ADVANCES IN MATHEMATICS 13, 268–273 (1974)

An Application of Galois Theory to Elementary Arithmetic

IAN RICHARDS*†

University of Minnesota, Minneapolis, Minnesota 55455

1. INTRODUCTION

After the ancient result about the irrationality of $\sqrt[n]{m}$, it is natural to consider linear combinations of radicals, like the sum $\sqrt[4]{3} + \sqrt[5]{4} + \sqrt[8]{72}$. Are such expressions irrational whenever their terms do not obviously cancel out? An affirmative answer is given by the theorem which follows.

THEOREM 1. *Let $n > 1$ be any integer, $p_1, \ldots, p_k$ distinct positive primes, and $\sqrt[n]{p_i}$ the positive n-th root of p_i; Q denotes the field of rational numbers. Then the field $Q(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_k})$ is of degree n^k over Q.*

The field $Q(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_k})$ is spanned by rational linear combinations of products of the terms $\sqrt[n]{p_i}$, no single term being repeated more than $(n-1)$ times. Thus, an equivalent formulation of Theorem 1 is:

THEOREM 1a. *Let $\{e_i\}$ denote the set of n^k radicals,*

$$\sqrt[n]{p_1^{m(1)} \cdots p_k^{m(k)}}, \qquad 0 \leqslant m(i) < n, \quad 1 \leqslant i \leqslant k. \tag{1}$$

Then the set $\{e_i\}$ is linearly independent over Q. (Clearly $\{e_i\}$ spans $Q(\sqrt[n]{p_1}, \ldots, \sqrt[n]{p_k})$.)

Theorem 1a is due to Besicovitch [1]. His proof is based on a Euclidean algorithm for polynomials in several variables (one variable at a time being distinguished). The purpose of this note is to show that the result is an easy consequence of Galois theory. (We add that the problem for square-roots, $n = 2$, is significantly easier than the general case; cf. Section 4 or [4, 7].)

* Partially supported by NSF Grant GP 1236-1.

† The author wishes to thank Lisl Gaal for encouraging his interest in this subject through many stimulating discussions.

AMS Subject Classifications: Primary: 10F35, 12A35, 12A55, 12F10. Secondary: 10-01, 10N99, 12-01, 12L99.

Some numerical examples. Consider the number $\sqrt[4]{3} + \sqrt[5]{4} + \sqrt[6]{72}$ mentioned above. Set $n = 60$, $\{p_i\} = \{2, 3\}$, $k = 2$. After Theorem 1, the field generated by $\sqrt[60]{2}$ and $\sqrt[60]{3}$ is of degree 3600 over Q. A basis is given by the set of radicals $\sqrt[60]{2^a 3^b}$, $0 \leqslant a < 60$, $0 \leqslant b < 60$. Each of the elements 1, $\sqrt[4]{3}$, $\sqrt[5]{4}$, $\sqrt[6]{72}$ is of that form, and since all 3600 elements are linearly independent, so in particular are the four terms in question.

Similar reasoning shows that $\sqrt{5}$ does not belong to the field generated over Q by all the *real* nth roots of 2 and 3 (i.e., $\sqrt{5}$ is not expressible as a finite rational function of such roots).

Remark. These theorems fail if Q is replaced by the field R generated by the nth roots of unity (e.g., if $n = 5$, R contains $\sqrt{5}$; and the result would fail for $n = 10$.)

Rather strangely, these number-theoretic results have applications in other areas. For instance, R. Fateman used them in connection with the theory of algorithms and computer design (he also referred me to work of Caviness [2], who proved and applied the theorems for the case of odd n). L. Markus has recently found an application to differential algebra; using Theorem 1a, he shows that:

The countable set of functions $f_p(z) = \sum_{n=1}^{\infty} (p^{1/n}/n!)z^n$, where p runs through the set of primes, is "differentiably independent" over the field $Q(z)$ of rational functions with coefficients in Q. This implies independence over $C(z)$ also (C = complex numbers), roughly because complex constants satisfy the trivial differential equation $d\alpha/dz = 0$.

Standing notations. Let ω denote a primitive nth root of unity; R, E, F denote the extension fields $R = Q(\omega)$, $E = Q(p_1^{1/n}, \ldots, p_k^{1/n})$, $F = R(p_1^{1/n}, \ldots, p_k^{1/n})$.

2. Proof of Theorem 1 for Odd n

In order to avoid bothersome complications, we begin by taking n to be odd. Then the field Q can be replaced by R, i.e., $[F: R] = n^k$ (contrary to the remark made in Section 1).

Note. Of course $[F: R] = n^k$ implies $[E: Q] = n^k$, since the linear independence of $\{e_i\}$ over R implies independence over Q (compare Theorems 1 and 1a).

The first two lemmas which follow are well known (cf. [3]), but we

include them for the sake of completeness. It is worth mentioning that Lemma 2 involves the structure of the Galois groups (commutativity), and not just their degree.

LEMMA 1. *Take any field $F \supset R$, and any element $a \in F$. Then either* (1) *the polynomial $x^n - a$ is irreducible over F, or* (2) *there exists an integer $m \mid n$, $m > 1$, such that $\sqrt[m]{a} \in F$.*

Proof. Write $x^n - a = (x - \omega a^{1/n})(x - \omega^2 a^{1/n}) \cdots (x - a^{1/n})$ (over a suitable extension field). Then any nontrivial factor of $x^n - a$ in $F[x]$ must have a constant term $b \in F$ of the form $b = \omega^r a^{s/n}$, where $0 < s < n$. Let $m = n/(s, n)$. Choose integers u, v so that $us + vn = (s, n)$. Then $b^u a^v = \omega^t a^{1/m}$ (some t), and since $\omega \in R$, $a^{1/m} \in F$. Q.E.D.

LEMMA 2. *No irrational number of the form $\sqrt[m]{a}$, m odd, $a > 0 \in Q$, lies in any of the fields $Q(\sqrt[n]{1})$ generated by n-th roots of unity (n can be arbitrary).*

Proof. Without loss of generality we may assume that m is prime. Let ω denote a primitive mth root of unity. Then $a^{1/m} \notin Q(\omega)$, since the degree $[Q(a^{1/m}): Q] = m$, whereas $[Q(\omega): Q] = m - 1$. Thus, since m is prime, $x^m - a$ is irreducible over $Q(\omega)$, and $[Q(a^{1/m}, \omega): Q] = m(m - 1)$.

Now, a simple calculation shows that the Galois group of $Q(a^{1/m}, \omega)$ over Q is not abelian. For, since the degree is $m(m - 1)$, all the "plausible automorphisms" actually *are* automorphisms: thus let φ_1 map $a^{1/m}$ onto $\omega a^{1/m}$ and leave ω fixed, and let φ_2 map ω onto ω^2 leaving $a^{1/m}$ fixed. Then $\varphi_1\varphi_2(a^{1/m}) = \omega a^{1/m}$ and $\varphi_2\varphi_1(a^{1/m}) = \omega^2 a^{1/m}$.

On the other hand, $Q(\sqrt[n]{1})$ is a normal abelian extension of Q for all n. Q.E.D.

Remark. The same result holds for $\sqrt[4]{a}$, $a > 0 \in Q$, if $\sqrt{a}$ is irrational.

LEMMA 3 (The key step). *Assume that Theorems* 1 *and* 1a (*with Q replaced by R*) *hold for some fixed k. Take a prime p_{k+1} distinct from $p_1, \ldots, p_k$. Then, for any integer $m > 1$ which divides n, the following equation is impossible*:

$$\sqrt[m]{p_{k+1}} = \sum_{i=1}^{n^k} c_i e_i, \qquad c_i \in R. \tag{2}$$

(Recall that $\{e_i\}$ is defined in Theorem 1a *as the set of n^k "essentially distinct" radicals generated from $\sqrt[n]{p_1},\ldots,\sqrt[n]{p_k}$. By the induction hypothesis, $\{e_i\}$ is linearly independent over R.)*

Proof. There are two cases:

(A) There is only one coefficient $c_i \neq 0$. This contradicts Lemma 2. (Here we use the assumption that the p_i are distinct, and the elementary theorem about the irrationality of nth roots.)

(B) There are at least two terms $c_i, c_j \neq 0$. Then since $e_i/e_j \notin R$ (by the "induction hypothesis"), and since the field $F = R(p_1^{1/n},\ldots,p_k^{1/n})$ is a normal extension of R, there is an automorphism φ of F over R with $\varphi(e_i)/\varphi(e_j) \neq e_i/e_j$.

Now apply φ to (2). Since every e_h is the nth root of an integer, $\varphi(e_h) = \omega^{r(h)}e_h$ (with some $r(h)$) for each h. Likewise, $\varphi(\sqrt[m]{p_{k+1}}) = \omega^{r(0)} \cdot \sqrt[m]{p_{k+1}}$ for some $r(0)$. Furthermore $r(i) \not\equiv r(j) \pmod{n}$; that is, e_i and e_j are multiplied by different nth roots of unity under the action of φ. Since $\omega \in R$, this contradicts the assumed linear independence of $\{e_i\}$ over R. That proves the lemma.

Now, Theorems 1 and 1a (with Q replaced by R) follow by induction on k. It is convenient to start the induction with the vacuous case $k = 0$. This done, let $F = R(p_1^{1/n},\ldots,p_k^{1/n})$, and assume $[F\colon R] = n^k$. Lemmas 1 and 3 together imply that the polynomial $x^n - p_{k+1}$ is irreducible over F, whence $[F(\sqrt[n]{p_{k+1}})\colon F] = n$. Thus $[F(\sqrt[n]{p_{k+1}})\colon R] = n^{k+1}$. This completes the proof for odd n.

3. Proof for the Case Where n is Even

Here Q can no longer be replaced by R throughout, although a partial result is true ((3) below). The proof requires the use of intermediate fields S_g and T_g (with $g \geqslant k$ *fixed*). We shall only sketch the main steps. First define:

$$S_g = Q(p_1^{1/2},\ldots,p_g^{1/2}), \qquad \text{with} \quad g \geqslant k;$$

$$T_g = R(p_1^{1/2},\ldots,p_g^{1/2});$$

$$E^* = S_g(p_1^{1/n},\ldots,p_k^{1/n});$$

$$F^* = T_g(p_1^{1/n},\ldots,p_k^{1/n}).$$

Remarks. Since we have to do an induction on k, and yet want to hold the intermediate fields S_g and T_g fixed, we imagine a fixed sequence $p_1, \ldots, p_g$ of distinct primes with $g \geqslant k$. If $g = k$, then E^* and F^* become our original extension fields E and F. The point of all this is that the square roots have to be separated out (because Lemma 2 breaks down).

Now the proof for even n proceeds as in the odd case, except for the following modifications:

In *Lemma* 2, the field R is replaced by T_g. (The Galois group of T_g over Q is also abelian.) Moreover, the lemma is extended to include the case of $\sqrt[4]{a}$, $a > 0 \in Q$, $\sqrt{a}$ irrational.

In *Lemma* 3, the field R is again replaced by T_g, and $m \mid n$ is any integer >2. (Then either m has an odd factor, or $4 \mid m$.)

Lemma 1 is then applied to the polynomial $x^{n/2} - \sqrt{p_{k+1}}$.

One obtains the relations:

$$[F^*: T_g] = (n/2)^k \qquad \text{for all} \quad k \leqslant g. \tag{3}$$

$$[S_g: Q] = 2^g \qquad \text{for all } g. \tag{4}$$

[The proof of (3) is exactly similar to the proof of Theorem 1 for odd n, and (4) can be proved the same way (and more easily). There is also an elementary proof of (4) (cf. §4).]

$[F^*: T_g] = (n/2)^k$ implies $[E^*: S_g] = (n/2)^k$ (see the "Note" at the beginning of §2). And combining $[E^*: S_g] = (n/2)^k$ with $[S_g: Q] = 2^g$ (for $g = k$) gives Theorem 1.

4. Elementary Treatment of Square Roots

The crucial step, of course, is Lemma 3; and in the "nontrivial" case (B) we have:

$$\sqrt{p_{k+1}} = \Sigma c_i e_i, \qquad c_i \in Q,$$

with at least two nonzero terms.

There must be at least one p_i which occurs with different exponents (1/2 and 0) in this sum, and we can assume that this $p_i = p_k$ and obtain

$$\sqrt{p_{k+1}} = A + B\sqrt{p_k}, \qquad \text{where} \quad A, B \in Q(p_1^{1/2}, \ldots, p_{k-1}^{1/2}), \quad A, B \neq 0.$$

Squaring both sides gives $p_{k+1} = (A^2 + B^2 p_k) + 2AB\sqrt{p_k}$, whence $\sqrt{p_k} \in Q(p_1^{1/2}, \ldots, p_{k-1}^{1/2})$, contradicting the "induction hypothesis."

This proof does not generalize, even to $n = 3$.

References

1. A. S. Besicovitch, On the linear independence of fractional powers of integers, *J. London Math. Soc.* **15** (1940), 3–6.
2. B. F. Caviness, "On Canonical Forms and Simplifications," Thesis, Carnegie-Mellon Univ., Pittsburgh, 1967.
3. N. Chebotarev (Tschebotaröw), "Grundzüge der Galois'schen Theorie," Noordhoff, Groningen, 1950.
4. H. Flanders, (Solution of a problem proposed by D. J. Newman), *Amer. Math. Monthly* **67** (1960), 188–189.
5. L. Gaal, "Classical Galois Theory with Examples," Markham, Chicago, 1971, reprinted by Chelsea, New York.
6. L. J. Mordell, On the linear independence of algebraic numbers, *Pacific J.* **3** (1953), 625–630.
7. R. L. Roth, On extensions of Q by square roots, *Amer. Math. Monthly* **78** (1971), 392–393.