Canad. Math. Bull. Vol. 17 (4), 1974

THE DEGREES OF RADICAL EXTENSIONS

BY
H. D. URSELL[1]

The results obtained here must have been known and settled centuries ago. However, they have proved impossible to locate in the available literature. H. K. Farahat has asked for proofs of the linear independence over the rationals of certain infinite sequences of real numbers such as $\sqrt{2}$, $\sqrt{3}$, $\sqrt{5}, \ldots$. He also raised the general question of determining the degree of the field extension generated over the rationals by a family of positive irrational numbers of the form $x=a^{1/m}$ where a, m are positive integers. We shall call such numbers *radical.* The *exponent* of a radical x is the least positive integer m such that x^m is a positive integer. We shall prove the following.

THEOREM. *Let $x_1, \ldots, x_n$ be radical numbers with exponents*[2] *$m_1, \ldots, m_n$. If the positive integers $x_1^{m_1}, \ldots, x_n^{m_n}$ are coprime then $x_1, \ldots, x_n$ generate a field extension of the rationals of degree $m_1m_2 \cdots m_n$.*

Proof. As usual, $[E:F]$ denotes the degree of the field extension E over F, $F(t_1, \ldots, t_r)$ denotes the field generated over F by the elements $t_1, \ldots, t_r$, and $\mathcal{Q}$ denotes the field of rational numbers. In addition, we set, for $\nu=1, 2, \ldots, n$, $x_\nu^{m_\nu}=a_\nu$ and $K_\nu=\mathcal{Q}(x_1, \ldots, x_{\nu-1}, x_{\nu+1}, \ldots, x_n)$; $K=\mathcal{Q}(x_1, \ldots, x_n)=K_\nu(x_\nu)$.

We shall prove that

$$(1) \qquad [K_\nu(x_\nu):K_\nu] = m_\nu$$

The theorem itself follows immediately from this by induction on n. Firstly, let us establish formula (1) in the case $n=1$. We have to see that the degree d of $\mathcal{Q}(x_1)$ over $\mathcal{Q}$ is equal to m_1. The d roots of the minimum polynomial $\mu(X)$ of x_1 over $\mathcal{Q}$ are roots of $X^{m_1}-a_1=X^{m_1}-x_1^{m_1}$, and consequently have absolute value x_1. Hence the absolute value of their product is $x_1^d=\pm\mu(0)$ which is a positive integer. Thus $d\geq m_1$, the exponent of x_1. But $\mu(X) \mid (X^{m_1}-a)$ implies that $d\leq m_1$. Hence $d=m_1$.

We prove (1), for general n, by contradiction. Suppose that (1) is not true in general, and choose a *minimal counter-example* $\{x_1, \ldots, x_n\}$ where minimality

[1] This paper was written by H. K. Farahat during March 1972, and is based on letters from H. D. Ursell, dating back almost exactly three years. The letters represent successive attempts at the problem amounting to the proofs given here. The facts established in this paper appear to be 'known' to many people. However their proofs do not seem to be readily available.

[2] Ursell's proof requires the exponents to be prime powers. The present version yields this stronger result (H. K. F.).

https://doi.org/10.4153/CMB-1974-114-x Published online by Cambridge University Press

is understood in the sense that n cannot be reduced and that no exponent m_ν can be reduced either. Note that therefore $n \geq 2$, and that

$$[K_\nu : \mathscr{Q}] = \prod_{\alpha \neq \nu} m_\alpha \tag{2}$$

because (1), and hence the theorem, holds for all smaller sets of radical elements. Furthermore, there exist values of $\nu(1 \leq \nu \leq n)$ such that

$$[K_\nu(x_\nu) : K_\nu] < m_\nu \tag{3}$$

Let ν be one such value and denote the degree of x_ν over K_ν by d_ν. By considering the constant term of the minimum polynomial of x_ν over K_ν we deduce, in a manner similar to a preceding argument, that $x_\nu^{d_\nu} \in K_\nu$. But we have also that $x_\nu^{m_\nu} = a_\nu \in K_\nu$, and consequently $x_\nu^h \in K_\nu$, where h is the highest common factor of d_ν, m_ν. If we replace x_ν by x_ν^h we obtain another counter-example where the exponent of x_ν^h is m_ν/h. By minimality of m_ν in our original counter-example we deduce that $h=1$, hence that $x_\nu \in K_\nu$, $d_\nu = 1$ and $K_\nu = K$. By (2) we see that

$$[K : \mathscr{Q}] = \prod_{\alpha \neq \nu} m_\alpha$$

It follows that (3) holds for *all* values of ν, because any value of ν yielding equality in (3) leads to $[K:\mathscr{Q}] = m_1 m_2 \cdots m_n$. Furthermore we now have

$$K_1 = K_2 = \cdots = K_n = K \tag{4}$$

We can now deduce from (2) that $m_1 = m_2 = \cdots = m_n = m$(say). The exponents in our minimal counter-example are therefore all equal. Let q be a prime factor of m and $m = qm'$. Then $\{x_1^{m'}, x_2, \ldots, x_n\}$ is also a counter-example with $x_1^{m'}$ having exponent $q \leq m$. Equality must hold by minimality, and consequently each x_ν has prime exponent q. Write $E = \mathscr{Q}(x_1, \ldots, x_{n-2})$. Then

$$E(x_n) = K = E(x_{n-1}), \; [K:E] = q.$$

For each element u of K we have its *trace*[3] in E, denoted by $T(u)$, and defined as usual as the trace of the E-linear mapping

$$z \in K \rightarrow uz \in K.$$

Since $\{1, x_{n-1}, x_{n-1}^2, \ldots, x_{n-1}^{q-1}\}$ and $\{1, x_n, x_n^2, \ldots, x_n^{q-1}\}$ are E-bases of K, there must exist j such that

$$T(x_n^j x_{n-1}) \neq 0, \qquad 0 \leq j \leq q-1.$$

But the trace of a linear transformation is also equal to the sum of roots of the characteristic polynomial. Now $x_n^j x_{n-1}$ is a root of the equation $X^q = a_n^j a_{n-1}$, and hence the roots of the corresponding characteristic polynomial are of the form

[3] Ursell does not make explicit use of the trace in his argument (H. K. F.).

https://doi.org/10.4153/CMB-1974-114-x Published online by Cambridge University Press

$\omega x_n^j x_{n-1}$ where ω is a qth root of unity. Thus E contains the element $T\{x_n^j x_{n-1}\}=\lambda x_n^j x_{n-1}\neq 0$ for some $\lambda\in E(e^{2\pi i/q})$. Consequently:

$$E(x_n^j x_{n-1})\subseteq E(e^{2\pi i/q}).$$

Now the right hand side has degree at most $q-1$ over E, because $e^{2\pi i/q}$ is a root of $X^{q-1}+X^{q-2}+\cdots+X+1=0$. Hence $E\{x_n^j x_{n-1}\}$ has degree *less* than q over E, and, since $a_1,\ldots,a_{n-2},a_n^j a_{n-1}$ are again coprime, we have a counter-example $\{x_1,\ldots,x_{n-2},x_n^j x_{n-1}\}$ of $n-1$ radical elements. This contradiction completes the proof.

Corollary. *Let $a_1,\ldots,a_n$ be coprime positive integers such that $\sqrt{a_1},\ldots,\sqrt{a_n}$ are irrational. Then $\mathcal{Q}[\sqrt{a_1},\ldots,\sqrt{a_n}]$ has degree 2^n over $\mathcal{Q}$.*

We can give a simple proof[4] of this Corollary independently of the main theorem. Write $F_\nu=\mathcal{Q}(\sqrt{a_1},\ldots,\sqrt{a_\nu})$ $(\nu\geq 0)$. Let n be the least positive integer, if such exist, for which a situation arises whereby $\sqrt{a_n}\in F_\nu$ for some ν, $0\leq\nu<n$ and choose ν minimal. Plainly $n\geq 1$, and we cannot have $\nu=0$ because $\sqrt{a_n}$ is irrational. We can find α, $\beta\in F_{\nu-1}$ such that

$$\sqrt{a_n}=\alpha+\beta\sqrt{a_\nu},$$

and, since ν is minimal, $\beta\neq 0$. Squaring the equation shows that $\beta\alpha\sqrt{a_\nu}\in\mathcal{Q}$. But $\sqrt{a_\nu}\notin F_{\nu-1}$. Thus $\alpha=0$, and $\sqrt{a_n}=\beta\sqrt{a_\nu}$, $\sqrt{(a_n a_\nu)}\in F_{\nu-1}$. This contradicts minimality of n because $a_1,\ldots,a_{\nu-1},a_\nu a_n,a_{\nu+1},\ldots,a_{n-1}$ are coprime. This contradiction proves that $[F_i:F_{i-1}]=2$ for all i and the result follows.

Appendix (H. K. F. 9 Feb. 1973)

I have recently run into several references dealing with the subject, and these are listed below.

1. A. Besikovitch, J. London Math. Society **15** (1940), 3–6.
2. L. J. Mordell, Pacific Journal of Math. **3** (1953), 625–630.
3. I. Kaplansky, *Fields and Rings*, Chicago University Press (1969) (page 60 et seq.).
4. R. L. Roth, American Mathematical Monthly, Vol. 78, No. 4, (1971), pp. 392–394.
5. L. Gaal, *Classical Galois Theory with examples*, Markham Publishing Co., Chicago (1971) (page 234).
6. American Mathematical Monthly (Comments) Vol. 78, No. 10, p. 1106 and Vol. 79, No. 10, p. 1102.

[4] This is due to P. Vamos.

https://doi.org/10.4153/CMB-1974-114-x Published online by Cambridge University Press