Proc. Indian Acad. Sci. (Math. Sci.) Vol. 119, No. 3, June 2009, pp. 267–274.

A finer classification of the unit sum number of the ring of integers of quadratic fields and complex cubic fields

NAHID ASHRAFI

Department of Mathematics, Semnan University, Semnan, Iran
E-mail: nashrafi@semnan.ac.ir; ashrafi49@yahoo.com

MS received 20 May 2008; revised 9 September 2008

Abstract. The unit sum number, $\mathbf{u}(R)$, of a ring R is the least k such that every element is the sum of k units; if there is no such k then $\mathbf{u}(R)$ is ω or ∞ depending on whether the units generate R additively or not. Here we introduce a finer classification for the unit sum number of a ring and in this new classification we completely determine the unit sum number of the ring of integers of a quadratic field. Further we obtain some results on cubic complex fields which one can decide whether the unit sum number is ω or ∞. Then we present some examples showing that all possibilities can occur.

Keywords. Unit; unit sum number; ring of integers; quadratic fields; complex cubic field.

1. Introduction

All rings in this paper will have identity elements. For a ring R, $U(R)$ will denote the multiplicative group of units (invertible elements) in R. In our previous paper [1], we showed that if R is the ring of integers of a quadratic or complex cubic number field then $\mathbf{u}(R) \geq \omega$ (Theorem 6 of [1]). Also we completely determined when the unit sum number of the ring of integers of a quadratic field is ω, and when it is ∞. Here we first introduce a finer classification for the case ω which we call ω^+ and ω^-. Then in §3 we improve our results about quadratic extension fields (Theorems 7, 8 of [1]) by determining in which cases unit sum number is ω^+ and when it is ω^-. Finally, in §4 we show that by using the discriminant Δ_K, which enable one to decide whether the unit sum number of a complex cubic extension field is ω or ∞; examples of all three cases ∞, ω^+, ω^- are presented.

2. Definitions and some simple facts

We first consider some basic definitions which may be found in [1, 2].

DEFINITION 1

An element $r \in R$ is said to be k-good if $r = u_1 + \cdots + u_k$ with $u_1, \ldots, u_k \in \mathrm{U}(R)$, and the ring R is said to be k-good if every element of R is k-good.

DEFINITION 2

For any element $a \in R$ we define the *unit sum set* of a to be $\mathbf{uss}(a) = \{k | a \text{ is } k\text{-good}\}$.

It is clear that the set $\mathbf{uss}(a)$ is a subset of $\mathbb{N}$ for all $a \in R$. If $\mathbf{uss}(a) = \emptyset$, then there is no k for which a is k-good and so a cannot be written as a finite sum of units, or equivalently, we can say that the group of units of R does not generate R additively. Since we can always write $0 = 1 + (-1)$, it follows that if $k \in \mathbf{uss}(a)$ then $k + 2 \in \mathbf{uss}(a)$ (from $a = 0 + a$) and therefore all integers of the form $k + 2n$ are in $\mathbf{uss}(a)$. Also, since 1 is l-good for all odd l, a is also lk-good for all odd l (from $a = 1 \cdot a$), so if $k \in \mathbf{uss}(a)$ then $lk \in \mathbf{uss}(a)$ for all odd l. However, this gives no additional information: since $lk - k = (l-1)k$, an even multiple of k, so $lk = (l-1)k + k$ is covered by the previous case. But we can see that there still may be lot of gaps in $\mathbf{uss}(a)$. For example in $\mathbb{Z}$, $\mathbf{uss}(1) = \{1, 3, 5, 7, \dots\}$ because the only units are $1, -1$ and so $\mathbf{uss}(1)$ does not contain any even integer. Thus in this case there are infinitely many gaps. But in some situations we can prove that if $k \in \mathbf{uss}(a)$ then for all $l \geqslant k,\ l \in \mathbf{uss}(a)$. The following result is well-known and its easy proof is omitted.

Lemma 3. *Let R be a ring. Then*

(i) *if R is k-good, then R is l-good for any integer $l \geq k$;*
(ii) *if $x \in R$ is k-good and 1 is 2-good, then x is l-good for any integer $l \geq k$.*

In view of the above lemma we see that in either of the cases set out above, if $k \in \mathbf{uss}(a)$ then there are just finitely many gaps in $\mathbf{uss}(a)$.

For completeness we recall the definition from [2] of the unit sum number $\mathbf{u}(R)$, an invariant of a ring which expresses, in a fairly precise way, how the units generate the ring additively.

DEFINITION 4

For a ring R the *unit sum number*, $\mathbf{u}(R)$, is given as

- $\min\{k | R \text{ is } k\text{-good}\}$ if R is k-good for some $k \geq 1$;
- ω if R is not k-good for any k, but every element of R is k-good for some k, (i.e. when at least $\mathrm{U}(R)$ generates R additively);
- ∞ otherwise (i.e. when $\mathrm{U}(R)$ does not generate R additively).

Obviously, the choice of ω is meant to signify less 'bad' behavior than having unit sum number ∞. Accordingly we will use the convention that $\omega < \infty$ and any finite number is less than ω. When $\mathbf{u}(R)$ is ω we can distinguish between two sub-cases which we will now define. This allows us to distinguish between the different behaviors of rings with unit sum number ω.

DEFINITION 5

Let $S \subseteq \mathbb{N}$, we say that S is *co-finite* if $|\mathbb{N} \backslash S| < \infty$, i.e. S eventually contains all natural numbers.

DEFINITION 6

Let R be a ring with $\mathbf{u}(R) = \omega$. If for all $a \in R,\ \mathbf{uss}(a)$ is co-finite then we say $\mathbf{u}(R) = \omega^-$. Otherwise we say $\mathbf{u}(R) = \omega^+$.

It seems to be necessary to explain why we called these two cases ω^- and ω^+. Of course ω^- signifies 'better' behavior in our view than ω^+, but just to preserve the ordering we named them like this. In fact, we order these new symbols so that

$$1 < \cdots < k < \cdots < \omega^- < \omega^+ < \infty.$$

Since ω^- and ω^+ are sub-cases of ω we will not compare them to ω. In the sequel we will use both notations but not simultaneously. Thus when we say that $\mathbf{u}(R) = \omega$ then we will mean that $\mathbf{u}(R)$ is either ω^- or ω^+, $\mathbf{u}(R) < \omega$ will mean as before, that $\mathbf{u}(R)$ is finite and $\mathbf{u}(R)$ is infinite and $\mathbf{u}(R) > \omega$ will mean as before that $\mathbf{u}(R) = \infty$. We will use ω^- and ω^+ for values of the unit sum number only when this finer classification can be ascertained.

Example 1. Let D be a division ring. If $|D| \geq 3$, then $\mathbf{u}(D) = 2$; whereas if $|D| = 2$ i.e $D = \mathbb{Z}_2$, the field of two elements, then $\mathbf{u}(\mathbb{Z}_2) = \omega^+$. By Ex. 1.1 of [2], we know that $\mathbf{u}(\mathbb{Z}_2) = \omega$. But since 0 is k-good precisely when k is even and 1 is k-good precisely when k is odd. So $\mathbf{u}(\mathbb{Z}_2) = \omega^+$.

Lemma 7. *Let R be a ring, then*:

(1) *if* $\mathbf{uss}(1)$ *is co-finite, then for all $a \in R$ such that* $\mathbf{uss}(a) \neq \varnothing$, $\mathbf{uss}(a)$ *is also co-finite*;
(2) *if* $\mathbf{u}(R) \leq \omega$ *and there exists $a \in R$ such that* $\mathbf{uss}(a)$ *is co-finite, then* $\mathbf{u}(R) \leq \omega^-$.

Proof.

(i) First of all we notice that if $\mathbf{uss}(1)$ is co-finite then there exists an integer $k_\circ \in \mathbf{uss}(1)$ such that for all integers $l \geq k_\circ$, $l \in \mathbf{uss}(1)$. Now let a be an arbitrary element of R with $\mathbf{uss}(a) \neq \varnothing$. So there is a $k \in \mathbb{N}$ such that a is k-good. Therefore there are units $u_1, u_2, \ldots, u_k \in \mathrm{U}(R)$ such that

$$a = u_1 + u_2 + \cdots + u_k = u_1 + u_2 + \cdots + u_{k-1} + 1 \cdot u_k. \tag{2.1}$$

Now for any $l \geq k_\circ$, $l \in \mathbf{uss}(1)$, so 1 can be written as a sum of l units. So by (2.1) a can be written as $k+l-1 \geq k+k_\circ-1$ units. Thus for any $n \geq k+k_\circ-1$, $n \in \mathbf{uss}(a)$. So we may just miss $1, 2, \ldots, k-1, k+1, \ldots, k+k_\circ-2$, a set of finitely many numbers. Therefore $\mathbf{uss}(a)$ is co-finite.

(ii) Since $\mathbf{uss}(a)$ is co-finite, we can assume that there is a $k \in \mathbf{uss}(a)$ such that for all integers $l \geq k$, $l \in \mathbf{uss}(a)$. Assume that $x \in R$ is an arbitrary element. Now consider $x - a$, since $\mathbf{u}(R) \leq \omega$, so there is an integer $k_\circ$ such that $(x-a)$ is $k_\circ$-good. As $x = (x-a) + a$ and $(x-a)$ is $k_\circ$-good and a is l-good for any integer $l \geq k$, then we can say that x is $(k_\circ + l)$-good for all integers $k_\circ + l \geq 0$. So it is clear that $\mathbf{uss}(x)$ is co-finite. Therefore $\mathbf{u}(R) \leq \omega^-$. □

The behaviour of unit sum numbers under quotients is easily dealt with.

PROPOSITION 8

Let I be an ideal of the ring R and for any $r \in R$ let $\bar{r}$ denote the residue class of r modulo I in the factor ring R/I. Then we have:

(a) *For any $r \in R$,* $\mathbf{uss}(r) \subseteq \mathbf{uss}(\bar{r})$ *with equality if $I \subseteq \mathrm{J}(R)$ (recall that* $\mathrm{J}(R)$ *denotes the Jacobson radical of R).*
(b) $\mathbf{u}(R/I) \leq \mathbf{u}(R)$ *with equality if* $I \subseteq \mathrm{J}(R)$.
(c) *Let* $I \subseteq \mathrm{J}(R)$. *If* $\mathbf{u}(R) = \omega^-$, *then* $\mathbf{u}(R/I) = \omega^-$ *and if* $\mathbf{u}(R) = \omega^+$ *then* $\mathbf{u}(R/I) = \omega^+$.

Proof. Let $t \in \mathbf{uss}(r)$, so $r = u_1 + \cdots + u_t$ for some units in $\mathrm{U}(R)$. Therefore $\bar{r} = \overline{u_1} + \cdots + \overline{u_t}$ and we note that $\overline{u_1}, \ldots, \overline{u_t}$ are in $\mathrm{U}(R/I)$. So $\bar{r}$ is also t-good and hence $t \in \mathbf{uss}(\bar{r})$. Now assume that $I \subseteq \mathrm{J}(R)$. If $\bar{u} = u + I$ is a unit in R/I then u will be a unit of R. Now let $\bar{r}$ be k-good in R/I and $\bar{r} = \overline{u_1} + \cdots + \overline{u_k}$. So by what we just said, $u_1, u_2, \ldots, u_k$ are in $\mathrm{U}(R)$ and $h = r - (u_1 + u_2 + \cdots + u_k) \in I \subseteq \mathrm{J}(R)$. So $1 + (u_1^{-1})h$ has a left inverse and $1 + h(u_1^{-1})$ has a right inverse, therefore $u_1 + h \in \mathrm{U}(R)$ and $r = (u_1 + h) + u_2 + \cdots + u_k$ shows that r is k-good. So $\mathbf{uss}(\bar{r}) = \mathbf{uss}(r)$ and in this case $\mathbf{u}(R/I) = \mathbf{u}(R)$.

In order to show the last part, let $\mathbf{u}(R) = \omega^-$. By assumption, $I \subseteq \mathrm{J}(R)$ and so it follows from (a) that $\mathbf{uss}(\bar{r}) = \mathbf{uss}(r)$. Clearly then $\mathbf{u}(R/I) = \omega^-$. A similar argument shows that if $\mathbf{u}(R) = \omega^+$, then $\mathbf{u}(R/I) = \omega^+$. □

Example 1 and Proposition 8 above now yield the following obvious obstruction to the finiteness of the unit sum number.

PROPOSITION 9

If the ring R has $\mathbb{Z}_2$ as a factor then $\mathbf{u}(R) \geq \omega^+$ and both possibilities $\mathbf{u}(R) = \omega^+$, $\mathbf{u}(R) = \infty$ can occur. Therefore R cannot be k-good for any k.

Proof. Since $\mathbb{Z}_2$ is a factor of R, there is a surjective map $g\colon R \longrightarrow \mathbb{Z}_2$ with $R/\operatorname{Ker} g \cong \mathbb{Z}_2$. If R is k-good for some integer k then by Proposition 8, $R/\operatorname{Ker} g$ and therefore $\mathbb{Z}_2$ would be k-good. But this contradicts Proposition 1. So R cannot be k-good for any integer k. In particular, since $\mathbb{Z}_2$ is a factor of $\mathbb{Z}$, then $\mathbf{u}(\mathbb{Z}) = \omega^+$ or ∞. But since every integer is a finite sum of 1 or -1 so $\mathbf{u}(\mathbb{Z}) = \omega^+$. On the other hand, if $R = \mathbb{Z}_2[x]$, then the only unit is 1, so $\mathbf{u}(R) = \infty$. □

It is easy to derive necessary and sufficient conditions for the equality $\mathbf{u}(R) = \omega^+$.

Theorem 10. *Let R be a ring then, $\mathbf{u}(R) = \omega^+$ if, and only if, $\mathbf{u}(R) = \omega$ and $\mathbb{Z}_2$ is a factor of R.*

Proof. First assume that $\mathbf{u}(R) = \omega$ and $\mathbb{Z}_2$ is a factor of R. By Proposition 9 it is clear that $\mathbf{u}(R) \geq \omega^+$. Since $\mathbf{u}(R) \neq \infty$, we have $\mathbf{u}(R) = \omega^+$.

Now assume $\mathbf{u}(R) = \omega^+$. First we claim that for all $r \in R$, exactly one of the following possibilities can occur: either $\mathbf{uss}(r) \subseteq 2\mathbb{N}$, or $\mathbf{uss}(r) \subseteq 1 + 2\mathbb{N}$. Suppose that there is an even number l and an odd number k in $\mathbf{uss}(r)$. So $\mathbf{uss}(r)$ contains any even number greater than l and any odd number greater than k. Therefore eventually $\mathbf{uss}(r)$ will contain all natural numbers greater than $\max(k, l)$, so it will be co-finite. But this contradicts $\mathbf{u}(R) = \omega^+$.

Now we define $\theta\colon R \longrightarrow \mathbb{Z}_2$ with

$$\theta(r) = \begin{cases} 0, & \text{if } \mathbf{uss}(r) \subseteq 2\mathbb{N}; \\ 1, & \text{if } \mathbf{uss}(r) \subseteq 1 + 2\mathbb{N}. \end{cases} \tag{2.2}$$

By what we proved earlier it is clear that θ is well defined. Also it is easy to see that θ is an epimorphism with kernel

$$K = \{r \in R | \theta(r) = 0\}.$$

Now consider the factor ring R/K. Clearly $R/K \cong \mathbb{Z}_2$, and so $\mathbb{Z}_2$ is a factor of R. □

3. Quadratic extension fields

We now turn our attention to quadratic extension fields. Let $K = \mathbb{Q}(\alpha)$ be a number field, $\mathcal{O}_K$ the ring of integers of K and let $\mathrm{U}(\mathcal{O}_K)$ denote the group of units of $\mathcal{O}_K$. First we try to find out when $\mathbb{Z}_2$ is a factor of $\mathcal{O}_K$ where K is a quadratic extension.

PROPOSITION 11

Let $K = \mathbb{Q}(\sqrt{d})$. Then $\mathbb{Z}_2$ is a factor of $\mathcal{O}_K$ if and only if $d \not\equiv 1 \pmod 4$ or $d \equiv 1 \pmod 8$.

Proof. Recall (Theorem 3.2 of [3]) that when $K = \mathbb{Q}(\sqrt{d})$ is a quadratic number field then $\mathcal{O}_K = \mathbb{Z}[\delta]$ has integral basis $1, \delta$ where

$$\delta = \begin{cases} \sqrt{d}, & \text{if } d \not\equiv 1 \pmod 4 \\ (1+\sqrt{d})/2, & \text{if } d \equiv 1 \pmod 4. \end{cases} \tag{3.1}$$

Also by Lemma 1 of [1] we know that $\mathbb{Z}_2$ is a factor of $\mathbb{Z}[\delta]$ if and only if the minimal polynomial of δ has a root in $\mathbb{Z}_2$.

Assume first that $d \not\equiv 1 \pmod 4$. In this case the minimal polynomial of $\delta = \sqrt{d}$ is $f(x) = x^2 - d$. Therefore $f(0) = -d$ and $f(1) = 1-d$, so $f(0)f(1) = d(d-1)$ which is even, so $f(x)$ has a root in $\mathbb{Z}_2$. Now let $d \equiv 1 \pmod 8$, so $\delta = (1+\sqrt{d})/2$. Therefore the minimal polynomial of δ will be $f(x) = x^2 - x + (1-d)/4$ and $f(0) = f(1) = (1-d)/4$. Thus as $2|(1-d)/4$, $f(0)f(1)$ is even. Therefore $f(x)$ always has a root in $\mathbb{Z}_2$. So $\mathbb{Z}_2$ is a factor.

Now let $\mathcal{O}_K$ have $\mathbb{Z}_2$ as a factor, then if $d \not\equiv 1 \pmod 4$ we have nothing to prove. So let $d \equiv 1 \pmod 4$; we need to prove that $2|(1-d)/4$. As we mentioned above, if $f(x)$ is the minimal polynomial of δ then $f(0) = f(1) = (1-d)/4$. But since $\mathbb{Z}_2$ is a factor of $\mathcal{O}_K$ then $f(x)$ should have a root in $\mathbb{Z}_2$ and $f(0)f(1)$ must be even. Therefore $(1-d)/4$ is even and therefore $d \equiv 1 \pmod 8$. □

By putting together Proposition 11 and Theorems 7, 8 of [1] we can further refine our classification of quadratic extensions.

Theorem 12. *Let $K = Q(\sqrt{d})$ be a quadratic extension field. Then*

(i) $\mathbf{u}(\mathcal{O}_K) = \omega^-$ *when precisely one of the following holds*:

  (a) $d > 0$, $d \equiv 1 \pmod 4$, $2 \nmid (1-d)/4$, *and* $d = a^2 \pm 4$ *for some* $a \in \mathbb{Z}$;
  (b) $d = -3$;

(ii) $\mathbf{u}(\mathcal{O}_K) = \omega^+$ *when precisely one of the following holds*:

  (a) $d > 0$, $d \not\equiv 1 \pmod 4$ *and* $d = a^2 \pm 1$ *for some integer* a;
  (b) $d > 0$, $d \equiv 1 \pmod 4$, $2|(1-d)/4$ *and* $d = a^2 \pm 4$ *for some* $a \in \mathbb{Z}$;
  (c) $d = -1$;

(iii) $\mathbf{u}(\mathcal{O}_K) = \infty$ *in all other cases.* □

Example 2. To illustrate the use of Theorem 12 we readily see that ω^-, ω^+ and ∞ can occur when $d \equiv 1 \pmod 4$. But when $d \not\equiv 1 \pmod 4$ just ω^+ and ∞ can occur.

(i) $d \not\equiv 1 \pmod 4$:

(a) $K = \mathbb{Q}(\sqrt{10})$ gives $\mathbf{u}(\mathcal{O}_K) = \omega^+$;
(b) $K = \mathbb{Q}(\sqrt{6})$ gives $\mathbf{u}(\mathcal{O}_K) = \infty$.

(ii) $d \equiv 1 \pmod 4$:

(a) $K = \mathbb{Q}(\sqrt{5})$ gives $\mathbf{u}(\mathcal{O}_K) = \omega^-$;
(b) $K = \mathbb{Q}(\sqrt{13})$ gives $\mathbf{u}(\mathcal{O}_K) = \omega^+$;
(c) $K = \mathbb{Q}(\sqrt{17})$ gives $\mathbf{u}(\mathcal{O}_K) = \infty$.

4. Complex cubic fields

By Theorem 6 of [1] we know that the ring of integers of a complex cubic fields is not k-good for any k. Now we want to find a criterion which allows us to decide when the unit sum number of $\mathcal{O}_K$ is ∞ and when it is ω. Also we will show that if K is a complex cubic number field and $\mathcal{O}_K = \mathbb{Z}[\alpha]$ where α is a unit, then by looking at the coefficients of the minimal polynomial of α we can decide when $\mathbf{u}(\mathcal{O}_K) = \omega^+$ and when it is ω^-. Then we will give some examples for the cases ∞, ω^+ and ω^-. First we note

Lemma 13. *Let $K = \mathbb{Q}(\alpha)$, $\beta \in \mathcal{O}_K$ and let $p(x) = x^m + a_{m-1}x^{m-1} + \cdots + a_1x + a_0$ be the minimal polynomial of β. Then β is unit if $a_0 = \pm 1$.*

Proof. First let $a_0 = \pm 1$ then since $p(\beta) = 0$ we have $\beta^m + a_{m-1}\beta^{m-1} + \cdots + a_1\beta + a_0 = 0$. So $\beta(\beta^{m-1} + a_{m-1}\beta^{m-2} + \cdots + a_1) = \pm 1$. Thus β is invertible.

Now let $g(x) = x^m + b_{m-1}x^{m-1} + \cdots + b_1x + b_0$ be the minimal polynomial of β^{-1} then, we have $\beta^{-m} + b_{m-1}\beta^{-(m-1)} + \cdots + b_1(\beta^{-1}) + b_0 = 0$. So $h(x) = 1 + b_{m-1}\beta + \cdots + b_1\beta^{m-1} + b_0\beta^m = 0$. Thus $p(x)$ the minimal polynomial of β should divide $h(x)$. Therefore the constant term a_0 should be ± 1. □

PROPOSITION 14

Let K be a quadratic extension field or a complex cubic extension field. If $\mathbf{u}(\mathcal{O}_K) = \omega$ then $\mathcal{O}_K = \mathbb{Z}[\eta]$ where η is a fundamental unit.

Proof. Since $\mathbf{u}(\mathcal{O}_K) = \omega$, for all $x \in \mathcal{O}_K$ there are units $u_1, u_2, \ldots, u_t$ such that $x = \sum_{i=1}^{t} u_i$. But as we know η is the only fundamental unit of $\mathcal{O}_K$, so for each u_i there is $\alpha_i \in \mathbb{Z}$ such that $u_i = \pm\eta^{\alpha_i}$. Thus $x = \sum_{i=1}^{s} a_i\eta^{\alpha_i}$ where $a_i, \alpha_i \in \mathbb{Z}$. But as η is a unit, by Lemma 13 the constant term in the minimal polynomial of η should be ± 1. So for the complex cubic case if $\eta^3 + b_2\eta^2 + b_1\eta \pm 1 = 0$ then $\eta(\eta^2 + b_2\eta + b_1) = \pm 1$. Thus $\eta^{-1} = \pm\eta^2 \pm b_2\eta \pm b_1$. Therefore every η^{α_i} can be written as a polynomial of degree at most 2 of η. Hence, $x = \sum_{1=0}^{2} c_i\eta^i \in \mathbb{Z}[\eta]$. So we have $\mathcal{O}_K = \mathbb{Z}[\eta]$. With a similar proof we can see that the statement is true for the quadratic case as well. □

Notation. Let $K = \mathbb{Q}(\alpha)$ be a number field of degree n and $\{1, \alpha, \ldots, \alpha^{n-1}\}$ be an integral basis for the ring of integers $\mathcal{O}_K$. Then $\triangle_k = \triangle(1, \alpha, \ldots, \alpha^{n-1})$ will denote the discriminant of K.

DEFINITION 15

Let K be a number field of degree n and ring of integers $\mathcal{O}_K$. When $\mathcal{O}_K = \mathbb{Z}[\alpha]$ for some $\alpha \in \mathcal{O}_K$, the set $\{1, \alpha, \ldots \alpha^{n-1}\}$ is a $\mathbb{Z}$-basis of $\mathcal{O}_K$. We call such a basis a *power basis*.

Theorem 16. *Let $\mathcal{O}_K$ be the ring of integers of the complex cubic number field $K = \mathbb{Q}(\alpha)$ and also let η be a fundamental unit of $\mathcal{O}_K$ then,*

$$\mathbf{u}(\mathcal{O}_K) = \omega \text{ if and only if } \mathbb{Z}[\eta] = \mathcal{O}_K \text{ if and only if } \Delta(1, \eta, \eta^2) = \Delta_K.$$

Proof. The proof of the first part clearly follows from Proposition 14 and Theorem 6 of [1]. To prove of the second part of the statement note that $\mathbb{Z}[\eta] = \mathcal{O}_K$ if and only if $[\mathcal{O}_K : \mathbb{Z}[\eta]] = 1$. But since

$$\Delta(1, \eta, \eta^2) = [\mathcal{O}_K : \mathbb{Z}[\eta]]^2 \cdot \Delta_K,$$

then $\mathbb{Z}[\eta] = \mathcal{O}_K$ if and only if $\Delta(1, \eta, \eta^2) = \Delta_K$. □

COROLLARY 17

Let K be a complex cubic number field. If $\mathcal{O}_K$ has no power basis then, $\mathbf{u}(\mathcal{O}_K) = \infty$.

Proof. Assume on the contrary $\mathbf{u}(\mathcal{O}_K) = \omega$. Then by Theorem 16 we know that there is a fundamental unit η such that $\mathcal{O}_K = \mathbb{Z}[\eta]$. So $\mathcal{O}_K$ has an integral basis $\{1, \eta, \eta^2\}$. But this is a contradiction. Thus $\mathrm{U}(\mathcal{O}_K) = \infty$. □

Example 3.

(i) The first example of a ring of integers lacking a power basis is due to Dedekind. It is the field $K = \mathbb{Q}(\alpha)$ where α is a root of the polynomial $x^3 + x^2 - 2x + 8$. The ring of integers of $\mathbb{Q}(\alpha)$ has no power basis, so $\mathbf{u}(\mathcal{O}_K) = \infty$.

(ii) Let $K = \mathbb{Q}(\sqrt[3]{175})$ and consider $t = \sqrt[3]{175}$ and $u = \sqrt[3]{245}$. Then if G is the abelian group generated by $\{1, t, u\}$ we can see that $\mathcal{O}_K = G$. In this case there is no $\mathbb{Z}$-basis of the form $\{1, \beta, \beta^2\}$ (Example 2.7 of [3]). So by Corollary 17, $\mathbf{u}(\mathcal{O}_K) = \infty$.

So in a complex cubic field when we have a fundamental unit η by calculating the discriminant of $\{1, \eta, \eta^2\}$ and by applying Theorem 16 and Corollary 17, we can decide whether the unit sum number of $\mathcal{O}_K$ is ω or ∞.

More interesting problems arise in the situation where the unit sum number is ω^+ than where it is ω^-.

PROPOSITION 18

Let K be a complex cubic number field. If $\mathcal{O}_K = \mathbb{Z}[\alpha]$ and α be a unit, then the minimal polynomial of α is $p(x) = x^3 + ax^2 + bx \pm 1$ and $\mathbf{u}(\mathcal{O}_K) = \omega^+$ if, and only if, $a + b$ is even.

Proof. In this case it is clear that $\mathbf{u}(\mathcal{O}_K) = \omega$. On the other hand, since α is a unit, by Lemma 13, the constant term of the minimal polynomial of α is ± 1. Thus $p(x) = x^3 + ax^2 + bx \pm 1$ is the minimal polynomial of α. By Lemma 1 of [1] and Theorem 10 we know that $\mathbf{u}(\mathcal{O}_K) = \omega^+$ if and only if $p(x)$ has a root in $\mathbb{Z}_2$, otherwise $\mathbf{u}(\mathcal{O}_K) = \omega^-$. But since $p(0) = \pm 1$ and $p(1) = a + b$ so, $\mathbf{u}(\mathcal{O}_K) = \omega^+$ if and only if $a + b$ is even. □

Thus, if one looks at tables of class numbers and units of complex cubic fields, one can find many examples where the unit sum number is ω^+ or ω^-. We list some of them in the following example.

Example 4.

(i) $\mathbf{u}(\mathcal{O}_K) = \omega^+$ when α is a real root of the following polynomials:

(a) $x^3 - x^2 - x - 1$;
(b) $x^3 + 2x - 1$;
(c) $x^3 + 4x - 1$;
(d) $x^3 + x^2 = 5x - 1$.

(ii) $\mathbf{u}(\mathcal{O}_K) = \omega^-$ if α is a real root of the following polynomials:

(a) $x^3 + x^2 - 1$;
(b) $x^3 - x^2 - 1$;
(c) $x^3 + x^2 + 2x - 1$;
(d) $x^3 + 3x - 1$;
(e) $x^3 - x^2 + 4x - 1$;
(f) $x^3 + x^2 + 4x - 1$;
(g) $x^3 + 5x - 1$;
(h) $x^3 - x^2 + 6x - 1$.

Acknowledgement

The research of the author is funded by a grant from the Semnan University of Iran.

References

[1] Ashrafi Nahid and Vámos Peter, On the unit sum number of some rings, *Quart. J. Math.* **56(1)** (2005) 1–12
[2] Goldsmith B, Pabst S and Scott A, Unit sum numbers of rings and modules, *Quart. J. Math. Oxford Ser. (2)* **49(195)** (1998) 331–344
[3] Stewart Ian and Tall David, Algebraic number theory, Chapman and Hall Mathematics series (Chapman and Hall) (1979)