Sums and products of algebraic numbers

G. J. O. Jameson

We call a polynomial "rational" if it has rational coefficients. As the reader will undoubtedly know, a number α (real or complex) is *algebraic* if there is a rational polynomial $p(x)$ such that $p(\alpha) = 0$. Of course, by multiplying through, one can then arrange for $p(x)$ to have *integer* coefficients, if this is desired.

A very basic fact about algebraic numbers is:

(A) if α and β are algebraic, then so are $\alpha + \beta$ and $\alpha\beta$.

How can one prove this? Given the polynomials that are zero at α and β, it is far from transparent how to exhibit polynomials that are zero at $\alpha + \beta$ and $\alpha\beta$. Also, what can be said about the degree of these polynomials?

An example will give some idea what to expect.

Example 1: Let $\alpha = 1+\sqrt{2}$ and $\beta = 1+\sqrt{3}$, so that $\alpha^2-2\alpha-1 = 0$ and $\beta^2-2\beta-2 = 0$. Let $\lambda = \alpha\beta = 1 + \sqrt{2} + \sqrt{3} + \sqrt{6}$. Rewrite this as $\lambda - 1 - \sqrt{6} = \sqrt{2} + \sqrt{3}$ and square both sides to obtain

$$(\lambda - 1)^2 - 2\sqrt{6}(\lambda - 1) + 6 = 5 + 2\sqrt{6},$$

which simplifies to $\lambda^2 - 2\lambda + 2 = 2\sqrt{6}\lambda$. Squaring again, we obtain

$$\lambda^4 - 4\lambda^3 - 16\lambda^2 - 8\lambda + 4 = 0.$$

Proofs of (A) in books (e.g. [ST],[R]) are often embedded in the machinery of algebraic number theory, involving concepts that are unnecessary for the modest objective of proving (A), such as field extensions and "algebraic integers". A fairly direct proof, disentangled from unnecessary notions, is given in [Chap]: this method is constructive, and depends on eigenvalues and determinants. Here we present a slightly simpler, but non-constructive, proof using only the notion of linear dependence. We then go on to describe a version of the constructive proof.

First, some elementary facts and notation. Given a rational polynomial such that $p(\alpha) = 0$, we can ensure, by taking a suitable multiple, that $p(x)$ is monic (i.e. has leading coefficient 1). Moreover, there will be a monic rational polynomial $p_0(x)$ of smallest degree with $p_0(\alpha) = 0$: this is the *minimal* polynomial for α: it is unique, for if $p_1(x)$ and $p_2(x)$ were two such polynomials, then $p_1(x) - p_2(x)$ would be a polynomial of smaller degree that

is zero at α. If the degree of the minimal polynomial is n, we say that α is "algebraic with degree n".

We denote by A_n the set of all (complex) numbers that are algebraic with degree not greater than n. The set of all algebraic numbers is then $A = \cup_{n=1}^{\infty} A_n$. (Some readers may prefer to restrict attention to real numbers: the statements and examples below that involve complex numbers are entirely dispensable.)

Of course, $A_1 = \mathbb{Q}$, the set of rational numbers: if $\alpha = a/b$, then $b\alpha - a = 0$. The numbers in A_2 are "quadratic numbers". Numbers of the form $a + \sqrt{b}$, with a, b rational, are quadratic, and by the quadratic formula, all quadratic numbers are of this form. This includes complex numbers of the form $a + i\sqrt{b}$, where b is a positive rational. In particular, i is quadratic: $i^2 + 1 = 0$.

Our problem is of the following type: given that certain numbers are algebraic, show that other numbers derived from them are also algebraic. Before tackling (A), we record some cases where this is very easy.

PROPOSITION 1. *If α ($\neq 0$) is in A_n, then so are $\alpha + a$ and $a\alpha$ (where $a \in \mathbb{Q}$), $1/\alpha$, the complex conjugate $\overline{\alpha}$ and α^2. If β is a square root of α, then $\beta \in A_{2n}$.*

Proof. Suppose that

$$p(\alpha) = c_0 + c_1\alpha + \ldots + c_n\alpha^n = 0.$$

If $\beta = \alpha + a$, then $p(\beta - a) = 0$: this is a polynomial in β, with rational coefficients, of degree n. Similarly, if $\beta = a\alpha$, then $p(\beta/a) = 0$. For $1/\alpha$, observe that

$$\frac{c_0}{\alpha^n} + \cdots + \frac{c_{n-1}}{\alpha} + c_0 = 0.$$

Since the coefficients in $p(x)$ are real, we have $p(\overline{\alpha}) = \overline{p(\alpha)} = 0$. For a square root β of α, we have $p(\beta^2) = 0$: this is a polynomial of degree $2n$ in β.

Now consider α^2. Define $q(x) = p(x)p(-x)$. Then q is a polynomial such that $q(-x) = q(x)$ for all x, which implies that the odd coefficients are 0 (one can also verify this algebraically), so $q(x)$ is of the form $\sum_{r=0}^{n} d_{2r}x^{2r}$. Also, $q(\alpha) = 0$, so $q_1(\alpha^2) = 0$, where $q_1(x) = \sum_{r=0}^{n} d_{2r}x^r$.

Note. Of course, α^2 may have degree less than n: if $\alpha = \sqrt{2}$, then $\alpha^2 = 2 \in A_1$.

The real numbers (equally, the complex numbers) form a vector space over the field $\mathbb{Q}$ (unlike the vector spaces that most people encounter first, these ones contain the underlying

field, but this doesn't matter). The following simple observation is key to our method: α is in A_n if and only if the elements $1, \alpha, \alpha^2, \ldots, \alpha^n$ are linearly dependent over $\mathbb{Q}$, beacuse this is equivalent to the existence of rationals c_r such that $c_0 + c_1\alpha + \cdots + c_n\alpha^n = 0$.

To exploit this fact, we introduce the set $\mathbb{Q}(\alpha)$, as follows. Suppose that α has minimal polynomial

$$p_0(x) = c_0 + c_1 x + \ldots + x^n.$$

Define $\mathbb{Q}(\alpha)$ to be the set of all numbers of the form

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1},$$

where $a_r \in \mathbb{Q}$ for each r, or in other words, the numbers expressible as $p(\alpha)$, where $p(x)$ is a rational polynomial of degree at most $n-1$. Then $\mathbb{Q}(\alpha)$ is a vector space over $\mathbb{Q}$, with basis 1, α, α^2, $\ldots \alpha^{n-1}$, so of dimension n (by the minimality of $p_0(x)$, these elements are linearly independent).

LEMMA 1. *$\alpha^r \in \mathbb{Q}(\alpha)$ for all $r \geq 1$, hence $p(\alpha) \in \mathbb{Q}(\alpha)$ for all rational polynomials p (of any degree). Also, $1/\alpha \in \mathbb{Q}(\alpha)$.*

Proof. First, we have

$$\alpha^n = -c_0 - c_1\alpha - \cdots - c_{n-1}\alpha^{n-1} \in \mathbb{Q}(\alpha).$$

In the same way, assuming (for induction) that $\alpha^k \in \mathbb{Q}(\alpha)$ for all $k \leq r-1$, it follows that $\alpha^r \in \mathbb{Q}(\alpha)$. Clearly, the second statement follows. Also,

$$\frac{c_0}{\alpha} = -c_1 - c_2\alpha - \cdots - \alpha^{n-1},$$

and $c_0 \neq 0$, because p_0 is minimal. Hence $1/\alpha \in \mathbb{Q}(\alpha)$. □

LEMMA 2. *If λ and μ are in $\mathbb{Q}(\alpha)$, then so is $\lambda\mu$ (so $\mathbb{Q}(\alpha)$ is a ring). In particular, $\lambda^r \in \mathbb{Q}(\alpha)$ for all $r \geq 1$.*

Proof. There are rational polynomials $p(x)$, $q(x)$ such that $\lambda = p(\alpha)$ and $\mu = q(\alpha)$. By Lemma 1, $\lambda\mu = p(\alpha)q(\alpha) \in \mathbb{Q}(\alpha)$. □

In elegant style, we now deduce the following result:

THEOREM 1. *If α is A_n, then so are all members of $\mathbb{Q}(\alpha)$.*

Proof. Let the degree of α be m, so $m \leq n$. Take λ in $\mathbb{Q}(\alpha)$. By Lemma 1, $\lambda^r \in Q(\alpha)$ for all $r \geq 1$. Since the dimension of $\mathbb{Q}(\alpha)$, as a vector space over $\mathbb{Q}$, is not greater than n, the $n+1$ elements 1, λ, λ^2, $\ldots$, λ^n are linearly dependent over $\mathbb{Q}$. So $\lambda \in A_n$. □

This re-proves most of the statements in Proposition 1, plus more. In particular, it shows that $\alpha^r \in A_n$ for all $r \geq 1$.

Note. Though it is not needed for our purposes, it would be telling less than the truth if we failed to mention the fact that $\mathbb{Q}(\alpha)$ is actually a *field*. In other words, in addition to the properties already mentioned, if λ ($\neq 0$) is in $\mathbb{Q}(\alpha)$, then so is $1/\lambda$. This can be proved quite simply, as follows (beware longer proofs in some books!). By Lemma 2, $\lambda^r \in \mathbb{Q}(\alpha)$ for all $r \geq 1$, hence $\mathbb{Q}(\lambda) \subseteq \mathbb{Q}(\alpha)$. By Lemma 1, $1/\lambda$ is in $\mathbb{Q}(\lambda)$. Hence it is in $\mathbb{Q}(\alpha)$.

We now prove (A) by a straightforward extension of this reasoning to two variables. Suppose that α, β have degree m, n respectively. Define $\mathbb{Q}(\alpha, \beta)$ to be the set of all numbers of the form

$$\sum_{r=0}^{m-1} \sum_{s=0}^{n-1} c_{r,s} \alpha^r \beta^s,$$

with each $c_{r,s}$ rational. Clearly, this is a vector space over $\mathbb{Q}$ of dimension at most mn, since it is spanned by the elements $\alpha^r \beta^s$. (If β is in $\mathbb{Q}(\alpha)$, then $\mathbb{Q}(\alpha, \beta)$ is just $\mathbb{Q}(\alpha)$ itself; if not, one can show that the elements $\alpha^r \beta^s$ are linearly independent, but we don't need this fact).

LEMMA 3. *If λ and μ are in $\mathbb{Q}(\alpha, \beta)$, then so is $\lambda\mu$.*

Proof. Clearly, $\lambda\mu$ is a linear combination of elements $\alpha^r \beta^s$, where $r \leq 2m-2$ and $s \leq 2n-2$. By Lemma 1, $\alpha^r \in \mathbb{Q}(\alpha)$ and $\beta^s \in \mathbb{Q}(\beta)$. From the definitions of these sets, it follows at once that $\alpha^r \beta^s$ is in $\mathbb{Q}(\alpha, \beta)$. □

The desired result now follows easily:

THEOREM 2. *If $\alpha \in A_m$ and $\beta \in A_n$, then all members of $\mathbb{Q}(\alpha, \beta)$, in particular $\alpha+\beta$ and $\alpha\beta$, are in A_{mn}. So if α and β are algebraic, then so are $\alpha + \beta$ and $\alpha\beta$.*

Proof. Take λ in $\mathbb{Q}(\alpha, \beta)$. By Lemma 2, λ^k is in $\mathbb{Q}(\alpha, \beta)$ for all $k \geq 1$. Since the dimension of $\mathbb{Q}(\alpha, \beta)$ is no more than mn, the $mn+1$ elements $1, \lambda, \lambda^2, \ldots, \lambda^{mn}$ are linearly dependent over $\mathbb{Q}$. □

So we have proved (A), together with the bound mn on the degree of the polynomials needed. We list a few of its implications, aided by the elementary facts from Proposition 1.

(1) A is a field: it admits sums, products and inverses of elements.

(2) If α is transcendental (i.e. not algebraic) and β is algebraic, then $\alpha + \beta$ and $\alpha\beta$ are transcendental, for if $\alpha + \beta$ were algebraic, then $\alpha = (\alpha + \beta) - \beta$ would be algebraic (and similarly for products). Well-known examples of transcendental numbers are e and π. So,

for example, $e + \sqrt{2}$ and $\pi\sqrt{2}$ are transcendental.

(3) If λ and μ are real algebraic numbers, then $(\lambda^2 + \mu^2)^{1/2}$ is algebraic.

(4) If $\alpha = \lambda + i\mu$, then α is algebraic if and only if λ and μ are algebraic, since, for example, $\lambda = \frac{1}{2}(\alpha + \overline{\alpha})$.

Finding the polynomials. One question remains: how can we actually find the polynomial that annihilates a given element λ of $\mathbb{Q}(\alpha, \beta)$, such as $\alpha + \beta$ or $\alpha\beta$? For the special case of a pair of quadratic numbers, this can always be achieved by squaring twice, with judicious reassembling, as in Example 1, but this procedure does not extend to the general case.

However, the proof above can be developed into a constructive method when combined with a further result from linear algebra, the fact that a singular matrix has determinant zero. We describe this slightly more generally. Suppose that M is a vector space over $\mathbb{Q}$ with basis $\gamma_1, \gamma_2, \ldots, \gamma_N$, and also that M is a ring (so M could be $\mathbb{Q}(\alpha)$ or $\mathbb{Q}(\alpha, \beta)$). Take $\lambda \in M$. Then for each i, we can express $\lambda\gamma_i$ as a linear combination $\sum_{j=1}^{N} c_{i,j}\gamma_j$, with $c_{i.j} \in \mathbb{Q}$. If C is the matrix $(c_{i,j})$ and $\mathbf{x}$ is the column vector $(\gamma_1, \gamma_2, \ldots, \gamma_N)$, this says that $C\mathbf{x} = \lambda\mathbf{x}$. So λ is an eigenvalue of C, and $C - \lambda I_N$ is singular, hence $\det(C - \lambda I_N) = 0$ (where I_N is the $N \times N$ identity matrix). This determinant (the "characteristic polynomial" of C) is a rational polynomial of degree N in λ.

We illustrate the method by applying it to the case considered in Example 1.

Example 1 revisited: Let α and β be as before. The basis elements are 1, α, β, $\alpha\beta$. We express the products with $\lambda = \alpha\beta$ in terms of them. To do this, we substitute the identities $\alpha^2 = 2\alpha + 1$ and $\beta^2 = 2\beta + 2$, not the explicit values of α and β. We obtain

$$\alpha\beta.1 = \alpha\beta,$$

$$\alpha\beta.\alpha = \alpha^2\beta = \beta + 2\alpha\beta,$$

$$\alpha\beta.\beta = \alpha\beta^2 = 2\alpha + 2\alpha\beta,$$

$$\alpha\beta.\alpha\beta = 2 + 4\alpha + 2\beta + 4\alpha\beta.$$

So the matrix C is given by

$$C = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 2 \\ 0 & 2 & 0 & 2 \\ 2 & 4 & 2 & 4 \end{pmatrix}.$$

After somewhat tedious calculations, which we will not reproduce here, we obtain

$$\det(C - \lambda I_4) = \lambda^4 - 4\lambda^3 - 16\lambda^2 - 8\lambda + 4,$$

agreeing with our previous solution.

The reader might care to work through the case of $\alpha + \beta$, by both methods.

References

[Chap] Robin Chapman, Notes on Algebraic Numbers, at:
empslocal.ex.ac.uk/people/staff/rjchapma

[R] H. E. Rose, *A Course in Number Theory*, Clarendon Press, Oxford (1988).

[ST] Ian Stewart and David Tall, *Algebraic Number Theory*, Chapman and Hall (1979).

updated 13 November 2015