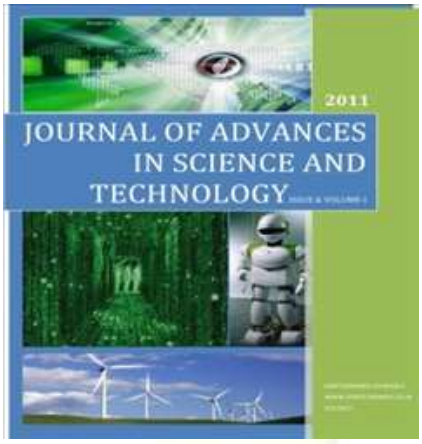
ISSN-2230-9659

# Theoretical Concept of Algebraic Number Theory




**Radheshyam Ramkisan Sharma**

Research Scholar

**ABSTRACT:-**

In this paper we present about theoretical concept of algebraic number theory. Algebraic number theory studies algebraic properties of the ring of algebraic integers in a number field. We describe various algebraic invariants of number fields, as well as their applications. These applications relate to prime ramification, the finiteness of the class number, cyclotomic extensions, and the unit theorem.

**Keywords: -** Number theory, Algebraic number, Polynomial

**INTRODUCTION:**

Number theory is often described as the study of the integers, algebraic number theory may be loosely described as the study of certain subrings of fields K with $[K : \mathbb{Q}] < \infty$; these rings, known as "rings of integers", tend to act as natural generalizations of the integers.

P.G.L. Dirichlet's (1805 - 1859) studies on what we today call units in the rings of integers of number fields, the notion was not that one was studying a collection called a "number field" but that one was simply studying the rational functions in a given algebraic number, i.e. expressions of the form

ISSN-2230-9659

$$\frac{c_m\alpha^m + c_{m-1}\alpha^{m-1} + \cdots + c_0}{d_n\alpha^n + d_{n-1}\alpha^{n-1} + \cdots + d_0}$$

Where the coefficients $c_i$ and $d_j$ were rational numbers, and where *a* was some fixed algebraic number, i.e. the root of a polynomial

$$a_k z^k + a_{k-1} z^{k-1} + \cdots + a_0$$

With rational coefficients.

**ALGORITHMS IN ALGEBRAIC NUMBER THEORY**

Algebraic number theory has in recent times been applied to the solution of algorithmic problems that, in their formulations, do not refer to algebraic number theory at all. That this occurs in the context of solving diophantine equations does not come as a surprise, since these lie at the very roots of algebraic number theory. A better example is furnished by the seemingly elementary problem of decomposing integers into prime factors. Among the ingredients that make modern primality tests work one may mention reciprocity laws in cyclotomic fields, arithmetic in cyclic fields, the construction of Hilbert class fields of imaginary quadratic fields, and class number estimates of fourth degree CM-fields. The best rigorously proved time bound for integer factorization is achieved by an algorithm that depends on quadratic fields , and the currently most promising practical approach to the same problem, the *number field sieve*, employs "random" number fields of which the discriminants are so huge that many traditional computational methods become totally inapplicable. The analysis of many algorithms related to algebraic number fields seriously challenges our theoretical understanding, and one is often forced to argue on the basis of heuristic assumptions that are formulated for the occasion.

Theorem- *Under deterministic polynomial time reductions, Problem - is equivalent to the problem of finding the largest square factor of a given positive integer.*

The problem of finding the largest square factor of a given positive integer *m* is easily reduced to Problem by considering the number field $K = \mathbf{Q}(\sqrt{m})$ For the opposite reduction, which in computer science language is a "Turing" reduction, Since there is no known algorithm for finding the largest square factor of a given integer *m* that is significantly faster than factoring *m*, Theorem shows that

ISSN-2230-9659

Problem is currently intractable. More seriously, even if someone *gives* us $\mathcal{O}$, we are not able to recognize it in polynomial time, even if probabilistic algorithms are allowed.

## NUMBER FIELDS

Definition. A nmnher field K is a fmito field extension of $\mathbb{Q}$. Its degree is $[K : Q]$. i.e.. Its dimension as a $\mathbb{Q}$-vector space.

Definition. An algebraic number $\alpha$ is an algebraic integer if it satisfies an inonic polynomial with integer coefficients. liquivalently. Its minimal polynomial over $\mathbb{Q}$ should have integer coefficients.

### COMPUTATIONAL NUMBER THEORY

Cohen 1993 and Pohst and Zassenhaus 1989 provide algorithms for most of the constructions we make in this course. The first assumes the reader knows number theory, whereas the second develops the whole subject algorithmically. Cohen's book is the more useful as a supplement to this course, but wasn't available when these notes were first written. While the books are concerned with more-or-less practical algorithms for fields of small degree and small discriminant, Lenstra (1992) concentrates on finding "good" general algorithms. Dedekind 1996, with its introduction by Stillwell, gives an excellent idea of how algebraic number theory developed. Edwards 1977 is a history of algebraic number theory, concentrating on the efforts to prove Fermat's last theorem. The notes in Narkiewicz 1990 document the origins of most significant results in algebraic number theory. Lemmermeyer 2009, which explains the origins of "ideal numbers", and other writings by the same author, e.g., Lemmermeyer 2000, 2007.

### CONCLUSION:

In this paper we found that the main interest of algorithms in algebraic number theory is that they provide number theorists with a means of satisfying their professional curiosity. The praise of numerical experimentation in number theoretic research is as widely sung as purely numerological investigations are indulged in, and for both activities good algorithms are indispensable.

### REFERENCES:


- COHEN, H. 1993. A course in computational algebraic number theory, volume 138 of Graduate Texts in Mathematics. Springer-Verlag, Berlin.

ISSN-2230-9659


- POHST, M. AND ZASSENHAUS, H. 1989. Algorithmic algebraic number theory, volume 30 of Encyclopedia of Mathematics and its Applications. Cambridge University Press, Cambridge
- DEDEKIND, R. 1996. Theory of algebraic integers. Cambridge Mathematical Library. Cambridge University Press, Cambridge. Translated from the 1877 French original and with an introduction by John Stillwell.
- EDWARDS, H. M. 1977. Fermat's last theorem, volume 50 of Graduate Texts in Mathematics. Springer-Verlag, New York. A genetic introduction to algebraic number theory.
- NARKIEWICZ, W. 1990. Elementary and analytic theory of algebraic numbers. SpringerVerlag, Berlin, second edition.
- LEMMERMEYER, F. 2000. Reciprocity laws. Springer Monographs in Mathematics. Springer-Verlag, Berlin. From Euler to Eisenstein.
- LEMMERMEYER, F. 2007. The development of the principal genus theorem, pp. 529–561. In The shaping of arithmetic after C. F. Gauss's Disquisitiones arithmeticae. Springer,Berlin.
- LEMMERMEYER, F. 2009. Jacobi and Kummer's ideal numbers. Abh. Math. Semin. Univ. Hambg. 79:165–187