Linearly Independent Integer Roots over the Scalar Field $\mathbb{Q}$

Eric Jaffe

July 12, 2007

It is easy to show that certain integer roots are irrational; the numbers $\sqrt{2}$ and $\sqrt[3]{4}$ are good examples. An equivalent statement is that the sets $\{1, \sqrt{2}\}$ and $\{1, \sqrt[3]{4}\}$, respectively, are linearly independent over the scalar field $\mathbb{Q}$.

Furthermore, it can be shown that $\sqrt{3} + \sqrt{2}$ is irrational, and that $q\sqrt{3} + r\sqrt{2}$ is irrational for all $q, r \in \mathbb{Q}$. In fact, we can say that $\{1, \sqrt{2}, \sqrt{3}\}$ is linearly independent over $\mathbb{Q}$.

In this paper we will generalize the above notions. First, we aim to determine for which integers ρ and $n > 0$ the set $\{1, \sqrt[n]{\rho}\}$ is linearly independent over $\mathbb{Q}$. We can do this quickly by employing Lemma 2, which is a critical insight concerning the prime numbers due to Euclid. Theorem 3 shows that $\{1, \sqrt[n]{\rho}\}$ is linearly independent exactly when ρ is not the nth power of some integer.

Lemma 1. *Let a be an integer, and p a prime. If p does not divide a then* $\gcd(p, a) = 1$.

Proof. We have $\gcd(p, a)|p$, so $\gcd(p, a) = 1$ or $\gcd(p, a) = p$ since p is prime. But by assumption p does not divide a, and $\gcd(p, a)$ does, so we must have $\gcd(p, a) = 1$. □

Lemma 2. *Let $a_1, a_2, \ldots, a_n$ be integers, and p a prime. If $p|a_1 a_2 \cdots a_n$ then there is some i, $1 \le i \le n$, such that $p|a_i$.*

Proof. The Lemma is clear for $n = 1$, so assume that it holds for $n - 1$.

Suppose that p does not divide a_1. Then $\gcd(p, a_1) = 1$ by Lemma 1. Hence there exist integers r, s such that

$$1 = ps + a_1 r.$$

It follows that

$$a_2 a_3 \cdots a_n = p a_2 a_3 \cdots a_n s + a_1 a_2 a_3 \cdots a_n r.$$

But p divides both terms on the right, so $p|a_2 a_3 \cdots a_n$. In particular, p divides one of $a_2, \ldots, a_n$ by the inductive hypothesis. This completes the proof. □

Theorem 3. *Let $\rho \neq 0$ and $n > 0$ be integers. The set $\{1, \sqrt[n]{\rho}\}$ is linearly independent over $\mathbb{Q}$ if and only if ρ is not the nth power of some integer.*

Proof. Suppose first that $\rho = \sigma^n, \sigma \in \mathbb{Z}$ (if n is even then let σ be positive). Then

$$1 - \frac{1}{\sigma} \sqrt[n]{\rho} = 0$$

is a nontrivial linear combination of 1 and $\sqrt[n]{\rho}$ with rational coefficients, so $\{1, \sqrt[n]{\rho}\}$ is linearly dependent.

Conversely, suppose $\{1, \sqrt[n]{\rho}\}$ is linearly dependent over $\mathbb{Q}$. Then there exist integers a and $b > 0$, with $\gcd(a, b) = 1$, such that $\rho = (a/b)^n$. Hence

$$\rho b^n = a^n.$$

In particular, this shows that $b|a^n$. Therefore if p is some prime that divides b, then p also divides a^n. It follows from Lemma 2 that $p|a$, which is impossible since $\gcd(a,b) = 1 < p$. Therefore b must have no prime divisors, so it must be that $b = 1$ and $\rho = a^n$. $\square$

This question of linear independence generalizes to larger sets of numbers, and in this paper we will answer a broader question involving sets of square roots. For example, the claim that $\{1, \sqrt{a_1}, \sqrt{a_2}, \ldots, \sqrt{a_n}\}$ is linearly independent over $\mathbb{Q}$ immediately implies that all numbers of the form

$$x_0 + x_1\sqrt{a_1} + x_2\sqrt{a_2} + \cdots + x_n\sqrt{a_n}$$

are irrational whenever $x_0, x_1, \ldots, x_n \in \mathbb{Q}$. The next theorem provides a class of $a_1, a_2, \ldots, a_n$ for which this is the case.

Theorem 4. *The set*

$$\mathcal{S} := \{\sqrt{n} : n \textit{ is a squarefree positive integer}\}$$

is linearly independent over $\mathbb{Q}$*.*

Note that an integer is **squarefree** if its prime factorization contains no prime more than once. The sequence of squarefree integers is

$$1, 2, 3, 5, 6, 7, 10, 11, 13, 14, 15, 17, 19, 21, \ldots$$

In order to prove Theorem 4, we shall use the concept of field extensions. If F_1 is a subfield of F_2, written $F_1 \leq F_2$, then we shall say that F_2 over F_1 is a **field extension**. We use the shorthand F_2/F_1 to refer to F_2 as a field extension over F_1, although such notation has nothing to do with quotient groups.

When F_2/F_1 is a field extension one can consider F_2 as a vector space over the scalar field F_1. We write $[F_2 : F_1]$ to denote the dimension of this space; this number is also called the **degree** of F_2/F_1. It can be shown that degrees are "multiplicative in towers"—that is, if $F_1 \leq F_2 \leq F_3$ then

$$[F_3 : F_1] = [F_3 : F_2][F_2 : F_1].$$

Finally, if F_2/F_1 is a field extension and $K \subset F_2$, then $F_1(K)$ is the smallest subfield of F_2 which contains K and is an extension of F_1. For example, when $\mathbb{Q}$ is considered as a subfield of $\mathbb{R}$,

$$\begin{aligned}
\mathbb{Q}(\sqrt{2}) &= \{a + b\sqrt{2} : a, b \in \mathbb{Q}\}; \\
\mathbb{Q}(\{\sqrt{2}, \sqrt{3}\}) = (\mathbb{Q}(\sqrt{2}))(\sqrt{3}) &= \{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b \in \mathbb{Q}\} \\
&= \{a + b\sqrt{3} : a, b \in \mathbb{Q}(\sqrt{2})\}.
\end{aligned}$$

We shall now prove the following Lemma. Observe that Lemma 5 implies Theorem 4, since for any finite subset $T \subset \mathcal{S}$ of squarefree positive integers, we can find a suitable set $\mathcal{A}_n$ such that $T = \mathcal{B}_n$ ($\mathcal{A}_n$ and $\mathcal{B}_n$ are defined below).

Lemma 5. *Suppose that* $\mathcal{A}_n := \{\rho_1, \rho_2, \ldots, \rho_n\} \subset \mathbb{Z}_+$ *is a set of positive integers such that no* $\rho_i \in \mathcal{A}_n$ *is the square of any integer, and every pair of elements in* $\mathcal{A}_n$ *is relatively prime. Then the set*

$$\mathcal{B}_n := \{\sqrt{\sigma_1\sigma_2\cdots\sigma_n} : 0 \leq k \leq n; \textit{each } \sigma_i \textit{ is a distinct element of } \mathcal{A}_n\}$$

is a basis of the space $\mathbb{Q}(\sqrt{\rho_1}, \sqrt{\rho_2}, \ldots, \sqrt{\rho_n})$ *over the scalar field* $\mathbb{Q}$*. (Note that* $\mathcal{B}_n$ *has exactly* 2^n *elements, corresponding to the power set of* $\mathcal{A}_n$*.)*

Proof. The proof is by induction on n. Suppose that ρ is a positive integer that is not a perfect square. Then $\{1, \sqrt{\rho}\}$ certainly spans $\mathbb{Q}(\sqrt{\rho})$, since every element of the latter is of the form $a+b\sqrt{\rho}$ for $a, b \in \mathbb{Q}$. Linear independence follows from Theorem 3. Hence the Lemma holds for $n = 1$. The Lemma also holds for $n = 0$, since $\{1\}$ is a basis of $\mathbb{Q}/\mathbb{Q}$.

Now suppose the Lemma holds for $n-1$ and $n-2$ and define the fields

$$\begin{aligned}
F_0 &:= \mathbb{Q} \\
F_1 &:= \mathbb{Q}(\sqrt{\rho_1}) \\
F_2 &:= F_1(\sqrt{\rho_2}) = \mathbb{Q}(\sqrt{\rho_1}, \sqrt{\rho_2}) \\
&\vdots \\
F_n &:= F_{n-1}(\sqrt{\rho_n}) = \mathbb{Q}(\sqrt{\rho_1}, \dots, \sqrt{\rho_n}).
\end{aligned}$$

By the induction hypothesis we have $[F_{n-1} : F_0] = 2^{n-1}$ since $\mathcal{B}_{n-1}$ is a basis of F_{n-1}/F_0. Let $\beta_1, \beta_2, \dots, \beta_{2^{n-1}}$ be the 2^{n-1} distinct elements of $\mathcal{B}_{n-1}$. Since $\{1, \sqrt{\rho_n}\}$ spans F_n/F_{n-1}, and then since $\mathcal{B}_{n-1}$ spans F_{n-1}/F_0, every element $x \in F_n$ can be written as

$$\begin{aligned}
x &= a_1 + a_2\sqrt{\rho_n}, && a_1, a_2 \in F_{n-1} \\
&= \sum_{k=1}^{2^{n-1}} b_k\beta_k + \sqrt{\rho_n} \sum_{k=1}^{2^{n-1}} b_{2^{n-1}+k}\beta_k, && b_1, \dots, b_{2^n} \in F_0 \\
&= \sum_{k=1}^{2^{n-1}} b_k\beta_k + \sum_{k=1}^{2^{n-1}} b_{2^{n-1}+k}(\beta_k\sqrt{\rho_n}).
\end{aligned}$$

But the 2^n numbers $\{\beta_1, \dots, \beta_{2^{n-1}}, \beta_1\sqrt{\rho_n}, \dots, \beta_{2^{n-1}}\sqrt{\rho_n}\}$ are exactly the elements of $\mathcal{B}_n$, so we conclude that $\mathcal{B}_n$ spans F_n/F_0 and $[F_n : F_0] \leq 2^n$.

It remains to show that $\mathcal{B}_n$ is linearly independent. This will now follow immediately if we can show that $[F_n : F_0] = 2^n$ (since $\mathcal{B}_n$ spans F_n/F_0, if it were linearly dependent then we could discard elements to obtain a basis of $< 2^n$ elements, which would be a contradiction). And degrees are multiplicative in towers, so it suffices to show that $[F_n : F_{n-1}] = 2$.

Suppose not. Then we must have $[F_n : F_{n-1}] = 1$, which means that F_n and F_{n-1} are the same field; in particular, $\sqrt{\rho_n} \in F_{n-1}$. Since $\{1, \sqrt{\rho_{n-1}}\}$ spans F_{n-1}/F_{n-2}, there exist scalars $a, b \in F_{n-2}$ such that

$$a + b\sqrt{\rho_{n-1}} = \sqrt{\rho_n}.$$

That is,

$$a^2 + 2ab\sqrt{\rho_{n-1}} + b^2\rho_{n-1} = \rho_n.$$

Now if $ab \neq 0$, then this would give an expression for $\sqrt{\rho_{n-1}}$ in terms of scalars in F_{n-2}. But $[F_{n-1} : F_{n-2}] = 2 \neq 1$ by the inductive hypothesis, so we must have $\sqrt{\rho_{n-1}} \notin F_{n-2}$ and therefore $ab = 0$. Since F_{n-2} is a field this means that either $a = 0$ or $b = 0$.

If $a = 0$ then we have $b\rho_{n-1} = \sqrt{\rho_n\rho_{n-1}}$, which implies that $\sqrt{\rho_n\rho_{n-1}} \in F_{n-2}$. Now $\rho_n\rho_{n-1}$ is not the square of any integer since ρ_n and ρ_{n-1} are relatively prime, so this contradicts the inductive hypothesis when applied to $\mathcal{A}_{n-1} = \{\rho_1, \rho_2, \dots, \rho_{n-2}, \rho_n\rho_{n-1}\}$. Similarly, if $b = 0$ then we have $\sqrt{\rho_n} \in F_{n-2}$, which contradicts the inductive hypothesis when applied to $\mathcal{A}_{n-1} = \{\rho_1, \rho_2, \dots, \rho_{n-2}, \rho_n\}$.

Therefore $\mathcal{B}_n$ is linearly independent over $\mathbb{Q}$, so it is a basis of F_n/F_0, as desired. $\square$