EXISTENCE OF ALGEBRAIC AND TRANSCENDENTAL NUMBERS

AASTHA JAIN

Abstract. In this paper we will be discussing the existence of algebraic and transcendental numbers in number theory. We will first discuss some definitions to better explain these terms. Then, provide examples of each definition. As well as state important theorems relating to irrationality and transcendence in number theory and provide examples of those as well.

1. Acknowledgement

Firstly, I would like to express my sincere gratitude to Simon Rubinstein-Salzedo, Stanford PhD, for his guidance and mentorship. I would also like to thank Annika Mauro, Stanford Mathematics '23, for providing me with support and assistance. Finally, I would like to thank my parents, for showing me the kind of unequivocal love and support that only family can give.

2. Introduction

Number theory is the study of numbers and integers and two main types of numbers which are also referred to as complex numbers are called Algebraic and Transcendental numbers. These are the types of numbers that are studied in this paper. First we go over the definitions of these numbers as well as go over the conditions of what a polynomial needs to have in order to be considered as an algebraic or transcendental number. We also take a look at the Gauss' Lemma and Eisenstein's Lemma to prove irreducibility within polynomials. After this we solely focus on the closure properties of Algebraic numbers. Then, we introduce transcendental numbers by stating some history about the people involved in proving that a number can be transcendental because it was certainly more difficult than proving that

Date: July 2023.

an algebraic number exists. So, we will also explain how mathematicians like Liouville and Cantor proved this. Lastly, we will talk about the irrationality of ζ and the prime number theorem as it is an essential theorem in number theory. Side note: all the information stated in this paper comes from Chapter 3 in "Irrationality and transcendence in number theory textbook by David Angell."

3. Preliminaries

Definition 3.1. An algebraic number is the root of a polynomial

$$\mathrm{a}_n z^n + a_{n-1}z^{n-1} + ... + a_1 z + a_0 \tag{3.1}$$

with rational coefficients while an algebraic integer is where $a_n \neq 0$. A transcendental number is any non-algebraic number.

Lemma 3.2. (1) *If the given polynomial is not equal to 0 with a coefficient that is also an integer then only is the complex number algebraic (over Q).*

Example. $z^2 + 1$ is irreducible over $\mathbb{Q}$. It has two roots ±i and degree of 2 which is the algebraic integer

(2) *If $g(a) = 0$, then g is a multiple of f_a and if $f_a(a) = 0$ then a is algebraic and has the smallest degree.*

Example. $\cos\frac{1}{7}\pi, \cos\frac{3}{7}\pi$ and $\cos\frac{5}{7}\pi$ are the roots of the cubic $8z^3 - 4z^2 - 4z + 1$. Polynomial is irreducible. Roots are degree 3 so algebraic.

(3) *A polynomial f_a that is irreducible over Q means that it can't be factored to have a product of two polynomials and also doesn't have f_a's smallest degree.*

Example. Example. $\zeta = e^{2\pi i/5}$ is a root of $z^5 - 1$. This polynomial is reducible since $z^5 - 1 = (z-1)(z^4 + z^3 + z^2 + z + 1)$

Proof. A polynomial with rational coefficients multiplied by the common denominator of its coefficients will demonstrate the first claim. The second statement makes it clear that f_a exists; if $g(a) = 0$, then dividing g by f_a produces

$$g(z) = f_a(z)q(z) + r(z) \tag{3.2}$$

$r(a) = 0$. However, because r is the zero polynomial since it has a smaller degree than f_a, g is a multiple of f_a. So each polynomial is a factor of the other if there are two polynomials with the minimal-degree property, the uniqueness of f_a follows. If $f_a = gh$ is properly factored, then either g or h has a as a root, which contradicts f_a minimality. This is how irreducibility is demonstrated.

□

Definition 3.3. Looking at lemma 1.2, the polynomial f_a and the degree of an algebraic number is equal to a minimal polynomial. Note that algebraic numbers and algebraic integers are not the same thing though. Algebraic integers are a type of algebraic number in which minimal polynomial coefficients are rationals.

Lemma 3.4. *Gauss' Lemma. If f factors in Q[x], then it must also factor in Z[x].*

Proof. Think about if we had to prove if 10 is a quadratic residue or quadratic non-residue modulo 23

The first thing to do is examine the given information which in this case are these 11 numbers:

(1) (1) (10), (2) (10), (3) (10), (4) (10), (5) (10), (6) (10), (7) (10), (8) (10), (9) (10), (10) (10), (11) (10) and when you do the math the result comes out to these numbers: 10, 20, 30, 40, 50, 60, 70, 80, 90, 100, 110. Using this list modulo 23, we get the following final numbers: 10, 20, 7, 17, 4, 14, 1, 11, 21, 8, 18.

Therefore we can see that 5 numbers are greater than 11. So, $(10/23) = (-1)^5 = -1$. So 10 is a quadratic non-residue modulo 23 since ten is an even number. It would be quadratic residue modulo if it was an odd number. □

4. Proving polynomials irreducible

Lemma 4.1. *Eisenstein's Lemma. f is irreducible over Q if there is a prime p which satisfies the conditions that p is a factor of a_0, a_1, . . . , a_{n-1}, p is not a factor of a_n, and p^2 is not a factor of a_0.*

Proof. Suppose that the polynomial is f(x)=$7x^6$ - $9x^4$+ $6x^2$ + 15 and the goal is to prove that it is irreducible over Q. To do this, the first thing to realize is that prime p is 3 and $p/15$, $p/6$, and $p/-9$ however $p \nmid 7$ and p^2 which is $9 \nmid 15$ so f is irreducible over Q by Eisenstein's Lemma.

□

Example. Eisenstein's Lemma simplifies the proof of irreducibility for

$$\text{f(z)} = \text{z}^5 - 1/z - 1 = z^4 + z^3 + z^2 + z + 1 \tag{4.1}$$

Looking at this factored:

$$\text{f(z + 1)} = \text{(z + 1)}^5 1/z = z^4 + 5z^3 + 10z^2 + 10z + 5 \tag{4.2}$$

We can see that the prime p=5 so $f(z+1)$ is irreducible and so is f.

Lemma 4.2. *Polynomials modulo m are factorized by lowering their coefficients to m and making sure that f_m has a degree n factor over Z_m.*

Proof. Think if $f = gh$ that's where g has degree n. If m is a factor of $g's$ leading coefficient then $f_m = g_m h_m$, and g_m has degree n. □

Example. Let $f(z) = z^3 - 4z^2 + 9z + 16$ and pick $m = 3$. We see that

$$\text{f}_3(z) = z^3 + 2z^2 + 1 \tag{4.3}$$

If f_3 is reducible it should also be factorable. Calculation in Z_3 would look like:

$$\mathrm{f}_3(0) = 1\ ,\ f_3(1) = 1 \text{ and } f_3(2) = 2 \tag{4.4}$$

Here, f_3 is irreducible because it has no roots in Z_3 and therefore it is also not factorable.

Example. The polynomial $f(z) = 2z^2 + 3z + 1$ is reducible over Z but $f_2(z) = z + 1$ so note that we still have to keep in mind that the leading coefficient f must not have a factor known as m.

Lemma 4.3. *Here we talking about an algabraic number denominator and saying that da is an algebraic integer when $d \neq 0$.*

Proof. Assume that: □

$$\mathrm{a}_n a^n + a_{n-1}a^{n-1} + a_{n-2}a^{n-2} + ... + a_1 a + a_0 = 0 \tag{4.5}$$

a_k is the integer and $a_n \neq 0$ instead $d = a_n$. So that on both sides we can multiply by a_n^{n-1} and get

$$(\mathrm{a}_n a)^n + a_{n-1}(a_n a)^{n-1} + a_{n-2}a_n(a_n a)^{n-2} + ... + a_1 a_n^{n-2}(a_n a) + a_0 a_n^{n-1} = 0 \tag{4.6}$$

This proves that $(a_n a)$ is an algebraic integer.

Definition 4.4. In an algebraic number denominator, da is an algebraic integer when $d \neq 0$ as mentioned earlier and so d in da is actually the denominator of a also known as den a.

Example. Going back to lemma 1.2 for example of number 2 where a = $cos1/7\pi$ and $8z^3 - 4z^2 - 4z + 1 = 0$ and it states that there is an algebraic integer at $8z$. Though, now it is visible to us that $8z$ is not the smallest integer because

$$(2\mathrm{a})^3 - (2a)^2 - 2(2a) + 1 = 0. \tag{4.7}$$

So, since d = 1 is not attainable as it is not an algebraic integer, den a= 2.

5. Closure properties of Algebraic Numbers

Lemma 5.1. *If complex integers had a set $S = ak|k \in K$, and the group of linear combinations*

$$\sum r_k a_k \tag{5.1}$$

with rational coefficients had a limited number of terms over the field Q, this suggests that r_k being a rational coefficient is a vector space over itself since any field over itself has a vector space.
Similarly, the group of linear combinations

$$\sum m_k a_k \tag{5.2}$$

with integer coefficients and a limited number of terms, suggests that m_k is part of the set that forms a group with the operation as addition and that operation is also commutative.

Lemma 5.2. *If you have some number of vectors, it is possible to take the vector space formed by taking all linear combinations of those vectors.*

(1) *So, if x and y are vectors then all numbers in the form ax+by for a and b real numbers is the span of x and y, which is a vector space.*
(2) *If a group is generated by some set of elements S, it means that there is an element g in G and s in S such that every element of the group is in the form of gs.*

Proof. Every power of a may be expressed as an integral linear combination of $1, a, a^2, ..., a^{n-1}$, if it is an algebraic number of degree n. As a result, this set builds the group. On the other hand, think that the group is made up of n components, p_1, p_2,..., p_n. Since each of these is an integer linear combination of powers of a, as are ap_1, ap_2,..., and ap_n, we may construct equations for each of them that look like this:

$$\text{ap}_k = m_{k1}p_1 + m_{k2}p_2 + ... + m_{kn}p_n \text{ for } k = 1, 2, ..., n \tag{5.3}$$

$m_{kj}p_j$ has a non-zero solution thus the determinant

$$\begin{array}{|c|c|c||c|}\hline a-m_{11} & -m_{12} & ... & -m_{1n} \\ -m_{21} & a-m_{22} & ... & -m_{2n} \\ -m_{n1} & -m_{n2} & ... & a-m_{nn} \\ \hline \end{array}$$

is zero. □

Theorem 5.3. *If a and B are algebraic, then aB and a±B are also algebraic.*

Proof. Every power of a+B looks like this:

$$\mathrm{(a{+}B)}^k = \sum_{j=0}^{k} \binom{k}{j} a^j B^{k-j} \tag{5.4}$$

And another way of writing every power of a+B is like this:

$$\mathrm{(a{+}B)}^k = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} r_{ij} a^i B^j \tag{5.5}$$

□

Proof. The goal is to show if b is algebraic than 1/b is also algebraic and that the reciprocal of 1/b is algebraic as well. This is shown by looking at B as a root of

$$\mathrm{b}_n z^n + b_{n-1} z^{n-1} + ... + b_1 z + b_0 \tag{5.6}$$

as well as exhibiting a polynomial which has 1/b as a root of

$$\mathrm{b}_0 z^n + b_1 z^{n-1} + ... + b_{n-1} z + b_n \tag{5.7}$$

□

Theorem 5.4. *A Complex number B is equivalent to the root of a polynomial*

$$a_n z^n + a_{n-1} z^{n-1} + ... + ab_1 z + a_0 \tag{5.8}$$

with algebraic coefficients and B is an algebraic number when $a_n \neq 0$*. B is an algebraic integer when there is a root B of a non-zero polynomial*

$$z^n + a_{n-1}z^{n-1} + ... + ab_1 z + a_0 \tag{5.9}$$

who has algebraic integer coefficients.

Proof. The goal here is to see how the complex number B can be written as linear expressions with rational coefficients

$$\mathrm{a}_0^{m_0} a_1^{m_1} ... a_{n-1}^{m_n - 1} B^m \tag{5.10}$$

The conditions that the exponents of linear expressions with rational coefficients satisfy are for all k this:

$$0 \leq mk < dk \tag{5.11}$$

And this:

$$0 \leq m < n \tag{5.12}$$

So the conclusion of the vector space of B is just looking at expressions such as

$$\mathrm{d}_0 d_1 ... d_{n-1} n \tag{5.13}$$

it can be told that B is algebraic and it is also a basis for finitely many expressions like the one above. □

6. Transcendental Numbers

Joseph Liouville was the first person to try to show that e is not an algebraic number, its actually a transcendental number. He wasn't exactly to prove this exact statement however, he was able to provide examples of transcendental numbers to show that they do indeed exist. Though, a few decades later a man named Georg Cantor was able to prove the existence of transcendental numbers by showing examples of them being more complicated and big numbers then algebraic numbers.

Theorem 6.1. *Transcendental numbers exist*

Proof. If Z is countable then S is also going to be countable. Looking at a Z(z) to S function of $an \neq 0$

$$\mathrm{a}_n z^n + a_{n-1} z^{n-1} + ... + a_1 z + a_0 \to (a_n, a_{n-1}, ..., a_1, a_0) \tag{6.1}$$

it can be seen that Z(z) is countable.

Example. (algebraic numbers) =

$$\bigcup_{f \in Z[z]} S_f$$

Going back to Liouville's methods, the goal is to approximate real numbers by rational numbers by choosing p and q:

$$|a - p/q| \tag{6.2}$$

A real number a approximates to order s if c and the inequality

$$|a - p/q| < c/q^s \tag{6.3}$$

satisfies the rational numbers p and q.

Note that s is probably going to be an integer, its not guaranteed though it is likely to be that way.

Also a is usually well approximable when s is big instead of small.

Let's look at this number:

$$a = \sum_{k=0}^{\infty} 10^{-2^k} \tag{6.4}$$

This has been proved to be irrational. If we use rationals p and q and the variable we use to measure everything is

$$\text{q}=10^{2^m} \tag{6.5}$$

we can also see that in particular terms of p and q as well as a being the approximable variable

$$|a - p/q| = \frac{1}{10^{2m+1}} + \frac{1}{10^{2m+2}} + ... < \frac{2}{10^{2m+1}} = \frac{2}{q^2} \tag{6.6}$$

Therefore it is visible that a is approximable to order 2. □

Lemma 6.2. *Have the variables s and q as real numbers alongside a being a real number as well as c being the number that stays the same.*

$$|a - p/q| < \frac{c}{q^s} \tag{6.7}$$

and

$$0 < q < Q \tag{6.8}$$

We can see that p and q paired integers are used as possible values that satisfy the inequalities.

Proof. P and q paired integers can satisfy the inequalities as it is shown here:

$$qa - \frac{c}{q^{s-1}} < p < qa + \frac{c}{q^{s-1}} \tag{6.9}$$

□

Theorem 6.3. *If a and s are both real numbers just s is positive then that means that a is approximable to s and again p and q paired integers can satisfy the inequalities as it is shown here:*

$$0 < |a - p/q| < \frac{c}{q^s} \tag{6.10}$$

but also there is a constant c to help p and q.

Theorem 6.4. *Have the variables s and t as real numbers alongside a being a real number as well as c being the number that stays the same.*

$$|a - p/q| < \tfrac{c}{q^t} \tag{6.11}$$

This shows that a is not approximable to a number > t.

Proof. There is also another constant c that satisfies the inequalities

$$\tfrac{c}{q^t} < |a - p/q| < \tfrac{c'}{q^s} \tag{6.12}$$

in terms of p and q. □

Theorem 6.5. *There can be any value that is approximable to the number 1.*

Proof. See when c is approximable to 1 in order of q, you get

$$|a - p/q| = \tfrac{|qa-p|}{q} \leq \tfrac{1}{2q} < \tfrac{c}{q} \tag{6.13}$$

so that works hence c and almost any rational number can be approximable by 1. □

Lemma 6.6. *There is a constant c where a is not approximable to p/q like show here:*

$$|a - p/q| \geq \tfrac{c}{q} \tag{6.14}$$

Proof. Another example of this is:

$$|a - p/q| = \tfrac{|aq-pb|}{bq} \geq \tfrac{1}{bq} \tag{6.15}$$

□

Theorem 6.7. *Any rational number is not approximable to any constant number ≥ 1.*

Example. A is approximable to any rational number including 2 like here:

$$a = \sum_{k=0}^{\infty} 10^{-2^k} \tag{6.16}$$

Theorem 6.8. *Just like any rational number can be approximable to 1, any irrational number can be approximable to 2.*

Proof. Take a to be an irrational number and let the rational number be p_1 over q_1

$$|a - \frac{p_1}{q_1}| < \frac{1}{Q_{1q1}} < \frac{1}{q_1^2} \tag{6.17}$$

Now let rational number be p_2 over q_2 and see what we get:

$$0 < |a - \frac{p_2}{q_2}| < \frac{1}{q_2^2} \tag{6.18}$$

$$And \tag{6.19}$$

$$|a - \frac{p_2}{q_2}| < \frac{1}{Q_2} < |a - \frac{p_1}{q_1}| \tag{6.20}$$

So, by this we can see that indeed any rational number can be approximable by 2 as $\frac{p_2}{q_2} \neq \frac{p_1}{q_1}$. □

Theorem 6.9. *Roth's Theorem says that any algebraic number cannot be approximable to any number > than 2.*

Theorem 6.10. *If a is algebraic number then a cannot be approximable to any number > than n.*

Proof. So, if let say a is an irrational algebraic number with a degree greater than or equal to 2 we can see using the Mean Value Theorem which is primarily introduced in Calculus that:

$$f'(y) = \frac{f(x) - f(a)}{x - a} \tag{6.21}$$

Now use p and q as the rational numbers and we can see this:

$$f\tfrac{p}{q} = -f'(y)(a - \tfrac{p}{q}) \tag{6.22}$$

□

Theorem 6.11. *If you want to see Liouville's transcendental number, then this is what it looks like:*

$$\lambda = \sum_{k=1}^{\infty} 10^{-k!} \tag{6.23}$$

Proof. Think that λ has n as a degree.

$$q = 10^{m!} \tag{6.24}$$

$$And \tag{6.25}$$

$$p = q \sum_{k=1}^{m} 10^{-k!} \tag{6.26}$$

Also because p and q only have one common factor and that is 1 we can see this:

$$|\lambda - p/q| = \tfrac{1}{10^{m+1!}} + \tfrac{1}{10^{m+2!}} + ... < \tfrac{2}{10^{m+1!}} = \tfrac{2}{q^{m+1}} < \tfrac{2}{q^{n+1}} \tag{6.27}$$

□

Theorem 6.12. *Use p and q as rational integers as well as a be an algebraic number of nth degree and c being the number that remains the same. This is what it looks like:*

$$|qa - p| \geq \tfrac{c}{q^{n-1}} \tag{6.28}$$

Theorem 6.13. *Use g of degree m and c being the number that remains the same as well a being an algebraic number of nth degree. This is what it looks like:*

$$|g(a)| \geq \tfrac{c^m}{H(g)^{n-1}} \tag{6.29}$$

Proof. The maximum of the conjugates absolute value also known as a in the sequence: $a_1, a_2, ..., a_n$ shows this:

$$a = max|a_k| \tag{6.30}$$

Above in theorem 1.25 we use H(g) so according to that meaning here we do

$$|g(a_k) < |g_m||a_k|^m + |g_{m-1}||a_k|^{m-1} + ... + |g_1||a_k| + |g_0| \leq H(g)(a^m + a^{m-1} + ... + a + 1) \\ \leq H(g)(a+1)^m \tag{6.31}$$

for k.

Then seeing d as a denominator for the same sequence looks like this:

$$d^m g_m(da_k)^m + dg_{m-1}(da_k)^{m-1} + ...d^{m-1}g_1 da_k + d^m g_0 \tag{6.32}$$

and we can also see that this is an algebraic integer which is not the number 0. So looking at this you will also get

$$N = \prod_{k=1}^{n} d^m g a_k$$

since this also shows an algebraic integer which is not the number 0. □

Theorem 6.14. *Use ε of degree m and c being the number that remains the same as well a being an algebraic number of nth degree. This is what it looks like:*

$$|a - \varepsilon| \geq \tfrac{c^m}{H\varepsilon^n} \tag{6.33}$$

7. Irrationality of ζ

Apéry was a French mathematician who explained the irrationality of ζ. He showed that ζ cannot be a rational integer since it is approximable to any number greater than 1.

Definition 7.1. The ζ means this:

$$\zeta = \sum_{n=1}^{\infty} \frac{1}{n^3} = 1 + \frac{1}{2^3} + \frac{1}{3^3} + \frac{1}{4^3} + ...$$

Example. Apéry proved that $\zeta =$

$$\lim_{n\to\infty} \frac{a_n}{b_n}$$

A more easy way to prove this is

$$\zeta - \frac{a_n}{b_n} = \sum_{k=n+1}^{\infty} \frac{6}{k^3 b_k b_{k-1}}$$

and continuing it we see

$$0 < \zeta - \tfrac{a_n}{b_n} < \tfrac{c_1}{b_n^2} \tag{7.1}$$

a constant c but it still doesn't show ζ as being approximable to 2 so to find that, we do

$$p_n = 2L_n^3 a_n \tag{7.2}$$

$$And \tag{7.3}$$

$$q_n = 2L_n^3 a_n \tag{7.4}$$

And to define p_n and q_n we do

$$0 < |\zeta - \tfrac{p_n}{q_n}| < \tfrac{c_1}{b_n^2} \tag{7.5}$$

We have to find a constant s that is approximable to a number greater than 1 so it would like this:

$$\tfrac{1}{b_n^2} < \tfrac{1}{q_n^s} \tag{7.6}$$

However we don't know anything about the size of b_n so to find that we do it as an example like this one:

$$\lambda = 17 + 12\sqrt{2} \tag{7.7}$$

and then continuing the same example we get

$$\frac{b_n}{\lambda^n/n^{3/2}} \tag{7.8}$$

seeing that a has a degree n which is infinity and so there are also going be constant c's that look like this:

$$\frac{c_2\lambda^n}{n^{3/2}} < b_n < \frac{c_3\lambda^n}{n^{3/2}} \tag{7.9}$$

Theorem 7.2. *The Prime Number Theorem is*

$$\pi(x) \sim \frac{x}{logx} \text{ as } x \to \infty \tag{7.10}$$

This theorem is used to find the lcm or least common multiple of the first n terms in a sequence so it would like this:

$$L_n = lcm(1, 2, ..., n) = \prod_{p \geq n} p^a \geq \prod_{p \geq n} n = n^{\pi(n)}$$

If c is a constant greater than e then the theorem would look like this;

$$\frac{\pi(n)}{\frac{n}{logn}} < \log c \tag{7.11}$$

And then this:

$$L_n \leq n^{\pi(n)} = e^{\pi(n)\log n} < c^n \tag{7.12}$$

References

[1] David Angell. *Irrationality and transcendence in number theory.* CRC Press, Taylor and Francis Group, Boca, Raton, 2022.

[2] Libretexts. 17.3: Irreducible polynomials.

[3] MathOnline. Example questions regarding gauss's lemma.

[4] Encyclopedia of Mathematics. Algebraic number.

[5] The Math Sorcerer. Proving a Polynomial is Irreducible with Eisentein's Criterion. `https://www.youtube.com/watch?v=DyYY6JwSdnk`, September 2020.

[6] D. Zagier. The american mathematical monthly, vol. 104, no. 8 (oct., 1997), pg. 705.

[2] [1] [4] [3] [5] [6]