5th International Conference on Recent Advances in Engineering Science and Management
YMCA, Connaught Place, New Delhi (India) (ICRAESM-18)
03rd February 2018, www.conferenceworld.in ISBN: 978-93-86171-97-9

Finding the ring of integers and its algorithms in algebraic number theory

[1]Dr.K.Vijaya Kumar , [2]Dr.C.Ashok Kumar

[1]Associate Prof., Dept. of Mathematics

Samskruthi college of Engineering and Technology, Hyderabad (India)

[2]Acadamic Consultant, HOD Dept.of Mathematics

University PG Centre Kollapur, Palamuru University, Telangana (India)

ABSTRACT

We examine the algorithmic problem of finding the ring of integers of a given algebraic number field. In practice it is often assumed that this problem is solved, but the theoretical results show that it is not manageable for the numerical fields defined by equations with very high coefficients.Such fields occur in the number field sieve algorithm for factoring integers. Applying a variant of a standard algorithm for finding rings of integers, one finds a subring of the number field that one may view as the "best guess" one has for the ring of integers. This best guess is probably often correct. Our main concern is what can be proved about this subring. We show that it has a particularly transparent local structure, which is reminiscent of the structure of tamely ramified extensions of local fields.

I. INTRODUCTION

In this work concerned with the following problem from algorithmic algebraic number theory: given an algebraic number field K, determine its ring of integers O. The apparent contradiction is easy to resolve. Namely, all computational experience so far is limited to "small" number fields K, such as number fields that are given as $K = Q[X]/fQ[X]$, where Q is the field of rational numbers and f is an irreducible polynomial of small degree with small integer coefficients. The algorithms that are used for small fields will not always work when they are applied to "large" number fields. Large number fields are already making their appearance in applications of algebraic number theory, and the determination of their rings of integers is generally avoided. One can attempt to determine the ring of integer's O of a given number field K in a similarly naive manner. One starts from an order in K, i. e., a subring A of O for which the index $(O: A)$ of additive groups is finite; for example, one may take $A = Z[\alpha]$, where $\alpha \in K$ is an algebraic integer with $K = Q(\alpha)$. As we shall see, one can determine O if the largest squarefree divisor m of the discriminant Δ_A of A is known.

Material and Methods

Given an algebraic number field K, determine its ring of integers O

In mathematics, the ring of integers of an algebraic number field K is the ring of all integral elements contained in K. An integral element is a root of a monic polynomial with rational integer coefficients, $x^n + c_{n-1}x^{n-1} + \ldots$

$+ c_0$. This ring is often denoted by O_K. Since any rational integer number belongs to K and is an integral element of K, the ring Z is always a subring of O_K.

The ring **Z** is the simplest possible ring of integers. Namely, **Z** = $O_{\mathbf{Q}}$ where **Q** is the field of rational numbers and indeed, in algebraic number theory the elements of **Z** are often called the "rational integers" because of this.The ring of integers of an algebraic number field is the unique maximal order in the field.The ring of integers O_K is a finitely-generated **Z**-module. Indeed, it is a free **Z**-module, and thus has an **integral basis**, that is a basis $b_1, \ldots, b_n \in O_K$ of the **Q**-vector space K such that each element x in O_K can be uniquely represented as

$$x = \sum_{i=1}^{n} a_i b_i$$

with $a_i \in \mathbf{Z}$The rank n of O_K as a free **Z**-module is equal to the degree of K over **Q**.

Definition 1.1. An algebraic number field is a finite algebraic extension of Q.

Definition 1.2. Let A be an integral domain, K be a field that contains A and L be an extension of K. x ∈ L is an integral element if and only if there exist

$$\alpha n-1, \ldots, \alpha 0 \in A \text{ such that } x^n + a_n - 1^{xn-1} \ldots + \alpha_0 = 0$$

In an algebraic number field, integral elements are called algebraic integers.

We will see that the integral elements form the Ring of Integers and that every element in the ring of integers can be decomposed into irreducible elements (using the Noetherian Ring property). However, uniqueness cannot always be insured. Instead, we will restrict our attention to the ideals of the Ring of Integers and demonstrate that they can be decomposed uniquely into prime ideals.

Integral Elements form a Ring. In order to show that the set of integral elements do indeed form a ring, we first need the following lemma.

Proposition 1. *$x \in K$ is integral over A if and only if there is a finitely generated A-submodule of K such that $xM \subset M$*

Proof. $\Rightarrow$ If $x^n + a_n - I^{x\,n-l} + \ldots + a_0 = 0$ for $a_{n-l}, \ldots, a_0 \in A$, then consider the A-module

$$N = span\ (1, x, \ldots, x^{n-1})$$

$\alpha_n = 1$ implies that $xn \in N$. Therefore, N is finitely generated and $xN \subset N$. The others powers of x follow from induction.

$\Leftarrow$ Conversely, let $M = \text{span}_A(u_1, \ldots, u_n)$ be a finitely generated module over K. Furthermore, assume that $xM \subset M$ for some $x \in K$. Then

$$xu_i = a_{i1}u_1 + \ldots + a_{in}u_n, \forall_i \in (1, \ldots, n)$$

This leads to the following linear equations:

$$(x - a_{11})u_1 - a_{12}u_2 - \ldots - a_{1n}u_n = 0$$

Let B be the matrix formed by the coefficients of these linear equations. Since B has a non-zero kernel, we conclude that det(B) = 0. This implies that x satisfies an equation of the form

$$\beta_n x^n + \beta_{n-1} x^{n-1} + \ldots + \beta_0 = 0$$

where the $\beta_i \in A$. This polynomial is monic since the permutation definition of the determinant shows that degree n terms only occur when multiplying $\prod b_{ii}$. Thus $\beta_n = 1$ and x is an integeral element.

Proposition: If A is an integral domain, K a field that contains A and L an extension of K, then the set

$$\{x \in L : \exists a_{n-1}, \ldots, a_0 \in A : x^n + a_{n-1}x^{n-1} + \ldots + a_0 = 0\}$$

forms a ring.

Proof. Let x and y be integral elements and M and N be finitely generated submodules of K such that $xM \subset M$ and $yN \subset N$. We verify that $x \cdot y$ and $x + y$ are also integral. We do so by considering the (finitely generated) submoduleMN formed by the span of all products of elements in M and N. MN is closed under multiplication by $x \cdot y$ and $x + y$ since $x\,m \in M$ and $yn \in N$for $m \in M$ and for $n \in N$.

Ring of Integers are Finitely Generated

Let K be a number field and $\alpha \in K$, then there exists an integer multiple of α that is an algebraic integer.

Proof. By assumption, α satisfies an equation of the form

$$\sum b_{i\alpha}{}^{i} = 0 \text{ where} b_i \in \text{Q and bn} = 1$$

Let l be the l.c.m of the b_i. Then, multiplying by l^m we have that

$$l^m\alpha^m + b_{n-1}l(l^{n-1})\alpha^{n-1} + \ldots + b_0 l^m = 0$$

Thus l α is an integral element.

II. RESULT AND DISCUSSION

Algebraic and integer algebraic numbers have a useful structure. For example, they are closed by addition and multiplication:

Let α and βbe algebraic numbers. Then$\frac{1}{\alpha}$(if$\alpha \neq 0$), $\alpha + \beta$, and $\alpha\beta$are also algebraic numbers. Ifα and $\beta$are algebraic integers, then so are $\alpha + \beta$and $\alpha\beta$.

Let α be a complex number. Then define $\mathbb{Q}(\alpha)$ tobe the set of all polynomials in α with rational coefficientsthat is, expressions of the form$a_0 + a_1\alpha + \ldots + a_k\alpha^k$ for the some k, where all the $a_i$arerational.

Define to be the set of all polynomials in α with integers coefficients.

If $\alpha$is an algebraic number, then $\mathbb{Q}(\alpha)$ equals the set of all expressions $a_0 + a_1\alpha + \ldots + a_{d-1}\alpha^{d-1}$, where $\mathbb{Z}[\alpha]$ d=deg(α) and the a_i are rational.

If $\alpha$is an algebraic integer, thenequals $\mathbb{Z}[\alpha]$ the set of all expressions $a_0 + a_1\alpha + \ldots + a_{d-1}\alpha^{d-1}$,where the a_i are integers.

PROOF

The point is that higher powers of α can be "reduced" using the minimal polynomial; since $\alpha^d + c_{d-1}\alpha^{d-1} + \ldots + c_0 = 0$ for some coefficients c_i, α^d can be rewritten as a linear combination of lower powers of α. This can similarly be done for α^{d+1}, α^{d+2}, and so on.

$\left(\frac{3+\sqrt{1}}{2}\right)$is thesetof expressions of the form $a + b\sqrt[3]{1/2} + c\sqrt[3]{1/4}$, because $\sqrt[3]{1/8} = \frac{1}{2}$can be absorbed into the α term,

$\mathbb{Q}$

$\sqrt[3]{1/16}=\frac{1}{2}\sqrt[3]{1/2}$can be absorbed into the *b*term, and so on.

The proof of the theorem uses some linear algebra to explicitly find polynomials that $\alpha+\beta$and $\alpha\beta$satisfy. The idea is to look at(α,β) or powers of $\alpha+\beta$ (or the powers of $\alpha\beta$). Rather than developing the machinery necessary to do the proof in general, it is easiest to look at an explicit example.

Z[α,β], and establish a dependency relation between the

Find the minimal polynomial of $\sqrt{2}+\sqrt{3}$.

Consider the powers of $\alpha=\sqrt{2}+\sqrt{3}$:

$\alpha^0=1+0\sqrt{2}+0\sqrt{3}+0\sqrt{6}$

$\alpha^1=0+1\sqrt{2}+1\sqrt{3}+0\sqrt{6}$

$\alpha^2=5+1\sqrt{2}+0\sqrt{3}+2\sqrt{6}$

$\alpha^3=0+11\sqrt{2}+9\sqrt{3}+0\sqrt{6}$

$\alpha^4=49+0\sqrt{2}+0\sqrt{3}+20\sqrt{6}$

Setting some linear combination of these powers equal to 0 yields four linear equations in five unknowns, this always have a nontrivial solution. In this case, it's not hard to see that $\alpha^4-10\alpha^2+1=0$. So the minimal polynomial isx^4-10x^2+1.

III. CONCLUSION

We conclude that there are well-defined operations of addition and multiplication on the set $Z_n$of congruence classes of integers modulo n:the sum of the congruence classes of integers *x* and *y* is the congruence class of *x+y*, and the product of these congruence classes is the congruence class of *xy*. These operations of addition and multiplication on congruence classes do not depend on the choice of representatives of those congruence classes.

REFERENCES

[1.] S.Y. Yan and T.H. Jackson, A new large amicable pair, *Computers Math. Applic.* 27 (6), 1 3 (1994).

[2.] G.L. Miller, Riemann's hypothesis and tests for primality, *Journal of Computer and System Science* 13, 300-317 (1976).

[3.] J.H. Davenport, Primality testing revisited, In *Proceedings of International Symposium of Symbolic and Algebraic Computations*, ACM Press, 123-129, (1992).

[4.] R.G.E. Pinch, Some primality testing algorithms, Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, (June 24, 1993).

[5.] I. Niven, H.S. Zuckerman and H.L. Montgomery, *An Introduction to the Theory of Numbers*, Fifth edition, John Wiley & Sons, (1991).

[6.] H. Reisel, *Prime Numbers and Computer Methods for Factorization*, Birkh~user, (1990).

[7.] R.J. Baillie and S.S. Wagstatf, Jr., Lucas pseudoprimes, *Mathematics of Computation* 35, 1391-1417 (1980).

[8.] C. Pomerance, J.L. Selfridge and S.S. Wagstaff, Jr., The pseudoprimes to 25.109, *Mathematics of Computation* 35, 1003-1026 (1980).

[9.] A.O.L. Atkin and F. Morain, Elliptic curves and primality proving, Department of Mathematics, University of Illinois at Chicago, (1991).

[10.] D.E. Knuth, *The Art of Computer Programming: Seminumerical Algorithms*, 2nd edition, Addison-Wesley, (1981).

[11.] S.Y. Yan, 68 new large amicable pairs, *Computers Math. Applic.* 28 (5), 71-74 (1994).