On class number formulae for real abelian fields

L.V. Kuz'min

Russian Research Center "Kurchatov Institute"
Institute of Information Technologies
Moscow 123182
RUSSIA

Arbeitsgruppe "Algebraische Geometrie und Zahlentheorie"
an der Humboldt Universität Berlin
Jägerstr. 10/11
D-10117 Berlin
GERMANY

Max-Planck-Institut
für Mathematik
Gottfried-Claren-Str. 26

D-53225 Bonn

Germany

MPI / 94-139

On class number formulae for real abelian fields

L.V. Kuz'min

November 30, 1994

Introduction

Let k be a real abelian field with class group $\mathrm{Cl}(k)$ and class number $h(k)$. If k is of the type $k = \mathbf{Q}(\varepsilon_\ell + \varepsilon_\ell^{-1})$, i.e. k is the maximal real subfield of the cyclotomic field $\mathbf{Q}(\varepsilon_\ell)$, where ε_ℓ is a primitive ℓ-th root of unity, then already Kummer proved that $h(k)$ is equal to the index of the subgroup of circular units $C(k)$ in the full group of units $U(k)$.

This result was generalized by a number of authors to various other types of real abelian fields and various types of circular units (see references in [13]). The most outstanding results in this subject are those of Sinnott. In [12] he proved that if k is the maximal real subfield of some cyclotomic field $\mathbf{Q}(\varepsilon_m)$, i.e. $k = \mathbf{Q}(\varepsilon_m + \varepsilon_m^{-1})$, then the equality

$$[U(k) : C(k)] = 2^b h(k) \tag{0.1}$$

holds true. Here $C(k)$ is the group of circular units in the sense of Sinnott (we reproduce his definition below in this section) and b is a nonnegative integer depending only on the number g of different prime divisors of m. To be precise,

$$b = 0 \text{ if } g = 1 \text{ and } b = 2^{g-2} - g + 1 \text{ if } g > 1. \tag{0.2}$$

Sinnott also gave the formula

$$[U(k) : C(k)] = c_k^+ h(k) \tag{0.3}$$

which holds for any real abelian field [13]. In this case the group of circular units $C(k)$ and the additional factor c_k^+ are defined in a more complicated fashion. Sinnott proved his formulae (0.1), (0.3) by exploiting the analytic class number formula. So his proofs can tell us nothing about the connection between two abelian groups $U(k)/C(k)$ and $\mathrm{Cl}(k)$ even in the case when these groups have the same order. The only thing that is well known is that these groups may be not isomorphic in general. For example, if k is a real quadratic field, then $U(k)/C(k)$ is always cyclic, while $\mathrm{Cl}(k)$ is not cyclic in general. Nevertheless, G.Gras [1] conjectured that for any real abelian k and a prime number ℓ such that ℓ is relatively prime to the degree $[k:\mathbf{Q}]$ the ℓ-components of $\mathrm{Cl}(k)$ and $U(k)/C(k)$ have isomorphic Jordan-Hölder series. This conjecture was first proved in [14]. It should be noted that recently Kolyvagin [11] gave a relatively simple proof of this conjecture for the case $k = \mathbf{Q}(\varepsilon_\ell + \varepsilon_\ell^{-1})$.

Our goal in this paper is to get a better understanding of the connection between $\mathrm{Cl}(k)$ and $U(k)/C(k)$ for any real abelian field k. In particular, we obtained a refinement of Sinnott's formulae (0.1), (0.3). To explain our main results, first note that we may treat "ℓ-parts" of (0.1) and (0.3) for an arbitrary but fixed prime ℓ. For example, (0.1) is equivalent to the assertion that for any prime ℓ the ℓ-components $(U(k)/C(k))_\ell$ and $\mathrm{Cl}(k)_\ell$ have the same order (with additional factor 2^b for $\ell = 2$). Our methods are of purely ℓ-adic nature. So in what follows we shall assume that all fields are subfields of a fixed algebraic closure $\overline{\mathbf{Q}_\ell}$ of the rational ℓ-adic numbers $\mathbf{Q}_\ell$ and all characters take their values in $\overline{\mathbf{Q}_\ell}$. Let $G = G(k/\mathbf{Q})$ and $G = G_\ell \times G_0$, where G_ℓ is the ℓ-Sylow subgroup of G and the order of G_0 is relatively prime to ℓ. Let φ be any $\mathbf{Q}_\ell$-irreducible character of G_0. Then for any $\mathbf{Z}_\ell[G]$-module A we have the decomposition $A = \bigoplus_{\varphi\in\Phi} A_\varphi$, where φ runs through the set Φ of all $\mathbf{Q}_\ell$-irreducible characters of G_0 and A_φ equals to $e_\varphi A$, where e_φ is the idempotent corresponding to φ. By φ_0 we denote the trivial character of G_0. For any finitely generated abelian group B we denote by $B[\ell]$ the pro-ℓ-completion of B. Then we prove the following.

Theorem 1 *Let k be the maximal real subfield of some cyclotomic field $\mathbf{Q}(\varepsilon_m)$. Then for any prime ℓ and any $\varphi \in \Phi$ we have*

$$[U(k)[\ell]_\varphi : C(k)[\ell]_\varphi] = \lambda |\mathrm{Cl}(k)_{\ell,\varphi}|, \qquad (0.4)$$

where

$$\lambda = \begin{cases} 1 & \text{if } \ell \neq 2 \\ 1 & \text{if } \ell = 2 \text{ and } \varphi \neq \varphi_0 \\ 2^b & \text{if } \ell = 2 \text{ and } \varphi = \varphi_0 \end{cases}$$

and b is given by (2).

Theorem 2 *Let k be any real abelian field. Then for any prime ℓ and any $\varphi \in \Phi$ we have*

$$[U(k)[\ell]_\varphi : C(k)[\ell]_\varphi] = c^+_{k,\varphi}|\mathrm{Cl}(k)_{\ell,\varphi}| \tag{0.5}$$

for some rational $c^+_{k,\varphi}$, where the definition of $c^+_{k,\varphi}$ does not depend explicitly on the arithmetic of k.

It will be shown later that the constant $c^+_{k,\varphi}$ is, in a natural sense, the φ-part of Sinnott's constant c^+_k. So we can consider (0.4) and (0.5) as a refinement of (0.1) and (0.3). Note that the Gras conjecture is equivalent to the assertion that for $G = G_0$ we have an equality

$$|U(k)[\ell]_\varphi : C(k)[\ell]_\varphi] = |\mathrm{Cl}(k)_{\ell,\varphi}|.$$

So we can consider Theorem 1 and Theorem 2 as a generalization of the Gras conjecture.

It turns out that Iwasawa theory gives a succesful approach to these theorems and some related results. This theory deals with the cyclotomic $\mathbf{Z}_\ell$-extension $k_\infty = \bigcup_{n=0}^{\infty} k_n$, $[k_n : k] = \ell^n$, of a given field $k = k_0$, where ℓ is a fixed prime number. For any such extension we have the Tate module (the Iwasawa module) $T_\ell(k_\infty)$ that can be defined as $\varprojlim \mathrm{Cl}(k_n)_{S,\ell}$. Here $\mathrm{Cl}(k_n)$ is the class group of k_n, $\mathrm{Cl}(k_n)_S$ is the quotien of $\mathrm{Cl}(k_n)$ by the subgroup generated by all the prime divisors $v \in S$, where S is the set of all the places over ℓ, a subscript ℓ means passing to ℓ-component and the limit is taken with respect to the norm maps. Global class field theory enables us to interpret $T_\ell(k_\infty)$ as a Galois group of the maximal abelian unramified ℓ-extension M_∞ of k_∞ such that all the places over ℓ decompose completely in M_∞/k_∞. The Galois group $T_\ell(k_\infty) = G(M_\infty/k_\infty)$ is an abelian pro-ℓ-group and a Γ-module for $\Gamma = G(k_\infty/k) \cong \mathbf{Z}_\ell$. Let us consider the group $T_\ell(k_\infty)_{(0)} = T_\ell(k_\infty)/(\gamma - 1)$, where γ is a fixed topological generator of Γ. The group $T_\ell(k_\infty)_{(0)}$ can be interpreted as the Galois group $G(M^0_\infty/k_\infty)$, where

M_∞^0 is the maximal subfield of M_∞ abelian over k. It is well known that the Leopoldt conjecture holds true for any real abelian field. So $T_\ell(k_\infty)_{(0)}$ is a finite abelian ℓ-group.

Our first principal result is an index formula that gives the order of $T_\ell(k_\infty)_{(0)}$ and $T_\ell(k_\infty)_{(0),\varphi}$ for any $\varphi \in \Phi$.

Theorem 3 *For any real abelian k and any $\varphi \in \Phi$ we have*

$$|T_\ell(k_\infty)_{(0)}| = [\widehat{U}_S(k) : C_S(k)], \tag{0.6}$$

$$|T_\ell(k_\infty)_{(0),\varphi}| = [\widehat{U}_S(k)_\varphi : C_S(k)_\varphi], \tag{0.7}$$

Here $\widehat{U}_S(k)$ is some modified group of units and $C_S(k)$ some modified group of circular units defined below.

Note that there are no additional factors at all in Theorem 3. We shall prove Theorem 3 via Iwasawa theory and then deduce Theorem 1 and Theorem 2 from Theorem 3.

Now we give the definitions of $\widehat{U}_S(k)$ and $C_S(k)$ and then we describe our method and the content of the paper in some more detail pointing out the most important results.

For any field k let k^* be the multiplicative group of k, $\mu(k)$ the group of all roots of unity in k and $\mu_\ell(k)$ the ℓ-component of $\mu(k)$. If k is an algebraic number field and k_v means a v-completion of k with respect to a place $v \mid \ell$, then we put $\mathcal{B}(k_v) := (k^*/\mu(k))[\ell]$ and $\mathcal{B}(k) := \prod_{v \mid \ell} \mathcal{B}(k_v)$. If $k_{\infty,v}$ is the cyclotomic $\mathbf{Z}_\ell$-extension of k_v, then we define $H(k_v)$ to be the subgroup of all universal norms in $\mathcal{B}(k_v)$ with respect to the extension $k_{\infty,v}/k_v$, i.e. $H(k_v) = \bigcap_{n=1}^{\infty} N_{k_{n,v}/k_v}\mathcal{B}(k_{n,v})$. Put $H(k) := \prod_{v \mid \ell} H(k_v)$. It follows from the local class field theory that $H(k_v)$ (resp. $H(k)$) is a free $\mathbf{Z}_\ell$-module of rank $[k_v : \mathbf{Q}_\ell]$ (resp. $[k : \mathbf{Q}]$).

For an abelian number field k let $U_S(k)$ be the group of S-units of k, where S is as above. Put $\overline{U}_S(k) = U_S(k)/\mu(k)$, $\overline{U}(k) = U(k)/\mu(k)$. As the Leopoldt conjecture is valid in k, the natural mapping $\overline{U}_S(k)[\ell] \to \mathcal{B}(k)$ is injective, so we may consider $\overline{U}_S(k)[\ell]$ as a subgroup of $\mathcal{B}(k)$. Put

$$\widehat{U}_S(k) := \overline{U}_S(k)[\ell] \cap H(k).$$

We may say that $\widehat{U}_S(k)$ is the subgroup of $\overline{U}_S(k)[\ell]$ consisting of the local universal norms from k_∞.

To define the group $C_S(k)$ of circular S-units for abelian number field k, we note that k is a subfield of some cyclotomic field $K = \mathbf{Q}(\varepsilon_m)$. We may assume that K contains a primitive ℓ-th root of unity (K contains $\sqrt{-1}$ if $\ell = 2$). Then any intermediate subfield K_n of the cyclotomic $\mathbf{Z}_\ell$-extension K_∞/K is cyclotomic itself.

Let $P(K_n)$ be Sinnott's group of cyclotomic numbers [12], i.e. $P(K_n)$ is the subgroup of K_n^* generated by all the numbers of the form $1-\varepsilon$, $\varepsilon \in \mu(K_n)$, $\varepsilon \neq 1$. Then Sinnott defines the circular units of K_n as $C(K_n) := P(K_n) \cap U(K_n)$, where $U(K_n)$ are the units of K_n. Put

$$C(K_\infty) := \varprojlim((C(K_n)/\mu(K_n)[\ell]), \ \ \overline{U}_S(K_\infty) := \varprojlim(\overline{U}_S(K_n)[\ell])$$

and

$$\overline{U}_S(k_\infty) := \varprojlim(\overline{U}_S(k_n)[\ell])$$

where all limits are taken with respect to the norm maps. We will consider $C(K_\infty)$ as subgroups of the group $H(K_\infty) := \varprojlim \mathcal{B}(K_n) = \varprojlim H(K_n)$. We define the groups $\overline{U}_S(k_\infty)$ and $H(k_\infty)$ in the same way. The natural inclusion $k_\infty \subset K_\infty$ implies the inclusions $H(k_\infty) \subset H(K_\infty)$, $\overline{U}_S(k_\infty) \subset \overline{U}_S(K_\infty)$. Put

$$\widetilde{C}(k_\infty) := C(K_\infty)^H, \ \ \widetilde{H}(k_\infty) := H(K_\infty)^H.$$

We put

$$\widetilde{C}_S(k_\infty) := \{x \in \widetilde{H}(k_\infty) \mid (\gamma_n - 1)x \in \widetilde{C}(k_\infty) \text{ for some natural } n\},$$

where $\gamma_n = \gamma^{\ell^n}$, and

$$C_S(k_\infty) = \widetilde{C}_S(k_\infty) \cap \overline{U}_S(k_\infty).$$

We have a natural projection

$$\pi : \overline{U}_S(k_\infty) \longrightarrow \overline{U}_S(k)[\ell], \tag{0.8}$$

and it is evident that $\operatorname{Im} \pi \subset \widehat{U}_S(k)$. We define the S-circular units of k by

$$C_S(k) := \pi(C_S(k_\infty)) \subset \widehat{U}_S(k).$$

Note that all these groups are Galois modules, moreover, the groups $H(K_\infty)$, $\overline{U}_S(K_\infty)$, $C(K_\infty)$ etc. carry the natural structure of R_∞-modules, where $R_\infty := \varprojlim \mathbf{Z}_\ell[G(K_n/\mathbf{Q})]$ is a complete group ring of the Galois group $G_\infty := G(K_\infty/\mathbf{Q})$. There exists the natural decomposition into the direct product $G(K_\infty/\mathbf{Q}) = \Gamma \times V$, where $\Gamma = G(\mathbf{Q}_\infty/\mathbf{Q})$ and $V = G(E/\mathbf{Q})$, E is the maximal subfield of K with conductor not divisible by ℓ^2 (by ℓ^3 for $\ell = 2$). We have $R_\infty = \Lambda[V]$, where $\Lambda = \mathbf{Z}_\ell[[\Gamma]] \cong \varprojlim[\Gamma/\Gamma_n]$ and Γ_n is the unique subgroup of Γ of index ℓ^n. Fixing a topological generator $\gamma \in \Gamma$, we get an isomorphism $\Lambda \cong \mathbf{Z}_\ell[[T]]$, $\gamma \to 1 + T$, where $\mathbf{Z}_\ell[[T]]$ is the ring of formal power series of one indeterminate T over $\mathbf{Z}_\ell$.

In Section 1 we characterize $C(K_\infty)$ as a Λ-module. Using results of Kubert [4, 5] on the universal ordinary distribution, we prove that $C(K_\infty)$ is a free Λ-module (Theorem 1.1).

In Section 2 we consider the characteristic series of a finitely generated Λ-torsion R_∞-module A. If A is free over $\mathbf{Z}_\ell$, we produce the formula expressing the order $|A^H_{(0),\varphi}| = |A^H_{\varphi,(0)}|$ in terms of characteristic series of A (Prop. 2.3), where H is a subgroup of V. Then we describe the characteristic series of R_∞ module $\mathcal{A}(K_\infty)/C(K_\infty)$ where $\mathcal{A}(K_\infty) := \varprojlim \mathcal{A}(K_n)$ and $\mathcal{A}(K_n) := \prod_{v\mid\ell} \overline{U}(K_{n,v})$, $\overline{U}(K_{n,v}) = U(K_{n,v})/\mu(K_{n,v})$. This description is based on the theorem of Iwasawa on the circular units [8], [9]. We show that the characteristic series in question are near to the so called Iwasawa series.

In Section 3 we continue our calculations on characteristic series. Let $T_\ell(K_\infty)^+$ be the maximal subgroup of $T_\ell(K_\infty)$ fixed by the automorphism of complex conjugation. Put $\overline{U}(K_\infty) = \varprojlim \overline{U}(K_n)[\ell]$. We prove (Theorem 3.1) that $T_\ell(K_\infty)^+$ and $\overline{U}(K_\infty)/C(K_\infty)$ have the same characteristic series for any even character of V. The proof is based on the so called "main conjecture" of Iwasawa theory [10], [14]. and on some form of Spiegelungsatz produced by the author in [7]. Then we generalize this result for any abelian number field k and its cyclotimic $\mathbf{Z}_\ell$-extension k_∞.

In Section 4 we prove Theorem 3 of the introduction. Briefly speaking, if k is a real abelian field, then we have an exact sequence

$$0 \longrightarrow P \longrightarrow T_\ell(k_\infty) \longrightarrow R \longrightarrow 0, \tag{0.9}$$

where P is the maximal finite submodule of $T_\ell(k_\infty)$ and R is $\mathbf{Z}_\ell$-free. We deduce from (0.9) that

$$|T_\ell(k_\infty)_{(0),\varphi}| = |P_{(0),\varphi}| \cdot |R_{(0),\varphi}| \tag{0.10}$$

for any φ. On the other hand, denoting by $U_S^*(k)$ the image $\pi\left(\overline{U}_S(k_\infty)\right)$ in (0.8), we get an inclusions $C_S \subseteq U_S^*(k) \subseteq \widehat{U}_S(k)$. Thus we have

$$|\widehat{U}_S(k)_\varphi / C_S(k)_\varphi| = [\widehat{U}_S(k)_\varphi \,:\, U_S^*(k)_\varphi] \cdot [U_S^*(k)_\varphi \,:\, C_S(k)_\varphi] \tag{0.11}$$

for any $\varphi \in \Phi$. Using the characteristic series, we prove that

$$|U_S^*(k)_\varphi \,:\, C_S(k)_\varphi| = |R_{(0),\varphi}| \tag{0.12}$$

for any φ.

It was proved in [6], Prop. 7.5 that there exists a natural isomorphism

$$\widehat{U}_S(k)/U_S^*(k) \cong T_\ell(k_\infty)^\Gamma \tag{0.13}$$

We give in Section 4 a short and selfcontained proof of (0.13) (see Prop. 4.3).Then Theorem 3 follows immediately from (0.10), (0.11), (0.12) and (0.13).

To deduce Theorem 1 and Theorem 2 from Theorem 3 we need a new form of Theorem 3. Let ν_ℓ be a ℓ-adic exponent in $\overline{\mathbf{Q}}_\ell$ normalized by the condition $\nu_\ell(\ell) = 1$. In Section 5 we prove

Theorem 4 *For a real abelian k and any $\varphi \in \Phi$ we have*

$$\nu_\ell\left(|T_\ell(k_\infty)_{(0),\varphi}|\right) = \nu_\ell\left([H(k)_\varphi : \widehat{U}_S(k)_\varphi]^{-1}\ell^{t_\varphi}\prod_{\substack{\chi\neq 1\\ \chi|\varphi}}\frac{1}{2}L_\ell(1,\ \chi)\right), \tag{0.14}$$

where χ runs over all nontrivial one-dimensional characters of $G = G(k/\mathbf{Q})$ such that $\chi|_{G_0}$ enters φ, t_φ is a constant given explicitly in Theorem 5.1 and $L_\ell(s,\ \chi)$ is an ℓ-adic L-function of Kubota-Leopoldt [3].

Note that we have

$$[\widehat{U}_S(k)_\varphi : C_S(k)_\varphi] = [H(k)_\varphi : \widehat{U}_S(k)_\varphi]^{-1}[H(k)_\varphi : C_S(k)_\varphi],$$

so the only difference from Theorem 3 is the explicit formula for the index $[H(k)_\varphi : C_S(k)_\varphi]$. We derive such a formula from consideration of the characteristic series of $H(k_\infty)/C_S(k_\infty)$. This series are closely connected with Iwasawa series. So the interrelation between Iwasawa series and ℓ-adic L-functions discovered by Iwasawa [3] explains why (0.14) contains the values $L_\ell(1, \chi)$.

In Section 6 we give a result that is, in some sense, a refinement of the conductor-discriminant formula of Hasse. For an abelian number field k we consider a Galois algebra $\mathbf{A}_k = k\otimes_{\mathbf{Q}}\overline{\mathbf{Q}}_\ell$. Let $\mathbf{R}_k$ be the maximal order of $\mathbf{A}_k$. The natural inclusion $k \hookrightarrow \mathbf{A}_k$ implies an inclusion $\alpha : \mathcal{O}_k \hookrightarrow \mathbf{R}_k$, where $\mathcal{O}_k$ is the ring of intergers of k. Put $\tilde{\mathcal{O}}_k = \overline{\mathcal{O}} \cdot \alpha(\mathcal{O}_k) \subset \mathbf{R}_k$, where $\overline{\mathcal{O}}$ is the ring of intergers of $\overline{\mathbf{Q}}_\ell$. Then we prove (Theorem 6.1)

Theorem 5 *For any $\varphi \in \Phi$ we have*

$$\nu_\ell((\mathbf{R}_{k,\varphi} : \mathcal{O}_{k,\varphi})) = \nu_\ell\left(\prod_{\substack{\chi\neq 1\\ \chi\mid\varphi}} g_{\overline{\chi}}\right),$$

where $(A : B)$ means generalized index in the sense of Sinnott [12], and $g_{\overline{\chi}}$ is the Gauss sum corresponding to the character $\overline{\chi} = \chi^{-1}$.

In Section 7 we calculate some unit indices. Let k be a real abelian field and $G = G(k/\mathbf{Q})$. As in [12], for a $\mathbf{Z}_\ell[G]$-module A free over $\mathbf{Z}_\ell$ we put

$$A_0 = \{x \in A \mid \operatorname{Sp}_G(x) = 0\},$$

where Sp_G is the trace map with respect to G. We prove (Theorem 7.1) that for any $\varphi \in \Phi$

$$\ell^{s_\varphi}\frac{|T_\ell(k_\infty)_{(0),\varphi}|}{|\mathrm{Cl}(k)_{\ell,\varphi}|} = \frac{|\mathcal{A}(k)_{0,\varphi} : \overline{U}(k)[\ell]_\varphi|}{H(k)_\varphi : \hat{U}_S(k)_\varphi|}, \tag{0.15}$$

where $s_\varphi = 0$ if $\varphi \neq \varphi_0$ and s_{φ_0} is some simple constant given explicitly in Prop. 7.4.

Let Log : $\overline{U}(k)[\ell] \hookrightarrow \mathbf{A}_k$ be the compositum of the mapping log : $\overline{U}(k)[\ell] \hookrightarrow k\otimes_{\mathbf{Q}}\mathbf{Q}_\ell$ induced by the ℓ-adic logarithm and the natural inclusion $k\otimes_{\mathbf{Q}}\mathbf{Q}_\ell \hookrightarrow \mathbf{A}_k = k\otimes_{\mathbf{Q}}\overline{\mathbf{Q}}_\ell$. Put $\tilde{U}(k) = \overline{\mathcal{O}} \cdot \operatorname{Log}(\overline{U}(k)[\ell])$. The following theorem (Theorem 7.3) may be considered as an ℓ-adic analytic class number formula for a φ-component of the ℓ-class group.

Theorem 6 *For a real abelian k and any $\varphi \in \Phi$ we have*

$$\nu_\ell\left(|\mathrm{Cl}(k)_{\ell,\varphi}|\right) = \nu_\ell\left((\mathbf{R}_{k,0,\varphi} : \widetilde{U}(k)_\varphi)^{-1} \prod_{\substack{\chi\in\widehat{G} \\ \chi\,|\,\varphi,\,\chi\neq 1}} \frac{1}{2}a(\chi)\right),$$

where

$$a(\chi) = \sum_{\substack{a \bmod f_\chi \\ (a,f_\chi)=1}} \overline{\chi}(a)\log(1-\varepsilon_\chi^a),$$

f_χ is the conductor of χ, ε_χ is a primitive f_χ-th root of unity and log *means the ℓ-adic logarithm.*

Note that the index $(\mathbf{R}_{k,0,\varphi} : \widetilde{U}(k)_\varphi)$ may be treated as a φ-component of the ℓ-adic regulator of k.

We deduce Theorem 6 from Theorem 4, Theorem 5 and (0.15). Then, using the method of Sinnott, we prove (Theorem 7.4) "an abstract index formula". This formula expresses $|\mathrm{Cl}(k)_{\ell,\varphi}|$ in terms of the index $[\overline{U}(k)[\ell]_\varphi : C_{k,\varphi}]$, where the circular units C_k are defined axiomatically.

In Section 8, using arguments of Sinnott, we deduce Theorem 1 from Theorem 7.4 (see Theorem 8.3).

In Section 9 we prove Theorem 2 (see Theorem 9.2). Then we prove a class number formula of another type (Theorem 9.3). This formula includes some modified circular units and some modified constants $c^+_{k,\varphi}$. In some particular cases we are able to calculate these modified constants explicitly, and these calculations yield nontrivial divisibility conditions for the class numbers of some real abelian fields (see Theorem 9.4 and Theorem 9.5).

In Section 10 we give some commentary to our results and formulate some open problems.

Acknowledgements. The author is in debt to Prof. Dr. H.Koch and his colleagues from Max-Planck-Arbeitsgruppe "Algebraische Geometrie und Zahlentheorie" whose hospitality allowed him to fulfil a considerable part of this work.

The author thanks M.Zh.Shmatikov who kindly tought him to use LaTeX and N.V.Igumnova for help in preparing the manuscript.

1 On the circular units in $\mathbf{Z}_\ell$-extensions

Let ℓ be a fixed prime number and $d \not\equiv 2 \pmod 4$ be a natural number prime to ℓ. We suppose d to be fixed throughout this section. Let μ_d be the group of all d-th roots of unity in a fixed algebraic closure $\overline{\mathbf{Q}}$ of $\mathbf{Q}$. We put $K_{-1} := \mathbf{Q}(\mu_d)$ and $K_n := \mathbf{Q}(\mu_d, \zeta_n)$ for any $n \geq 0$, where $\zeta_n \in \overline{\mathbf{Q}}$ is a ℓ^{n+1}-th primitive root of unity (a ℓ^{n+2}-th primitive root of unity if $\ell = 2$). We choose the roots ζ_n in such a way that the equality $\zeta_{n+1}^\ell = \zeta_n$ holds true for any n. Then any cyclotomic field is of the form K_n for some d and n, and for a fixed d the fields K_n, $n \geq 0$, form a tower of all intermediate subfields of the cyclotomic $\mathbf{Z}_\ell$-extension K_∞/K_0, where we put $K_\infty := \bigcup_{n=1}^{\infty} K_n$. We denote by $\mu(K_n)$ (resp. $\mu_\ell(K_n)$) the group of all roots of unity in K_n (resp. the ℓ-component of $\mu(K_n)$).

Let $P(K_n)$ and $C(K_n)$ be the groups of cyclotomic numbers and cyclotomic units respectively defined in the introduction. Note that the elements $(1 - \alpha\zeta_n^i)$, $\alpha \in \mu_d$, $i = 0, \ldots, \ell^{n+1+\delta} - 1$ generate the full group $P(K_n)$. If there is no danger of confusion, we denote this groups simply by P_n and C_n omitting the symbol K. We put $P_\infty := \varprojlim \overline{P}_n[\ell]$, $C_\infty := \varprojlim \overline{C}_n[\ell]$ where $\overline{P}_n := P_n/\mu(K_n)$, $\overline{C}_n := C_n/(\mu(K_n) \cap C_n)$ and the symbol $[\ell]$ means ℓ-completion. So P_∞ and C_∞ are R_∞-modules and Λ-modules as it was pointed out in the introduction.

If $\alpha \in \mu_d$, then we put $\varepsilon_n(\alpha) := 1 - \alpha^{\ell^{-n-\delta}}\zeta_n$, where $\delta = 0$ if $\ell \neq 2$ and $\delta = 1$ if $\ell = 2$. The elements $\varepsilon_n(\alpha)$ for $n \geq 0$ form a coherent sequence with respect to the norm maps, and thus we have an element

$$\varepsilon_\infty(\alpha) := \varprojlim \varepsilon_n(\alpha) \in P_\infty.$$

Proposition 1.1 *The elements $E_\infty(\alpha)$, where α runs over μ_d, generate P_∞ as a R_∞-module.*

Proof. Let D_n be the Galois submodule of $\overline{P}_n$ generated by all $\varepsilon_n(\alpha)$ for $\alpha \in \mu_d$. As $N_{K_n/K_r}(\varepsilon_n(\alpha)) = \varepsilon_r(\alpha)$ for $n > r \geq 0$, we have $\overline{P}_n = D_n \cdot \overline{P}_{-1}$. Hence $P_\infty = \varprojlim \overline{P}_n[\ell] = \varprojlim D_n[\ell]$ as desired.

□

To investigate the Galois module structure of P_∞ and C_∞, we need some results on the universal distribution [4], [5]. The universal distribution on

$\frac{1}{N}\mathbf{Z}/\mathbf{Z}$ for a natural number N is by definition an abelian group $U(N)$ generated by the symbols (a) for all $a \in \frac{1}{N}\mathbf{Z}/\mathbf{Z}$, satisfying the relations

$$\sum_{mb=a} (b) = (a) \text{ for any } a \in \frac{1}{N}\mathbf{Z}/\mathbf{Z},\ m \mid N. \tag{1.1}$$

By [4] $U(N)$ is a free abelian group. The natural action of $G(N) = (\mathbf{Z}/N\mathbf{Z})^*$ on $\frac{1}{N}\mathbf{Z}/\mathbf{Z}$ induces an action of $G(N)$ on $U(N)$, and we have a $G(N)$-module isomorphism [4], Theorem 4.11,

$$U(N)\otimes_{\mathbf{Z}}\mathbf{Q} \cong \mathbf{Q}[G(N)]. \tag{1.2}$$

If $N \mid N_1$, then the natural inclusion $\frac{1}{N}\mathbf{Z}/\mathbf{Z} \hookrightarrow \frac{1}{N_1}\mathbf{Z}/\mathbf{Z}$ and the mapping $\frac{1}{N_1}\mathbf{Z}/\mathbf{Z} \to \frac{1}{N}\mathbf{Z}/\mathbf{Z}$ sending $x \in \frac{1}{N_1}\mathbf{Z}/\mathbf{Z}$ into $\frac{N_1}{N}x \in \frac{1}{N}\mathbf{Z}/\mathbf{Z}$ induce the mappings $i(N, N_1) : U(N) \to U(N_1)$ and $N(N_1, N) : U(N_1) \to U(N)$. It is well known that $i(N, N_1)$ is always an injective map. From (1.1) it follows immediately

Proposition 1.2 *For any prime ℓ let $N \equiv 0 \pmod{\ell}$, and put $N_1 = \ell N$. Let $H(N_1, N)$ be the kernel of the natural projection $G(N_1) \to G(N)$. Then the map $i(N, N_1) \circ N(N_1, N) : U(N_1) \to U(N_1)$ coincides with the norm map with respect to $H(N_1, N)$.*

For a natural number N let $Z^*(N)$ be the set of all primitive elements in $\frac{1}{N}\mathbf{Z}/\mathbf{Z}$, i.e. the elements of an order exactly N. Let $N = \prod_{p \mid N} p^{n(p)}$ be the prime factorization of N. Then we have the natural decompositions

$$\frac{1}{N}\mathbf{Z}/\mathbf{Z} = \prod_{p \mid N} \left(\frac{1}{p^{n(p)}}\mathbf{Z}/\mathbf{Z}\right), \quad Z^*(N) = \prod_{p \mid N} Z^*(p^{n(p)}).$$

Theorem A. *([4], Theorem 1.8, Prop.1.9). Put*

$$T(N) := \prod_{p \mid N} \left[Z^*(p^{n(p)}) - \left\{\frac{1}{p^{n(p)}}\right\} \bigcup \{0\} \right].$$

Then the elements (t) for $t \in T(N)$ form a basis of the free abelian group $U(N)$.

Let ℓ be a prime number, d prime with ℓ, $d \not\equiv 2 \pmod 4$. Put

$$U(\ell^\infty d) := \varprojlim (U(\ell^n d) \otimes_{\mathbf{Z}} \mathbf{Z}_\ell),$$

where the inverse limit is taken with respect to the maps $N(\ell^{n+1}d,\, \ell^n d)$. We have a natural action of $G_\infty := \varprojlim G(\ell^n d)$ on $U(\ell^\infty d)$. Let Γ be the kernel of the natural projection $G_\infty \to G(qd)$, where $q = \ell$ if $\ell \neq 2$ and $q = 4$ if $\ell = 2$. Then the group $\Gamma \cong \mathbf{Z}_\ell$ acts on $U(\ell^\infty d)$, thus $U(\ell^\infty d)$ has a natural structure of a Λ-module.

Proposition 1.3 *The group $U(\ell^\infty d)$ is a free Λ-module of rank $\varphi(qd)$, where $\varphi(x)$ is the Euler function.*

Proof. For $N = \ell^n d$, $d = \prod\limits_{p\,|\,d} p^{n(p)}$, we present the set $T(\ell^n d)$ as a disjoint union $T(\ell^n d) = T(\ell^n d)_1 \cup T(\ell^n d)_2$, where

$$T(\ell^n d)_1 := \left[Z^*(\ell^n) - \left\{\frac{1}{\ell^n}\right\}\right] \times \prod_{p\,|\,d} \left[Z^*(p^{n(p)}) - \left\{\frac{1}{p^{n(p)}}\right\} \bigcup \{0\}\right]$$

and

$$T(\ell^n d)_2 := \{0\} \times \prod_{p\,|\,d} \left[Z^*(p^{n(p)}) - \left\{\frac{1}{p^{n(p)}}\right\} \bigcup \{0\}\right].$$

According to the decomposition $\frac{1}{\ell^n d}\mathbf{Z}/\mathbf{Z} \cong \frac{1}{\ell^n}\mathbf{Z}/\mathbf{Z} \oplus \frac{1}{d}\mathbf{Z}/\mathbf{Z}$, any $a \in \frac{1}{\ell^n d}\mathbf{Z}/\mathbf{Z}$ can be presented uniquely in a form $a = (a',\, a'')$, where $a' \in \frac{1}{\ell^n}\mathbf{Z}/\mathbf{Z}$, $a'' \in \frac{1}{d}\mathbf{Z}/\mathbf{Z}$. If $H_n \cong (\mathbf{Z}/\ell^n\mathbf{Z})^*$ is the kernel of the natural projection $G(\ell^n d) \to G(d)$, then any two elements $a,\, b \in \frac{1}{\ell^n d}\mathbf{Z}/\mathbf{Z}$ of the form $a = (a',\, a'')$, $b = (b',\, b'')$ are conjugated with respect to the action of H_n if and only if $a'' = b''$ and a', b' have the same order as elements of $\frac{1}{\ell^n}\mathbf{Z}/\mathbf{Z}$. It means that the $\mathbf{Z}_\ell[G(\ell^n d)]$-submodule $U_1(\ell^n d)$ of $U(\ell^n d) \otimes_{\mathbf{Z}} \mathbf{Z}_\ell$ which is generated by all (t), $t \in T(\ell^n d)_1$, can be generated as a H_n-module by the set of $\varphi(d)$ elements (t), where t runs over the set

$$T(\ell^n d)_3 := \left\{\frac{1}{\ell^n}\right\} \times \prod_{p\,|\,d} \left[Z^*(p^{n(p)}) - \left\{\frac{1}{p^{n(p)}}\right\} \bigcup \{0\}\right].$$

Passing to the inverse limit with respect to the maps $N(\ell^{n+1}d,\, \ell^n d)$, we get that the module $U_1(\ell^\infty d) := \varprojlim U_1(\ell^n d)$ can be generated by $\varphi(d)$ elements as a H_∞-module, where $H_\infty := \varprojlim H_n \cong \mathbf{Z}_\ell^*$. Hence, $U_1(\ell^\infty d)$ can be generated by $\varphi(q)\varphi(d) = \varphi(qd)$ elements as a Λ-module. Let $U_2(\ell^n d)$ be the $\mathbf{Z}_\ell[G(\ell_n d)]$-submodule of $U(\ell^n d)\otimes_{\mathbf{Z}}\mathbf{Z}_\ell$ generated by all (t), where t runs over $T(\ell^n d)_2$. Then reasoning as in the proof of Prop. 1.1, we get

$$U(\ell^\infty d) := \varprojlim(U_1(\ell^n d)\cdot U_2(\ell^n d)) = \varprojlim U_1(\ell^n d) = U_1(\ell^\infty d).$$

Thus there exists a surjective map of Λ-modules $\alpha : \Lambda^{\varphi(qd)} \to U(\ell^\infty d)$. To prove that $U(\ell^\infty d)$ is Λ-free of rank $\varphi(qd)$, note the natural projection $p_n : U_1(\ell^\infty d) \to U_1(\ell^n d)$ is surjective for any n. The surjection $p_n \circ \alpha : \Lambda^{\varphi(qd)} \to U_1(\ell^n d)$ induces a surjection $\beta_n : \Lambda^{\varphi(qd)}_{(n-\delta-1)} \to U_1(\ell^n d)$, where $\delta = 0$ if $\ell \neq 2$, $\delta = 1$ if $\ell = 2$, and for any G_∞-module A the notion $A_{(i)}$ means factoring A by the action of the subgroup $\Gamma_i \subseteq \Gamma$ of index ℓ^i (thus $\Gamma_{n-\delta-1}$ is the kernel of the natural map $G_\infty \to G(\ell^n d)$). Denoting by $\mathrm{rk}(A)$ the $\mathbf{Z}_\ell$-rank of A, we get $\mathrm{rk}(\Lambda^{\varphi(qd)}_{(n-\delta-1)}) = \varphi(\ell^n d)$ and $\mathrm{rk}(U_1(\ell^n d)) \geq \mathrm{rk}(U(\ell^n d)) - |T(\ell^n d)_2| = \varphi(\ell^n d) - \varphi(d)$. Thus $\mathrm{rk}(\mathrm{Ker}\beta_n) \leq \varphi(d)$, therefore $\mathrm{Ker}\,\alpha = \varprojlim \mathrm{Ker}\,\beta_n = 0$.

□

Theorem B *([5], Theorem 2.16, Prop. 3.3). Let* $\{\pm\mathrm{id}\} \subset G(N)$ *be the subgroup generated by the elements* ± 1. *Then for any* k *we have* $H^k(\pm\mathrm{id}, U(N)) \cong (\mathbf{Z}/2\mathbf{Z})^r$, *where* $H^k(\ ,\ )$ *is the Tate cohomology groups,* $r = 2^{\nu(N)-1}$ *and* $\nu(N)$ *is the number of distinct prime divisors of* N. *Let* $M \mid N$, $\nu(M) = \nu(N)$ *and* $M \not\equiv 2 \pmod 4$, *then the inclusion* $i(M,N) : U(M) \hookrightarrow U(N)$ *induces an isomorphism*

$$i^*(M,\ N) : H^k(\pm\mathrm{id},\ U(M)) \cong H^k(\pm\mathrm{id},\ U(N)).$$

Corollary. If $\ell = 2$ then we have for any k

$$H^k(\pm\mathrm{id},\ U(\ell^\infty d)) = 0.$$

Indeed, if $\ell = 2$, then by virtue of Theorem B the norm map with respect to the group $H(\ell^n d,\ \ell^{n-1}d)$ coincides with multiplying by $|H(\ell^n d,\ \ell^{n-1}d)| = 2$ for $n \geq 3$, and thus annihilates the group $H^k(\pm\mathrm{id},\ U(\ell^n d))$ for any k. Then it follows from Prop. 1.2 and an isomorphic character of $i^*(\ell^{n-1}d,\ \ell^n d)$ that the map $N(\ell^n d,\ \ell^{n-1}d)$ annihilates $H^k(\pm\mathrm{id},\ U(\ell^n d))$ for any k and $n \geq 3$. Therefore

$$H^k(\pm\mathrm{id},\ U(\ell^\infty d)) = 0.$$

□

Theorem 1.1 *The Λ-modules P_∞ and C_∞ are Λ-free modules of rank $\frac{1}{2}[K_0 : \mathbf{Q}]$.*

Proof. Let α be a fixed generator of μ_d. For any

$$\frac{c}{\ell^{n+1+\delta}d} \in \frac{1}{\ell^{n+1+\delta}d}\mathbf{Z}/\mathbf{Z}, \quad c \in \mathbf{Z},$$

put

$$\psi^n(0) = 1,\ \psi^n\left(\frac{c}{\ell^n d}\right) = (1 - \alpha^{\ell^{-n}c}\zeta_n^c) \pmod{P_n \cap (\mathbf{Q}^* \times \mu(K^n))}.$$

Then we get the mapping

$$\psi^n : \frac{1}{\ell^{n+1+\delta}d}\mathbf{Z}/\mathbf{Z} \to P_n/P_n \cap (\mathbf{Q}^* \times \mu(K_n)).$$

The mappings ψ^n is an even distribution in the sense of [4], i.e. the relations

$$\sum_{mb=a} \psi^n(b) = \psi^n(a) \text{ for any } a \in \frac{1}{\ell^{n+1+\delta}d}\mathbf{Z}/\mathbf{Z}, \quad m \mid \ell^{n+1+\delta}d$$

and

$$\psi^n(-a) = \psi^n(a)$$

hold true. Thus ψ^n defines a natural surjection

$$\overline{\psi}^n : U(\ell^{n+1+\delta}d) \otimes_{\mathbf{Z}} \mathbf{Z}_\ell \to (P_n/P_n \cap \mathbf{Q}^* \times \mu(K_n))[\ell].$$

The mappings $\overline{\psi}^n$ are compatible with the action of the group $G(\ell^{n+1+\delta}d) \cong G(K_n/\mathbf{Q})$ and with the norm maps. Hence, passing to the inverse limit with respect to the norm maps, we get the surjective map of R_∞-modules

$$\overline{\psi}_\infty : U(\ell^\infty d)/U(\ell^\infty d)^- \longrightarrow \varprojlim((P_n/P_n \cap \mathbf{Q}^* \times \mu(K_n))[\ell] = P_\infty,$$

where $U(\ell^\infty d)^-$ means the maximal subgroup of $U(\ell^\infty d)$ on which $-\mathrm{id}$ acts as multiplication by -1.

As we can consider P_∞ as a Λ-submodule of the R_∞-module $H(K_\infty)$, defined in the introduction, we get that P_∞ has no Λ-torsion. It follows from

Prop. 1.3 and the definition of $U(\ell^\infty d)^-$ that $U(\ell^\infty d)/U(\ell^\infty d)^-$ has no Λ-torsion as well. Let $U(\ell^\infty d)^+$ be the maximal subgroup of $U(\ell^\infty)$ fixed under the action of $-\mathrm{id}$. Then it can be checked easily that both modules $U(\ell^\infty d)^+$ and $U(\ell^\infty d)^-$ have Λ-rank $\frac{1}{2}[K_0 : \mathbf{Q}]$.

By Prop. 1.1 we have for any n a natural surjection $P_\infty \to D_n[\ell]$. By [12], Theor 4.1 C_n has finite index in the unit group $U(K_n)$, hence we have that $\mathbf{Z}_\ell$-rank of $D_n[\ell]$ satisfies for any n the condition

$$\mathrm{rk}\, D_n[\ell] \geq \mathrm{rk} U(K_n)[\ell] \; - \; \mathrm{rk}\, \overline{P}_{-1}[\ell],$$

i.e. $\mathrm{rk}\, D_n[\ell] \geq \frac{1}{2}[K_n : \mathbf{Q}] - c$, where c does not depend on n. Then by [6], Prop. 1.2 we get that the Λ-rank of P_∞ equals $\frac{1}{2}[K_0 : \mathbf{Q}]$, hence $\overline{\psi}_\infty$ is an isomorphism.

If $\ell \neq 2$, then we have $= U(\ell^\infty d) = U(\ell^\infty d)^+ \oplus U(\ell^\infty d)^-$, so $\overline{\psi}_\infty$ induces an isomorphism $U(\ell^\infty d)^+ \cong P_\infty$. Hence P_∞ is a free Λ-module in this case.

If $\ell = 2$, then we have an isomorphism

$$P_\infty \cong U(\ell^\infty d)/U(\ell^\infty d)^- \cong N(U(\ell^\infty d)),$$

where $N(\;)$ means the image of the norm map with respect to $\{\pm\mathrm{id}\}$. By the corollary from Theorem B we have $H^0(\{\pm\mathrm{id}\}, U(\ell^\infty d)) = 0$, thus $N(U(\ell^\infty d)) = U(\ell^\infty d)^+$. To prove that $U(\ell^\infty d)^+$ is Λ-free we note that $U(\ell^\infty d))^+$ is a submodule of a Λ-free module $U(\ell^\infty d)$; and $U(\ell^\infty d)/U(\ell^\infty d)^+$ has no torsion. So our assertion follows from [6]., Prop. 1.1.

Thus we have proved that P_∞ is Λ-free in any case. To prove that C_∞ is Λ-free we note that any $x \in \overline{P}_n[\ell]$ may belong to the image of the natural projection $P_\infty \to \overline{P}_n[\ell]$ only if x belongs to the ℓ-completion of S-units, where S consists of all prime divisors of ℓ. Let ε_m be a primitive m-th root of unity. It is well known that the number $1 - \varepsilon_m$ is a unit if and only if m is a composed number. If $m = p^r$ for some prime p, then $1 - \varepsilon_{p^r}$ is a prime element of the local field $\mathbf{Q}_p(E_{p^r})$. Thus it follows easily that we have the exact sequence of Λ-modules

$$0 \longrightarrow C_\infty \longrightarrow P_\infty \longrightarrow \mathbf{Z}_\ell \longrightarrow 0,$$

where $\mathbf{Z}_\ell$ is generated by $\varepsilon_\infty(1)$. As P_∞ is Λ-free, we get from [6], Prop. 1.1. that C_∞ is Λ-free as well.

□

2 On some characteristic series

Let $R_\infty := \mathbf{Z}_\ell[[G_\infty]] := \varprojlim \mathbf{Z}_\ell[G(K_n/\mathbf{Q})]$ be the ring defined in the introduction. We have the natural direct product decomposition $G_\infty := G(K_\infty/\mathbf{Q}) = \Gamma \times V$, where $\Gamma \cong G(\mathbf{Q}_\infty/\mathbf{Q}) \cong G(K_\infty/K_0)$, $V \cong G(K_0/\mathbf{Q}) \cong G(K_\infty/\mathbf{Q}_\infty)$. If we fix a topological generator $\gamma \in \Gamma$, then we get the isomorphism $\Lambda := \mathbf{Z}_\ell[[\Gamma]] \cong \mathbf{Z}_\ell[[T]]$, $\gamma = 1 + T$, where $\mathbf{Z}_\ell[[T]]$ is a ring of formal power series. We have $R_\infty = \Lambda[V]$. All R_∞-modules considered below are assumed to be finitely generated over R_∞. If χ is any one-dimensional character of V taking its values in the algebraic closure $\overline{\mathbf{Q}}_\ell$ of $\mathbf{Q}_\ell$, then the ring $\mathcal{O}_\chi$ generated over $\mathbf{Z}_\ell$ by all the values of χ has a natural structure of V-module, if we put $\sigma(a) = \chi(\sigma)a$ for any $\sigma \in V$, $a \in \mathcal{O}_\chi$. For any R_∞-module A we define the χ-component of A by

$$A_\chi = A \otimes_{\mathbf{Z}_\ell[V]} \mathcal{O}_\chi.$$

Thus we have $R_{\infty,\chi} \cong \mathcal{O}_\chi[[\Gamma]] \cong \mathcal{O}_\chi[[T]]$. We may treat A_χ as a $R_{\infty,\chi}$-module, if we put $T(a \otimes b) = T(a) \otimes b$, $\tau(a \otimes b) = a \otimes \tau(b)$ for $a \in A$, $b, \tau \in \mathcal{O}_\chi$. Put $V = V_\ell \times V_0$, where V_ℓ is the ℓ-Sylow subgroup of V and $(|V_0|, \ell) = 1$. Let Φ be the set of all $\mathbf{Q}_\ell$-irreducible characters of V_0. Then for any R_∞-module A we have the decomposition into the direct product

$$A = \bigoplus_{\varphi \in \Phi} A_\varphi,$$

where $A_\varphi = e_\varphi A$ and e_φ is the idempotent corresponding to φ. For a one-dimensional character $\chi \in \widehat{V}$, where $\widehat{V}$ is the group of all the characters of V, the notion $\chi \,|\, \varphi$ means that the restriction $\chi|_{V_0}$ of χ on V_0 enters φ as its irreducible component over $\overline{\mathbf{Q}}_\ell$. We have

$$(2.1) \qquad (A_\varphi)_\chi = \begin{cases} A_\chi \cong A_\varphi & \text{if } \chi \mid \varphi \\ 0 & \text{otherwise} \end{cases}$$

If A is Λ-torsion, then there is defined the characteristic series $f_A = f_A(T) \in \Lambda$ of A (see [3], [9]). We recall some properties of these series. At first, note that f_A is defined uniquely up to multiplication by any unit $u \in \Lambda^*$. If A, B are quasi-isomorphic Λ-torsion modules (i.e. there exists a homomorphism $f : A \to B$ with finite kernel and cokernel, we shall write $A \sim B$ in such a case), then $f_A = f_B$. If $A = \bigoplus_{i=1}^{r} \Lambda/f_i\Lambda$ for some $f_i \in \Lambda$, $f_i \neq 0$, then

$f_A = \prod_{i=1}^{r} f_i$. It is known that any Λ-torsion A is quasi-isomorphic to a module of the form $\bigoplus_{i=1}^{r} \Lambda/f_i\Lambda$.

Let a Λ-module A be finitely generated over $\mathbf{Z}_\ell$ (this is the only case we shall deal with in this paper). Then f_A is of the form $f_1(T)u$, where $u \in \Lambda^*$ and $f_1(T)$ is a distinguished polynomial of the form $T^\lambda + a_{\lambda-1}T^{\lambda-1} + \ldots + a_0$, $a_{\lambda-1}, \ldots, a_0 \in \ell\mathbf{Z}_\ell$. Note that we may treat $f_1(T)$ as a characteristic polynomial of $T = \gamma - 1$ acting on the λ-dimensional $\mathbf{Q}_\ell$-space $A \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$. If R_∞-module A is Λ-torsion, then for any $\chi \in V$ we have the characteristic series $f_A(T, \chi)$ of $\mathcal{O}_\chi[[T]]$-module A_χ, defined in the same manner. The next statement is well known.

Proposition 2.1 *Let A be a R_∞-module such that A is finitely generated over $\mathbf{Z}_\ell$ and thus Λ-torsion. Then we have*

$$f_A(T) = \prod_{\chi \in \widehat{V}} f_A(T, \chi), \; f_{A_\varphi}(T) = \prod_{\chi \mid \varphi} f_A(T, \chi) \tag{2.2}$$

for any $\varphi \in \Phi$, where we put $f_A(T, \chi) = 1$ if A_χ is finite.

Let

$$0 \longrightarrow A \longrightarrow B \longrightarrow C \longrightarrow 0$$

be an exact sequence of R_∞-modules finitely generated over $\mathbf{Z}_\ell$. Then we have

$$f_B = f_A \cdot f_C, \; f_B(T, \chi) = f_A(T, \chi) \cdot f_C(T, \chi) \text{ for any } \chi \in \widehat{V}. \tag{2.3}$$

By $\nu_\ell(\;)$ we denote the ℓ-adic exponent in $\overline{\mathbf{Q}}_\ell$ such that $\nu_\ell(\ell) = 1$.

Proposition 2.2 *Let A be a Λ-torsion module. Then the group $A_{(0)} = A/(\gamma - 1)A$ is finite if and only if $f_A(0) \neq 0$. If A is $\mathbf{Z}_\ell$-free, then we have*

$$\nu_\ell(|A_{(0)}|) = \nu_\ell(f_A(0)). \tag{2.4}$$

Proof. The condition $f_A(0) \neq 0$ means that A^Γ is finite. The group A^Γ is finite if and only if so is $A_{(0)}$. If A, B are $\mathbf{Z}_\ell$-free and A is quasi-isomorphic to B, then $|A_{(0)}| = |B_{(0)}|$. So it is enough to check (2.4) for A of the form $A = \bigoplus_{i=1}^{r} \Lambda/f_i\Lambda$, where f_i are distinguished polynomials. In this last case formula (2.4) is evident.

□

The next proposition is a far-reaching extension of Prop. 2.2. Let $\tau : G_\infty \to G$ be a surjective mapping of G_∞ onto a finite group G. Then $\operatorname{Ker}\tau = H \times \overline{\Gamma}$, where $H = V \cap \operatorname{Ker}\tau$ and the group $\overline{\Gamma} \cong \mathbf{Z}_\ell$ is defined noncanonically. We meet such a situation in the case, when $G = G(k/\mathbf{Q})$ for some algebraic number field $k \subset K_\infty$. In such a case we have $H = G(K_\infty/k_\infty)$, $\overline{\Gamma} \cong G(k_\infty/k)$. Note that we can choose the topological generator $\overline{\gamma}$ of $\overline{\Gamma}$ in the form

$$\overline{\gamma} = \gamma^{\ell^r}\sigma \tag{2.5}$$

for some $\sigma \in V$, and the integer $r \geq 0$ is an invariant of the field k. If the R_∞-module A is Λ-torsion and $\mathbf{Z}_\ell$-free, then so is $((V/H) \times \overline{\Gamma})$-module A^H.

Proposition 2.3 *If the group $A_{(0)}$ is finite, then so is the group $(A^H)_{(0)} := A^H/(\overline{\gamma} - 1)$, and its order ℓ^t is given by the formula*

$$t = \nu_\ell\left(\prod_{\chi \in \widehat{V/H}} \prod_{\zeta^{\ell^r}=1} f_A(\zeta\zeta_\chi^{-1} - 1,\, \chi)\right), \tag{2.6}$$

where ζ_χ is defined by the condition

$$\zeta_\chi^{\ell^r} = \chi(\sigma),$$

ζ runs over all the roots of unity of degree ℓ^r, and σ, r are given by (2.5). Let φ be any $\mathbf{Q}_\ell$-irreducible character of $V_0/V_0 \cap H$, and let ℓ^{t_φ} be the order of $(A^H)_{(0),\varphi} = ((A^H)_\varphi)_{(0)}$. Then we have

$$t_\varphi = \nu_\ell\left(\prod_{\substack{\chi \in \widehat{V/H} \\ \chi \mid \varphi}} \prod_{\zeta^{\ell^r}=1} f_A(\zeta\zeta_\chi^{-1} - 1,\, \chi)\right), \tag{2.7}$$

where ζ_χ and ζ are as above.

Proof. Note first that the value $\nu_\ell(f_A(0))$ in (2.4) equals to $\nu_\ell(\prod_{i=1}^{\lambda} \alpha_i)$, where $\alpha_1, \ldots, \alpha_\lambda$ are all the roots of the distinguished polynomial $f_1(T)$ or, equivalently, all the eigenvalues of $\gamma - 1$ on $A \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$. Now let $\alpha(\chi)_1, \ldots, \alpha(\chi)_{\lambda(\chi)}$ be the roots of the distinguished polynomial corresponding to the characteristic series $f_A(T,\chi)$ for some $\chi \in \widehat{G/H}$. An element σ defined in (2.5) acts on $(A^H)_\chi$ as multiplication by $\chi(\sigma)$, thus the operator $\bar{\gamma}$, acting on the $\mathbf{Q}_\ell$-space $(A^H)_\chi \otimes_{\mathbf{Z}_\ell} \mathbf{Q}_\ell$, has the eigenvalues $(1+\alpha(\chi)_1)^{\ell^r}\chi(\sigma), \ldots, (1+\alpha(\chi)_{\lambda(\chi)})^{\ell^r}\chi(\sigma)$. Then by (2.2) and Prop. 2.2 we have

$$t = \nu_\ell \left(\prod_{\chi \in \widehat{V/H}} \prod_{i=1}^{\lambda(\chi)} ((1+\alpha(\chi)_i)^{\ell^r}\chi(\sigma) - 1) \right).$$

As we have

$$(1+\alpha(\chi)_i)^{\ell^r}\chi(\sigma) - 1 = \prod_{\zeta^{\ell^r}=1} ((1+\alpha(\chi)_i)\zeta_\chi - \zeta) = \prod_{\zeta^{\ell^r}=1} \zeta_\chi(1+\alpha(\chi)_i - \zeta_\chi^{-1}\zeta)$$

and

$$f_1(T,\chi) = \prod_{i=1}^{\lambda(\chi)} (T - \alpha(\chi)_i),$$

we get

$$t = \nu_\ell \left(\eta \prod_{\chi \in \widehat{V/H}} \prod_{\zeta^{\ell^r}=1} \prod_{i=1}^{\lambda(\chi)} (\zeta_\chi^{-1}\zeta - 1 - \alpha(\chi)_i) \right) = \nu_\ell \left(\eta \prod_{\chi \in \widehat{V/H}} \prod_{\zeta^{\ell^r}=1} f_A(\zeta\zeta_\chi^{-1} - 1, \chi) \right),$$

where $\eta = \pm 1$. This proves (2.6). The proof of (2.7) is quite analogous.

□

Corollary. In the situation of Prop. 2.3 put $|A_{(n)}| = \ell^{t(n)}$, $|A_{(n),\varphi}| = \ell^{t(n)_\varphi}$, where $A_{(n)} := A/(\gamma_n - 1)$, $\gamma_n = \gamma^{\ell^n}$. Then

$$t(n) = \nu_\ell \left(\prod_{\chi \in \widehat{V}} \prod_{\zeta^{\ell^n}=1} f_A(\zeta - 1, \chi) \right) \tag{2.8}$$

$$t(n)_\varphi = \nu_\ell \left(\prod_{\substack{\chi \in \widehat{V} \\ \chi | \varphi}} \prod_{\zeta^{\ell^n}=1} f_A(\zeta - 1, \chi) \right). \tag{2.9}$$

To prove it, it is enough to apply Prop. 2.3 to the surjective mapping $\tau : G_\infty = V \times \Gamma \to V \times \Gamma/\Gamma_n$, where $\Gamma_n := \langle \gamma_n \rangle$.

□

Now let K_∞ be the cyclotomic $\mathbf{Z}_\ell$-extension of a cyclotomic field $K_0 = \mathbf{Q}(\mu_d, \zeta_0)$. Recall that we have defined in the introduction the R_∞-modules $\mathcal{A}(K_\infty)$ and $H(K_\infty)$ such that we have the natural inclusions $C(K_\infty) \subset \mathcal{A}(K_\infty) \subset H(K_\infty)$. In what follows we work with some fixed K_∞, so instead of $C(K_\infty)$, $\mathcal{A}(K_\infty)$, etc. we shall write C_∞, $\mathcal{A}_\infty$, etc. Let $j \in G_\infty$ be the automorphism of complex conjugation of K_∞. For any R_∞-module A we put

$$A^+ = \{a \in A \mid j(a) = a\}, \quad A^- = \{a \in A \mid j(a) = -a\}.$$

Proposition 2.4 *The groups $\mathcal{A}_\infty$, H_∞ are free Λ-modules of rank $[K_0 : \mathbf{Q}]$. The groups $\mathcal{A}_\infty^+$, H_∞^+ are free Λ-modules of rank $\frac{1}{2}[K_0 : \mathbf{Q}]$.*

Proof. By [6], Lemma 7.2 and Prop. 7.1 H_∞ is Λ-free of rank $[K_0 : \mathbf{Q}]$. There exists the natural exact sequence

$$0 \longrightarrow \mathcal{A}_\infty \longrightarrow H_\infty \longrightarrow \mathcal{D}_\infty \longrightarrow 0,$$

where $\mathcal{D}_\infty$ is a finitely generated free $\mathbf{Z}_\ell$-module generated by all the places $v \mid \ell$ of K_∞. Then, reasoning as in the proof of Theorem 1.1, we get that $\mathcal{A}_\infty$ is Λ-free as well. As H_∞/H_∞^+, $\mathcal{A}_\infty/\mathcal{A}_\infty^+$ are Λ-torsionfree, it follows from [6], Prop. 1.1 that H_∞^+ and $\mathcal{A}_\infty^+$ are free Λ-modules. Using arguments of [6], Section 7 one can prove easily that H_∞^+ and $\mathcal{A}_\infty^+$ are of Λ-rank $\frac{1}{2}[K_0 : \mathbf{Q}]$.

□

Now we are going to compute the characteristic series of the Λ -torsion R_∞-module $\mathcal{A}_\infty/C_\infty$. To do this, we need some further notations and definitions. We may consider any character $\chi \in \widehat{V}$, $V = G(K_0/\mathbf{Q})$ as a primitive Dirichlet character of conductor $f_\chi \mid dq$, where $q = \ell$ if $\ell \neq 2$; $q = 4$ if $\ell = 2$. Any such χ is a character of the first kind in the sense of Iwasawa [3]. For any such χ define the idempotent

$$e_\chi = \mid V \mid^{-1} \sum_{\chi \in V} \overline{\chi}(\sigma)\sigma, \text{ where } \overline{\chi}(\sigma) = \chi(\sigma)^{-1}.$$

Put

$$e^+ = \frac{1+j}{2}, \quad e^- = \frac{1-j}{2}.$$

As in [12], formula (3.3), we define the "minus component" of the Stickelberger element $s(a, \ell^{n+1+\delta}d)$, $a \not\equiv 0 \pmod{\ell^{n+1+\delta}d}$ corresponding to the field K_n of conductor $\ell^{n+1+\delta}d$ by

$$e^- s(a, \ell^{n+1+\delta}d) = \sum_{\substack{i \pmod{\ell^{n+1+\delta}} \\ (i,\ell d)=1}} \left(-\left\langle \frac{ai}{\ell^{n+1+\delta}d} \right\rangle + \frac{1}{2}\right) \sigma_i^{-1} \in \mathbf{Q}_\ell[G(K_n/\mathbf{Q})],$$

where $\langle x \rangle$ denote the unique rational x', $0 \le x' < 1$, such that $x \equiv x' \pmod{\mathbf{Z}}$, and σ_i is the element of $G(K_n/\mathbf{Q})$ sending ε into ε^i for any $\varepsilon \in \mu(K_n)$. The elements $e^- s(a, \ell^{n+1+\delta}d)$ are compatible for different n with respect to the natural projections $\mathbf{Q}_\ell[G(K_{n_2}/\mathbf{Q})] \to \mathbf{Q}_\ell[G(K_{n_1}/\mathbf{Q})]$ for any $n_2 > n_1$. Thus, passing to the inverse limit, we get the element

$$s(a, \ell^\infty d) := \varprojlim e^- s(a, \ell^{n+1+\delta}d) \in \varprojlim \mathbf{Q}_\ell[G(K_n/\mathbf{Q})].$$

It is well known (see [12], Sect. 3) that $(\sigma_i - i) \cdot s(a, \ell^\infty d) \in R_\infty$ for any i prime with $d\ell$. So we can consider $s(a, \ell^\infty d)$ as an element of $L[V]$, where L is the quotien field of Λ. It follows just from the definition of the Iwasawa series given in [3] that in the quotien field of the ring $R_{\infty,\chi} = \mathcal{O}_\chi[[T]]$ the equality

$$\frac{1}{2} e_\chi s(1, \ell^\infty f_\chi) = f(T, \chi) \tag{2.10}$$

holds true. Here χ is an odd character (i.e. $\chi(-1) = -1$) of the first kind with conductor f_χ and $f(T, \chi)$ is the Iwasawa series corresponding to χ. In [3] $f(T, \chi)$ is referred to as the series corresponding to the even character $\theta = \overline{\chi}\omega$, where ω is the Teichmüller character, $\omega : V \to \mathbf{Z}_\ell^*$, $\omega(\sigma_i) \equiv i \pmod{q}$ for any $\sigma_i \in V$. It was proved in [3] that $f(T, \chi) \in \mathcal{O}_\chi[[T]]$ if $\chi \neq \omega$. If $\chi = \omega$, then

$$f(T, \omega) = \left(1 - \frac{\kappa}{1+T}\right)^{-1} \eta(T, \omega),$$

where $\eta(T, \omega)$ is an invertible element of $\mathbf{Z}_\ell[[T]]$ and $\kappa \in 1 + \mathbf{Z}_\ell$ is defined by the formula $\gamma(\zeta_n) = \zeta_n^\kappa$ for any $n \ge 0$. Put

$$Y(K_n) := \prod_{v \mid \ell} \mu_\ell(K_{n,v}),$$

where $K_{n,v}$ is a completion of K_n with respect to v, and put $Y_\infty := \varprojlim Y(K_n)$, where the inverse limit is taken with respect to the norm maps. Note that as a $\mathbf{Z}_\ell$-module Y_∞ is isomorphic to $\mathcal{D}_\infty$ from the proof of Prop. 2.4.

Theorem 2.1 *Let $h(T,\theta)$ (resp. $y(T,\theta)$) be the characteristic series of the Λ-torsion R_∞-module $\mathcal{A}^+_\infty/C_\infty$ (resp. Y_∞) corresponding to an even character of the first kind θ. Then putting $\overline{\theta}(\sigma)=\theta(\sigma)^{-1}$, we have*

$$h(T,\theta)=f\left(\frac{\kappa}{1+T}-1,\,\overline{\theta}\omega\right)\,y(T,\theta)^{-1}\text{ if }\theta\neq 1, \tag{2.11}$$

$$h(T,\theta)=\eta\left(\frac{\kappa}{1+T}-1,\,\omega\right)y(T,\,1)^{-1}= \tag{2.12}$$

$$(-T)f\left(\frac{\kappa}{1+T}-1,\omega\right)y(T,1)^{-1}\ \text{ if }\theta=1.$$

Proof. We shall deduce (2.11) and (2.12) from [8], Theorem 4.1. To formulate this last statement we need some definitions. Let S'_∞ be the R_∞-module generated in $L[V]$ by the elements $s(a,\ell^\infty d)$ for all $a\in\mathbf{Z}\setminus\{0\}$. It can be checked easily that S'_∞ is generated as a R_∞-module by the set $s(a,\ell^\infty d)$ for all $a\in\mathbf{Z}\setminus\{0\}$, $a=1,\dots,dq$. So S'_∞ is a finitely generated R_∞-module. We define the Stickelberger ideal in R_∞ as $S_\infty:=S'_\infty\cap R_\infty$. In [8] we have defined for the field K_∞ a free R_∞-module on one generator $V(K_\infty)$ such that $\mathcal{A}(K_\infty)\in V(K_\infty)$ and (noncanonically)

$$V(K_\infty)/\mathcal{A}(K_\infty)\cong Y_\infty, \tag{2.13}$$

(see [8], (1.10)). Let $\kappa: G_\infty\to\mathbf{Z}_\ell^*$ be the cyclotomic character defined by $\zeta_n^\sigma=\zeta_n^{\kappa(\sigma)}$ for $n=1,2,\dots$ We define the automorphism $w: R_\infty\to R_\infty$ by $w(\sigma)=\kappa(\sigma)\sigma^{-1}$ for any $\sigma\in G_\infty$.

Theorem C *([8], Theorem 4.1). For given K_∞ we have*

$$C_\infty = w(S_\infty)V(K_\infty)$$

$$P_\infty = w(S'_\infty)V(K_\infty).$$

The Λ-torsion modules $V(K_\infty)^+/C_\infty$ and $R^+_\infty/w(S_\infty)$ are isomorphic as R_∞-modules.

As is well known (and may be easily deduced from Lemma 2.1 of [12]), the characteristic series of the Λ-torsion R_∞-module R^-_∞/S_∞ are the Iwasawa series for odd χ, $\chi \neq \omega$, and $\eta(T,\omega)$ for $\chi = \omega$. By the theorem of Ferrero-Washington R^-_∞/S_∞ is finitely generated over Z_ℓ. Therefore R^-_∞/S_∞ has trivial Iwasawa series for even characters χ. Thus, $V(K_\infty)^+/C_\infty$ has trivial characteristic series for odd characters χ. As $w(\gamma) = \kappa\gamma^{-1}$, we have $w(T) = \frac{\kappa}{1+T} - 1$. The automorphism w maps $(R^-_\infty/S_\infty)_\chi$ onto $(R^+_\infty/w(S_\infty))_{\overline{\chi}\omega}$. Hence by Theorem C the characteristic series of $V(K_\infty)^+/C_\infty$ corresponding to the even character θ coincides with $f(\frac{\kappa}{1+T} - 1, \overline{\theta}\omega)$ if $\theta \neq 1$ (resp. with $\eta(\frac{\kappa}{1+T} - 1, \omega)$ if $\theta = 1$). Taking into account (2.13) and (2.3), we get (2.11). To get (2.12) it is enough to note that the θ-component $Y_{\infty,\theta}$ is finite for $\theta = 1$.

□

3 The calculation of some characteristic series

Let K_∞ be as in Section 2. Let $\overline{M}_\infty$ be the maximal unramified abelian ℓ-extension of K_∞ and M_∞ be the maximal subextension of $\overline{M}_\infty/K_\infty$ such that ℓ is completely decomposed in M_∞/K_∞. Put $\overline{T}_\ell(K_\infty) := G(\overline{M}_\infty/K_\infty)$, $T_\ell(K_\infty) = G(M_\infty/K_\infty)$. Let $R_\ell(K_\infty)$ be the kernel of the natural surjection $\overline{T}_\ell(K_\infty) \to T_\ell(K_\infty)$. So the group $R_\ell(K_\infty) = G(\overline{M}_\infty/M_\infty)$ coincides with the subgroup of $\overline{T}_\ell(K_\infty)$ generated by the decomposition subgroups of all the places over ℓ. Note that $\overline{T}_\ell(K_\infty)$, $T_\ell(K_\infty)$ and $R_\ell(K_\infty)$ are R_∞-modules in a natural way.

The next theorem, known as the "Main Conjecture of Iwasawa theory," gives the characteristic series of $\overline{T}_\ell(K_\infty)$ corresponding to the odd character χ of the first kind or, equivalently, the characteristic series of $\overline{T}_\ell(K_\infty)^-$ for all χ of the first kind.

Theorem D *For any odd character of the first kind $\chi \neq \omega$ the corresponding characteristic series of $\overline{T}_\ell(K_\infty)$ coincides with the Iwasawa series $f(T,\chi)$. The characteristic series of $\overline{T}_\ell(K_\infty)$ for $\chi = \omega$ coincides with $\eta(T,\omega)$ (and thus is invertible).*

This theorem was proved in [10] (for odd ℓ) and in [14] (for $\ell = 2$). Another proof for $K_\infty = \bigcup_{n=1}^{\infty} \mathbf{Q}(\zeta_n)$, based on Euler systems of Kolyvagin was given by Rubin [9] (see also [11]). Put $\mathbf{Z}_\ell(1) = \varprojlim \mu_\ell(K_n)$. For any R_∞-module A finitely generated over $\mathbf{Z}_\ell$ we turn $\mathrm{Hom}_{\mathbf{Z}_\ell}(A,\ \mathbf{Z}_\ell(1))$ into a R_∞-module putting $(\sigma\chi)(a) = \kappa(\sigma)\chi(\sigma^{-1}(a))$ for any $\sigma \in G_\infty$, $\chi \in \mathrm{Hom}_{\mathbf{Z}_\ell}(A,\ \mathbf{Z}_\ell(1))$, $a \in A$.

Proposition 3.1 *The R_∞-modules $\mathcal{A}^+_\infty/C_\infty$ and $\mathrm{Hom}_{\mathbf{Z}_\ell}(T_\ell(K_\infty)^-,\ \mathbf{Z}_\ell(1))$ have the same characteristic series for any character.*

Proof. For any odd character of the first kind χ put $\theta = \overline{\chi}\omega$. Then R_∞-modules $\mathrm{Hom}_{\mathbf{Z}_\ell}\left((\overline{T}_\ell(K_\infty)^-)_\chi,\ \mathbf{Z}_\ell(1)\right)$ and $\left(\mathrm{Hom}_{\mathbf{Z}_\ell}\left(\overline{T}_\ell(K_\infty)^-,\ \mathbf{Z}_\ell(1)\right)\right)_\theta$ are quasi-isomorphic and therefore have the same characteristic series. By Theorem D the module $(\overline{T}_\ell(K_\infty)^-)_\chi = \overline{T}_\ell(K_\infty)_\chi$ has the only nontrivial characteristic series $f(T,\chi)$ corresponding to χ ($\eta(T,\omega)$ if $\chi = \omega$). If $\alpha_1, \ldots, \alpha_r$ are all the zeroes of this series then $1+\alpha_1, \ldots, 1+\alpha_r$ are all the eigenvalues of γ acting on $\overline{T}_\ell(K_\infty)_\chi \otimes_{\mathcal{O}_\chi} L_\chi)$, where L_χ is the quotien field of $\mathcal{O}_\chi$. Then γ, considering as an operator on the L_χ-space $\left(\mathrm{Hom}_{\mathbf{Z}_\ell}(\overline{T}_\ell(K_\infty)^-,\ \mathbf{Z}_\ell(1)\right)_\theta \otimes_{\mathcal{O}_\chi} L_\chi$, has the eigenvalues $\beta_1 = \kappa(1+\alpha_1)^{-1}, \ldots, \beta_r = \kappa(1+\alpha_r)^{-1}$. The direct checking shows that $\beta_1 - 1, \ldots, \beta_r - 1$ are all the zeroes of the series

$$(3.1) \qquad g(T,\theta) = f\left(\frac{\kappa}{1+T} - 1,\ \overline{\theta}\omega\right),\ \text{if } \theta \neq 1,$$

$$(3.2) \qquad g(T,\theta) = \eta\left(\frac{\kappa}{1+T} - 1,\ \overline{\theta}\omega\right)\ \text{if } \theta = \omega.$$

satisfying the condition $\nu_\ell(\beta_i - 1) > 0$ for $i = 1, \ldots, r$. Therefore $\beta_1 - 1, \ldots, \beta_r - 1$ are all the roots of the distinguished polynomial associated with $g(T,\theta)$.

Hence $g(T,\theta)$ is the characteristic series of $\mathrm{Hom}_{\mathbf{Z}_\ell}(\overline{T}_\ell(K_\infty)^-,\ \mathbf{Z}_\ell(1))$ for any even character of the first kind θ. Now consider the natural sequence

$$(3.3)\qquad 0 \longrightarrow R_\ell(K_\infty)^- \longrightarrow \overline{T}_\ell(K_\infty)^- \longrightarrow T_\ell(K_\infty)^- \longrightarrow 0.$$

The sequence (3.3) is exact up to finite groups. Let $\mathcal{D}_\infty$ be the R_∞-module from the proof of Prop. 2.4. Then $\mathcal{D}_\infty \cong \mathbf{Z}_\ell[G_\infty/G_{\infty,v}]$ as a R_∞-module, where $G_{\infty,v}$ is the decomposition subgroup of any $v \mid \ell$ in G_∞. We have the natural surjective map $f : \mathcal{D}_\infty \to R_\ell(K_\infty)$ that sends any place $v \mid \ell$ into the Frobenius automorphism of its decomposition subgroup in $\overline{T}_\ell(K_\infty)$. The mapping f induces the mapping $f^- : \mathcal{D}_\infty^- \longrightarrow R_\ell(K_\infty)^-$ which is known to be a quasi-isomorphism (even an isomorphism if $\ell \neq 2$). It follows from the explicit form of $\mathcal{D}_\infty$ and Y_∞ that

$$\mathrm{Hom}_{\mathbf{Z}_\ell}(\mathcal{D}_\infty,\ \mathbf{Z}_\ell(1)) \cong Y_\infty \text{ (noncanonically).}$$

Thus, we have a quasi-isomorphism

$$(3.4)\qquad \mathrm{Hom}_{\mathbf{Z}_\ell}(\mathcal{D}_\infty^-,\ \mathbf{Z}_\ell(1)) \cong Y_\infty^+.$$

Combining Theorem 2.1 with (3.1), (3.2), (3.3), (3.4) and noting that $(Y_\infty)_\theta$ is finite for $\theta = 1$, we get our proposition.

□

For any K_n and its group of units $U(K_n)$ we put $\overline{U}(K_n) := U(K_n)/\mu(K_n)$ and $U_\infty = \varprojlim(\overline{U}(K_n)[\ell])$, where the inverse limit is taken with respect to the norm maps. We have the natural inclusion $C_\infty \subseteq U_\infty \subseteq \mathcal{A}_\infty^+$, and thus, the exact sequence

$$(3.5)\qquad 0 \longrightarrow U_\infty/C_\infty \longrightarrow \mathcal{A}_\infty^+/C_\infty \longrightarrow \mathcal{A}_\infty^+/U_\infty \longrightarrow 0.$$

Let $U_S(K_n)$ be the group of S-units of K_n, where S is the set of all the places over ℓ in K_n. Put $\overline{U}_S(K_n) := U_S(K_n)/\mu(K_n)$ and $U_{S,\infty} := \varprojlim \overline{U}_S(K_n)[\ell]$, where the inverse limit is taken with respect to the norm maps. Note that we have the natural inclusion $U_{S,\infty} \subseteq H(K_\infty)^+$.

If k is any real abelian field and k_∞ is the cyclotomic $\mathbf{Z}_\ell$-extension of k then we can define the abelian pro-ℓ-groups $H(k_\infty)$, $\mathcal{A}(k_\infty)$, $U(k_\infty)$ and $U_S(k_\infty)$ in the same manner. If $k_\infty \subseteq K_\infty$ for some cyclotomic field $K = K_0$, then we can consider all these groups as R_∞-modules.

Proposition 3.2 *The R_∞-modules $\mathcal{A}^+_\infty/U_\infty$ and $H^+_\infty/U_{S,\infty}$ are quasi-isomorphic. If k is any real abelian field, k_∞ is the cyclotomic $\mathbf{Z}_\ell$-extension of k and $k_\infty \subseteq K_\infty$ for some cyclotomic K then the R_∞-modules $\mathcal{A}(k_\infty)/U(k_\infty)$ and $H(k_\infty)/U_S(k_\infty)$ are quasi-isomorphic.*

Proof. As we have $U_\infty = U_{S,\infty} \cap \mathcal{A}^+_\infty$, the natural mapping

$$i : \mathcal{A}^+_\infty/U_\infty \longrightarrow H^+_\infty/U_{S,\infty}$$

is an injection. Thus it is enough to check that i has a finite cokernel. To do this, we shall give class field theoretic interpretation of the groups in question. Let N_∞ be the maximal ℓ-ramified abelian ℓ-extension of K_∞, and put $X_\infty := G(N_\infty/K_\infty)$. Then we have the natural exact sequences of R_∞-modules

$$(3.6) \qquad 0 \longrightarrow W_\infty \longrightarrow X_\infty \longrightarrow T_\ell(K_\infty) \longrightarrow 0,$$

$$(3.7) \qquad 0 \longrightarrow \overline{W}_\infty \longrightarrow X_\infty \longrightarrow \overline{T}_\ell(K_\infty) \longrightarrow 0,$$

where W_∞ (resp. $\overline{W}_\infty$) is the subgroup of X_∞ generated by the decomposition subgroups (resp. by the inertia subgroups) of all the places $v \mid \ell$ of K_∞. Let $f : Y_\infty \to X_\infty$ be the natural map defined by the class field theory. Then $\operatorname{Im} f \subset \overline{W}_\infty \subseteq W_\infty$, and it follows from class field theory that

$$W_\infty/\operatorname{Im} f \cong H_\infty/U_{S,\infty}, \;\; \overline{W}_\infty/\operatorname{Im} f \cong \mathcal{A}_\infty/U_\infty.$$

Thus

$$W_\infty/\overline{W}_\infty = R_\ell(K_\infty) \cong H_\infty/(\mathcal{A}_\infty \cdot U_{S,\infty}) \supset \operatorname{Coker} i = H^+_\infty/\mathcal{A}^+_\infty \cdot U_{S,\infty},$$

Therefore $\operatorname{Coker} i \subset R_\ell(K_\infty)^+$. Note that the group $R_\ell(K_\infty)^+$ is finitely generated. On the other hand, by Leopoldt conjecture there is no noncyclotomic $\mathbf{Z}_\ell$-extension over K_n^+ for any n. Thus $R_\ell(K_\infty)^+$ is torsion, hence finite. Thus $\operatorname{Coker} i$ is finite, hence i is a quasi-isomorphism.

A quasi-isomorphism between $\mathcal{A}(k_\infty)/U(k_\infty)$ and $H(k_\infty)/U_S(k_\infty)$ can be established in the same way.

□

Theorem 3.1 *The R_∞-modules $T_\ell(K_\infty)^+$ and U_∞/C_∞ have the same characteristic series (for any even character of the first kind θ).*

Proof. We shall deduce our Theorem from some duality results of [7]. Put $\overline{X}_\infty := X_\infty/f(Y_\infty)$ and $\mathcal{A}_\ell(K) = \overline{X}_\infty/H_\infty^-$, where X_∞, Y_∞ are as in the proof of Prop. 3.2. Then we have

Theorem E. *The R_∞-modules $2\mathcal{A}_\ell(K)$ and $\mathrm{Hom}_{\mathbf{Z}_\ell}(2\mathcal{A}_\ell(K),\ \mathbf{Z}_\ell(1))$ are quasi-isomorphic.*

Indeed, if $\ell \neq 2$ then by the Ferrero-Washington theorem $\mathcal{A}_\ell(K)$ is finitely generated over $\mathbf{Z}_\ell$. Then by [7], Corollary of Theorem 4.1, we have $\mathcal{A}_\ell(K) \cong \mathrm{Hom}_{\mathbf{Z}_\ell}(\mathcal{A}_\ell(K),\ \mathbf{Z}_\ell(1))$. Although the case $\ell = 2$ was not considered explicitly in [7], it was noted that all the results of that paper are correct for $\ell = 2$ up to subgroups and quotiens of exponent 2. If $\ell = 2$ then $2\mathcal{A}_\ell(K)$ is finitely generated over $\mathbf{Z}_\ell$, and repeating the proof of Theorem 4.1 of [7], we get the statement of Theorem E.

□

It follows from Theorem E that we have a quasi-isomorphism

(3.8) $$2\mathcal{A}_\ell(K)^+ \sim \mathrm{Hom}_{\mathbf{Z}_\ell}(2\mathcal{A}_\ell(K)^-,\ \mathbf{Z}_\ell(1)).$$

The definition of $\mathcal{A}_\ell(K)$ and (3.6) show that

(3.9) $$2\mathcal{A}_\ell(K)^- \sim T_\ell(K_\infty)^-$$

Therefore $2\mathcal{A}_\ell(K)^+$ enters the exact sequence

(3.10) $$0 \longrightarrow 2H_\infty/(2H_\infty \cap (H_\infty^- \cdot U_{S,\infty})) \xrightarrow{\alpha} 2\mathcal{A}_\ell(K)^+ \xrightarrow{\beta} 2T_\ell(K_\infty)^+$$

with finite coker β.

It follows from Prop. 3.1 and formulae (3.8), (3.9) that $2\mathcal{A}_\ell(K)^+$ and $\mathcal{A}^+_\infty/C_\infty$ have the same characteristic series. Then it follows from Prop. 3.2 that

$$2H_\infty/(2H_\infty \cap (H^-_\infty \cdot U_{S,\infty})) \sim H^-_\infty/U_{S,\infty} \sim \mathcal{A}^+_\infty/U_\infty.$$

Then we get from (3.5), (3.10) and Prop. 2.1 that U_∞/C_∞ and $T_\ell(K_\infty)^+$ have the same characteristic series.

□

Now let k be any real abelian field, k_∞ be the cyclotomic $\mathbf{Z}_\ell$-extension of k and $k_\infty \subset K_\infty$ for a suitable choice of the cyclotomic field $K = K_0$.

Theorem 3.2 *Let k_∞ and K_∞ be as before. Put $H = G(K_\infty/k_\infty)$. Then the R_∞-modules $T_\ell(k_\infty)$ and U^H_∞/C^H_∞ have the same characteristic series.*

Proof. We have quasi-isomorphisms $T_\ell(k_\infty) \sim T_\ell(K_\infty)^H$, $U^H_\infty/C^H_\infty \sim (U_\infty/C_\infty)^H$, so our theorem follows immediately from Theorem 3.1.

□

4 The proof of Theorem 3

Let k, k_∞, K_∞, R_∞ and $H = G(K_\infty/k_\infty)$ be as in Section 3. Note that we have R_∞-modules $H(k_\infty)$, $U_S(k_\infty)$, and these modules are fixed under the action of H. Put $\widetilde{H}(k_\infty) := (H_\infty)^H$, $\widetilde{U}_S(k_\infty) := (U_{S,\infty})^H$, $\widetilde{C}(k_\infty) := (C_\infty)^H$. then by [6], Prop. 1.1 the R_∞-modules $\widetilde{H}(k_\infty)$, $\widetilde{U}_S(k_\infty)$, $\widetilde{C}(k_\infty)$ are Λ-free. Let $H(k)$ (resp. $\widetilde{H}(k)$) be the image of the natural projection $H(k_\infty) \to \mathcal{B}(k)$ (resp. $\widetilde{H}(k_\infty) \to \mathcal{B}(k)\otimes_{\mathbf{Z}_\ell}\mathbf{Q}_\ell$). Let $U^*_S(k)$ (resp. $\widetilde{U}^*_S(k)$) be the image of the natural projection $U_S(k_\infty) \to H(k)$ (resp. $\widetilde{U}_S(k_\infty) \to \widetilde{H}(k)$). put $\widehat{U}_S(k) := \overline{U}_S(k)[\ell] \cap H(k)$. Thus, $\widehat{U}_S(k)$ is the subgroup of all the elements of $\overline{U}_S(k)[\ell]$ that are local universal norms from k_∞. Put

$$\widetilde{C}_S(k_\infty) := \left\{x \in \widetilde{H}(k_\infty) \mid (\gamma_n - 1)x \in \widetilde{C}(k_\infty) \text{ for some } n\right\},$$

$$C_S(k_\infty) := \widetilde{C}_S(k_\infty) \cap U_S(k_\infty).$$

It follows from the definition and from Prop. 3.2 that the modules $\widetilde{H}(k_\infty)/\widetilde{C}_S(k_\infty)$ and $(\mathcal{A}_\infty^+/C_\infty)^H$ are quasi-isomorphic.

Let $\widetilde{C}_S(k)$ (resp. $C_S(k)$) be the image of the natural projection $\widetilde{C}_S(k_\infty) \to \widetilde{H}(k)$ (resp. $C_S(k_\infty) \to H(k)$). We shall call the group $C_S(k)$ the group of circular S-units. The following proposition makes clear the connection between all these groups.

Proposition 4.1 *There exist natural inclusions*

$$(4.1) \qquad \widetilde{H}(k) \supseteq \widetilde{U}_S^*(k) \supseteq \widetilde{C}_S(k),\ H(k) \supseteq \widehat{U}_S(k) \supseteq U_S^*(k) \supseteq C_S(k)$$

such that all the indices that appear in (4.1) *are finite.*
If $\ell \neq 2$, *then* $H(k) = \widetilde{H}(k_\infty)$, $U_S(k_\infty) = \widetilde{U}_S(k_\infty)$, $C_S(k_\infty) = \widetilde{C}_S(k_\infty)$, $H(k) = \widetilde{H}(k)$, $U_S^*(k) = \widetilde{U}_S^*(k)$ *and* $C_S(k) = \widetilde{C}_S(k)$.

If $\ell = 2$ *and* $\sqrt{-1} \in k_{\infty,v}$ *for some* $v \mid \ell$ *(hence for any* $v \mid \ell$ *), then* $H(k_\infty) = \widetilde{H}(k_\infty)$, $H(k) = \widetilde{H}(k)$.

If $\ell = 2$ *and* $\sqrt{-1} \notin k_{\infty,v}$ for $v \mid \ell$, *then*

$$\widetilde{H}(k_\infty)/H(k_\infty) \cong \prod_{v \mid \ell} \mu_\ell(k_{\infty,v}) \cong (\mathbf{Z}/2\mathbf{Z})^r,$$

where r *is the number of places* $v \mid \ell$ *in* k_∞.

If $\ell = 2$, *then in any case we have*

$$(4.2) \qquad [\widetilde{U}_S(k_\infty) : U_S(k_\infty)] = [\widetilde{C}_S(k_\infty) : C_S(k_\infty)] = [\widetilde{U}_S^*(k) : U_S^*(k)] =$$

$$[\widetilde{C}_S(k) : C_S(k)] = 2,$$

$$(4.3) \qquad \widetilde{U}_S(k)/\widetilde{C}_S(k) = U_S^*(k)/C_S(k).$$

Proof. If $\overline{\Gamma} = G(k_\infty/k)$, then for any sufficiently large n the natural projection $G_\infty \to G(k_\infty/\mathbf{Q})$ maps Γ_n onto $\overline{\Gamma}_{n-s}$, where $s \geq 0$ does not depend on n. The natural inclusion $\widetilde{H}(k_\infty)/\widetilde{U}_S(k_\infty) \subseteq H_\infty^+/U_{S,\infty}$ induces for all sufficiently large n the inclusion

$$(\widetilde{H}(k_\infty)/\widetilde{U}_S(k_\infty))^{\overline{\Gamma}_{n-s}} \subseteq (H_\infty^+/U_{S,\infty})^{\Gamma_n}.$$

By [6], Lemma 7.2 and Theorem 7.2 the Λ-modules H_∞ and $U_{S,\infty}$ are free. Hence H_∞^+ is Λ-free and $H_\infty^+/U_{S,\infty}$ does not contain any nontrivial finite submodule. On the other hand, the module $(H_\infty^+/U_{S,\infty})^{\Gamma_n}$ does not contain any Λ-submodule that is Λ-isomorphic to $\mathbf{Z}_\ell$ because of the Leopoldt conjecture. Thus $(H_\infty^+/U_{S,\infty})^{\Gamma_n} = 0$ and $\left(\widetilde{H}(k_\infty)/\widetilde{U}_S(k_\infty)\right)^{\overline{\Gamma}_n} = 0$ for all sufficiently large n. It follows from the definition of $\widetilde{C}_S(k_\infty)$ and the last equality that $\widetilde{C}_S(k_\infty) \subseteq \widetilde{U}_S(k_\infty)$. Therefore $\widetilde{C}_S(k_\infty) \subseteq \widetilde{U}_S(k_\infty)$, and $\widetilde{C}_S(k) \subseteq \widetilde{U}_S^*(k)$, $C_S(k) \subseteq U_S^*(k)$. The other inclusions of (4.1) are obvious.

By Theorem 1.1 H_∞^+/C_∞ is Λ-torsion, hence $\widetilde{H}(k_\infty)/\widetilde{C}_S(k_\infty)$ is $\overline{\Gamma}$-torsion, and it follows from the definition of $\widetilde{C}_S(k_\infty)$ that $\left(\widetilde{H}(k_\infty)/\widetilde{C}_S(k_\infty)\right)^{\overline{\Gamma}_n} = 0$ for any n. As $\widetilde{H}(k_\infty)$ and $\widetilde{C}_S(k_\infty)$ are $\overline{\Gamma}$-free, we get the natural exact sequence (see [6], (1.2))

$$(4.4) \qquad 0 = \left(\widetilde{H}(k_\infty)/\widetilde{C}_S(k_\infty)\right)^{\overline{\Gamma}} \longrightarrow \widetilde{C}_S(k_\infty)_{(0)} \longrightarrow \widetilde{H}(k_\infty)_{(0)} \longrightarrow \left(\widetilde{H}(k_\infty)/\widetilde{C}_S(k_\infty)\right)_{(0)} \longrightarrow 0,$$

where $A_{(0)} = A/(\overline{\gamma}-1)A$ for any $\overline{\Gamma}$-module A.

It follows from the local class field theory that $\widetilde{H}(k_\infty)_{(0)} \cong \widetilde{H}(k)$. Hence (4.4) shows that $\widetilde{C}_S(k_\infty)_{(0)} \cong \widetilde{C}_S(k)$ and

$$(4.5) \qquad \left(\widetilde{H}(k_\infty)/\widetilde{C}_S(k_\infty)\right)_{(0)} \cong \widetilde{H}(k)/\widetilde{C}_S(k).$$

As $\widetilde{H}(k_\infty)$ and $\widetilde{C}_S(k_\infty)$ are $\overline{\Gamma}$-free modules of the same rank, the groups $\widetilde{C}_S(k_\infty)_{(0)}$ and $\widetilde{H}(k_\infty)_{(0)}$ are free $\mathbf{Z}_\ell$-modules of the same rank. Then (4.4) shows that the groups in (4.5) are finite. From this and from the equalities $C_S(k) = \widetilde{C}_S(k)$ if $\ell \neq 2$, $[\widetilde{C}_S(k) : C_S(k)] = 2$ if $\ell = 2$, that will be proved below, we get the finitness of all the indices in (4.1).

If $\ell \neq 2$, then by [6], Lemma 7.2 we have that H_∞ is Γ-free and $H(k_\infty)$ is $\overline{\Gamma}$-free. Consider the inclusions $\widetilde{H}(k_\infty) \supseteq H(k_\infty) \supseteq N_H(H_\infty)$, where $H = G(K_\infty)/k_\infty)$. It follows from the local class field theory that the Tate cohomology group $H^0(H, H_\infty)$ is finite and therefore $[\widetilde{H}(k_\infty) : H(k_\infty)] < \infty$. As both modules in question are $\overline{\Gamma}$-free, we get that $\widetilde{H}(k_\infty) = H(k_\infty)$.

The equality $\widetilde{U}_S(k_\infty) = U_S(k_\infty)$ can be proved by the same reasoning. It follows from [6], Theorem 7.2 that $U_{S,\infty}$ is Γ-free and $U_S(k_\infty)$ is $\overline{\Gamma}$-free. The orders of the Tate groups $H^0(H, \overline{U}_S(K_n))$ can be majorated in terms of the number of generators of the ℓ-class groups $\mathrm{Cl}(K_n)$. So the finiteness of $H^0(H, U_{S,\infty})$ follows from the triviality of the Iwasawa μ-invariant of K_∞.

Then we get $\widetilde{C}_S(k_\infty) = C_S(k_\infty)$, $\widetilde{H}(k) = H(k)$, $\widetilde{U}_S^*(k) = U_S^*(k)$. This proves the proposition if $\ell \neq 2$.

If $\ell = 2$ and $\sqrt{-1} \in k_{\infty,v}$ for any $v \,|\, \ell$, then applying [6], Lemma 7.2, we get again that $H(k_\infty)$ is $\overline{\Gamma}$-free and $\widetilde{H}(k_\infty) = H(k_\infty)$.

If $\ell = 2$ and $\sqrt{-1} \notin k_{\infty,v}$ for any $v|\ell$, then Lemma 7.2 of [6] needs some correction. The correct statement (which can be proved easily using local class field theory) asserts that in this case $H(k_\infty)$ is a $\overline{\Gamma}$-module without torsion and there exists an inclusion $H(k_\infty) \hookrightarrow F$, where F is $\overline{\Gamma}$-free and $F/H(k_\infty) \cong \prod_{v|\ell} \mu_\ell(k_{\infty,v})$ as a Galois module (note that $\mu_\ell(k_{\infty,v}) = \{\pm 1\}$ for any $v|\ell$).

If $\ell = 2$ and $\sqrt{-1} \notin k_\infty$ (this is the case if k is real abelian) then Theorem 7.2 of [6] also needs a correction. In this case the correct statement asserts that $U_S(k_\infty)$ is isomorphic to a submodule of index 2 of some $\overline{\Gamma}$-free module. Indeed, Theorem 7.2 and its proof given in [6] are valid for the field $k_\infty' = k_\infty(\sqrt{-1})$. Thus $U_S(k_\infty')$ is $\overline{\Gamma}$-free. It follows from the Kummer theory that $[U_S(k_\infty') : U_S(k_\infty)] \leq 2$. On the other hand, $U_S(k_\infty)$ is not $\overline{\Gamma}$-free. This last assertion follows from [6], Prop. 1.2, and the observation that -1 is in the image of the natural projection $U_S(k_\infty) \to U_S(k_n)[\ell]$ (it is sufficient to check it for $k = \mathbf{Q}$. Hehce we have $[U_S(k_\infty') : U_S(k_\infty)] = 2$ as desired. Moreover, we have $\widetilde{U}_S(k_\infty) = U_S(k_\infty')$.

Now consider the circular number $\varepsilon_\infty(1) = \varprojlim(1 - \zeta_n) \in U_S(k_\infty')$. As was shown by Sinnott (see [12], Section 1), for any n we have

$$1 - \zeta_n \notin U_S(k_n) \cdot \mu(k_n(\sqrt{-1})). \tag{4.6}$$

It means that $\varepsilon_\infty(1) \notin U_S(k_\infty)$. As it follows from the definition of $\widetilde{C}(k_\infty)$ that $\varepsilon_\infty(1) \in \widetilde{C}_S(k_\infty)$, we get the first two indices of (4.2) equal to 2. Let n_0 be the maximal index such that $\zeta_{n_0} \in k(\sqrt{-1})$. Then the natural projection $\widetilde{C}_S(k_\infty) \to \widetilde{C}_S(k)$ sends $\varepsilon_\infty(1)$ into $(1 - \zeta_{n_0})$. Then (4.6) implies $\widetilde{U}_S^*(k) \neq U_S^*(k)$, $\widetilde{C}_S(k) \neq C_S(k)$. As $[\widetilde{U}_S(k_\infty) : U_S(k_\infty)] \geq [\widetilde{U}_S^*(k) : U_S^*(k)]$ and $[\widetilde{C}_S(k_\infty) : C_S(k_\infty)] \geq [\widetilde{C}_S(k) : C_S(k)]$, we get that the last two indices of (4.2) equal to 2 as well. This proves (4.2) completely.

To prove (4.3) it is sufficient to note that $\widetilde{U}_S(k) = U_S^*(k) \times < (1 - \zeta_{n_0}) >$ and $\widetilde{C}_S(k) = C_S(k) \times < (1 - \zeta_{n_0}) >$.

□

Proposition 4.2 *There exist natural isomorphisms of the finite abelian groups*

$$(\widetilde{H}(k_\infty)/\widetilde{C}_S(k))_{(0)} \cong \widetilde{H}(k)/\widetilde{C}_S(k),$$

$$(\widetilde{U}_S(k_\infty)/\widetilde{C}_S(k_\infty))_{(0)} \cong \widetilde{U}_S(k)/\widetilde{C}_S(k).$$

Proof. The first formula is already proved (see (4.5)). The last one can be proved in the same way using the fact that $\widetilde{U}_S(k_\infty)$ is Λ-free and hence $\overline{\Gamma}$-free.

□

Proposition 4.3 *([6], Prop. 7.5). There esists a natural isomorphism*

$$T_\ell(k_\infty)^{\overline{\Gamma}} \cong \widetilde{U}_S(k)/U_S^*(k).$$

For the convinience of the reader we give here a short and selfcontained proof of this statement.

Proof. Let $\widetilde{X}$ be the Galois group of the maximal abelian ℓ-extension of k_∞ and $\widetilde{W}$ be the subgroup of $\widetilde{X}$ generated by the inertia subgroups for $v \nmid \ell$ and the decomposition subgroups for $v|\ell$. Then we have the exact sequence

$$0 \longrightarrow \widetilde{W} \longrightarrow \widetilde{X} \longrightarrow T_\ell(k_\infty) \longrightarrow 0. \tag{4.7}$$

It is well known that $\widetilde{X}^{\Gamma} = 0$, hence (4.7) induces the exact sequence

$$0 \longrightarrow T_\ell(k_\infty)^{\overline{\Gamma}} \longrightarrow \widetilde{W}_{(0)} \xrightarrow{\beta} \widetilde{X}_{(0)} \xrightarrow{\alpha} T_\ell(k_\infty)_{(0)} \longrightarrow 0.$$

Put $\widetilde{H}(k_v) = \bigcap_{n=1}^{\infty} N_{k_{n,v}/k_v}(k_{n,v}^*[\ell])$ and

$$E(k) = \left(\prod_{v \nmid \ell} U(k_v)[\ell]\right) \times \left(\prod_{v|\ell} \widetilde{H}(k_v)\right).$$

Note that for real v we have $U(k_v)[\ell] = \{\pm 1\}$.

Put $\widehat{\mathcal{U}}_S(k) = U_S(k)[\ell] \cap E(k)$. Then we have the exact sequence

$$1 \longrightarrow \mu_\ell(k) \longrightarrow \widehat{\mathcal{U}}_S(k) \longrightarrow \widehat{U}_S(k) \longrightarrow 1.$$

We define $E(k_n)$ and $\widehat{\mathcal{U}}_S(k_n)$ in the same way. Using the class field theory we get that

$$\mathrm{Im}\,\beta = \mathrm{Ker}\,\alpha \cong E(k)/\widehat{\mathcal{U}}_S(k). \tag{4.8}$$

By the same reason we have

$$\widetilde{W} = \varprojlim (E(k_n)/\widehat{\mathcal{U}}_S(k_n)) = (\varprojlim E(k_n))/(\varprojlim U_S(k_n)[\ell]). \tag{4.9}$$

As $E(k_n)$ is a cohomologically trivial $G(k_n/k)$-module, we get from (4.9) that

$$\widetilde{W}_{(0)} \cong E(k)/\mathcal{U}_S^*(k), \tag{4.10}$$

where $\mathcal{U}_S^*(k)$ is the image of the natural projection $\varprojlim U_S(k_n)[\ell] \to \widehat{\mathcal{U}}_S(k)$. Note that β is induced by the identical map id : $E(k) \to E(k)$. By (4.8) and (4.9) we have

$$T_\ell(k_\infty)^\Gamma \cong \mathrm{Ker}\beta \cong \widehat{\mathcal{U}}_S(k)/\mathcal{U}_S^*(k) = \widetilde{U}_S(k)/U_S^*(k).$$

□

For real abelian k with the Galois group $G = G(k/\mathbf{Q})$ put $G = G_\ell \times G_0$, where G_ℓ is the ℓ-Sylow subgroup of G and $(|G_0|, \ell) = 1$. Let Φ be the set of all $\mathbf{Q}_\ell$-irreducible characters of G_0.

Theorem 4.1 *(Theorem 3 of the introduction.) For any real abelian k we have*

$$|T_\ell(k_\infty)_{(0)}| = [\widehat{U}_S(k) : C_S(k)].$$

For any $\varphi \in \Phi$ we have

$$|T_\ell(k_\infty)_{(0),\varphi}| = [\widehat{U}_S(k)_\varphi : C_S(k)_\varphi].$$

Proof. Let P be the maximal finite submodule of $T_\ell(k_\infty)$ and $R := T_\ell(k_\infty)/P$. Then for any $\varphi \in \Phi$ there exists the exact sequence

$$0 \longrightarrow P_\varphi \longrightarrow T_\ell(k_\infty)_\varphi \longrightarrow R_\varphi \longrightarrow 0 \tag{4.11}$$

with $\mathbf{Z}_\ell$-free R. As the Leopoldt conjecture holds true in k, we have $R^\Gamma = 0$. Hence (4.11) induces the exact sequence of finite abelian groups

$$0 \longrightarrow P_{(0),\varphi} \longrightarrow T_\ell(k_\infty)_{(0),\varphi} \longrightarrow R_{(0),\varphi} \longrightarrow 0. \tag{4.12}$$

It follows from Theorem 3.2 that $\mathbf{Z}_\ell$-free R_∞-modules R and $\tilde{U}(k_\infty)/\tilde{C}(k_\infty)$ have the same characteristic series. Then by Prop. 2.3 we have for any $\varphi \in \Phi$

$$|(\tilde{U}(k_\infty)/\tilde{C}(k_\infty))_{(0)}, \varphi| = |R_{(0),\varphi}|.$$

From Prop. 4.1 and 4.2 we get

$$(\tilde{U}(k_\infty)/\tilde{C}(k_\infty))_{(0),\varphi} \cong (U_S^*(k)_\varphi : C_S(k)_\varphi).$$

Thus

$$|R_{(0),\varphi}| = [U_S^*(k)_\varphi : C_S(k)_\varphi]. \tag{4.13}$$

As $T_\ell(k_\infty)^{\overline{\Gamma}} = P^{\overline{\Gamma}}$, we get from Prop. 4.3 that

$$|P_{(0),\varphi}| = [\hat{U}_S(k)_\varphi : U_S^*(k)_\varphi]. \tag{4.14}$$

Combining (4.12), (4.13), (4.14), we get the last assertion of the theorem. The first one may be proved just in the same way.

□

5 The proof of Theorem 4

Let k be any real abelian field and $G = G(k/\mathbf{Q})$. As in Section 4, put $G = G_\ell \times G_0$, where G_ℓ is the ℓ-Sylow subgroup of G and $(|G_0|, \ell) = 1$. If χ is any $\overline{\mathbf{Q}_\ell^*}$-valued one-dimensional character of G and Φ is the set of the all $\mathbf{Q}_\ell$-irreducible characters of G_0, then the notion $\chi|\varphi$ for $\varphi \in \Phi$ means that $\chi|_{G_0}$ is an irreducible component of φ. By φ_0 we denote the trivial character of G_0, i.e. $\varphi_0(\sigma) = 1$ for any $\sigma \in G_0$. Put $Y(k) = \prod_{v|\ell} \mu_\ell(k_v)$.

Theorem 5.1 *(Theorem 4 of the introduction.) For any real abelian k and any $\varphi \in \Phi$ we have*

$$\nu_\ell\left(|T_\ell(k_\infty)_{(0)}|\right) = \nu_\ell\left([H(k) : \hat{U}_S(k)]^{-1}|Y(k)|^{-1}\ell^t \prod_{\substack{\chi\in\hat{G}\\ \chi\neq 1}} \frac{1}{2} L_\ell(1, \chi)\right), \tag{5.1}$$

$$(5.2) \qquad \nu_\ell\left(|T_\ell(k_\infty)_{(0),\varphi}|\right) =$$

$$\nu_\ell\left([H(k)_\varphi : \widehat{U}_S(k)_\varphi]^{-1}|Y(k)_\varphi|^{-1}\ell^{t_\varphi} \prod_{\substack{\chi\in\widehat{G} \\ \chi\,|\,\varphi,\chi\neq 1}} \frac{1}{2}L_\ell(1,\ \chi)\right),$$

where the exponents t and t_φ are defined by

$$t = \begin{cases} r & \text{if} \ell \neq 2 \\ r+1 & \text{if} \ell = 2 \end{cases}$$

$$t_\varphi = \begin{cases} t & \text{if} \varphi = \varphi_0 \\ 0 & \text{if} \varphi \neq \varphi_0 \end{cases}$$

and r is given by (2.5).

Proof. By Prop. 3.2 we have $\mathcal{A}(k_\infty)/C(k_\infty) \sim \widetilde{H}(k_\infty)/\widetilde{C}_S(k_\infty)$. This last module is $\mathbf{Z}_\ell$-free. So we may calculate the order

$$(5.3) \qquad \ell^{s_\varphi} := |(\widetilde{H}(k_\infty)/\widetilde{C}_S(k_\infty))_{(0),\varphi}|$$

via (2.7), where $A_{(0)} = A/(\overline{\gamma}-1)A$ for any $\overline{\Gamma}$-module A. As $\mathcal{A}(k_\infty)/C(k_\infty) \sim (\mathcal{A}_\infty^+/C_\infty)^H$, we have

$$(5.4) \qquad s_\varphi = \nu_\ell\left(\prod_{\substack{\theta\in\widehat{V/H} \\ \theta\,|\,\varphi}} \prod_{\zeta^{\ell^r}=1} h(\zeta\zeta_\theta^{-1}-1,\ \theta)\right),$$

where $h(T,\ \theta)$ are the characteristic series of $\mathcal{A}_\infty^+/C_\infty$ given by Theorem 2.1, $H = G(K_\infty/k_\infty)$, $V = G(K_0/\mathbf{Q})$, ζ_θ is defined by $\zeta_\theta^{\ell^r} = \theta(\sigma)$, and r, σ are as in (2.5).

Combining (2.11), (2.12) and (5.4), we get

$$(5.5) \qquad s_\varphi = \begin{cases} \nu_\ell(a_\varphi b_\varphi^{-1}) & \text{if}\varphi \neq \varphi_0 \\ \nu_\ell(c_{\varphi_0} b_{\varphi_0}^{-1}) & \text{if}\varphi = \varphi_0 \end{cases}$$

where

$$(5.6) \qquad a_\varphi := \prod_{\substack{\theta\in\widehat{V/H} \\ \theta\,|\,\varphi}} \prod_{\zeta^{\ell^r}=1} f(\kappa\zeta_\theta\zeta^{-1}-1,\ \overline{\theta}\omega),$$

$$(5.7)\qquad b_\varphi = \prod_{\substack{\theta\in\widehat{V/H}\\ \theta\mid\varphi}} \prod_{\zeta^{\ell^r}=1} g(\zeta\zeta_\theta^{-1}-1,\ \theta),$$

$$(5.8)\qquad c_{\varphi_0} = \left[\prod_{\substack{\theta\in\widehat{V/H}\\ \theta\mid\varphi_0,\,\theta\neq1}} \prod_{\zeta^{\ell^r}=1} f(\kappa\zeta_\theta\zeta^{-1}-1,\ \overline{\theta}\omega)\right] \times \prod_{\zeta^{\ell^r}=1} \eta(\zeta-1,\ \omega),$$

and b_{φ_0} is defined by (5.7) for $\varphi = \varphi_0$.

Let χ be any character of G_∞ which is even as a Dirichlet character. Then χ may be presented in a form $\chi = \theta\pi$, where θ and π are the characters of the first and of the second kind in the sense of Iwasawa respectively. By the famous Iwasawa relation between ℓ-adic L-functions and Iwasawa series given in [3], we have

$$(5.9)\qquad \frac{1}{2}L_\ell(s,\ \chi) = f(\xi\kappa^s-1,\ \overline{\theta}\omega),$$

where $L_\ell(s,\ \chi)$ is the ℓ-adic L-function of Kubota-Leopoldt corresponding to χ and $\xi = \chi(\gamma)^{-1} = \pi(\gamma)^{-1}$.

Note that χ is a character of $G = G(k/\mathbf{Q})$ if and only if $\theta|_H = 1$, i.e. θ is a character of V/H, and $\chi(\overline{\gamma}) = 1$, i.e. $\chi(\gamma^{\ell^r}\sigma) = \pi(\gamma)^{\ell^r}\theta(\sigma) = 1$. Thus all the characters χ of G with given θ are of the form $\theta\pi$, where $\pi(\gamma)^{-1} = \zeta_\theta\zeta^{-1}$ and ζ runs over all ℓ^r-th roots of unity.

So we get from (5.6) and (5.9)

$$(5.10)\qquad a_\varphi = \prod_{\substack{\chi\in\widehat{G}\\ \chi\mid\varphi}} \frac{1}{2}L_\ell(1,\ \chi).$$

To compute c_{φ_0} we note that, reasoning as before, we get

$$(5.11)\qquad \prod_{\substack{\theta\in\widehat{V/H}\\ \theta\mid\varphi_0,\,\theta\neq1}} \prod_{\zeta^{\ell^r}=1} f(\kappa\zeta_\theta\zeta^{-1}-1,\ \overline{\theta}\omega) = \prod_{\substack{\chi\in\widehat{G},\chi=\theta\pi\\ \theta\mid\varphi_0,\,\theta\neq1}} \frac{1}{2}L_\ell(1,\ \chi),$$

where χ runs over all the characters of G of the form $\chi = \theta\pi$ with $\theta\mid\varphi_0$ and $\theta\neq1$.

To compute the last product of (5.8), we note that by (2.12) we have

$$(5.12)\ \prod_{\zeta^{\ell^r}=1} \eta(\kappa\zeta-1,\ \omega) = \eta(\kappa-1,\ \omega) \times \prod_{\substack{\zeta^{\ell^r}=1\\ \zeta\neq 1}} [(1-\zeta)\cdot f(\kappa\zeta-1,\ \omega)] =$$

$$\ell^r\eta(\kappa-1,\ \omega) \times \prod_{\substack{\chi\in\widehat{G}\\ \chi=\theta\pi,\theta=1}} \frac{1}{2}L_\ell(1,\ \chi).$$

So in the last product χ runs over all the characters of $\widehat{G}$ that are characters of the second kind.

Combining (5.11) and (5.12) and taking into account that $\eta(T,\ \omega)$ is invertible, we get

$$(5.13)\qquad c_{\varphi_0} = \varepsilon\ell^r \prod_{\substack{\chi\in\widehat{G}\\ \chi\mid\varphi_0,\chi\neq 1}} \frac{1}{2}L_\ell(1,\ \chi)$$

for some invertible ε.

To compute $\nu_\ell(b_\varphi)$, we note that by (2.7) we have

$$\nu_\ell(b_\varphi) = \nu_\ell(|(Y_\infty^H)_{(0),\varphi}|).$$

Put $Y(k_n) := \prod_{v|\ell} \mu_\ell(k_{n,v})$ and $Y(k_\infty) := \varprojlim Y(k_n)$, where the inverse limit is taken with respect to the norm maps. Then $Y_\infty^H \cong Y(k_\infty)$, so $(Y_\infty^H)_{(0)} \cong Y(k_\infty)_{(0)}$. If $\ell \neq 2$ and $\zeta_0 \notin k_v$, then $\zeta_0 \notin k_{n,v}$ for any n, and we have $Y(k_\infty)_{(0)} = Y(k) = 0$. If $\ell \neq 2$ and $\zeta_0 \in k_v$ then $Y(k_n)$ is a cohomologically trivial $G(k_n/k)$-module, hence $Y(k_\infty)_{(0)} \cong Y(k)$.

If $\ell = 2$ and $\sqrt{-1} \notin k_{\infty,v}$, then $Y(k_\infty) = 0$. If $\ell = 2$ and $\sqrt{-1} \in k_v$, then, again, the groups $Y(k_n)$ are cohomologically trivial, and we have $Y(k_\infty)_{(0)} \cong Y(k)$.

Finally, if $\ell = 2$, $\sqrt{-1} \notin k_v$ and $\sqrt{-1} \in k_{\infty,v}$, then we have again $Y(k_\infty)_{(0)} \cong Y(k)$. Indeed, if any place $v|\ell$ of k do not decompose in k_∞/k, then $\overline{\gamma}$ acts on $Y(k_\infty)$ as multiplication by some $\lambda \in \mathbf{Z}_2^*$. It can be checked easily that $\lambda \not\equiv 1 \pmod 4$, thus $Y(k_\infty)_{(0)} \cong Y(k_\infty)/2Y(k_\infty) \cong Y(k)$. The general case can be reduced to the considered one. Therefore we get that up to the multiplication by a unit

$$(5.14)\qquad b_\varphi = \begin{cases} 1 & \text{if } \ell = 2 \text{ and } \sqrt{-1} \notin k_{\infty,v} \text{ for } v|\ell \\ |Y(k)_\varphi| & \text{otherwise} \end{cases}$$

Note that if $\ell \neq 2$, then $b_{\varphi_0} = 1$ because $Y(k)_{\varphi_0} = 1$ in this case. Therefore it follows from (5.3), (5.5), (5.10), (5.13) and (5.14) that

$$[\widetilde{H}(k)_\varphi : \widetilde{C}(k)_\varphi] = |(\widetilde{H}(k_\infty)/\widetilde{C}(k_\infty))_{(0),\varphi}| = \ell^{s_\varphi},$$

where for $\ell \neq 2$ s_φ is given by

$$(5.15) \qquad s_\varphi = \begin{cases} \nu_\ell\left(\left(\prod_{\substack{\chi\in\widehat{G} \\ \chi\mid\varphi}} \frac{1}{2}L_\ell(1,\ \chi)\right)|Y(k)_\varphi|^{-1}\right) & \text{if} \varphi \neq \varphi_0 \\ \nu_\ell\left(\ell^r \prod_{\substack{\chi\in\widehat{G} \\ \chi\mid\varphi_0,\chi\neq 1}} \frac{1}{2}L_\ell(1,\ \chi)\right) & \text{if} \varphi = \varphi_0 \end{cases}$$

If $\ell = 2$ then s_φ is given by

$$s_\varphi = \begin{cases} \nu_\ell\left(\prod_{\substack{\chi\in\widehat{G} \\ \chi\mid\varphi}} \frac{1}{2}L_\ell(1,\ \chi)\right) & \text{if } \varphi \neq \varphi_0,\ \sqrt{-1} \notin k_{\infty,v} \text{ for } v|\ell \\ \nu_\ell\left(\ell^r \prod_{\substack{\chi\in\widehat{G} \\ \chi\mid\varphi_0,\chi\neq 1}} \frac{1}{2}L_\ell(1,\ \chi)\right) & \text{if } \varphi = \varphi_0, \sqrt{-1} \notin k_{\infty,v} \text{ for } v|\ell \\ \nu_\ell\left(\left(\prod_{\substack{\chi\in\widehat{G} \\ \chi\mid\varphi}} \frac{1}{2}L_\ell(1,\ \chi)\right)|Y(k)_\varphi|^{-1}\right) & \text{if } \varphi \neq \varphi_0,\ \sqrt{-1} \in k_{\infty,v} \text{ for } v|\ell \\ \nu_\ell\left(\ell^r\left(\prod_{\substack{\chi\in\widehat{G} \\ \chi\mid\varphi_0,\chi\neq 1}} \frac{1}{2}L_\ell(1,\ \chi)\right)|Y(k)_{\varphi_0}|^{-1}\right) & \text{if } \varphi = \varphi_0,\ \sqrt{-1} \in k_{\infty,v} \text{ for } v|\ell \end{cases}$$

(5.16)

By Theorem 4.1 we have

$$|T_\ell(k_\infty)_{(0)}| = [H(k) : C_S(k)][H(k) : \widehat{U}_S(k)]^{-1}$$

$$|T_\ell(k_\infty)_{(0),\varphi}| = [H(k)_\varphi : C_S(k)_\varphi][H(k)_\varphi : \widehat{U}_S(k)_\varphi]^{-1}$$

for any φ.

If $\ell \neq 2$, then $\widetilde{H}(k_\infty) = H(k_\infty)$ and $\tilde{C}(k_\infty) = C(k_\infty)$. So $(\widetilde{H}(k_\infty)/\tilde{C}(k_\infty))_{(0)} = (H(k_\infty)/C(k_\infty))_{(0)} \cong H(k)/C(k)$. Thus for $\ell \neq 2$ the assertion of the theorem follows from (5.3) and (5.15).

If $\ell = 2$ and $\sqrt{-1} \notin k_{\infty,v}$ for $v|\ell$, then $\widetilde{H}(k)/H(k) \cong {}_2Y(k) = Y(k)$, where ${}_2Y(k) = \{y \in Y(k) \mid 2y = 0\}$ and $\tilde{C}_S(k)/C_S(k) \cong \mathbf{Z}/2\mathbf{Z}$. If $\sqrt{-1} \in k_{\infty,v}$ for $v|\ell$, then $\widetilde{H}(k) = H(k)$ and $\tilde{C}_S(k)/C_S(k) \cong \mathbf{Z}/2\mathbf{Z}$. Therefore

$$[H(k) : C_S(k)] = \begin{cases} 2|Y(k)|^{-1}[\widetilde{H}(k) : \tilde{C}_S(k)] & \text{if } \sqrt{-1} \notin k_{\infty,v} \text{ for } v|\ell \\ 2[\widetilde{H}(k) : \tilde{C}_S(k)] & \text{if } \sqrt{-1} \in k_{\infty,v} \text{ for } v|\ell \end{cases}$$

If $\varphi \neq \varphi_0$, then

$$[H(k)_\varphi : C_S(k)_\varphi] = \begin{cases} |Y(k)_\varphi|^{-1}[\widetilde{H}(k)_\varphi : \tilde{C}_S(k)_\varphi] & \text{if } \sqrt{-1} \notin k_{\infty,v} \text{ for } v|\ell \\ [\widetilde{H}(k)_\varphi : \tilde{C}_S(k)_\varphi] & \text{if } \sqrt{-1} \in k_{\infty,v} \text{ for } v|\ell \end{cases}$$

If $\varphi = \varphi_0$, then

$$[H(k)_{\varphi_0} : C_S(k)_{\varphi_0}] = \begin{cases} 2|Y(k)_{\varphi_0}|^{-1}[\widetilde{H}(k)_{\varphi_0} : \tilde{C}_S(k)_{\varphi_0}] & \text{if } \sqrt{-1} \notin k_{\infty,v} \text{ for } v|\ell \\ 2[\widetilde{H}(k)_{\varphi_0} : \tilde{C}_S(k)_{\varphi_0}] & \text{if } \sqrt{-1} \in k_{\infty,v} \text{ for } v|\ell. \end{cases}$$

Now the assertion of the theorem for $\ell = 2$ follows from (5.3) and (5.16).

□

6 A refinement of the conductor-discriminant formula of Hasse

Let k be an algebraic number field of degree t, Galois over $\mathbf{Q}$ and having the Galois group $G = G(k/\mathbf{Q})$. We consider k as a subfield of a fixed algebraic closure $\overline{\mathbf{Q}}_\ell$ of $\mathbf{Q}_\ell$. Put

$$\mathbf{A}_k = \{(x_{\sigma_1}, \ldots, x_{\sigma_t}) \mid x_{\sigma_i} \in \overline{\mathbf{Q}}_\ell,\ G = \{\sigma_1 = 1, \sigma_2, \ldots, \sigma_t\}\}.$$

So $\mathbf{A}_k$ is the set of all t-vectors with coordinates in $\overline{\mathbf{Q}}_\ell$ having G as the set of indices. We define addition and multiplication in $\mathbf{A}_k$ componentwise. For $\lambda \in \overline{\mathbf{Q}}_\ell$ and $\sigma \in G$ we put $\lambda(x_{\sigma_1}, \ldots, x_{\sigma_t}) = (\lambda x_{\sigma_1}, \ldots, \lambda x_{\sigma_t})$,

(6.1) $\sigma(x_{\sigma_1}, \ldots, x_{\sigma_t}) = (y_{\sigma_1}, \ldots, y_{\sigma_t})$, where $y_{\sigma_i} = x_{\sigma_i\sigma}$ for $i = 1, \ldots, t$.

So the action of G commutes with multiplication by $\lambda \in \mathbf{Q}_\ell$, and we may consider $\mathbf{A}_k$ as a $\overline{\mathbf{Q}}_\ell[G]$-algebra.

Put $f_i = \{0, \dots, 0, 1, 0 \dots, 0\} \in \mathbf{A}_k$, where the only nonzero coordinate has the index σ_i. Then the set $\{f_1, \dots, f_t\}$ forms a basis of $\mathbf{A}_k$ over $\overline{\mathbf{Q}}_\ell$ and any of f_i generates $\mathbf{A}_k$ as a $\overline{\mathbf{Q}}_\ell[G]$-module. So $\mathbf{A}_k \cong \overline{\mathbf{Q}}_\ell[G]$ as a $\overline{\mathbf{Q}}_\ell[G]$-module. Namely, we have $\sigma(f_i) = f_j$, where $\sigma_j = \sigma_i\sigma$.

We define the injection $\alpha : k \hookrightarrow \mathbf{A}_k$ by $\alpha(x) = (x_{\sigma_1}, \dots, x_{\sigma_t})$, where $x_{\sigma_i} = \sigma_i^{-1}(x)$, $i = 1, \dots, t$. Thus we have $\alpha(\sigma(x)) = \sigma(\alpha(x))$ for any $\alpha \in k$ and $\sigma \in G$.

If $e_1, \dots, e_t \in k$ form a basis of k over $\mathbf{Q}$, then $\alpha(e_1), \dots, \alpha(e_t)$ form a basis of $\mathbf{A}_k$ over $\overline{\mathbf{Q}}_\ell$. Hence α induces an isomorphism

$$\overline{\mathbf{Q}}_\ell \otimes_{\mathbf{Q}} k \cong \mathbf{A}_k,\ \lambda \otimes x \to \lambda\alpha(x) \text{ for any} \lambda \in \overline{\mathbf{Q}}_\ell,\ x \in k.$$

If $\overline{\mathcal{O}}$ is the ring of integers of $\overline{\mathbf{Q}}_\ell$, then the set

$$\mathbf{R}_k = \{(x_{\sigma_1}, \dots, x_{\sigma_t}) \in \mathbf{A}_k \mid x_{\sigma_i} \in \overline{\mathcal{O}} \text{ for all } \sigma_i \in G\}$$

is the maximal order of $\mathbf{A}_k$. Note that $\mathbf{R}_k$ is a free $\overline{\mathcal{O}}[G]$-module of rank 1 generated by any of $f_1, \dots, f_t$.

If $\mathcal{O}_k$ is the ring of integers of k and $\{e_1, \dots, e_t\}$ form a $\mathbf{Z}$-basis of $\mathcal{O}_k$, then $\{\alpha(e_1), \dots, \alpha(e_n)\}$ form a $\overline{\mathcal{O}}$-basis of $\tilde{\mathcal{O}}_k := \overline{\mathcal{O}} \otimes_{\mathbf{Z}} \mathcal{O}_k$.

Let V be a $\overline{\mathbf{Q}}_\ell$-subspace of $\mathbf{A}_k$ and $L,\ M \subset V$ be full $\overline{\mathcal{O}}$-lattices in V. It means that both L, M are finitely generated over $\overline{\mathcal{O}}$ and each of them spans V as a $\overline{\mathbf{Q}}_\ell$-space. Then there exists a nonsingular linear transformation $A : V \to V$, such that $A(L) = M$. Then, as in [12], we define

$$(L : M) = \det(A),$$

$\det(A)$ denoting the determinant of A. So $(L : M) \in \overline{\mathbf{Q}}_\ell^*$ and $(L : M)$ is defined uniquely up to multiplication by a unit of $\overline{\mathcal{O}}$. Therefore
$\nu_\ell((L : M))$ does not depend on the choice of A. If $L \subseteq M$, we have
$\nu_\ell((L : M)) = 0$ if and only if $L = M$.

We define a $\overline{\mathbf{Q}}_\ell$-bilinear form $\psi : \mathbf{A}_k \times \mathbf{A}_k \to \overline{\mathbf{Q}}_\ell$ by $\psi(x, y) = \sum_{\sigma_i \in G} x_{\sigma_i} y_{\sigma_i}$ for $x = (x_{\sigma_1}, \dots, x_{\sigma_t})$, $y = (y_{\sigma_1}, \dots, y_{\sigma_t}) \in \mathbf{A}_k$.

Then we have for any $a, b \in k$

$$\psi(\alpha(a), \alpha(b)) = \mathrm{Sp}_{k/\mathbf{Q}}(ab),$$

where $\mathrm{Sp}_{k/\mathbf{Q}}$ is the trace map from k to $\mathbf{Q}$.

Let A be the matrix of the $\overline{\mathbf{Q}}_\ell$-linear transformation, such that $Af_i = \alpha(e_i)$, $i = 1, \ldots, t$, where $\{f_1, \ldots, f_t\}$ and $\{\alpha(e_1), \ldots, \alpha(e_t)\}$ are as above.

The form ψ has the matrices $E = 1$ with respect to $\{f_1, \ldots, f_t\}$ and $C = (\mathrm{Sp}_{k/\mathbf{Q}}(e_i e_j))$ with respect to $\{e_1, \ldots, e_t\}$. So $(\det(A))^2 = \det(C)$, and therefore $(\mathbf{R}_k : \tilde{\mathcal{O}}_k)^2 = d_k$, where d_k is the absolute discriminant of k.

From now on we assume k to be an abelian field. By the conductor-discriminant formula of Hasse we have

$$d_k = \prod_{\chi \in \widehat{G}} f_\chi = \prod_{\substack{\chi \in \widehat{G} \\ \chi \neq 1}} f_\chi,$$

where $\widehat{G}$ is the dual group of G and f_χ is the conductor of χ, when we consider χ as a primitive Dirichlet cheracter. We consider all the characters of G having their values in $\overline{\mathbf{Q}}_\ell$. For given $\chi \in \widehat{G}$ let ζ be any primitive f_χ-th root of unity in $\overline{\mathbf{Q}}_\ell$. Then we can form the Gauss sum

$$g_\chi = \sum_{\substack{a \pmod{f_\chi} \\ (a, f_\chi)=1}} \chi(a)\zeta^a \in \overline{\mathbf{Q}}_\ell.$$

It is well known that $\nu_\ell(g_\chi)$ does not depend on the particular choice of ζ. It is well known also that $g_\chi \overline{g}_\chi = f_\chi$ and $\overline{g}_\chi = \chi(-1) g_{\overline{\chi}}$, where $\overline{\chi} = \chi^{-1}$ and

$$\overline{g}_\chi = \sum_{\substack{a \pmod{f_\chi} \\ (a, f_\chi)=1}} \overline{\chi}(a)\zeta^{-a}.$$

Then the ℓ-part of the conductor-discriminant formula of Hasse can be restated in the form

$$(6.2) \qquad \nu_\ell((\mathbf{R}_k : \tilde{\mathcal{O}}_k)) = \nu_\ell\left(\prod_{\substack{\chi \in \widehat{G} \\ \chi \neq 1}} g_\chi\right).$$

Let Φ be as before. The next result is a refinement of (6.2).

Theorem 6.1 *For any $\varphi \in \Phi$ the index $(\mathbf{R}_{k,\varphi} : \tilde{\mathcal{O}}_{k,\varphi})$ is defined and*

$$(6.3) \qquad \nu_\ell((\mathbf{R}_{k,\varphi} : \tilde{\mathcal{O}}_{k,\varphi})) = \nu_\ell\left(\prod_{\substack{\chi \in \widehat{G} \\ \chi \mid \varphi,\ \chi \neq 1}} g_{\overline{\chi}}\right).$$

Proof. Let k have conductor $N = \ell^m d$, $(d, \ell) = 1$. We shall prove our theorem by induction on m.

1. If $N = d$ (thus $m = 0$), then d_k is prime with ℓ and $\mathbf{R}_k = \tilde{\mathcal{O}}_k$. Then $\mathbf{R}_{k,\varphi} = \tilde{\mathcal{O}}_{k,\varphi}$ and $\nu_\ell((\mathbf{R}_{k,\varphi} : \tilde{\mathcal{O}}_{k,\varphi})) = 0$ for any $\varphi \in \Phi$. On the other hand, the relation $g_\chi g_{\overline{\chi}} = \chi(-1) f_\chi$, $f_\chi | d$ for algebraic integers g_χ, $g_{\overline{\chi}}$ shows that $\nu_\ell(g_\chi) = 0$ for any χ. This proves (6.3) for $m = 0$.

2. Let ℓ be odd. We claim that to prove (6.3) for k it is sufficient to prove (6.3) for $k_1 = k(\zeta_0)$, where ζ_0 is a primitive ℓ-th root of unity. Put $G_1 = G(k_1/\mathbf{Q})$, $H_1 = G(k_1/k)$. Then H_1 is a cyclic group of prime with ℓ order. For $\varphi \in \Phi$ and $\chi \in \widehat{G}$ we denote by φ_1 (resp.χ_1) the image of inflation of φ (resp.χ) from G to G_1. Then φ_1 is a $\overline{\mathbf{Q}}_\ell$-irreducible character of G_1 trivial on H_1 and on the ℓ-Sylow subgroup of G_1. So any $\chi' \in \widehat{G_1}$, such that $\chi' | \varphi_1$, is the inflation of some $\chi \in \widehat{G}$, $\chi | \varphi$. As χ and χ_1 have the same conductor, we have $g_\chi = g_{\chi_1}$. Therefore

$$\prod_{\substack{\chi \in \widehat{G} \\ \chi | \varphi,\ \chi \neq 1}} g_{\overline{\chi}} = \prod_{\substack{\chi_1 \in \widehat{G}_1 \\ \chi_1 | \varphi_1,\ \chi_1 \neq 1}} g_{\overline{\chi}_1}.$$

On the other hand, the trace map $\mathrm{Sp}_{k_1/k}$ induces isomorphisms $\mathbf{R}_{k_1,\varphi_1} \cong \mathbf{R}_{k,\varphi}$, $\tilde{\mathcal{O}}_{k_1,\varphi_1} \cong \tilde{\mathcal{O}}_{k,\varphi}$. Thus our assertion holds true.

3. Now let ℓ be odd and $m = 1$, i.e. k has only tame ramification. By step 2 we may suppose that $k = E(\zeta_0)$, where E is unramified over ℓ. Then $k = E \cdot \mathbf{Q}(\zeta_0)$ and $G = G(k/\mathbf{Q}) \cong F \times \Delta$, where $F = G(E/\mathbf{Q})$, $\Delta = G(\mathbf{Q}(\zeta_0)/\mathbf{Q})$. Thus any $\mathbf{Q}_\ell$-irreducible character φ of G is of the form $\varphi = \varphi_1 \otimes \omega^i$, where φ_1 is a $\mathbf{Q}_\ell$-irreducible character of F and ω^i is some power of the Teichmüller character $\omega : \Delta \to \mathbf{Z}_\ell^*$, $i = 0, \ldots, \ell - 2$. If $\chi \in \widehat{G}$ and $\chi | \varphi$, then $\chi = \chi_1 \otimes \omega^i$, where $\chi_1 \in \widehat{F}$ and $\chi_1 | \varphi_1$. Certainly, we may assume that $i \neq 0$ (if $i = 0$, then we are in the position of Step 1). As χ_1 and ω^i have relatively prime conductors, we have $g_{\overline{\chi}} = g_{\overline{\chi}_1} g_{\overline{\omega}^i}$, thus

$$\prod_{\chi | \varphi} g_{\overline{\chi}} = \prod_{\chi_1 | \varphi_1} g_{\overline{\chi}_1} \cdot g_{\overline{\omega}^i}. \tag{6.4}$$

Lemma 6.1 *Let $g_{\omega^i} \in \overline{\mathbf{Q}}_\ell$ be the Gauss sum corresponding to ω^i. Then*

$$\nu_\ell(g_{\omega^i}) = \frac{\ell - 1 - i}{\ell - 1} \quad \textit{for} \ \ i = 1, \ldots, \ell - 2.$$

Proof. If $\omega^i = \overline{\omega}$, i.e. $i = \ell - 2$, then, putting $\pi_0 = 1 - \zeta_0$, where ζ_0 is a primitive ℓ-th root of unity, we get

$$g_{\overline{\omega}} = \sum_{a=1}^{\ell-2} \overline{\omega}(a)(1-\pi_0)^a \equiv \sum_{a=1}^{\ell-2} -\overline{\omega}(a)a\pi_0 \equiv \pi_0 \pmod{\pi_0^2}.$$

Hence $\nu_\ell(g_{\overline{\omega}}) = 1/(\ell - 1)$.

If $\delta_b \in \Delta$ sends ζ_0 into ζ_0^b, then $\delta_b(g_{\omega^i}) = \overline{\omega}^i(b)g_{\omega^i}$, $\delta_b(g_{\overline{\omega}}) = \omega(b)g_{\overline{\omega}}$. So $(g_{\omega^i})^{\ell-1} \in \mathbf{Q}_\ell$, and by the Kummer theory $g_{\omega^i} = (g_{\overline{\omega}})^c a$ for some $c = 1, \ldots, \ell - 2$ and $a \in \mathbf{Q}_\ell$. As $\delta_b(g_{\omega^i}) = \overline{\omega}^i(b)g_{\omega^i} = \omega(b)^c(g_{\overline{\omega}})^c$, we get that $c = (\ell - 1) - i$. The relation $g_{\omega^i}\overline{g_{\omega^i}} = \ell$ implies that $\nu_\ell(g_{\omega^i}) \leq 1$, hence $\nu_\ell(a) = 0$. Therefore $\nu_\ell(g_{\omega^i}) = \frac{\ell-1-i}{\ell-1}$.

□

If $\mathcal{O}_F$ (resp. $\mathcal{O}_k$) is the ring of integers of F (resp. of k), then $\mathcal{O}_k = \mathcal{O}_F + \mathcal{O}_F\zeta_0 + \cdots + \mathcal{O}_F\zeta_0^{\ell-2}$. Let $e_{\omega^i} = |\Delta|^{-1}\sum_{\delta\in\Delta}\overline{\omega}^i(\delta)\delta$ be the idempotent corresponding to ω^i. Then $e_{\omega^i}\zeta_0^b = |\Delta|^{-1}\omega^i(b)g_{\overline{\omega}^i}$. Hence $\mathcal{O}_{k,\varphi} = g_{\overline{\omega}^i}\mathcal{O}_{F,\varphi_1}$. Taking into account that $\tilde{\mathcal{O}}_{k,\varphi} = \overline{\mathcal{O}} \cdot \mathcal{O}_{k,\varphi}$, we get that $\nu_\ell((\mathbf{R}_{k,\varphi} : \tilde{\mathcal{O}}_{k,\varphi})) = s\nu_\ell(g_{\overline{\omega}^i})$, where s is the $\mathbf{Z}_\ell$-rank of $\mathcal{O}_{F,\varphi_1}$, i.e. the dimension of φ_1. Comparing this with (6.4) and Lemma 6.1 and noting that $\nu_\ell(g_{\overline{\chi}_1}) = 0$ for any $\chi_1 \,|\, \varphi_1$, we get (6.3) for the case of tame ramification.

4. Let an abelian number field k with conductor N be wildly ramified over ℓ. By step 2 we may assume that $\zeta_0 \in k$ for $\ell \neq 2$. We have $N = \ell^m d$, where $m \geq 1$ if $\ell \neq 2$ and $m \geq 2$ if $\ell = 2$. Put $K_n = \mathbf{Q}(\mu_d, \zeta_n)$, where $n = m - 1$ if $\ell \neq 2$; $n = m - 2$ if $\ell = 2$. Then $k \subseteq K_n$ and $k \not\subseteq K_{n-1}$, thus, putting $k_0 := k \cap K_{n-1}$, we get the following diagram of fields

$$\begin{array}{ccc} k & \subseteq & K_n \\ | & & | \\ k_0 & \subseteq & K_{n-1} \end{array} \tag{6.5}$$

Put $H = G(K_n/K_{n-1}) \cong G(k/k_0)$ and $F = G(K_n/k) \cong G(K_{n-1}/k_0)$. Note that $H \cong \mathbf{Z}/\ell\mathbf{Z}$.

Lemma 6.2 *Let k have conductor $N \equiv 0 \pmod{\ell^2}$ ($N \equiv 0 \pmod 8$ if $\ell = 2$) and k_0 be as in (6.5). Let $\mathbf{B}_k$ be the kernel of the trace map $\mathrm{Sp}_{k/k_0} : \tilde{\mathcal{O}}_k \to \tilde{\mathcal{O}}_{k_0}$. Then $\mathbf{B}_k$ is a cyclic $\overline{\mathcal{O}}[G]$-module isomorphic to $\mathbf{R}_k/\mathbf{R}_k^H$ and $\mathrm{Sp}_{k/k_0}(\tilde{\mathcal{O}}_k) = \ell\tilde{\mathcal{O}}(k_0)$. If K_n and k are as in (6.5), then $\mathrm{Sp}_{K_n/k} : \tilde{\mathcal{O}}_{K_n} \to \tilde{\mathcal{O}}_k$ induces a surjection $\mathbf{B}_{K_n} \to \mathbf{B}_k$.*

Proof. First suppose that $k = K_n$ (hence $k_0 = K_{n-1}$). If $\alpha : K_n \hookrightarrow \mathbf{A}_{K_n}$ is the mapping defined above, then the elements of the form $\alpha(\varepsilon\zeta_n^s)$, $s \in \mathbf{Z}$, generate $\tilde{\mathcal{O}}_{K_n}$ as a $\overline{\mathcal{O}}$-module. We have

$$\mathrm{Sp}_{K_n/K_{n-1}}(\alpha(\varepsilon\zeta_n^s)) = \begin{cases} 0 & \text{if } s \not\equiv 0 \pmod{\ell} \\ \ell\alpha(\varepsilon\zeta_n^s) & \text{if } s \equiv 0 \pmod{\ell}. \end{cases}$$

So the elements $\alpha(\varepsilon\zeta_n^s)$ with $s \not\equiv 0 \pmod{\ell}$ generate $\mathbf{B}_{K_n}$ and therefore

$$\tilde{\mathcal{O}}_{K_n} = \mathbf{B}_{K_n} \oplus \tilde{\mathcal{O}}_{K_{n-1}}. \tag{6.6}$$

The field $K_{-1} = \mathbf{Q}(\mu_d)$ is unramified over ℓ, hence $\tilde{\mathcal{O}}_{K_{-1}}$ is a free $\overline{\mathcal{O}}[G(K_{-1}/\mathbf{Q}]$-module on one generator, say x. Then $x \cdot \alpha(\zeta_n)$ generates $\mathbf{B}_{K_n}$ as a $G(K_n/\mathbf{Q})$-module, i.e. $\mathbf{B}_{K_n}$ is cyclic, therefore there exists a surjection $p : \mathbf{R}_{K_n} \to \mathbf{B}_{K_n}$. Surely, we have $\mathbf{R}_{K_n}^H \subset \mathrm{Ker}\, p$. As $\mathbf{R}_{K_n}/\mathbf{R}_{K_n}^H$ is $\overline{\mathcal{O}}$-torsionfree and has the same $\overline{\mathcal{O}}$-rank as $\mathbf{B}_{K_n}$, we get that p induces an isomorphism $\mathbf{B}_{K_n} \cong \mathbf{R}_{K_n}/\mathbf{R}_{K_n}^H$. This proves the lemma if $k = K_n$.

If k is any abelian field, then we have the commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 \longrightarrow & \mathbf{B}_{K_n} & \longrightarrow & \tilde{\mathcal{O}}_{K_n} & \xrightarrow{\mathrm{Sp}_H} & \tilde{\mathcal{O}}_{K_{n-1}} \\ & \downarrow \mathrm{Sp}_F & & \downarrow \mathrm{Sp}_F & & \downarrow \mathrm{Sp}_F \\ 0 \longrightarrow & \mathbf{B}_k & \longrightarrow & \tilde{\mathcal{O}}_k & \xrightarrow{\mathrm{Sp}_H} & \tilde{\mathcal{O}}_{k_0} \end{array} \tag{6.7}$$

where K_n, K_{n-1} and k_0 are as in (6.5).

Let suppose at first that K_n/k is unramified over ℓ. Then K_{n-1}/k_0 is unramified over ℓ, and the mappings $\mathrm{Sp}_F : \tilde{\mathcal{O}}_{K_n} \to \tilde{\mathcal{O}}_k$, $\mathrm{Sp}_F : \tilde{\mathcal{O}}_{K_{n-1}} \to \tilde{\mathcal{O}}_{k_0}$ are surjections. Hence

$$\mathrm{Sp}_H(\tilde{\mathcal{O}}_k) = \mathrm{Sp}_H \cdot \mathrm{Sp}_F(\tilde{\mathcal{O}}_{K_n}) = \mathrm{Sp}_F \cdot \mathrm{Sp}_H(\tilde{\mathcal{O}}_{K_n}) = \mathrm{Sp}_F(\ell\tilde{\mathcal{O}}_{K_{n-1}}) = \ell\tilde{\mathcal{O}}_{k_0}.$$

So any $x \in \tilde{\mathcal{O}}_k$ can be presented in a form $x = (x - \ell^{-1}\mathrm{Sp}_H x) + \ell^{-1}\mathrm{Sp}_H x$, where $(x - \ell^{-1}\mathrm{Sp}_H x) \in \mathbf{B}_k$, $\ell^{-1}\mathrm{Sp}_H x \in \tilde{\mathcal{O}}_{k_0}$, therefore $\tilde{\mathcal{O}}_k = \mathbf{B}_k \oplus \tilde{\mathcal{O}}_{k_0}$. The decomposition (6.6) shows that the mapping $\mathrm{Sp}_F : \mathbf{B}_{K_n} \to \mathbf{B}_k$ is a surjection. Hence $\mathbf{B}_k$ is a cyclic $\overline{\mathcal{O}}[G]$-module and, reasoning as before, we get that $\mathbf{B}_k \cong \mathbf{R}_k/\mathbf{R}_k^H$. This proves the lemma if K_n/k is unramified over ℓ.

Note that this is the case if $\ell \neq 2$ or $\ell = 2$ and $n = 0$. Indeed, as we have $\zeta_0 \in k_0$ for $\ell \neq 2$ (by Step 2), the inertia subgroup W of ℓ in $G(K_n/k_0)$ is a cyclic ℓ-group, and $G(K_n/K_{n-1}) \subset W$. As $G(K_n/k) \cap G(K_n/K_{n-1}) = 1$, we have $G(K_n/k) \cap W = 1$, thus K_n/k is unramified over ℓ.

Now to finish the proof of the lemma, we have to consider the case when $\ell = 2$, $n \geq 1$, and K_n/k is ramified over 2. Let W be the inertia subgroup of 2 in $G(K_n/\mathbf{Q})$. Then $W \cong (\mathbf{Z}/\ell^m\mathbf{Z})^*$, so $W = V \times \Delta$, where $\Delta \cong \{\pm 1\}$ and $V \cong (1+4\mathbf{Z})/(1+2^m\mathbf{Z}) \cong \mathbf{Z}/2^n\mathbf{Z}$. As $k \not\subseteq K_{n-1}$, we have $F \cap V = 1$. Let σ be the only element of order 2 in V and τ be the nonunit element of Δ, thus $\sigma(\zeta_n) = -\zeta_n$, $\tau(\zeta_n) = \zeta_n^{-1}$. Then $H = \{1, \sigma\}$ and the condition $F \cap W = 1$ means that either $F \cap W = \{1, \tau\}$ or $F \cap W = \{1, \sigma\tau\}$. Let k_1 be the fixed field of $F \cap W$. Then $K_n \supset k_1 \supseteq k$, $[K_n : k_1] = 2$, $G(K_n/k_1) = \{1, \tau\}$ or $\{1, \sigma\tau\}$ and k_1/k is unramified over ℓ.

Now we are going to determine the ℓ-parts of the differents of all extensions in (6.5). In what follows the symbol $\mathcal{D}$ will stand for the ℓ-part of the different. It is well known that $\mathcal{D}_{K_n/K_{n-1}} = (2)$. If $G(K_n/k_1) = \{1, \tau\}$, then $\mathrm{Sp}_{K_n/k_1}(\zeta_n^i) = \zeta_n^i + \zeta_n^{-i}$. Put $\pi = 1 - \zeta_{n-1}$. As $\mathrm{Sp}_{K_n/k_1}(\zeta_n) = \zeta_n + \zeta_n^{-1} \equiv \zeta_n^{-1}(1-\zeta_{n-1}) \pmod 2$, we get $\mathrm{Sp}_{K-n/k_1}(\mathcal{O}_{K_n}) = \pi\mathcal{O}_{k_1}$, so $\mathrm{Sp}_{K_n/k_1}(\pi^{-1}\mathcal{O}_{K_n}) = \mathcal{O}_{k_1}$. As $\mathrm{Sp}_{K_n/k_1}((1-\zeta_n)\pi^{-2}) \notin \mathcal{O}_{k_1}$, we get that $\mathcal{D}_{K_n/k_1} = (\pi)$. The extension k_1/k is unramified over ℓ, hence $\mathcal{D}_{K_n/k} = \mathcal{D}_{K_n/k_1} = (\pi)$ and $\nu_\ell(\mathcal{D}_{K_n}/k) = 2^{-n}$. If $G(K_n/k_1) = \{1, \sigma\tau\}$, then reasoning as before and putting $\pi = \zeta_n - \zeta_n^{-1}$, we get again that $\nu_\ell(\mathcal{D}_{K_n/k}) = 2^{-n}$.

By the multiplicative property of differents we have

$$\mathcal{D}_{K_n/k} \cdot \mathcal{D}_{k/k_0} = \mathcal{D}_{K_n/K_{n-1}} \cdot \mathcal{D}_{K_{n-1}}/k_0.$$

We have computed $\mathcal{D}_{K_n/k}$. It is well known that $\mathcal{D}_{K_n/K_{n-1}} = (2)$. Note that the places over 2 ramify in k/k_0 (because $K_n = k \cdot K_{n-1}$) hence they ramify in K_{n-1}/k_0. Thus if $n \geq 2$, then, reasoning as before, we get that $\nu_\ell(\mathcal{D}_{K_{n-1}}/k_0) = 2^{1-n}$. If $n = 1$, then $k_0/\mathbf{Q}$ is unramified over 2, hence $\mathcal{D}_{K_0/k_0} = (2)$ and $\nu_\ell(\pi) = \frac{1}{2}$. Thus in any case we have $\nu_\ell(\mathcal{D}_{k/k_0}) = \nu_\ell(2\pi)$. Therefore $\mathrm{Sp}_{k/k_0}(\tilde{\mathcal{O}}_k) = 2\tilde{\mathcal{O}}_k$.

If $x \in \tilde{\mathcal{O}}_k \setminus \alpha(\pi)\tilde{\mathcal{O}}_k$, then we can present x in the form $x = x_1 + x_2$, where $x_1 \in \tilde{\mathcal{O}}_{k_0}^*$ and $x_2 \in \alpha(\pi)\tilde{\mathcal{O}}_k$. Let $\pi_0 \in k_0$ be a local parameter at any place $v \mid \ell$ of k_0. Then $\alpha(\pi)\tilde{\mathcal{O}}_k = \alpha(\pi^{-1}\pi_0)\tilde{\mathcal{O}}_k$, hence we have $\mathrm{Sp}_H(x_2) \subset \mathrm{Sp}_H(\alpha(\pi^{-1}\pi_0)\tilde{\mathcal{O}}_k) \subset \alpha(2\pi_0)\tilde{\mathcal{O}}_k$, because $\nu_\ell(\mathcal{D}_{k/k_0}) = \nu_\ell(2\pi)$. On the other hand, we have $\mathrm{Sp}_H(x_1) = 2x_1 \notin \alpha(2\pi_0\tilde{\mathcal{O}}_{k_0})$. Therefore $\mathrm{Sp}_H(x) \neq 0$, i.e. $x \notin \mathbf{B}_k$, so we get $\mathbf{B}_k \subset \alpha(\pi)\tilde{\mathcal{O}}_k = \mathrm{Sp}_{K_n/k}(\tilde{\mathcal{O}}_{K_n})$. If $a \in \mathbf{B}_k$ and $a = \mathrm{Sp}_F(b), b \in \tilde{\mathcal{O}}_{K_n}$, then by (6.6) we have $b = b_1 + b_2$, where $b_1 \in \mathbf{B}_{K_n}$, $b_2 \in \tilde{\mathcal{O}}_{K_{n-1}}$. Then

$$0 = \mathrm{Sp}_H(a) = \mathrm{Sp}_H\mathrm{Sp}_F(b_1 + b_2) = \mathrm{Sp}_F\mathrm{Sp}_H(b_1) + \mathrm{Sp}_F\mathrm{Sp}_H(b_2) = \mathrm{Sp}_F(2b_2).$$

Hence $\mathrm{Sp}_F(b_2) = 0$ and $a = \mathrm{Sp}_F(b_1)$, i.e. the mapping $\mathrm{Sp}_F : \mathbf{B}_{K_n} \to \mathbf{B}_k$ in (6.7) is a surjection. Therefore $\mathbf{B}_k$ is a cyclic $\overline{\mathcal{O}}[G]$-module and thus $\mathbf{B}_k \cong \mathbf{R}_k/\mathbf{R}_k^H$. This proves the lemma.

□

Lemma 6.3 *Let k, k_0 and H be as in (6.5). Put $\mathbf{N}_k := (1 - \ell^{-1}\mathrm{Sp}_H)\mathbf{R}_k \subset \ell^{-1}\mathbf{R}_k$. Then*

$$(\mathbf{R}_{k,\varphi} : \tilde{\mathcal{O}}_{k,\varphi}) = (\mathbf{N}_{k,\varphi} : \mathbf{B}_{k,\varphi})(\mathbf{R}_{k,\varphi} : \tilde{\mathcal{O}}_{k,\varphi}) \text{ for any } \varphi \in \Phi.$$

Proof. Let $\mathbf{M}_k$ be the kernel of the trace map $\mathrm{Sp}_H : \mathbf{R}_k \to \mathbf{R}_{k_0}$. Then for a given $\varphi \in \Phi$ we have the commutative diagram with exact rows

$$\text{(6.8)} \qquad \begin{array}{ccccccccc} 0 \longrightarrow & \mathbf{B}_{k,\varphi} & \longrightarrow & \tilde{\mathcal{O}}_{k,\varphi} & \xrightarrow{\mathrm{Sp}_H} & \ell\tilde{\mathcal{O}}_{k_0,\varphi} & \longrightarrow 0 \\ & \downarrow & & \downarrow & & \downarrow & \\ 0 \longrightarrow & \mathbf{M}_{k,\varphi} & \longrightarrow & \widetilde{\mathbf{R}}_{k,\varphi} & \xrightarrow{\mathrm{Sp}_H} & \widetilde{\mathbf{R}}_{k_0,\varphi} & \longrightarrow 0 \end{array}$$

where the vertical arrows are the natural inclusions.

It follows from (6.8) that

$$\text{(6.9)} \qquad (\mathbf{R}_{k,\varphi} : \tilde{\mathcal{O}}_{k,\varphi}) = (\mathbf{M}_{k,\varphi} : \mathbf{B}_{k,\varphi})(\mathbf{R}_{k_0,\varphi} : \ell\tilde{\mathcal{O}}_{k_0,\varphi}).$$

As $\mathbf{R}_k \cong \overline{\mathcal{O}}[G]$ as an $\overline{\mathcal{O}}[G]$-module, the mapping $\mathrm{Sp}_H : \mathbf{R}_k \to \mathbf{R}_{k_0}$ induces the isomorphism $\mathbf{N}_k/\mathbf{M}_k \cong \mathbf{R}_{k_0}/\ell\mathbf{R}_{k_0}$. Therefore $(\mathbf{N}_{k,\varphi} : \mathbf{M}_{k,\varphi}) = (\mathbf{R}_{k_0,\varphi} : \ell\mathbf{R}_{k_0,\varphi})$, and it follows from (6.9) that

$$\begin{aligned}(\mathbf{R}_{k,\varphi} : \tilde{\mathcal{O}}_{k,\varphi}) &= (\mathbf{M}_{k,\varphi} : \mathbf{B}_{k,\varphi})(\mathbf{R}_{k_0,\varphi} : \ell\mathbf{R}_{k_0,\varphi})(\ell\mathbf{R}_{k_0,\varphi} : \ell\tilde{\mathcal{O}}_{k_0,\varphi}) \\ &= (\mathbf{N}_{k,\varphi} : \mathbf{B}_{k,\varphi})(\mathbf{R}_{k_0,\varphi} : \tilde{\mathcal{O}}_{k_0,\varphi}).\end{aligned}$$

□

Lemma 6.4 *Let L, $M \subset \mathbf{A}_k$ be two lattices that span the same $\overline{\mathbf{Q}}_\ell$-space $V \subseteq \mathbf{A}_k$. Let L, M be $\overline{\mathcal{O}}[G]$-modules. For $\chi \in \widehat{G}$ put $L_\chi = e_\chi L$, $M_\chi = e_\chi M$, where $e_\chi = |G|^{-1} \sum_{\sigma \in G} \overline{\chi}(\sigma)\sigma$ is the idempotent corresponding to χ. If $L \cong M$ as an $\overline{\mathcal{O}}[G]$-module, then*

$$(L : M) = \prod_{\chi \in \widehat{G}} (L_\chi : M_\chi)$$

and for any $\varphi \in \Phi$

$$(L_\varphi : M_\varphi) = \prod_{\substack{\chi \in \widehat{G} \\ \chi \mid \varphi}} (L_\chi : M_\chi),$$

where we put $(L_\varphi : M_\varphi) = 1$ *if* $L_\varphi = M_\varphi = 0$.

Proof. Put $L' = \bigoplus_{\chi \in \widehat{G}} L_\chi$, $M' = \bigoplus_{\chi \in \widehat{G}} M_\chi$. If $f : L \cong M$ is an $\overline{\mathcal{O}}[G]$-isomorphism, then f induces isomorphisms $L' \cong M'$ and $L'/L \cong M'/M$. Then

$$(L : M) = (L : L')(L' : M')(M' : M).$$

As $(L : L')^{-1} = (M' : M)$ and $(L' : M') = \prod_{\chi \in \widehat{G}} (L_\chi : M_\chi)$, we get the first assertion of the lemma. The second one may be proved in the same way.

□

Now we can finish the proof of the theorem. If k is unramified over ℓ, then (6.3) was proved in Step 3. By Step 2 we may assume that $\zeta_0 \in k$ if $\ell \neq 2$. So let $\zeta_0 \in k$ and k of conductor $N = \ell^m d$, where $m \geq 2$. Let k_0 be as in (6.5). As k_0 has conductor $\ell^{m_0} d$, where $m_0 = m - 1$ ($m_0 = m - 2$ if $\ell = m = 2$), we may assume that (6.3) holds true for k_0. Therefore by Lemma 6.3 we have for a given $\varphi \in \Phi$

$$(6.10) \qquad (\mathbf{R}_{k,\varphi} : \tilde{\mathcal{O}}_{k,\varphi}) = (\mathbf{N}_{k,\varphi} : \mathbf{B}_{k,\varphi})(\mathbf{R}_{k_0,\varphi} : \tilde{\mathcal{O}}_{k_0,\varphi}),$$

where by the assumption of induction we have

$$(6.11) \qquad \nu_\ell\left((\mathbf{R}_{k_0,\varphi} : \tilde{\mathcal{O}}_{k_0,\varphi})\right) = \nu_\ell\left(\prod_{\substack{\chi \in G(\widehat{k_0/\mathbf{Q}}) \\ \chi \mid \varphi}} G_{\overline{\chi}}\right).$$

For $\chi \in G(\widehat{k_0/\mathbf{Q}})$ let χ' be χ considered as a character of G. Then $\chi \mid \varphi$ if and only if $\chi' \mid \varphi$ and $g_{\overline{\chi}} = g_{\overline{\chi'}}$. So we have

$$(6.12) \qquad \prod_{\substack{\chi \in G(\widehat{k_0/\mathbf{Q}}) \\ \chi \mid \varphi,\ \chi \neq 1}} g_{\overline{\chi}} = \prod_{\substack{\chi \in \widehat{G},\ \chi \mid \varphi \\ \chi|_H = 1,\ \chi \neq 1}} g_{\overline{\chi}}.$$

It follows from Lemma 6.2 and the definition of $\mathbf{N}_k$ that $\mathbf{N}_k \cong \mathbf{B}_k$ as $\overline{\mathcal{O}}[G]$-modules. Therefore by Lemma 6.4 we have

$$(\mathbf{N}_{k,\varphi} : \mathbf{B}_{k,\varphi}) = \prod_{\substack{\chi\in\widehat{G} \\ \chi\mid\varphi}} (\mathbf{N}_{k,\chi} : \mathbf{B}_{k,\chi}). \tag{6.13}$$

Note that Sp_H annihilates $\mathbf{N}_k$ and $\mathbf{B}_k$. Hence if $\chi|_H = 1$, then $\mathbf{N}_{k,\chi} = \mathbf{B}_{k,\chi} = 0$. So we may restate (6.13) in the form

$$(\mathbf{N}_{k,\varphi} : \mathbf{B}_{k,\varphi}) = \prod_{\substack{\chi\in\widehat{G} \\ \chi\mid\varphi,\, \chi|_H\neq 1}} (\mathbf{N}_{k,\chi} : \mathbf{B}_{k,\chi}). \tag{6.14}$$

To compute the index $(\mathbf{N}_{k,\chi} : \mathbf{B}_{k,\chi})$, we shall compute at first the index $(\mathbf{N}_{K_n,\chi} : \mathbf{B}_{K_n,\chi})$, where we treat χ as a character of $G(K_n/\mathbf{Q})$. If $\chi|_H \neq 1$, then $e_\chi \mathbf{N}_{K_n} = e_\chi \mathbf{R}_{K_n} = \overline{\mathcal{O}} e_\chi f_1$, where $f_1 = (1, 0, \ldots, 0) \in \mathbf{R}_{K_n}$ is the generator of an $\overline{\mathcal{O}}[G(K_n/\mathbf{Q})]$-module $\mathbf{R}_{K_n}$ defined at the beginning of the section.

We know that $\mathbf{B}_{K_n}$ is generated over $\overline{\mathcal{O}}$ by all the elements of the form $\alpha(\varepsilon\zeta_n^i)$, where $\varepsilon \in \mu_d$ and $i \not\equiv 0 \pmod{\ell}$. Note that $\varepsilon\zeta_n^i$ is a primitive $\ell^m d_0$-th root of unity for some $d_0 \mid d$. If $\chi|_H \neq 1$, then χ has conductor $f_\chi = \ell^m d_1$ for some $d_1 \mid d$. Let ξ be a primitive $d_0\ell^m$-th root of unity for some $d_0 \mid d$. Then

$$e_\chi \alpha(\xi) = \sum_{\sigma\in G_n} \overline{\chi}(\sigma)\sigma(\xi) e_\chi f_1,$$

where $G_n = G(K_n/\mathbf{Q})$.

Let $H(\chi)$ be the kernel of the natural projection $G(K_n/\mathbf{Q}) = (\mathbf{Z}/\ell^m d\mathbf{Z})^* \to (\mathbf{Z}/f_\chi\mathbf{Z})^*$ and $H(\xi)$ be the kernel of the natural projection $G(K_n/\mathbf{Q}) = (\mathbf{Z}/\ell^m d\mathbf{Z})^* \to (\mathbf{Z}/\ell^m d_0\mathbf{Z})^*$, so $H(\chi) \cong \mathrm{Ker}((\mathbf{Z}/d\mathbf{Z})^* \to (\mathbf{Z}/d_1\mathbf{Z})^*)$ and $H(\xi) \cong \mathrm{Ker}((\mathbf{Z}/d\mathbf{Z})^* \to (\mathbf{Z}/d_0\mathbf{Z})^*)$.

If If $d_1 \not| d_0$, then, putting $G_n/H(\chi)\cap H(\xi) = S$, $H(\xi)/H(\chi)\cap H(\xi) = T \neq 1$, we get

$$\sum_{\sigma\in G_n} \overline{\chi}(\sigma)\sigma(\xi) = |H(\chi)\cap H(\xi)| \sum_{\sigma\in S} \overline{\chi}(\sigma)\sigma(\xi) =$$

$$|H(\chi)\cap H(\xi)| \sum_{\sigma\in \overline{S/T}} \sum_{\tau\in T} \overline{\chi}(\sigma\tau)\sigma\tau(\xi),$$

where $\overline{S/T} \subset S$ is a system of representatives for G/H. We have $\sigma\tau(\xi) = \sigma(\xi)$ for any $\tau \in T$ and $\sum_{\tau\in T} \overline{\chi}(\sigma\tau) = \overline{\chi}(\sigma) \sum_{\tau\in T} \overline{\chi}(\tau)$. Note that $\chi|_{H(\xi)} \neq 1$ hence $\chi|_T \neq 1$ and $\sum_{\tau\in T} \overline{\chi}(\tau) = 0$. Thus if $d_1 \nmid d_0$, then $\sum_{\sigma\in G_n} \overline{\chi}(\sigma)\sigma(\xi) = 0$.

If $d_1 | d_0$, then $H(\xi) \subseteq H(\chi)$ and, putting $A = H(\chi)/H(\xi)$, $B = G_n/H(\xi)$, $C = G_n/H(\chi)$, we get

$$\sum_{\sigma\in G_n} \overline{\chi}(\sigma)\sigma(\xi) = |H(\xi)| \sum_{\sigma\in B} \overline{\chi}(\sigma)\sigma(\xi) = \sum_{\sigma\in C} \overline{\chi}(\sigma)\sigma(\mathrm{Sp}_A(\xi)). \tag{6.15}$$

Let $d_0/d_1 = q_1^{s_1}, \ldots, q_r^{s_r}$ be the prime factorization of d_0/d_1. It is well known that, if μ is a primitive p^n-th root of unity for some prime p, then

$$\mathrm{Sp}_{\mathbf{Q}(\mu)/\mathbf{Q}}(\mu) = \begin{cases} -1 & \text{if } n = 1 \\ 0 & \text{if } n \geq 1 \end{cases}$$

Moreover, if $n \geq 1$, then $\mathrm{Sp}_{\mathbf{Q}(\mu)/\mathbf{Q}(\mu^p)}(\mu) = 0$. Thus we have

$$\mathrm{Sp}_A(\xi) = \begin{cases} 0 & \text{if } s_i \geq 1 \text{ for some } i = 1, \ldots, r \\ 0 & \text{if } d_1 \equiv 0 \pmod{q_i} \text{ for some } i = 1, \ldots, r \\ \pm\xi_1 & \text{if } s_1 = \ldots = s_r = 1 \text{ and } (d_1,\, d_0/d_1) = 1, \end{cases}$$

where ξ_1 is an $\ell^m d_1$-th primitive root of unity.

So in any case we have that

$$\sum_{\sigma\in G_n} \overline{\chi}(\sigma)\sigma(\xi) = |H(\xi)|\eta g_{\overline{\chi}}, \tag{6.16}$$

where η is a root of unity or $\eta = 0$. Therefore $e_\chi \mathbf{B}_{K_n} \subseteq \overline{\mathcal{O}} g_{\overline{\chi}} e_\chi f_1$.

Let $p_1, \ldots, p_r$ be all the prime divisors of d/d_1 such that $(p_i,\, d_1) = 1$ for $i = 1, \ldots, r$. We put $d_0 = d_1 p_1 \cdots p_r$ and $\xi = \zeta\varepsilon_{d_1}\varepsilon_{p_1} \cdots \varepsilon_{p_r}$, where we denote by ε_n a primitive n-th root of unity. Then ξ is a primitive $\ell^m d_0$-th root of unity, and for our choice of d_0 we have that $\mathrm{Sp}_A(\xi)$ in (6.15) is given by

$$\mathrm{Sp}_A(\xi) = (-1)^r \xi_1,$$

where ξ_1 is a primitive $\ell^m d_1$-th root of unity. Note that any prime divisor p of d divides d_0, hence p divides the order of $H(\xi)$ only if $p \,|\, d$. Therefore $|H(\xi)|$ is prime with ℓ. So the factor $|H(\xi)|\eta$ is a unit in $\overline{\mathcal{O}}$. This proves that

$$e_\chi \mathbf{B}_{K_n} = \overline{\mathcal{O}} g_{\overline{\chi}} e_\chi f_1 \text{ and } (\mathbf{N}_{K_n,\chi} : \mathbf{B}_{K_n,\chi}) = g_{\overline{\chi}}.$$

Now, if $\chi \in \widehat{G}$, then we can consider χ as a character of $G_n = G(K_n/\mathbf{Q})$ such that $\chi|_F = 1$. As we have the surjecions

$$(6.17) \qquad \mathrm{Sp}_F : \mathbf{N}_{K_n,\chi} \to \mathbf{N}_{k,\chi}, \ \mathrm{Sp}_F : \mathbf{B}_{K_n,\chi} \to \mathbf{B}_{k,\chi}$$

(by Lemma 6.2) and all these modules are of rank 1 over $\overline{\mathcal{O}}$, the mappings (6.17) are isomorphisms. Therefore

$$(6.18) \qquad (\mathbf{N}_{k,\chi} : \mathbf{B}_{k,\chi}) = (\mathbf{N}_{K_n,\chi} : \mathbf{B}_{K_n,\chi}) = g_{\overline{\chi}},$$

where for $\chi = 1$ we put $g_{\overline{\chi}} = 1$ by definition. Combining (6.10), (6.11), (6.12), (6.14) and (6.18) we get (6.3). This proves our theorem completely.

□

7 On some indices

Let k be a real abelian field and $\mathbf{A}_k$, $\mathbf{R}_k$, $\widetilde{\mathcal{O}}_k$ be as in Section 6. As in the introduction, we put $\mathcal{A}(k) = \prod_{v|\ell}(U(k_v)/\mu(k_v))$. For any $v|\ell$ we have an injective mapping $\log_v : U(k_v)/\mu(k_v) \to k_v$ defined by the ℓ-adic logarithm. Taking the direct product of $\log_v$ over all $v|\ell$, we get the injective mapping

$$(7.1) \qquad \log : \mathcal{A}(k) \hookrightarrow \prod_{v|\ell} k_v.$$

The mapping (7.1) is a homomorphism of the $\mathbf{Z}_\ell[G]$-modules, where $G = G(k/\mathbf{Q})$ and the action of G on $\mathcal{A}(k)$ and $\prod_{v|\ell} k_v$ is defined via the identification $\prod_{v|\ell} k_v \cong \mathbf{Q}_\ell \otimes_{\mathbf{Q}} k$. The natural inclusion $\mathbf{Q}_\ell \hookrightarrow \overline{\mathbf{Q}}_\ell$ induces the inclusion

$$i : \prod_{v|\ell} k_v \cong \mathbf{Q}_\ell \otimes_{\mathbf{Q}} k \hookrightarrow \overline{\mathbf{Q}}_\ell \otimes_{\mathbf{Q}} k = \mathbf{A}_k.$$

Putting $\mathrm{Log} = i \cdot \log$, we get an injection of $\mathbf{Z}_\ell[G]$-modules

$$(7.2) \qquad \mathrm{Log} : \mathcal{A}(k) \longrightarrow \mathbf{A}_k.$$

By $\widetilde{\mathcal{A}}(k)$ we denote the $\overline{\mathcal{O}}[G]$-submodule $\overline{\mathcal{O}} \cdot \mathrm{Log}(\mathcal{A}(k))$ of $\mathbf{A}_k$.

Let L, M be two $\mathbf{Z}_\ell$-lattices in $\prod_{v \mid \ell} k_v$ that span the same $\mathbf{Q}_\ell$-space $V \subseteq \prod_{v \mid \ell} k_v$. Then, as in [12], we define the index $(L : M)$ as $\det(A)$, where A is a $\mathbf{Q}_\ell$-linear transformation of V such that $A(L) = M$. The index $(L : M)$ is defined uniquely up to multiplication by an element of $\mathbf{Z}_\ell^*$. If $L \supseteq M$ and the index $(L : M)$ exists, then the index $[L : M]$ is finite and

$$\nu_\ell((L : M)) = \nu_\ell([L : M]).$$

If we put $\widetilde{L} = \overline{\mathcal{O}} \cdot i(L)$, $\widetilde{M} = \overline{\mathcal{O}} \cdot i(M)$, then the index $(\widetilde{L} : \widetilde{M})$ defined in Section 6 exists if and only if the index $(L : M)$ exists, and, if this is the case, then

$$\nu_\ell((L : M)) = \nu_\ell((\widetilde{L} : \widetilde{M})). \tag{7.3}$$

Let $\widetilde{\mathcal{O}}_k$ be as in Section 6.

Proposition 7.1 *The index $(\widetilde{\mathcal{A}}(k) : \widetilde{\mathcal{O}}_k)$ exists, and*

$$(\widetilde{\mathcal{O}}_k : \widetilde{\mathcal{A}}(k)) = |P(k)| \cdot |Y(k)|,$$

where $P(k) = \prod_{v \mid \ell} \overline{k}_v$, $\overline{k}_v$ is the residue field of k_v and $Y(k)$ is as in Theorem 5.1.

For any $\varphi \in \Phi$ we have

$$(\widetilde{\mathcal{O}}_{k,\varphi} : \widetilde{\mathcal{A}}(k)_\varphi) = |P(k)_\varphi| \cdot |Y(k)_\varphi|.$$

Proof. Let $\mathcal{O}_v = \mathcal{O}(k_v)$ be the ring of integers of k_v and put $\mathcal{O}_\ell = \prod_{v \mid \ell} \mathcal{O}_v$. Then by (7.3) we have

$$(\widetilde{\mathcal{O}}_k : \widetilde{\mathcal{A}}(k)) = (\mathcal{O}_\ell : \log \mathcal{A}(k)) \text{ and } (\widetilde{\mathcal{O}}_{k,\varphi} : \widetilde{\mathcal{A}}(k)_\varphi) = (\mathcal{O}_{\ell,\varphi} : (\log \mathcal{A}(k))_\varphi).$$

Let π_v be a local parameter of k_v, and put

$$U^{(i)}(k_v) = \{x \in U(k_v) \mid x \equiv 1 \pmod{\pi_v^i}\}.$$

It is well known that for all sufficiently large i the ℓ-adic logarithm $\log_v$ defines an isomorphism $\log_v : U^{(i)}(k_v) \cong \pi_v^i \mathcal{O}_v$. Hence the mapping (7.1) induces for such i the exact sequence

$$0 \longrightarrow Y(k) \longrightarrow \prod_{v \mid \ell} (U^{(1)}(k_v)/U^{(i)}(k_v)) \xrightarrow{\log^{(i)}} \prod_{v \mid \ell} (k_v/\pi_v^i \mathcal{O}_v). \tag{7.4}$$

As we have $\prod_{v|\ell}(U^{(i)}(k_v)/U^{(i+1)}(k_v)) \cong P(k)$ for any $i \geq 1$ and $\prod_{v|\ell}(\pi_v^i\mathcal{O}_v/\pi_v^{i+1}\mathcal{O}_v) \cong P(k)$ for any $i \geq 0$, we get from (7.4) that

$$(\mathcal{O}_\ell : \log \mathcal{A}(k)) = |Y(k)| \cdot |P(k)|.$$

This proves the first assertion of the proposition. The second one may be proved in the same way.

□

As in [12], we put for any G-module A

$$A_0 = \{a \in A \mid s(G)a = 0\},$$

where $s(G) = \sum_{\sigma \in G} \sigma$. We have $(A_\varphi)_0 = (A_0)_\varphi$ for any $\varphi \in \Phi$, and, if $\varphi \neq \varphi_0$, then $(A_\varphi)_0 = A_\varphi$. Thus we may write simply $A_{\varphi,0}$.

Let k have conductor $N = \ell^m d$, $(d, \ell) = 1$, and put $K_n = \mathbf{Q}(\mu_d, \zeta_n)$. To formulate our further results we recall that it was shown in the proof of Lemma 6.2 that for $\ell = 2$ we have three possibilities:

(A) The extension K_n/k is unramified over ℓ;

(B) $G(K_n/k) \cap G(K_n/K_{-1}) = \{1, \tau\}$;

(C) $G(K_n/k) \cap G(K_n/K_{-1}) = \{1, \sigma\tau\}$;

where σ, τ were defined in the proof of Lemma 6.2. Note that in the cases (B), (C) any place $v|\ell$ has the ramification index 2 in K_n/k.

Proposition 7.2 *We have*

$$(\tilde{\mathcal{O}}_{k,0} : \tilde{\mathcal{A}}(k)_0) = \ell^a |P(k)| \cdot |Y(k)|,$$

$$(\tilde{\mathcal{O}}_{k,0,\varphi_0} : \tilde{\mathcal{A}}(k)_{0,\varphi_0}) = \ell^a |P(k)_{\varphi_0}| \cdot |Y(k)_{\varphi_0}|,$$

where $a = -1$ for $\ell \neq 2$. For $\ell = 2$ we have $a = -2$ if $m = 0$. If $m > 0$, then

$$a = \begin{cases} -1 & \text{if } k \text{ is of the types (A), (C)} \\ -2 & \text{if } k \text{ is of the type (B)} \end{cases}$$

Proof. Let L, M be any $\overline{\mathcal{O}}$-lattices in $\mathbf{A}_k$ (resp. $\mathbf{Z}_\ell$-lattices in $\prod_{v|\ell} k_v$) such that L, M are G-modules, and the index $(L : M)$ exists. Then both indices $(L_0 : M_0)$ and $(\mathrm{Sp}_G(L) : \mathrm{Sp}_G(M))$ are defined, and

$$(7.5) \qquad (L : M) = (L_0 : M_0)(\mathrm{Sp}_G(L) : \mathrm{Sp}_G(M)).$$

Indeed, the analogous statement was proved in [12], Lemma 6.1, for $\mathbf{Z}$-lattices in $\mathbf{Q}[G]$. The same arguments show that (7.5) holds true for $\overline{\mathcal{O}}$-lattices or $\mathbf{Z}_\ell$-lattices as well. Hence we have to calculate the index

$$\ell^{-a} = (\mathrm{Sp}_G(\tilde{\mathcal{O}}_k) : \mathrm{Sp}_G(\tilde{\mathcal{A}}(k)) = (\mathrm{Sp}_G(\tilde{\mathcal{O}}_{k,\varphi_0}) : \mathrm{Sp}_G(\tilde{\mathcal{A}}(k)_{\varphi_0})).$$

Note that by (7.3) we have

$$(7.6) \qquad (\mathrm{Sp}_G(\tilde{\mathcal{O}}_k) : \mathrm{Sp}_G(\tilde{\mathcal{A}}(k)) = (\mathrm{Sp}_G(\mathcal{O}_\ell) : \mathrm{Sp}_G(\log \mathcal{A}(k))).$$

If G_v is the decomposition subgroup of some $v|\ell$, then

$$(\mathrm{Sp}_G(\mathcal{O}_\ell) : \mathrm{Sp}_G(\log \mathcal{A}(k)) = (\mathrm{Sp}_{G_v}(\mathcal{O}(k_v)) : \mathrm{Sp}_{G_v}(\log \overline{U}(k_v))).$$

Let $T_v \neq 1$ be the ramification subgroup of G_v. Then

$$\nu_\ell(|T_v|) = \begin{cases} m-1 & \text{if } \ell \neq 2 \\ m-1 & \ell = 2 \text{ and } k \text{ is of the type (A)} \\ m-2 & \text{if } \ell = 2 \text{ and } k \text{ is of the types (B), (C)} \end{cases}$$

If $F_v = k_v^{T_v}$, then $F_v/\mathbf{Q}_\ell$ is unramified, and $\mathrm{Sp}_{F_v/\mathbf{Q}_\ell}(\mathcal{O}_{F_v}) = \mathbf{Z}_\ell$. Let $\mathcal{D}_{k_v/\mathbf{Q}_\ell}$ be the different of $k_v/\mathbf{Q}_\ell$. Then, using the calculation in the proof of Lemma 6.2, one can check easily that in any case $\mathcal{D}_{k_v/\mathbf{Q}_\ell} \subseteq |T_v|\mathcal{O}(k_v)$, hence $\mathrm{Sp}_{G_v}(\mathcal{O}(k_v)) \subseteq T_v\mathbf{Z}_\ell$. On the other hand, $\mathrm{Sp}_{G_v}(\mathcal{O}(F_v)) = |T_v|\mathbf{Z}_\ell$. Thus in any case, including the case $T_v = 1$ we have $\mathrm{Sp}_{G_v}(\mathcal{O}(k_v)) = |T_v|\mathbf{Z}_\ell$.

To compute $\mathrm{Sp}_{G_v}(\log \overline{U}(k_v))$, we note that $\mathrm{Sp}_{G_v}(\log \overline{U}(k_v)) = \log N_{k_v/\mathbf{Q}_\ell}(U(k_v))$. By the local class field theory we have $\mathbf{Z}_\ell^*/N_{k_v/\mathbf{Q}_\ell}(U(k_v)) \cong T_v$. Taking into account that $\log(\mathbf{Z}_\ell^*) = \ell\mathbf{Z}_\ell$ if $\ell \neq 2$ (resp. $\ell^2\mathbf{Z}_\ell$ if $\ell = 2$), we get that $\mathrm{Sp}_{G_v}(\log \overline{U}(k_v)) = \ell^m\mathbf{Z}_\ell$ for $\ell \neq 2$. This proves the proposition for $\ell \neq 2$. If $\ell = 2$ and $m = 0$, then $\mathrm{Sp}_{G_v}(\log \overline{U}(k_v)) = \ell^2\mathbf{Z}_\ell$.
If $\ell = 2$, and $m > 0$, then

$$N_{k_v/\mathbf{Q}_\ell}(U(k_v)) = \begin{cases} 1 + \ell^m\mathbf{Z}_\ell & \text{if } k \text{ is of the type (A)} \\ \{\pm 1\} \times (1 + \ell^m\mathbf{Z}_\ell) & \text{if } k \text{ is of the type (B)} \\ < -(1 + \ell^{m-1}) > & \text{if } k \text{ is of the type (C).} \end{cases}$$

Therefore

$$\mathrm{Sp}_{G_v}(\log \overline{U}(k_v)) = \begin{cases} \ell|T_v|\mathbf{Z}_\ell & \text{if } k \text{ is of the type (A)} \\ \ell^2|T_v|\mathbf{Z}_\ell) & \text{if } k \text{ is of the type (B)} \\ \ell|T_v|\mathbf{Z}_\ell & \text{if } k \text{ is of the type (C).} \end{cases}$$

□

Proposition 7.3 *Let k have conductor $N = \ell^m d$, $(d, \ell) = 1$ and $G = G(k/\mathbf{Q})$. Then*

$$\nu_\ell((\mathbf{R}_{k,0} : \widetilde{O}_{k,0})) = -c + \nu_\ell \left(\prod_{\substack{\chi \in \widehat{G} \\ \chi \neq 1}} g_{\overline{\chi}} \right), \tag{7.7}$$

$$\nu_\ell((\mathbf{R}_{k,\varphi_0,0} : \widetilde{O}_{k,\varphi_0,0})) = -c + \nu_\ell \left(\prod_{\substack{\chi \in \widehat{G} \\ \chi | \varphi_0, \chi \neq 1}} g_{\overline{\chi}} \right), \tag{7.8}$$

where

$$c = \begin{cases} 0 & \textit{if } m = 0 \\ m-1 & \textit{if } m > 0 \textit{ and } \ell \neq 2 \\ m-1 & \textit{if } m > 0,\ \ell = 2 \textit{ and } k \textit{ is of the type (A)} \\ m-2 & \textit{if } m > 0,\ \ell = 2 \textit{ and } k \textit{ is of the type (B) or (C).} \end{cases}$$

Proof. The mapping $\mathrm{Sp}_G : \mathbf{A}_k \to \mathbf{A}_\mathbf{Q}$ maps $\mathbf{R}_k$ onto $\overline{\mathcal{O}}$. In the proof of Prop. 7.2 we have shown that $\mathrm{Sp}_G(\mathcal{O}_\ell) = \ell^c \mathbf{Z}_\ell$, where c is as above. Hence $\mathrm{Sp}_G(\widetilde{\mathcal{O}}_k) = \ell^c \overline{\mathcal{O}}$. Combining this with Theorem 6.1 and using (7.5), we get the proposition.

□

Let k be as in Prop. 7.3, and put $K_\infty = \bigcup_{n=1}^{\infty} \mathbf{Q}(\mu_d, \zeta_n)$. Let $\tau : G_\infty = G(K_\infty/\mathbf{Q}) \to G$ be the natural surjection induced by the inclusion $k \in K_\infty$.

Proposition 7.4 *Let k have conductor $\ell^m d$, as above, and r be the constant corresponding to τ defined by (2.5). Let k_s be the maximal subfield of k_∞ such* *that k_s/k is unramified (recall that $[k_s : k] = \ell^s$). If $m = 0$, then $s = r = 0$. If $m > 0$, then*

$$s = \begin{cases} m-1-r & \text{if } \ell \neq 2 \\ m-2-r & \text{if } \ell = 2 \text{ and } k \text{ is of the types (A), (B)} \\ m-3-r & \text{if } \ell = 2 \text{ and } k \text{ is of the type (C)} \end{cases}$$

Proof. Let $\mathbf{Q}_\infty$ be the cyclotomic $\mathbf{Z}_\ell$-extension of $\mathbf{Q}$, $\mathbf{Q}_\infty = \bigcup_{i=1}^{\infty} \mathbf{Q}_i$, where $[\mathbf{Q}_i : \mathbf{Q}] = \ell^i$. Then (2.5) shows that $\mathbf{Q}_r \subseteq k$, $\mathbf{Q}_{r+1} \not\subseteq k$, in other words, $k_i = k \cdot \mathbf{Q}_{r+i}$ for any $i \geq 1$.

If $m = 0$, then $k \subseteq \mathbf{Q}(\mu_d)$. Thus all the places $v|\ell$ are fully ramified in k_∞/k, hence we have $r = s = 0$ in this case as desired.

If $m > 0$ and $\ell \neq 2$, then K_n/k has no wild ramification. Hence the field $k_{n-r} = K_n \cap k_\infty$ has no wild ramification over k, so k_{n-r}/k is unramified. As $K_{n+1} = k_{n-r+1}K_n$, we get that k_{n-r+1} is ramified over k. Therefore $s = n - r = m - 1 - r$ in this case. If $\ell = 2$, $m > 0$, and k is of the types (A), (B), then, reasoning as before, we get $s = n - r = m - 2 - r$.

If $\ell = 2$, $m > 0$, and k is of the type (C), then we have $G(K_n/k) \cap G(K_n/K_{-1}) = \{1, \sigma\tau\}$. In this case the inertia subgroups of $v|\ell$ in $G(k_\infty/\mathbf{Q})$ and $G(K_\infty/\mathbf{Q})$ are isomorphic, hence we have $k_{n-r} = K_n \cap k_\infty$, and K_n/k_{n-r} is unramified. As K_n/k is ramified and has the ramification index 2 at any $v|\ell$, we get that k_{n-r}/k_{n-r-1} is ramified and k_{n-r-1}/k has no ramification. So $s = n - r - 1 = m - 3 - r$ in this case.

□

The diagonal injection $U(k) \hookrightarrow \prod_{v|\ell} U(k_v)$ for real abelian k induces an injective mapping $\overline{U}(k)[\ell] \hookrightarrow \mathcal{A}(k)$. So we may consider $\overline{U}(k)[\ell]$ as a subgroup of $\mathcal{A}(k)$. As $N_{k/\mathbf{Q}}(\overline{U}(k)[\ell]) = 1$, we have $\overline{U}(k)[\ell] \subseteq \mathcal{A}(k)_0$. As $\overline{U}(k)[\ell]$ and $\mathcal{A}(k)_0$ have the same $\mathbf{Z}_\ell$-rank, we get that $\overline{U}(k)[\ell]$ has a finite index in $\mathcal{A}(k)_0$.

Theorem 7.1 *Let k be a real abelian field. Let $T_\ell(k_\infty)_{(0)}$, $H(k)$ and $\widehat{U}_S(k)$ be as in Theorem 5.1. By $\mathrm{Cl}(k)_\ell$ we denote the ℓ-component of the class group of k. Let s be the constant defined in Prop. 7.4.*
Then

$$\frac{\ell^s |T_\ell(k_\infty)_{(0)}|}{|\mathrm{Cl}(k)_\ell|} = \frac{[\mathcal{A}(k)_0 : \overline{U}(k)[\ell]]}{[H(k) : \widehat{U}_S(k)]}.$$

For any $\varphi \in \Phi$, $\varphi \neq \varphi_0$ *we have*

$$\frac{|T_\ell(k_\infty)_{(0),\varphi}|}{|\mathrm{Cl}(k)_{\ell,\varphi}|} = \frac{[\mathcal{A}(k)_\varphi : \overline{U}(k)[\ell]_\varphi]}{[H(k)_\varphi : \widehat{U}_S(k)_\varphi]}.$$

If $\varphi = \varphi_0$, *then*

$$\frac{\ell^s|T_\ell(k_\infty)_{(0),\varphi_0}|}{|\mathrm{Cl}(k)_{\ell,\varphi_0}|} = \frac{[\mathcal{A}(k)_{0,\varphi_0} : \overline{U}(k)[\ell]_{\varphi_0}]}{[H(k)_{\varphi_0} : \widehat{U}_S(k)_{\varphi_0}]}.$$

Proof. Put $\mathrm{Cl}_S(k) := \mathrm{Cl}(k)/P_S(k)$, where $P_S(k)$ is the subgroup of $\mathrm{Cl}(k)$ generated by all the primes over ℓ. Let $\mathrm{Cl}_S(k)_\ell$ be the ℓ-component of $\mathrm{Cl}_S(k)$. According class field theory, we have the natural isomorphism $\mathrm{Cl}_S(k)_\ell \cong G(k_{S,\ell}/k)$, the Galois group of the maximal abelian unramified ℓ-extension of k in which all the places $v|\ell$ completely decompose. Then we have the natural mappings

$$T_\ell(k_\infty)_{(0)} \xrightarrow{\alpha} \mathrm{Cl}_S(k)_\ell \xleftarrow{\beta} \mathrm{Cl}(k)_\ell, \tag{7.9}$$

where α is induced by inclusion $k_{S,\ell} \subset M_\infty$, M_∞ be defined in Section 3, and β means factoring by $P_S(k)$. Thus β is always a surjection, whence $\mathrm{Coker}\,\alpha \cong G(k_{s_0}/k)$, $s_0 \geq 0$ being the maximal index such that all the places $v|\ell$ decompose completely in k_{s_0}/k.

To interpret the groups $\mathrm{Ker}\,\alpha$ and $\mathrm{Ker}\,\beta$, we put $\mathcal{B}(k_v) = (k_v^*/\mu(k_v))[\ell]$ for any $v|\ell$, and $\mathcal{B}(k) = \prod_{v|\ell} \mathcal{B}(k_v)$. Let denote by Γ_v the decomposition subgroup $G(k_{\infty,v}/k_v)$. Then by local class field theory we have the natural surjection $\lambda_v : \mathcal{B}(k_v) \to \Gamma_v$. On the other hand, we have the surjection $\eta_v : \mathcal{B}(k_v) \to D_v$, where $D_v \cong \mathbf{Z}_\ell$, and for $x \in k_v^*$, $x = \pi_v^n u$, $u \in U(k_v)$, π_v being a local parameter of k_v, we put $\eta_v(x) = n$. Thus, putting $\mathcal{R} = \prod_{v|\ell} \Gamma_v$, we get the natural G-homomorphisms

$$\lambda = \prod_{v|\ell} \lambda_v : \mathcal{B}(k) \to \mathcal{R}, \quad \eta = \prod_{v|\ell} \eta_v : \mathcal{B}(k) \to D_\ell := \prod_{v|\ell} D_v,$$

where G acts on $\mathcal{R}$ and D_ℓ via its acting on the set S of all the places of k over ℓ. Thus $\mathcal{R} \cong D_\ell \cong \mathbf{Z}_\ell[G/G_v]$ as Galois modules. As Γ_v is the decomposition subgroup of v in $\overline{\Gamma} = G(k_\infty/k)$, we have the natural mapping $\mathcal{R} \to \overline{\Gamma}$, the kernel of which coincides with $\mathcal{R}_0$. Then by the global class field theory we get

(7.10) $$\operatorname{Ker}\alpha = \mathcal{R}_0/\lambda(\overline{U}_S(k)[\ell]).$$

On the other hand, we have

(7.11) $$\operatorname{Ker}\beta = P_S(k) \cong D_\ell/\eta(\overline{U}_S(k)[\ell]).$$

It follows from the local class field theory that for $x \in \mathcal{B}(k_{n,v})$ we have $\lambda_v(x) = 0$ if and only if $x \in \bigcap_{n=1}^{\infty} N_{k_n/k}\mathcal{B}(k_{n,v})$. Then we get $\operatorname{Ker}\lambda = H(k)$. It follows from the definition of η that $\operatorname{Ker}\eta = \mathcal{A}(k)$. Therefore we have

$$\overline{U}_S(k)[\ell] \cap \operatorname{Ker}\lambda = \widehat{U}_S(k), \quad \overline{U}_S(k)[\ell] \cap \operatorname{Ker}\eta = \overline{U}(k)[\ell].$$

Put

$$V := \operatorname{Ker}\lambda \cap \operatorname{Ker}\eta = H(k) \cap \mathcal{A}(k);$$

$$E := \overline{U}_S(k)[\ell] \cap \operatorname{Ker}\lambda \cap \operatorname{Ker}\eta = \widehat{U}_S(k) \cap \operatorname{Ker}\eta = \overline{U}(k)[\ell] \cap \operatorname{Ker}\lambda.$$

Then we have a pair of exact sequences (in additive notation)

$$0 \longrightarrow V/E \longrightarrow \mathcal{A}(k)_0/\overline{U}(k)[\ell] \longrightarrow \mathcal{A}(k)_0/V\overline{U}(k)[\ell] \longrightarrow 0,$$

$$0 \longrightarrow V/E \longrightarrow H(k)/\widehat{U}_S(k) \longrightarrow H(k)/V\widehat{U}_S(k) \longrightarrow 0.$$

Thus we get

(7.12) $$\frac{[\mathcal{A}(k)_0 : \overline{U}(k)[\ell]]}{[H(k) : \widehat{U}_S(k)]} = \frac{[\mathcal{A}(k)_0 : V\overline{U}(k)[\ell]]}{[H(k) : V\widehat{U}_S(k)]},$$

(7.13) $$\frac{[\mathcal{A}(k)_{0,\varphi} : \overline{U}(k)[\ell]_\varphi]}{[H(k)_\varphi : \widehat{U}_S(k)_\varphi]} = \frac{[\mathcal{A}(k)_{0,\varphi} : (V\overline{U}(k)[\ell])_\varphi]}{[H(k)_\varphi : (V\widehat{U}_S(k))_\varphi]}$$

for any $\varphi \in \Phi$.

For $v|\ell$ let $\overline{\Gamma}'_v$ be the inertia subgroup of v in $\overline{\Gamma}$. Then $\Gamma'_v \subseteq \Gamma_v$, and for any $v|\ell$ $[\Gamma_v : \Gamma'_v] = \ell^u$, where $u = s - s_0$. By the local class field theory we have $\lambda(\mathcal{A}(k)) = \prod_{v|\ell} \Gamma'_v = \ell^u\mathcal{R}$. Let $\lambda' : \mathcal{B}(k) \to \mathcal{R}/\ell^u\mathcal{R}$ be the composition of λ and the natural mapping $\mathcal{R} \to \mathcal{R}/\ell^u\mathcal{R}$. Then $\operatorname{Ker}\lambda' = \mathcal{A}(k)\cdot H(k)$. Note that λ maps $\mathcal{A}(k)_0$ onto $\ell^u\mathcal{R}_0$. Therefore (7.10) induces the exact sequence

(7.14) $$0 \longrightarrow \mathcal{A}(k)_0/V\overline{U}(k)[\ell] \longrightarrow \operatorname{Ker}\alpha$$

$$\longrightarrow (\mathcal{R}_0/\ell^u\mathcal{R}_0)/\lambda'(\overline{U}_S(k)[\ell]) \longrightarrow 0.$$

Now let $\eta' : \mathcal{B}(k) \to D_\ell/\ell^u D_\ell$ be the composition of η and the natural mapping $D_\ell \to D_\ell/\ell^u D_\ell$. As all the places $v|\ell$ of k_{s_0} stay inert in k_s/k_{s_0} and totally ramify in k_∞/k_s, we get that $x \in H(k)$ implies $\eta'(x) = 0$. On the other hand, if $x \in \mathcal{B}(k)$ and $\eta'(x) = 0$, then we can find $y \in \mathcal{A}(k)$ such that $xy \in H(k)$. Therefore we have

$$\text{(7.15)} \qquad \operatorname{Ker}\eta' = \mathcal{A}(k)\cdot H(k) = \operatorname{Ker}\lambda',$$

and (7.11) induces the exact sequence

$$\text{(7.16)}\; 0 \longrightarrow H(k)/V\widehat{U}_S(k) \longrightarrow \operatorname{Ker}\beta \longrightarrow (D_\ell/\ell^u D_\ell)/\eta'(\overline{U}_S(k)[\ell]) \longrightarrow 0.$$

As $\mathcal{R} \cong D_\ell$, we have $\mathcal{R}/\ell^u\mathcal{R} \cong D_\ell/\ell^u D_\ell$. One can check easily that $(\mathcal{R}/\ell^u\mathcal{R})/(\mathcal{R}_0/\ell^u\mathcal{R}_0) \cong \mathbf{Z}/\ell^u\mathbf{Z}$ (with trivial action of G). By (7.15) we have

$$\lambda'(\overline{U}_S(k)[\ell]) \cong \overline{U}_S(k)[\ell]/(\overline{U}_S(k)[\ell] \cap \mathcal{A}(k)\cdot H(k)) \cong \eta'(\overline{U}_S(k)[\ell]).$$

So we get from (7.14) and (7.16)

$$\text{(7.17)} \qquad \frac{[\mathcal{A}(k)_0 : V\overline{U}(k)[\ell]]}{[H(k) : V\widehat{U}_S(k)]} = \ell^{-u}\frac{|(\operatorname{Ker}\alpha)|}{|\operatorname{Ker}\beta|},$$

$$\text{(7.18)} \qquad \frac{[\mathcal{A}(k)_{0,\varphi} : (V\overline{U}(k)[\ell])_\varphi]}{[H(k)_\varphi : (V\widehat{U}_S(k))_\varphi]} = \ell^{-u_\varphi}\frac{|(\operatorname{Ker}\alpha)_\varphi|}{|(\operatorname{Ker}\beta)_\varphi|},$$

where $u_\varphi = 0$, if $\varphi \neq \varphi_0$, $u_\varphi = u$, if $\varphi = \varphi_0$.

Combining (7.12), (7.17), (7.9), we get the first formula of the theorem. To prove the last two formulae of the theorem, we have to combine (7.13), (7.18) and (7.9).

□

The next result is an analog of Theorem 5.1.

Theorem 7.2 *For any real abelian k and any $\varphi \in \Phi$ we have*

$$\nu_\ell(|\mathrm{Cl}(k)_\ell|) = \nu_\ell\left(\ell^{s+t}|Y(k)|^{-1}[\mathcal{A}(k)_0 : \overline{U}(k)[\ell]]^{-1}\prod_{\substack{\chi\in\widehat{G}\\ \chi\neq 1}}\frac{1}{2}L_\ell(1,\ \chi)\right),$$

$$\nu_\ell(|\mathrm{Cl}(k)_{\ell,\varphi}|) = \nu_\ell\left(\ell^{s_\varphi+t_\varphi}|Y(k)_\varphi|^{-1}[\mathcal{A}(k)_{0,\varphi} : \overline{U}(k)[\ell]_\varphi]^{-1} \prod_{\substack{\chi\in\widehat{G}\\ \chi|\varphi,\chi\neq 1}} \frac{1}{2}L_\ell(1,\ \chi)\right),$$

where t, t_φ are defined in Theorem 5.1, s is as in Prop. 7.4 and $s_\varphi = 0$ for $\varphi \neq \varphi_0$, $s_{\varphi_0} = s$.

Proof. The theorem follows immediately from Theorem 5.1 and Theorem 7.1.

□

Put $\widetilde{U}(k) = \overline{\mathcal{O}}\cdot\mathrm{Log}(\overline{U}(k)[\ell])$, where Log is the mapping defined by (7.2). Then the index $(\widetilde{\mathcal{A}}(k)_0 : \widetilde{U}(k))$ exists and

$$(\widetilde{\mathcal{A}}(k)_0 : \widetilde{U}(k)) = (\mathcal{A}(k)_0 : \overline{U}(k)[\ell]),\quad (\widetilde{\mathcal{A}}(k)_{0,\varphi} : \widetilde{U}(k)_\varphi) = (\mathcal{A}(k)_{0,\varphi} : \overline{U}(k)[\ell]_\varphi).$$

Theorem 7.3 *For any real abelian k and any $\varphi \in \Phi$ we have*

$$\nu_\ell(|\mathrm{Cl}(k)_\ell|) = \nu_\ell\left((\mathbf{R}_{k,0} : \widetilde{U}(k))^{-1} \prod_{\substack{\chi\in\widehat{G}\\ \chi\neq 1}} \frac{1}{2}a(\chi)\right),$$

$$\nu_\ell(|\mathrm{Cl}(k)_{\ell,\varphi}|) = \nu_\ell\left((\mathbf{R}_{k,0,\varphi} : \widetilde{U}(k)_\varphi)^{-1} \prod_{\substack{\chi\in\widehat{G}\\ \chi|\varphi,\chi\neq 1}} \frac{1}{2}a(\chi)\right),$$

where for $\chi \neq 1$

(7.19) $$a(\chi) = \sum_{\substack{a \pmod{f_\chi}\\ (a,f_\chi)=1}} \overline{\chi}(a)\log(1-\varepsilon_\chi^a),$$

f_χ is the conductor of χ and ε_χ is a primitive f_χ-th root of unity (note that $\nu_\ell(a(\chi))$ does not depend on the choice of ε_χ).

Proof. We have

$$(\mathbf{R}_{k,0} : \widetilde{U}(k)) = (\mathbf{R}_{k,0} : \widetilde{\mathcal{O}}_{k,0})(\widetilde{\mathcal{O}}_{k,0} : \widetilde{\mathcal{A}}_{k,0})(\widetilde{\mathcal{A}}_{k,0} : \widetilde{\mathcal{U}}(k))$$

and

$$(\mathbf{R}_{k,0,\varphi} : \widetilde{U}(k)_\varphi) = (\mathbf{R}_{k,0,\varphi} : \widetilde{\mathcal{O}}_{k,0,\varphi})(\widetilde{\mathcal{O}}_{k,0,\varphi} : \widetilde{\mathcal{A}}_{k,0,\varphi})(\widetilde{\mathcal{A}}_{k,0,\varphi} : \widetilde{U}(k)_\varphi)$$

for any $\varphi \in \Phi$.

It follows from (7.3) that

$$[\mathcal{A}(k)_0 : \overline{U}(k)[\ell]] = (\widetilde{\mathcal{A}}_{k,0} : \widetilde{U}(k)),$$

$$[\mathcal{A}(k)_{0,\varphi} : \overline{U}(k)[\ell]_\varphi] = (\widetilde{\mathcal{A}}_{k,0,\varphi} : \widetilde{U}(k)_\varphi),$$

for any $\varphi \in \Phi$.
Then we get from Theorem 7.2

$$\nu_\ell(|\mathrm{Cl}(k)_\ell|) = \tag{7.20}$$

$$\nu_\ell\left(\ell^{s+t}|Y(k)|^{-1}(\mathbf{R}_{k,0} : \widetilde{U}(k))^{-1}(\mathbf{R}_{k,0} : \widetilde{\mathcal{O}}_{k,0})(\widetilde{\mathcal{O}}_{k,0} : \widetilde{\mathcal{A}}_{k,0}) \prod_{\substack{\chi\in\widehat{G} \\ \chi\neq 1}} \frac{1}{2}L_\ell(1,\ \chi)\right),$$

$$\nu_\ell(|\mathrm{Cl}(k)_{\ell,\varphi}|) = \nu_\ell\left(\ell^{s_\varphi+t_\varphi}|Y(k)_\varphi|^{-1}\right) + \tag{7.21}$$

$$\nu_\ell\left((\mathbf{R}_{k,0,\varphi} : \widetilde{U}(k)_\varphi)^{-1}(\mathbf{R}_{k,0,\varphi} : \widetilde{\mathcal{O}}_{k,0,\varphi})(\widetilde{\mathcal{O}}_{k,0,\varphi} : \widetilde{\mathcal{A}}_{k,0,\varphi}) \prod_{\substack{\chi\in\widehat{G} \\ \chi|\varphi,\chi\neq 1}} \frac{1}{2}L_\ell(1,\ \chi)\right).$$

It follows from Theorem 5.1 and Prop. 7.4 that

$$s+t = \begin{cases} m-2 & \text{if } \ell = 2 \text{ and } k \text{ is of the type (C)} \\ m-1 & \text{in all the other cases} \end{cases}$$

and

$$s_\varphi + t_\varphi = 0 \text{ if } \varphi \neq \varphi_0;\ \ s_{\varphi_0} + t_{\varphi_0} = s+t.$$

From Prop. 7.1, 7.2, 7.3 and Theorem 6.1 we get that

$$\nu_\ell((\mathbf{R}_{k,0} : \widetilde{\mathcal{O}}_{k,0})(\widetilde{\mathcal{O}}_{k,0} : \widetilde{\mathcal{A}}_{k,0})) = \nu_\ell\left(|P(k)| \cdot |Y(k)| \cdot \ell^{a-c} \prod_{\substack{\chi\in\widehat{G} \\ \chi\neq 1}} g_{\overline{\chi}}\right),$$

$$\nu_\ell((\mathbf{R}_{k,0,\varphi} : \tilde{O}_{k,0,\varphi})(\tilde{O}_{k,0,\varphi} : \tilde{A}_{k,0,\varphi})) = \nu_\ell\left(|P(k)_\varphi| \cdot |Y(k)_\varphi| \cdot \ell^{a_\varphi - c_\varphi} \prod_{\substack{\chi\in\widehat{G} \\ \chi|\varphi,\chi\neq 1}} g_{\overline{\chi}} \right),$$

where a (resp. c) is defined in Prop. 7.2 (resp. Prop. 7.3); $a_\varphi = c_\varphi = 0$ if $\varphi \neq \varphi_0$; and $a_{\varphi_0} = a$, $c_{\varphi_0} = c$.

If $m = 0$, then

$$a - c = \begin{cases} -1 & \text{if } \ell \neq 2 \\ -2 & \text{if } \ell = 2. \end{cases}$$

If $m > 0$, then

$$a - c = \begin{cases} -m + 1 & \text{if } \ell = 2 \text{ and } k \text{ is of the type (C)} \\ -m & \text{in all the other cases.} \end{cases}$$

Hence $s + t + a - c = -1$ in any case. Then it follows from (7.20) and (7.21) that

(7.22)
$$\nu_\ell(|\mathrm{Cl}(k)_\ell|) =$$
$$\nu_\ell\left((\mathbf{R}_{k,0} : \tilde{U}(k))^{-1} \cdot \ell^{-1} |P(k)| \prod_{\substack{\chi\in\widehat{G} \\ \chi\neq 1}} \frac{1}{2} g_{\overline{\chi}} L_\ell(1,\ \chi) \right),$$

(7.23)
$$\nu_\ell(|\mathrm{Cl}(k)_{\ell,\varphi}|) =$$
$$\nu_\ell\left((\mathbf{R}_{k,0,\varphi} : \tilde{U}(k)_\varphi)^{-1} \cdot \ell^{b} |P(k)_\varphi| \prod_{\substack{\chi\in\widehat{G} \\ \chi|\varphi,\chi\neq 1}} \frac{1}{2} g_{\overline{\chi}} L_\ell(1,\ \chi) \right),$$

where $b = -1$ if $\varphi = \varphi_0$; $b = 0$ if $\varphi \neq \varphi_0$.

It is well known (see [9], for example) that for $\chi \neq 1$

$$L_\ell(1,\ \chi) = -\left(1 - \frac{\chi(\ell)}{\ell}\right) \frac{g_\chi}{f_\chi} a(\chi).$$

As $g_\chi g_{\overline{\chi}} = f_\chi \cdot \chi(-1)$, we have

(7.24)
$$g_{\overline{\chi}} L_\ell(1,\ \chi) = \pm\left(1 - \frac{\chi(\ell)}{\ell}\right) a(\chi).$$

Note that

$$\nu_\ell\left(1-\frac{\chi(\ell)}{\ell}\right)=\begin{cases}0 & \text{if } \chi(\ell)=0\\ -1 & \text{if } \chi(\ell)\neq 0.\end{cases}$$

Let k' be the maximal subfield of k such that ℓ is unramified in $k'/\mathbf{Q}$. Then for $\chi\in\widehat{G}$ we have $\chi(\ell)=0$ if and only if $\chi|_{G(k/k')}=1$, in other words, χ is a character of $G(k'/\mathbf{Q})$. Taking into account that $P(k)\cong\mathbf{Z}/\ell\mathbf{Z}[G(k'/\mathbf{Q})]$ as a Galois module, we get

$$\nu_\ell\left(\prod_{\substack{\chi\in\widehat{G}\\ \chi\neq 1}}\left(1-\frac{\chi(\ell)}{\ell}\right)\right)=\nu_\ell(\ell\,|P(k)|), \tag{7.25}$$

$$\nu_\ell\left(\prod_{\substack{\chi\in\widehat{G}\\ \chi|\varphi,\chi\neq 1}}\left(1-\frac{\chi(\ell)}{\ell}\right)\right)=\nu_\ell(\ell^{-b}|P(k)_\varphi|), \tag{7.26}$$

where $b=-1$ if $\varphi=\varphi_0$; $b=0$ if $\varphi\neq\varphi_0$. Combining (7.22), (7.24) and (7.25), we get the first formula of the theorem. To prove the second formula, we have to combine (7.23), (7.24) and (7.26).

□

Remark 1. It is well known that for any $\chi\in\widehat{G}$, $\chi\neq 1$ we have $a(\chi)\neq 0$.
Remark 2. Theorem 7.3 may be considered as an ℓ-adic analytic class number formula for the order of $\mathrm{Cl}(k)_{\ell,\varphi}$. The index $(\mathbf{R}_{k,0,\varphi}:\widetilde{U}(k)_\varphi)$ may be considered as a φ-component of the ℓ-adic regulator of k.

For a real abelian field k with the Galois group $G=G(k/\mathbf{Q})$ put $\mathcal{R}_k=\mathbf{Z}_\ell[G]$. Let $\mathbf{R}_k$ be as in Theorem 7.3. Let be given a $\mathcal{R}_k$-submodule $\mathcal{U}_k\subset\mathbf{Q}_\ell[G]$ such that the index $(\mathcal{R}_{k,0}:\mathcal{U}_{k,0})$ is defined. Put $\mathbf{U}_k=\overline{\mathcal{O}}\cdot\mathcal{U}_k\subset\mathbf{A}_k$. Suppose given a $\mathcal{R}_k$-submodule $\mathcal{T}_k$ of $\overline{U}(k)[\ell]\otimes_{\mathbf{Z}_\ell}\mathbf{Q}_\ell$ such that the group $\overline{U}(k)[\ell]\cap\mathcal{T}_k$ has finite index both in $\overline{U}(k)[\ell]$ and in $\mathcal{T}_k$. (Note that $\mathcal{T}_k=\mathcal{T}_{k,0}$). Let $C_k\subseteq\overline{U}(k)[\ell]\cap\mathcal{T}_k$ be a subgroup such that C_k has finite index both in $\overline{U}(k)[\ell]$ and $\mathcal{T}_k$. Put $\mathbf{T}_k=\overline{\mathcal{O}}\cdot\mathrm{Log}(\mathcal{T}_k)$ and $\mathbf{C}_k=\overline{\mathcal{O}}\cdot\mathrm{Log}C_k$, where Log is the mapping (7.2).

Theorem 7.4 *Let $\mathcal{R}_k$, $\mathbf{R}_k$, $\mathcal{U}_k$, $\mathbf{U}_k$, $\mathcal{T}_k$, $\mathbf{T}_k$ and C_k, $\mathbf{C}_k$ be as above. Let $\mathbf{U}_{k,0}$ and $\mathbf{T}_k$ be isomorphic as $\mathbf{R}_k$-modules and $e_\chi\mathbf{T}_k=\frac{1}{2}a(\chi)e_\chi\mathbf{U}_k$ for any*

$\chi \in \widehat{G}, \chi \neq 1$. *Then*

$$|\mathrm{Cl}(k)_\ell| = (\mathcal{R}_{k,0} : \mathcal{U}_{k,0})^{-1}[\mathcal{T}_k : C_k]^{-1}[\overline{U}(k)[\ell] : C_k]$$

and

$$|\mathrm{Cl}(k)_{\ell,\varphi}| = (\mathcal{R}_{k,0,\varphi} : \mathcal{U}_{k,0,\varphi})^{-1}[\mathcal{T}_{k,\varphi} : C_{k,\varphi}]^{-1}[\overline{U}(k)[\ell]_\varphi : C_{k,\varphi}]$$

for any $\varphi \in \Phi$.

Proof. By Lemma 6.4 we have

$$\nu_\ell((\mathbf{U}_{k,0} : \mathbf{T}_k)) = \nu_\ell\left(\prod_{\substack{\chi\in\widehat{G}\\ \chi\neq 1}} \frac{1}{2}a(\chi)\right)$$

and

$$\nu_\ell((\mathbf{U}_{k,0,\varphi} : \mathbf{T}_{k,\varphi})) = \nu_\ell\left(\prod_{\substack{\chi\in\widehat{G}\\ \chi|\varphi,\chi\neq 1}} \frac{1}{2}a(\chi)\right)$$

for any $\varphi \in \Phi$. Then by Theorem 7.3 we have

$$\nu_\ell(|\mathrm{Cl}(k)_\ell|) = \nu_\ell\left((\mathbf{R}_{k,0} : \widetilde{U}(k))^{-1}\prod_{\substack{\chi\in\widehat{G}\\ \chi\neq 1}} \frac{1}{2}a(\chi)\right) =$$

$$(\mathbf{R}_{k,0} : \mathbf{U}_{k,0})^{-1}(\widetilde{U}(k) : \mathbf{R}_{k,0})(\mathbf{R}_{k,0} : \mathbf{U}_{k,0})(\mathbf{U}_{k,0} : \mathbf{T}_k)(\mathbf{T}_k : \mathbf{C}_k)(\mathbf{T}_k : \mathbf{C}_k)^{-1}$$
$$= (\mathbf{R}_{k,0} : \mathbf{U}_{k,0})^{-1}(\mathbf{T}_k : \mathbf{C}_k)^{-1}(\widetilde{U}(k) : \mathbf{C}_k).$$

By (6.4) we have

$$(\mathbf{R}_{k,0} : \mathbf{U}_{k,0}) = (\mathcal{R}_{k,0} : \mathcal{U}_{k,0}),$$
$$(\mathbf{T}_k : \mathbf{C}_k) = (\mathcal{T}_k : C_k) = [\mathcal{T}_k : C_k],$$
$$(\widetilde{U}(k) : \mathbf{C}_k) = (\overline{U}(k)[\ell] : C_k) = [\overline{U}(k)[\ell] : C_k].$$

This proves the first formula of the theorem. The last formula may be proved by the same arguments.

□

8 The proof of Theorem 1

In this section we define the modules $\mathcal{U}_k$ and $\mathcal{T}_k$ satisfying the conditions of Theorem 7.4 for $k = K^+ = \mathbf{Q}(\epsilon_m + \epsilon_m^{-1})$, the maximal real subfield of the cyclotomic field $K = \mathbf{Q}(\epsilon_m)$. Our results are based on that of [12], so we adopt here some notations of [12].

Let $\mathcal{G} \cong (\mathbf{Z}/m\mathbf{Z})^*$ be the Galois group of $K/\mathbf{Q}$. If $m = \prod_i p_i^{s_i}$ is the prime decomposition of m, then $\mathcal{G}$ is the internal direct product of the inertia subgroups $T_{p_i} \cong (\mathbf{Z}/p_i^{s_i}\mathbf{Z})^*$:

$$\mathcal{G} = \prod_{p\,|\,m} T_p.$$

For $p\,|\,m$ put $e_p = |T_p|^{-1} \sum_{\sigma \in T_p} \sigma$. As in [12], put $\overline{\sigma}_p = \lambda_p^{-1} e_p$, where $\lambda_p \in \mathcal{G}$ and $\lambda_p \bmod T_p$ is the Frobenius automorphism of $K^{T_p}/\mathbf{Q}$ corresponding to p. For $f|m$ let H_f be the kernel of the natural surjection $(\mathbf{Z}/m\mathbf{Z})^* \to (\mathbf{Z}/f\mathbf{Z})^*$. Put $\mathcal{R} := \mathbf{Z}_\ell[\mathcal{G}]$.

We define the $\mathcal{R}$-module $\mathcal{U} \subset \mathbf{Q}_\ell[\mathcal{G}]$ to be the ℓ-completion of $\mathbf{Z}[\mathcal{G}]$-module $\mathcal{U}$ defined in [12], Section 2, that is, $\mathcal{U}$ is a $\mathbf{Z}_\ell[\mathcal{G}]$-module generated in $\mathbf{Q}_\ell[\mathcal{G}]$ by the elements

$$\alpha_f = s(H_f) \prod_{p\,|\,f} (1 - \overline{\sigma}_p), \qquad 1 \le f \le m, \quad f\,|\,m,$$

the product taken over the primes p dividing f. The next statement is an immediate consequence of [12], Prop. 5.1.

Proposition 8.1 *For prime $p\,|\,m$ let $\mathcal{U}_p$ be the $\mathcal{R}$-module generated in $\mathbf{Q}_\ell[\mathcal{G}]$ by $s(T_p) = \sum_{\sigma \in T_p} \sigma$ and $1 - \overline{\sigma}_p$:*

$$\mathcal{U}_p = \mathcal{R}s(T_p) + \mathcal{R}(1 - \overline{\sigma}_p).$$

Then

(8.1) $$\mathcal{U} = \prod_{p\,|\,m} \mathcal{U}_p,$$

where the product is taken over the primes $p\,|\,m$, and $\prod$ means multiplication in the group algebra $\mathbf{Q}_\ell[\mathcal{G}]$.

As in [12], put $\overline{m} = \prod_{p\,|\,m} p$, and for any $r\,|\,\overline{m}$ put

$$\mathcal{U}_r = \prod_{p\,|\,r} \mathcal{U}_p,\ \ T_r = \prod_{p\,|\,r} T_p.$$

We have $\mathcal{U}_1 = \mathcal{R}$, $T_1 = \{1\}$ by definition, and $\mathcal{U}_{\overline{m}} = \mathcal{U}, T_{\overline{m}} = \mathcal{G}$. Note that any $\mathcal{U}_p$ is a full $\mathbf{Z}_\ell$-lattice in $\mathbf{Q}_\ell[\mathcal{G}]$.

If $r\,|\,\overline{m}$, $p\,|\,\overline{m}$ and $(p, r) = 1$, then we have a pair of exact sequences of $\mathcal{R}$-modules

(8.2) $$0 \longrightarrow \mathcal{U}_r^{T_p} \longrightarrow \mathcal{U}_r \longrightarrow Y \longrightarrow 0,$$

(8.3) $$0 \longrightarrow \mathcal{U}_{rp}^{T_p} \longrightarrow \mathcal{U}_{rp} \longrightarrow Y \longrightarrow 0$$

(see [12], (5.3) and (5.4)). Here $Y = (1 - e_p)\mathcal{U}_r = (1 - e_p)\mathcal{U}_{rp}$, and the surjections in (8.2) and (8.3) are the maps induced by multiplication by $1 - e_p$.

The next two lemmas are the exact analogs for $\mathbf{Q}_\ell[\mathcal{G}]$-modules of Lemmas 5.1 and 5.2 of [12], and may be proved by the same arguments:

Lemma 8.1 *Let H be a subgroup of $\mathcal{G}$ such that $H \cap T_p = \{1\}$. Let A be any HT_p-submodule of $\mathbf{Q}_\ell[\mathcal{G}]$ such that A is free over $\mathbf{Z}_\ell[HT_p]$. Then A^{T_p} and $(1 - e_p)A$ are both free over $\mathbf{Z}_\ell[H]$.*

Lemma 8.2 *Let A be an $\mathcal{R}$-submodule of $\mathbf{Q}_\ell[\mathcal{G}]$. Then*

$$(A\mathcal{U}_p)^{T_p} = s(T_p)A + (1 - \lambda_p^{-1})A^{T_p}.$$

Hence if A is free over T_p, then

$$(A\mathcal{U}_p)^{T_p} = A^{T_p} = s(T_p)A.$$

From now we fix a cyclic subgroup $H \subset \mathcal{G}$ such that $H \cap T_r = \{1\}$ for any $r\,|\,\overline{m}$, $r \neq \overline{m}$. For the aims of this section it is enough to put $H = J = \{1, j\}$, where j is the automorphism of complex conjugation. In the next section we shall deal with some other types of H.

Proposition 8.2 *Let r and r' be relatively prime divisors of $\overline{m}$. Then $\mathcal{U}_r$ is a free $HT_{r'}$-module. If, in addition, $rr' \neq \overline{m}$, then $\mathcal{U}_r$ is a free $HT_{r'}$-module.*

To prove this proposition, we have to repeat the proof of Prop. 5.2 of [12], replacing U_r by $\mathcal{U}_r$ and J by H. Note that the only property of J that is used in that proof is: $J \cap T_r = \{1\}$ for any $r \neq \overline{m}$.

□

As a consequence, we have that for $(p, r) = 1$

$$\mathcal{U}_r^{T_p} = \mathcal{U}_{rp}^{T_p}. \tag{8.4}$$

Indeed, $\mathcal{U}_r$ is T_p-free, hence $\mathcal{U}_r^{T_p} = s(T_p)\mathcal{U}_r$, and (8.4) follows from Lemma 8.2.

Now we are going to calculate some cohomology groups arising from $\mathcal{U}$ and $\mathcal{U}_r$. Let A be an $\mathcal{R}$-module and F be a subgroup of $\mathcal{G}$. Then the Tate cohomology groups $H^q(F, A)$ are $\mathcal{G}/F$-modules and hence $\mathcal{G}$-modules in the natural way. If $E \supseteq F$ are subgroups of $\mathcal{G}$, then $\mathrm{Res}: H^q(E, A) \to H^q(F, A)$ and $\mathrm{Inf}: H^q(E/F, A^F) \to H^q(E, A)$ are $\mathcal{G}$-maps for any $q > 0$.

The next proposition is an exact analog of Prop. 5.3 of [12] and may be proved by the same arguments (with U_r replaced by $\mathcal{U}_r$ and J by H).

Proposition 8.3 *Let r and r' be relatively prime, and suppose that neither r nor r' is equal to $\overline{m}$.*
Then for all $q > 0$ we have

$$H^q(T_{r'}, \mathcal{U}_r^H) \cong H^q(HT_{r'}, \mathcal{U}_r) \cong H^q(H, \mathcal{U}_r^{T_{r'}}).$$

These are $\mathcal{G}$-module isomorphism. Moreover, these groups are trivial unless $rr' = \overline{m}$.

As in [12], Section 5, for any $q > 0$ and any $r \mid m$ we put $r' = \overline{m}/r$ and

$$A_r^q = H^q(H, \mathcal{U}_r^{T_{r'}}).$$

Lemma 8.3 *For any $q > 0$ and $r|m$ $\mathcal{G}$ acts trivially on A_r^q.*

This lemma may be proved by the same arguments as Lemma 5.3 of [12].

□

Lemma 8.4 *Suppose that $p \nmid r$. For any integer $q > 0$, there is an exact sequence*

$$0 \longrightarrow A_r^q \longrightarrow A_{rp}^q \longrightarrow A_r^{q+1} \longrightarrow 0.$$

This lemma may be proved by the same arguments as Lemma 5.4 of [12].

□

Remark. It follows from the proof given in [12] that the injection $A^q_r \to A^q_{rp}$ of Lemma 8.4 is induced by the natural inclusion of H-modules:

$$\mathcal{U}_r^H = \mathcal{U}_{rp}^H \hookrightarrow \mathcal{U}_{rp}.$$

Proposition 8.4 *Let n be the number of primes dividing r. If $n = 0$, we have, for any q,*

$$A_1^q = \begin{cases} 0 & \text{if } q \text{ is odd} \\ \mathbf{Z}_\ell/|H|\mathbf{Z}_\ell & \text{if } q \text{ is even} \end{cases}$$

If $n > 0$, we have

$$A_r^q \cong (\mathbf{Z}_\ell/|H|\mathbf{Z}_\ell)^{2^{n-1}}$$

for any $q > 0$.

Proof. As H is cyclic, it is enough to consider the case $q > 0$. If $n = 0$, then $r = 1$, $\mathcal{U}_1 = \mathcal{R}$ and

$$A_1^q = H^q(H, \mathcal{R}^{\mathcal{G}}) = H^q(H, \mathbf{Z}_\ell),$$

from which the first statement of the proposition follows. As $|H| \cdot A_r^q = 0$ for any q, r and A_r^q are ℓ-groups, all A_r^q are $(\mathbf{Z}_\ell/|H|\mathbf{Z}_\ell)$-modules. Using Lemma 8.4, we can prove by induction that all A_r^q are $(\mathbf{Z}_\ell/|H|\mathbf{Z}_\ell)$-free. Then the second statement of the proposition follows from Lemma 8.4.

□

Put $G = \mathcal{G}/H$, $G = G_\ell \times G_0$, where G_ℓ is the ℓ-Sylow subgroup of G and $(|G_0|, \ell) = 1$. Let Φ be the set of all $\mathbf{Q}_\ell$-irreducible characters of G_0.

Theorem 8.1 *Let H be a cyclic subgroup of G such that $H \cap T_r = \{1\}$ for any $r \,|\, \overline{m}$, $r \neq \overline{m}$. Let g be the number of distinct prime divisors of m. If $g = 1$, then*

$$\nu_\ell((\mathcal{U}^H : \mathcal{R}^H)) = 0,$$
$$\nu_\ell((\mathcal{R}^H : \mathrm{Sp}_H \mathcal{U})) = \nu_\ell(|H|).$$

If $g \geq 2$, then

$$\nu_\ell((\mathcal{U}^H : \mathcal{R}^H)) = \nu_\ell((\mathcal{R}^H : \mathrm{Sp}_H \mathcal{U})) = 2^{g-2}\nu_\ell(|H|).$$

Let Φ be as above. Then, for any $\varphi \in \Phi$, we have:
If $g = 1$, then

$$\nu_\ell((\mathcal{U}^H_\varphi : \mathcal{R}^H_\varphi)) = 0, \quad \nu_\ell((\mathcal{R}^H_\varphi : \mathrm{Sp}_H \mathcal{U}_\varphi)) = \begin{cases} 0 & \text{if } \varphi \neq \varphi_0 \\ \nu_\ell(|H|) & \text{if } \varphi = \varphi_0. \end{cases}$$

If $g \geq 2$, then

$$\nu_\ell((\mathcal{U}^H_\varphi : \mathcal{R}^H_\varphi)) = \nu_\ell((\mathcal{R}^H_\varphi : \mathrm{Sp}_H \mathcal{U}_\varphi)) = \begin{cases} 0 & \text{if } \varphi \neq \varphi_0 \\ 2^{g-2}\nu_\ell(|H|) & \text{if } \varphi = \varphi_0. \end{cases}$$

Proof. Let $p_1, \ldots, p_g$ be the primes dividing m. Let $r_i = p_1 \cdots p_i$, $i = 1, \ldots, g$ and $r_0 = 1$. We have $\mathcal{U}_{r_0} = \mathcal{R}$, $\mathcal{U}_{r_g} = \mathcal{U}_{\overline{m}} = \mathcal{U}$. Hence

$$(\mathcal{U}^H : \mathcal{R}^H) = \prod_{i=1}^{g} (\mathcal{U}^H_{r_i} : \mathcal{U}^H_{r_{i-1}})$$

and

$$(\mathcal{U}^H_\varphi : \mathcal{R}^H_\varphi) = \prod_{i=1}^{g} (\mathcal{U}^H_{r_i,\varphi} : \mathcal{U}^H_{r_{i-1},\varphi})$$

for any $\varphi \in \Phi$.

For $i = 1, \ldots, g$ put $r_{i-1} = r$, $p_i = p$, $r_i = rp$. To compute the index $(\mathcal{U}^H_r : \mathcal{U}^H_{rp})$, we note that the exact sequences (8.2), (8.3) and equality (8.4) yield a pair of exact sequences of G-modules

$$(8.5) \qquad \begin{array}{ccccccccc} 0 \longrightarrow \mathcal{U}^{HT_p}_r & \longrightarrow & \mathcal{U}^H_r & \xrightarrow{\alpha} & Y^H & \xrightarrow{\gamma} & H^1(H, \mathcal{U}^{T_p}_r) & \longrightarrow & H^1(H, \mathcal{U}_r) \\ \| & & & & \| & & \| & & \\ 0 \longrightarrow \mathcal{U}^{HT_p}_{rp} & \longrightarrow & \mathcal{U}^H_{rp} & \xrightarrow{\beta} & Y^H & \xrightarrow{\delta} & H^1(H, \mathcal{U}^{T_p}_{rp}) & \xrightarrow{\epsilon} & H^1(H, \mathcal{U}_{rp}). \end{array}$$

Since $r \neq \overline{m}$, it follows from Prop. 8.3 that $H^1(H, \mathcal{U}_r) = 0$, hence γ is a surjection. On the other hand, ϵ is an injection (see Remark after Lemma 8.4). Therefore $\delta = 0$ and β is a surjection. Thus we have

$$(8.6) \qquad (\mathcal{U}^H_{rp} : \mathcal{U}^H_r) = (\mathcal{U}^{HT_p}_{rp} : \mathcal{U}^{HT_p}_r)(\mathrm{Im}\,\beta : \mathrm{Im}\,\alpha) =$$

$$(\mathrm{Im}\,\beta : \mathrm{Im}\,\alpha) = |\mathrm{Coker}\alpha| \cdot |\mathrm{Coker}\beta|^{-1} = |\mathrm{Coker}\alpha| = |H^1(H,\ \mathcal{U}_r^{T_p})|.$$

If $g = 1$, then $r = 1$, $\mathcal{U}_r^{T_p} \cong \mathbf{Z}_\ell$ and $H^1(H,\ \mathcal{U}_r^{T_p}) = 0$. Hence $(\mathcal{U}^H : \mathcal{R}^H) = 1$ in this case. By Prop. 8.4 $\mathcal{U}^H/\mathrm{Sp}_H\mathcal{U} \cong (\mathbf{Z}_\ell/|H|\mathbf{Z}_\ell)$, hence $\nu_\ell((\mathcal{R}^H : \mathrm{Sp}_H\mathcal{U})) = \nu_\ell(|H|)$.

If $g > 1$ and $rp \neq \overline{m}$ in (8.5), then by Prop. 8.3 $H^1(H,\ \mathcal{U}_r^{T_p}) = 0$, hence by (8.6) we have $(\mathcal{U}_{rp}^H : \mathcal{U}_r^H) = 1$. If $rp = \overline{m}$, then by (8.6) and Prop. 8.4 we have

$$\nu_\ell((\mathcal{U}_{rp}^H : \mathcal{U}_r^H)) = \nu_\ell(|H^1(H,\ \mathcal{U}_r^{T_p})|) = 2^{g-2}\nu_\ell(|H|).$$

By Prop. 8.4 $\nu_\ell((\mathcal{U}^H : \mathrm{Sp}_H\mathcal{U})) = 2^{g-1}\nu_\ell(|H|)$, hence $\nu_\ell((\mathcal{R}^H : \mathrm{Sp}_H\mathcal{U})) = 2^{g-2}\nu_\ell(|H|)$. This proves the first two statements of the theorem.

If $\varphi \in \Phi$, then, taking the φ-components of all the groups entering (8.5) and reasoning as before, we get

$$(\mathcal{U}_{rp,\varphi}^H : \mathcal{U}_{r,\varphi}^H) = |H^1(H,\ \mathcal{U}_r^{T_p})_\varphi|.$$

By Lemma 8.3 $\mathcal{G}$ acts trivially on $H^1(H,\ \mathcal{U}_r^{T_p})$, hence we have

$$|H^1(H,\ \mathcal{U}_r^{T_p})_\varphi| = \begin{cases} 1 & \text{if } \varphi \neq \varphi_0 \\ |H^1(H,\ \mathcal{U}_r^{T_p})| & \text{if } \varphi = \varphi_0. \end{cases}$$

This proves the remaining part of the theorem.

□

Note that for any $\mathcal{R}$-module $A \subset \mathbf{Q}_\ell[\mathcal{G}]$ we have $(A_0)^H = (A^H)_0$ and $(\mathrm{Sp}_H A)_0 = \mathrm{Sp}_H(A_0)$, hence we may write simply A_0^H and $\mathrm{Sp}_H A_0$.

Proposition 8.5 *Under the assumptions of Theorem 8.1 we have*

$$\nu_\ell((\mathcal{U}_0^H : \mathcal{R}_0^H)) = \nu_\ell((\mathcal{U}_{0,\varphi_0}^H : \mathcal{R}_{0,\varphi_0}^H)) = \nu_\ell(|\mathcal{G}/H| \cdot (\mathcal{U}^H : \mathcal{R}^H)),$$

$$\nu_\ell((\mathcal{R}_0^H : \mathrm{Sp}_H\mathcal{U}_0)) = \nu_\ell((\mathcal{R}_{0,\varphi_0}^H : \mathrm{Sp}_H\mathcal{U}_{0,\varphi_0})) = \nu_\ell(|\mathcal{G}|^{-1} \cdot (\mathcal{R}^H : \mathrm{Sp}_H\mathcal{U})).$$

Proof. Put $G = \mathcal{G}/H$. Then by (7.5) we have

$$(\mathcal{R}_0^H : \mathrm{Sp}_H\mathcal{U}_0) = (\mathcal{R}^H : \mathrm{Sp}_H\mathcal{U})(\mathrm{Sp}_G(\mathrm{Sp}_H\mathcal{U}) : \mathrm{Sp}_G(\mathcal{R}^H)).$$

Note that $\mathcal{R}$ is $\mathcal{G}$-free, hence $\mathcal{R}^H = \mathrm{Sp}_H\mathcal{R}$, and

$$(\mathrm{Sp}_G(\mathrm{Sp}_H\mathcal{U}) : \mathrm{Sp}_G(\mathcal{R}^H)) = (\mathrm{Sp}_\mathcal{G}\mathcal{U} : \mathrm{Sp}_\mathcal{G}\mathcal{R}).$$

It is obvious that $\mathrm{Sp}_{\mathcal{G}}\mathcal{R} = s(\mathcal{G})\mathbf{Z}_\ell$. On the other hand,

$$\mathcal{U} = \mathcal{U}_0 + s(\mathcal{G})\mathbf{Z}_\ell \tag{8.7}$$

(see [12], (4.11)). Therefore $\mathrm{Sp}_{\mathcal{G}}\mathcal{U} = |\mathcal{G}|s(\mathcal{G})\mathbf{Z}_\ell$. This proves the last formula of the proposition. To prove the first one, we note that by (8.6)

$$\mathcal{U}^H = (\mathcal{U}_0 + s(\mathcal{G})\mathbf{Z}_\ell)^H = \mathcal{U}_0^H + s(\mathcal{G})\mathbf{Z}_\ell.$$

Hence $\mathrm{Sp}_G(\mathcal{U}^H) = |G|s(\mathcal{G})\mathbf{Z}_\ell$ and

$$(\mathcal{U}_0^H : \mathcal{R}_0^H) = (\mathcal{U}^H : \mathcal{R}^H) \cdot (s(\mathcal{G})\mathbf{Z}_\ell : |G|s(\mathcal{G})\mathbf{Z}_\ell) = |G| \cdot (\mathcal{U}^H : \mathcal{R}^H).$$

□

If K^+ is the maximal real subfield of $K = \mathbf{Q}(\epsilon_m)$, then we have $H = J = G(K/K^+)$ and $G = G(K^+/\mathbf{Q})$.

Definition. For K^+ as above, we put $\mathcal{U}_{K^+} = \mathrm{Sp}_J(\mathcal{U})$.

The following is an immediate consequence of Theorem 8.1 and Prop. 8.5.

Proposition 8.6 *Let $\mathcal{U}_{K^+}$ be as defined above. Then*

$$\nu_\ell((\mathcal{R}_0^J : \mathcal{U}_{K^+,0})) = \nu_\ell(|\mathcal{G}|^{-1}2^{b_1}),$$

where

$$b_1 = \begin{cases} 1 & \text{if } g = 1 \\ 2^{g-2} & \text{if } g \geq 2. \end{cases}$$

For any $\varphi \in \Phi$ we have

$$\nu_\ell((\mathcal{R}_{0,\varphi}^J : \mathcal{U}_{K^+,0\varphi})) = \begin{cases} 0 & \text{if } \varphi \neq \varphi_0 \\ \nu_\ell(|\mathcal{G}|^{-1}2^{b_1}) & \text{if } \varphi = \varphi_0. \end{cases}$$

Now we will recall some results of [12] concerning circular units and circular numbers. Let $P \subset K^*$ be the group of circular numbers as it was defined in [12], Section 4, i.e. P is the subgroup of the multiplicative group K^* of the field $K = \mathbf{Q}(\varepsilon_m)$ generated by the elements $1 - \zeta$ for $\zeta \in K$, $\zeta^m = 1$, $\zeta \neq 1$. The group of circular units C of K is defined by $C = P \cap E$, where E is the units of K. Note that we have $\mu(K) \subset C$ (see [12], Section 1), so we put

$\overline{P} = P/\mu(K)$, $\overline{C} = C/\mu(K)$. In [12], Section 4 it was defined a logarithmic mapping l of P such that $\operatorname{Ker} l = \mu(K)$. Hence the module $T = l(P)$ defined in [12] is naturally isomorphic to $\overline{P}$. We will reproduce here some results on T proved in [12].

Lemma 8.5 *([12], Lemma 4.2). We have $l(C) = T_0$. In other words, $\overline{C} = \overline{P}_0$.*

Lemma 8.6 *([12], Lemma 4.3). Let $e_1 = |\mathcal{G}|^{-1}s(\mathcal{G})$. Then $T_0 = T \cap (1 - e_1)T$, T_0 has finite index in $(1 - e_1)T$, and*

$$[(1 - e_1)T : T_0] = 2^{-g}|\mathcal{G}|.$$

In other words, $\overline{C} = \overline{P} \cap (1 - e_1)\overline{P}$ and

$$[(1 - e_1)\overline{P} : \overline{C}] = 2^{-g}|\mathcal{G}|.$$

We give a brief proof here since we need some details of it in the next section.

Proof. Since $\overline{P}_0 = \overline{P} \cap (1 - e_1)\overline{P}$, $(1 - e_1)\overline{P} + \overline{P} = e_1\overline{P} + \overline{P}$ and $e_1\overline{P} \cap \overline{P}^{\mathcal{G}} = \overline{P}^{\mathcal{G}}$, we have

$$(8.8)((1 - e_1)\overline{P})/\overline{P}_0 \cong ((1 - e_1)\overline{P} + \overline{P})/\overline{P} \cong (e_1\overline{P} + \overline{P})/\overline{P} \cong (e_1\overline{P})/\overline{P}^{\mathcal{G}}.$$

Let $D_{\overline{M}}$ be the subgroup of $\mathbf{Q}^*$ generated by the primes p dividing $\overline{m}$. Then the norm mapping $N_{K/\mathbf{Q}} : \overline{P} \to D_{\overline{m}}$ induces an injection

$$N_{K/\mathbf{Q}} : e_1\overline{P} \hookrightarrow D_{\overline{m}}.$$

If $\varepsilon \in \mu(K)$, and the order of ε is not a prime power, then

$$N_{K/\mathbf{Q}}(1 - \varepsilon) = 1.$$

If the order of ε is p^a for some prime p and some integer $a > 0$, then

$$N_{K/\mathbf{Q}}(1 - \varepsilon) = p^{\phi(m)/\phi(p^a)},$$

where $\phi(n)$ is the Euler function. Hence the group $N_{K/\mathbf{Q}}(e_1\overline{P}) = N_{K/\mathbf{Q}}(\overline{P})$ is generated by the elements $p^{\phi(m)/\phi(p^e)}$, $p \,|\, \overline{m}$, where p^e is the maximal power of p dividing m; of course, e depends on p.

It was proved by Sinnott ([12], page 121) that $\overline{P}^{\mathcal{G}}$ (or T^G in his notation) is generated by the elements α_p, $p\,|\,m$, where $\alpha_p = \prod_{a=1}^{(p-1)/2} (1-\varepsilon_p^a)$ for p odd, $\alpha_2 = 1-\varepsilon_4$, ε_m is a primitive m-th root of unity. The elements α_p satisfy the condition $N_J(\alpha_p) = p$, hence $N_{K/\mathbf{Q}}(\alpha_p) = p^{\phi(m)/2}$ for any p. Therefore $\overline{P}^{\mathcal{G}} = D_{\overline{m}}^{\phi(m)/2}$ and

$$e_1\overline{P}/\overline{P}^{\mathcal{G}} \cong \prod_{p\,|\,\overline{m}} \mathbf{Z}/p^{\phi(p^e)/2}\mathbf{Z}.$$

□

Taking into account that $\mathcal{G}$ acts trivially on $(1-e_1)\overline{P}/\overline{C}$, we may restate Lemma 8.6 as follows:

Lemma 8.7 *Let $\overline{C}[\ell]$ and $\overline{P}[\ell]$ be the ℓ-completions of $\overline{C}$ and $\overline{P}$, respectively. Then $\overline{C}[\ell]$ has finite index in $(1-e_1)\overline{P}[\ell]$, and for any $\varphi \in \Phi$ we have*

$$\nu_\ell([(1-e_1)\overline{P}[\ell]_\varphi : \overline{C}[\ell]_\varphi]) = \begin{cases} 0 & \text{if } \varphi \neq \varphi_0 \\ \nu_\ell(2^{-g}|\mathcal{G}|) & \text{if } \varphi = \varphi_0. \end{cases}$$

Definition. Let $K^+ = \mathbf{Q}(\varepsilon_m + \varepsilon_m^{-1})$ be the maximal real subfield of a cyclotomic field $K = \mathbf{Q}(\varepsilon_m)$. Then we put $\mathcal{T}_{K^+} := (1-e_1)\overline{P}[\ell]$.

Combining the diagonal injection

$$\overline{C}[\ell] \hookrightarrow \mathcal{A}(K^+)$$

with the mapping (7.2), we get the injection

$$\text{Log} : \overline{C}[\ell] \hookrightarrow \mathbf{A}_{K^+}\,. \tag{8.9}$$

Extending the mapping (8.9) by linearity on $\mathcal{T}_{K^+}$, we we get the mapping

$$\text{Log} : \mathcal{T}_{K^+} \hookrightarrow \mathbf{A}_{K^+}. \tag{8.10}$$

Using the isomorphism $\mathbf{A}_{K^+} \cong \overline{\mathbf{Q}}_\ell[G]$ of Section 6 and the natural injection $\mathbf{Q}_\ell[G] \hookrightarrow \overline{\mathbf{Q}}_\ell[G]$, we get an injection $i : \mathcal{U}_{K^+} \hookrightarrow \mathbf{A}_{K^+}$.

Definition. We put $\mathbf{T}_{K^+} = \overline{\mathcal{O}} \cdot \text{Log}(\mathcal{T}_{K^+})$ and $\mathbf{U}_{K^+} = \overline{\mathcal{O}} \cdot i(\mathcal{U}_{K^+})$.

For $a \in \mathbf{Z},\ a \not\equiv 0 \pmod{m}$, put

$$\eta(a) := l(1-\varepsilon_m^a) := \sum_{\substack{t \bmod m \\ (t,m)=1}} -\frac{1}{2}\log(1-\varepsilon_m^{at})\sigma_t^{-1} \in \overline{\mathbf{Q}}_\ell[\mathcal{G}] = \mathbf{A}_K.$$

As in [12], Section 2, let V be an $\overline{\mathcal{O}}$-submodule of $\mathbf{A}_K$ generated by $\eta(a),\ a \in \mathbf{Z},\ a \not\equiv 0 \pmod{m}$. Then V is an $\overline{\mathcal{O}}[\mathcal{G}]$-module, and the elements $\eta(d),\ d \mid m$ generate V as an $\mathbf{R}_K$-module.

For $r = a/m,\ a \in \mathbf{Z}, a \not\equiv 0 \pmod{m}$, we put

$$u(r) = -\frac{1}{2}\log(1-\varepsilon_m^a) \in \overline{\mathbf{Q}}_\ell.$$

If $\chi \in \widehat{\mathcal{G}}$ is a primitive Dirichlet character with conductor $f > 1$, we put, as in [12], Section 2,

$$u(\chi) = \sum_{\substack{a \pmod{f} \\ (a,f)=1}} \chi(a) u\left(\frac{a}{f}\right). \tag{8.11}$$

Put

$$\omega = \sum_{\substack{\chi \in \widehat{\mathcal{G}} \\ \chi \neq 1}} u(\overline{\chi}) e_\chi \in \mathbf{A}_K.$$

Proposition 8.7 *Let V be as above, and put $\mathbf{U} = \overline{\mathcal{O}} \cdot \mathcal{U} \subset \mathbf{A}_K$. Then*

$$(1-e_1)V = \omega \cdot \mathbf{U}.$$

This proposition may be proved by the same arguments as Prop. 2.1 of [12].

□

Theorem 8.2 *The $\overline{\mathcal{O}}[G]$-modules $\mathbf{T}_{K^+}$ and $\mathbf{U}_{K^+,0}$ are isomorphic, and for any $\chi \in \widehat{G},\ \chi \neq 1$, we have*

$$e_\chi \mathbf{T}_{K^+} = \frac{1}{2} a(\chi) e_\chi \mathbf{U}_{K^+},$$

where $a(\chi)$ is given by (7.19).

Proof. Note that (8.11) induces an isomorphism

$$l : \mathbf{T}_{K^+} \cong (1 - e_1)V,$$

and $\mathrm{Sp}_J \cdot l = \mathrm{id}$. On the other hand, $u(\overline{\chi}) = 0$ for χ odd, hence $\omega\mathbf{U} = \omega e^+\mathbf{U}$, where $e^+ = \frac{1+j}{2}$. By (8.7) we have $\omega\mathbf{U} = \omega e^+\mathbf{U}_0$. The mapping Sp_J maps isomorphically $l((1 - e_1)V)$ onto $\mathbf{T}_{K^+}$ and $\omega\mathbf{U}$ onto $\omega\mathbf{U}_{K^+}$. Therefore we have in $\mathbf{A}_{K^+}$ the equality

(8.12) $$\mathbf{T}_{K^+} = \omega\mathbf{U}_{K^+}\,.$$

If $\chi \neq 1$ is an even character of $\mathcal{G}$, then we may consider χ as a character of G, and it follows from (7.19) and (8.11) that $\frac{1}{2}a(\chi) = \mu u(\overline{\chi})$, where μ is a root of unity depending on the choice of ε_χ in (7.19). The Corollary of Theorem 7.3 shows that $u(\overline{\chi}) \neq 0$ for any even $\chi \in \widehat{\mathcal{G}}$, $\chi \neq 1$, hence (8.12) defines an isomorphism of $\overline{\mathcal{O}}[G]$-modules

$$\mathbf{T}_{K^+} \cong \mathbf{U}_{K^+,0}\,,$$

and for any such χ

$$e_\chi\mathbf{T}_{K^+} = (e_\chi\omega)e_\chi\mathbf{U}_{K^+} = u(\overline{\chi})e_\chi\mathbf{U}_{K^+} = \frac{1}{2}a(\chi)e_\chi\mathbf{U}_{K^+}\,.$$

□

Theorem 8.3 *(Theorem 1 of the introduction). Let K^+ be the maximal real subfield of a cyclotomic field $K = \mathbf{Q}(\varepsilon_m)$ with conductor m. Let $U(K^+)$ be the units of K^+ and $C^+ = C \cap U(K^+)$, where C is the group of circular units of K defined above. Then*

$$|\,\mathrm{Cl}(K^+)_\ell\,| = \begin{cases} [\,U(K^+)[\ell] : C^+[\ell]\,] & \text{if } \ell \neq 2 \\ 2^{-b}\,[\,U(K^+)[\ell] : C^+[\ell]\,] & \text{if } \ell = 2, \end{cases}$$

and for any $\varphi \in \Phi$

$$|\,\mathrm{Cl}(K^+)_{\ell,\varphi}\,| = \begin{cases} \left[U(K^+)[\ell]_\varphi : C^+[\ell]_\varphi\right] & \text{if } \ell \neq 2 \\ \left[U(K^+)[\ell]_\varphi : C^+[\ell]_\varphi\right] & \text{if } \ell = 2,\ \varphi \neq \varphi_0 \\ 2^{-b}\left[U(K^+)[\ell]_{\varphi_0} : C^+[\ell]_{\varphi_0}\right] & \text{if } \ell = 2,\ \varphi = \varphi_0, \end{cases}$$

where b is defined as follows. Let g be the number of distinct primes dividing m. Then $b = 0$ if $g = 1$, and $b = 2^{g-2} + 1 - g$, if $g > 1$.

Proof. Theorem 8.2 shows that a pair of modules $\mathcal{U}_{K^+}$, $\mathcal{T}_{K^+}$ defined above satisfies all the conditions of Theorem 7.4. Then, applying this theorem, we get

$$|\operatorname{Cl}(K^+)_\ell| = (\mathcal{R}_{K^+,0} : \mathcal{U}_{K^+,0})^{-1} [\mathcal{T}_{K^+} : C_{K^+}]^{-1} \left[\overline{U}(K^+)[\ell] : C_{K^+}\right],$$

$$|\operatorname{Cl}(K^+)_{\ell,\varphi}| = (\mathcal{R}_{K^+,0,\varphi} : \mathcal{U}_{K^+,0,\varphi})^{-1} [\mathcal{T}_{K^+,\varphi} : C_{K^+,\varphi}]^{-1} \left[\overline{U}(K^+)[\ell]_\varphi : C_{K^+,\varphi}\right].$$

By definition we have $C_{K^+} = \overline{U}(K^+)[\ell] \cap \mathcal{T}_{K^+} = C^+[\ell] / \{\pm 1\}$, hence $\overline{U}(K^+)[\ell] / C_{K^+} \cong U(K^+)[\ell] / C^+[\ell]$.

The index $Q = [\overline{C}[\ell] : (C^+[\ell] / \{\pm 1\})]$ is the so called "unit index". It is well known (see, for example, [12], Section 1) that $Q = 1$ if $g = 1$, and $Q = 2$ if $g \geq 2$. Combining this with Lemma 8.7, we get

$$\nu_\ell([\mathcal{T}_{K^+} : C_{K^+}]) = \begin{cases} \nu_\ell(2^{-g}|\mathcal{G}|) & \text{if } g = 1 \\ \nu_\ell(2^{1-g}|\mathcal{G}|) & \text{if } g > 1 \end{cases} \tag{8.13}$$

$$[\mathcal{T}_{K^+,\varphi} : C_{K^+,\varphi}] = \begin{cases} 1 & \text{if } \varphi \neq \varphi_0 \\ [\mathcal{T}_{K^+} : C_{K^+}] & \text{if } \varphi = \varphi_0. \end{cases} \tag{8.14}$$

We have $\mathcal{R}_{K^+,0} = \mathcal{R}_0^J$, so the indices $(\mathcal{R}_{K^+,0} : \mathcal{U}_{K^+,0})$ and $(\mathcal{R}_{K^+,0,\varphi} : \mathcal{U}_{K^+,0,\varphi})$ are given by Prop. 8.6. Combining Prop. 8.6 with (8.13) and (8.14), we get the assertion of the theorem.

□

The next result is an immediate consequence of Theorem 8.3.

Theorem 8.4 *Let K, K^+ be as in Theorem 8.3. Let ℓ be a fixed prime, and let k be a subfield of K^+ such that $[K^+ : k]$ is relatively prime with ℓ. Let $U(k)$ be the units of k, and put $C^+(k) = C^+ \cap U(k)$. Let $\varphi \in \Phi$ be a character of $G = G(K^+/\mathbf{Q})$ such that φ restricted on $G(K^+/k)$ is trivial (thus φ may be considered as a character of $G(k/\mathbf{Q})$). Then*

$$|\operatorname{Cl}(k)_\ell| = \begin{cases} [U(k)[\ell] : C^+(k)[\ell]] & \text{if } \ell \neq 2 \\ 2^{-b}[U(k)[\ell] : C^+(k)[\ell]] & \text{if } \ell = 2 \end{cases}$$

$$|\operatorname{Cl}(k)_{\ell,\varphi}| = \begin{cases} [U(k)[\ell]_\varphi : C^+(k)[\ell]_\varphi] & \text{if } \ell \neq 2 \\ \left[U(k)[\ell]_\varphi : C^+(k)[\ell]_\varphi\right] & \text{if } \ell = 2,\ \varphi \neq \varphi_0 \\ 2^{-b}[U(k)[\ell]_{\varphi_0} : C^+(k)[\ell]_{\varphi_0}] & \text{if } \ell = 2,\ \varphi = \varphi_0, \end{cases}$$

where b is as in Theorem 8.3.

Proof. If φ is as above, then $\mathrm{Cl}(k)_{\ell,\varphi} = \mathrm{Cl}(K^+)_{\ell,\varphi}$, $U(k)[\ell]_\varphi = U(K^+)[\ell]_\varphi$ and $C^+(k)[\ell]_\varphi = C^+[\ell]_\varphi$.

□

9 The proof of Theorem 2 and some related results

Let k be any real abelian field. If k has conductor m, then k is a subfield of the cyclotomic field $K = K_m = \mathbf{Q}(\varepsilon_m)$. Moreover, k is a subfield of the maximal real subfield $K^+ = K_m^+$ of K_m. Put $H = G(K^+/k)$, $G = G(k/\mathbf{Q})$ and $\mathcal{R}_k = \mathbf{Z}_\ell[G]$. In this section we define the modules $\mathcal{U}_k$ and $\mathcal{T}_k$ for arbitrary k. We have at least three ways to do it.

Definition 1. Put $\mathcal{U}_k^{(1)} := \pi_H(\mathcal{U}_{K^+})$, $\mathcal{T}_k^{(1)} = N_H\mathcal{T}_{K^+}$, and $C_k^{(1)} = N_H C_{K^+}$, where π_H is the natural projection $\mathbf{Q}_\ell[G(K^+/\mathbf{Q})] \to \mathbf{Q}_\ell[G]$ and N_H is the mapping $\overline{U}(K^+)\otimes_{\mathbf{Z}}\mathbf{Q}_\ell \to \overline{U}(k)\otimes_{\mathbf{Z}}\mathbf{Q}_\ell$ induced by the norm mapping $N_H : U(K^+) \to U(k)$.

For any natural $n\,|\,m$ we put, as in [13], $k_n = K_n \cap k$, where $K_n = \mathbf{Q}(\varepsilon_n)$, the cyclotomic field with conductor n. Note that any k_n is a subfield of the maximal real subfield K_n^+ of K_n. Let π_n be the natural projection $\mathbf{Q}_\ell[G(K_n^+/\mathbf{Q})] \to \mathbf{Q}_\ell[G(k_n/\mathbf{Q})]$, and $i_n : \mathbf{Q}_\ell[G(k_n/\mathbf{Q})] \to \mathbf{Q}_\ell[G]$ be the mapping defined by $i_n(\sigma) = \sum_{\tau\in G(k/k_n)} \overline{\sigma}\tau$, where $\sigma \in G(k_n/\mathbf{Q})$ and $\overline{\sigma}$ is any representative of σ in G. On the other hand, we have for any $n\,|\,m$ the norm mapping $N_{K_n^+/k_n} : \overline{U}(K_n^+)\otimes_{\mathbf{Z}}\mathbf{Q}_\ell \to \overline{U}(k_n)\otimes_{\mathbf{Z}}\mathbf{Q}_\ell$ and the natural inclusion $j_n : \overline{U}(k_n)\otimes_{\mathbf{Z}}\mathbf{Q}_\ell \hookrightarrow \overline{U}(k)\otimes_{\mathbf{Z}}\mathbf{Q}_\ell$. The next definition follows to that given in [13].

Definition 2. Put $\mathcal{U}_k^{(2)}$ be the $\mathcal{R}_k$-submodule of $\mathbf{Q}_\ell[G]$ generated by the groups $i_n \circ \pi_n(\mathcal{U}_{K_n^+})$ for all $n\,|\,m$. Put $\mathcal{T}_k^{(2)}$ be the $\mathcal{R}_k$-submodule of $\overline{U}(k)\otimes_{\mathbf{Z}}\mathbf{Q}_\ell$ generated by the groups $j_n \circ N_{K_n^+/k_n}(\mathcal{T}_{K_n^+})$ for all $n\,|\,m$. Let $C_k^{(2)}$ be the $\mathcal{R}_k$-submodule of $\overline{U}(k)[\ell]$ generated by the groups $j_n \circ N_{K_n/k_n}C(K_n)$, where $C(K_n)$ is the group of circular units defined in the introduction.

Remark. Note that $\mathcal{U}_k^{(2)} \supseteq i_1 \circ \pi(\mathcal{U}_{K_1}^+) = s(G)\mathbf{Z}_\ell$. Hence

$$\mathcal{U}_k^{(2)} = \mathcal{U}_{k,0}^{(2)} + s(G)\mathbf{Z}_\ell. \tag{9.1}$$

Definition 3. Put $\mathcal{U}_k^{(3)} := i_m^{-1}(\mathcal{U}_{K_m^+}^H) \subset \mathbf{Q}_\ell[G]$, $\mathcal{T}_k^{(3)} := j_m^{-1}(\mathcal{T}_{K_m^+}^H) \subset \overline{U}(k)\otimes_{\mathbf{Z}}\mathbf{Q}_\ell$, and $C_k^{(3)} := C_{K^+}^H = \overline{U}(k) \cap C_{K^+}$.

In what follows we shall denote the module $\mathcal{U} \subset \mathbf{Q}_\ell[G(K_m/\mathbf{Q})]$ defined in Section 8 by $\mathcal{U}_m$, if we wish to make explicit its dependence on K_m. For $i = 1, 2, 3$ put $\mathbf{U}_k^{(i)} = \overline{\mathcal{O}} \cdot \mathcal{U}_k^{(i)} \subset \mathbf{A}_k$ and $\mathbf{T}_k^{(i)} = \overline{\mathcal{O}} \cdot \mathrm{Log}(\mathcal{T}_k^{(i)})$, where $\mathrm{Log} : \mathcal{T}_k^{(i)} \hookrightarrow \mathbf{A}_k$ is defined as in (8.10).

Proposition 9.1 *Let $\omega \in \mathbf{A}_{K_m}$ be as in Prop. 8.7. Then for $i = 1, 2, 3$ we have*

$$\mathbf{T}_k^{(i)} = \omega \mathbf{U}_k^{(i)}.$$

Proof. By (8.12) we have $\mathbf{T}_{K^+} = \omega \mathbf{U}_{K^+}$, where $K^+ = K_m^+$. It follows from Definition 1 and the identity $\log \cdot N_H = \mathrm{Sp}_H \cdot \log$ that $\mathbf{T}_k^{(1)} = \mathrm{Sp}_H \mathbf{T}_{K^+}$ and $\mathbf{U}_k^{(1)} = \mathrm{Sp}_H \mathbf{U}_{K^+}$. Thus $\mathbf{T}_k^{(1)} = \mathrm{Sp}_H(\omega \mathbf{U}_{K^+}) = \omega \cdot \mathrm{Sp}_H(\mathbf{U}_{K^+}) = \omega \mathbf{U}_k(1)$. This proves the proposition for $i = 1$.

As the multiplication by ω in (8.12) induces an isomorphism $\mathbf{T}_{K^+} \cong \mathbf{U}_{K^+,0}$, we have

$$\mathbf{T}_k^{(3)} = \mathbf{T}_{K^+}^H = \omega \mathbf{U}_{K^+}^H = \omega \mathbf{U}_k^{(3)}.$$

This proves the proposition for $i = 3$.

For $i = 2$ and $n \mid m$ put

$$\omega_n = \sum_{\substack{\chi \in G(K_n/\mathbf{Q}) \\ \chi \neq 1}} u(\overline{\chi}) e_\chi \in \mathbf{A}_{K_n}.$$

Applying Prop. 8.7 to the field K_n, we get

$$\mathbf{T}_{K_n^+} = \omega_n \mathbf{U}_{K_n^+}.$$

If $x \in \mathbf{A}_K^{G(K/K_n)} = \mathbf{A}_{K_n}$, then for any character $\chi \in \widehat{G}$ such that χ restricted on $G(K/K_n)$ is not trivial, we have $e_\chi \cdot x = 0$. Hence we have $\omega_n \cdot x = \omega \cdot x$

for any $x \in \mathbf{A}_{K_n}$ and therefore $\mathbf{T}_{K_n^+} = \omega \mathbf{U}_{K_n^+}$ for any $n \mid m$. It follows from Definition 2 that $\mathbf{T}_k^{(2)}$ is generated in $\mathbf{A}_k$ by $\mathrm{Sp}_{K_n/k_n}(\mathbf{T}_{K_n^+})$ for all $n \mid m$ and $\mathbf{U}_k^{(2)}$ is generated in $\mathbf{A}_k$ by $\mathrm{Sp}_{K_n/k_n}(\mathbf{U}_{K_n^+})$ for all $n \mid m$. As $\omega \cdot \mathrm{Sp}_{K_n/k_n}(x) = \mathrm{Sp}_{K_n/k_n}(\omega \cdot x)$ for any $x \in \mathbf{A}_{K_n}$, we get

$$\mathbf{T}_k^{(2)} = \omega \mathbf{U}_k^{(2)}.$$

□

As an immediate consequence of Theorem 7.4 and Prop. 9.1 we have

Theorem 9.1 *Let k be a real abelian field. Then for $i = 1, 2, 3$ and any $\varphi \in \Phi$ we have*

$$|\mathrm{Cl}(k)_\ell| = (\mathcal{R}_{k,0} : \mathcal{U}_{k,0}^{(i)})^{-1}[\mathcal{T}_k^{(i)} : C_k^{(i)}]^{-1}[\overline{U}(k)[\ell] : C_k^{(i)}]$$

and

$$|\mathrm{Cl}(k)_{\ell,\varphi}| = (\mathcal{R}_{k,0,\varphi} : \mathcal{U}_{k,0,\varphi}^{(i)})^{-1}[\mathcal{T}_{k,\varphi}^{(i)} : C_{k,\varphi}^{(i)}]^{-1}[\overline{U}(k)[\ell]_\varphi : C_{k,\varphi}^{(i)}].$$

Proposition 9.2 *The index $(\mathcal{R}_{k,0} : \mathcal{U}_{k,0}^{(i)})$ is defined by*

$$(R_{k,0} : \mathcal{U}_{k,0}^{(i)}) = \ell^c(\mathcal{R}_k : \mathcal{U}_k^{(i)}),$$

where

$$c = \begin{cases} \nu_\ell([K : \mathbf{Q}]) & \text{if } i = 1 \\ \nu_\ell([k : \mathbf{Q}]) & \text{if } i = 2, 3 \end{cases}$$

Proof. For $i = 1, 3$ the assertion follows immediately from (7.5) and (8.7). If $i = 2$, then the assertion follows from (7.5) and (9.1).

□

Proposition 9.3 *For a real abelian k let $U \subset \mathbf{Q}[G]$ be the module defined by Sinnott in [13]. Then we have*

$$\mathcal{U}_k^{(2)} = U[\ell].$$

Proof. As in Section 8, put $\overline{m} = \prod_{p\,|\,m} p$. Let T_p (resp. $T_p(k)$) be the inertia subgroup of p in $\mathcal{G} = G(K_m/\mathbf{Q})$ (resp. in $G = G(k/\mathbf{Q})$). As was shown in the proof of Prop. 5.1 of [12], the module $\mathcal{U}_m$ is generated as a $\mathbf{Z}_\ell[\mathcal{G}]$-module by the elements

$$p_{m,r} := \prod_{p\,|\,r} s(T_p) \prod_{p\,|\,\overline{m}/r} (1 - \overline{\sigma}_p), \quad 1 \leq r \leq \overline{m}, \ r\,|\,m.$$

For $p\,|\,m$ put $(p,\, k)^* = \lambda_p^{-1} e'_p$, where $e'_p = |T_p(k)|^{-1} \sum_{\sigma \in T_p(k)} \sigma$ and λ_p is any element of G such that λ_p mod $T_p(k)$ is the Frobenius automorphism for p in $G/T_p(k)$. For $r\,|\,\overline{m}$ put $T_r(k)$ be the compositum in G of the inertia groups $T_p(k)$ for each p dividing r. As was shown in Prop. 2.3 of [13], the module U is generated as a $\mathbf{Z}[G]$-module by the elements

$$q_r := s(T_r(k)) \prod_{p\,|\,\overline{m}/r} (1 - (p,\, k)^*),$$

where r runs over all positive divisors of $\overline{m}$.

Let $r\,|\,\overline{n}\,|\,\overline{m}$. We will prove that $i_n \circ \pi_n(p_n,\, r) \in U$. Let $T_r(k_n)$ (resp. $T_r(K_n)$) be the compositum in $G = G(k_n/\mathbf{Q})$ (resp. in $G(K_n/\mathbf{Q})$) of the inertia groups $T_p(k_n)$ (resp. $T_p(K_n)$) for each p dividing r. As the mapping π_n is a homomorphism of rings and $\pi_n(\overline{\sigma}_p) = (p,\, k_n)^*$, we have

$$\pi_n(p_{n,r}) = \frac{|T_r(K_n)|}{|T_r(k_n)|} s(T_r(k_n)) \prod_{p\,|\,\overline{n}/r} (1 - (p,\, k)^*).$$

Put $r_1 = r\overline{m}/\overline{n}$, i.e. $\overline{m}/r_1 = \overline{n}/r$. Let $\pi^{(n)}$ be the natural mapping $\mathbf{Q}[G] \to \mathbf{Q}[G(k_n/\mathbf{Q})]$. Then, reasoning as before and taking into account that $\pi^{(n)}(T_{r_1}(k)) = T_r(k_n)$, we get

$$\pi_n(q_{r_1}) = \frac{|T_{r_1}(k)|}{|T_r(k_n)|} s(T_r(k_n)) \prod_{p\,|\,\overline{n}/r} (1 - (p,\, k)^*) = \tag{9.2}$$

$$\frac{|T_{r_1}(k)|}{|T_r(K_n)|} \pi_n(p_{n,r}).$$

Consider the exact sequence

$$0 \longrightarrow G(k/k_n) \cap T_{r_1}(k) \longrightarrow T_{r_1}(k) \longrightarrow T_r(k_n) \longrightarrow 0.$$

We have

$$|G(k/k_n)\cap T_{r_1}(k)| = \frac{|T_{r_1}(k)|}{|T_r(k_n)|}.$$

Let $S \subset G(k/k_n)$ be a set of representatives for $G(k/k_n)/(G(k/k_n)\cap T_{r_1}(k))$. Then

$$i_n \circ \pi^{(n)}(q_{r_1}) = \mathrm{Sp}_{k/k_n}(q_{r_1}) = \frac{|T_{r_1}(k)|}{|T_r(k_n)|}\sum_{\sigma\in S}\sigma(q_{r_1}).$$

Thus it follows from (9.2) that

$$i_n \circ \pi^{(n)}(p_{n,r}) = \frac{|T_r(K_n)|}{|T_{r_1}(k)|}\mathrm{Sp}_{k/k_n}(q_{r_1}) = \frac{|T_r(K_n)|}{|T_r(k_n)|}\sum_{\sigma\in S}\sigma(q_{r_1}).$$

Hence $i_n \circ \pi_n(p_{n,r}) \in U$ for any $n\,|\,m$, $r\,|\,\overline{n}$. Therefore $\mathcal{U}_k^{(2)} \subseteq U[\ell]$.

Now we will prove that $q_2 \in \mathcal{U}_k^{(2)}$ for any $r\,|\,\overline{m}$. Put $m = ab$, where $(b, r) = 1$ and a prime p divides a if and only if p divides r (so we have $\overline{a} = r$). Note that we have $T_r(k) = G(k/k_b)$. Consider

$$p_{b,1} = \prod_{p\,|\,\overline{m}/r}(1-\overline{\sigma}_p).$$

We have

$$\pi_b(p_{b,1}) = \prod_{p\,|\,\overline{m}/r}(1-(p,\,k_b)^*).$$

As $q_r \in \mathbf{Q}[G]^{T_r(k)}$, we have $q_r = |T_r(k)|^{-1}\cdot i_b \circ \pi^{(b)}(q_r)$. Note that

$$\pi^{(b)}(q_r) = |T_r(k)|\cdot \prod_{p\,|\,\overline{m}/r}(1-(p,k_b)^*).$$

Thus $\pi_b(p_{b,1}) = |T_r(k)|^{-1}\pi^{(b)}(q_r)$. Therefore

$$q_r = i_b \circ \pi_b(p_{b,1}).$$

This proves that $\mathcal{U}_k^{(2)} \supseteq U[\ell]$.

□

Proposition 9.4 *The group $(\mathcal{T}_k^{(2)})^2$, where $\mathcal{T}_k^{(2)}$ is the group from Definition 2, coincides with $(1-e_G)(D/\{\pm1\})$, where $e_G = |G|^{-1}\sum_{\sigma\in G}\sigma$ and D is the group of circular numbers of k defined by Sinnott in [13], Sect. 4.*

The group $C_k^{(2)}$ of Definition 2 coincides with $C/\{\pm1\}$, where C is the group of circular units of k defined in [13], Sect. 4.

Proof. The group D is defined as follows. Let n be any integer > 1 and let a be any integer not divisible by n; then the number $N_{K_n/k_n}(1-\varepsilon_n^a)$ lies in k. Sinnott defines the circular numbers D of k to be the group generated in k^* by -1 and all such elements $N_{K_n/k_n}(1-\varepsilon_n^a)$. The circular units C are then defined by $C = U(k) \cap D$. Note that any $x \in D$ is an algebraic integer, so such x is a unit if and only if $N_{k/\mathbf{Q}}(x) = \pm 1$. Therefore $C/\{\pm 1\} = (D/\{\pm 1\})_0$.

Lemma 9.1 *Let D_1 be the subgroup of D generated by -1 and all the elements $N_{K_n/k_n}(1-\varepsilon_n^a)$ for $n \mid m$, and let D_2 be a subgroup of $\mathbf{Q}^*$ generated by all primes $q \nmid m$. Then there is a decomposition into the direct product $D \cong D_1 \times D_2$.*

Proof. It was shown in [13] that $D \supset \mathbf{Q}^*$, therefore $D_2 \subset D$. It is obvious that $D_1 \subset D$ and $D_1 \cap D_2 = \{1\}$. Fix some $n = n_1 n_2$, where $(m, n_2) = 1$ and a prime number p divides n_1 if and only if $p \mid m$. Then $K_n = K_{n_1} \cdot K_{n_2}$ and $K_{n_2} \cap k = \mathbf{Q}$.

If $n_1 = 1$, i.e. $(n, m) = 1$, then $k_n = \mathbf{Q}$ and, taking into account that $N_{K_n/k_n}(x)$ is totally positive for any $x \in K_n$, we get that $N_{K_n/k_n}(1-\varepsilon_n^a) \in D_2$.

If $n_2 = 1$, then, putting $E = K_n \cap K_m$, we have $N_{K_n/k_n} = N_{E/k_n} \circ N_{K_n/E}$. The direct calculation shows that $N_{K_n/E}(1-\varepsilon_n^a) \in P(E)$, thus $N_{K_n/k}(1-\varepsilon_n^a) \in D_1$.

If $n_1 \neq 1$, $n_2 \neq 1$, then, reasoning as before and putting $E = K_n \cap K_m$, we have $N_{K_n/k_n}(1-\varepsilon_n^a) = N_{E/k_n} \circ N_{K_n/E}(1-\varepsilon_n^a)$. As $(1-\varepsilon_n^a)$ is a unit in this case, we see that $N_{K_n/E}(1-\varepsilon_n^a) \in P(E)$, thus $N_{K_n/k}(1-\varepsilon_n^a) \in D_1$.

□

It follows from Lemma 9.1 that $(1-e_G)(D/\{\pm 1\}) = (1-e_G)(D_1/\{\pm 1\})$. It may be checked easily that $(1-e_G)D_1$ is generated by the groups $(1-e_n)\overline{P}_n$ for all $n \mid m$, where P_n is the group of circular numbers of K_n, $\overline{P}_n = P_n/\mu(K_n)$ and $e_n = |G(K_n/\mathbf{Q}|^{-1} \sum_{\sigma \in G(K_n/\mathbf{Q})} \sigma$. By definition $\mathcal{T}_{K_n^+} = (1-e_n)\overline{P}_n$. Noting that we use the mapping $N_{K_n^+/k_n}$ in the definition of $\mathcal{T}_k^{(2)}$ and the mapping $N_{K_n/k}$ in the definition of D, we get that $(\mathcal{T}_k^{(2)})^2 = (1-e_G)(D/\{\pm 1\})$.

In order to prove the last assertion of the proposition, we note that the inclusion $C_k^{(2)} \subseteq C/\{\pm 1\} = (D/\{\pm 1\})_0$ is obvious. Suppose that $x \in D$ and $x \pmod{\{\pm 1\}} \in (D/\{\pm 1\})_0$. Then x can be presented in the form

$x = u \cdot \prod_{p\,|\,m} A_p$, where $u \in C_k^{(2)}$ and A_p is as follows. Let p^e be the greatest power of p dividing m. For $1 \leq j \leq e$ put $K(j) = K_{p^j}$ and $k(j) = k_{p^j}$. Then A_p is of the form $A_p = \prod_{j=1}^{e} B_j$, where $B_j = N_{K(j)/k(j)}(b_j)$ for some $b_j \in P(K(j))$. As the elements A_p are relatively prime in k, we get that x is a unit if and only if A_p is a unit for any $p\,|\,m$. The group $G(k_{p^e}/\mathbf{Q})$ is cyclic (the group $G^+_{p^e}/\mathbf{Q})$ is cyclic for $p = 2$), hence, taking into account that p^e is the exact power of p dividing the conductor of k, we get that $[K_{p^j} : k_{p^j}]$ does not depend on j for $1 \leq j \leq e$. Therefore for any $a \in K_{p^e}$ we have

$$N_{k(e)/k(j)} \circ N_{K(e)/k(e)}(a) = N_{K(j)/k(j)} \circ N_{K(e)/K(j)}(a).$$

The norm $N_{K(e)/K(j)}$ maps $P(K_{p^e})$ onto $P(K_{p^j})$. Hence A_p is of the form $A_p = N_{K(e)/k(e)}(c_p)$ for some $c_p \in P(K_{p^e})$. Obviously, A_p is a unit if and only if c_p is a unit, i.e. if $c_p \in C(K_{p^e})$. Therefore $A_p \in C_k^{(2)}$. This proves the inclusion $C_k^{(2)} \supseteq C/\{\pm 1\}$.

□

For $\varphi \in \Phi$ put $d = |G| = [k : \mathbf{Q}]$, $d_\varphi = \dim_{\mathbf{Q}_\ell} \varphi = \dim_{\mathbf{Q}_\ell} \mathbf{Q}_\ell[G]_\varphi$, where $G = G(k/\mathbf{Q})$. Put $d_{\varphi_0} = d_0$.

Proposition 9.5 *The group $C_k^{(2)}$ has finite index in $\mathcal{T}_k^{(2)}$, and for any $\varphi \in \Phi$ we have*

$$[\mathcal{T}_k^{(2)} : C_k^{(2)}] = 2^{d-1} \prod_{p\,|\,m} [k_{p^e} : \mathbf{Q}],$$

$$[\mathcal{T}_{k,\varphi}^{(2)} : C_{k,\varphi}^{(2)}] = \begin{cases} 2^{d_\varphi} & \text{if } \varphi \neq \varphi_0 \\ 2^{d_0 - 1} \prod_{p\,|\,m} [k_{p^e} : \mathbf{Q}] & \text{if } \varphi = \varphi_0, \end{cases}$$

the product taken over all primes p dividing the conductor m of k. For each such p, p^e denotes the greatest power of p dividing m.

Proof. It was proved in [13], Prop. 4.1 that for some group $T \cong D/\{\pm 1\}$ defined in [13] we have

$$[(1 - e_G)T : T_0] = \prod_{p\,|\,m} [k_{p^e} : \mathbf{Q}].$$

It follows from Prop. 9.4 that

$$[(\mathcal{T}_k^{(2)})^2_\varphi : C_{k,\varphi}^{(2)}] = [(1-e_G)T_\varphi : T_{0,\varphi}],$$

where $T \cong D/\{\pm 1\}$. Now the assertion of the proposition follows from the fact that

$$[\mathcal{T}_{k,\varphi}^{(2)} : (\mathcal{T}_k^{(2)})^2_\varphi] = \begin{cases} 2^{d_\varphi} & \text{if } \varphi \neq \varphi_0 \\ 2^{d_0-1} & \text{if } \varphi = \varphi_0 \end{cases}$$

□

Combining Theorem 9.1, Prop. 9.2 and Prop. 9.5, we get the following result that is a refinement of Theorem 4.1 of [13].

Theorem 9.2 *(Theorem 2 of the introduction.) For any real abelian k we have*

$$\nu_\ell([\overline{U}(k)[\ell] : C_k^{(2)}]) = \nu_\ell\left(|\mathrm{Cl}(k)_\ell| 2^{d-1} \frac{\prod_{p|m}[k_{p^e} : \mathbf{Q}]}{[k : \mathbf{Q}]} [\mathcal{R}_k : \mathcal{U}_k]\right).$$

For any $\varphi \in \Phi$ we have

$$\nu_\ell([\overline{U}(k)[\ell]_\varphi : C_{k,\varphi}]) =$$

$$\begin{cases} \nu_\ell(|\mathrm{Cl}(k)_{\ell,\varphi}| 2^{d_\varphi} [\mathcal{R}_{k,\varphi} : \mathcal{U}_{k,\varphi}]) & \text{if } \varphi \neq \varphi_0 \\ \nu_\ell\left(|\mathrm{Cl}(k)_{\ell,\varphi_0}| 2^{d_0-1} \frac{\prod_{p|m}[k_{p^e} : \mathbf{Q}]}{[k:\mathbf{Q}]} [\mathcal{R}_{k,\varphi_0} : \mathcal{U}_{k,\varphi_0}]\right) & \text{if } \varphi = \varphi_0 \end{cases}$$

For $i = 1, 3$ the author was unable to compute the index $[\mathcal{T}_{k,\varphi}^{(i)} : C_{k,\varphi}^{(i)}]$ pricisely. Nevertheless, we have the following trivial result for $i = 3$ (the case $i = 1$ may be treated in the same way, but this last case does not yield any interesting consequences).

Proposition 9.6 *Let k be a real abelian field with conductor m. If $i = 3$ and $\ell \neq 2$, then for any $\varphi \in \Phi$ we have*

$$[\mathcal{T}_k^{(3)} : C_k^{(3)}] = \ell^r,$$

$$[\mathcal{T}_{k,\varphi}^{(3)} : C_{k,\varphi}^{(3)}] = \begin{cases} 1 & \text{if } \varphi \neq \varphi_0 \\ \ell^r & \text{if } \varphi = \varphi_0, \end{cases}$$

where ℓ^r is the power of ℓ dividing the order of $\mathcal{G} = G(K_m/\mathbf{Q})$.

Proof. Put $K_m = K$. We have $\mathcal{T}_{K^+}^H / C_{K^+}^H \subseteq \mathcal{T}_{K^+}/C_{K^+}$. Note that for $\ell \neq 2$ we have $C_{K^+} = \overline{C}(K)[\ell]$ and $C_{K^+}^H = C_k^{(3)}$. Thus the proposition follows immediately from Lemma 8.7.

□

Theorem 9.3 *For any real abelian k and for $\ell \neq 2$ we have*

$$|\mathrm{Cl}(k)_\ell| = (\mathcal{R}_k : \mathcal{U}_k^{(3)})^{-1} \ell^{r-c} [\overline{U}(k)[\ell] : C_k^{(3)}],$$

where $c = \nu_\ell([k : \mathbf{Q}])$ and ℓ^r divides the degree $[K : \mathbf{Q}]$.

For any $\varphi \in \Phi$ we have

$$(9.3) \qquad |\mathrm{Cl}(k)_{\ell,\varphi}| = \begin{cases} A_\varphi & \text{if } \varphi \neq \varphi_0 \\ \ell^{r-c} A_\varphi & \text{if } \varphi = \varphi_0, \end{cases}$$

where $A_\varphi = (\mathcal{R}_{k,\varphi} : \mathcal{U}_{k,\varphi}^{(3)})^{-1} [\overline{U}(k)[\ell]_\varphi : C_{k,\varphi}^{(3)}]$.

Proof. Follows immediately from Theorem 9.1, Prop. 9.2 and Prop. 9.6.

□

Theorem 9.3 implies the following interesting consequence:

Theorem 9.4 *Let $K = K_m$ and $k = (K^+)^H$, where H is a cyclic subgroup of $G(K^+/\mathbf{Q})$ such that $H \cap T_r = \{1\}$ for any $r \,|\, \overline{m}$, $r \neq \overline{m}$ and T_r being as in Theorem 8.1. Let $g \geq 2$ be the number of distinct prime divisors of m. For $\ell \neq 2$ put $t = \nu_\ell(|H|)$. Then*

$$|\mathrm{Cl}(k)_\ell| \equiv |\mathrm{Cl}(k)_{\ell,\varphi_0}| \equiv 0 \pmod{\ell^{t(2^{g-2}-1)}}.$$

Proof. We have $\mathcal{U}_m = \mathcal{U}_m^+ \oplus \mathcal{U}_m^-$. By Lemma 8.3 $\mathcal{U}_m^-$ is a cohomologically trivial H-module. Then it follows from Theorem 8.1 that $\nu_\ell((\mathcal{U}_k^{(3)} : \mathcal{R}_k)) = \nu_\ell((\mathcal{U}_{k,\varphi_0}^{(3)} : \mathcal{R}_{k,\varphi_0})) = \nu_\ell((\mathcal{U}_m^+)^H : \mathcal{R}_k) = 2^{g-2}t$. We have that ℓ^{r-c} divides $|H|$. Thus the theorem follows from (9.3) and the fact that the index $[\overline{U}(k)[\ell]_\varphi : C_{k,\varphi}^{(3)}]$ is an integer.

□

Corollary. Let k_0 be the maximal ℓ-extension of $\mathbf{Q}$ containing in k, where k is as in Theorem 9.4. Then

$$|\mathrm{Cl}(k_0)_\ell| \equiv 0 \pmod{\ell^{t(2^{g-2}-1)}}.$$

Indeed, we have $|\mathrm{Cl}(k_0)_\ell| = \mathrm{Cl}(k)_{\ell,\varphi_0}$.

Proposition 9.7 *Let t be a positive integer. Suppose that for any prime $p\,|\,m$ we have $\varphi(p^e) \equiv 0 \pmod{\ell^t}$, where ℓ is an odd prime and $\varphi(p^e)$ is the Euler function, i.e. $p \equiv 1 \pmod{\ell^t}$ if $p \neq \ell$ and $e \geq t+1$ if $p = \ell$. Then there exists a subgroup $H \subset G(K_m/\mathbf{Q})$ such that $H \cap T_r = \{1\}$ for any $r\,|\,\overline{m}$, $r \neq \overline{m}$.*

Proof. Choose for any $p\,|\,m$ an element $\sigma_p \in T_p$ of the exact order ℓ^t and put $H =< \sigma >$, where $\sigma = \prod_{p\,|\,m} \sigma_p$.

□

Theorem 9.5 *Let $K = K_m$ be a cyclotomic field such that for a given t we have $\varphi(p^e) \equiv 0 \pmod{\ell^t}$ for any $p\,|\,m$, where p^e is the greatest power of p dividing m. Then we have*

$$|\mathrm{Cl}(K_m^+)_\ell| \equiv |\mathrm{Cl}(K_m^+)_{\ell,\varphi_0}| \equiv 0 \pmod{\ell^{t(2^{g-2}-2)}}.$$

Proof. By Prop. 9.7 we can find a subfield $k \subset K_m^+$ such that the group $H = G(K_m^+/k)$ has an order ℓ^t and satticfies the conditions of Theorem 9.4. If the order of $\mathrm{Cl}(k)_{\varphi_0}$ is divisible by ℓ^a for some a, then there exists an abelian unramified ℓ-extension M/k of degree divisible by ℓ^a such that M is Galois over $\mathbf{Q}$ and $G(M/k) = G(M/k)_{\varphi_0}$. Then the degree of MK_m^+/K_m^+ divides ℓ^{a-t}. Hence

$$|\mathrm{Cl}(K_m^+)| \equiv |\mathrm{Cl}(K_m^+)_{\varphi_0}| \equiv 0 \pmod{\ell^{a-t}}.$$

□

Corollary. Let ℓ be odd. If the number g of distinct prime divisors of m is ≥ 4, then the field K_m^+ has nontrivial ℓ-class group. Let K_0 be the maximal ℓ-extension of $\mathbf{Q}$ containing in K_m^+. Then K_0 has nontrivial ℓ-class group.

10 Concluding remarks

The groups $T_\ell(k_\infty)_{(0)}$ may be considered as analogs of ℓ-class groups of function field. Thus we have

Problem 1. For given real abelian k, is the group $\prod_\ell T_\ell(k_\infty)_{(0)}$ finite, in other words, are the groups $T_\ell(k_\infty)$ trivial for all but finitely many ℓ?

Note that the proof of Theorem 3.2 given is Sect.3 is rather complicated. It seems that one can simplify this proof, using methods of Kolyvagin (see[9]). On the other hand, R.Greenberg conjectured in [2] that $T_\ell(k_\infty)$ is finite for any totally real field k. If this conjecture is true, then we can deduce Theorem 3 immediately from Prop. 4.3. Moreover, we have

Theorem 10.1 *Suppose that Greenberg's conjecture holds true for k_∞/k. Then for any intermediate subfield k_n, $k_\infty \supset k_n \supset k$ we have for all sufficiently large n*

$$T_\ell(k_\infty)_{(n)} \cong U_S^\wedge(k_n)/C_S(k_n).$$

Problem 2. Does Theorem 10.1 hold for any real abelian k?

Problem 3. Generalize Theorem 6.1 to the case of relatively abelian extensions.

Note that such a generalization, if it exists, needs some generalization of Gauss sums g_χ.

It should be mentioned that Theorem 7.1 and its proof stay valid for any totally real k.

Problem 4. Generalize Theorem 7.1 to any algebraic number field.

Note that we deduced Theorem 9.4 and Theorem 9.5 from some calculations on cohomology groups of U. We may ask whether there are any other interesting examples of subgroups $H \subset G(K_m/\mathbf{Q})$ that yield other nontrivial divisibility conditions for the class group of cyclotomic fields.

Finally, we note that the most interesting problem is to generalize the results of this paper to other fields having a system of special units, such as abelian extensions of imaginary quadratic fields.

References

[1] *G.Gras*, Classes d'ideaux des corps abélienn et nombres de Bernoulli généralisés, Ann. Inst. Fourier **27** (1977), 1-66.

[2] *R.Greenberg*, On the Iwasawa invariants of totally real number fields. Amer. J. Math. **98** (1976), N1, 263-284.

[3] *K.Iwasawa*, Lectures on p-adic L-functions. Princeton. Princeton Univ. Press and Univ. of Tokyo Press. 1972.

[4] *D.S.Kubert*, The universal ordinary distribution. Bull. Soc. math. France, **107** 1979, 179-202.

[5] *D.S.Kubert*, The $\mathbf{Z}/2\mathbf{Z}$ cohomology of the universal ordinary distribution. Bull. Soc. math. France, **107** 1979, 203-224.

[6] *L.V.Kuz'min*, The Tate module for algebraic number fields, Izv. Akad. Nauk SSSR Ser.Mat. **36** (1972), 267-327; English transl. in Math. USSR Izv. **6** (1972).

[7] *L.V.Kuz'min*, Some duality theorems for cyclotomic Γ-extensions of algebraic number fields of CM-type, Izv.Akad.Nauk SSSR Ser. Mat. **43** (1979), 483-546; English transl. in Math. USSR Izv. **14** (1980).

[8] *L.V.Kuz'min*, Some explicit calculations in local and global cyclotomic fields. Submitted to Trudy MIRAN.

[9] *S.Lang*, Cyclotomic fields I, II, combined 2-nd edition Grad. Texts in Math. **121** Springer-Verlag, New York, 1990.

[10] *B.Mazur, A.Wiles*, Class fields of abelian extensions of **Q**. Invent. math. **76** (1984), 179-330.

[11] *K. Rubin*, Kolivagin's system of Gauss sums, preprint.

[12] *W.Sinnott*, On the Stickelberger ideal and the circular units of a cyclotomic field. Ann. of Math.**108** (1978), 107-134.

[13] *W.Sinnott*, On the Stickelberger ideal and the circular units of an abelian field. Invent. math. **62** (1980), 181-234.

[14] *A.Wiles*, The Iwasawa conjecture for totally real fields, Ann. of Math. **131** (1990), 493-540.

Russian Research Center "Kurchatov Institute"
Institute of Information Technologies
Moscow 123182, Russia