Journal de Théorie des Nombres
de Bordeaux **17** (2005), 195–206

On the existence of Minkowski units in totally real cyclic fields

par FRANTIŠEK MARKO

RÉSUMÉ. Soit K un corps de nombres cyclique réel de degré n qui est le produit de deux nombres premiers distincts et tel que le nombre de classes du n-ième corps cyclotomique soit égal à 1. Nous établissons certaines conditions nécessaires et suffisantes pour l'existence d'une unité de Minkowski pour K.

ABSTRACT. Let K be a totally real cyclic number field of degree n that is the product of two distinct primes and such that the class number of the n-th cyclotomic field equals 1. We derive certain necessary and sufficient conditions for the existence of a Minkowski unit for K.

1. Introduction

The main result (Theorem II.1) of [1] states a necessary and sufficient condition for the existence of the Minkowski unit in the totally real cyclic fields of degree p^n. These conditions are of an inductive nature as they relate the existence of the Minkowski unit in such a field K_n to the existence of the Minkowski unit in the subfield K_{n-1}. Additional necessary conditions are the isomorphism of the factor-group of units $E_{K_n}/E_{K_{n-1}}$ and the group $\mathbb{Z}[\zeta_{p^n}]$ of integers of the p^n-th cyclotomic field together with the surjectivity of the norm map from K_n to K_{n-1} on units modulo $\{\pm 1\}$. For the sufficient conditions it is necessary to know the Minkowski unit of K_{n-1} and the generator of $E_{K_n}/E_{K_{n-1}}$ over $\mathbb{Z}[\zeta_{p^n}]$. The relationship between these generators is then described using a coordinate element from $\mathbb{Z}[\zeta_{p^n}]$. If the coordinate element can be represented by a unit of a certain ring and the previously mentioned norm map on units is surjective, the existence of the Minkowski unit follows. This method works best when all the invertible classes can be covered by units as is the case for the degrees $p^n = 4, 8$ and 9. For these degrees the existence of the Minkowski unit is equivalent to the surjectivity of the norm map on units, see [1], Theorem II.2.

The general idea of local generators and coordinates similar to [1] extends to totally real cyclic number fields of degree n for which the ring $\mathbb{Z}[\zeta_n]$ of

the integers of the n-th cyclotomic field is a unique factorisation domain. We treat in detail the case when n is a product of two distinct primes. Among other results we prove the following statement.

Theorem 1.1. *Let K be a totally real cyclic number field of degree $n = 6, 10$ or 14. Then K contains a Minkowski unit if and only if the norm maps from K to its subfields are surjective on units.*

For precise formulation see Corollary 5.3. This theorem is a generalization of Theorem 3 of [3].

2. Notation

Throughout the paper the symbols p, q will denote distinct prime numbers, n a positive composite integer, $K = K_n$ a totally real cyclic number field of degree n over the field $\mathbb{Q}$ of rational numbers. Denote by σ a generator of the Galois group G of K over $\mathbb{Q}$, by K_m a subfield of K of degree $m > 1$ over $\mathbb{Q}$ that is fixed by the subgroup of G generated by σ^m. The letters m, l, d will be reserved for divisors of n that are larger than 1, hence they correspond to subfields of K. Let E_{K_m} be the group of all units of the field K_m and $U_{K_m} = E_{K_m}/\{\pm 1\}$. Further denote by $\varphi_m(x)$ the m-th cyclotomic polynomial, let ζ_m a primitive m-th root of unity and put $\psi_m(x) = \sum_{i=0}^{\frac{n}{m}-1} x^{im} = \frac{x^n-1}{x^m-1} = \prod_{l|n;l\nmid m} \varphi_l(x)$, $O = \mathbb{Z}[x]/(\frac{x^n-1}{x-1})$ and $O_m = \mathbb{Z}[x]/(\varphi_m(x))$. Note that U_K is not only a G-module but an O-module as well.

A unit $u \in E_{K_m}$ is called a *Minkowski unit* of K_m if the conjugates of u generate U_{K_m}; this is equivalent to the Galois module U_{K_m} being cyclic.

For an O-module W denote $W_m = W^{\psi_m(x)}$ and $\tilde{W}^m = \prod_{p|m} W_{\frac{m}{p}}$ and $\tilde{W}_m = W_m/\tilde{W}^m$. An O-module W will be called *structured* if $\tilde{W}_m$ is a nontrivial cyclic O_m-module for each $m|n$. Actually $\tilde{W}_m \cong O_m$ as O-modules in that case.

The number of isomorphism classes of O-structured modules is denoted by $M(n)$. We conjecture that each isomorphism class of structured O-modules contains U_K for some number field K. In any case the index $M(n)$ is an upper bound for the number of isoclasses of structured Galois modules U_K for fields K of degree n.

The function $\Omega(m)$ is defined as the sum of the exponents in the prime factorization of m, i.e. if $m = \prod_{i=1}^{t} p_i^{e_i}$, then $\Omega(m) = \sum_{i=1}^{t} e_i$. For a structured module W we say that its element w has length k and write $\ell(w) = k$ if $w \in \prod_{m;\Omega(m)=k} W_m$ but $w \notin \prod_{m;\Omega(m)=k-1} W_m$.

3. Coordinates and Galois structure

We start with an observation. Let $m = \prod_{k=1}^{s} p_k^{a_k}$, and put $A_k(x) = \prod_{l|m;l\nmid\frac{m}{p_k}} \varphi_l(x)$.

Lemma 3.1. *The ideal of $\mathbb{Z}[x]$ generated by polynomials A_k for $k = 1, \ldots, s$ equals $(\varphi_m(x))$.*

Proof. Clearly $\varphi_m(x)$ divides A_k, so write $A_k = \varphi_m(x)g_k(x)$. The polynomials φ_k are all irreducible, and this implies that the polynomials g_k are pairwise relatively prime. Therefore the ideal of $\mathbb{Z}[x]$ generated by all g_k's equals $c\mathbb{Z}[x]$ for a certain non-zero $c \in \mathbb{Z}[x]$. This shows that the ideal I generated by the A_k's is principal, and is generated by $c\varphi_m(x)$. Hence all coefficients of polynomials lying in I are divisible by c, however the polynomals A_k are monic, and this forces c to be 1. □

Existence of a Minkowski unit of K implies certain structural properties of the groups of units of subfields of K.

Proposition 3.2. *If K has a Minkowski unit, then $Norm_{K/K_m} U_K = U_{K_m}$ for each subfield K_m of K. Moreover, the O-module $U_{K_m}/\prod_{p|m} U_{K_{\frac{m}{p}}}$ is isomorphic to O_m.*

Proof. If K has a Minkowski unit ϵ, then by [4], Prop.I.3, the $\mathbb{Z}[G]$-module U_K is isomorphic to O, where the generator ϵ corresponds to 1 and the conjugation by σ corresponds to multiplication by x. Moreover, in this case according to [4], Prop.I.4, and its corollary, each subfield K_m has a Minkowski unit and $Norm_{K/K_m} U_K = U_{K_m}$ for each subfield K_m of K. The group U_{K_m} is isomorphic to $\psi_m(x)O$ and the factor-group $U_K/\prod_{p|n} U_{K_{\frac{n}{p}}}$ is isomorphic to O modulo the ideal generated by all $\psi_{\frac{n}{p}}(x)$. Using Lemma 3.1, we get that this factor-group is isomorphic to $\mathbb{Z}[x]/(\varphi_n(x))$. It is an immediate consequence of $R(m)$ that the ideal of O generated by all $\psi_{\frac{m}{p}}(x)$ for all $p|m$ equals $(\varphi_m(x)\psi_m(x))$. Therefore for each $m|n$ the factor-group $U_{K_m}/\prod_{p|m} U_{K_{\frac{m}{p}}}$ is isomorphic to $O_m = \mathbb{Z}[x]/(\varphi_m(x))$. □

Corollary 3.3. *The O-module O is structured. Moreover, if K has a Minkowski unit, then $U = U_K$ is structured.*

Proof. Since $U_{K_m} = Norm_{K/K_m} U = U^{\psi_m(x)}$ we have $U_{K_m} = U_m$ for each $m|n$. □

For special values of n the Galois module U is structured if the norm maps on units are surjective (without the assumption about the existence of the Minkowski unit).

Proposition 3.4. *If $\mathbb{Z}[\zeta_n]$ is a principal ideal domain and $Norm_{K/K_m} U_K = U_{K_m}$ for each subfield K_m of K, then U_K is structured.*

Proof. According to [3], U_K is isomorphic as a G-module to an ideal M of the ring O. Assuming that the norm map on units are surjective (that is $Norm_{K/K_m}U_K = U_{K_m}$ for each subfield K_m of K) we obtain that $U_m = U_{K_m}$ corresponds to module $\psi_m(x)M$ that is annihilated by $\prod_{l|n;l\nmid m}\varphi_l(x)$ and $\tilde{U}_m$ is isomorphic to $\psi_m(x)M/(\psi_{\frac{m}{p}}(x)M; p|m)$. Lemma 3.1 implies that $\psi_m(x)M/(\psi_{\frac{m}{p}}(x)M; p|m)$ is a module over $\mathbb{Z}[\zeta_m]$. If $\mathbb{Z}[\zeta_n]$ is a principal ideal domain, then so is $\mathbb{Z}[\zeta_m]$ and in this case $\tilde{U}_m$ is a cyclic $\mathbb{Z}[\zeta_m]$-module. The fact that it is nontrivial follows from the Dirichlet unit theorem. □

From now on assume that an O-module W is structured. Keep in mind the prominent example of the structured O-module, namely the group U_K of the field K that is given by Proposition 3.4.

Fix and denote by w_m an element of W_m whose class represents a generator of $\tilde{W}_m$ as an O_m-module. Note that each w_m can be written as $w_m = v_m^{\psi_m(x)}$ where $v_m \in W$. Then each $w \in W$ can be written uniquely as a product $w = \prod_{m|n} w_m^{\alpha_m(w)}$, where $\alpha_m(w)$ is a polynomial from O such that its degree does not exceed the degree of $\varphi_m(x)$. The exponents $\alpha_m(u)$ are called *coordinates* of w.

The elements $\{w_m; m|d\}$ (as well as $\{v_m; m|d\}$) are generators of W as an O- module. In order to work with the above factorizations and to determine the O-structure of W, we will derive conditions describing when $\prod_{m|n} w_m^{a_m(x)} = 1$ for arbitrary polynomials $\alpha_m(x)$ from O.

For each w_m and each $d|m$ we have $w_m^{\frac{\psi_d(x)}{\psi_m(x)}} = v_m^{\psi_d(x)}$. Denote $a_{m,d} = \alpha_d(v_m^{\psi_d(x)})$. Then $a_{m,m} = 1$ and the collection of all such $a_{m,d}$ for $d|m; d \neq m$ is called the *coordinate system* of W.

Proposition 3.5. *Let $a_m(x); m|n$ be polynomials in O. Then $\prod_{m|n} w_m^{a_m(x)} = 1$ if and only if for all $d|n$ the condition $C_d : \sum_{d|m|n} \frac{n}{m} a_m(x) a_{m,d} \equiv 0 \pmod{\varphi_m(x)}$ is satisfied.*

Proof. We proceed in steps depending on the upper bound for the length of $w = \prod_{m|n} w_m^{a_m(x)}$. First, $\ell(w) < \Omega(n)$ if and only if $w \in \tilde{W}^n$ which is equivalent to $a_n(x) \equiv 0 \pmod{\varphi_n(x)}$ and that is condition C_n. Next assume that $\ell(w) \leq k$. We are looking for conditions that are equivalent to $\ell(w) < k$. The assumption $\ell(w) \leq k$ means that $w \in \prod_{l|n;\ell(l)=k} W_l$, say $w = \prod_{l|n;\ell(l)=k} z_l$ with $z_l \in W_l$. Choose $l_0|n$ such that $\ell(l_0) = k$ and consider $w^{\psi_{l_0}(x)}$. It is a product of $z_{l_0}^{\psi_{l_0}(x)}$ and other terms $z_l^{\psi_{l_0}(x)}$ for $l \neq l_0$. Since each $z_l = y_l^{\psi_l(x)}$ for some $y_l \in W$ and $\psi_{l_0}(x)\psi_l(x) \in (\psi_{l_0}(x)\varphi_{l_0}(x))$ for $l \neq l_0$, each $z_l^{\psi_{l_o}(x)}$ belongs to $\tilde{W}^{l_0}$. Therefore $z_{l_0} \in \tilde{W}^{l_0}$ if and only if $w^{\psi_{l_0}(x)} \in \tilde{W}^{l_0}$ which is the same as $\alpha_{l_0}(w^{\psi_{l_0}(x)}) = 0$. Since $\alpha_{l_0}(w_m^{\psi_{l_0}(x)}) = \frac{n}{l_0} a_{m,l_0}$ the last

equality is equivalent to C_{l_0}. Therefore $\ell(w) < k$ if and only if all conditions C_l for $\ell(l) = k$ are satisfied. Hence $u = 1$ if and only if all conditions C_d for $d|n$ are satisfied. □

Although the above conditions C_d do not describe explicitly the Galois action on w_m they provide a means of checking whether the computations involving Galois action on generators w_m are correct.

It is interesting that only the leading exponent $a_{m,d}$ in the factorization of $w_m^{\frac{\psi_d(x)}{\psi_m(x)}}$ with respect to generators w_l is needed in the above theorem.

The polynomials $a_{m,d}$ are related by various congruences. They vary depending on the type of decomposition of n into the product of primes and therefore we will investigate the relationship between $a_{m,d}$ separately for each such type.

In the next sections we will be looking for conditions on a coordinate system $a_{m,d}$ of U that will guarantee the existence of a Minkowski unit in K. For that purpose we will investigate the relationship between coordinate systems for various fields of the same degree n.

4. The case $n = p^2$

The main priority in the case $n = p^2$ is not to prove new results but to explain our method in the simplest nontrivial case, show a connection with the work of [1], and view and reprove some of their results from a different perspective. First note that $\varphi_{p^2}(x) \equiv p \pmod{\varphi_p(x)}$.

A structured O-module T is given by a generating set $\{t_{p^2}, t_p\}$ and the coordinate $a_{p^2,p}$. If $t = t_{p^2}^{\alpha_{p^2}(t)} t_p^{\alpha_p(t)}$, then $t^{\psi_p(x)} = t_p^{a_{p^2,p}\alpha_{p^2}(t)+p\alpha_p(t)}$. Since $T^{\psi_p(x)} = T_p$ the congruence $a_{p^2,p}\alpha_{p^2}(t)+p\alpha_p(t) \equiv 1 \pmod{\varphi_p(x)}$ must have a solution which is equivalent to $a_{p^2,p}$ being invertible modulo $(p, \varphi_p(x))$.

Conversely, if a polynomial $a_{p^2,p}$ is invertible modulo $(p, \varphi_p(x))$, then we can define an O-module $\tilde{T}$ generated by $\{\tilde{t}_{p^2}, \tilde{t}_p\}$ that is structured and $a_{p^2,p}$ is its coordinate. Set $\tilde{T} = O_{p^2} \oplus O_p$ as an abelian group and $\tilde{t}_{p^2} = (1,0), \tilde{t}_p = (0,1)$. A $Z[x]$-module structure on $\tilde{T}$ is defined as $c(x)(a(x), b(x)) = (f(x), a_{p^2,p}e(x) + b(x)c(x))$, where $e(x)$ and $f(x)$ are the quotient and the remainder respectively after the division of the polynomial $a(x)c(x)$ by $\varphi_{p^2}(x)$.

Assume now that we have two structured O-modules T and W generated by $\{t_{p^2}, t_p\}$ and $\{w_{p^2}, w_p\}$ respectively, with coordinates $a_{p^2,p}$ and $b_{p^2,p}$ respectively.

We would like to determine when T and W are isomorphic as O-modules. As a special case, for number fields K and K' of degree $n = 4, 9$ or 25 satisfying $Norm_{K/K_p}U_K = U_{K_p}$ and $Norm_{K'/K'_p}U'_{K'} = U'_{K_p}$ this would allow us to compare Galois structures of U_K and $U_{K'}$ as well as to determine

whether K has an Minkowski unit (if U_K is isomorphic to the structured module O).

If $L : T \to W$ is an O-morphism, then $L(T_p) \subset W_p$ and therefore $L(t_{p^2}) = w_{p^2}^{a(x)} w_p^{b(x)}$ and $L(t_p) = w_p^{c(x)}$ for some $a(x) \in O$ and $b(x), c(x) \in O_p$. A map L defined on generators in the above way is a morphism of O-modules if $t_{p^2}^{k(x)} t_p^{l(x)} = 1$ for $k(x) \in O, l(x) \in O_p$ implies $L(t_{p^2})^{k(x)} L(t_p)^{l(x)} = 1$.

Proposition 3.5 applied to T shows $t_{p^2}^{k(x)} t_p^{l(x)} = 1$ if and only if

$$k(x) \equiv 0 \pmod{\varphi_{p^2}(x)} \quad \text{and} \quad a_{p^2,p} k(x) + p l(x) \equiv 0 \pmod{\varphi_p(x)}.$$

That means

$$k(x) = \varphi_{p^2}(x) k'(x) \quad \text{and} \quad l(x) \equiv -a_{p^2,p} k'(x) \pmod{\varphi_p(x)}.$$

Use Proposition 3.5 again for W to see that

$$L(t_{p^2})^{k(x)} L(t_p)^{l(x)} = w_{p^2}^{a(x)k(x)} w_p^{b(x)k(x)+c(x)l(x)} = 1$$

if and only if $a(x)k(x) \equiv 0 \pmod{\varphi_{p^2}(x)}$ and

$$b_{p^2,p} a(x)k(x) + p(b(x)k(x) + c(x)l(x)) \equiv 0 \pmod{\varphi_p(x)}.$$

The first congruence is clearly satisfied and the second one is equivalent to

$$b_{p^2,p} a(x) k'(x) + p b(x) k'(x) - c(x) a_{p^2,p} k'(x) \equiv 0 \pmod{\varphi_p(x)}.$$

Since there are no restrictions on the values of $k'(x)$ we can choose $k'(x) = 1$ and obtain

$$b_{p^2,p} a(x) - a_{p^2,p} c(x) \equiv -p b(x) \pmod{\varphi_p(x)}.$$

This congruence gives a necessary and sufficient condition for L to be an O-morphism from T to W.

Therefore the existence of an O-morphism L from T to W as above is given by the following congruence:

$$b_{p^2,p} a(x) \equiv a_{p^2,p} c(x) \pmod{(p, \varphi_p(x))}.$$

If this congruence is satisfied for some $a(x), c(x)$, we can compute $b(x)$ as required to make L an O-morphism.

Assume now that L as above is an isomorphism. Then $L(T_p) = W_p$ and since $L(t_p^{l(x)}) = w_p^{c(x)l(x)}$, the class of $c(x)$ modulo $\varphi_p(x)$ must be invertible. Since $L(T) = W$ the class of $a(x)$ modulo $\varphi_{p^2}(x)$ must be invertible as well. Conversely, we will show that if $a(x)$ is invertible modulo $\varphi_{p^2}(x)$ and $c(x)$ is invertible modulo $\varphi_p(x)$, then L is an isomorphism. Assume $t \in Ker(L)$ and $k(x), l(x)$ are coordinates of t with respect to the generators $\{t_{p^2}, t_p\}$. Then $L(t) = w_{p^2}^{a(x)k(x)} w_p^{b(x)k(x)+c(x)l(x)} = 1$ implies $a(x)k(x) \equiv 0 \pmod{\varphi_{p^2}(x)}$ and since the class of $a(x)$ is invertible, we have $k(x) = 0$. Therefore $L(t) = w_p^{c(x)l(x)} = 1$ and since the class of $c(x)$ is invertible we

also have $l(x) = 0$ and thus $t = 1$. We have established that such map L is injective. If $c(x)$ is invertible modulo $\varphi_p(x)$, then clearly $L(T_p) = W_p$. If also the class of $a(x)$ modulo $\varphi_{p^2}(x)$ is invertible, then L also induces a map onto $\tilde{W} = W/W_p$ and thus L is surjective.

Hence we determined the conditions for an isomorphism between structured modules.

Proposition 4.1. *Let T and W be structured O-modules for $n = p^2$ with coordinates $a_{p^2,p}$ and $b_{p^2,p}$ respectively. Then $T \cong W$ as O-modules if and only if there is $a(x) \in O$ that is invertible modulo $\varphi_{p^2}(x)$, $c(x) \in O_p$ that is invertible modulo $\varphi_p(x)$ and*

$$b_{p^2,p}a(x) \equiv a_{p^2,p}c(x) \pmod{(p, \varphi_p(x))}.$$

When comparing this result with [1], Theorem II.1, it is worth noting that the congruence classes there appear as a consequence of a choice of generators whereas congruence classes here appear because of the requirement for morphism.

The above criteria further simplifies for $n = p^2 = 4, 9$ and 25. This is the case when the class number of $\mathbb{Z}[\zeta_n]$ and $\mathbb{Z}[\zeta_p]$ equals 1 and hence all units in these rings are $\pm$ cyclotomic units.

If a polynomial is represented by a cyclotomic unit $\frac{x^a-1}{x-1}$ for $(a, p) = 1$ modulo $\varphi_{p^2}(x)$, then its class modulo $\varphi_p(x)$ is also represented by a unit. Thus if $a(x)$ is represented by a unit modulo $\varphi_{p^2}(x)$ then $a(x)$ is also represented by a unit modulo $\varphi_p(x)$. Therefore the condition of Proposition 4.1 is satisfied if and only if the invertible class of $b_{p^2,p}a_{p^2,p}^{-1}$ modulo $(p, \varphi_p(x))$ is represented by a unit modulo $\varphi_p(x)$. This also means that if an isomorphism of T and W exists, then there is one with $a(x) = 1$. We have thus proved the following statement.

Proposition 4.2. *If $n = p^2 = 4, 9$ or 25, then structured modules T and W are isomorphic as O-modules if and only if the invertible class of $b_{p^2,p}a_{p^2,p}^{-1}$ modulo $(p, \varphi_p(x))$ is represented by a unit modulo $\varphi_p(x)$.*

Corollary 4.3. *If K is a totally real cyclic number field of degree $n = p^2 = 4$ or 9, then K contains a Minkowski unit if and only if $Norm_{K/K_p}U_K = U_{K_p}$.*

Corollary 4.4. *If K is a totally real cyclic number field of degree $n = 25$ such that $Norm_{K/K_5}U_K = U_{K_5}$, then K contains a Minkowski unit if and only if the class of its coordinate $b_{25,5}$ modulo $(5, \varphi_5(x))$ is represented by a unit modulo $\varphi_5(x)$.*

Proof. Assumption $Norm_{K/K_p}U_K = U_{K_p}$ implies that $T = U_K$ is structured. Put $W = O$ in the above proposition. Since the coordinate $b_{p^2,p} = 1$ for O, the modules U_K and O are isomorphic (meaning a Minkowski unit

exists for K) if and only if $a_{p^2,p}$ modulo $(p, \varphi_p(x))$ has a representative that is a unit modulo $\varphi_p(x)$. It can be checked easily that every for $n = 4, 9$, every invertible class modulo $(p, \varphi_p(x))$ satisfies this condition. □

Corollary 4.5. $M(25) = 5$.

Proof. It can be easily verified that the condition in Corollary 4.4 is true only for 20 out of 100 invertible classes. □

Therefore there are at most 5 nonisomorphic Galois structures of U_K for fields K of degree $n = 25$ with $Norm_{K/K_5} U = U_{K_5}$.

5. The case $n = pq$

We will proceed in the same way as outlined in section 4. First note that $(\varphi_p(x), \varphi_q(x)) = 1$,$\psi_p(x) = \varphi_{pq}(x)\varphi_q(x) \equiv q \pmod{\varphi_p(x)}$ and $\psi_q(x) = \varphi_{pq}(x)\varphi_p(x) \equiv p \pmod{\varphi_q(x)}$.

A structured O-module T is given by a generating set $\{t_{pq}, t_p, t_q\}$ and the coordinate system $\{a_{pq,p}, a_{pq,q}\}$. If $t = t_{pq}^{\alpha_{pq}(t)} t_p^{\alpha_p(t)} t_q^{\alpha_q(t)}$, then $t^{\psi_p(x)} = t_p^{a_{pq,p}\alpha_{pq}(t)+q\alpha_p(t)}$ and $t^{\psi_q(x)} = t_q^{a_{pq,q}\alpha_{pq}(t)+p\alpha_q(t)}$. Since $T^{\psi_p(x)} = T_p$ and $T^{\psi_q(x)} = T_q$ the congruences $a_{pq,p}\alpha_{pq}(t) + q\alpha_p(t) \equiv 1 \pmod{\varphi_p(x)}$ and $a_{pq,q}\alpha_{pq}(t) + p\alpha_q(t) \equiv 1 \pmod{\varphi_q(x)}$ must have solutions which is equivalent to $a_{pq,p}$ being invertible modulo $(q, \varphi_p(x))$ and $a_{pq,q}$ being invertible modulo $(p, \varphi_p(x))$.

Conversely, given a pair $\{a_{pq,p}, a_{pq,q}\}$ such that the polynomial $a_{pq,p}$ is invertible modulo $(q, \varphi_p(x))$ and the polynomial $a_{pq,q}$ is invertible modulo $(p, \varphi_p(x))$, we can define an O-module $\tilde{T}$ generated by $\{\tilde{t}_{pq}, \tilde{t}_p, \tilde{t}_q\}$ that is structured and $\{a_{pq,p}, a_{pq,q}\}$ is its coordinate system. Set $\tilde{T} = O_{pq} \oplus O_p \oplus O_q$ as an abelian group and $\tilde{t}_{pq} = (1, 0, 0), \tilde{t}_p = (0, 1, 0), \tilde{t}_q = (0, 0, 1)$. Let $\gamma_p(x)$ and $\gamma_q(x)$ be polynomials such that $\varphi_p(x)\gamma_p(x) + \varphi_q(x)\gamma_q(x) = 1$. A $Z[x]$-module structure on $\tilde{T}$ is defined as $d(x)(a(x), b(x), c(x)) = (f(x), \gamma_p(x)a_{pq,p}e(x) + b(x)d(x), \gamma_q(x)a_{pq,q}e(x) + c(x)d(x))$, where $e(x)$ and $f(x)$ are the quotient and the remainder respectively after the division of the polynomial $a(x)d(x)$ by $\varphi_{pq}(x)$.

Assume now that we have two structured O-modules T and W generated by $\{t_{pq}, t_p, t_q\}$ and $\{w_{pq}, w_p, w_q\}$ respectively with the coordinate systems $\{a_{pq,p}, a_{pq,q}\}$ and $\{b_{pq,p}, b_{pq,q}\}$ respectively.

If $L : T \to W$ is an O-morphism, then $L(T_p) \subset W_p$ and $L(T_q) \subset W_q$ and therefore $L(t_{pq}) = w_{pq}^{a(x)} w_p^{b(x)} w_q^{c(x)}$, $L(t_p) = w_p^{d(x)}$ and $L(t_q) = w_q^{e(x)}$ for some $a(x) \in O$, $b(x), d(x) \in O_p$ and $c(x), e(x) \in O_q$. A map L defined on generators in the above way is a morphism of O-modules if $t_{pq}^{k(x)} t_p^{l(x)} t_q^{m(x)} = 1$ for $k(x) \in O$, $l(x) \in O_p$ and $m(x) \in O_q$ implies $L(t_{pq})^{k(x)} L(t_p)^{l(x)} L(t_q)^{m(x)} = 1$.

Proposition 3.5 applied to T shows $t_{pq}^{k(x)}t_p^{l(x)}t_q^{m(x)} = 1$ if and only if

$$k(x) \equiv 0 \pmod{\varphi_{pq}(x)}, \quad a_{pq,p}k(x) + ql(x) \equiv 0 \pmod{\varphi_p(x)}$$

and

$$a_{pq,q}k(x) + pm(x) \equiv 0 \pmod{\varphi_q(x)}.$$

That means

$$k(x) = \varphi_{pq}(x)k'(x), \quad l(x) \equiv -a_{pq,p}k'(x) \pmod{\varphi_p(x)}$$

and

$$m(x) \equiv -a_{pq,q}k'(x) \pmod{\varphi_q(x)}.$$

Use Proposition 3.5 again for W to see that

$$L(t_{pq})^{k(x)}L(t_p)^{l(x)}L(t_q)^{m(x)} = w_{pq}^{a(x)k(x)}w_p^{b(x)k(x)+d(x)l(x)}w_q^{c(x)k(x)+e(x)m(x)}$$

$= 1$ if and only if $a(x)k(x) \equiv 0 \pmod{\varphi_{pq}(x)}$,

$$b_{pq,p}a(x)k(x) + q(b(x)k(x) + d(x)l(x)) \equiv 0 \pmod{\varphi_p(x)}$$

and

$$b_{pq,q}a(x)k(x) + p(c(x)k(x) + e(x)m(x)) \equiv 0 \pmod{\varphi_q(x)}.$$

The first congruence is clearly satisfied and the later ones are equivalent to

$$b_{pq,p}a(x)k'(x) + qb(x)k'(x) - d(x)a_{pq,p}k'(x) \equiv 0 \pmod{\varphi_p(x)}$$

and

$$b_{pq,q}a(x)k'(x) + pc(x)k'(x) - e(x)a_{pq,q}k'(x) \equiv 0 \pmod{\varphi_q(x)}.$$

Since there are no restrictions on the values of $k'(x)$ we can choose $k'(x) = 1$ to verify that both

$$b_{pq,p}a(x) - a_{pq,p}d(x) \equiv -qb(x) \pmod{\varphi_p(x)}$$

and

$$b_{pq,q}a(x) - a_{pq,q}e(x) \equiv -pc(x) \pmod{\varphi_q(x)}$$

must have solutions. These congruences provide a necessary and sufficient condition for L to be an O-morphism from T to W.

If the following system of congruences

$$b_{pq,p}a(x) \equiv a_{pq,p}d(x) \pmod{(q, \varphi_p(x))}$$

$$b_{pq,q}a(x) \equiv a_{pq,q}e(x) \pmod{(p, \varphi_q(x))}$$

has a solution, then we can compute $b(x), c(x)$ as required to make L an O-morphism.

An element $t = t_{pq}^{k(x)}t_p^{l(x)}t_q^{m(x)}$ of T is been mapped by L to

$$w_{pq}^{a(x)k(x)}w_p^{b(x)k(x)+d(x)l(x)}w_q^{c(x)k(x)+e(x)m(x)}.$$

Assume now that L as above is an isomorphism. Then $L(T_p) = W_p$ and $L(T_q) = W_q$ and since $L(t_p^{l(x)}) = w_p^{d(x)l(x)}$ and $L(t_q^{m(x)}) = w_q^{e(x)m(x)}$ the classes of $d(x)$ modulo $\varphi_p(x)$ and $e(x)$ modulo $\varphi_q(x)$ must be invertible. Since $L(T) = W$ the class of $a(x)$ modulo $\varphi_{pq}(x)$ must be invertible as well. Conversely, we will show that if $a(x)$ is invertible modulo $\varphi_{pq}(x)$, $d(x)$ is invertible modulo $\varphi_p(x)$ and $e(x)$ is invertible modulo $\varphi_q(x)$, then L is an isomorphism. Assume $t \in Ker(L)$ and $k(x), l(x), m(x)$ are coordinates of t with respect to the generators $\{t_{pq}, t_p, t_q\}$. Then

$$L(t) = w_{pq}^{a(x)k(x)} w_p^{b(x)k(x)+d(x)l(x)} w_q^{c(x)k(x)+e(x)m(x)} = 1$$

implies $a(x)k(x) \equiv 0 \pmod{\varphi_{pq}(x)}$ and since the class of $a(x)$ is invertible, we have $k(x) = 0$. Therefore $L(t) = w_p^{d(x)l(x)} w_q^{e(x)m(x)} = 1$. Then $(\varphi_p(x), \varphi_q(x)) = 1$ implies $w_p^{d(x)l(x)} = 1$ and $w_q^{e(x)m(x)} = 1$. Since the classes of $d(x)$ and $e(x)$ are invertible we must have $l(x) = 0$ and $m(x) = 0$ hence $t = 1$. We have established that such map L is injective. If $d(x)$ is invertible modulo $\varphi_p(x)$ and $e(x)$ is invertible modulo $\varphi_q(x)$, then clearly $L(T_p) = W_p$ and $L(T_q) = W_q$. If also the class of $a(x)$ modulo $\varphi_{pq}(x)$ is invertible, then L also induces a map onto $\tilde{W} = W/W_pW_q$ and hence L is surjective.

Hence we determined the conditions for an isomorphism between structured modules.

Proposition 5.1. *Let T and W be structured O-modules for $n = pq$ with coordinate systems $\{a_{pq,p}, a_{pq,q}\}$ and $\{b_{pq,p}, b_{pq,q}\}$ respectively. Then $T \cong W$ as O-modules if and only if there there is $a(x) \in O$ that is invertible modulo $\varphi_{pq}(x)$, $d(x) \in O_p$ that is invertible modulo $\varphi_p(x)$, $e(x) \in O_q$ that is invertible modulo $\varphi_q(x)$ and*

$$b_{pq,p}a(x) \equiv a_{pq,p}d(x) \pmod{(q, \varphi_p(x))}$$

$$b_{pq,q}a(x) \equiv a_{pq,q}e(x) \pmod{(p, \varphi_q(x))}.$$

The above criteria further simplifies when the class number of $\mathbb{Z}[\zeta_{pq}]$ equals 1 and hence all units in $\mathbb{Z}[\zeta_{pq}], \mathbb{Z}[\zeta_p]$ and $\mathbb{Z}[\zeta_q]$ are $\pm$ cyclotomic units. This is the case if and only if $n = 6, 10, 14, 15, 21, 22, 26, 33, 34, 35$ or 38.

We will look first at the case when $n = 2p$, that is $n = 6, 10, 14, 22, 26, 34, 38$. If $a(x)$ is invertible modulo $\varphi_{2p}(x)$ then there is polynomial $a^*(x)$ such that $a(x)a^*(x) \equiv 1 \pmod{\varphi_{2p}(x)}$. Since $\varphi_{2p}(x) = \varphi_p(-x)$ it is equivalent to $a(-x)a^*(-x) \equiv 1 \pmod{\varphi_p(x)}$ that is $a(-x)$ is invertible modulo $\varphi_p(x)$. But $a(x) \equiv a(-x) \pmod 2$ shows that classes modulo $(2, \varphi_p(x))$ represented by polynomials that are invertible modulo $\varphi_{2p}(x)$ coincide with those classes modulo $(2, \varphi_p(x))$ represented by polynomials invertible modulo

$\varphi_p(x)$. We can therefore replace the first congruence of Proposition 5.1 by congruence $b_{2p,p}a_{2p,p}^{-1} \equiv d'(x) \pmod{(2, \varphi_p(x))}$ for a polynomial $d'(x)$ invertible modulo $\varphi_p(x)$.

How about congruence classes of $a(x)$ modulo $(p, x+1)$ for $a(x)$ invertible modulo $\varphi_{2p}(x)$? For $p = 3, 5, 11, 13$ and 19, the polynomial $1-x$ is invertible modulo $\varphi_{2p}(x)$ and $1 - x \equiv 2 \pmod{x+1}$, and since 2 is a primitive root modulo p, every nonzero class modulo $(p, x+1)$ is represented by a polynomial invertible modulo $\varphi_{2p}(x)$. For the remaining cases $p = 7$ and 17, the polynomial $1-x+x^2$ is invertible modulo $\varphi_{2p}(x)$ and $1-x+x^2 \equiv 3 \pmod{x+1}$ and we use the fact that 3 is now a primitive root modulo p to see that each nonzero class modulo $(p, x+1)$ is represented by a polynomial invertible modulo $\varphi_{2p}(x)$. We have thus established that we can always choose $a(x)$ such that the second congruence is satisfied.

We have proved the following proposition.

Proposition 5.2. *Let $n = 6, 10, 14, 22, 26, 34$ or 38. Then the structured modules T and W are isomorphic as O-modules if and only if the invertible class of $b_{2p,p}a_{2p,p}^{-1}$ modulo $(2, \varphi_p(x))$ can be represented by a polynomial invertible modulo $\varphi_p(x)$.*

Corollary 5.3. *If K is a totally real cyclic number field of degree $n = 2p = 6, 10$ or 14, then K contains a Minkowski unit if and only if $Norm_{K/K_p}U_K = U_{K_p}$ and $Norm_{K/K_2}U_K = U_{K_2}$.*

Corollary 5.4. *If K is a totally real cyclic number field of degree $n = 2p = 22, 26, 34$ or 38 such that $Norm_{K/K_p}U_K = U_{K_p}$ and $Norm_{K/K_2}U_K = U_{K_2}$, then K contains a Minkowski unit if and only if the class of its coordinate $b_{2p,p}$ modulo $(2, \varphi_p(x))$ is represented by a unit modulo $\varphi_p(x)$.*

Proof. Assumption of the corollaries imply that $T = U_K$ is structured. For $W = O$ the coordinate system $a_{2p,p} = 1, a_{2p,2} = 1$ and the modules U_K and O are isomorphic (meaning Minkowski unit exists for K) if and only if the invertible class $b_{2p,p}$ modulo $(p, \varphi_p(x))$ has a representative that is a unit modulo $\varphi_p(x)$. For $n = 2p = 6, 10$ powers of a cyclotomic unit $1 + x$ modulo $\varphi_p(x)$ cover all nonzero classes modulo $(2, \varphi_p(x))$. For $n = 2p = 14$ the prime 2 has index 2 modulo 7 and hence $\varphi_7(x)$ modulo factors into a product of two irreducible polynomials of degree 3. Therefore there are 49 invertible classes modulo $(2, \varphi_7(x))$ all of which can be represented by classes that are products of powers of cyclotomic units $1+x$ and $1+x+x^2$ modulo $\varphi_7(x)$. □

In relation to Corollary 5.4 it is natural to ask how many possible classes $b_{2p,p}$ modulo $(2, \varphi_p(x))$ are represented by units modulo $\varphi_p(x)$ or better yet what is the index of classes covered by units modulo $\varphi_p(x)$ in the subroup of invertible classes modulo $(2, \varphi_p(x))$? This index coincides with $M(n)$ for

these particular values of n. More generally, according to Proposition 5.1, the index $M(n)$ equals the index of all coordinate systems $\{b_{pq,p}, b_{pq,q}\}$ for which $b_{pq,p}$ is represented by a unit modulo $\varphi_p(x)$ and $b_{pq,q}$ is represented by a unit modulo $\varphi_q(x)$ in the set of all coordinate systems $\{b_{pq,p}, b_{pq,q}\}$.

Proposition 5.5. *$M(22) = 3, M(26) = 5, M(34) = 17, M(38) = 27$ and $M(15) = 2, M(21) = 4, M(33) = 44, M(35) = 90$.*

Proof. The claim can be established for $n = 22, 26, 34$ and 38 by using Corollary 5.4 and computing the number of classes modulo $(2, \varphi_p(x))$ that can be covered by units modulo $\varphi_p(x)$. For the remaining classes $n = 15, 21, 33$ and 35 we have to use Proposition 5.1. Also, in this case we used the generators for the n-th cyclotomic units from [2].

The computation of these values was done using the software package PARI with the help of my undergraduate student Anthony Disabella. □

Acknowledgement

The author would like to thank the referee for a valuable suggestion.

References

[1] L. BOUVIER, J. PAYAN *Modules sur certains anneaux de Dedekind*. J. Reine Angew. Math. **274/275** (1975), 278–286.

[2] R. KUČERA *On bases of the Stickelberger ideal and of the group of circular units of a cyclotomic field*. J. Number Theory **40** (1992), 284–316.

[3] F. MARKO *On the existence of p-units and Minkowski units in totally real cyclic fields*. Abh. Math. Sem. Univ. Hamburg **66** (1996), 89–111.

[4] N. MOSER *Unités et nombre de classes d'une extension Galoisienne diédrale de* $\mathbb{Q}$. Abh. Math. Sem. Univ. Hamburg **48** (1979), 54–75.

František MARKO
Pennsylvania State University
76 University Drive
Hazleton, PA 18202, USA
and
Mathematical Institute
Slovak Academy of Sciences
Štefánikova 49
814 38 Bratislava, Slovakia
E-mail : fxm13psu.edu