A question on linear independence of square roots

Martin Klazar[1]

August 17, 2009

Jakub Tomek, student in my calculus class, raised the following question. How can one show that the square roots of distinct squarefree numbers are linearly independent over the rationals? That is, we want to prove that if the k integers $0 < n_1 < n_2 < \cdots < n_k$ are squarefree (a number is called squarefree if it is a products of mutually distinct prime numbers) and

$$a_1\sqrt{n_1} + a_2\sqrt{n_2} + \cdots + a_k\sqrt{n_k} = 0, \quad a_i \in \mathbb{Q},$$

then $a_1 = a_2 = \cdots = a_k = 0$. We give a proof here; our aim is to use as little commutative algebra as possible. Then we mention some references.

If such nontrivial linear dependence exists, for example,

$$a_1\sqrt{2\cdot 17} + a_2\sqrt{5\cdot 11\cdot 13} + a_3\sqrt{3\cdot 17} + a_4\sqrt{1} = 0$$

with all $a_i \in \mathbb{Q}$ and nonzero, we single out any of the primes involved and express its root rationally in terms of the roots of the other primes:

$$\sqrt{17} = -\frac{a_2\sqrt{5}\cdot\sqrt{11}\cdot\sqrt{13} + a_4}{a_1\sqrt{2} + a_3\sqrt{3}},$$

for example. If division was illegal, it means that $a_1\sqrt{2} + a_3\sqrt{3} = 0$ and we replace the original linear dependence with this simpler one and repeat the argument. After finitely many steps we end up with a relation

$$\sqrt{p_k} \in \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_{k-1}})$$

where $p_1, p_2, \ldots, p_k$, $k \geq 1$, are distinct prime numbers, that is, $\sqrt{p_k}$ expresses rationally in terms of the roots $\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_{k-1}}$. We show that such relation is impossible.

Let us have a closer look at the displayed notation for field adjunction which really means $\mathbb{Q}(\{\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_{k-1}}\})$. If $X \subset \mathbb{R}$ is any set of real numbers then $\mathbb{Q}(X)$ is by definition the smallest (to inclusion) subfield of the

[1]klazar@kam.mff.cuni.cz

field $\mathbb{R}$ containing the set $\mathbb{Q} \cup X$. In more practical terms, it is easy to see that the field $\mathbb{Q}(X)$ consists exactly of the elements

$$\frac{\sum_i a_i x_i}{\sum_i b_i y_i}, \quad a_i, b_i \in \mathbb{Q},$$

where every x_i and y_i is a product of (possibly repeating) elements from X (for empty products are x_i, y_i equal to 1). We fix an element of X, say α, and set $X' = X \backslash \{\alpha\}$. Taking α out we rewrite the sums in the denominator and numerator as

$$\frac{c_0 + c_1\alpha + c_2\alpha^2 + \cdots + c_k\alpha^k}{d_0 + d_1\alpha + d_2\alpha^2 + \cdots + d_l\alpha^l}, \quad c_i, d_i \in \mathbb{Q}(X').$$

If $\alpha^2 \in \mathbb{Q}$ then, as $\alpha^i \in \mathbb{Q}$ for even i and $\alpha^i = \alpha^{i-1}\alpha$, $\alpha^{i-1} \in \mathbb{Q}$, for odd i, we can simplify the sums to

$$\frac{a + b\alpha}{c + d\alpha}, \quad a, b, c, d \in \mathbb{Q}(X').$$

Multiplying the denominator and numerator by $c - d\alpha$ (which is nonzero unless $\alpha \in \mathbb{Q}(X')$), we get

$$\frac{(a + b\alpha)(c - d\alpha)}{(c + d\alpha)(c - d\alpha)} = \frac{ac - bd\alpha^2}{c^2 - d^2\alpha^2} + \frac{bc - ad}{c^2 - d^2\alpha^2} \cdot \alpha = a' + b'\alpha, \quad a', b' \in \mathbb{Q}(X').$$

To summarize, if $X = X' \cup \{\alpha\}$ is any set of real numbers and $\alpha^2 \in \mathbb{Q}$, then $\mathbb{Q}(X)$ consists exactly of the elements

$$a + b\alpha, \quad a, b \in \mathbb{Q}(X').$$

(If $\alpha \in \mathbb{Q}(X')$, we may set always $b = 0$.)

Now we state and prove a result showing that relations like

$$\sqrt{p_k} \in \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_{k-1}}), \quad p_1 < p_2 < \cdots < p_k \text{ all prime},$$

are impossible. We introduce a notation. If $\alpha_1, \alpha_2, \ldots$ is an infinite sequence of real numbers and $I \subset \mathbb{N}$, where $\mathbb{N} = \{1, 2, 3, \ldots\}$, is a finite set, we write

$$\alpha(I) = \prod_{i \in I} \alpha_i \quad \text{and} \quad \mathbb{Q}([I]) = \mathbb{Q}(\{\alpha_i \mid i \in I\}).$$

Then $\alpha(\emptyset) = 1$ (empty product) and $\mathbb{Q}([\emptyset]) = \mathbb{Q}$.

Proposition. *Let $\alpha_1, \alpha_2, \ldots$ be real numbers such that $\alpha(I) \notin \mathbb{Q}$ for every finite and nonempty set $I \subset \mathbb{N}$ (in particular, no α_i is in $\mathbb{Q}$) but every square α_i^2 is in $\mathbb{Q}$. Then for every two finite sets $I, J \subset \mathbb{N}$ with $I \neq \emptyset$ and $I \cap J = \emptyset$ we have*

$$\alpha(I) \notin \mathbb{Q}([J]).$$

Proof. We proceed by contradiction and take a minimum counterexample, which is a membership

$$\alpha(I) \in \mathbb{Q}([J]),$$

where I, J are finite and disjoint subsets of $\mathbb{N}$, $I \neq \emptyset$ and *the cardinality of J is minimum.* By the assumption on α_i, the set J is nonempty as well. We take arbitrary index $l \in J$ and set $J' = J \backslash \{l\}$. As we noted above,

$$\alpha(I) = a + b\alpha_l, \quad a, b \in \mathbb{Q}([J']).$$

Squaring gives

$$2ab\alpha_l = \alpha(I)^2 - a^2 - b^2\alpha_l^2.$$

By the assumption on α_i, the right side is in $\mathbb{Q}([J'])$. We distinguish three cases. For $ab \neq 0$ division by $2ab$ in the last equality shows that $\alpha_l = \alpha(\{l\}) \in \mathbb{Q}([J'])$, which is a smaller counterexample. If $b = 0$ then again $\alpha(I) = a \in \mathbb{Q}([J'])$ is a smaller counterexample. Finally, in the last and crucial case when $a = 0$ we have $\alpha(I) = b\alpha_l$. Multiplying by α_l, we get

$$\alpha(I \cup \{l\}) = \alpha(I)\alpha_l = b\alpha_l^2 \in \mathbb{Q}([J'])$$

(note that $l \notin I$), which is again a smaller counterexample. We have contradiction in all three cases. □

The sequence $\alpha_i = \sqrt{p_i}$, where

$$p_1 = 2 < p_2 = 3 < p_3 = 5 < \ldots$$

is the sequence of all prime numbers, satisfies the assumption because $\alpha(I) = \sqrt{p(I)}$, $I \neq \emptyset$, is always irrational. Thus $\sqrt{p_k} \notin \mathbb{Q}(\{\sqrt{p_j} \mid j \in J\})$ if $k \notin J$, in fact even $\sqrt{p(I)} \notin \mathbb{Q}(\{\sqrt{p_j} \mid j \in J\})$ if $I \neq \emptyset$ and $I \cap J = \emptyset$ (but the cases

$|I| = 1$ and $|I| \geq 1$ are in fact equivalent), and the original question on linear independence of roots is answered.

As for the references, inspection of the memory and (manual!) search of the library first revealed that the textbooks by Hlawka, Schoißengaier and Taschner [4, Exercise 7 to Chapter 2] and Laczkovich [5, Exercises 4.2 and 4.3] contain the original question as an exercise. They give no references but the former book mentions useful key words "Besicovitch's theorem". It is then a short way to a proof and nice discussion by Dubuque [3] and the original paper [1] by Besicovitch. Many more references pertaining to the topic now could be added, containing illustrious names like Mordell or Siegel, but we leave them for the really interested reader to find and restrict only to two, the recent article by Carr and O'Sullivan [2] and the note by Roth [6] which contains proof almost identical to the one presented above.

References

[1] A. S. Besicovitch, On the linear independence of fractional powers of integers, *J. London Math. Soc.* 15 (1940) 3–6.

[2] R. Carr and C. O'Sullivan, On the linear independence of roots, *Int. J. Number Theory* 5 (2009) 161–171. [available in ArXiv]

[3] B. Dubuque, discussion on Math Forum, February 2004, available at `http://groups.google.com/group/sci.math/msg/ef2809b124af8930`

[4] E. Hlawka, J. Schoißengaier and R. Taschner, *Geometric and Analytic Number Theory*, Springer, 1986.

[5] M. Laczkovich, *Conjecture and Proof*, TypoTEX, Budapest, 1998.

[6] R. L. Roth, Classroom notes: On extensions of Q by square roots, *Amer. Math. Monthly* 78 (1971) 392–393.