Delta 3 (1973), 11-15.

# NOTE ON EXTENSIONS OF THE RATIONALS BY SQUARE ROOTS

KENNETH S. WILLIAMS
*Carleton University, Ottawa, Canada*

Let $Q$ denote the field of rational numbers. In a recent note Roth [4] proved the following theorem.

**Theorem.** Let $p_1,\ldots,p_n$ be $n(\geqslant 1)$ distinct positive primes and let $s$ be a squarefree integer $>1$ with $p_i \nmid s$ ($i = 1,\ldots,n$). Then $\sqrt{s} \notin Q(\sqrt{p_1},\ldots,\sqrt{p_n})$.

Using this theorem we prove

**Theorem 1.** Let $s_1,\ldots,s_n$ be $n(\geqslant 1)$ distinct squarefree integers $> 1$. Then $1, \sqrt{s_1},\ldots,\sqrt{s_n}$ are linearly independent over $Q$.

**Theorem 2.** Let $s_1,\ldots,s_n$ be $n(\geqslant 1)$ squarefree integers $> 1$ and let $p_1,\ldots,p_m$ be the $m(\geqslant 1)$ distinct primes dividing $s_1 \ldots s_n$, so that for $j = 1,\ldots,n$ we have

$$s_j = p_1^{a_{1j}} \cdots p_m^{a_{mj}},$$

where each $a_{ij}$ ($i = 1,\ldots,m$; $j = 1,\ldots,n$) is 1 or 0 according as $p_i$ divides $s_j$ or not. Regarding the $a_{ij}$ as elements of $GF(2)$ we set

$$r(s_1,\ldots,s_n) = \operatorname{rank}_{GF(2)}(a_{ij})$$

Then

$$[Q(\sqrt{s_1}, \ldots, \sqrt{s_n}) : Q] = 2^{r(s_1, \ldots, s_n)} .$$

**Proof of Theorem 1.** Let $m$ be the number of distinct primes dividing $s_1 \ldots s_n$. If $m = 1$, then clearly $n = 1$, and $s_1$ is prime. In this case it is well-known that 1, $\sqrt{s_1}$ are linearly independent over $Q$. Thus the theorem is true when $m = 1$ and we proceed by induction on $m$, assuming $m \geqslant 2$.

Let $p$ be any prime dividing $s_1 \ldots s_n$. By relabelling $s_1, \ldots, s_n$ if necessary we can assume without loss of generality that $p$ divides the first $r$ of the $s_j$ (where $1 \leqslant r \leqslant n$) and does not divide the remaining $s_j$. For $j = 1, \ldots, r$ we set $s_j = pt_j$. Now let

$$\lambda_0 + \lambda_1\sqrt{s_1} + \ldots + \lambda_n\sqrt{s_n} = 0, \tag{4}$$

where $\lambda_0, \ldots, \lambda_n \in Q$. In order to prove that $1, \sqrt{s_1}, \ldots, \sqrt{s_n}$ are linearly independent over $Q$ it suffices to show that (4) implies $\lambda_0 = \lambda_1 = \ldots = \lambda_n = 0$. Using the notation above we can rewrite (4) as

$$\sqrt{p}(\lambda_1\sqrt{t_1} + \ldots + \lambda_r\sqrt{t_r}) = -\lambda_0 - \lambda_{r+1}\sqrt{s_{r+1}} - \ldots - \lambda_n\sqrt{s_n}. \tag{5}$$

If $\lambda_1\sqrt{t_1} + \ldots + \lambda_r\sqrt{t_r} \neq 0$, then (5) implies $\sqrt{p} \in Q(\sqrt{p_1}, \ldots, \sqrt{p_{k-1}})$, where $p_1, \ldots, p_{k-1}$ are the $k-1$ ( $\geqslant 1$ ) primes $\neq p$ which divide $s_1 \ldots s_n$. This is impossible by Roth's theorem and so we must have

$$\lambda_1\sqrt{t_1} + \ldots + \lambda_r\sqrt{t_r} = 0, \tag{6}$$

and so from (5) we deduce

$$\lambda_0 + \lambda_{r+1}\sqrt{s_{r+1}} + \ldots + \lambda_n\sqrt{s_n} = 0.$$

Now at most $k-1$ primes (namely those in the set $\{p_1, \ldots, p_{k-1}\}$)

divide $t_1 \ldots t_r$ and $t_1, \ldots, t_r$ are distinct square free integers and so $\sqrt{t_1}, \ldots, \sqrt{t_r}$ are linearly independent over $Q$. Hence from (6) we have $\lambda_1 = \ldots = \lambda_r = 0$. Similarly at most $k-1$ primes divide $s_{r+1} \ldots s_n$; and (7) shows that $\lambda_0 = \lambda_{r+1} = \ldots = \lambda_n = 0$. This completes the proof of the theorem.

**Proof of Theorem 2.** We begin by showing that $\sqrt{s_n} \in Q(\sqrt{s_1}, \ldots, \sqrt{s_{n-1}})$, where $n \geqslant 2$, if and only if $r(s_1, \ldots, s_{n-1}) = r(s_1, \ldots, s_n)$. Let $t_1, \ldots, t_h$ be the distinct maximal squarefree divisors of the products $s_{i_1} \ldots s_{i_k}$, where $1 \leqslant i_1 < \ldots < i_k \leqslant n-1$ and $k = 1, \ldots, n-1$. Then $Q(\sqrt{s_1}, \ldots, \sqrt{s_{n-1}})$ considered as a vectorspace over $Q$ has $\{1, \sqrt{t_1}, \ldots, \sqrt{t_h}\}$ as a basis. Thus $\sqrt{s_n} \in Q(\sqrt{s_1}, \ldots, \sqrt{s_{n-1}})$ if and only if $\sqrt{s_n}$ is a linear combination of $1, \sqrt{t_1}, \ldots, \sqrt{t_h}$ with coefficients in $Q$. Hence $1, \sqrt{t_1}, \ldots, \sqrt{t_h}, \sqrt{s_n}$ are linearly dependent over $Q$ and since the $t_i$ are distinct, by theorem 1 we must have $s_n = t_j$ for some $j$. Thus we have $t^2 s_n = s_{i_1} \ldots s_{i_k}$ for some $t \neq 0$ and integers $k, i_1, \ldots, i_k$ with $1 \leqslant k \leqslant r-1$ and $1 \leqslant i_1 < i_k \leqslant n-1$ Now for $l = 1, \ldots, n-1$ we define

$$x_l = \begin{cases} 1, \text{ if } l = i_r \text{ for some } r \text{ with } 1 \leqslant r \leqslant k, \\ 0, \text{ otherwise,} \end{cases}$$

and the condition $t^2 s_n = s_{i_1} \ldots s_{i_k}$ becomes $t^2\, s_n = s_1{}^{x_1} \ldots s_{n-1}{}^{x_{n-1}}$ that is

$$t^2 = p_1{}^{a_{11}x_1 + \cdots + a_{1n-1}x_{n-1} - a_{1n}} \cdots p_m{}^{a_{m1}x_1 + \cdots + a_{mn-1}x_{n-1} - ar_{mn}},$$

which is soluble for $x_1, \ldots, x_{n-1}$ and $t$ if and if only $r(s_1, \ldots, s_{n-1}) = r(s_1, \ldots, s_n)$.

We can now prove the theorem by induction. If $n = 1$ the result is clearly true as

$$r(s_1) = \operatorname{rank}_{GF(2)} \begin{bmatrix} 1 \\ 1 \\ \vdots \\ 1 \end{bmatrix} = 1,\ [Q(\sqrt{s_1}) : Q] = 2.$$

For $n \geqslant 2$ we assume that

$$[Q(\sqrt{s_1}, \ldots, \sqrt{s_{n-1}}) : Q] = 2^{r(s_1, \ldots, s_{n-1})}.$$

Then we have

$$[Q(\sqrt{s_1}, \ldots, \sqrt{s_n}) : Q] = [Q(\sqrt{s_1}, \ldots, \sqrt{s_n}) : Q(\sqrt{s_1}, \ldots, \sqrt{s_{n-1}})] \\ [Q(\sqrt{s_1}, \ldots, \sqrt{s_{n-1}}) : Q]$$

$$= \begin{cases} 2.2^{r(s_1, \ldots, s_{n-1})}, \text{ if } \sqrt{s_n} \notin Q(\sqrt{s_1}, \ldots, \sqrt{s_{n-1}}), \\ 2^{r(s_1, \ldots, s_{n-1})}, \text{ if } \sqrt{s_n} \in Q(\sqrt{s_1}, \ldots, \sqrt{s_{n-1}}), \end{cases}$$

$$= \begin{cases} 2^{r(s_1, \ldots, s_{n-1})+1}, \text{ if } r(s_1, \ldots, s_{n-1}) \neq r(s_1, \ldots, s_n), \\ 2^{r(s_1, \ldots, s_{n-1})}, \text{ if } r(s_1, \ldots, s_{n-1}) = r(s_1, \ldots, s_n), \end{cases}$$

$$= 2^{r(s_1, \ldots, s_n)},$$

as $r(s_1, \ldots, s_n) = r(s_1, \ldots, s_{n-1}) + 1$ when $r(s_1, \ldots, s_{n-1}) \neq (s_1, \ldots, s_n)$.

The theorem now follows by induction.

We remark that the results of this note are well known (see for example [2]). More general results have been given by A. S. Besicovich [1] and L.J. Mordell [3].

### Acknowledgement

I would like to thank Dr. J. D. Dixon for his simplifications of my original proofs of theorems 1 and 2, and also Dr. R. Fischler and Mr. J. W. Lawrence for helpful discussions in connection with the preparation of this note.

## REFERENCES

1. **A. S. Besicovich**, On the linear independence of fractional powers of integers, Jour. Lond. Math. Soc. 15 (1940), 3–6.

2. **L. Gaal**. Classical Galois Theory, Markham Publishing Co., 1971.

3. **L. J. Mordell**. On the linear independence of fractional powers of integers, Pacific J. Math. 3 (1953), 625.

4. **R. L. Roth**, On extensions of Q by square-roots, Amer'. Math. Monthly 78 (1971), 392--393.