Department of Mathematics
University of Education, Lahore

Foundations and Applications of Algebraic Number Theory

Submitted By: Ayesha Arif (BSF1900982)
Supervisor: Dr. Samina Mazhar

Abstract

This project explores the fundamental aspects of Algebraic Number Theory, including number fields, algebraic integers, factorization in rings of integers, Galois theory, and various applications in cryptography and modern number theory. The project also highlights real-world uses, including secure communications and error correction methods.

Contents

1 Introduction

Algebraic Number Theory (ANT) is the study of algebraic structures related to the set of integers. It extends classical number theory by considering numbers as elements of larger algebraic systems. The field provides a framework to understand prime factorization in more general settings and is crucial for solving problems in pure and applied mathematics.

The roots of ANT lie in the work of mathematicians like Gauss, Dedekind, and Noether. Their ideas led to deep results concerning number fields, ideal class groups, and Diophantine equations. This project will explore these foundational concepts and their significance.

2 Number Fields and Algebraic Integers

2.1 Number Fields

A number field is a finite field extension of the rational numbers $\mathbb{Q}$. That is, a number field K is formed by adding algebraic numbers to $\mathbb{Q}$. The minimal polynomial of these numbers determines the structure of K.

Example: $\mathbb{Q}(\sqrt{2})$ is a quadratic number field obtained by adjoining $\sqrt{2}$ to $\mathbb{Q}$.

2.2 Algebraic Integers

An algebraic integer is a complex number that is a root of a monic polynomial with integer coefficients. The set of all algebraic integers in a number field forms a ring, known as the ring of integers $\mathcal{O}_K$.

Example: In $\mathbb{Q}(\sqrt{-3})$, the ring of integers is $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, which includes elements like $1+\sqrt{-3}$.

3 Factorization in Rings of Integers

In contrast to the integers, where every number has a unique prime factorization, the same is not always true in number fields. Some number fields lack unique factorization, requiring the study of ideal factorization.

Example: In $\mathbb{Q}(\sqrt{-5})$, the number 6 has multiple factorizations:

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5}).$$

Since these factorizations are non-trivial, unique factorization does not hold in this field.

To resolve this, we introduce ideal factorization, where every ideal in the ring of integers can be uniquely factored into prime ideals.

4 Galois Theory and Its Role in Number Fields

4.1 Galois Groups

A Galois group describes the symmetries of a field extension. The study of these groups helps classify number fields and solve polynomial equations.

Example: The Galois group of $\mathbb{Q}(\sqrt{2})$ over $\mathbb{Q}$ consists of two elements: the identity function and the automorphism mapping $\sqrt{2}$ to $-\sqrt{2}$.

4.2 Solvability by Radicals

A polynomial equation is solvable by radicals if its Galois group is a solvable group. This explains why general quintic equations cannot be solved using radicals.

5 Prime Ideals and Class Groups

Prime ideals generalize prime numbers to the setting of number fields. They help describe factorization in rings of integers and play a fundamental role in modern algebraic number theory.

The class group of a number field measures the failure of unique factorization. It is given by the set of fractional ideals modulo principal ideals.

Example: The class number of $\mathbb{Q}(\sqrt{-23})$ is 3, indicating that it has three distinct ideal classes.

6 Applications of Algebraic Number Theory

6.1 Cryptography

Many modern encryption schemes, such as RSA and lattice-based cryptography, rely on properties of algebraic number theory.

Example: RSA encryption is based on the difficulty of factoring large numbers into their prime components, a fundamental problem in number theory.

6.2 Error-Correcting Codes

Reed-Solomon and BCH codes use algebraic number theory to construct efficient error detection and correction systems.

6.3 Fermat's Last Theorem

Andrew Wiles' proof of Fermat's Last Theorem was deeply rooted in algebraic number theory, particularly in the study of elliptic curves and modular forms.

7 Conclusion

Algebraic Number Theory provides a bridge between classical number theory and modern applications. The study of number fields, prime factorization, and Galois theory has led to profound mathematical insights and real-world applications in cryptography, error correction, and theoretical physics.

Future research in algebraic number theory continues to uncover new results, particularly in the realms of computational number theory and algebraic geometry.

References

1. Marcus, D. "Number Fields."
2. Silverman, J. "Advanced Topics in the Arithmetic of Elliptic Curves."
3. Cox, D. "Primes of the Form $x^2 + ny^2$."
4. Lang, S. "Algebraic Number Theory."