Real Analysis

Project Work

Chinmay Sharma
Roll No. 2022113005
Group 10

December 2022

1 Introduction and Acknowledgement

This project work was undertaken to study the applications of topics related to real analysis covered in class in various fields and to create an original question related to them.

I would like to express my gratitude towards Prof. Siddhartha Das and Mr. Prithwi Bagchi whose inputs were essential to the creation of this project.

2 Question

Problem: *Prove that the set of infinite binary sequences is equivalent to the set of irrational numbers without assigning Cardinal Numbers to these sets*

Let the set of infinite binary sequences be denoted by B and the set of irrational numbers by I. This problem is trivial if we are allowed to use the Cardinal Numbers, since

$$|I| = |B| = |P(\mathbb{N})| = \aleph_1 \tag{1}$$

This is the original motivation for the problem. Since these sets have the same cardinality, it should be possible to compare them directly or exhibit an indirect comparison between them. To prove this we demonstrate injection in two ways and utilise the **Cantor-Schröder-Bernstein Theorem** to compare the cardinalities of these sets.

Proof of injection from B to $\mathbb{R}/\mathbb{Q}$: First we index each binary string by $\mathbb{N}$. For each binary string b, define the function $f\colon B \to \mathbb{R}/\mathbb{Q}$

$$f(b) = \sum_{i=1}^{\infty} \cos\left(\frac{\pi}{i+3}\right) \ (\forall i \in \mathbb{N}\colon b_i = 1) \tag{2}$$

i.e we choose i such that there is a 1 in the nth index of the binary sequence.

Lemma: $\cos\frac{\pi}{n}$ **is irrational** $\forall n > 3$

Proof: Note that if the lemma is true $\forall$ odd $n > 3$, then it will hold $\forall n > 3$. This is true because $\cos\frac{\pi}{2n}$ being rational implies that $cos\frac{\pi}{n}$ is rational by double angle formulas.

Now assume for the sake of contradiction that $\cos\frac{\pi}{n} = \frac{p}{q}$ where p and q are coprime.

$(\cos\frac{\pi}{n} + i\sin\frac{\pi}{n})^n = -1$ Now we have $\sin\frac{\pi}{n} = \sqrt{1-\frac{p^2}{q^2}}$. We expand using the binomial theorem, and consider only the real part. Note that we will only have even powers of sin terms, since odd powers are imaginary. We now obtain:

$$\frac{p^n}{q^n}\binom{n}{2}\frac{p^{n-2}}{q^{n2}}(1-\frac{p^2}{q^2}) + \binom{n}{4}\frac{p^{n-4}}{q^{n-4}}(1-\frac{p^2}{q^2})^2 \ldots = -1 \tag{3}$$

. Multiplying both sides by q^n , we obtain:

$$p^n - \binom{n}{2}p^{n-2}(p^2-q^2) + \binom{n}{4}p^n(p^2-q^2)^2 \ldots = -q^n \tag{4}$$

Since n is odd, the last term on the LHS will still have a factor of p, so p divides the LHS, implying $p \mid -q^n$. But since $cos(\frac{\pi}{n})$ is increasing in n for $n \geq 3$, we have $\frac{1}{2} < cos(\frac{\pi}{n}) < 1$ which implies that p is at least 2. So $p \mid -q^n$ is a contradiction since p and q are coprime and p is not 1.

Since such a sum is possible for all binary sequences, It is easy to check that this function is an injection from the set of binary sequences onto a subset of irrationals. However we know that if $f\colon A \to B$ is an injective function then $|A| \leq |B|$. This proves the first part of the question.

Proof of Injection from I to B: First we prove that the composition of injections is an injection. Then we construct a series of such injections which maps $\mathbb{R} \to$ B, hence mapping $\mathbb{R}/\mathbb{Q} \to B$

Lemma 1. *Composition of Injections is an Injection*

assume f and g are injective and suppose $g \circ f(x_1) = g \circ f(x_2)$ This means $g(f(x_1)) = g(f(x_2))$ this implies (by the injectivity of g), $f(x_1) = f(x_2)$ Injectivity of f allows us to argue that $x_1 = x_2$

Consider the injection from $\mathbb{R} \setminus \mathbb{Q}$ to $(0,1)$, given by

$$f(x) = \frac{1}{\pi}\arctan(x) + \frac{1}{2} \tag{5}$$

this is a bijection from $\mathbb{R}$ to (0,1) and it is trivial to verify that it is hence an injection from $\mathbb{R}\backslash\mathbb{Q}$ to (0,1).

Let B:=0,1N with N=1,2,.... Consider the inverse of the function given by:

$$g(x) := \sum_{k=1}^{\infty} x_k 2^{-k} \tag{6}$$

This function interprets a string $x \in B$ as infinite binary fraction $0.x_1x_2x_3 \ldots$

The function g maps B almost bijectively onto [0,1]. The dyadic rationals in $]0,1[$ have two preimages, e.g., $g(1,0,0,0,\dots) = g(0,1,1,1,\dots)$. Since we are only concerned with $\mathbb{R}\backslash\mathbb{Q}$, these cases do not need to be considered. We see that the inverse of this function exists and is an injection from (0,1) into B.

we know that if $f\colon A \to B$ is an injective function then $|A| \leq |B|$. This proves the second part of the question. Using the Cantor-Schröder-Bernstein theorem it is now possible to say that these two sets are equivalent.

3 Restricted Comprehension Principle

Russell's Paradox: a statement found in 1901 by Bertrand Russell which challenged the basic assumptions of naive set theory. This led to the axiomatization of set theory with the development of systems like ZF.

Restricted Comprehension Principle and Formulation of Russell's Paradox: In naive set theory, there is the principle of Unrestricted comprehension which states that:

$$(\exists y)(y = x\colon Fx) \tag{7}$$

i.e, To every condition we place, there exists a set of objects satisfying only those conditions[2]. Russell's Paradox comes about when we consider the formula Fx to be:

$$R = (x\colon x \notin x) \tag{8}$$

Solution to Russell's Paradox and the Axiom of Specification: As explained in the previous paragraph, Russell's paradox arises when we consider 'The set of all sets which are not members of themselves'. The Axiom of specification provides a solution to this problem.

Axiom 1. ***Axiom of Specification:*** *If A is a set and S(x) is a logical condition, then there is a set B whose elements are exactly those $x \in A$ such that S(x) is true*

In this formulation of the Axiom of Specification, we allow predicates only to be applied to subsets of an already constructed set. Hence, we cannot arbitrarily construct any set with any predicates we want. In particular, to construct the set R as defined above, we need to have already constructed R. This is prevented by other axioms in ZF, namely the Axiom of Regularity and the Axiom of pairing.

Axiom 2. ***Axiom of Pairing*** *Given sets A and B, there is a set C whose elements are exactly the two sets. That is, $C = \{A, B\}$*

Axiom 3. ***Axiom of Regularity*** *Given a set $A \neq \phi$, there is an $x \in A$ such that when x is a set it satisfies $A \cap x = \phi$*

Applications: Many concepts in mathematics can be precisely defined only with set theoretic concepts. This example demonstrates the ideas and approach of analysis where we rigorously define and study the properties of mathematical objects. In trying to rigorously define the basic notions of the system of mathematics, such a paradox was revealed which led to a more robust reformulation for the foundations of mathematics. The **axiomatic method** has far reaching consequences for all fields of mathematics such as graph theory, linear algebra, topology, analysis etc. and hence its effects and applications extend to the interaction of all these mathematical fields with other disciplines such as physics, economics, natural sciences etc.

4 Fermat's Little Theorem and Euler's Theorem

Fermat's little theorem is an important result in number theory. Since its initial proposition in 1640, there have been various proofs of this result which have had widespread applications. Here we present a solution based on introductory group theoretic concepts which then generalizes to a proof of Euler's Theorem.

Definition 1. *A **group** is a set G with a binary operation $*\colon G \times G \to G$ such that:*

1 **Closure:** G is closed under the binary operation *

$$\forall a, b \in G, a * b \in G \tag{9}$$

2 **Identity:** There exists an identity e contained in G such that

$$a * e = a = e * a \tag{10}$$

3 **Associativity:**The operation $*$ is associative, so

$$\forall a, b, c \in G, a * (b * c) = (a * b) * c. \tag{11}$$

4 **Inverse**There are inverses for all elements in G, thus

$$\forall a \in G, \exists a^{-1} \in G\colon a * a^{-1} = e \tag{12}$$

Note that a group may not be commutative. Groups that satisfy commutativity are called **Abelian Groups**.

Definition 2. *A **subgroup** H is a nonempty subset of a group G which is a group under the restricted operation. We denote a subgroup by $H \leq G$.*

Definition 3. *The **order** of a group or subgroup, denoted $|G|$, is the number of elements contained in it i.e its cardinality.*

Theorem 1. ***Lagrange's Theorem:*** *If G is a finite group and H a subgroup then $|H|$ divides $|G|$*

Proof: Define a relation $\sim$ on G by $g_1 \sim g_2$ iff $g_1^{-1}g_2 \in H$. This is reflexive (since H contains the identity), symmetric (since $g_2^{-1}g_1 = (g_1^{-1}g_2)^{-1}$ and H is closed under inverses) and transitive (as $g_1^{-1}g_3 = (g_1^{-1}g_2)(g_2^{-1}g_3)$ and H is closed under products).

Hence it is an equivalence relation, and G is partitioned into equivalence classes. We now claim that for each $g \in G$ its equivalence class $[g]$ has size $|H|$, so that $|G| = |H| \times$ No. of equivalence classes is divisible by $|H|$. We define a map $f\colon [g] \to H$ by $x \to g^1 x$

To show that f is well-defined: If $x \in [g]$ then $g^{-1}(x) \in H$ so $f(x) \in H$.

To show that f is bijective : Its inverse is $x \to gx$ (this is similarly well-defined $H \to |g|$). Thus $|[g]| = |H|$ and we're done

Theorem 2. ***Bezout's Identity:*** *Let a and b be integers with greatest common divisor d. Then there exist integers x and y such that $ax + by = d$. Moreover, the integers of the form $az + bt$ are exactly the multiples of d.*

The proof of Bézout's identity uses the property that for nonzero integers a and b, dividing a by b leaves a remainder of r_1 strictly less than $|b|\gcd(a, b) = \gcd(r_1, b)$. Then by repeated applications of the Euclidean division algorithm, we have

a = b x$_1 + r_1, 0 < r_1 < |b|$
$b = r_1 x_2 + r_2, 0 < r_2 < r_1$
$\vdots$
$r_{n-1} = r_n x_{n+1} + r_{n+1}, 0 < r_{n+1} < r_n$
$r_n = r_{n+1} x_{n+2}$

where the r_{n+1} is the last nonzero remainder in the division process. Now, as illustrated in the example above, we can use the second to last equation to solve for r_{n+1} as a combination of r_n and r_{n-1}. Unfolding this, we can solve for r_n as a combination of r_{n-1} and r_{n-2}, etc. until we eventually write r_{n+1} as a linear combination of a and b. Since r_{n+1} is the last nonzero remainder in the division process, it is the greatest common divisor of a and b, which proves Bézout's identity.

Lemma 2. *The set G of residues modulo p is a group under the group operation of multiplication*

Proof: We prove that G satisfies all the group axioms hence proving that it is a group.

1 **Closure-** Since each $x \in \mathbb{Z}$ can be represented as a residue from $(0, .., (p-1))$ and closure is inherited from Z, we just need to check that the product of two elements does not equal 0 to prove this. However, this is trivial since p is a prime and its only divisors are 1 and p. So the multiplication of any numbers in this set cannot equal 0 and hence the set is closed.

2 **Associativity-** is inherited from $\mathbb{Z}$

3 **Identity element-** 1, is inherited from $\mathbb{Z}$

4 **Inverse-** We use Bezout's Lemma to show that the elements of G are invertible. If we take $g \in G$ and p, they must be relatively prime since p is prime. This implies that $gcd(g, p) = 1$. By Bezout's Lemma there exists integers x, y such that

$$gx + py = gcd(g, p) = 1 \tag{13}$$

When we put this in terms of modular arithmetic,

$$gx \equiv 1 \pmod{p} \tag{14}$$

. As a result, x must be an inverse of g.

Hence, G satisfies all the group axioms and hence it is a group.

Theorem 3. ***Fermat's Little Theorem*** *For any natural number a and prime p, we have the following:*

$$a^p \equiv a \pmod{p} \tag{15}$$

Proof: Suppose p (assume as above, the other case is trivial). Since the set of residues modulo p forms a group and a is coprime to p, the group performed by multiplying each of these members by a is a permutation of these same modular inverses and is hence also a group. I.e the set of powers forms a subgroup of $(\mathbb{Z}/p)^*$. Its order is the multiplicative order of a; if it is $x > 0$, the subgroup consists of the x elements $\{1, a, a^2, \ldots, a^{x-1}\}$. By Lagrange's theorem, x divides the order of $(\mathbb{Z}/p)^*$ which is p-1. So $xy = p - 1$ for some integer y. Then:

$$a^{p-1} \equiv a^{xy} \equiv (a^x)^y \equiv 1^y \equiv 1 \pmod{p}. \tag{16}$$

Multiplying this equation by a gives the required result. This is possible because a is coprime to p.

Fermat's Little Theorem is a special case of Euler's Theorem in number theory.

Theorem 4. *Let n be a positive integer, and let a be an integer that is relatively prime to n. Then*

$$a^{\phi(n)} \equiv 1 \pmod{n}, \tag{17}$$

where $\phi(n)$ is ***Euler's Totient function****, which counts the number of positive integers which are relatively prime to n.*

The proof of Euler's Totient function is similar to Fermat's Little Theorem, where we consider only the set of residues of n which are coprime (through the totient function) with n which equips it with similar structure as the residues modulo a prime.

Applications: Both of these theorems have applications in public key cryptography and primality testing. Euler's theorem in particular underlies the RSA cryptosystem, which is widely used for Internet communications. In this system, Euler's theorem is used with n being a product of two large prime numbers, and the security of the system is based on the difficulty of factoring such an integer.

5 Bibliography

1. Chapter 1- Describing the approach of analysis
2. The Axiomatic Method
3. Russell's Paradox
4. Axiom of Comprehension
5. Paper on proving Fermat's theorem through group theory
6. Handout on proving Bezout's identity and the Extended Euclidean Algorithm
7. Original Paper by RSA, utilizing Fermat's theorem as a check for correctness