BULLETIN DE LA S. M. F.

DANIEL S. KUBERT

SERGE LANG

Modular units inside cyclotomic units

Bulletin de la S. M. F., tome 107 (1979), p. 161-178

<http://www.numdam.org/item?id=BSMF_1979__107__161_0>

Bull. Soc. math. France,
107, 1979, p. 161-178.

MODULAR UNITS INSIDE CYCLOTOMIC UNITS

BY

DANIEL S. KUBERT and SERGE LANG (*)

RÉSUMÉ. — On considère les unités de Siegel-Ramachandra-Robert dans le corps de classes de rayon p sur le corps quadratique imaginaire $\mathbf{Q}(\sqrt{-p})$. Les normes par rapport au corps cyclotomique $\mathbf{Q}(\mu_p)$ sont des unités. On démontre qu'elles sont contenues dans les unités cyclotomiques, et l'on donne une expression explicite des unes en fonction des autres. La démonstration se fait en écrivant les valeurs des séries L en $s = 1$, provenant d'une part de la formule limite de Kronecker, et d'autre part de l'expression usuelle pour les séries L de Dirichlet. On obtient ainsi suffisamment de relations pour résoudre les équations linéaires liant les logarithmes des unités modulaires et les logarithmes des unités cyclotomiques.

ABSTRACT. — We consider the Siegel-Ramachandra-Robert units in the ray class field of conductor p over the imaginary quadratic field $\mathbf{Q}(\sqrt{-p})$. The norms to the cyclotomic field $\mathbf{Q}(\mu_p)$ are units. We prove that they are contained in the cyclotomic units, and give explicit expressions of the former in terms of the latter. This is done by writing the values of L-series at $s = 1$, both from the Kronecker limit formula, and from the usual Drichlet L-series. Enough linear relations are obtained between the logs of the two kinds of units to solve for each in terms of the other.

In a series of papers, we have studied units in the modular function field, and in [KL 1] we already mentioned the possibility of investigating their specializations to number fields. On the other hand, SIEGEL [Si], RAMACHANDRA [Ra], and especially ROBERT [Ro] have investigated certain units in the complex multiplication case, obtained as values of certain theta functions.

In the present paper, we begin the special case of units in the cyclotomic fields of p-th roots of unity, p prime. For ease of exposition, we separate the results in two parts: $p \equiv 1 \bmod 4$ in this part, and $p \equiv -1 \bmod 4$

(*) Texte reçu le 16 mai 1978.
Supported by N.S.F. grants. KUBERT is also a Sloan Fellow.
Daniel S. KUBERT, Mathematics Department, Cornell University, Ithaca, N.Y. 14853 (U.S.A.), and Serge LANG, Mathematics Department, Yale University, New Haven, Conn. 06520 (U.S.A.).

in the next part. We show how the units obtained as values of modular functions (Siegel units) in the cyclotomic field can be expressed in terms of cyclotomic units, by means of an explicit formula. In particular, these modular units are contained in the cyclotomic units.

In paragraph 1, we give general facts and notation. In paragraph 2, we write down a system of linear relations relating the modular units and cyclotomic units by using the decomposition of appropriate L-series. In paragraph 3, we complete these relations for the trivial character. In paragraph 4, we solve for the modular units as power products of the cyclotomic units. This pattern is followed in both parts.

We let

$$K = \mathbf{Q}(\sqrt{-p}) \qquad \text{and} \qquad H = K(\mu_p).$$

We let $\mathfrak{p} = (\sqrt{-p})$ be the prime ideal in the ring of algebraic integers $\mathfrak{o}_K = \mathfrak{o}$. We let $K(1)$ be the Hilbert class field of K, and $K(\mathfrak{p})$ the ray class field of conductor $\mathfrak{p}$. This notation applies to both parts.

Part one : $p \equiv -1 \bmod 4$

1. General facts

We assume $p \equiv -1 \bmod 4$ and $p \geqslant 5$. Then $K \subset \mathbf{Q}(\mu_p) = H$. If $\alpha \in \mathfrak{o}$ and $\alpha \equiv 1 \bmod \mathfrak{p}$, then $\mathbf{N}\,\alpha \equiv 1 \bmod p$, so H is contained in the ray class field $K(\mathfrak{p})$.

THEOREM 1.1. — $K(1)\,\mathbf{Q}(\mu_p) = K(\mathfrak{p})$.

Proof. — Let $\mathfrak{a}$ be an ideal of K prime to $\mathfrak{p}$. It suffices to show that if $(\mathfrak{a}, K)$ fixes $\mathbf{Q}(\mu_p)$ and $K(1)$, then $(\mathfrak{a}, K)$ fixes $K(\mathfrak{p})$. Since $(\mathfrak{a}, K)$ fixes $K(1)$, it follows that $\mathfrak{a}$ is principal, $\mathfrak{a} = (\alpha)$. Since $(\mathfrak{a}, K)$ fixes H, it follows that $\alpha \equiv \pm 1 \bmod \mathfrak{p}$, so $\mathfrak{a}$ is in the unit class for $K(\mathfrak{p})$, as was to be shown.

We let $\mathrm{Cl}(H/K)$ be the ideal class group isomorphic to $\mathrm{Gal}(H/K)$ under the reciprocity law mapping

$$C \mapsto \sigma_C \quad \text{or} \quad \sigma(C).$$

Observe that all non-trivial characters of $\mathrm{Gal}(H/K) \approx \mathrm{Cl}(H/K)$ are primitive, with conductor $\mathfrak{p}$, because H is totally ramified over K at $\mathfrak{p}$.

The extensions H and $K(1)$ of K are linearly disjoint over K because H is totally ramified at $\mathfrak{p}$. Thre is a natural identification

$$\mathrm{Gal}(H/K) \approx \mathrm{Gal}(K(\mathfrak{p})/K(1))$$

from the diagram

$$\begin{tikzcd}[column sep=small]
 & K(\mathfrak{p}) = HK(1) \arrow[dl, dash] \arrow[dr, dash] & \\
H \arrow[dr, dash] & & K(1) \arrow[dl, dash] \\
 & K \arrow[d, dash] & \\
 & \mathbf{Q} &
\end{tikzcd}$$

Under the class field theoretic isomorphism between ideal class groups and Galois groups, we have a commutative diagram:

$$\begin{tikzcd}
\mathrm{Cl}(H/K) \arrow[r, leftrightarrow] \arrow[d, leftrightarrow] & \mathrm{Gal}(H/K) \subset \mathrm{Gal}(H/\mathbf{Q}) \arrow[d, leftrightarrow] \\
\mathfrak{o}(\mathfrak{p})^*/\pm 1 \arrow[r] & \mathbf{Z}(p)^{*2}
\end{tikzcd}$$

The arrow on top is the correspondence $C \mapsto \sigma_C$, arising from the above field diagram. The ideal classes of $\mathrm{Cl}(H/K)$ are precisely the principal ideal classes, modulo those generated by elements $\equiv 1 \bmod \mathfrak{p}$. This gives rise to the vertical arrow on the left.

The bottom arrow is induced by the norm map. Taking into account the natural isomorphism

$$\mathfrak{o}(\mathfrak{p}) \approx \mathbf{Z}(p),$$

the norm map amounts to the squaring map $x \mapsto x^2$.

The right vertical arrow arises from the usual correspondence between elements of $\mathbf{Z}(p)^*$ and $\mathrm{Gal}(H/\mathbf{Q})$:

$$a \mapsto \sigma_a, \qquad \text{with} \quad \sigma_a \zeta = \zeta^a.$$

The elements a corresponding to elements of $\mathrm{Gal}(H/K)$ are precisely the squares. Consequently an ideal class $C \in \mathrm{Cl}(H/K)$ corresponds uniquely to an element $a \in \mathbf{Z}(p)^{*2}$, and we shall write this correspondence as

$$C_a \leftrightarrow a.$$

Let χ be a non-trivial character of $\mathrm{Gal}(H/K)$. The induced character to $\mathrm{Gal}(H/\mathbf{Q})$ is the direct sum of two characters χ_1, χ_2, with one of them odd, the other even. Say χ_1 is odd. These are the two characters of $\mathrm{Gal}(H/\mathbf{Q})$ restricting to χ on $\mathrm{Gal}(H/K)$. If C contains a principal ideal (t), then

$$\chi(C) = \chi((t)) = \chi_1(t^2) = \chi_2(t^2).$$

2. Linear relations for $\chi \neq 1$

We shall apply the above considerations to the L-series. We note that

$$\chi_2 = \chi_1 \chi_K,$$

and χ_K is odd. By classical formulas pertaining to cyclotomic fields (*cf.* for instance [L 1]), we have:

L 1
$$L(1, \chi_1) = \frac{1}{p} \pi i S(\chi_1) B_{1, \bar{\chi}_1},$$

L 2
$$L(1, \chi_2) = -\frac{1}{p} S(\chi_2) \sum_{b \in \mathbf{Z}(p)^*} \bar{\chi}_2(b) \log |1-\zeta^b|.$$

As usual, $S(\psi)$ is the Gauss sum formed with a multiplicative character ψ on $\mathbf{Z}(p)^*$, and the additive character

$$x \mapsto e^{2\pi i x/p} = \zeta^x, \qquad \text{where} \quad \zeta = e^{2\pi i/p}.$$

We have the L-series decomposition (*cf.* [L 3], chapter XII, § 2):

L 3
$$L(\chi, H/K, s) = L(\chi_1, H/\mathbf{Q}, s) L(\chi_2, H/\mathbf{Q}, s),$$

and also

L 4
$$L(\chi, H/K, s) = L(\chi, K(\mathfrak{p})/K, s).$$

The values of the L-series over K at 1 are given in terms of the Siegel functions as follows.

Let $\mathfrak{k}(z, L)$ be the Klein form (*cf.* [KL 2] and [L 2], chapter XV). We define

$$g^{12p}(z, L) = \mathfrak{k}^{12p}(z, L) \Delta(L)^p.$$

Let $\mathrm{Cl}(\mathfrak{p})$ be the ray class group of conductor $\mathfrak{p}$. For $C' \in \mathrm{Cl}(\mathfrak{p})$, we define

$$g_{\mathfrak{p}}(C') = g^{12p}(1, \mathfrak{p}\mathfrak{c}^{-1}),$$

where $\mathfrak{c}$ is any ideal in C'. The value is independent of $\mathfrak{c}$. If $C \in \mathrm{Cl}(H/K)$, *we define*

$$g_H(C) = N_{K(\mathfrak{p})/H} \, g_{\mathfrak{p}}(C'),$$

for any C' lying above C under the canonical homomorphism

$$\mathrm{Cl}(\mathfrak{p}) \to \mathrm{Cl}(H/K).$$

These are the invariants defined by RAMACHANDRA and ROBERT [Ro], paragraphs 2.2 and 2.4 (ROBERT uses the letter φ where we use g). See lso the last section of [KL 1].

From the Kronecker limit formula one obtains the value of the L-series in **L 4** at $s = 1$, as in MEYER [Me], SIEGEL [Si].

$$\textbf{L 5} \quad L(\chi, H/K, 1) = \frac{-2\pi}{6\, p w_1(\mathfrak{p})\, S_K(\bar{\chi}) \sqrt{d_K}} \sum_{C \in \mathrm{Cl}(H/K)} \bar{\chi}(C) \log |g_H(C)|.$$

We have used the usual notation:

$w_1(\mathfrak{p})$ = number of roots of unity in K which are $\equiv 1 \bmod \mathfrak{p}$. Since we took $p \geqslant 5$, it follows that $w_1(\mathfrak{p}) = 1$;

$\mathbf{d}_K = p$ = absolute value of the discriminant of K;

$S_K(\chi)$ is the Gauss sum relative to K, that is

$$S_K(\chi) = \sum_{x \in \mathfrak{o}(\mathfrak{p})^*} \chi((x))\, e^{2\pi i \mathrm{Tr}(x)/p}.$$

For the proof see also [L 4] (chapter 22, § 2, Theorem 2). In the notation of that chapter, we take $\gamma = 1/p$, and $\mathfrak{d} = (\sqrt{-p})$, so $\mathfrak{d}\mathfrak{p} = (p)$. Furthermore, for any character χ we have

$$\chi(C) = \chi(\bar{C}).$$

Indeed, C contains principal ideals (t), and $t \equiv \bar{t} \bmod \mathfrak{p}$. Finally, as explained in the last section of [KL 1], we have

$$g_{\mathfrak{p}}(C) = \Phi_{\mathfrak{p}}(\bar{C}).$$

These remarks show how the formula in the above reference imply the formula as stated here.

From the values of the L-series at 1, and the factorization **L 3**, we find the following Lemma.

LEMMA 2.1. – *For a non-trivial character* χ *of* Gal $(H/K) \approx$ Cl (H/K):

$$\sum_C \bar{\chi}(C) \log |g_H(C)|$$
$$= 3i \frac{1}{\sqrt{p}} S(\chi_1) S(\chi_2) S_K(\bar{\chi}) B_{1,\bar{\chi}_1} \sum_{b \in \mathbf{Z}(p)^*} \bar{\chi}_2(b) \log |1 - \zeta^b|.$$

We note that

$$S_K(\bar{\chi}) = \sum_{z \in \mathbf{Z}(p)} \bar{\chi}_1^2(z)\, e^{2\pi i 2z/p}$$

and therefore

$$S_K(\bar{\chi}) = \chi_1^2(2)\, S(\bar{\chi}_1^2).$$

As a special case of the Davenport-Hasse relation (*cf.* for instance [L 1], Chapter 2, § 10), we have

$$S(\chi_1)\, S(\chi_2) = \bar{\chi}_1^2(2)\, S(\chi_1^2)\, S(\chi_K).$$

Furthermore, the sign of a Gauss sum is always positive (*cf.* for instance [L 3], chapter IV, § 3), and so we have

$$S(\chi_K) = i\sqrt{p}.$$

Therefore the linear relation becomes:

LEMMA 2.2

$$\sum_C \bar{\chi}(C) \log |g_H(C)| = -3\, p B_{1,\bar{\chi}_1} \sum_{b \in \mathbf{Z}(p)^*} \bar{\chi}_2(b) \log |1-\zeta^b|.$$

3. The relations for all characters

We now restate the linear relations, including the trivial character.

THEOREM 3.1. — *Let* χ *be any character of* $\mathrm{Cl}(H/K)$, *trivial or not. Then*

$$\sum_C \chi(C) \log |g_H(C)| = -3\, p B_{1,\chi_1} \sum_{b \in \mathbf{Z}(p)^*} \chi_2(b) \log |1-\zeta^b|.$$

If $\chi = 1$, *then* $\bar{\chi}_1 = \chi_1 = \chi_K$.

Proof. — The statement for non-trivial χ has been proved, so we suppose that χ is trivial. Then:

$$\sum_{C \in \mathrm{Cl}(H/K)} \log |g_H(C)|$$
$$= \sum_{C \in \mathrm{Cl}(\mathfrak{p})} \log |g_{\mathfrak{p}}(C)|$$
$$= \sum_{C \in \mathrm{Cl}(1)} \sum_{C' \subset C} \log |g_{\mathfrak{p}}(C')|$$

[where Cl (1) is the group of ordinary ideal classes]

$$= \sum_{C \in \mathrm{Cl}(1)} \frac{p}{2} \log \left| \frac{\Delta(\mathfrak{c}^{-1})}{\Delta(\mathfrak{p}\mathfrak{c}^{-1})} \right| \quad \text{by [Ro] (§ 2.3, Theorem 2 (iii))}$$

[where $\mathfrak{c}$ is any ideal in C], and since $\mathfrak{p} = (\sqrt{-p})$ is principal,

$$= \sum_{C \in \mathrm{Cl}(1)} 3\, p \log p$$
$$= h_K 3\, p \log p.$$

But the classical class number formula for K gives

$$h_K = w_K \left(-\frac{1}{2} B_{1,\chi_K} \right) = -B_{1,\chi_K}.$$

The Theorem follows from the obvious value for the sum

$$\sum_b \log |1-\zeta^b| = \log p.$$

4. Modular units as cyclotomic units

For any element u in K^* we consider the *regulator map* ρ given by

$$\rho(u) = \sum_C \log |u^{\sigma(C)}| \sigma_C^{-1}.$$

This map will be applied to p-units. Writing $C = C_a$ with $a \in \mathbf{Z}(p)^{*2}$, the above map can be viewed has having its values in the group algebra $\mathbf{C}[G]$, where

$$G = \mathrm{Gal}(H/K) \approx \mathbf{Z}(p)^{*2}.$$

We shall take $u = g_H(C_1)$, and take into account the fact that

$$g_H(C_1)^{\sigma(C)} = g_H(C).$$

We may write

$$\rho(g_H(C_1)) = \sum_C \log|g_H(C)|\,\sigma_C^{-1} = \sum_a \log|g_H(C_a)|\,\sigma_a^{-1}.$$

THEOREM 4.1. — *We have*

$$\rho(g_H(C_1)) = -12\,p \sum_a \sum_b \mathbf{B}_1\left(\left\langle\frac{b^{-1}a}{p}\right\rangle\right)\log|1-\zeta^b|\,\sigma_a^{-1}.$$

The sums on the right are taken over a, $b \in \mathbf{Z}(p)^{*2}$. In particular

$$\log|g_H(C_a)| = -12\,p \sum_b \mathbf{B}_1\left(\left\langle\frac{b^{-1}a}{p}\right\rangle\right)\log|1-\zeta^b|.$$

Proof. — Apply any character χ to $\rho(g_H(C_1))$. From paragraph 3 we find:

$$\sum_a \bar{\chi}(a)\log|g_H(C_a)| = -6\,p B_{1,\bar{\chi}_1} \sum_b \bar{\chi}_2(b)\log|1-\zeta^b|.$$

On the other hand applying χ to the right hand side of the formula to be proved, we find:

$$-12\,p \sum_b \sum_a \mathbf{B}_1\left(\left\langle\frac{b^{-1}a}{p}\right\rangle\right)\log|1-\zeta^b|\,\bar{\chi}_2(a)$$

$$= -12\,p \sum_b \sum_a \mathbf{B}_1\left(\left\langle\frac{a}{p}\right\rangle\right)\log|1-\zeta^b|\,\bar{\chi}_2(b)\bar{\chi}_2(a)$$

$$= -6\,p B_{1,\bar{\chi}_1} \sum_b \bar{\chi}_2(b)\log|1-\zeta^b|$$

because χ_1 and χ_2 have the same values on squares. Furthermore,

$$2\sum_a \mathbf{B}_1\left(\left\langle\frac{a}{p}\right\rangle\right)\bar{\chi}_1(a) = \sum_{t\in\mathbf{Z}(p)^*} B_1\left(\left\langle\frac{t}{p}\right\rangle\right)\bar{\chi}_1(t) = B_{1,\bar{\chi}_1},$$

because $\mathbf{B}_1$ is an odd function, and -1 is not a square mod p. This proves the Theorem.

We may now translate this result into a multiplicative notation. Let

$$\alpha = \prod_{b\in\mathbf{Z}(p)^{*2}} (1-\zeta^b)^{m(b^{-1}d)}/g_H(C_d).$$

We wish to prove that α is a root of unity. We know that $g_H(C_d)$ is a p-unit because it is obtained as a product of values of Siegel functions whose q-expansions (and those of their conjugates) are p-units in the integral closure of $\mathbf{Z}[j]$ in the modular function field. Furthermore, α has absolute value 1 at all archimedean absolute values by the above calculation. Therefore α must have absolute value 1 at $\mathfrak{p}$ by the product formula. Therefore α has absolute value 1.

Making the change of variables $a \mapsto d$ and $b^{-1} a \mapsto b$ in Theorem 4.1, we have proved the following.

THEOREM 4.2. — *For* $d \in \mathbf{Z}(p)^{*2}$ *we have*

$$g_H(C_d) = \varepsilon(d) \prod_{b \in \mathbf{Z}(p)^{*2}} (1 - \zeta^{b^{-1}d})^{m(b)},$$

where $\varepsilon(d)$ *is a root of unity, and*

$$m(b) = -12\, p\, \mathbf{B}_1\left(\left\langle \frac{b}{p} \right\rangle\right).$$

The notation is standard: we denote by $\mathbf{B}_1$ the first Bernoulli polynomial,

$$\mathbf{B}_1(X) = X - \frac{1}{2}.$$

For any real number r, we let $\langle r \rangle$ be the unique number satisfying

$$r \equiv \langle r \rangle \bmod \mathbf{Z} \quad \text{and} \quad 0 \leqslant \langle r \rangle < 1.$$

Remark. — If we write $\varepsilon(1) = \eta \varepsilon_0$ with $\varepsilon_0 = \pm 1$, and $\eta \in \mu_p$, then

$$\varepsilon(d) = \eta^d \varepsilon_0.$$

The numbers $g_H(C)$ are p-units, and their quotients

$$g_H(C)/g_H(C'),$$

are units (RAMACHANDRA and ROBERT). Let:

$\Phi_{p,H} = \Phi_p$ = group generated by all values $g_H(C)$ and μ_H;

$\Phi_H = \Phi$ = group generated all quotients $g_H(C)/g_H(C')$ and μ_H;

$\Phi_p(w_H)$ = group of p-units of the form;

$$\prod g_H(C)^{n(C)},$$

where the exponents $n(C)$ satisfy the condition

$$\sum_C n(C) \mathbf{N}\,\mathfrak{a}(C) \equiv 0 \bmod w_H,$$

where $\mathfrak{a}(C)$ is any ideal prime to w_H in the class C, and $w_H = 2p$ is the number of roots of unity in H. In the present case, we can write these units in the form

$$\prod_d g_H(C_d)^{n(d)} = \prod_d \varepsilon(d)^{n(d)} \prod_b (1 - \zeta^b)^{-12 p v(b)},$$

where

$$\sum n(d)\, d \equiv 0 \bmod p \qquad \text{and} \qquad \sum n(d) \equiv 0 \bmod 2.$$

The exponent $\nu(b)$ is given by the formula:

$$\nu(b) = \sum_d n(d)\,\mathbf{B}_1\left(\left\langle \frac{b^{-1}d}{p} \right\rangle\right) \in \mathbf{Z}.$$

Since $\varepsilon(d) = \eta^d \varepsilon_0$ (*cf.* remark above), we have

$$\prod_d \varepsilon(d)^{n(d)} = \varepsilon_0^{\sum n(d)} \eta^{\sum n(d)\, d} = 1,$$

so that

$$\prod_d g_H(C_d)^{n(d)} = \prod_b (1-\zeta^b)^{-12p\nu(b)}.$$

The root of unity factor has gone out.

Using similar notation, we let

$\Phi_H(w_H)$ = subgroup of Φ_H satisfying the above condition.

An element of $\Phi_{p,H}$ lies in Φ_H if, and only if, the exponents $n(C)$ satisfy

$$\sum_C n(C) = 0.$$

We have also given a proof in the present instance for Robert's result that the elements of $\Phi(w_H)$ (or $\Phi_p(w_H)$) are $12\,p$-th powers in H. As in ROBERT [Ro], this allows us to take $12\,p$-roots, and we define:

$E_{p,\mathrm{cyc}}$ = group generated by μ_H and by the cyclotomic p-units $\zeta^b - 1$, with $b \in \mathbf{Z}(p)^{*2}$;

$E_{p,\mathrm{mod}}$ = group generated by μ_H and all elements $\alpha \in H$ such that $\alpha^{12p} \in \Phi_p(w_H)$.

We define E_{cyc} and E_{mod} in a similar way, taking the elements of degree 0 to get units instead of p-units. We call the groups $E_{p,\mathrm{mod}}$ or E_{mod} the groups of *modular p-units* or *modular units* respectively. The latter could also be called the group of *Robert units.* For any element $\alpha \neq 0$ of H, we let

$$\rho(\alpha) = \sum_{\sigma \in G} \log|\sigma\alpha|\,\sigma^{-1},$$

where $G \approx \mathbf{Z}(p)^{*2}$ is the Galois group of H over K. Thus ρ is the usual ,'regulator'' map. Then

$$E_{p,\mathrm{cyc}}/E_{p,\mathrm{mod}} \approx \rho(E_{p,\mathrm{cyc}})/\rho(E_{p,\mathrm{mod}}).$$

Let $R = \mathbf{Z}[G]$, and let ξ be the element of $\mathbf{C}R$ given by

$$\xi = \sum_a \log|\zeta^a - 1|\,\sigma_a^{-1}.$$

Let the *Stickelberger element* be

$$\Theta = \sum_b \mathbf{B}_1\left(\left\langle \frac{b}{p} \right\rangle\right)\sigma_b^{-1}.$$

Let:

I_H = ideal of elements $\sum n(d)\,\sigma_d$, $n(d) \in \mathbf{Z}$, d prime to $2p$, satisfying the conditions

$$\sum n(d)\,d \equiv 0 \bmod p \qquad \text{and} \qquad \sum n(d) \equiv 0 \bmod 2.$$

$\mathcal{S}$ = *Stickelberger ideal* = $I_H\,\Theta \subset R$ because 2 divides w_H. Then

$$\rho(E_{p,\,\mathrm{cyc}}) = R\,\xi, \qquad \rho(\Phi_p) = 12\,p\,R\,\xi\Theta.$$
$$\rho(E_{p,\,\mathrm{mod}}) = \mathcal{S}\,\xi.$$

Consequently we obtain an isomorphism.

THEOREM 4.3. — $E_{p,\,\mathrm{cyc}}/E_{p,\,\mathrm{mod}} \approx R\,\xi/\mathcal{S}\,\xi \approx R\,\mathcal{S}$.

A similar isomorphism is obtained for $E_{\mathrm{cyc}}/E_{\mathrm{mod}}$ by considering the elements of degree 0.

Remark. — For the record, it may be useful to have the expression of the cyclotomic units as *rational* power products of the modular units. In Theorem 4.1, we apply a character $\bar{\chi}$, divide by $-6\,p\,B_{1,\,\chi_1}$, and sum over $\bar{\chi}$. We find:

$$\begin{aligned} -\frac{1}{6\,p}&\sum_C \log g_H(C) \sum_\chi \frac{1}{B_{1,\,\chi_1}}\,\chi(C) \\ &= \sum_{b \in (\mathbf{Z}(p)^*)^2} \log|1-\zeta^b| \sum_\chi \chi_2(b) \\ &= \frac{p-1}{2}\log|1-\zeta|. \end{aligned}$$

Therefore, we have the following Theorem.

THEOREM 4.4

$$\log|1-\zeta| = \frac{-1}{3\,p(p-1)}\sum_C m'(C)\log|g_H(C)|,$$

where

$$m'(C) = \sum_\chi \frac{1}{B_{1,\,\chi_1}}\,\chi(C).$$

In multiplicative notation, up to a root of unity, this yields

$$1-\zeta^a = \varepsilon'(a)\prod_C g_H(C)^{-\frac{1}{3\,p(p-1)}\,m'(C/C_a)}.$$

Part two: $p \equiv 1 \bmod 4$

1. General facts

As before, we have the following Theorem.

THEOREM 1.1. – $K(\mathfrak{p}) = K(1)\,\mathbf{Q}(\mu_p)$.

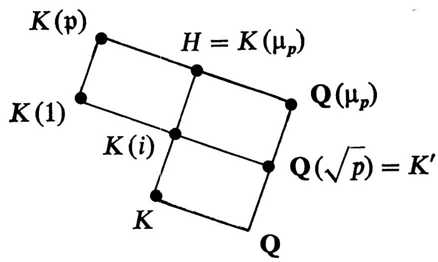
The proof is similar and can be omitted. We let $K' = \mathbf{Q}(\sqrt{p})$. We let

$$H = K(\mu_p) = \mathbf{Q}(\mu_{4p}).$$

Then

$$[H:K] = [K(\mu_p):K] = p-1,$$

so $\mathrm{Gal}(K(\mu_p)/K) \approx \mathbf{Z}(p)^*$ in a natural way. We have the following diagram of fields.



Note that $K(i)$ is unramified over K (because only 2 can ramify, and $K(i)$ is also obtained by adjoining $\sqrt{p}$ to K). Thus $K(i) = K(1) \cap K(\mu_p)$, and we denote

$$K(i) = H_1 = H \cap K(1).$$

We have a diagram similar to the other case.

$$\begin{array}{ccc} \mathrm{Cl}(H/H_1) & \overset{\approx}{\longleftrightarrow} & \mathrm{Gal}(H/H_1) \\ \updownarrow & & \updownarrow \\ (\mathfrak{o}/\mathfrak{p})^*/\pm 1 & \xrightarrow[\text{square}]{} & \mathbf{Z}(p)^{*2} \end{array}$$

Let χ be a character on $\mathrm{Gal}(H/K)$. We denote by $\chi_{\mathbf{Q}}$ the corresponding character on the isomorphic group $\mathrm{Gal}(\mathbf{Q}(\mu_p)/\mathbf{Q})$, and also view $\chi_{\mathbf{Q}}$ as a character on $\mathbf{Z}(p)^*$ under the usual isomorphism.

$$a \mapsto \sigma_a.$$

As before, for any class $C \in \mathrm{Cl}(H/K)$, we have

$$\chi(C) = \chi(\bar{C}),$$

because for any ideal $\mathfrak{c}$ in C,

$$\chi(C) = \chi_{\mathbf{Q}}(\mathrm{N}\,\mathfrak{c}) = \chi_{\mathbf{Q}}(\mathrm{N}\,\bar{\mathfrak{c}}) = \chi(\bar{C}).$$

Note that $\chi^2 \neq 1$ *if and only if conductor of* $\chi = \mathfrak{p}$.

There are three characters of order 2 on $\mathbf{Z}(4p)^*$, corresponding to the three subfields of degree 2 over $\mathbf{Q}$, namely

$$\chi_K, \quad \chi_{K'}, \quad \chi_{\mathbf{Q}(i)}, \quad \text{and we have} \quad \chi_{K'} = \chi_K \chi_{\mathbf{Q}(i)}.$$

2. Linear relation for $\chi^2 \neq 1$

We assume $\chi^2 \neq 1$. We apply the Kronecker limit formula as in [L 4], that is

$$L(\chi, H/K, 1) = -\frac{2\pi}{6p\,S_K(\bar{\chi})\sqrt{d_K}} \sum_C \bar{\chi}(C) \log |g_H(C)|.$$

In the notation of [L 4], $S_K(\bar{\chi}) = \bar{\chi}(\gamma\,\mathfrak{d}\mathfrak{p})\,T(\bar{\chi}, \gamma)$, where $\mathfrak{d} = (2\sqrt{-p})$, and we can take $\gamma = 1/2p$. Thus

$$S_K(\bar{\chi}) = S(\bar{\chi}_{\mathbf{Q}}^2).$$

Also, $d_K = 4p$. We use the decomposition

$$L(\chi, H/K, 1) = L(\chi_{\mathbf{Q}}, H/\mathbf{Q}, 1)\,L(\chi'_{\mathbf{Q}}, H/\mathbf{Q}, 1),$$

where $\chi'_{\mathbf{Q}}$ is the other character on $\mathbf{Z}(4p)^*$ restricting to χ. *A priori*, we do not know which of $\chi_{\mathbf{Q}}$ or $\chi'_{\mathbf{Q}}$ is even or odd, and we use again χ_1, χ_2 to denote the odd and even characters respectively equal to $\chi_{\mathbf{Q}}$ or $\chi'_{\mathbf{Q}}$. In the specific determination of the values of the L-series, we shall have to distinguish corresponding cases. We have

$$\chi'_{\mathbf{Q}} = \chi_{\mathbf{Q}} \chi_K = \chi_{\mathbf{Q}} \chi_{K'} \chi_{\mathbf{Q}(i)}.$$

We let m_2 = conductor of χ_2. Then

$$L(\chi, H/K, 1) = \frac{1}{i/p}\pi i\,S(\chi_1)\,B_{1,\bar{\chi}_1}\left(-\frac{1}{p}\right) S(\chi_2) \times \sum_{b \in \mathbf{Z}(m_2)^*} \bar{\chi}_2(b) \log |1 - \zeta^b|,$$

where $\zeta = ie^{2\pi i/p}$ (resp. $\zeta = {}^{2\pi i/p}$) according as $m_2 = 4p$ or $m_2 = p$. From this we get the following relation.

LEMMA 2.1

$$\sum_C \bar{\chi}(C) \log |g_H(C)| = \frac{3i}{2\sqrt{p}} S(\chi_{\mathbf{Q}})\,S(\chi'_{\mathbf{Q}})\,S(\bar{\chi}_{\mathbf{Q}}^2)\,B_{1,\bar{\chi}_1} \sum_{b \in \mathbf{Z}(m_2)^*} \bar{\chi}_2(b) \log |1 - \zeta^b|.$$

We now simplify the Gauss sums and their products.

LEMMA 2.2. – $S(\chi_{\mathbf{Q}})\,S(\chi'_{\mathbf{Q}}) = \bar{\chi}_{\mathbf{Q}}^2(2)\,S(\chi_{\mathbf{Q}}^2)\,S(\chi_K)$.

Proof. – This is a special case of the Davenport-Hasse distribution relation (*cf.* for instance [L 1], chapter 2, § 10).

In the present case, we have from the prime power decomposition (with respect to the primes p and 2),

$$S(\chi_K) = S(\chi_{K'})\,S(\chi_{\mathbf{Q}(i)}) = 2\,i\sqrt{p},$$

because the signe of the Gauss sum is always positive (*see* for instance [L 3], chapter IV, § 3). This yields:

LEMMA 2.3

$$\begin{aligned}&\textstyle\sum_C \bar{\chi}(C)\log|g_H(C)|\\ &\quad = -3\,p\,\bar{\chi}_{\mathbf{Q}}^2(2)\,B_{1,\bar{\chi}_1}\textstyle\sum_{b\in \mathbf{Z}(m_2)^*}\bar{\chi}_{\mathbf{Q}}(b)\log|1-\zeta^b|.\end{aligned}$$

We must then distinguish two cases.

Case 1: $\chi_{\mathbf{Q}} = \chi_2$. – The expression in Lemma 2.3 is then equal to

$$-3\,p\,\bar{\chi}_{\mathbf{Q}}^2(2)\,B_{1,\bar{\chi}_{\mathbf{Q}}\chi_K}\textstyle\sum_{b\in \mathbf{Z}(p)^*}\bar{\chi}_{\mathbf{Q}}(b)\log|1-\zeta^b|.$$

Case 2: $\chi_{\mathbf{Q}} = \chi_1$. – The expression in Lemma 2.3 is then equal to

$$\begin{aligned}&-3\,p\,\bar{\chi}_{\mathbf{Q}}^2(2)\,B_{1,\bar{\chi}_{\mathbf{Q}}}\textstyle\sum_{b\in \mathbf{Z}(4p)^*}\bar{\chi}_{\mathbf{Q}}\chi_K(b)\log|1-\zeta^b|\\ &= -3\,p\,\bar{\chi}_{\mathbf{Q}}^2(2)\,B_{1,\bar{\chi}_{\mathbf{Q}}}\Big[\textstyle\sum_{b\in \mathbf{Z}(4p)^*,\,b\equiv 1 \bmod 4}\bar{\chi}_{\mathbf{Q}}(b)\left(\dfrac{b}{p}\right)\log|1-\zeta_p^b\zeta_4|\\ &\qquad -\textstyle\sum_{b\in \mathbf{Z}(4p)^*,\,b\equiv -1 \bmod 4}\bar{\chi}_{\mathbf{Q}}(b)\left(\dfrac{b}{p}\right)\log|1-\zeta_p^b\zeta_4^{-1}|\Big],\end{aligned}$$

where (b/p) is the quadratic symbol, $\zeta_p = e^{2\pi i/p}$, $\zeta_4 = i$.

3. Linear relations for $\chi^2 = 1$

We distinguish two cases, depending on whether χ is trivial or not.

Case $\chi = 1$. – Then case 1 of Lemma 2.3 also holds here, that is

$$\textstyle\sum_C \log|g_H(C)| = 3\,p(\log p)\,h_K = -3\,p(\log p)\,B_{1,\chi_K}.$$

The proof is the same as in the case $p \equiv -1 \bmod 4$, we did not need any special property of p for this relation.

Case $\chi \neq 1$, so $\chi_{\mathbf{Q}} = \chi_{K'}$. – Then

$$\textstyle\sum_C \chi(C)\log|g_H(C)| = 0.$$

Proof. — As in the proof of the other case, we first write the sum as a sum over elements of $Cl(\mathfrak{p})$, and then as a sum

$$\sum_{c \in \mathrm{Cl}(1)} \chi(c) \log \left| \frac{\Delta(\mathfrak{c}^{-1})}{\Delta(\mathfrak{c}^{-1}\mathfrak{p})} \right| = 0,$$

because $\mathfrak{p}$ is principal, so we can use the homogeneity of the delta function, and end up with the sum of the non-trivial character over all elements of Cl (1), thus yielding 0.

4. Modular units as cyclotomic units

Let $\zeta_n = e^{2\pi i/n}$. We wish to give an expression for the modular units

$$g_H(C_1) = \varepsilon \prod_b (1-\zeta_p^b)^{m(b)} (1-\zeta_p^b \zeta_4)^{r'(b)} (1-\zeta_p^b \zeta_4^{-1})^{r''(b)},$$

where $m(b)$, $r'(b)$, $r''(b)$ are rational numbers, and the product is taken for $b \in \mathbf{Z}(p)^*$. Since

$$(1-\zeta_p^b \zeta_4)(1-\zeta_p^b \zeta_4^{-1}) = 1+\zeta_p^{2b} = \frac{1-\zeta_p^{4b}}{1-\zeta_p^{2b}},$$

we may assume that the expression has the form

$$g_H(C_1) = \varepsilon \prod_b (1-\zeta_p^b)^{m(b)} \left(\frac{1-\zeta_p^b \zeta_4}{1-\zeta_p^b \zeta_4^{-1}} \right)^{r(b)},$$

where ε is a root of unity, and

$b \mapsto m(b)$ is an even function,

$b \mapsto r(b)$ is an odd function.

THEOREM 4.1. — *There is an expression as above, with*

$$m(b) = -3p\left(\frac{b}{p}\right)\left[\mathbf{B}_1\left(\left\langle \frac{b^{-1}}{p} + \frac{1}{4} \right\rangle\right) - \mathbf{B}_1\left(\left\langle \frac{b^{-1}}{p} - \frac{1}{4} \right\rangle\right)\right],$$

$$r(b) = -3p\left(\frac{b}{p}\right)\mathbf{B}_1\left(\left\langle \frac{4^{-1}b^{-1}}{p} \right\rangle\right).$$

We have the regulator relation:

$$\sum_C \log |g_H(C)| \sigma_C^{-1}$$
$$= \sum_a \left[\sum_b m(ba^{-1}) \log |1-\zeta_p^b| + \left(\frac{a}{p}\right) r(ba^{-1}) \log \left| \frac{1-\zeta_p^b \zeta_4}{1-\zeta_p^b \zeta_4^{-1}} \right| \right] \sigma_a^{-1}.$$

If $\mathfrak{c}$ is an ideal in the class C, and $a = \mathbf{N}\,\mathfrak{c}$, we also put

$$C = C_a.$$

Then we may also write the above relation in the form:

$$\log|g_H(C_a)| = \sum_b m(ba^{-1})\log|1-\zeta_p^b| + \left(\frac{a}{p}\right) r(ba^{-1})\log\left|\frac{1-\zeta_p^b\zeta_4}{1-\zeta_p^b\zeta_4^{-1}}\right|.$$

Remark 1. – The expression in brackets [ ] in the definition of $m(b)$ is always $1/2$ or $-1/2$. The product is taken over all b in $\mathbf{Z}(p)^*$. Consequently combining the values for $m(b)$ and $m(-b)$, we see that the factor involving $m(b)$ already gives an integral representation in terms of the cyclotomic numbers $1-\zeta_p^b$. A similar remark applies to the factor involving $r(b)$. As before, considering the subgroup generated by the $g_H(C)$ satisfying the Robert congruence conditions on the exponents shows that elements of this subgroup have p-th roots in the cyclotomic units.

Remark 2. – The factor (a/p) in front of $r(ba^{-1})$ in the formula arises from the Galois action on the 4-th roots of unity.

Proof of Theorem 4.1. – We apply an arbitrary character $\chi_{\mathbf{Q}}$, to the expression on the right hand side (RHS) of the regulator relation to be proved, and verify that it gives the desired value from paragraphs 2 and 3

Suppose first that $\chi_{\mathbf{Q}}$ is even. The sum over the terms containing $r(ba^{-1})$ will be 0, because $a \mapsto \chi_{\mathbf{Q}}(a)$ is even, and

$$a \mapsto \left(\frac{a}{p}\right) r(ba^{-1}),$$

is odd. After a change of variables, we thus obtain

$$\begin{aligned}\chi_{\mathbf{Q}}(\mathrm{RHS}) &= \sum_a \sum_b \chi_{\mathbf{Q}}(a)\bar{\chi}_{\mathbf{Q}}(b)\, m(a)\log|1-\zeta_p^b| \\ &= \sum_a \chi_{\mathbf{Q}}(a)\, m(4a). \sum_b \bar{\chi}_{\mathbf{Q}}(4b)\log|1-\zeta_p^b| \\ &= S_a S_b, \text{ say.}\end{aligned}$$

Furthermore,

$$\begin{aligned}S_a &= \sum_a \bar{\chi}_{\mathbf{Q}}(a)\, m(4^{-1}a^{-1}) \\ &= \sum_a \bar{\chi}_{\mathbf{Q}}(a)\left(\frac{a}{p}\right)\left[\left\langle \frac{4^{-1}a}{p} + \frac{1}{4}\right\rangle - \left\langle \frac{4^{-1}a}{p} - \frac{1}{4}\right\rangle\right] \\ &= \sum_{t \in \mathbf{Z}(4p)^*,\, t \equiv 1 \bmod 4} \bar{\chi}_{\mathbf{Q}}(t)\left(\frac{t}{p}\right)\mathbf{B}_1\left(\left\langle \frac{4}{4p}\right\rangle\right) \\ &\quad - \sum_{t \in \mathbf{Z}(4p)^*,\, t \equiv -1 \bmod 4} \bar{\chi}_{\mathbf{Q}}(t)\left(\frac{t}{p}\right)\mathbf{B}_1\left(\left\langle \frac{t}{4p}\right\rangle\right).\end{aligned}$$

Note that

$$S_a = B_{1,\bar{\chi}_{\mathbf{Q}}\chi_K}^{(4p)} = \sum_t \bar{\chi}_{\mathbf{Q}}\chi_K(t)\,\mathbf{B}_1\left(\left\langle\frac{t}{4p}\right\rangle\right),$$

is the sum defining the Bernoulli-Leopoldt number at level $4p$ with respect to the character $\bar{\chi}_{\mathbf{Q}}\chi_K$.

If $\chi_{\mathbf{Q}} \neq \chi_{K'}$ then $\bar{\chi}_{\mathbf{Q}}\chi_K$ has conductor $4p$, and we get the desired value corresponding to Lemma 2.3.

If $\chi_{\mathbf{Q}} = \chi_{K'}$, then this Bernoulli number is 0 (corresponding to the value found in paragraph). Indeed, the standard reduction for computing Bernoulli numbers from one level to a lower level with one fewer prime factor introduces the factor

$$1-\bar{\chi}_{\mathbf{Q}}(p)\chi_K(p) = 0,$$

because $\chi_K\chi_{K'}(p) = \chi_{\mathbf{Q}(i)}(p) = 1$ (*cf.* for instance [L 1], the Lemma of chapter 2, § 8). This concludes the proof of the case when $\chi_{\mathbf{Q}}$ is even.

Suppose now that $\chi_{\mathbf{Q}}$ is odd, so $\chi_{\mathbf{Q}} = \chi_1$. Then

$$\chi_2 = \chi_1\chi_K,$$

and the conductor of χ_2 is $4p$. Then the term with m drops out, for parity reasons again and we get a sum with the terms containing $r(ba^{-1})$. For simplicity, abbreviate

$$Z(b) = \frac{1-\zeta_p^b\zeta_4}{1-\zeta_p^b\zeta_4^{-1}}.$$

Then we find:

$$\begin{aligned}\chi_{\mathbf{Q}}(\mathrm{RHS}) &= -3p\sum_b\sum_a\bar{\chi}_{\mathbf{Q}}(a)\left(\frac{a}{p}\right)\left(\frac{ba^{-1}}{p}\right)\mathbf{B}_1\left(\left\langle\frac{4^{-1}b^{-1}a}{p}\right\rangle\right)\log|Z(b)|\\ &= -3p\bar{\chi}_{\mathbf{Q}}(4)\,S_a\,S_b,\end{aligned}$$

where

$$S_a = \sum_a\bar{\chi}_{\mathbf{Q}}(a)\,\mathbf{B}_1\left(\left\langle\frac{a}{p}\right\rangle\right) = B_{1,\bar{\chi}_{\mathbf{Q}}}$$

$$S_b = \sum_b\bar{\chi}_{\mathbf{Q}}(b)\left(\frac{b}{p}\right)\log|Z(b)|.$$

It now suffices to verify that S_b is equal to the sum in brackets in case 2 of Lemma 2.3, namely we must show

$$S_b = \sum_{t\in\mathbf{Z}(4p)^*}\bar{\chi}_2(t)\log|1-\zeta^t|.$$

To do this, we decompose the right hand side, writing $\zeta = \zeta_p \zeta_4$, and sum over $b \in \mathbf{Z}(p)^*$ corresponding to values

$$t \equiv b \bmod p, \qquad t \equiv 1 \bmod 4$$

and also

$$t \equiv b \bmod p, \qquad t \equiv -1 \bmod 4.$$

The desired equality drops out.

As in the previous case, let

$$\alpha = \prod_b (1-\zeta_p^b)^{m(b)} Z(b)^{r(b)} / g_H(C_1).$$

We want to prove that α is a root of unity. By the above calculations, α has absolute value 1 at all archimedean absolutes values. Moreoever, α is a unit outside of primes deviding p in $\mathbf{Q}(\mu_{4p})$. We have

$$p = (\mathfrak{p}_1 \mathfrak{p}_2)^{(p-1)/2}.$$

We note that the valuation of the numerator of α at $\mathfrak{p}_1$ equals the valuation of the numerator at $\mathfrak{p}_2$ since the contributions come from elements of $\mathbf{Q}(\mu_p)$. The same is true of the denominator, as one can see from the distribution relations (ROBERT-RAMACHANDRA). Thus this is true for α, and then by the product formula, α must be a unit at $\mathfrak{p}_1$ and at $\mathfrak{p}_2$. Therefore α is a root of unity. This proves Theorem 4.1.

Remark. — In the present case, when H contains a non-trivial unramified extension of K, the group generated by the values $g_H(C)$ is not of finite index in the cyclotomic p-units. From ROBERT [Ro], we know that unramified units formed with the delta function must also be taken into account to get a full group of units. One can follow the same method to carry this out. This will be done elsewhere. *Cf.* KERSEY's thesis for a treatment of the general case, of an arbitrary imaginary quadratic field and nth roots of unity.

BIBLIOGRAPHY

[KL 1] KUBERT (D.) and LANG (S.). — Units in the modular function field, I, *Math. Annalen*, t. 218, 1975, p. 67-96.

[KL 2] KUBERT (D.) and LANG (S.). — Units in the modular function field, II: A full set of units, *Math. Annalen*, t. 218, 1975, p. 175-189.

[L 1] LANG (D.). — *Cyclotomic fields.* — Berlin, Springer-Verlag, 1978.

[L 2] LANG (S.). — *Introduction to modular forms.* — Berlin, Springer-Verlag, 1976 (*Grundlehren der mathematischen Wissenschaften*, 222).

[L 3] LANG (S.). — *Algebraic number theory.* — Reading, Addison-Wesley, 1970 (*Addison-Wesley Series in Mathematics*).

[L 4] LANG (S.). — *Elliptic functions*. — Reading, Addison-Wesley, 1973 (*Addison-Wesley Series in Mathematics*).

[Me] MEYER (C.). — *Die Berechnung der Klassenzahl Abelscher Körper über quadratischen Zahlkorpern*. — Berlin, Akademie-Verlag, 1957 (*Mathematische Lehrbücher und Monographien*, 2).

[Ra] RAMACHANDRA (K.). — Some applications of Kronecker's limit formula, *Annals of Math.*, Series 2, t. 80, 1964, p. 104-148.

[Ro] ROBERT (G.). — Unités elliptiques, *Bull. Soc. math. France*, Mémoire n° 36, 1973, 77 p.

[Si] SIEGEL (C. L.). — *Lectures on advanced analytic number*. — Bombay, Tata Institute of fundamental Research, 1961 (*Tata Institute, Lectures on Mathematics*, 23.