FEATURE

10

MY FAVORITE PROBLEM

Linear Independence of Radicals

Iurie Boreico[†]
Harvard University '11
Cambridge, MA 02138
boreico@fas.harvard.edu

The problem I intend to discuss here was mentioned in the prior *HCMR*—in particular, author Zachary Abel [Ab, p. 79] stated that "the set $\{\sqrt{n} \mid n \in \mathbb{N} \text{ is squarefree}\}$ is linearly independent over rationals." More formally:

Problem. *Let $n_1, n_2, \ldots, n_k$ be distinct squarefree integers. Show that if $a_1, a_2, \ldots, a_k \in \mathbb{Z}$ are not all zero, then the sum $S = a_1\sqrt{n_1} + a_2\sqrt{n_2} + \ldots + a_k\sqrt{n_k}$ is non-zero.*

Note that this problem is equivalent to Abel's statement, since we may clear denominators to obtain coefficients in $\mathbb{Z}$.

10.1 Preliminary Analysis

By setting $A_i = a_i^2 n_i$, the problem can be restated as follows: if

$$\sum_{i=1}^{k} \pm\sqrt{A_i} = 0,$$

then at least one of the expressions A_i/A_j must be a perfect square. Indeed, in our case none of the expressions $A_i/A_j = (a_i/a_j)^2 n_i/n_j$ is a perfect square, so the sum

$$a_1\sqrt{n_1} + a_2\sqrt{n_2} + \ldots + a_k\sqrt{n_k} = \sum_{i=1}^{k} \pm\sqrt{A_i}$$

must not be zero. The converse follows similarly.

In this form, the problem can be tackled for small values of k by simply squaring. For example, if $k = 2$, we have $\sqrt{A_1} - \sqrt{A_2} = 0$, so $\sqrt{A_1} = \sqrt{A_2}$. Squaring gives $A_1 = A_2$ and thus $A_1/A_2 = 1$, which is a perfect square. If $k = 3$ we have WLOG that $\sqrt{A_1} = \pm\sqrt{A_2} + \sqrt{A_3}$, and so again squaring gives $A_1 = A_2 + A_3 \pm 2\sqrt{A_2A_3}$. Hence $\sqrt{A_2A_3} = \pm(A_2 + A_3 - A_1)/2$, which implies $A_2A_3 = (A_2 + A_3 - A_1)^2/4$ is a perfect square, and so

$$\frac{A_2}{A_3} = \frac{A_2A_3}{A_3^2} = \left(\frac{A_2 + A_3 - A_1}{2A_3}\right)^2.$$

For $k = 4$ we may rewrite the problem as $\pm\sqrt{A_1} \pm \sqrt{A_2} = \pm\sqrt{A_3} \pm \sqrt{A_4}$. Then by squaring we have $A_1 + A_2 - A_3 - A_4 \pm 2\sqrt{A_1A_2} \pm 2\sqrt{A_3A_4} = 0$ and we handle this using the previously established case $k = 3$.

[†]Iurie Boreico, Harvard '11, is a prospective mathematics concentrator residing in Weld. His mathematical knowledge is yet too vague to define his interests, but they tend towards number theory. When not doing math, he usually misses his home country, Moldova, or wastes his time in some other way.

Unfortunately, this approach does not extend to $k > 4$, for however we rearrange the given expressions, squaring only *increases* the number of radicals. In fact, as an olympiad-style problem, this problem is very hard, and probably very few would be successful in solving it. With enough patience and creativity, however, several solutions are possible.

10.2 Solutions

Solution 1 from [Kv]. Let $p_1, p_2, \ldots, p_N$ be all the primes dividing $n_1 n_2 \cdots n_k$. We will prove the following statement by induction on N:

Recall that $S = a_1\sqrt{n_1} + a_2\sqrt{n_2} + \ldots + a_k\sqrt{n_k}$. Then there exists an expression $S' = b_1\sqrt{m_1} + b_2\sqrt{m_2} + \ldots + b_l\sqrt{m_l}$ where $m_1, m_2, \ldots, m_l$ are squarefree integers with prime factors among the $p_1, p_2, \ldots, p_N$ and b_i are integers, such that SS' is a non-zero integer (in particular, $S \neq 0$, as desired).

For $N = 0$ this is obvious, as in this case $k = 1, n_1 = 1$ and we get $S = a_1 \neq 0$ so we can set $S' = 1$. For $N = 1$ we either have $S = a_1\sqrt{p_1}$, in which case we may let $S' = \sqrt{p_1}$, or we have $S = a_1\sqrt{p_1} + a_2$. In the last case we may take $S' = -a_1\sqrt{p_1} + a_2$, so $SS' = a_2^2 - a_1^2 p_1$. This is non-zero as a_2^2 is divisible by an even power of p_1, whereas $a_1^2 p_1$ is divisible by an odd power of p_1, so the two cannot be equal.

Now we perform the induction step. Assume that the theorem is true for $N \leq n$; we prove it for $N = n + 1$. Let $p_N = p_{n+1} = p$. We may write $S = S_1 + S_2\sqrt{p}$ where the primes appearing in the radicals in S_1, S_2 are among $p_1, \ldots, p_n$, and further, neither S_1 nor S_2 is identically 0 (else we would already be done, as p would be irrelevant). So there exists a sum S_2' of the form given in the claim such that $S_2 S_2'$ is a non-zero integer k.

The intermediate product SS_2' can then be written as $S_4 + k\sqrt{p}$ where the primes appearing in the radicals in S_4 are also among $p_1, \ldots, p_n$. We may thus multiply it by $S_4 - k\sqrt{p}$ to get $S_4^2 - k^2 p$. Finally, it is easy to see that all prime factors of radicals of $S_4^2 - k^2 p$ are among $p_1, \ldots, p_n$, so, assuming this number is not itself zero, the induction hypothesis implies that there exists a non-zero weighted sum of radicals S_5 whose prime factors appear among $p_1, p_2, \ldots, p_n$ such that $(S_4^2 - k^2 p)S_5$ is a non-zero integer. So we obtain the desired representation $SS_2'(S_4 - k\sqrt{p})S_5 \in \mathbb{Z} \setminus \{0\}$ where $S' = S_2'(S_4 - k\sqrt{p})S_5$ is a sum of radicals of the desired type.

Thus, we are done if we manage to prove we do not run into trouble when multiplying $S_4 - k\sqrt{p}$, as the product could become zero at that step (e.g. if $S_4 - k\sqrt{p} = 0$). It is sufficient to prove that $S_4^2 - k^2 p \neq 0$. If S_4 is an integer this is clear, and if S_4 is of form $u\sqrt{q}$ this also true because $u^2 q \neq k^2 p$, as p does not divide q. Otherwise, S_4 contains at least two distinct radicals in its canonical expression (if we consider $\sqrt{1}$ as a radical),[1] and we can assume without loss of generality that p_n appears in one of these two radicals but not in the other. So $S_4 = S_6 + S_7\sqrt{p_n}$ where S_6, S_7 are sums of radicals with prime factors among $p_1, p_2, \ldots, p_{n-1}$, and $S_6, S_7 \neq 0$. Therefore $S_4^2 - k^2 p = S_6^2 + 2S_6 S_7\sqrt{p_n} + S_7^2 p_n - k^2 p$. As $S_6 S_7 \neq 0$, by expanding the expression $S_4^2 - k^2 p$ we will get at least one radical containing p_n. But then by the induction hypothesis, the expression is non-zero as claimed. □

This solution, even if it might seem somewhat unnatural and tedious, is completely logical in its construction. By starting from the well-known idea of multiplication by a conjugate (the case $N = 1$ above), the idea is to actually produce a sort of "conjugate" expression for more complicated sums involving radicals, *i.e.* something involving the same radicals which when multiplied by the original produces an integer. The (somewhat unappealing) induction step is just a set of technical manipulations that help realize this idea.

[1] By the canonical representation of an expression involving radicals we mean its simplest possible form—that is, the form obtained by extracting the squares out of the radicals and grouping together the terms which have the same square-free numbers under the radicals. For example, $(\sqrt{2} + \sqrt{10})^2 = 2 + 2\sqrt{2} \cdot \sqrt{10} + 10$ would be brought to $2 + 4\sqrt{5} + 10 = 12 + 4\sqrt{5}$. The statement of the problem is just the fact that the canonical representation is indeed "canonical," that is, the same number can not be written as such a sum in two different ways (otherwise subtracting the two expressions would produce a counterexample).

If one takes as a starting point the mentioned idea of conjugate expressions, one might consider the following question:

Question. *What is the expression conjugate to* $\sqrt{a_1}+\sqrt{a_2}+\ldots+\sqrt{a_n}$*?*

We know that for $n=2$ the conjugate is $\sqrt{a_1}-\sqrt{a_2}$. Of course we could have chosen some other combination of signs, like $-\sqrt{a_1}-\sqrt{a_2}$ or $-\sqrt{a_1}+\sqrt{a_2}$, but we do not get anything new from them, as these two expression are just the original ones with the opposite sign. Given this example, we might thnk that the expression $\sqrt{a_1}+\sqrt{a_2}+\ldots+\sqrt{a_n}$ has many conjugates, and that they represent all expressions of form $\pm\sqrt{a_1}\pm\sqrt{a_2}\pm\ldots\pm\sqrt{a_n}$ for all combinations of pluses and minuses. Again, we need to ensure that the same expression does not occur twice, the second time with opposite sign, which can be realized by requiring that the sign of $\sqrt{a_1}$ is always positive. We get a family of 2^{n-1} alike sums: $\sqrt{a_1}\pm\sqrt{a_2}\pm\sqrt{a_3}\pm\ldots\pm\sqrt{a_n}$. This might suggest that the product of this entire family could in fact be the required non-zero integer we sought in Solution 1, but unfortunately while it is indeed possible that this product is an integer, there is no obvious way to handle this huge expression directly and prove that it is non-zero.

These considerations inspire the next solution:

Solution 2. Consider the linear expression $L(x_1,x_2,\ldots,x_n)=a_1x_1+a_2x_2+\ldots+a_nx_n$. We will also consider its conjugate expressions of form $L'(x_1,x_2,\ldots,x_n)=a_1x_1\pm a_2x_2\pm a_3x_3\pm\ldots\pm a_nx_n$. There are 2^{n-1} such expressions. Now take a variable T and consider the polynomial

$$F_{L,x_1,x_2,\ldots,x_n}(T)=\prod_{L'}\left(T-L'(x_1,x_2,\ldots,x_n)\right)=\prod\left(T-a_1x_1\pm a_2x_2\pm\ldots\pm a_nx_n\right),$$

where the product is taken over all conjugate expressions L' (including L).

Note that $F_{L,x_1,x_2,\ldots,x_n}(T)$ is written as a polynomial in T, but can be considered as a polynomial in $x_1,x_2,\ldots,x_n$. Also note that changing the signs of any of $x_2,x_3,\ldots,x_n$ will not affect F because doing so only permutes the set $\{L'\}$. Therefore

$$F_{L,x_1,x_2,\ldots,x_n}(T)=F_{L,x_1,\pm x_2,\pm x_3,\ldots,\pm x_n}(T).$$

In particular, if we expand the product representation of F into a sum of monomials, each monomial term will contain only even powers of x_k ($k=2,\ldots,n$), because otherwise changing the sign of x_k would change the sign of the monomial. Note that this is not true for x_1, as doing so sends the set $\{L'\}$ to the set $\{-L'\}$. But by expanding F into a sum of monomials and grouping the monomials with odd and even powers of x_1 we can write

$$F_{L,x_1,x_2,\ldots,x_n}(T)=x_1P(x_1^2,x_2,x_3,\ldots,x_n,T)+Q(x_1^2,x_2,x_3,\ldots,x_n,T).$$

As we have seen above, P and Q do involve only monomials with even powers of $x_2,x_3,\ldots,x_n$, and so they depend only on $x_2^2,x_3^2,\ldots,x_n^2$. So we can actually write

$$F_{L,x_1,x_2,\ldots,x_n}(T)=x_1P_2(x_1^2,x_2^2,x_3^2,\ldots,x_n^2,T)+Q_2(x_1^2,x_2^2,x_3^2,\ldots,x_n^2,T).$$

It is also clear that if a_i are integers then all the coefficients of P and Q will be integers.

Now let us return to the problem. We actually prove a different version of it: that is, that no non-zero integer M can be represented as a nontrivial canonical sum of radicals. To see that this implies the original problem, assume that $\sum_{i=1}^{k}a_i\sqrt{n_i}=0$. Then, by multiplying by $\sqrt{n_k}$, we get $\sum_{i=1}^{k-1}a_i\sqrt{n_in_k}=-a_kn_k$, which is a contradiction if we prove that no non-zero integer can be represented as a canonical sum of radicals. So let us prove this version, by induction on k. The base case, $k=1$, is clear.

If we assume that an expression of form $a_1\sqrt{n_1}+a_2\sqrt{n_2}+\ldots+a_k\sqrt{n_k}$ equals $M\in\mathbb{Z}\setminus\{0\}$, then the polynomial $F_{L,\sqrt{n_1},\sqrt{n_2},\ldots,\sqrt{n_k}}(T)$ would vanish at $T=M$. But we saw the polynomial can be written simply as

$$\sqrt{n_1}P_2(n_1,n_2,\ldots,n_k,T)+Q_2(n_1,n_2,\ldots,n_k,T),$$

so we would have $\sqrt{n_1}P_2(n_1, n_2, \ldots, n_k, M) + Q_2(n_1, n_2, \ldots, n_k, M) = 0$. But $P_2(n_1, \ldots, n_k, T)$ and $Q_2(n_1, \ldots, n_k, T)$ are integers. By the base case, $A+B\sqrt{n_1} = 0$ implies $A = B = 0$, so we have

$$P(n_1, n_2, \ldots, n_k, M) = Q(n_1, n_2, \ldots, n_k, M) = 0.$$

Hence,

$$-\sqrt{n_1}P(n_1, n_2, \ldots, n_k, M) + Q(n_1, n_2, \ldots, n_k, M) = 0,$$

i.e. $F_{M,-\sqrt{n_1},\sqrt{n_2},\ldots,\sqrt{n_k}}(M) = 0$. Thus,

$$\prod(M + a_1\sqrt{n_1} \pm a_2\sqrt{n_2} \pm a_3\sqrt{n_3} \pm \ldots \pm a_k\sqrt{n_k}) = 0,$$

and so $M = -a_1\sqrt{n_1} \pm a_2\sqrt{n_2} \pm \ldots \pm a_k\sqrt{n_k}$ for some combination of signs. However, we already have $M = a_1\sqrt{n_1} + a_2\sqrt{n_2} + \ldots + a_k\sqrt{n_k}$, and summing these two equalities gives

$$2M = (a_2 \pm a_2)\sqrt{n_2} + (a_3 \pm a_3)\sqrt{n_3} + \ldots + (a_k \pm a_k)\sqrt{n_k}.$$

This cannot happen by the induction hypothesis, and we have reached our contradiction. □

10.3 Further Ideas

Now I will explain why I like this problem. The essential reason is that the solutions hint at many important concepts in algebra and number theory. let us talk about some of them:

The primitive element theorem. The primitive element theorem states that any finite separable field extension L/K contains a primitive element, *i.e.* an element that generates the whole extension. This problem allows us to explicitly find a primitive element (in fact many of them) for the extension $\mathbb{Q}[\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_k}]/\mathbb{Q}$, where $p_1, p_2, \ldots, p_k$ are distinct primes.

The field $\mathbb{Q}[\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_k}]$ consists of all combinations $\sum a_i\sqrt{n_i}$ where $a_i \in \mathbb{Q}$ and $n_1, n_2, \ldots, n_{2^k}$ are all possible products that can be formed with $p_1, p_2, \ldots, p_k$. As we have proven that $\sqrt{n_1}, \sqrt{n_2}, \ldots, \sqrt{n_k}$ are independent over $\mathbb{Q}$, it follows that the degree of the extension over $\mathbb{Q}$ is 2^k. Thus to find a primitive element means to find an element θ in $\mathbb{Q}[\sqrt{p_1}, \ldots, \sqrt{p_k}]$ which is a root of an irreducible polynomial of degree 2^k. We claim our friend $\sqrt{p_1} + \sqrt{p_2} + \ldots + \sqrt{p_k}$ (or any of its conjugates) can be taken as θ.

Assume $P \in \mathbb{Q}[X]$ and $P(\theta) = 0$, with P irreducible over $\mathbb{Q}$. We can expand each power of θ in $P(\theta)$ and write it as a sum of radicals, and then combine these radicals to obtain $P(\theta) = a_1\sqrt{n_1} + a_2\sqrt{n_2} + \ldots + a_{2^k}\sqrt{n_k}$. The results proven above tell us that $P(\theta) = 0$ if and only if all a_i are 0. Let us take now a conjugate of θ, say $\theta' = \epsilon_1\sqrt{p_1} + \epsilon_2\sqrt{p_2} + \ldots + \epsilon_k\sqrt{p_k}$ where $\epsilon_i \in \{-1, 1\}$. We claim $P(\theta') = 0$. Indeed, if we expand θ'^k, the coefficient of $\sqrt{n_i}$ will either be the same as the coefficient of $\sqrt{n_i}$ in θ^k, or it will be the additive inverse of that coefficient, depending on how many of p_j with $\epsilon_j = -1$ divide $\sqrt{n_i}$. We thus get $P(\theta') = \sum_i a_i\mu_i\sqrt{n_i}$ where $\mu_i = \prod_{p_j|n_i} \epsilon_j$. As all a_i are zero, we get $P(\theta') = 0$. Hence P has as roots all the conjugates of $\pm\theta$, of which there are 2^k, so P has degree at least 2^k. In fact it must have degree 2^k because θ lies in an extension of degree 2^k, so θ is indeed a primitive element.

It is also clear now that $P(X) = \prod_{\epsilon_i \in \{-1,1\}}(X - \epsilon_1\sqrt{p_1} - \epsilon_2\sqrt{p_2} - \ldots - \epsilon_k\sqrt{p_k})$. The fact that this polynomial has rational coefficients follows from the fact that

$$P(X) = F_{L,\sqrt{p_1},\sqrt{p_2},\ldots,\sqrt{p_k}}(X) \cdot F_{L,-\sqrt{p_1},\sqrt{p_2},\ldots,\sqrt{p_k}}(X)$$

(we keep the notations of Solution 2) and this has integer coefficients from Solution 2.

The degree of extensions of radicals. We noted above that $[\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_k}) : \mathbb{Q}] = 2^k$ when $p_1, p_2, \ldots, p_k$ are distinct primes. It would be interesting to show that $[\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_k}) : \mathbb{Q}] = 2^k$ with a constraint weaker than that p_i be primes. The degree of this extension is trivially at most 2^k, but it may be less than that. For example we might have $\sqrt{p_3} \in \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2})$ if $\sqrt{p_3} = m\sqrt{p_1p_2}$, where $m \in \mathbb{Q}$, in which case adjoining p_3 would not alter the extension. We

will prove that these are exactly the "uncomfortable" cases. Namely, let us take from $p_1, p_2, \ldots, p_k$ a maximal sequence $p_1, \ldots, p_l$ which is multiplicatively independent, by which we mean that the product of any nonempty subset of elements in the sequence is not a perfect square. More explicitly, $p_1, p_2, \ldots, p_l$ is multiplicatively independent, but for any $j > l$, there exist $1 \leq i_1, \ldots, i_r \leq l$ such that $p_j p_{i_1} p_{i_2} \cdots p_{i_r} = a^2$ is a perfect square. This means

$$\sqrt{p_j} = \frac{a}{p_{i_1} p_{i_2} \ldots p_{i_r}} \sqrt{p_{i_1} p_{i_2} \cdots p_{i_r}} \in \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_l}),$$

and so $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_l}, \sqrt{p_j}) = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_l})$. It is easy to see that $[\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_l}) : \mathbb{Q}] = 2^l$, by arguments similar to those in previous paragraph, as the numbers $p_1, p_2 \ldots p_l$ have distinct squarefree parts and so are linearly independent over $\mathbb{Q}$. (If they did not, they could be multiplied to obtain perfect squares). Also, as above, $\sqrt{p_1} + \sqrt{p_2} + \ldots + \sqrt{p_l}$ is a primitive element of the extension, so the primitive element theorem is verified explicitly in this case.

Note that $\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_k}$ with the operation of multiplication (and division) generate an abelian group A. Let $\mathbb{Q}^\times$ be the multiplicative group $(\mathbb{Q}, \cdot)$. The group $G = A\mathbb{Q}^\times$ satisfies $[G : \mathbb{Q}^\times] = 2^l$, with $\sqrt{n_1}, \sqrt{n_2}, \ldots, \sqrt{n_l}$ forming a complete set of representatives for $G/\mathbb{Q}^\times$, where the n_i are all the possible 2^l products $\prod_{i \in J \subset \{1,2,\ldots,l\}} p_i$. (The quotient $G/\mathbb{Q}^\times$ is generated by the images of $\sqrt{n_1}, \sqrt{n_2}, \ldots, \sqrt{n_l}$ and is isomorphic to $(\mathbb{Z}/2\mathbb{Z})^l$). Therefore the result obtained in this section can be rewritten as $[\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_k}) : \mathbb{Q}] = [G : \mathbb{Q}^\times]$. In this abstract form, the result is easier to generalize.

Galois groups. The freedom with which one interchanged signs in front of radicals may suggest in fact that there is no visible difference between $\sqrt{p}$ and $-\sqrt{p}$, and they can be interchanged in expressions when one is concerned with rationals. This idea leads to the Galois groups. Indeed, if $p_1, p_2, \ldots, p_l$ are multiplicatively independent then in any expression $F(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_k})$ with $F \in \mathbb{Q}[X_1, X_2, \ldots, X_k]$ one may change the signs to get $F(\pm\sqrt{p_1}, \pm\sqrt{p_2}, \ldots, \pm\sqrt{p_k})$, and the new expression will be conjugate to the original. In particular, it will equal 0 if and only if the original equals 0. We thus have 2^l isomorphisms of $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \sqrt{p_3}, \ldots, \sqrt{p_l})$ for any choices of signs $\epsilon_1, \epsilon_2, \ldots, \epsilon_l \in \{-1, 1\}$, characterized by sending $\sqrt{p_i}$ to $\epsilon_i \sqrt{p_i}$. As the extension is normal (since $\mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \ldots, \sqrt{p_l})$ is the splitting field of $(X^2 - p_1)(X^2 - p_2) \ldots (X^2 - p_l)$) and has degree 2^l, we have found the Galois group of the extension: $(\mathbb{Z}/2\mathbb{Z})^l$.

Higher powers. The natural question is whether the statement of the problem can be extended to radicals of any degree. Specifically, we prove that if $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n \in \mathbb{Q}^+$ and $\sqrt[k]{b_i}$ are not all rational, then $\sum_{i=1}^n a_i \sqrt[k]{b_i}$ is not rational. The solution is a generalization of Solution 2. Firstly, we may assume all the k_i equal, as otherwise we can replace them by their least common multiple and adjust the b_i accordingly. So we need to prove that a sum of form $\sum_{i=1}^n a_i \sqrt[k]{b_i} = M \in \mathbb{Z}$ cannot occur if at least one of the b_i is not a perfect k-th power. Again, we use induction on n.

Consider ξ a primitive k-th root of unity. Take the polynomial

$$P(X, b) = \prod \left(X - b - \xi^{i_2} a_2 \sqrt[k]{b_2} - \ldots - \xi^{i_n} a_n \sqrt[k]{b_n} \right)$$

with a_i rational, where the product is taken over all choices of $i_2, i_3, \ldots, i_n \in \{0, 1, \ldots, k-1\}$. As replacing $\sqrt[k]{b_i}$ by $\xi \sqrt[k]{b_i}$ in the above expression preserves P, we conclude that P can be written as a polynomial in X and b with coefficients in $\mathbb{Q}[b_2, b_3, \ldots, b_n] = \mathbb{Q}$ (we did not argue this rigorously since it is completely similar to the argument used in the original problem). Now if $M \in \mathbb{Q}$ can be written as $\sum_{i=1}^n a_i \sqrt[k]{b_i}$ then $P(M, a_1 \sqrt[k]{b_1}) = 0$. Let $d \mid k, d > 1$ be the smallest integer such that $\sqrt[k]{b_1^d} \in \mathbb{Q}$; then $P(M, x)$ can be written as

$$q_0(x^d) + x q_1(x^d) + \ldots + x^{d-1} q_{d-1}(x^d)$$

where $q_0, q_1, \ldots, q_{d-1} \in \mathbb{Q}[X]$. So if $(a_1 \sqrt[k]{b_1})^d = u \in \mathbb{Q}$ we have

$$q_0(u) + q_1(u)\sqrt[d]{u} + \ldots + q_{d-1}(u)\sqrt[d]{u^{d-1}} = 0.$$

Now note that $1, \sqrt[d]{u}, \ldots, \sqrt[d]{u^{d-1}}$ are independent over $\mathbb{Q}$, because $\sqrt[d]{u}$ is the root of the irreducible polynomial $X^d - u$. (To see that this polynomial is irreducible, note that the roots of $X^d - u$ have absolute value $\sqrt[d]{|u|}$, so if $f(x) \mid X^d - u$ has degree m, then $|f(0)| = \sqrt[d]{|u|^m}$. But for $0 < m < d$ this is not rational, for if it were then $(a_1 \sqrt[k]{b_1})^m = \pm\sqrt[d]{|u|^m}$ would be rational, contradicting the minimality of d. So $X^d - u$ does not have proper factors in $\mathbb{Q}[X]$ and is irreducible.) Therefore we conclude that $q_0(u) = q_1(u) = q_2(u) = \ldots = q_{d-1}(u) = 0$. If ϵ is a primitive d-th root of unity we may conclude that

$$P(M, \epsilon u) = q_0(u) + q_1(u)\epsilon\sqrt[d]{u} + \ldots + q_{d-1}(u)\epsilon^{d-1}\sqrt[d]{u^{d-1}} = 0,$$

so $M = \epsilon\sqrt[d]{u} + \sum_{i=2}^{n} \xi^{l_i} a_i \sqrt[k]{b_i}$ for some $\{l_i\}$. But then

$$\epsilon\sqrt[d]{u} + \sum_{i=2}^{n} \xi^{l_i} a_i \sqrt[k]{b_i} = \sqrt[d]{u} + \sum_{i=2}^{n} a_i \sqrt[k]{b_i}.$$

This is impossible as each of the terms in the left-hand side has real part less than or equal to the corresponding term of the right-hand side (which a positive real of the same absolute value), and the inequality is strict for the first term.

References

[Ab] Zachary Abel: My Favorite Problem: Bert and Ernie, *The Harvard College Mathematics Review* **1** #2 (2007), 78–83.

[Kv] Irrationality of a Sum of Radicals (in Russian), *Kvant* **2** (1972).