ON THE LINEAR INDEPENDENCE OF ALGEBRAIC NUMBERS

L. J. MORDELL

1. **Introduction.** Besicovitch [1] has proved by elementary methods involving only the concept of the irreducibility of equations the following:

THEOREM. *Let*

$$a_1 = b_1 p_1, \ a_2 = b_2 p_2, \cdots, a_s = b_s p_s ,$$

where $p_1, p_2, \cdots, p_s$ *are different primes, and* $b_1, b_2, \cdots, b_s$ *are positive integers not divisible by any of these primes. If* $x_1, x_2, \cdots, x_s$ *are positive real roots of the equations*

$$x^{n_1} - a_1 = 0, \ x^{n_2} - a_2 = 0, \cdots, x^{n_s} - a_s = 0,$$

and $P(x_1, x_2, \cdots, x_s)$ *is a polynomial with rational coefficients of degree less than or equal to* $n_1 - 1$ *with respect to* x_1, *less than or equal to* $n_2 - 1$ *with respect to* x_2, *and so on, then* $P(x_1 x_2, \cdots, x_s)$ *can vanish only if all its coefficients vanish.*

It is rather surprising that this has not been proved before, since results of this kind occur as particular cases of a general investigation in the theory of algebraic numbers, and some have been known for many years. We have the well-known general problem:

PROBLEM. Let K be an algebraic number field, and let $x_1, x_2, \cdots, x_s$ be algebraic numbers of degrees $n_1, n_2, \cdots, n_s$ over K. When does the field $K(x_1, x_2, \cdots, x_s)$ have degree $n_1 n_2 \cdots n_s$ over K?

This holds if either the degrees or the discriminants over K of the fields $K(x_1), K(x_2), \cdots, K(x_s)$ are relatively prime in pairs. The first part is a simple consequence of the usual theory of reducibility when $s = 2$, and the extension is obvious. The second part for $s = 2$ is given as Theorem 87 in Hilbert's report on algebraic number fields, and its proof depends on algebraic number

Received July 8, 1952.
Pacific J. Math. 3 (1953), 625-630

theory. The result for general s follows easily.

We discuss here the special case when $x_1, x_2, \cdots, x_s$ are specified roots of the respective equations

$$(1) \qquad x^{n_1} = a_1, x^{n_2} = a_2, \cdots, x^{n_s} = a_s,$$

where $a_1, a_2, \cdots, a_s$ are numbers in K. In the particular case when $n_1 a_1$, $n_2 a_2, \cdots, n_s a_s$ are relatively prime in pairs, the discriminants of the fields $K(x_1)$, $K(x_2), \cdots, K(x_s)$ are certainly relatively prime in pairs, and the foregoing conclusion holds. We consider two types of more general fields K. For the first, K and $x_1, x_2, \cdots, x_s$ are all real. For the second, K includes all the n_1th, n_2th, $\cdots$, n_sth roots of unity, and then the fields

$$K(x_1), K(x_2), \cdots, K(x_s)$$

are the so-called Kummer fields and have been known for many years. The elementary ideas used in their discussion are similar to those employed by Besicovitch. We have now the result really asked for in the problem, but stated as follows:

THEOREM. *A polynomial $P(x_1, x_2, \cdots, x_s)$ with coefficients in K and of degrees in $x_1, x_2, \cdots, x_s$, less than $n_1, n_2, \cdots, n_s$, respectively, can vanish only if all its coefficients vanish provided that the algebraic number field K is such that there exists no relation of the form*

$$(2) \qquad x_1^{\nu_1} x_2^{\nu_2} \cdots x_s^{\nu_s} = a,$$

where a is a number in K, unless

$$\nu_1 \equiv 0 \pmod{n_1}, \ \nu_2 \equiv 0 \pmod{n_2}, \cdots, \nu_s \equiv 0 \pmod{n_s}.$$

If K is of the first type, then a particular case, which includes the result of Besicovitch and is equivalent to it, arises when K is the rational number field, the x's are all real, the a's are integers, a_r $(r = 1, 2, \cdots, s)$ is exactly divisible by a prime power $p_r^{\alpha_r}$ (that is, by no higher power of p) with $(\alpha_r, n_r) = 1$, the p_r are all different, and p_r is prime to a_t when $r \neq t$. The condition implied in (2) is satisfied, as follows easily from the lemma below.

When K is of the second type, the theorem is given by Hasse [2], in the equivalent form that K includes all the nth roots of unity, where n is the least common multiple of $n_1, n_2, \cdots, n_s$. Hasse, however, is also investigating the relation of the Galois group of the field $K(x_1, x_2, \cdots, x_s)$ to those of $K(x_1)$, $K(x_2)$, and so on, and so his proof is not particularly elementary. In view of all this, an elementary proof of the theorem may be worth while.

2. **Lemma.** We prove first, for completeness, a well-known result:

LEMMA. *Let K be an algebraic number-field such that either K is real and the equation $x^n - a = 0$, where a is in K, has a real root, or K contains all the nth roots of unity. Then the equation $x^n - a = 0$ is reducible in K if and only if a is the Nth power of a number in K for some $N > 1$ dividing n. When K is of the first type, a real root is the root of an irreducible binomial equation in K. When K is of the second type, $x^n - a$ factorizes completely into binomial factors $x^m - b$ in K and irreducible in K.*

Proof. Let us suppose that $x^n - a = 0$ is reducible in K. Write it as

$$x^n - a = f(x)\, g(x),$$

where

$$f(x) = x^m + b_1 x^{m-1} + \cdots + b_m,$$

the b's are in K, and $f(x)$ is irreducible in K. When K is of the first type, we may suppose x', a specified real root of $x^n - a = 0$, is a root of $f(x) = 0$. All the roots of $f(x) = 0$ are roots of $x^n - a = 0$, and so they have the form $\epsilon' x'$, where ϵ' is an nth root of unity and x' is any specified root of $x^n - a = 0$, but the specified real root when K is of the first type. From the product of the roots of $f(x) = 0$,

$$x'^m = \pm\, \epsilon b_m,$$

where ϵ is an nth root of unity. Hence x' is also the root of an equation

$$x^m = b,$$

where b is in K since, for the first type, $\epsilon = \pm 1$. Hence the irreducible equation $f(x) = 0$ of degree m must be the same as the binomial equation $x^m - b = 0$.

Further, the equations $x^n - a = 0$, $x^m - b = 0$ have a common root. Write $d = (m, n)$, $n = dN$, $m = dM$, where $(N, M) = 1$ and $a^M = b^N$. There exist rational integers u, v such that $uM + vN = 1$. Then

$$a = a^{uM+vN} = (b^u a^v)^N,$$

where $N \mid n$. Conversely if $a = A^N$, where A is in K and $N \mid n$, the equation $x^n - a = 0$ is obviously reducible in K.

This proves the lemma.

3. **Proof of theorem.** The ideas involved are not essentially different from those of Besicovitch. The given conditions imply that the theorem holds for $s = 1$. It will be proved by induction on s, and so it may be assumed that no such relation as $P = 0$ holds for s or fewer roots of equations satisfying the given conditions. We then prove it for $s + 1$ roots. Suppose a relation such as

$$P(x_1, x_2, \cdots, x_{s+1}) = 0 \tag{3}$$

holds, so that x_1 is a root of the equation, supposed irreducible in K,

$$P_0 x^r + P_1 x^{r-1} + \cdots + P_r = 0, \tag{4}$$

where $P_0, P_1, \cdots, P_r$ are polynomials with coefficients in K, and of degrees in $x_2, x_3, \cdots, x_{s+1}$ respectively less than $n_2, n_3, \cdots, n_{s+1}$. Since $1/P_0$ can be expressed as a polynomial in $x_2, x_3, \cdots, x_{s+1}$ with coefficients in K, we may take $P_0 = 1$. We write

$$P_1 = P_1(x_2) = P_1(x_2, x_3, \cdots, x_{s+1}),$$

and so on, according to the variable occuring in P_1 which we wish to emphasize.

Each root of the equation (4) in x can be written as

$$x = \epsilon' x_1, \qquad \text{where } \epsilon'^{n_1} = 1.$$

Hence from the product of the roots of (4), x_1 is also a root of an equation

$$\epsilon x^r = \pm P_r, \qquad \text{where } \epsilon^{n_1} = 1,$$

Also $\epsilon = 1$ when the field K is of the first type. Write

$$X_1 = \epsilon x_1^r, \quad \text{and so} \quad X_1^{n_1} = a_1^r.$$

Then by the lemma, X_1 is a root of an equation irreducible in K,

$$X_1^{N_1} = A_1 ,$$

where A_1 is in K. Also,

$$(5) \qquad X_1 = \pm P_r = Q = Q(x_2) = Q(x_2, x_3, \cdots, x_{s+1}),$$

say. Hence the relation (3) is replaced, when the new variable X_1 is introduced, by the relation (5) which is in general simpler. The equation

$$(6) \qquad (Q(x))^{N_1} - A_1 = 0$$

has a root $x = x_2$; and since $x^{n_2} - a_2$ is irreducible in the field $K(x_3, x_4, \cdots, x_{s+1})$ by the hypothesis for s variables, each root of $x^{n_2} - a_2 = 0$, for example, the conjugate x_2' of x_2, must be a root of (6); so

$$Q(x_2') = X_1' ,$$

where X_1' is one of the conjugates of X_1 since $X^{N_1} - A_1$ is irreducible in K.

Now $X_1 = Q(x_2)$ is the root of the equation in $K(x_3, x_4, \cdots, x_{s+1})$,

$$F = (X - Q(x_2))\ (X - Q(x_2')) \cdots = 0,$$

where the product is extended to all the conjugates of x_2. Since all the roots of the equation $F = 0$ in X are conjugates of X_1, and since, by the hypothesis for s variables, $X^{N_1} - A_1$ is irreducible in $K(x_3, x_4, \cdots, x_{s+1})$, we must have

$$F = (X^{N_1} - A_1)^{M_1}$$

for some integer $M_1 > 0$, and so $n_2 = M_1 N_1$. Since $N_1 > 1$, on comparing coefficients of $X^{n_2 - 1}$, we obtain

$$(7) \qquad \sum Q(x_2') = 0, \ \sum X_1' = 0,$$

where the sum is extended over all the conjugates of x_2 and X_1, respectively. There are of course exactly M_1 conjugates of x_2 which give the same X_1.

Write now

$$X = Q(x) = B_0 x^{n_2 - 1} + B_1 x^{n_2 - 2} +, \cdots, + B_{n_2 - 1},$$

where $B_0 = B_0(x_3, x_4, \cdots, x_{s+1})$, and consider all the relations obtained by changing x into x_2 and all its conjugates. By addition, on noting (7), we get $B_{n_2-1} = 0$. Write now

$$X_1 / x_2 = X_1'.$$

Then by our condition and by our lemma, X_1' must be the root of an irreducible equation in K,

$$X'^{N'} = A',$$

and the conditions involved in (2) still hold. Proceeding as before, we get $B_{n_2-2} = 0$, and so on until $B_1 = 0$. By the theorem for s variables, a relation such as

$$X_1 / x_2^{n_2-1} = B_0$$

is impossible since $X_1 / x_2^{n_2-1}$ is the root of an irreducible binomial equation. This finishes the proof.

REFERENCES

1. Besicovitch, *On the linear independence of fractional powers of integers*, J. London Math. Soc. 15 (1940), 3-6.

2. Hasse, *Klassenkörpertheorie* (Mimeographed lectures, Marburg 1932-33), 187-195.

ST JOHN'S COLLEGE,
CAMBRIDGE, ENGLAND