International Journal of Applied Research 2015; 1(7): 810-812

ISSN Print: 2394-7500
ISSN Online: 2394-5869
Impact Factor: 3.4
IJAR 2015; 1(7): 810-812
www.allresearchjournal.com
Received: 07-04-2015
Accepted: 10-05-2015

Nurul Amin
Research Scholar,
Maharishi University of Information Technology, Lucknow, Uttar Pradesh, India.

Dr. VK Rathaur
(Phd in Mathematics),
Maharishi University of Information Technology, Lucknow, Uttar Pradesh, India.

Correspondence
Nurul Amin
Research Scholar,
Maharishi University of Information Technology, Lucknow, Uttar Pradesh, India.

Theoretical concept of number fields theory

Nurul Amin, Dr. VK Rathaur

Abstract
Algebraic Geometry is the study of sets of common zeros of a family of polynomials. Such a set is called an algebraic variety. Some geometers at LSU work mostly over the complex numbers. Some work mostly over the real numbers, where one studies semi-algebraic sets whose points satisfy polynomial inequalities. Some work over finite fields, where there are connections with algebraic number theory and applications to areas such as error-correcting codes. Arithmetic algebraic geometry, the study of algebraic varieties over number fields, is also represented at LSU. The tools in this specialty include techniques from analysis and computational number theory. In all these facets of algebraic geometry, the main focus is the interplay between the geometry and the algebra. For example, to each point of an algebraic variety one can associate a ring and the question of whether this point is a smooth point or a singular point on this variety can be answered by understanding the algebraic structure of this ring.

Keywords: Algebraic, Geometry, number theory, Arithmetic.

Introduction

Algebraic number theory is a rich and diverse subfield of abstract algebra and number theory, applying the concepts of number fields and algebraic numbers to number theory to improve upon applications such as prime factorization and primarily testing [1-4]. In this study, we will begin with an overview of algebraic number fields and algebraic numbers. We will then move into some important results of algebraic number theory, focusing on the quadratic, or Gauss reciprocity law. In this research, we will cover the basics of what is called algebraic number theory. Just as 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. However, although algebraic number theory has evolved into a subject in its own right, we begin by emphasizing that the subject evolved naturally as a systematic method of treating certain classical questions about the integers themselves [5]. Much of our endeavor in the theoretical study of computation is aimed towards either finding an efficient algorithm for a problem or gauging the *hairiness* of a problem. And in meeting both these goals mathematical insights and ingenuities are constant companions. In particular, two branches of mathematics - combinatory, and algebra and number theory, have found extensive applications in theoretical computer science. In this paper, our focus is on problems belonging to the latter branch [6].

Review of Literature

An algebraic number field is a finite extension of $\mathbb{Q}$; an algebraic number is an element of an algebraic number field. Algebraic number theory studies the arithmetic of algebraic number fields — the ring of integers in the number field, the ideals in the ring of integers, the units, the extent to which the ring of integers fails to behave unique factorization, and so on. One important tool for this is "localization", in which we complete the number field relative to a metric attached to a prime ideal of the number field [7]. The completed field is called a local field — its arithmetic is much simpler than that of the number field, and sometimes we can answer questions by first solving them locally, that is, in the local fields [8].
An abelian extension of a field is a Galois extension of the field with abelian Galois group

[9]. Global class field theory classifies the abelian extensions of a number field K in terms of the arithmetic of K; local class field theory does the same for local fields. This course is concerned with algebraic number theory. Its sequel is on class field theory [10].

I now give a quick sketch of what the course will cover. The fundamental theorem of arithmetic says that integers can be uniquely factored into products of prime powers: an $m \neq 0$ in $\mathbb{Z}$ can be written in the form, $m = up_1^{r_1} \cdots p_n^{r_n}, \quad u = \pm 1, \; p_i$ prime number, $r_i > 0,$ and this factorization is essentially unique.

Consider more generally an integral domain A. An element $a \in A$ is said to be a unit if it has an inverse in A: I write $A^{\times}$ for the multiplicative group of units in A. An element p of A is said to prime if it is neither zero nor a unit, and if

$$p|ab \Rightarrow p|a \text{ or } p|b.$$

If A is a principal ideal domain, then every nonzero no unit element a of A can be written in the form, $a = p_1^{r_1} \cdots p_n^{r_n}, \; p_i$ prime element, $r_i > 0,$ and the factorization is unique up to order and replacing each p_i with an associate, i.e., with its product with a unit.

Our first task will be to discover to what extent unique factorization holds, or fails to hold, in number fields. Three problems present themselves [11]. First, factorization in a field only makes sense with respect to a subring, and so we must define the "ring of integers" $\mathcal{O}_K$ in our number field K. Secondly, since unique factorization will in general fail, we shall need to find a way of measuring by how much it fails. Finally, since factorization is only considered up to units, in order to fully understand the arithmetic of K, we need to understand the structure of the group of units UK in $\mathcal{O}_K$ resolving these three problems will occupy the first five sections of the course [12].

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

Definition: An algebraic number α is an algebraic integer if it satisfies an ionic polynomial with integer coefficients. Liquid valiantly its minimal polynomial over $\mathbb{Q}$ should have integer coefficients.

Definition: Let K be a number field. Its ring of integers $\mathcal{O}_K$ consists of the elements of K which are algebraic integers.

(i) $\mathcal{O}_K$ is a Noetherian ring.

(ii) $\operatorname{rank}_{\mathbb{Z}} \mathcal{O}_K = [K : \mathbb{Q}]$. i.e. $\mathcal{O}_K$ is a finitely generated abelian group under addition, and isomorphic to $\mathbb{Z}^{\oplus[K:\mathbb{Q}]}$

(iii) For every $\alpha \in K$ there exists $n \in N$ with $\alpha n \in \mathcal{O}_K$

(iv) $\mathcal{O}_K$ is the maximal subring of K which is finitely generated as an abelian group.

(v) $\mathcal{O}_K$ is integrally closed, i.e.. ii" $f(X) \in \mathcal{O}_K[X]$ is ionic and $f(\alpha) = 0$ for some $\alpha \in K$ then $\alpha \in \mathcal{O}_K$

Example

Number field K	Ring of integers $\mathcal{O}_K$
$\mathbb{Q}$	$\mathbb{Z}$
$\mathbb{Q}(\sqrt{d})$, $d \in \mathbb{Z} - \{0,1\}$ squarefree	$\mathbb{Z}[\sqrt{d}]$ if $d \equiv 2, 3 \pmod 4$,
	$\mathbb{Z}[(1+\sqrt{d})/2]$ if $d \equiv 1 \pmod 4$
$\mathbb{Q}(\zeta_n)$, ζ_n a primitive nth root of unity	$\mathbb{Z}[\zeta_n]$

Example $K = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta_3)$ since $\zeta_3 = (-1+\sqrt{-3})/2$. $\mathcal{O}_K = \mathbb{Z}[\zeta_3]$

Units

Definition: A *unit*, in a number field *K* is an element such that the group of units in *K* is denoted by $\mathcal{O}_K^{\times}$ $\alpha \in \mathcal{O}_K$ $\alpha^{-1} \in \mathcal{O}_K$

Example

For $K = \mathbb{Q}$ we have $\mathcal{O}_K = \mathbb{Z}$ and $\mathcal{O}_K^{\times} = \{\pm 1\}$.

For $K = \mathbb{Q}(\sqrt{-3})$ we have $\mathcal{O}_K = \mathbb{Z}[(1+\sqrt{-3})/2]$ And $\mathcal{O}_K^{\times} = \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\}$

Theorem 3.1 (Dirichlet I nit Theorem) Lt^t *K* be a number field. Then $\mathcal{O}_K^{\times}$ is a finitely generated abelian group more precisely

$$\mathcal{O}_K^{\times} = \Delta \times \mathbb{Z}^{r_1+r_2-1}$$

Where Δ is the finite group of roots of unity in K. and r\ and ro denoting the number of real embedding's $K \hookrightarrow \mathbb{R}$ and complex conjugate einbeddiugs $K \hookrightarrow \mathbb{C}$ with image not contained in $\mathbb{R}$. So $r_1 + 2r_2 = [K : \mathbb{Q}]$

Corollary 3.1: The only number fields with finitely many units art; $\mathbb{Q}$ and $\mathbb{Q}(\sqrt{-D})$ $6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$ $D > 0$

Factorisation

Example: $\mathbb{Z}$ lias unique factorization. We do not have this luxury in $\mathcal{O}_K$ in general, e.g.. let $K = \mathbb{Q}(\sqrt{-5})$ with $\mathcal{O}_K = \mathbb{Z}[\sqrt{-5}]$ then where $2, 3, 1 \pm \sqrt{-5}$ are irreducible and 2,3 are not equal to $1 \pm \sqrt{-5}$ up to units.

Theorem 3.2 (Unique Factorization of Ideals) Let *K* be a number field. Then every non-zero ideal of $\mathcal{O}_K$ admits a factorisation into prime ideals. This factorisation is unique up to order.

Example: In $K = \mathbb{Q}(\sqrt{-5})$

$= (2)(3) = (2, 1+\sqrt{-5})^2(3, 1+\sqrt{-5})(3, 1-\sqrt{-5})$

$(1+\sqrt{-5})(1-\sqrt{-5}) = (2, 1+\sqrt{-5})(3, 1+\sqrt{-5})(2, 1+\sqrt{-5})(3, 1-\sqrt{5})$

Where $(2, 1+\sqrt{-5})$, $(3, 1+\sqrt{-5})$, $(3, 1-\sqrt{-5})$ are prime ideals.

Definition: Let $A, B \subset \mathcal{O}_K$ be ideals. Then *A divides D.* $A \mid B$. If there exists $C \subset \mathcal{O}_K$ such that *A. C = D.* liquivalently. IL ‘in the prime factorizations

$$A = P_1^{m_1} \cdots P_k^{m_k}, \qquad B = P_1^{n_1} \cdots P_k^{n_k}$$

we have $m_i \leq m_i$ for all $1 \leq i \leq k$

Remark:

(i) For $\alpha, \beta \in \mathcal{O}_K$ (α)=(β) if and only if $\alpha = \beta u$ for some $u \in \mathcal{O}_K^\times$

(ii) For ideals $A, B \subset \mathcal{O}_K$, $A \mid B$ if and only if $A \supset B$

(iii) To multiply ideals, just multiply their generators, e.g..

$$\begin{aligned}(2)(3) &= (6)\\ (2, 1+\sqrt{-5})(3, 1+\sqrt{-5}) &= (6, 2+2\sqrt{-5}, 3+3\sqrt{-5}, -4+2\sqrt{-5})\\ &= (6, 1+\sqrt{-5})\\ &= (1+\sqrt{-5}).\end{aligned}$$

(iv) Addition of ideals works completely differently, simply combine the generators. **e.g,**

$$(2) + (3) = (2, 3) = (1) = \mathcal{O}_K.$$

Conclusion

We hope to show that the study of algorithms not only increases our understanding of algebraic number fields but also stimulates our curiosity about them. The discussion is concentrated of three topics: the determination of Galois groups, the determination of the ring of integers of an algebraic number field, and the computation of the group of units and the class group of that ring of integers. In this study we discuss the basic problems of algorithmic algebraic number theory. The emphasis is on aspects that are of interest from a purely mathematical point of view, and practical issues are largely disregarded. We describe what has been done and, more importantly, what remains to be done in the area. Some work over finite fields, where there are connections with algebraic number theory and applications to areas such as error-correcting codes. Arithmetic algebraic geometry, the study of algebraic varieties over number fields, is also represented at LSU. The tools in this specialty include techniques from analysis (for example, theta functions) and computational number theory.

References

1. Buchmann JA, Lenstra HW Jr. Approximating rings of integers in number fields, J. Th_eor. Nombres Bordeaux 6 (1994), no. 2, 221{260. MR 1360644 (96m:11092)
2. Kimball Martin. Nonunique factorization and principalization in number fields. Proc. Amer. Math. Soc 2011; 139(9):3025-3038.
3. Artin M. Algebra, Prentice Hall Inc., Englewood Clients, NJ, 1991, MR 92g:00001
4. Michael Atiyah, Ian G. Macdonald. Introduction to Commutative Algebra. Addison-Wesley, 1969.
5. Mollin, Richard. Algebraic Number Theory. Chapman and Hall/CRC Press, 1999
6. Murty, R. Problems in Analytic Number Theory, GTM/RIM 206, Springer-Verlag, 2001.
7. Ono Takashi. An Introduction to Algebraic Number Theory. Plenum Publishing Corporation, 1990
8. S Lang. Algebraic numbers, Addison-Wesley Publishing Co., Inc., Reading, Mass.-Palo Alto-London, 1964, MR 28 #3974
9. Schwermer Joachim. \Minkowski, Hensel, and Hasse: On the Beginnings of the Local-Global Principle". In: Episodes in the History of Modern Algebra, 2007, 1800-1950.
10. Serge Lang. Algebra. Springer-Verlag, New York Inc., third edition, 2002. 11
11. Steve Chien, Alistair Sinclair. Algebras with Polynomial Identities and Computing the Determinant. In FOCS, 352{361, 2004. 82
12. Victor Shoup. A Computational Introduction to Number Theory and Algebra. Cambridge University Press, New York, 2009. Available from http://shoup.net/ntb/. 19