# ON CIRCULAR AND SPECIAL UNITS OF AN ABELIAN NUMBER FIELD

*Trajano Nóbrega*

**RELATÓRIO TÉCNICO Nº 18/89**

ABSTRACT. The purpose of this paper is to show that the concepts of circular units defined by Thaine and Sinnott are equivalent. Furthermore we show that circular units are Special units, in the sense of Rubin.

Universidade Estadual de Campinas
Instituto de Matemática, Estatística e Ciência da Computação
IMECC - UNICAMP
Caixa Postal 6065
13.081 - Campinas, SP
BRASIL



Maio - 1989

# ON CIRCULAR AND SPECIAL UNITS

# OF AN ABELIAN NUMBER FIELD [1]

Trajano Nóbrega

## 1. Introduction:

Let $p$ an odd prime. In their study of p-class group of an abelian number field K, Sinnott [4] and Thaine [5] have introduced different notions of "circular units" and shown that these groups are of finite index in $O_K^{\cdot}$, the group of all units of $K$. We show in this note that the two notions are indeed equivalent, thereby answering a question posed in [5, p.1]. Generalizing the ideas of Thaine to elliptic fields, Rubin [2] introduced a group $S(K)$ which he called the group of special units. We show in this note that $C_S(K) = C_T(K) \subseteq S(K)$, where $C_S(K)$ and $C_T(K)$ denote the groups of circular units of Sinnott and Thaine respectively.

Thoughout this note $K$ will denote an abelian number field and $G = Gal(K/Q)$ its Galois group.

We denote by $O_K$ the ring of integers of $K$ and by $O_K^{\cdot}$ the group of the units of $O_K$. When we say the group of the units of $K$ we are refering to $O_K^{\cdot}$. By Dirichlet's Theorem on the units of $K$, we have $O_K^{\cdot} \cong T \times F$, where $T$ is the group of the roots of the unity in $K$ and $F$ is a free $\mathbb{Z}$-modulo whose rank is easy of calculate.

To describe explicity a set of multiplicatively independent generators for $F$ is

[1]This research was done at UNICAMP, while the author was Doctoral student having Prof. Francisco Thaine as Promotor

an open question; but, if $K$ is an abelian number field, there are many subgroups of $O_K^*$ of finite index in $O_K^*$, for which on can explicitly give a set of multiplicatively independent generators. These subgroups, of which there are many, arise according to the puporse of the authors.

If $m$ is a positive integer, $m$ odd or divisible by 4, let $\xi_m = e^{\frac{2\pi}{m}}$ , $K_m = Q(\xi_m)$ and $G_m = Gal(K_m/Q)$. We recall that there is a positive integer $m$ such that $K \subset K_m$ (Theorem 14.1 [6]) and the smallest $m$ such that $K \subset K_m$ is called the conductor of $K$ and denoted by $m_0$.

We denote by $O_F$ the ring of integers of a number field $F$, $O_F^*$ the group of units of $F$, $(a,b)$ the greatest common divisor of the integers $a$ and $b$. If $n$ is a positive integer, we write $k_n = K \cap K_n$ and $G'_n = Gal(K_n/k_n)$.

Let $n \not\equiv 2 \pmod 4$ and let $V_n$ be the multiplicative group generated by $\{\pm\xi_n, 1-\xi_n^a : 1 \leq a \leq n-1\}$. Let $E_n$ the group of the units of $K_n$ and define $C_n = V_n \cap E_n$. $C_n$ is called the group of cyclotomic units of $K_n$. More generally, for the abelian number field $K$, we can define the cyclotomic units of $K$ in two ways: In the first definition, we let $K \subseteq K_m$, for some $m$ and we take $C_K = O_K^* \cap C_m$. It is easy to see that $C_K$ depends only on $m_0$, the conductor of $K$. Now in the second definition we take the image by the norm from $K_{m_0}$ to $K$ of the cyclotomic units of $K_{m_0}$. If the first group we denote by $C_I(K)$ and the second by $C_N(K)$, we can see that $C_N(K) \subseteq C_I(K)$.

Yet, for abelian number fields, there are others groups of units that we will be dealing with in this work.

The group of the circular units of $K$ defined by Sinnott in [4], which will be denoted by $C_S(K)$ is the intersection of $O_K^*$ and the subgroup of $K$ generated by the elements $\alpha(n,a) = N_{K_n/k_n}(1-\xi_n^a)$, with $n, a$ integers and $a \not\equiv 0$ (mod n).

Since $K_n \cap K_m = K_{(n,m)}$ we only need consider the integers $n$ such that $n$ divides $m_0$, the conductor of $K$.

The group of the circular units of $K$, defined by Thaine in [5], which we will denote by $C_T(K)$, is defined as follows: If $m_0$ is the conductor of $K$ and $j$ is a positive integer, we let

$$C_j(X) = \left\{ f(X) = \pm \prod_{i=1}^{j} \prod_{K=1}^{m_0 - 1} (X^i - \xi_{m_0}^K)^{a_{iK}};\ a_{iK} \in \mathbb{Z},\ f(X) \in K(X) \right.$$

$$\left. \text{and} \quad f(1) \in O_K^{\cdot} \right\}.$$

where $X$ is an indeterminate. $C_T(K) = \bigcup_{j=1}^{\infty} C_j(1)$.

Finally, we have the group of special units defined by Rubin in [2], denoted by $S(K)$ and defined as follows: Let $S$ denote the set of all rational prime which split completely in $K$. Write $K_q^+ = K_q \cap \mathbb{R}$, $L_q = K \cdot K_q^+$, $\varepsilon(q) = \{u \in O_{L_q}^{\cdot} : N_{L_q/K}(u) = 1\}$ and $C(q) = \{\varepsilon \in O_K^{\cdot}$ such that there is $u \in \varepsilon(q)$ with $\varepsilon^2 \equiv u (mod \bar{q})$, where $\bar{q} = (1 - \xi_q)(1 - \xi_q^{-1})O_{Lq}\}$. Now, $S(K) = \{\varepsilon \in O_K^{\cdot}; \varepsilon \in C(q)$ for almost all $q$ in $S\}$.

## 2. The Main Results:

We begin with the two groups mentioned in the introduction.

**Theorem 1:** For an abelian number field $K$ the two groups $C_S(K)$ and $C_T(K)$ of circular units of Sinnott and Thaine are equal.

The proof will be based in three lemmas. First we need some notation.

For each $m \geq 1$, devisible by $m_0$ the conductor of $K$, we write

$$C_j(X,m) = \{f(X) = \pm \prod_{i=1}^{j} \prod_{K=1}^{m-1} (X^i - \xi_m^K)^{a_{iK}} : a_{iK} \in \mathbb{Z},\ f(X) \in K(X) \text{ and } f(1) \in O_K^*\},$$

and

$$C_j(1,m) = \{f(1);\ f(X) \in C_j(X,m)\}.$$

It is easy to see that $C_j(1,m)$ is a group $(j = 1,2,\ldots)$ and that $C_1(1,m) \subseteq C_2(1,m) \subseteq \ldots$ So, $C(m) = \bigcup_{j=1}^{\infty} C_j(1,m)$ is a group and $C(m_0) = C_T(K)$.

**Lemma 2:** With the notation above, we have:

i) $C_j(X,m) \subseteq C_1(X,t \cdot m)$ for some integer $t$

ii) $C_1(1,m) \subseteq C_1(1,tm)$ for all positive integers $t$

iii) $C = \bigcup_{t=1}^{\infty} C_1(1,tm_0)$ is a group

iv) $C_T(K) \subseteq C$.

**Proof:** For i) we can see that if $f(X) \in C_j(X,m)$ then the zeros of $f(X)$ are $tm-th$ roots of unit for $t = [1,2,\ldots,j]$, where $[a_1,\ldots,a_n]$ indicates the least common multiple of the integers $a_1,\ldots,a_n$. So $f(X) \in C_1(X,tm)$.

ii) Immediate

iii) $C$ is a group because for each $m$, $C_1(1,m)$ is a group and given $m_1$ and $m_2$ multiples of $m_0$, there is $m$, multiple of $m_0$, such that $C_1(1,m_1)$ and $C_1(1,m_2)$

are contained in $C_1(1,m)$.

iv) Immediate, since $C_T(K) = C_1(m_0)$.

The next lemma states how to decompose a polinomial $f(X) = \prod_{i=1}^{m-1}(X - \xi_m^i)^{a_i} \in K(X)$ into a convenient product.

**Lemma 3:** If $f(X) = \prod_{i=1}^{m-1}(X - \xi_m^i)^{a_i} \in K(X)$, then $f(X) = \prod_{j=1}^{m} f_j(X)$, with $f_j(X) = \prod_{\substack{i=1 \\ (i,m)=j}}^{m-1} (X - \xi_m^i)^{a_i} \in k_{\frac{m}{j}}(X)$ and we may suppose that $m$ is multiple of $m_0$.

**Proof:** Without loss of generality, we can suppose that $f(X) \in K[X]$. It is clear that we can write $f(X) = \prod_{j=1}^{m} f_j(X)$, where

$$f_j(X) = \prod_{\substack{i=1 \\ (i,\frac{m}{j})=1}}^{\frac{m}{j}-1} (X - \xi_{\frac{m}{j}}^i)^{a_{ij}} \in K_{\frac{m}{j}}[X].$$

So, we only need to show that $f_j(X) \in K[X]$, that is, $f_j^\sigma(X) = f_j(X)$ for all $\sigma \in G'_m$. But if $\sigma \in G'_m$ and $\xi_m^i$ is a primitive $\frac{m}{j} - th$ root of unity, so is $\sigma(\xi_m^i)$; in other words, $\sigma$ preserves the factors $f_j(X)$, that is, $f_j^\sigma(X) = f_j(X)$. Thus $f_j(X) \in K[X] \cap K_{\frac{m}{j}}[X] = k_{\frac{m}{j}}[X]$.

**Lemma 4:** If $n$ is a positive integer, $L$ is a subfield of $K_n$ and $G' = Gal(Kn/L)$, then there are $\theta_1, \ldots, \theta_s \in G_n$ such that:

i) $G_n = \bigcup_{i=1}^{s} \theta_i G'$

ii) $g_i(X) = \prod_{\sigma \in G'} (X - \xi_n^{\theta_i \sigma}) \in L[X]$ and are irreducible in $L, i = 1, 2, \ldots, s$.

iii) $g_i(1) = N_{Kn/L}(1 - \xi_n^{\theta_i})$ , $i = 1, 2, \ldots, s$

iv) The set $\{g(X) = \prod_{\substack{i=1 \\ (i,n)=1}}^{n-1} (X - \xi_n^i)^{a_i} : a_i \in \mathbb{Z}$ and $g(X) \in L(X)\}$ is a free $\mathbb{Z}$-module of rank equal to $[K : Q]$ and generated by $g_i(X)$ , $i = 1, 2, \ldots, s$.

Proof: For i) we can take $\theta_i$ such that $G_n$ is disjoint union of cosets represented by $\theta_i$. For the other items the proof is an immediate consequence of the definition.

We can now return to Theorem 1.

**Proof of Theorem 1:** Firstly we show that $C_S(K) \subseteq C_1(1)$. Let $\varepsilon = \pi\alpha(n,a)^{b_{n,a}} \in C_S(K)$, where $\alpha(n,a) = N_{K_n/k_n}(1 - \xi_n^a)$. We let $f_{n,a} = \prod_{\sigma \in G'_n} (X - \xi_n^{a\sigma})$. Then $f(X) = \pi f_{n,a}(X)^{b_{n,a}} \in K(X)$ because each $f_{n,a}(X) \in K(X)$ and $\varepsilon = f(1) \in O_K^{\cdot}$, so $\varepsilon \in C_1(1)$. Now, we will show that $C \subseteq C_S(K)$. Let $\varepsilon \in C$ and $f(X) = \prod_{i=1}^{m-1} (X - \xi_m^i)^{a_i}$ for some multiple $m$ of $m_0$, such that $f(X) \in K(X)$ and $\varepsilon = f(1)$. But

$$f(X) = \prod_{j=1}^{m} f_j(X) \quad \text{with} \quad f_j(X) = \prod_{\substack{i=1 \\ (i,\frac{m}{j})=1}}^{\frac{m}{j}-1} (X - \xi_{\frac{m}{j}}^i)^{a_{ij}} \in k_{\frac{m}{j}}(X)$$

(lemma 3). Now, for each $j$ divisor of $m$, there are polinomials $g_{ij}(X) \in k_{\frac{m}{j}}[X]$ irreducibles such that

$$f_j(X) = \pi g_{ij}(X)^{b_{i,j}} \quad \text{and} \quad g_i(1) = N_{k_{\frac{m}{j}}/k_{\frac{m}{j}}}(1 - \xi_{\frac{m}{j}}^i)$$

(lemma 4). then $f_i(1) = \pi N_{K_{\frac{m}{j}}/k_{\frac{m}{j}}}(1 - \xi_{\frac{m}{j}}^i)^{b_{i,j}}$ and so $f(1) \in C_S(K)$

**Corollary 5:** The groups $C_i(1)$ defined in [5] are all equal to each other, in particular $C_T(K) = C_1(1)$.

We now turn to the group $S(K)$ of Special units of Rubin.

**Theorem 6:** If $K$ is an abelian number field, then $C_T(K) \subseteq S(K)$.

**Proof:** We will show that if $\varepsilon \in C_T(K)$ then $\varepsilon \in C(p)$, for all $p$ that splits completely in $K$. Let $K_p^+ = K_p \cap \mathbb{R}$, $L = K \cdot K_p^+$, $L_1 = K_{m_0} \cdot K_p^+$, $\tilde{p} =$ product of all primes of $L$ that lie over $p$ and $\tilde{p}_1 = \tilde{p}\theta_{L_1}$. If $\varepsilon_i = 1 - \xi_{m_0}^i$ and $u_i = (1 - \xi_{m_0}^i \xi_p^i)(1 - \xi_{m_0}^i \xi_p^{-1})$ then $u_i \in L_1$ and $\varepsilon_i^2 \equiv u_i (mod\ \tilde{p}_1)$. Now let $\varepsilon \in C_T(K)$ and $f(X) = \prod_{i=1}^{m_0-1}(X - \xi_{m_0}^i)^{a_i} \in K(X)$ such that $\varepsilon = f(1)$. We let

$$g(X) = \prod_{i=1}^{m_0-1}\left[(X - \xi_{m_0}^i \xi_p)(X - \xi_{m_0}^i \xi_p^{-1})\right]^{a_i}.$$

Now we can see that since $f(X) \in K(X)$ then $g(x) \in L(X)$, $f(1)^2 \equiv g(1)(mod\ \tilde{p})$ and $N_{L/K}(g(1)) = g(1)^{\sigma_p - 1}$, where $\sigma_p$ is the Frobenius map for $p$ in the Galois group $K/Q$; so $N_{L/K}(g(1)) = 1$, then $f(1) \in S(K)$ as we wanted to prove.

**Lemma 7:** Let $F \subset L$ number fields, $O_F^*$ and $O_L^*$ the groups of units of $F$ and $L$, respectively. If $N$ is the norm from $L$ to $F$, we can restrict $N$ to $O_L^*$ and $N(O_L^*)$ is a subgroup of $O_F^*$. Further more, the index $[O^* F : N(O_L^*)]$ is finite.

**Proof:** Since $O_F^{*s} \subseteq N(O_L^*) \subseteq O_F^*$, where $s = [L : F]$ then $N(O_L^*)$ has the same rank of $O_F^*$, because $O_F^{*s}$ does.

**Corollary 8:** If $K$ is an abelian number field, then $C_T(K), C_I(K), C_N(K)$ and $S(K)$ are of finite index in $O_K^*$.

**Proof:** Since the group of cyclotomic units of a cyclotomic field in of finite index in the group of global units (Theorem 1, [1]), then $C_N(K)$ has finite index in $O_K^{\cdot}$. Since $C_N(K)$ is contained in $C_T(K), C_I(K)$, and $S(K)$ up to roots of unity, the corollary follows.

**Remark:** When $K$ is a real abelian number field, we have $C_T(K) = C_N(K)$

**Added in Type:** After this work was prepared, I received a preprint of Günter Lettl, wherein he proves our Theorem 1. Our proof is different from his and leads naturally to our Theorem 6.

## References


[1] K. Ramachandra, On the Units of Cyclotomic Fields, Acta Arithmetica, XII (1966)

[2] K. Rubin, Global Units and Ideal Class Groups, Invent. Math. 89, 511–526 (1987)

[3] P. Samuel, Théorie Algébrique des Nombres, Hermann, Paris, (1967).

[4] W. Sinnott, On Stickelberger Ideal and the Circular Units of an Abelian Field, Invent. math. 62, 181–234 (1980)

[5] F. Thaine, On the Ideal Class Groups of Real Abelian Number Fields, Ann. of Math. 128, 1–18 (1988).

[6] L.C. Washington, Introduction to Cyclotomic Fields, Graduate texts in Mathematics, Springer-Verlag, New York (1982).

# RELATÓRIOS TÉCNICOS — 1989

**01/89** — **Uniform Approximation of Continuous Functions With Values in [0, 1]** — *João B. Prolla.*

**02/89** — **On Some Nonlinear Iterative Relaxation Methods in Remote Sensing** — *A. R. De Pierro.*

**03/89** — **A Parallel Iterative Method for Convex Programming with Quadratic Objective** — *Alfredo N. Iusem* and *Alvaro R. De Pierro.*

**04/89** — **Fifth Force, Sixth Force, and all that: a Theoretical (Classical) Comment** — *Erasmo Recami* and *Vilson Tonin-Zanchin.*

**05/89** — **An Application of Singer's Theorem to Homogeneous Polynomials** — *Raymundo Alencar.*

**06/89** — **Summhammer's Experimental Test of the Non-Ergodic Interpretation of Quantum Mechanics** — *Vincent Buonomano.*

**07/89** — **Privileged Reference Frames in General Relativity** — *Waldyr A. Rodrigues Jr.* and *Mirian E. F. Scanavini.*

**08/89** — **On the Numerical Solution of Bound Constrained Optimization Problems** — *Ana Friedlander* and *José Mario Martínez.*

**09/89** — **Dual Extremun Principles for the Heat Equation Solved by Finite Element Methods I** — *Vera Lucia da Rocha Lopes* and *José Vitório Zago.*

**10/89** — **Local Convergence Theory of Inexact Newton Methods Based on Structured Least Chance Updates** — *José Mario Martínez*

**11/89** — **Real Spin-Clifford Bundle and the Spinor Structure of Space-Time** — *Waldyr A. Rodrigues Jr.* and *Vera L. Figueiredo.*

**12/89** — **A Multiplier Theorem on Weighted Orlicz Spaces** — *B. Bordin* and *J. B. Garcia.*

**13/89** — **Dual Extremum Principles For The Heat Equation Solved By Finite Element Methods II** — *Vera Lucia da Rocha Lopes* and *José Vitório Zago.*

**14/89** — **Dirac and Maxwell Equations in the Clifford and Spin-Clifford Bundels** — *W. A. Rodrigues Jr.* and *E. Capelas de Oliveira.*

**15/89** — **Formal Structures, The Concepts of Covariance Invariance, Equivalent Reference Frames, and the Principle of Relativity** — *W. A. Rodrigues Jr., M. E. F. Scanavini* and *L. P. de Alcantara.*

**16/89** — **Local Minimizers of a Quadratic Function With a Spherical Constraint** — *José Mario Martínez.*

**17/89** — **On Pseudo-Convex Polycircular Domains In Banach Spaces** — *Mário C. Matos.*