u_i,$$

$$D^*(g/h) = \frac{hD^*g - gD^*h}{h^2},$$

is well defined and is a derivation of $K(x)$.

Consider the special case where (x) consists of one element x. Let D be a given derivation on K.

Case 1. x is separable algebraic over K. Let $f(X)$ be the irreducible polynomial satisfied by x over K. Then $f'(x) \neq 0$. We have

$$0 = f^D(x) + f'(x)u,$$

whence $u = -f^D(x)/f'(x)$. Hence D extends to $K(x)$ uniquely. If D is trivial on K, then D is trivial on $K(x)$.

Case 2. x is transcendental over K. Then D extends, and u can be selected arbitrarily in $K(x)$.

Case 3. x is purely inseparable over K, so $x^p - a = 0$, with $a \in K$. Then D extends to $K(x)$ if and only if $Da = 0$. In particular if D is trivial on K, then u can be selected arbitrarily.

Proposition 5.2. *A finitely generated extension $K(x)$ over K is separable algebraic if and only if every derivation D of $K(x)$ which is trivial on K is trivial on $K(x)$.*

Proof. If $K(x)$ is separable algebraic over K, this is Case 1. Conversely, if it is not, we can make a tower of extensions between K and $K(x)$, such

that each step is covered by one of the three above cases. At least one step will be covered by Case 2 or 3. Taking the uppermost step of this latter type, one sees immediately how to construct a derivation trivial on the bottom and nontrivial on top of the tower.

Proposition 5.3. *Given K and elements $(x) = (x_1, \ldots, x_n)$ in some extension field, assume that there exist n polynomials $f_i \in K[X]$ such that:*

(i) $f_i(x) = 0$, *and*
(ii) $\det(\partial f_i/\partial x_j) \neq 0$.

Then (x) is separably algebraic over K.

Proof. Let D be a derivation on $K(x)$, trivial on K. Having $f_i(x) = 0$ we must have $Df_i(x) = 0$, whence the Dx_i satisfy n linear equations such that the coefficient matrix has non-zero determinant. Hence $Dx_i = 0$, so D is trivial on $K(x)$. Hence $K(x)$ is separable algebraic over K by Proposition 5.2.

The following proposition will follow directly from Cases 1 and 2.

Proposition 5.4. *Let $K = k(x)$ be a finitely generated extension of k. An element z of K is in $K^p k$ if and only if every derivation D of K over k is such that $Dz = 0$.*

Proof. If z is in $K^p k$, then it is obvious that every derivation D of K over k vanishes on z. Conversely, if $z \notin K^p k$, then z is purely inseparable over $K^p k$, and by Case 3 of the extension theorem, we can find a derivation D trivial on $K^p k$ such that $Dz = 1$. This derivation is at first defined on the field $K^p k(z)$. One can extend it to K as follows. Suppose there is an element $w \in K$ such that $w \notin K^p k(z)$. Then $w^p \in K^p k$, and D vanishes on w^p. We can then again apply Case 3 to extend D from $K^p k(z)$ to $K^p k(z, w)$. Proceeding stepwise, we finally reach K, thus proving our proposition.

The derivations D of a field K form a vector space over K if we define zD for $z \in K$ by $(zD)(x) = zDx$.

Let K be a finitely generated extension of k, of dimension r over k. We denote by $\mathfrak{D}$ the K-vector space of derivations D of K over k (derivations of K which are trivial on k). For each $z \in K$, we have a pairing

$$(D, z) \mapsto Dz$$

of $(\mathfrak{D}, K)$ into K. Each element z of K gives therefore a K-linear functional of $\mathfrak{D}$. This functional is denoted by dz. We have

$$d(yz) = y\,dz + z\,dy,$$

$$d(y + z) = dy + dz.$$

These linear functionals form a subspace $\mathfrak{F}$ of the dual space of $\mathfrak{D}$, if we define $y\,dz$ by $(D, y\,dz) \mapsto yDz$.

Proposition 5.5. *Assume that K is a separably generated and finitely generated extension of k of transcendence degree r. Then the vector space $\mathfrak{D}$ (over K) of derivations of K over k has dimension r. Elements $t_1, \ldots, t_r$ of K from a separating transcendence base of K over k if and only if $dt_1, \ldots, dt_r$ form a basis of the dual space of $\mathfrak{D}$ over K.*

Proof. If $t_1, \ldots, t_r$ is a separating transcendence base for K over k, then we can find derivations $D_1, \ldots, D_r$ of K over k such that $D_i t_j = \delta_{ij}$, by Cases 1 and 2 of the extension theorem. Given $D \in \mathfrak{D}$, let $w_i = Dt_i$. Then clearly $D = \sum w_i D_i$, and so the D_i form a basis for $\mathfrak{D}$ over K, and the dt_i form the dual basis. Conversely, if $dt_1, \ldots, dt_r$ is a basis for $\mathfrak{F}$ over K, and if K is not separably generated over $k(t)$, then by Cases 2 and 3 we can find a derivation D which is trivial on $k(t)$ but nontrivial on K. If $D_1, \ldots, D_r$ is the dual basis of $dt_1, \ldots, dt_r$ (so $D_i t_j = \delta_{ij}$) then $D, D_1, \ldots, D_r$ would be linearly independent over K, contradicting the first part of the theorem.

Corollary 5.6. *Let K be a finitely generated and separably generated extension of k. Let z be an element of K transcendental over k. Then K is separable over $k(z)$ if and only if there exists a derivation D of K over k such that $Dz \neq 0$.*

Proof. If K is separable over $k(z)$, then z can be completed to a separating base of K over k and we can apply the proposition. If $Dz \neq 0$, then $dz \neq 0$, and we can complete dz to a basis of $\mathfrak{F}$ over K. Again from the proposition, it follows that K will be separable over $k(z)$.

Note. Here we have discussed derivations of fields. For derivations in the context of rings and modules, see Chapter XVI.

As an application, we prove:

Theorem 5.7. (Zariski–Matsusaka). *Let K be a finitely generated separable extension of a field k. Let $y, z \in K$ and $z \notin K^p k$ if the characteristic is $p > 0$. Let u be transcendental over K, and put $k_u = k(u)$, $K_u = K(u)$.*

(a) *For all except possibly one value of $c \in k$, K is a separable extension of $k(y + cz)$. Furthermore, K_u is separable over $k_u(y + uz)$.*

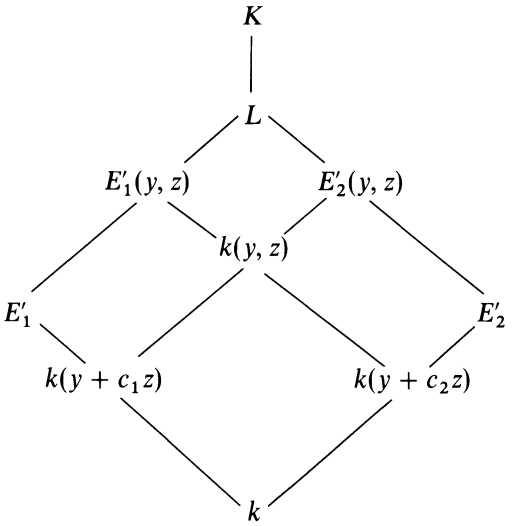
(b) *Assume that K is regular over k, and that its transcendence degree is at least 2. Then for all but a finite number of elements $c \in k$, K is a regular extension of $k(y + cz)$. Furthermore, K_u is regular over $k_u(y + uz)$.*

Proof. We shall use throughout the fact that a subfield of a finitely generated extension is also finitely generated (see Exercise 4).

If w is an element of K, and if there exists a derivation D of K over k such that $Dw \neq 0$, then K is separable over $k(w)$, by Corollary 5.6. Also by Corollary 5.6, there exists D such that $Dz \neq 0$. Then for all elements $c \in k$, except possibly one, we have $D(y + cz) = Dy + cDz \neq 0$. Also we may extend D to K_u over k_u by putting $Du = 0$, and then one sees that

$D(y+uz)= Dy + uDz \neq 0$, so K is separable over $k(y + cz)$ except possibly for one value of c, and K_u is separable over $k_u(y + uz)$. In what follows, we assume that the constants $c_1, c_2, \ldots$ are different from the exceptional constant, and hence that K is separable over $k(y + c_i z)$ for $i = 1, 2$.

Assume next that K is regular over k and that the transcendence degree is at least 2. Let $E_i = k(y + c_i z)$ $(i = 1, 2)$ and let E_i' be the algebraic closure of E_i in K. We must show that $E_i' = E_i$ for all but a finite number of constants. Note that $k(y, z) = E_1 E_2$ is the compositum of E_1 and E_2, and that $k(y, z)$ has transcendence degree 2 over k. Hence E_1' and E_2' are free over k. Being subfields of a regular extension of k, they are regular over k, and are therefore linearly disjoint by Theorem 4.12.



By construction, E_1' and E_2' are finite separable algebraic extensions of E_1 and E_2 respectively. Let L be the separable algebraic closure of $k(y, z)$ in K. There is only a finite number of intermediate fields between $k(y, z)$ and L. Furthermore, by Proposition 3.1 the fields $E_1'(y, z)$ and $E_2'(y, z)$ are linearly disjoint over $k(y, z)$. Let c_1 range over the finite number of constants which will exhaust the intermediate extensions between L and $k(y, z)$ obtainable by lifting over $k(y, z)$ a field of type E_i'. If c_2 is now chosen different from any one of these constants c_1, then the only way in which the condition of linear disjointness mentioned above can be compatible with our choice of c_2 is that $E_2'(y, z) = k(y, z)$, i.e. that $E_2' = k(y + c_2 z)$. This means that $k(y + c_2 z)$ is algebraically closed in K, and hence that K is regular over $k(y + c_2 z)$.

As for K_u, let $u_1, u_2, \ldots$ be infinitely many elements algebraically independent over K. Let $k' = k(u_1, u_2, \ldots)$ and $K' = K(u_1, u_2, \ldots)$ be the fields obtained by adjoining these elements to k and K respectively. By what has already been proved, we know that K' is regular over $k'(u + u_i z)$ for all but a finite number of integers i, say for $i = 1$. Our assertion (a) is then a consequence of Corollary 4.14. This concludes the proof of Theorem 5.7.

Theorem 5.8. *Let $K = k(x_1, \ldots, x_n) = k(x)$ be a finitely generated regular extension of a field k. Let $u_1, \ldots, u_n$ be algebraically independent over $k(x)$. Let*

$$u_{n+1} = u_1 x_1 + \cdots + u_n x_n,$$

and let $k_u = k(u_1, \ldots, u_n, u_{n+1})$. Then $k_u(x)$ is separable over k_u, and if the transcendence degree of $k(x)$ over k is $\geqq 2$, then $k_u(x)$ is regular over k_u.

Proof. By the separability of $k(x)$ over k, some x_i does not lie in $K^p k$, say $x_n \notin K^p k$. Then we take

$$y = u_1 x_1 + \cdots + u_{n-1} x_{n-1} \qquad \text{and} \qquad z = x_n,$$

so that $u_{n+1} = y + u_n z$, and we apply Theorem 5.7 to conclude the proof.

Remark. In the geometric language of the next chapter, Theorem 5.8 asserts that the intersection of a k-variety with a generic hyperplane

$$u_1 X_1 + \cdots + u_n X_n - u_{n+1} = 0$$

is a k_u-variety, if the dimension of the k-variety is $\geqq 2$. In any case, the extension $k_u(x)$ is separable over k_u.

EXERCISES

1. Prove that the complex numbers have infinitely many automorphisms. [*Hint*: Use transcendence bases.] Describe all automorphisms and their cardinality.

2. A subfield k of a field K is said to be algebraically closed in K if every element of K which is algebraic over k is contained in k. Prove: If k is algebraically closed in K, and K, L are free over k, and L is separable over k or K is separable over k, then L is algebraically closed in KL.

3. Let $k \subset E \subset K$ be extension fields. Show that

$$\text{tr. deg. } (K/k) = \text{tr. deg. } (K/E) + \text{tr. deg. } (E/k).$$

If $\{x_i\}$ is a transcendence base of E/k, and $\{y_j\}$ is a transcendence base of K/E, then $\{x_i, y_j\}$ is a transcendence base of K/k.

4. Let K/k be a finitely generated extension, and let $K \supset E \supset k$ be a subextension. Show that E/k is finitely generated.

5. Let k be a field and $k(x_1, \ldots, x_n) = k(x)$ a finite separable extension. Let $u_1, \ldots, u_n$ be algebraically independent over k. Let

$$w = u_1 x_1 + \cdots + u_n x_n.$$

Let $k_u = k(u_1, \ldots, u_n)$. Show that $k_u(w) = k_u(x)$.

6. Let $k(x) = k(x_1, \ldots, x_n)$ be a separable extension of transcendence degree $r \geqq 1$. Let u_{ij} $(i = 1, \ldots, r;\ j = 1, \ldots, n)$ be algebraically independent over $k(x)$. Let

$$y_i = \sum_{j=1}^{n} u_{ij} x_j.$$

Let $k_u = k(u_{ij})_{\text{all } i,j}$.

(a) Show that $k_u(x)$ is separable algebraic over $k_u(y_1, \ldots, y_r)$.

(b) Show that there exists a polynomial $P(u) \in k[u]$ having the following property. Let $(c) = (c_{ij})$ be elements of k such that $P(c) \neq 0$. Let

$$y_i' = \sum_{j=1}^{n} c_{ij} x_j.$$

Then $k(x)$ is separable algebraic over $k(y')$.

7. Let k be a field and $k[x_1, \ldots, x_n] = R$ a finitely generated entire ring over k with quotient field $k(x)$. Let L be a finite extension of $k(x)$. Let I be the integral closure of R in L. Show that I is a finite R-module. [Use Noether normalization, and deal with the inseparability problem and the separable case in two steps.]

8. Let D be a derivation of a field K. Then $D^n\colon K \to K$ is a linear map. Let $P_n = \operatorname{Ker} D^n$, so P_n is an additive subgroup of K. An element $x \in K$ is called a **logarithmic derivative** (in K) if there exists $y \in K$ such that $x = Dy/y$. Prove:

(a) An element $x \in K$ is the logarithmic derivative of an element $y \in P_n$ but $y \notin P_{n-1}$ $(n > 0)$ if and only if

$$(D + x)^n(1) = 0 \qquad \text{and} \qquad (D + x)^{n-1}(1) \neq 0.$$

(b) Assume that $K = \bigcup P_n$, i.e. given $x \in K$ then $x \in P_n$ for some $n > 0$. Let F be a subfield of K such that $DF \subset F$. Prove that x is a logarithmic derivative in F if and only if x is a logarithmic derivative in K. [*Hint*: If $x = Dy/y$ then $(D + x) = y^{-1}D \circ y$ and conversely.]

9. Let k be a field of characteristic 0, and let $z_1, \ldots, z_r$ be algebraically independent over k. Let (e_{ij}), $i = 1, \ldots, m$ and $j = 1, \ldots, r$ be a matrix of integers with $r \geqq m$, and assume that this matrix has rank m. Let

$$w_i = z_1^{e_{i1}} \cdots z_r^{e_{ir}} \qquad \text{for} \quad i = 1, \ldots, m.$$

Show that $w_1, \ldots, w_m$ are algebraically independent over k. [*Hint*: Consider the K-homomorphism mapping the K-space of derivations of K/k into $K^{(r)}$ given by

$$D \mapsto (Dz_1/z_1, \ldots, Dz_r/z_r),$$

and derive a linear condition for those D vanishing on $k(w_1, \ldots, w_m)$.]

10. Let k, (z) be as in Exercise 9. Show that if P is a rational function then

$$d(P(z)) = \operatorname{grad} P(z) \cdot dz,$$

using vector notation, i.e. $dz = (dz_1, \ldots, dz_r)$ and $\operatorname{grad} P = (D_1 P, \ldots, D_r P)$. Define $d \log P$ and express it in terms of coordinates. If P, Q are rational functions in $k(z)$ show that

$$d \log(PQ) = d \log P + d \log Q.$$