A note on finitely generated *Z*-module and algebraic integers

Lijiang Zeng
(Research Centre of Zunyi Normal College,
Zunyi 563099, GuiZhou, P. R. China)
E-mail: zlj4383@sina.com

***Abstract*-- The theory of algebraic integer has its many applications, such as in algebraic coding, cryptology, information system and other fields. The research of algebraic integer can not leave finitely generated module, and the finitely generated module itself be also applied in group theory, ring theory, and some applied science. In this paper, we research the theory of algebraic integer using finitely generated module as tool, we obtained necessary and sufficient condition that an element is algebraic integer, and an intrinsic connects between algebraic number field and finitely generated *Z*-module.**

***Keywords*-- algebraic coding; information system; algebraic integer; monic irreducible polynomial**

I. INTRODUCTION

As we know, the theory of algebraic integer[1-6] has its many applications, such as in algebraic coding, cryptology, information system[7-9] and other fields. The research of algebraic integer can not leave finitely generated module[10-12], and the finitely generated module itself be also applied in group theory, ring theory, and some applied science[13-14]. In this paper, we research the theory of algebraic integer using finitely generated module as tool, First, we introduce two lemmas in primitive polynomial, finite extension, monic irreducible polynomial, and other concepts and symbols, and then regard the two lemmas as tool, we obtained necessary and sufficient condition that an element is algebraic integer, and an intrinsic connects between algebraic number field and finitely generated *Z*-module.

II. SOME PREPARATIONS AND LEMMAS

Let Q denote rational field throughout this paper, and let Z be the ring of rational integers[15-16]. Let x be an indeterminate over Q. A polynomial $F[x]$ is monic if its leading coefficient is l. For an element α of finite extension[15] of Q, we let $Irr(\alpha, Q)$ denote the unique monic irreducible polynomial in $Q[x]$ of which α is a zero.

Definition 1. An algebraic integer is an element α of finite extension of Q for which $Irr(\alpha, Q) \in Z[x]$.

Obviously, all elements of Z are algebraic integers.

Lemma 1 A rational number is an algebraic integer if and only if it is a rational integer. □

The proof of **Lemma 1** can be found from some papers[17-18].

Lemma 2. Any zero of monic polynomial in $Z[x]$ is an algebraic integer.

Proof. Let α be a zero of the monic polynomial $h(x) \in Z[x]$, where $h(x)$ may be reducible. If $f(x) = Irr(\alpha, Q)$, we have

$$h(x) = f(x)\, g(x) \quad g(x) \in Q[x] \qquad (1)$$

The polynomial $f(x)$ has rational coefficients; let us write $f(x) = cF(x)/a$, where a and c are positive integers, and where $F(x) \in Z[x]$ is a primitive polynomial (that is, the G.C.D.[19] of the coefficients of $F(x)$ is l). Similarly, write $g(x) = dG(x)/b$, whether $G(x) \in Z[x]$ is primitive and b and d are positive integers. From (1)

we obtain

$$cdF(x)G(x) = abh(x) \qquad (2)$$

If we can show that the product $F(x)G(x)$ of the two primitive polynomials $F(x)$, $G(x)$ is again primitive, then (2) will imply that $ab=cd$, whence $F(x)\ G(x) = h(x)$. Therefore $F(x)$ must be monic, so $c=a$, and $f(x) \in Z[x]$. This implies the desired conclusion. □

Suppose $F(x)G(x)$ were not primitive; there would then exist a rational prime p such that

$$F(x)G(x) \equiv 0 \pmod{p} \qquad (3)$$

coefficientwise. Let $\overline{Z}$ be the finite field Z/pZ, and let $\overline{F}[x] \in \overline{Z}[x]$ be gotten from $F(x)$ by replacing each coefficient of $F(x)$ by its residue class mod p. Since $F(x)$ and $G(x)$ are both primitive, have $\overline{F}[x] \neq 0$, $\overline{G}[x] \neq 0$. However, $\overline{FG} = \overline{F}\ \overline{G}$, so (3) implies

$\overline{F}[x]\overline{G}[x] = 0$. This is a contradiction: we have two non-zero polynomials in $\overline{Z}[x]$ whose product is zero.

III. MAJOR RESULTS ABOUT ALGEBRAIC INTEGERS

We now obtain major results of this paper about algebraic integers.

Theorem 1. An element α of an extension field of Q is an algebraic integer if and only if $Z[\alpha]$ is a finitely generated

Z-module.

Proof. If α is an algebraic integer, then clearly from **Lemma 2** and **Lemma 1**

$$Z[\alpha] = Z \oplus Z\alpha \oplus Z\alpha^2 \oplus \cdots \oplus Z\alpha^{m-1}$$

where *m* is the degree of *Irr*(α , *Q*).

Suppose, conversely, that $Z[\alpha]$ is a finitely generated *Z*-module,

$$Z[\alpha] = Zf_1(\alpha) + Zf_2(\alpha) + \cdots + Zf_n(\alpha)$$

With each $f_i(x) \in Z[x]$. Choose *N* greater than the degrees of all the $\{f_i(x)\}$. Since $\alpha^N \in Z[\alpha]$, we may write.

$$\alpha^N = a_1 f_1(\alpha) + a_2 f_2(\alpha) + \cdots + a_n f_n(\alpha) \qquad a_i \in Z$$

But this shows that α is a zero of a monic polynomial in $Z[x]$, from **Lemma 2** above, we know that α is an algebraic integer. This completes the proof. □

Corollary 1. Let α , β be elements of finite extension of *Q*. If α and β are algebraic integers, so are $\alpha \pm \beta$ and $\alpha\beta$.

Proof. From the hypothesis we see that $Z[\alpha]$ and $Z[\beta]$ are finitely generated *Z*-modules, say

$$Z[\alpha] = \sum_i Z\alpha_i , \qquad Z[\beta] = \sum_j Z\beta_j ,$$

$$Z[\alpha, \beta] = Z[\alpha][\beta] = \sum_i Z[\beta]\alpha_i = \sum_{i,j} Z\beta_j\alpha_i$$

so $Z[\alpha, \beta]$ is finitely generated. Then every *Z*-submodule of $Z[\alpha, \beta]$ is also finitely generated. Since $Z[\alpha+\beta], Z[\alpha-\beta]$ and $Z[\alpha\beta]$ are all submodules of $Z[\alpha, \beta]$, the result now follows from **Theorem 1**. □

IV. THE FURTHER RESULTS

Definition 2. An algebraic number field is a finite extension field of *Q*.

Let *R=alg.int.*{*K*} denote the set of all algebraic integers contained in an algebraic number field K(It is same below). By **Corollary 1**, *R* is a subring of *K* and so *R* is obviously an integral domain. We claim that *K* is the quotient field of *R*. For let $\gamma \in K$ be a zero of the primitive irreducible polynomial $g(x) \in Z[x]$, and let

$$g(x) = a_0 x^n + a_1 x^{n-1} + \cdots + a_n$$

Then $a_0\lambda$ is a zero of

$$y^n + a_1 y^{n-1} + a_0 a_2 y^{n-2} \cdots + a_0^{n-1} a_n ,$$

a monic polynomial in $Z[y]$. Hence $a_0\gamma \in R$, and, since $a_0 \in Z \subset R$, this shows that γ is a quotient of elements of *R*. (In fact, it establishes the stronger result that every element of *K* is the quotient algebraic integer and a rational integer.)

Theorem 2. Let *R=alg.int.*{*K*}, where *K* is an algebraic number field. Then *R* is a finitely generated *Z*-module, and $(R:Z) = (K:Q)$.

Proof. Since *K* is a finite separable extension of *Q*, there exists an element $\gamma \in K$ such that $K = Q(\gamma)$. By the above discussion, we may then choose $a \in Z$, $a \neq 0$ such that $a\gamma \in R$. Set $\alpha = a\gamma$; we then have $K = Q(\alpha)$ and $Z(\alpha) \subset R$.

Now let $\beta \in R$; we may write

$$\beta = \sum_{i=0}^{n-1} b_i \alpha^i \qquad\qquad b_i \in Q$$

where *n*=(*K*: *Q*). Let $\alpha = \alpha_1$, α_2 , …, α_n be the distinct conjugates of α in some normal extension *L* of *Q* which contains *K*. Then the conjugates of β in *L* are $\beta = \beta_1$, β_2 , …, β_n , (not necessarily distinct) where

$$\beta_j = \sum_{i=0}^{n-1} b_i \alpha_j^i \qquad 1 \le j \le n \qquad (4)$$

Let *A* denote the $n \times n$ matrix whose (i, j) entry is α_j^{i-1} ; since

$\{\alpha_1$, α_2 , …, $\alpha_n\}$ are distinct, the van der Monde determinant $|A|$ is 0. Further, $|A|^2$ is unchanged by all automorphisms in the Galois group of *L* over *Q* and so must lie in *Q*. On the other hand, $|A|^2$ is a polynomial with rational integral coefficients in the algebraic integers $\{\alpha_j^i\}$. Therefore, $|A|^2$ is also an algebraic integer. How ever, the only rational numbers which are algebraic integers are the rational integers, and therefore $|A|^2 \in Z$. Thus, setting $c = |A|^2$ we see that *c* is a non-zero element of *Z*.

We now use Cramer's rule to solve equations (4) for the

coefficients $\{b_i\}$, obtaining

$$b_i = |A|^{-1} \sum_{j=1}^{n} \gamma_{i,j} \beta_j \qquad 0 \le i \le n-1$$

where the $\{\gamma_{i,j}\}$ are polynomials with rational integral coefficients in the $\{\alpha_j^i\}$. Therefore each $\gamma_{i,j}$ is an algebraic integer (lying in *L*

but not necessarily in *K*); since each β_j is an algebraic integer, we deduce that, for each *i*, cb_i is an algebraic integer. However, $cb_i \in Q$ and consequently $cb_i \in Z$ (see **Lemma 1**), Thus, every $\beta \in R$ is expressible in the form

$$\beta = c^{-1} \sum_{i=0}^{n-1} a_i \alpha^i \qquad a_i \in Z$$

which shows that $R \subset c^{-1}Z[\alpha]$. Since $c^{-1}Z[\alpha]$ is a finitely generated *Z*-module, each of its submodules is also finitely generated. Therefore *R* is a finitely generated torsion-free *Z*-module and so must have a *Z*-basis. Finally it is easily seen that any *Z*-basis of *R* is also *Q*-basis for *K*. □

The preceding proof also establishes

Corollary 2 Let *R=alg.int.*$\{K\}$, where $(K:Q)=n$ and let $\alpha \in R$ be such that $K = Q(\alpha)$. Let α_1, α_2, …, α_n be the conjugates of α_1, α_2, …, α_n over *Q*, and set

$$c = \prod_{1 \le i < j \le n} (\alpha_i - \alpha_j)^2$$

Then $c \bullet R \subset Z[\varepsilon]$. □

V. ACKNOWLEDGMENTS

This work was supported by Natural Science Foundation(16339952) of China; Natural Science Foundation([2015]2067) of Science and Technology Department of Guizhou; Natural Science Foundation([2015]722) of Education Department of Guizhou; Hundred of talents project(2015) of Zunyi Normal College.

REFERENCE

[1] Zhang Y. Research Announcements Mixed Product of Modules of Infinite－dimensional Lie Superalgebras of Cartan[J]. Advance in Mathematics(China). 1996(04) .43-48

[2] Wolfgang M. Schmidt. Simultaneous approximation to algebraic numbers by rationals[J]. Acta Mathematica. 1970 (1).21-26

[3] Hermann Minkowski. Über periodische Approximationen algebraischer Zahlen[J]. Acta Mathematica . 1902 (1).98-102

[4] Long Bialgebras, Dimodule Algebras and Quantum Yang-Baxter Modules over Long Bialgebras[J]. Acta Mathematica Sinica(English Series). 2006(04).78-85

[5] Li Q, Duan Q, Chen D, Zhang J. Exact Solutions of Ablowitz–Ladik Hierarchy with Self-Consistent Sources Revisited and Reductions[J]. Communications in Theoretical Physics. 2014(07).51-57

[6] Zeng L. On the algebraic integers in cyclotomic fields[C], Proceedings of International Conference on Engineering and Business Management(EBM2011), March, 22-24,2011 （ Wuhan ） pp2293-2296.32-37

[7] Zeng Y, Li Y, Chen D. A HIERARCHY OF INTEGRABLE HAMILTONIAN SYSTEMS WITH NEUMANN TYPE CONSTRAINT[J]. Chinese Annals of Mathematics. 1992(03).64-69

[8] Algebraic dynamics solutions and algebraic dynamics algorithm for nonlinear partial differential evolution equations of dynamical systems[J]. Science in China(Series G: Physics Mechanics & Astronomy). 2008(06).43-48

[9] Zeng Y, Chen D. THE GENERAL SCHEME OF THE GENERALIZED WRONSKIAN TECHNIQUE[J]. Chinese Annals of Mathematics. 1984(02).54-62

[10] Zeng L. Reducible property of a finitely generated module [J]. Advances in Natural Science(Canada),2010：3(2).pp270-276

[11] Zeng L. Equivalence on finitely generated R[G] module[C]. Proceedings of 2011 Asia-Pacific Youth Conference on Communication （2011APYCC）, April,4-6,2011（Hangzhou）pp434-436

[12] Zhang Z, Yang Y. LINEAR COMPLEXITY AND RANDOM SEQUENCES WITH PERIOD2~n[J]. Systems Science and Mathematical Sciences.1990(02).52-57

[13] Wu C. ON CONSTRUCTING THE NATURAL EXPONENTIAL FAMILIES WITH POLYNOMIAL VARIANCE FUNCTIONS[J]. Systems Science and Mathematical Sciences. 1990(02).42-47

[14] Chen W, Qi X, Deng S. THE EIGEN-PROBLEM AND PERIOD ANALYSIS OF THE DISCRETE-EVENT SYSTEM[J]. Systems Science and Mathematical Sciences. 1990(03).31-35

[15] Weidman, D. R. The character ring of a finite group[J]. Illinois J. Mathematics Journal, 1966(2).11-16

[16] Fan Y, Liu H, Lluis Puig. Generalized Hamming weights and equivalences of codes[J]. Science in China, Ser. A. 2003(05).32-36

[17] Oskar Perron. Grundlagen für eine Theorie des Jacobischen Kettenbruchal gorithmus[J]. Mathematische Annalen. 1907 (1).85-89

[18] Zeng L. Two Theorems about Nilpotent Subgroup[J]. Applied Mathematics(America), May 2011:2(5), pp562-564

[19] Wu W. ON THE CONSTRUCTION OF GROEBNER BASIS OF A POLYNOMIAL IDEAL BASED ON RIQUIER-JANET THEORY[J]. Systems Science and Mathematical Sciences. 1991(03).43-51