THE MINIMUM NUMBER OF GENERATORS FOR INSEPARABLE ALGEBRAIC EXTENSIONS[1]

M. F. BECKER AND S. MACLANE

1. Finite algebraic extensions of imperfect fields. A finite separable algebraic extension L of a given field K can always be generated by a single primitive element x, in the form $L=K(x)$. If K has characteristic p, while L/K is inseparable, there may be no such primitive element. The necessary and sufficient condition for the existence of such an element is to be found in Steinitz.[2] When there is no such primitive element, there is the question:[3] given K, what is the minimum integer m such that *every* finite extension L/K has a generation $L=K(x_1, x_2, \cdots, x_m)$ by not more than m elements?

The question can be answered by employing Teichmüller's[4] notion of the "degree of imperfection" of K. In invariant fashion, a field K of characteristic p determines a subfield K^p consisting of all pth powers of elements of K. If the extension K/K^p is finite, its degree $[K:K^p]$ is a power p^m of the characteristic, and the exponent m is called the *degree of imperfection* of K. For instance, let P be a perfect field of characteristic p and let x, y be elements algebraically independent with respect to P. Form the fields

$$S = P(x), \qquad T = P(x, y). \tag{1}$$

Then $S=S^p(x)$, $[S:S^p]=p$, while $[T:T^p]=p^2$, so that T is "more imperfect" than S.

THEOREM 1. *If the field K of characteristic p has a finite degree of imperfection m, then every finite algebraic extension $L \supset K$ can be obtained by adjoining not more than m elements to K. Furthermore, there exist finite extensions $L \supset K$ which cannot be obtained by adjoining fewer than m elements to K.*

PROOF. First consider the particular extension $K^{1/p}$ consisting of all pth roots of elements in K. Because of the isomorphism $a \longleftrightarrow a^{1/p}$,

$$[K^{1/p}:K] = [K:K^p] = p^m. \tag{2}$$

Each element y in $K^{1/p}$ satisfies over K an equation $y^p=a$ of degree p.

[1] Presented to the Society, October 28, 1939.

[2] E. Steinitz, *Algebraische Theorie der Körper*, Berlin, de Gruyter, 1930, p. 72.

[3] This problem was suggested to one of us by O. Ore.

[4] O. Teichmüller, *p-Algebren*, Deutsche Mathematik, vol. 1 (1936), pp. 362–388.

If $K^{1/p}$ had generators $y_1, \cdots, y_n$ in number less than m, the degree $[K^{1/p}:K]$ could not exceed p^n, a contradiction to (2).

An explicit generation for K/K^p can be found by successively choosing elements x_i of K such that each x_i is not in $K^p(x_1, \cdots, x_{i-1})$. Then each x_i satisfies an irreducible equation[5] $x_i^p = a_i$ over $K^p(x_1, \cdots, x_{i-1})$. The adjunction of x_i is an extension of degree p; so

$$(3) \qquad K = K^p(x_1, x_2, \cdots, x_m), \qquad [K:K^p] = p^m,$$

where m is the degree of imperfection[6] of K.

Now let L be any finite extension of K. Because of the isomorphism $a \longleftrightarrow a^p$, one has $[L:K] = [L^p:K^p]$. Hence

$$(4) \qquad [L:L^p] = [L:K]\cdot[K:K^p]/[L^p:K^p] = [K:K^p] = p^m.$$

Therefore K and L have the same degree of imperfection. But L has an explicit generation $L = L^p(y_1, \cdots, y_m)$ like that of (3). If L^{p^n} denotes the field of all p^nth powers of elements of L, the isomorphism $a \longleftrightarrow a^{p^n}$ yields $L^{p^n} = L^{p^{n+1}}(y_1^{p^n}, \cdots, y_m^{p^n})$. By an induction on n,

$$(5) \qquad L = L^{p^n}(y_1, \cdots, y_m).$$

Since L/K is finite, there is an integer n so large that for each y in L the power y^{p^n} is separable over K. The separable extension[7] $K(L^{p^n})/K$ has a single generator $K(L^{p^n}) = K(y_0)$. Since y_0 is separable, the usual theorem[8] of the primitive element yields a single element y' such that $K(y_0, y_1) = K(y')$. Thus, by (5),

$$L = K(y_0, y_1, y_2, \cdots, y_m) = K(y', y_2, \cdots, y_m).$$

This is a generation by m elements, as required.

The degree of imperfection of a field K may be *infinite*, in the sense that the extension K/K^p used in the definition is infinite. Our arguments in this case give the following result.

THEOREM 2. *If the degree of imperfection of a field K is infinite, then for each integer $n > 0$ there exists a finite algebraic extension $L \supset K$ which cannot be obtained by adjoining fewer than n elements to K.*

---

[5] For the usual properties of such equations, cf. A. A. Albert, *Modern Higher Algebra*, chap. 7.

[6] The set $\{x_1, \cdots, x_m\}$ of independent generators is called a *p-basis* for K. See O. Teichmüller, loc. cit., §3, or S. MacLane, *Modular fields*, I. *Separating transcedence bases*, Duke Mathematical Journal, vol. 5 (1939), pp. 372–393.

[7] Here $K(L^{p^n})$ denotes the field obtained from K by adjoining all elements of the field L^{p^n}.

[8] B. L. van der Waerden, *Moderne Algebra*, vol. 1, 1st edition, §34. Cf. also Steinitz, loc. cit., p. 72.

It might be thought that the minimum number of generators for an extension L/K is related to t, the transcendence degree of K over its maximum perfect subfield. However, this degree t may be larger than the degree of imperfection m. For a power series field K, Teichmüller observed that $m=1$, while t is infinite. Even when t and m are both finite, they can differ, as one of us showed by a more involved example[9] with $t=2$, $m=1$.

2. **Infinite algebraic extensions of imperfect fields.** In applying our criterion for the minimum number of generators one needs to compute the degree of imperfection of a given field. A perfect field contains pth roots of all of its elements, hence has degree of imperfection zero. A simple transcendental extension $K(t)$ has a degree of imperfection one greater than the degree of imperfection of K, as Teichmüller has proved (cf. also the examples (1)). On the other hand, the computation (4) proves the following theorem.

THEOREM 3. *The degree of imperfection of a field is not changed by a finite algebraic extension.*

There remains the case of an infinite algebraic extension L/K. Such an extension is purely inseparable (or, a "radical" extension) if for each element a of L some power a^{p^e} lies in K. In this case we have the following result.

THEOREM 4. *If K has a finite degree of imperfection m, then the degree of imperfection of a purely inseparable infinite extension of K is less than m, the degree of imperfection of K.*

Let L be a purely inseparable, infinite extension of K. We use a chain of intermediate fields

$$K \subset L_1 \subset L_2 \subset L_3 \subset \cdots \subset L_n \subset \cdots \subset L, \tag{6}$$

where L_n consists of all elements of L with p^nth power in K. The field L_{n+1} is obtained from L_n by adjoining pth roots of a sufficient number of elements of L_n. By (4), the degree of imperfection of each L_n is m. Hence, L_{n+1} is a field of degree at most p^m over L_n. Since $[L_n:K]$ is then finite, each L_{n+1} is larger than the preceding L_n.

By the definition of the tower (6), each $L_n \supset L_{n+1}^p$. Since $L^p \supset L_{n+1}^p$, any element α of L_n has over L_{n+1}^p a degree[10] $[\alpha:L_{n+1}^p] \geqq [\alpha:L^p]$. In other words,

---

[9] S. MacLane, loc. cit., §10.

[10] In fact, $[\alpha:L_{n+1}^p]=[\alpha:L^p]$. Since α is an element of L_n, $[\alpha:L_{n+1}^p]=p$ or 1, hence $[\alpha:L^p]=p$ or 1. If $[\alpha:L^p]=1$, $\alpha^{p^{-1}}$ is in L and $(\alpha^{p^{-1}})^{p^{n+1}}=\alpha^{p^n}$ is in K. Thus, by definition of L_{n+1}, $\alpha^{p^{-1}}$ is in L_{n+1}, so $[\alpha:L_{n+1}^p]=1$.

$$[L^p(L_n):L^p] \leqq [L_{n+1}^p(L_n):L_{n+1}^p].$$

But $L_{n+1}^p(L_n)=L_n$, while $L_{n+1}>L_n$ and $[L_{n+1}^p:L_n^p]>1$. Thus

$$[L^p(L_n):L^p] \leqq [L_n:L_{n+1}^p] < [L_n:L_{n+1}^p]\cdot[L_{n+1}^p:L_n^p] = [L_n:L_n^p].$$

This degree $[L_n:L_n^p]$ is simply p^m, with m the degree of imperfection of L_n; so

$$[L^p(L_n):L^p] \leqq p^{m-1}. \tag{7}$$

The maximum value of these degrees in (7) thus determines an integer $\delta \leqq m-1$ with

$$p^\delta = \max\,[L^p(L_n):L^p], \qquad \delta < m. \tag{8}$$

We assert that δ is the degree of imperfection of L. In the first place, $L \supset L^p(L_n)$; so $[L:L^p] \geqq [L^p(L_n):L^p]=p^\delta$, where we have so chosen n as to give the maximum in (8). If, however, $[L:L^p]$ exceeds p^δ, there must be $\delta+1$ elements $a_0, a_1, \cdots, a_\delta$ in L such that

$$[L^p(a_0, a_1, \cdots, a_\delta):L^p] = p^{\delta+1},$$

contrary to the definition (8) of δ. Thus δ, the degree of imperfection of L, is less than the corresponding degree of imperfection for K.

The degrees used in the computation (8) of δ can be expressed explicitly by choosing a p-basis $x_1, \cdots, x_m$ for each L_n, for then

$$[L^p(L_n):L^p] = [L^p(L_n^p(x_1, \cdots, x_m)):L^p] = [L^p(x_1, \cdots, x_m):L^p].$$

Consider now an infinite extension L/K which is not purely inseparable, and let M denote the field of all elements of L separable over K. Even if M/K is infinite, M and K still have the same degree of imperfection, according to a result of Teichmüller.[11] If the *exponent* of L is taken to be the least integer e such that all powers a^{p^e} of elements a in L are separable over K, we then have the following theorem.

THEOREM 5. *If K has a finite degree of imperfection, then an algebraic extension L of K has the same or a smaller degree of imperfection according as L has a finite or an infinite exponent over K.*

3. **Generators for given extensions.** In §1 we determined the minimum number of generators for all algebraic extensions of a fixed base field. Suppose, however, L is a specific extension of K. We wish to

[11] Any p-basis for K is also a p-basis for an arbitrary separable algebraic extension M of K; cf. Teichmüller, loc. cit., p. 170.

get the minimum number of generators for this particular extension. It clearly suffices to consider L a purely inseparable finite extension of K.

Whether the degree of imperfection of L is finite or infinite there is a subset U in L such that $L^p(U) = L$. By the same argument as in §1

$$L = L^{p^n}(U) \tag{9}$$

for integral n.

Consider, now, the field $L^p(K)$ between L and K. For L/K finite, $L/L^p(K)$ is finite and $[L:L^p(K)] = p^r$. Since the pth power of every element in L is contained in $L^p(K)$, r elements $X_1, X_2, \cdots, X_r$ in L can be chosen such that

$$L = L^p(K)(X_1, \cdots, X_r) = L^p(K, X_1, X_2, \cdots, X_r).$$

If e is the exponent of L/K, using (9) we obtain

$$L = L^{p^e}(K, X_1, \cdots, X_r) = K(X_1, X_2, \cdots, X_r),$$

Hence L/K can be generated by r elements.

Moreover, r is the minimum number of generators. For if $L = K(Y_1, \cdots, Y_s)$ where $s < r$,

$$L^p = K^p(Y_1^p, \cdots, Y_s^p), \qquad L^p(K) = K(Y_1^p, \cdots, Y_s^p),$$
$$p^r = [L:L^p(K)] = [K(Y_1, \cdots, Y_s):K(Y_1^p, \cdots, Y_s^p)] \leqq p^s,$$

and $r \leqq s$, against assumption.

THEOREM 6. *If L is a purely inseparable finite extension of K, the minimum number of generators of L/K is r, the exponent determined by the degree $[L:L^p(K)] = p^r$.*

NEW YORK, N.Y., AND
HARVARD UNIVERSITY