A System of Algebraically Independent Numbers

John von Neumann

Abstract

We say that $a_1, \ldots, a_m \in \mathbb{C}$ form an algebraically independent system if, for any polynomial Φ with rational coefficients, we have $\Phi(a_1, \ldots, a_m) = 0$ only if $\Phi \equiv 0$. The aim of this work is to find a set M for which each finite subset is an algebraically independent system such that card $M = \mathfrak{c}$.

It should be noted that H. Lebesgue [1] and E. Steinitz [2] have proved the existence of a set M^*, called an "algebraic basis of numbers," which has the following two properties:

(1) Every finite subset of M^* is an algebraically independent system.

(2) For all $x \notin M^*$, there is a finite subset $S \subseteq M^*$ such that $S \cup \{x\}$ is not an algebraically independent system.

One can conclude, then, that such a set M^* has cardinality card $M^* = \mathfrak{c}$. However, this set M^* is constructed using the well-ordering theorem, while we will construct a set M without the use of the axiom of choice. It should be noted, however, that this set will not satisfy the second property. It is unlikely that an "algebraic basis of numbers," that is a set satisfying both properties (1) and (2), can be constructed without use of the well-ordering theorem.

The set M which we claim will satisfy property (1) is the set consisting of the numbers

$$A_t = \sum_{n=0}^{\infty} 2^{\left(2^{\lfloor tn \rfloor} - 2^{n^2}\right)}, \quad t > 0,$$

where $\lfloor x \rfloor$ denotes the greatest integer which is at most x.[1] It is clear that this series converges for $t > 0$ and that, for $s < t$, $A_s < A_t$. Hence, card $M = \mathfrak{c}$.[2] We must now show that any finite subset of M is algebraically independent.

We must show that if $\Phi(x_1, \ldots, x_m)$ is a polynomial with rational coefficients, and $t_1, \ldots, t_m > 0$ pairwise distinct, then $\Phi(A_{t_1}, \ldots, A_{t_m}) = 0$ gives $\Phi \equiv 0$. It is clear that we may look at polynomials with only integer coefficients.

We first prove a lemma.

Lemma. Let $t_1, \ldots, t_m > 0$ be pairwise distinct. If $\varphi(x_1, \ldots, x_m)$ is a polynomial with integer coefficients which is not identically 0, then there is an N and an $\varepsilon > 0$ so that

$$\left|\varphi\left(2^{2^{\lfloor t_1 n \rfloor}}, \ldots, 2^{2^{\lfloor t_m n \rfloor}}\right)\right| \geq \varepsilon$$

[1] Hence, the dyadic expansions of the numbers A_t are defined explicitly. It should be noted that the real reason for the algebraic independence of A_t is analogous to the reason that Liouville numbers are transcendental. Whenever $0 < s < t$, the number A_t is better approximated by rational numbers than A_s, and so they should not be algebraically dependent.

[2] We see for $s \neq t$ that $A_s \neq A_t$ as, otherwise, $\Phi(x_1, x_2) = x_1 - x_2$ would give $\Phi(A_s, A_t) = 0$.

whenever $n \geq N$.

Proof.

This proof is by induction on m. For $m = 0$, φ is a constant. If $\varphi \neq 0$, then we choose $N = 1$ and $\varepsilon = |\varphi| > 0$.

Now suppose that the result holds for m. We want to show the result holds for $m + 1$. Assume, without loss in generality, that t_{m+1} is the largest of $t_1, \ldots, t_{m+1}$. Then, we have

$$\varphi\left(x_1, \ldots, x_{m+1}\right) = \psi_0\left(x_1, \ldots, x_m\right) x_{m+1}^s + \psi_1\left(x_1, \ldots, x_m\right) x_{m+1}^{s-1} + \cdots + \psi_s\left(x_1, \ldots, x_m\right),$$

where $\psi_0 \not\equiv 0$. For $s = 0$, $\varphi\left(x_1, \ldots, x_{m+1}\right) = \psi_0\left(x_1, \ldots, x_m\right)$, and since the result holds for m, we are done. So, take $s \geq 1$.

Since the result holds for $\psi_0\left(x_1, \ldots, x_m\right)$, choose N and $\varepsilon > 0$ so that $\left|\psi_0\left(2^{2^{\lfloor t_1 n\rfloor}}, \ldots, 2^{2^{\lfloor t_m n\rfloor}}\right)\right| \geq \varepsilon$ whenever $n \geq N$. Let $t = \max\left(t_1, \ldots, t_m\right) < t_{m+1}$, let d be the highest degree of the degrees of $\psi_1, \ldots, \psi_s$, and let C be the sum of the absolute values of all of its coefficients. Then, for $n \geq N$, we have

$$\left|\varphi\left(2^{2^{\lfloor t_1 n\rfloor}}, \ldots, 2^{2^{\lfloor t_{m+1} n\rfloor}}\right)\right| \geq \left|\psi_0\left(2^{2^{\lfloor t_1 n\rfloor}}, \ldots, 2^{2^{\lfloor t_m n\rfloor}}\right)\right| \cdot 2^{s2^{\lfloor t_{m+1} n\rfloor}} -$$

$$\left(\left|\psi_1\left(2^{2^{\lfloor t_1 n\rfloor}}, \ldots, 2^{2^{\lfloor t_m n\rfloor}}\right)\right| 2^{(s-1)2^{\lfloor t_{m+1} n\rfloor}} + \cdots + \left|\psi_s\left(2^{2^{\lfloor t_1 n\rfloor}}, \ldots, 2^{2^{\lfloor t_m n\rfloor}}\right)\right|\right) \geq$$

$$\varepsilon 2^{s2^{\lfloor t_{m+1} n\rfloor}} - C2^{d2^{\lfloor tn\rfloor}} \cdot 2^{(s-1)2^{\lfloor t_{m+1} n\rfloor}} =$$

$$\varepsilon 2^{s2^{\lfloor t_{m+1} n\rfloor}} \cdot \left(1 - \frac{C}{\varepsilon} 2^{d2^{\lfloor tn\rfloor} - 2^{\lfloor t_{m+1} n\rfloor}}\right).$$

The second factor is always at least 1, and the third factor tends to 1, because $t_{m+1} > t$. Therefore, there is $N' \geq N$ such that, for $n \geq N'$, we have

$$\left|\varphi\left(2^{2^{\lfloor t_1 n\rfloor}}, \ldots, 2^{2^{\lfloor t_{m+1} n\rfloor}}\right)\right| \geq \varepsilon \cdot 1 \cdot \frac{1}{2} = \frac{\varepsilon}{2}.$$

QED

We now prove the main theorem.

Theorem. Let $t_1, \ldots, t_m > 0$ be pairwise distinct, and let $\Phi\left(x_1, \ldots, x_m\right)$ be a polynomial with integer coefficients. Suppose that $\Phi\left(A_{t_1}, \ldots, A_{t_m}\right) = 0$. Then, $\Phi \equiv 0$.

Proof.

Suppose, for a contradiction, that $\Phi \not\equiv 0$. Let s be the degree of Φ and let Ψ be the homogeneous part of degree s of Φ. Then, $\Psi \not\equiv 0$. Now, choose C so that for $0 \leq x_1 \leq y_1 \leq A_{t_1}, \ldots, 0 \leq x_m \leq y_m \leq A_{t_m}$, we have $\left|\Phi\left(x_1, \ldots, x_m\right) - \Phi\left(y_1, \ldots, y_m\right)\right| \leq C \cdot \max\left(y_1 - x_1, \ldots, y_m - x_m\right)$. Let $r \geq \max\left(t_1, \ldots, t_m\right)$ be an integer and let D be the sum of the absolute values of the coefficients of $\Psi\left(x_1, \ldots, x_m\right)$.

Now, let $\ell \geq 1$ be any integer. Then, we have

$$\left|\Phi\left(A_{t_1}, \ldots, A_{t_m}\right) - \Phi\left(\sum_{n=0}^{\ell} 2^{2^{\lfloor t_1 n\rfloor} - 2^{n^2}}, \ldots, \sum_{n=0}^{\ell} 2^{2^{\lfloor t_m n\rfloor} - 2^{n^2}}\right)\right| \leq$$

$$C \cdot \max \left(\sum_{n=\ell+1}^{\infty} 2^{2^{\lfloor t_1 n \rfloor} - 2^{n_2}}, \ldots, \sum_{n=\ell+1}^{\infty} 2^{2^{\lfloor t_1 n \rfloor} - 2^{n_2}} \right) \leq C \cdot \sum_{n=\ell+1}^{\infty} 2^{2^{rn} - 2^{n^2}}.$$

Whenever $n \geq r$, we have

$$\frac{2^{2^{r(n+1)}}}{2^{2^{(n+1)^2}}} \Big/ \frac{2^{2^{rn}}}{2^{2^{n^2}}} = 2^{-2^{(n+1)^2} - 2^{rn} + 2^{n^2} + 2^{r(n+1)}} \leq$$

$$2^{-2^{(n+1)^2} + 2^{n^2} + 2^{r(n+1)}} < 2^{-2^{(n+1)^2} + 2^{n^2 + n + 1}} < \frac{1}{2},$$

so that for $\ell \geq r$, we have

$$\sum_{n=\ell+1}^{\infty} 2^{2^{rn} - 2^{n^2}} \leq 2^{2^{r(\ell+1)} - 2^{(\ell+1)^2}} \left(\sum_{n=0}^{\infty} 2^{-n} \right) = 2 \cdot 2^{2^{r(\ell+1)} - 2^{(\ell+1)^2}} =$$

$$2^{-2^{(\ell+1)^2} + 2^{r(\ell+1)} + 1} \leq 2^{-2^{(\ell+1)^2} + 2^{\ell(\ell+1)} + 1} \leq 2^{-2^{(\ell+1)^2} + 2^{\ell^2 + \ell + 1}} =$$

$$2^{-2^{\ell^2 + \ell + 1}(2^{\ell} - 1)} \leq 2^{-2^{\ell^2 + \ell + 1}}.$$

So when $2^{\ell+1} \geq s + 1$ (such as when $\ell \geq s$), we have

$$2^{-2^{\ell^2 + \ell + 1}} \leq 2^{-(s+1)2^{\ell^2}} = \frac{1}{2^{(s+1)2^{\ell^2}}}.$$

In summary, we have that, for $\ell \geq r, s$,

$$\left| \Phi\left(A_{t_1}, \ldots, A_{t_m}\right) - \Phi\left(\sum_{n=0}^{\ell} 2^{2^{\lfloor t_1 n \rfloor} - 2^{n^2}}, \ldots, \sum_{n=0}^{\ell} 2^{2^{\lfloor t_m n \rfloor} - 2^{n^2}} \right) \right| \leq \frac{C}{2^{(s+1)2^{\ell^2}}}.$$

Hence, since $\Phi\left(A_{t_1}, \ldots, A_{t_m}\right) = 0$, we have

$$\left| 2^{s 2^{\ell^2}} \Phi\left(\sum_{n=0}^{\ell} 2^{2^{\lfloor t_1 n \rfloor} - 2^{n^2}}, \ldots, \sum_{n=0}^{\ell} 2^{2^{\lfloor t_m n \rfloor} - 2^{n^2}} \right) \right| \leq \frac{C}{2^{2^{\ell^2}}}.$$

Now the Φ term should be multiplied out. All of its terms are rational with powers of two in the denominator. We divide these terms into three groups as follows.

The first group consists of those terms in which the last term $2^{2^{\lfloor t_i \ell \rfloor} - 2^{n^2}}$ remains after taking out powers of $\sum_{n=0}^{\ell} 2^{2^{\lfloor t_i n \rfloor} - 2^{n^2}}$. These terms have denominators of the form 2^u, where $u \leq (s-1)\, 2^{\ell^2} + 2^{(\ell+1)^2}$. So, if we multiply by $2^{s 2^{\ell^2}}$, we end up with integers divisible by

$$2^{s 2^{\ell^2} - (s-1) 2^{\ell^2} - 2^{(\ell-1)^2}} = 2^{2^{\ell^2} - 2^{(\ell-1)^2}}.$$

Since the exponent of each term is at least $2^{\ell^2} - 2^{\ell^2-1} = 2^{\ell^2-1}$, they are also divisible by $2^{2^{\ell^2-1}}$.

The second group consists of those terms in which the last term $2^{2^{\lfloor t_i \ell \rfloor} - 2^{\ell^2}}$ is taken out, but only by parts of Φ of degree strictly less than s. Again, these are rational numbers with denominators of the form 2^u, where now we have $u \leq (s-1)\,2^{\ell^2}$. After multication by $2^{s2^{\ell^2}}$, we end up with integers divisible by

$$2^{s2^{\ell^2}-(s-1)2^{\ell^2}} = 2^{2^{\ell^2}},$$

which is then divisible by $2^{2^{\ell^2}-1}$.

The third group, finally, consists of those terms in which the last term $2^{2^{\lfloor t_i \ell \rfloor} - 2^{\ell^2}}$ is taken out, this time by a part of Φ of degree s. We see, then, that the sum of these terms is $\frac{\Psi\left(2^{2^{\lfloor t_1 \ell \rfloor}}, \ldots, 2^{2^{\lfloor t_m \ell \rfloor}}\right)}{2^{s2^{\ell^2}}}$ which, after multiplication by $2^{s2^{\ell^2}}$ is $\Psi\left(2^{2^{\lfloor t_1 \ell \rfloor}}, \ldots, 2^{2^{\lfloor t_m \ell \rfloor}}\right)$.

Therefore, we have that

$$2^{s2^{\ell^2}} \Phi\left(\sum_{n=0}^{\ell} 2^{2^{\lfloor t_1 n \rfloor} - 2^{n^2}}, \ldots, \sum_{n=0}^{\ell} 2^{2^{\lfloor t_m n \rfloor} - 2^{n^2}}\right) = p_\ell + q_\ell,$$

where, for sufficiently large ℓ, p_ℓ, the sum of the terms from the first two groups, is an integer divisible by $2^{2^{\ell^2-1}}$, and q_ℓ, the sum of the terms from the third group, is $\Psi\left(2^{2^{\lfloor t_1 \ell \rfloor}}, \ldots, 2^{2^{\lfloor t_m \ell \rfloor}}\right)$, which is, hence, an integer.

Therefore, for all sufficiently large ℓ, we have that

$$|p_\ell + q_\ell| \leq C 2^{-2^{\ell^2}}.$$

The right hand side tends to 0, so eventually less than 1, but since p_ℓ and q_ℓ are integers, we must have, for sufficiently large ℓ, that $p_\ell + q_\ell = 0$, which gives

$$q_\ell = -p_\ell.$$

Thus, q_ℓ must also be divisible by $2^{2^{\ell^2-1}}$, but we will show, for all ℓ sufficiently large, that $q_\ell \neq 0$, but that $|q_\ell| < 2^{2^{\ell^2-1}}$, which is impossible.

By our lemma, we know that $q_\ell \neq 0$, so it is enough to show that $|q_\ell| < 2^{2^{\ell^2-1}}$. Now,

$$|q_\ell| = \left|\Psi\left(2^{2^{\lfloor t_1 \ell \rfloor}}, \ldots, 2^{2^{\lfloor t_m \ell \rfloor}}\right)\right| \leq D \cdot 2^{s2^{r\ell}}.$$

Therefore, for sufficiently large ℓ, we have that $|q_\ell| < 2^{2^{\ell^2-1}}$.

QED[3]

[3] The proof may be reproduced almost verbatim for any system of numbers

$$C_k = \sum_{n=0}^{\infty} 2^{2^{\varphi_k(n)} - 2^{n^2}}, \;\; k = 1, 2, \ldots, m,$$

when the functions φ_k satisfy the following: When $n \to \infty$, $\varphi_k(n) \to \infty$, $\varphi_{k+1}(n) - \varphi_k(n) \to \infty$, and $n^2 - \varphi_k(n) \to \infty$. This, of course, applies to $\varphi_k(n) = \lfloor t_k n \rfloor$ when $0 < t_1 < \cdots < t_m$.

As a consequence, it is easy to make $\mathfrak{c}$-many more algebraically independent systems of numbers.

Note: For any $t > 0$, if R_t is rational, then the set M' consisting of $A_t + R_t$ also satisfies property (1). In fact, card $M = \mathfrak{c}$, because $s \neq t$ implies $A_s + R_s \neq A_t + R_t$ (since, otherwise, they would be a zero of $\Phi(x_1, x_2) = (x_1 - x_2) + (R_s - R_t)$). From the algebraic independence of $A_{t_1}, \ldots, A_{t_m}$ follows the algebraic independence of $A_{t_1} + R_{t_1}, \ldots, A_{t_m} + R_{t_m}$.

Since we are free to choose the R_t, we can build sets M' which satisfy additional properties. For example, we can cram M' into an arbitrarily small interval $a < x < b$. We just choose R_t with $a - A_t < R_t < b - A_t$.

We may also make it so that every interval contains $\mathfrak{c}$ points of M'. Let $I_1, I_2, \ldots$ be the sequence of all intervals with rational endpoints, where I_p has enpoints $a_p < b_p$. Then, for $p - 1 < t \leq p$, we choose rationals R_t so that $a_p - A_t < R_t < b_p - A_t$.

Remarks. Our set M solves problems posed by S. Mazurkiewicz [3] and S. Ruziewicz [4].

The problem of Mazurkiewicz is: Can we give an example of a set of real numbers such that it contains any sum, difference, product, and quotient of its elements, but it is not all of $\mathbb{R}$? These conditions are satisfied by the set of all rational functions with integer coefficients evaluated at A_t, $0 < t < 1$.

The problem of Ruziewicz is: Can we give an example of an uncountable set of complex numbers so that, for distinct z_1, z_2, we have $P\left(e^i\right) z_1 + Q\left(e^i\right) z_2 + R\left(e^i\right) \neq 0$ when P, Q, R are non-zero polynomials with rational coefficients? We solve this as follows:

Let M_1 be the set of A_t, $0 < t \leq 1$, and M_2 the set of A_t, $1 < t \leq 2$. Both have cardinality $\mathfrak{c}$, and one of them satisfies the condition. If

$$P\left(e^i\right) z_1 + Q\left(e^i\right) z_2 + R\left(e^i\right) = 0,$$

$$U\left(e^i\right) z_3 + V\left(e^i\right) z_4 + W\left(e^i\right) = 0,$$

where $z_1, z_2 \in M_1$ and $z_3, z_4 \in M_2$ are pairwise distinct, we may eliminate e^i, giving us $\Phi(z_1, z_2, z_3, z_4) = 0$ where $\Phi \not\equiv 0$. However, this is impossible, as these are different elements of M.

Now, it may seem incomplete that we have not decided which of M_1 or M_2 is the desired set, but we can fix this by replacing e^i with another transcendental number ε with $|\varepsilon| = 1$, as this makes no difference for Ruziewicz' purposes.

To do this, let R be a rational with $-1 < A_1 - R < 1$, and set $\varepsilon = (A_1 - R) + i\sqrt{1 - (A_1 - R)^2}$. This is transcendental and $|\varepsilon| = (A_1 - R)^2 + 1 - (A_1 - R)^2 = 1$. Now, let M be the set of A_t, where $1 \neq t > 0$.

(Received 2 May 1927)

(Translated 4 October 2014)

References

[1] Lebesgue, H., *Sur les transformations ponctuelles transformant les plans en plans qu'on peut définir par des procédés analytiques* (Atti Accad. Sci. Torino, 1907, 3-10).

[2] Steinitz, E., *Algebraische Theorie der Körper*, Journ. f. r. u. a. Mathematik.

[3] Mazurkiewicz, S., *Probléme 8*, Fund. Math. 1 (1920).

[4] Ruziewicz, S., *Sur un ensemble de non dénombrable points, superposable avec les moitiés de sa parties aliquot*, Fund. Math. 2 (1921).

[5] von Neumann, J., *Ein System algebraisch unabhüngiger Zahlen*, Math. Ann. 99 (1928).

> "There was a seminar for advanced students in Zürich and von Neumann was in the class. I came to a certain theorem, and I said it is not proved and it may be difficult. Von Neumann didn't say anything, but after five minutes he raised his hand. When I called on him, he went to the blackboard and proceeded to write down the proof. After that, I was afraid of von Neumann."
>
> \- George Pólya