

THE PARITY OF THE CLASS NUMBER OF THE CYCLOTOMIC FIELDS OF PRIME CONDUCTOR

PIETRO CORNACCHIA

(Communicated by William W. Adams)

ABSTRACT. Using a duality result for cyclotomic units proved by G. Gras, we derive a relation between the vanishing of some χ -components of the ideal class groups of abelian fields of prime conductor (Theorem 1). As a consequence, we obtain a criterion for the parity of the class number of any abelian number field of prime conductor.

1. INTRODUCTION

The problem of the parity of the plus class numbers of cyclotomic fields has been studied before; for example in [1] it is proven that if n is an integer divisible by at least five different primes, then the order of the plus part of the ideal class group of the cyclotomic fields of the n -th roots of unity is even. When n is divisible by two, three or four primes, parity results are also given under additional assumptions. The case n prime seems to be more difficult, and the methods of [1] cannot be applied. In [14] this case is studied, and a parity criterion is given in terms of polynomials over the field with two elements.

We fix a prime number l and consider the cyclotomic field of the l -th roots of unity $\mathbf{Q}(\zeta_l)$; it has degree $l - 1$ over \mathbf{Q} . If $l - 1 = m2^e$ with m odd, we have $\text{Gal}(\mathbf{Q}(\zeta_l)/\mathbf{Q}) \cong \Delta \times P$ with Δ a cyclic group of order m , and P a cyclic 2-group of order 2^e . Let χ be a 2-adic character of Δ of order d . To simplify notations, we fix d , and denote by K_e the subfield of $\mathbf{Q}(\zeta_l)$ of degree $d2^e$ over \mathbf{Q} , and by K_0 the subfield of K_e of degree d over \mathbf{Q} .

$$\mathbf{Q} \subset K_0 \subset K_e \subset \mathbf{Q}(\zeta_l).$$

We denote by $\text{Cl}_e(\chi)$ and by $\text{Cl}_0(\chi)$ the χ -part of the 2-part of the ideal class groups of K_e and of K_0 (these will be defined precisely in the next section).

We prove the following:

Theorem 1. *The groups $\text{Cl}_0(\chi)$ and $\text{Cl}_0(\chi^{-1})$ are both trivial if and only if either $\text{Cl}_e(\chi)$ or $\text{Cl}_e(\chi^{-1})$ is trivial.*

We give a consequence of Theorem 1. The characters χ and χ^{-1} are conjugate under $\text{Gal}(\overline{\mathbf{Q}}_2/\mathbf{Q}_2)$ if and only if -1 is a power of 2 modulo d . In this case the χ and the χ^{-1} components of a Galois module coincide, and we have that $\text{Cl}_0(\chi)$ is trivial if and only if $\text{Cl}_e(\chi)$ is.

Received by the editors January 18, 1996 and, in revised form, May 17, 1996.

1991 *Mathematics Subject Classification.* Primary 11R29, 11R18; Secondary 11R27.

From Theorem 1 we also get a parity criterion for the class number of any abelian field of prime conductor l . In fact, every such field has degree $d2^j$ over \mathbf{Q} , with $d \mid m$ and $j \leq e$. Dropping the index d , we denote this field by K_j and its class group by Cl_j . The field K_e is totally imaginary. We denote by Cl^- the cokernel of the natural map $\text{Cl}_{e-1} \rightarrow \text{Cl}_e$. The map $\text{Cl}_{e-1} \rightarrow \text{Cl}_e$ is injective (see for example [10], Chapter 3, Theorem 4.2), and composed with the norm map $\text{Cl}_e \rightarrow \text{Cl}_{e-1}$ which is surjective, is multiplication by 2. From this it follows that $\text{Cl}_e(\chi)$ is trivial if and only if $\text{Cl}^-(\chi)$ is trivial. This last condition is equivalent, by the 2-adic class number formula proved in [7], to saying that $\frac{1}{2}B_{1,\chi^{-1}}$ is a 2-adic unit, where $B_{1,\chi^{-1}}$ is a Bernoulli number. If $j < e$, then K_j is totally real, and we have the following

Corollary 1. *The following are equivalent:*

1. *Either $\frac{1}{2}B_{1,\chi}$ or $\frac{1}{2}B_{1,\chi^{-1}}$ is a unit;*
2. *$\text{Cl}_0(\chi) \cong 0$ and $\text{Cl}_0(\chi^{-1}) \cong 0$;*
3. *$\text{Cl}_j(\chi) \cong 0$ and $\text{Cl}_j(\chi^{-1}) \cong 0$, for every $0 \leq j < e$.*

Proof (sketch). We have just seen that the first assertion is equivalent to saying that either $\text{Cl}_e(\chi)$ or $\text{Cl}_e(\chi^{-1})$ is trivial. Now we apply Theorem 1, and we get the equivalence of the first two assertions. The equivalence of the last two assertions can be proved using an argument similar to Lemma 1 and its corollary (it is enough to substitute e by j and Cl_0^∞ by Cl_0).

We present some examples which show that Theorem 1 is in some sense sharp.

1. $d = 3, 5$. In this case χ and χ^{-1} are conjugate; thus $\#\text{Cl}_0(\chi)$ is even if and only if $\#\text{Cl}^-(\chi)$ is even.
2. $d = 7$. In this case χ and χ^{-1} are not conjugate. For $l = 491$ we have that only one of $\text{Cl}_0(\chi)$ or $\text{Cl}_0(\chi^{-1})$ is nontrivial; for $l = 7841$ both are nontrivial.
3. $d = 15, l = 18121$. There are two nonequivalent characters of order 15: χ and χ^{-1} . We computed $\#\text{Cl}^-(\chi) = \#\text{Cl}^-(\chi^{-1}) = 2^4$. Then one of $\text{Cl}_0(\chi)$ or $\text{Cl}_0(\chi^{-1})$ is nontrivial. See [6], page 189.
4. $d = 31$. There are 6 nonequivalent characters. For $l = 311$ there are two characters χ_1 and χ_2 such that $\text{Cl}_1(\chi_i)$ is nontrivial ($i = 1, 2$), but χ_1 is not equivalent to χ_2^{-1} . In this case $\text{Cl}_0(\chi)$ is trivial for every χ of order 31.

In section 2 we introduce our notations, the characters and the definitions of χ -parts; in section 3 we prove a series of lemmas which lead to the proof of Theorem 1.

2. PRELIMINARIES

We recall some standard facts on Galois modules, and fix some notation. Let p be a fixed prime number and L an abelian number field of degree mp^e with $\gcd(p, m) = 1$. Let $G = \text{Gal}(L/\mathbf{Q})$.

We can decompose G as

$$G = \Delta \times P$$

where P is the p -part of G and $\gcd(\#\Delta, p) = 1$. Let χ be a p -adic character $\chi : \Delta \rightarrow \overline{\mathbf{Q}}_p^*$. We say that two such characters are equivalent when they are $\text{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$ -conjugates. The ring $\mathbf{Z}_p[\Delta]$ is a direct sum of discrete valuation rings:

$$\mathbf{Z}_p[\Delta] \cong \bigoplus_{\chi} O_{\chi}$$

where χ runs over the set of p -adic characters of Δ modulo equivalence and the rings O_{χ} are $\mathbf{Z}_p[\text{Im}(\chi)]$. Actually, each O_{χ} is a $\mathbf{Z}_p[\Delta]$ -algebra via the rule $\delta.x = \chi(\delta)x$,

for $x \in O_\chi$ and $\delta \in \Delta$. If M is a $\mathbf{Z}[G]$ -module and $\chi : \Delta \rightarrow \overline{\mathbf{Q}}_p^*$ a p -adic character, we can define its χ -component $M(\chi)$ as:

$$M(\chi) = O_\chi \otimes_{\mathbf{Z}_p[\Delta]} (\mathbf{Z}_p \otimes_{\mathbf{Z}} M).$$

We obtain thus a decomposition

$$M \otimes \mathbf{Z}_p \cong \oplus_\chi M(\chi).$$

We observe that each $M(\chi)$ is an $O_\chi[P]$ module.

Now we specialize to the case $p = 2$. We fix a prime number l , and consider the cyclotomic field $\mathbf{Q}(\zeta_l)$. We will deal with 2-adic characters χ of odd order d of the maximal subgroup Δ of $\text{Gal}[\mathbf{Q}(\zeta_l)/\mathbf{Q}]$ of odd order. Now that l, d and e are fixed, we denote by K_0 the subfield of $\mathbf{Q}(\zeta_l)$ of degree d over \mathbf{Q} , and by K_e the subfield of $\mathbf{Q}(\zeta_l)$ of degree $d2^e$. The field K_e is an extension of K_0 of degree 2^e , and it is the subfield of L fixed by $\ker(\chi)$. We denote by Cl_e and by Cl_0 the 2-part of the ideal class groups of K_e and of K_0 respectively. We denote by Cl_0^∞ the 2-part of the narrow ideal class group of K_0 .

We observe that the norm map identifies the χ -component of the 2-part of the ideal class group of $\mathbf{Q}(\zeta_l)$ with a direct summand of Cl_e .

Lemma 1. *Denote by σ a generator of the cyclic group $P = \text{Gal}(K_e/K_0)$. The norm map $\text{Cl}_e \rightarrow \text{Cl}_0^\infty$ induces an isomorphism of $\text{Gal}(K_e/\mathbf{Q})$ -modules $\text{Cl}_0^\infty \cong \text{Cl}_e/\text{Cl}_e^{1-\sigma}$.*

Proof. Since the extension K_e/K_0 is totally ramified at the prime above l , it follows from class field theory that the natural map of Galois modules $N : \text{Cl}_e \rightarrow \text{Cl}_0^\infty$ induced by the norms of ideals is surjective. The group $\text{Cl}_e^{1-\sigma}$ is clearly contained in the kernel. The extension K_e/K_0 is ramified at only one finite place. The Hasse norm principle gives us that a unit of K_0 is a norm of an element of K_e if and only if it is totally positive. Applying the genus theory formula (see for example [10], Chapter 13, Lemma 4.1), it follows easily that $\#\text{Cl}_e^P = \#\text{Cl}_0^\infty$. Since $\#\text{Cl}_0^\infty = \#\text{Cl}_e^P = \#(\text{Cl}_e/\text{Cl}_e^{1-\sigma})$, we see that N induces an isomorphism.

Corollary 2. *Under the hypotheses and notations of the previous theorem, if χ is any 2-adic character, then $\text{Cl}_e(\chi)$ is trivial if and only if $\text{Cl}_0^\infty(\chi)$ is.*

Proof. Since $\text{Cl}_e(\chi)$ and $\text{Cl}_0^\infty(\chi)$ are $O_\chi[P]$ modules, and $1 - \sigma$ is contained in the maximal ideal of this local ring, the result follows from Nakayama's lemma.

3. SIGNATURE OF UNITS AND PARITY OF CLASS NUMBERS

Now we will work with the field K_0 . Let E be the units of K_0 , and F the cyclotomic units, defined as the subgroup of E generated by $\{\pm 1\}$ and the norms of cyclotomic units of $\mathbf{Q}(\zeta_l)^+$.

Then we have (see [7])

$$(1) \quad \#(E/F)(\chi) = \#\text{Cl}_0(\chi).$$

Beware that in [7], as in [13], the cyclotomic units are norms of elements in $\mathbf{Q}(\zeta_l)$ rather than $\mathbf{Q}(\zeta_l)^+$. This gives an extra power 2^d in their formulas. Let R be $\mathbf{Z}/2[\text{Gal}(K_0/\mathbf{Q})]$; the ring R is a semisimple ring.

Lemma 2. *The groups $F/F^2(\chi)$ and $E/E^2(\chi)$ are one dimensional vector spaces over the field $O_\chi/2O_\chi$.*

Proof. The group F of cyclotomic units is a cyclic Galois submodule of E of finite index and containing -1 . Hence F/F^2 is isomorphic to the semisimple ring R : it is isomorphic to a direct sum of the simple modules $\mathbf{Z}_2[\text{Im}(\chi)]/2$, where χ runs over all 2-adic characters of $\text{Gal}(K_0/\mathbf{Q})$ modulo equivalence. In particular $F/F^2(\chi)$ is a one dimensional vector space on $O_\chi/2O_\chi$. We consider the diagram with exact rows:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & F & \longrightarrow & E & \longrightarrow & D & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & F & \longrightarrow & E & \longrightarrow & D & \longrightarrow & 0 \end{array}$$

where D is the finite quotient E/F and the vertical arrows are squarings. We apply the snake lemma and obtain an exact sequence:

$$0 \rightarrow \{\pm 1\} \rightarrow \{\pm 1\} \rightarrow D[2] \rightarrow F/F^2 \rightarrow E/E^2 \rightarrow D/D^2 \rightarrow 0.$$

We take the χ -parts, for some character χ . If χ is not trivial, we have $D[2](\chi) \cong D/D^2(\chi)$ as follows from the structure theorem of finite torsion modules over the principal ideal domain O_χ . We get $F/F^2(\chi) \cong E/E^2(\chi)$. If χ is the trivial character, we still have equality of the χ -components. This concludes the proof.

We denote by E_+ the units of K_0 which are totally positive and by F_+ the cyclotomic units which are totally positive.

Lemma 3. *There is an exact sequence*

$$0 \rightarrow (E_+/E^2) \rightarrow \text{Cl}_0^\infty \rightarrow \text{Cl}_0 \rightarrow 0.$$

Proof. We need to introduce some notation. Let K_+^* denote the set of totally positive elements of K_0^* . Let P and P_+ be the principal fractional ideals of the ring of integers of K_0 and the principal fractional ideals generated by a totally positive element respectively.

We have the following diagram of two exact sequences:

$$\begin{array}{ccccccc} & & & & 0 & & \\ & & & & \downarrow & & \\ 0 & \rightarrow & E_+/E^2 & \rightarrow & E/E^2 & \rightarrow & E/E_+ & \rightarrow & 0 \\ & & & & \downarrow & & K_0^*/K_+^* & & \\ & & & & \downarrow & & P/P_+ & & \\ & & & & \downarrow & & 0 & & \end{array}$$

We observe that K_0^*/K_+^* is a one dimensional free R -module, generated by an element $a \in K_0^*$ which is negative at one real valuation and positive at the remaining ones. In particular $K_0^*/K_+^*(\chi)$ is a one dimensional vector space over $O_\chi/2O_\chi$. Taking χ -parts in the above diagram, we get a diagram of $O_\chi/2O_\chi$ vector spaces, and we obtain $E_+/E^2(\chi) \cong P/P_+(\chi)$ for every χ . Therefore $P/P_+ \cong E_+/E^2$ and the result follows from the exact sequence

$$0 \rightarrow P/P_+ \rightarrow \text{Cl}_0^\infty(K) \rightarrow \text{Cl}_0 \rightarrow 0.$$

Theorem 2. $\text{Cl}_e(\chi)$ is trivial if and only if $F_+/F^2(\chi)$ is trivial.

Proof. Suppose $F_+/F^2(\chi)$ is trivial. Then so is $(E^2 \cap F)/F^2(\chi)$. Taking the χ -part of the exact sequence

$$(2) \quad 0 \rightarrow (E^2 \cap F)/F^2 \rightarrow F/F^2 \rightarrow E/E^2 \rightarrow (E/F) \otimes \mathbf{Z}/2 \rightarrow 0$$

and using Lemma 2, we get $E(\chi) \cong F(\chi)$. The following are equivalent:

1. $(F_+/F^2)(\chi) \cong 0$;
2. $(F_+/F^2)(\chi) \cong 0$ and $E(\chi) \cong F(\chi)$;
3. $(E_+/E^2)(\chi) \cong 0$ and $E(\chi) \cong F(\chi)$;
4. $(E_+/E^2)(\chi) \cong 0$ and $\text{Cl}_0(\chi) \cong 0$ by equation (1);
5. $\text{Cl}_0^\infty(\chi) \cong 0$, by Lemma 3;
6. $\text{Cl}_e(\chi) \cong 0$, by Corollary 2.

This concludes the proof.

We introduce some new notation. Let E_0 and F_0 be the subgroups of the elements of E (F respectively) whose square roots give an extension of K_0 which is unramified over 2.

Another important ingredient is G. Gras's theorem (cf. [6]):

Theorem 3 (G. Gras). *For every 2-adic character χ we have an isomorphism of abelian groups $F_0/F^2(\chi) \cong F_+/F^2(\chi^{-1})$. Besides, Cl_0 has even order if and only if $(F_0/F^2) \cap (F_+/F^2)$ is nontrivial.*

Proof of Theorem 1. Suppose $\text{Cl}_0(\chi)$ and $\text{Cl}_0(\chi^{-1})$ are both trivial. Then $E(\chi) \cong F(\chi)$ and $E(\chi^{-1}) \cong F(\chi^{-1})$ by equation (1). So we can apply Gras's theorem to E rather than to F . The ring $E(\chi)$ is a free rank one O_χ -module. We have the following inclusions:

$$E^2(\chi) \subset E_+(\chi), \quad E_0(\chi) \subset E(\chi)$$

and each one of $E_+(\chi)$ and $E_0(\chi)$ must be equal to $E^2(\chi)$ or to $E(\chi)$. Suppose $E_+(\chi) \cong E_0(\chi) \cong E(\chi)$. Then the group $E/E^2(\chi)$ generates a nontrivial Kummer extension of K_0 which is abelian and unramified over K_0 . This corresponds, via Kummer duality and class field theory, to a nontrivial quotient of $\text{Cl}_0(\chi^{-1})$, contrary to our assumption. So either $E_+(\chi) \cong E^2(\chi)$, or $E_0(\chi) \cong E^2(\chi)$. In the first case Lemma 3 and the hypothesis give $\text{Cl}_0^\infty(\chi) \cong 0$; hence $\text{Cl}_e(\chi) \cong 0$. In the second case, by Gras's theorem we get $E_+(\chi^{-1}) \cong E^2(\chi^{-1})$ and as above we conclude $\text{Cl}_e(\chi^{-1}) \cong 0$.

Now suppose $\text{Cl}_e(\chi) \cong 0$. By Theorem 2 we know that $(F_+/F^2)(\chi) \cong 0$. Gras's theorem implies $(F_0/F^2)(\chi^{-1}) \cong 0$. Thus we have that $(E^2 \cap F)/F^2(\chi)$ and $(E^2 \cap F)/F^2(\chi^{-1})$ are trivial. Using lemma 2 and sequence (2) we get that $(E/F)(\chi)$ and $(E/F)(\chi^{-1})$ are trivial; hence $\text{Cl}_0(\chi)$ and $\text{Cl}_0(\chi^{-1})$ are trivial as well. This completes the proof of the theorem.

ACKNOWLEDGEMENTS

The author wishes to thank René Schoof for his suggestions and advices and the Ohio State University where this research was done, for its hospitality.

REFERENCES

- [1] G. Cornell and M. I. Rosen, *The l -rank of the real class group of cyclotomic fields*, *Compositio Math.* **53** (1984), 133–141 MR **86d**:11090
- [2] A. Garbanati, *Unit signatures, and even class numbers, and relative class numbers*, *Journal für die reine und angewandte Mathematik* **274/275** (1975), 376–384

- [3] A. Garbanati, *Units with norm -1 and signatures of units*, Journal für die reine und angewandte Mathematik **283/284** (1976), 164–75
- [4] G. Gras and M.-N. Gras, *Signatures des unités cyclotomiques et parité du nombre de classes des extensions cycliques de \mathbf{Q} de degré premier impair*, Ann. Inst. Fourier, Grenoble, **25**, 1 (1975), 1–22 MR **52**:13728
- [5] G. Gras, *Parité du nombre de classes et unités cyclotomiques*, Astérisque **24-25** (1975), 37–45 MR **52**:3109
- [6] G. Gras, *Critère de parité du nombre de classes des extensions abéliennes réelles de \mathbf{Q} de degré impair*, Bull. Soc. Math. France, **103** (1975), 177–190 MR **52**:8081
- [7] C. Greither, *Class groups of abelian fields, and the main conjecture*, Ann. Inst. Fourier, Grenoble **42**, 3 (1992), 449–499 MR **93j**:11071
- [8] I. Hughes and R. Mollin, *Totally positive units and squares*, Proc. of the A.M.S., **87**, 4 (1983), 613–616 MR **84d**:12006
- [9] F. Keqin, *An elementary criterion on parity of class number of cyclic number field*, Scientia Sinica (Series A), Vol. **XXV** (1982), 1032–1041
- [10] S. Lang, *Cyclotomic fields I and II*, combined 2nd edition, Graduate Texts in Math. **121**, Springer Verlag, New York 1990 MR **91c**:11001
- [11] R. Schoof, *The structure of the minus class groups of abelian number fields*, Séminaire de Théorie des Nombres, Paris 1988–89, 185–204 MR **92e**:11126
- [12] R. Schoof, *Minus class groups of the fields of the l -th roots of unity*, to appear in Math. of Comp.
- [13] W. Sinnott, *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. **62** (1980), 181–234 MR **82i**:12004
- [14] P. Stevenhagen, *Class number parity for the p -th cyclotomic fields*, Mathematics of Comp., Vol. **63**, (1994), 773–784 MR **95a**:11099
- [15] L.C. Washington, *Introduction to cyclotomic fields*, Graduate Texts in Math. **83**, Springer Verlag, New York 1982 MR **85g**:11001

DIPARTIMENTO DI MATEMATICA, UNIVERSITÀ DI PISA, VIA BUONARROTI 2, 56127 PISA, ITALY
E-mail address: `cornac@gauss.dm.unipi.it`