Expression of Algebraic and Transcendental Numbers

Aastha

Euler Circle

2023

Complex Number

An algebraic number is the root of a polynomial

$$a_n z^n + a_{n-1} z^{n-1} + ... + a_1 z + a_0 \tag{1}$$

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

Complex Number

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

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. Ex. $\cos\frac{1}{7}\pi, \cos\frac{3}{7}\pi$ 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.

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

Complex Number

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

$$g(z) = f_a(z)q(z) + r(z) \tag{2}$$

$r(a) = 0$. 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.

Complex Number

Looking back to the second complex number slide, 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.

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.

Proving polynomials irreducible

Lemma

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. □

Eisenstein's Lemma

Eisenstein's Lemma simplifies the proof of irreducibility for

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

Looking at this factored:

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

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

Proving Polynomials Irreducible

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. □

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

$$\mathrm{f}_3(z) = z^3 + 2z^2 + 1 \tag{5}$$

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

$$\mathrm{f}_3(0) = 1 \text{ , } f_3(1) = 1 \text{ and } f_3(2) = 2 \tag{6}$$

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

Proving Polynomials Irreducible

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

Proof.

Assume that: □

$$a_n a^n + a_{n-1} a^{n-1} + a_{n-2} a^{n-2} + \ldots + a_1 a + a_0 = 0 \tag{7}$$

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

$$(a_n a)^n + a_{n-1}(a_n a)^{n-1} + a_{n-2} a_n (a_n a)^{n-2} + \ldots + a_1 a_n^{n-2}(a_n a) + a_0 a_n^{n-1} = 0 \tag{8}$$

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

Proving Polynomials Irreducible

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.

Going back to lemma 1.2 for example of number 2 where a $=$ $cos 1/7\pi$ 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

$$(2\text{a})^3 - (2a)^2 - 2(2a) + 1 = 0. \tag{9}$$

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

Proving Polynomials Irreducible

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

$$\sum \mathrm{r}_k a_k \tag{10}$$

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

$$\sum \mathrm{m}_k a_k \tag{11}$$

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.

Proving Polynomials Irreducible

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 $1, a, a^2, \ldots, a^{n-1}$, 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:

$$\mathrm{ap}_k = m_{k1}p_1 + m_{k2}p_2 + \ldots + m_{kn}p_n \text{ for } k = 1, 2, \ldots, n \quad (12)$$

Proving Polynomials Irreducible

If a and B are algebraic, then aB and a$\pm$B are also algebraic.

Proof.

Every power of a+B looks like this:

$$(\mathrm{a}+\mathrm{B})^k = \sum_{j=0}^{k} \binom{k}{j} a^j B^{k-j} \tag{13}$$

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

$$(\mathrm{a}+\mathrm{B})^k = \sum_{i=0}^{m-1} \sum_{j=0}^{n-1} r_{ij} a^i B^j \tag{14}$$

□

Proving Polynomials Irreducible

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

$$\mathrm{b}_n z^n + b_{n-1} z^{n-1} + ... + b_1 z + b_0 \tag{15}$$

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

$$\mathrm{b}_0 z^n + b_1 z^{n-1} + ... + b_{n-1} z + b_n \tag{16}$$

Proving Polynomials Irreducible

A Complex number B is equivalent to the root of a polynomial

$$a_n z^n + a_{n-1} z^{n-1} + ... + ab_1 z + a_0 \tag{17}$$

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

$$z^n + a_{n-1} z^{n-1} + ... + ab_1 z + a_0 \tag{18}$$

who has algebraic integer coefficients.

Proving Polynomials Irreducible

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

$$\mathrm{a}_0^{m_0} a_1^{m_1} \ldots a_{n-1}^{m_n - 1} B^m \tag{19}$$

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

$$0 \leq mk < dk \tag{20}$$

And this:

$$0 \leq m < n \tag{21}$$

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

$$\mathrm{d}_0 d_1 \ldots d_{n-1} n \tag{22}$$

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

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.

Transcendental Numbers

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 $an \neq 0$

$$a_n z^n + a_{n-1} z^{n-1} + ... + a_1 z + a_0 \rightarrow (a_n, a_{n-1}, ..., a_1, a_0) \quad (23)$$

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:

$$|a - p/q| \tag{24}$$

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

$$|a - p/q| < c/q^s \tag{25}$$

satisfies the rational numbers p and q.

Transcendental Numbers

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:

$$a = \sum_{k=0}^{\infty} 10^{-2^k} \tag{26}$$

This has been proved to be irrational.

Transcendental Numbers

If we use rationals p and q and the variable we use to measure everything is

$$q = 10^{2^m} \tag{27}$$

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

$$|a - p/q| = \frac{1}{10^{2m+1}} + \frac{1}{10^{2m+2}} + ... < \frac{2}{10^{2m+1}} = \frac{2}{q^2} \tag{28}$$

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