ACTA ARITHMETICA
174.3 (2016)

The circular units and the Stickelberger ideal of a cyclotomic field revisited

by

Radan Kučera (Brno)

Introduction. For a cyclotomic field, a basis of the group of circular units is constructed in [3], and bases of the Stickelberger ideal and of the group of circular units are constructed in [7]. Unfortunately the proof given there is indirect: by some cohomological computations it is proven that the subgroup generated by a given set of elements, which turns out to be linearly independent later on, is of index one in the group. But this says nothing about expressing elements in terms of the basis.

The aim of this paper is to give a direct proof which not only seems to be shorter and easier to understand but which is also constructive in some way: it describes a procedure allowing one to express a given element as a linear combination of elements of the basis (see Lemma 3.2). The coefficients in this linear combination can be found by induction, using relations (2.3) and (2.4) together with the Ennola relations given by Theorem 2.2 (the existence of relations of this kind was proven by Ennola [2]; their explicit form is a subject of recent research—see [5]). Even though this theorem states only the existence of some relations, the required element α_Q could be found explicitly as a sum of elements appearing in the proof of Proposition 2.1.

A key role in the construction in [7] of bases of the Stickelberger ideal and of the group of circular units is played by bases of odd and even universal ordinary distributions given in [6]. This paper describes a presentation of these distributions; they appear here as quotients of the additive group of the semigroup ring $\mathbb{Z}[G^*]$, considered as a $\mathbb{Z}[G]$-module, by its submodules $\mathcal{I}_1$ and $\mathcal{I}_{-1}$ described in Section 2. Theorem 2.2 plays an important role in

2010 *Mathematics Subject Classification*: Primary 11R18.
Key words and phrases: circular (cyclotomic) units, Stickelberger ideal, odd and even universal ordinary distributions, Ennola relations.
Received 21 November 2014; revised 6 April 2016.
Published online 12 July 2016.

DOI: 10.4064/aa8009-4-2016

Section 3 where the modules $\mathcal{N}_{\pm1} = \mathbb{Z}[G^*]/\mathcal{I}_{\pm1}$ are described in Theorem 3.6 by means of $\mathbb{Z}$-bases $M_{\pm1}$ defined before Lemma 3.1. This also allows one to study the torsion parts of $\mathcal{N}_{\pm1}$; in some respects this is easier and more straightforward in comparison with the original papers [12] and [9]. A basis of the group of circular units of a cyclotomic field is also constructed in [3] and [1] where the authors need to know the torsion part of the even universal punctured distribution (in other words, the first cohomology group of $\{1,-1\}$ with coefficients in the universal punctured distribution), which was computed by Schmidt [9] (mentioned in [11, before 12.18]); so again our approach seems to be shorter and in some sense easier.

Let us briefly explain the connection to cyclotomic fields. Taking any cyclotomic field K, or even more generally any compositum of imaginary abelian fields K_p such that each K_p is ramified at only one prime p, the absolute Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ is the direct product of its inertia subgroups $G_p \cong \mathrm{Gal}(K_p/\mathbb{Q})$. Each G_p contains a distinguished element j_p of order 2 given in $\mathrm{Gal}(K_p/\mathbb{Q})$ by complex conjugation. We enlarge each group G_p to a semigroup G_p^* by adding a new element g_p^*, and define G^* as the direct product of all semigroups G_p^*. Then the modules $\mathcal{N}_{\pm1}$ can be used to describe the Stickelberger ideal of K and the group of circular units of K as follows: The Stickelberger ideal of K is defined as the intersection $\mathcal{S} = \mathbb{Z}[G] \cap \mathcal{S}'$ where $\mathcal{S}' \subset \mathbb{Q}[G]$ is a $\mathbb{Z}[G]$-module isomorphic to $\mathbb{Z} \oplus (\mathcal{N}_{-1}/\mathrm{Tor}(\mathcal{N}_{-1}))$. Similarly, the $\mathbb{Z}[G]$-modules of circular units and numbers of K can be described by $\mathcal{N}_1$: denoting by $\mathcal{C}$, $\mathcal{D}$, and $\mathcal{E}$ the groups of circular units, circular numbers, and all units of K, respectively, by definition, $\mathcal{C} = \mathcal{D} \cap \mathcal{E}$ and $\mathbb{Z} \oplus (\mathcal{D}^{1+j}/\langle P\rangle) \cong \mathcal{N}_1/\mathrm{Tor}(\mathcal{N}_1)$, where $j \in G$ is the complex conjugation and $\langle P\rangle \subseteq \mathbb{Q}^\times$ is the subgroup generated by the primes ramifying in $K/\mathbb{Q}$. This allows us to describe $\mathbb{Z}$-bases of $\mathcal{D}$ and $\mathcal{C}$ in Theorem 4.2 and Corollary 4.3, and a $\mathbb{Z}$-basis of $\mathcal{S}'$ in Theorem 6.2. Moreover we obtain a presentation of $\mathcal{D}$ in Theorem 4.5. This presentation, which has not appeared in the literature yet, seems to be a useful tool in the study of circular numbers and units.

1. An auxiliary result on a group ring. This section is devoted to a result on the integral group ring over a finite abelian group of even order which appears to be useful in the next section.

Lemma 1.1. *Let G be a finite abelian group, and $j \in G$ be an element of order 2, i.e. $j \neq 1$ and $j^2 = 1$. Then there is a set $T \subseteq G$ and, for each $\sigma \in G$, a fixed $R_\sigma \in \mathbb{Z}[G]$ such that*

(i) *$R_1 = 0$ and $R_j = \sum_{\rho\in T} \rho$;*
(ii) *$1 \in T$ and for any $\sigma \in G$ we have $\sigma \in T$ if and only if $j\sigma \notin T$;*
(iii) *for any $\sigma, \tau \in G$ we have $(1-\tau)R_\sigma = (1-\sigma)R_\tau$.*

Proof. We can write $G = H \times H'$, where H is the 2-Sylow subgroup of G and H' is the subgroup of all elements of odd order. The well-known theorem on the structure of finite abelian groups says that there are $x_1, \dots, x_n \in H$ such that each x_i is of order 2^{a_i}, where $1 \le a_1 \le \dots \le a_n$, and $H = \langle x_1, \dots, x_n \rangle \cong \langle x_1 \rangle \times \dots \times \langle x_n \rangle$ is of order $2^{a_1+\dots+a_n}$. As $j \in H$ is of order 2, there are unique $e_1, \dots, e_n \in \{0,1\}$, not all zero, such that $j = \prod_{i=1}^n x_i^{e_i 2^{a_i-1}}$. Set $c = \min\{i;\, e_i \neq 0\}$ and $z = \prod_{i=c}^n x_i^{e_i 2^{a_i-a_c}}$. Then $z^{2^{a_c-1}} = j$ and so z is of order 2^{a_c}. Moreover $H = \langle z, x_1, \dots, x_{c-1}, x_{c+1}, \dots, x_n \rangle$. Let

$$H'' = \langle \{x_1, \dots, x_{c-1}, x_{c+1}, \dots, x_n\} \cup H' \rangle.$$

Then any $\sigma \in G$ can be uniquely written in the form $\sigma = z^i \cdot h$, where $0 \le i < 2^{a_c}$ and $h \in H''$, and we define

$$R_\sigma = \Big(\sum_{l \in H''} l \Big) \cdot \sum_{k=0}^{i-1} z^k,$$

where for $i = 0$ we have an empty sum, which should be understood as 0. Let

$$T = \{ z^k \cdot l;\, 0 \le k < 2^{a_c-1},\, l \in H'' \}.$$

It is easy to see that conditions (i) and (ii) are satisfied.

To prove (iii), let $\sigma = z^s \cdot u$ and $\tau = z^t \cdot v$, where $0 \le s < 2^{a_c}$, $0 \le t < 2^{a_c}$, $u, v \in H''$. Then

$$\begin{aligned}
(1-\tau)R_\sigma &= (1 - z^t \cdot v) \cdot \Big(\sum_{h \in H''} h \Big) \cdot \Big(\sum_{k=0}^{s-1} z^k \Big) \\
&= (1 - z^t) \cdot \Big(\sum_{h \in H''} h \Big) \cdot \Big(\sum_{k=0}^{s-1} z^k \Big) \\
&= (1 - z) \cdot \Big(\sum_{k=0}^{t-1} z^k \Big) \cdot \Big(\sum_{h \in H''} h \Big) \cdot \Big(\sum_{k=0}^{s-1} z^k \Big),
\end{aligned}$$

which is symmetric with respect to $\sigma \leftrightarrow \tau$, so (iii) follows. ∎

2. The relation modules $\mathcal{I}_1$ and $\mathcal{I}_{-1}$. Suppose that we have a finite abelian group G_p with an element $j_p \in G_p$ of order 2 for each p in a non-empty linearly ordered finite set $(P, \le)$. Let $G = \prod_{p \in P} G_p$ be the product of these groups. For each $p \in P$ we shall identify G_p with the corresponding subgroup of G. Then for each $p \in P$ there are $T_p \subseteq G_p$ and $R_\sigma \in \mathbb{Z}[G_p] \subseteq \mathbb{Z}[G]$ for each $\sigma \in G_p$ given by Lemma 1.1. There is no danger of confusion as $G_p \cap G_q = \{1\}$ if $p \neq q$ and $R_1 = 0$.

For each $p \in P$ we enlarge G_p by a new element g_p^* to get an abelian semigroup $G_p^* = G_p \cup \{g_p^*\}$, where $u \cdot g_p^* = g_p^*$ for any $u \in G_p^*$. These new

elements depend on p; we assume $g_p^* \neq g_q^*$ for $p \neq q$. Let $G^* = \prod_{p\in P} G_p^*$ be the product of these semigroups. Then the additive group of the semigroup ring $\mathbb{Z}[G^*]$ is a $\mathbb{Z}[G]$-module (the action of G is by multiplication). We have the following isomorphism of $\mathbb{Z}[G]$-modules:

$$\mathbb{Z}[G^*] \cong \bigoplus_{Q\subseteq P} \mathbb{Z}\Big[\prod_{p\in Q} G_p\Big] \tag{2.1}$$

where, for each $Q \subseteq P$, the product $\prod_{p\in P-Q} g_p^*$ is sent to the element having 1 in the Qth summand and 0's everywhere else; the action of G on $\mathbb{Z}\big[\prod_{p\in Q} G_p\big]$ is via the projection $G \to \prod_{p\in Q} G_p$.

For any subset $A \subseteq G$ we define $S(A) = \sum_{h\in A} h$. Lemma 1 gives

$$(1 + j_p)R_{j_p} = S(G_p) \tag{2.2}$$

for each $p \in P$.

Fix $\epsilon \in \{1, -1\}$. For any distinct $p, q \in P$ we fix $\sigma_{p,q} \in G_q$. The $\sigma_{p,q}$ play the role of Frobenius automorphisms (more precisely, in Section 4, the Frobenius automorphism of p acts as $\prod_{q\in P-\{p\}} \sigma_{p,q}^{-1}$).

Let $\mathcal{I}_\epsilon$ be the $\mathbb{Z}[G]$-submodule of $\mathbb{Z}[G^*]$ generated by

$$\Big(S(G_p) - g_p^* \cdot \Big(1 - \prod_{q\in P-\{p\}} \sigma_{p,q}\Big)\Big) \cdot \prod_{q\in V} g_q^* \tag{2.3}$$

for all $p \in P$ and $V \subseteq P - \{p\}$, and by

$$\Big(1 - \epsilon \prod_{p\in P} j_p\Big) \cdot \prod_{q\in V} g_q^* \tag{2.4}$$

for all $V \subseteq P$ (an empty product for $V = \emptyset$ is understood as 1). Warning: $\mathcal{I}_\epsilon$ is not an ideal of the semigroup ring $\mathbb{Z}[G^*]$, for example supposing $P = \{1, 2\}$, $\sigma_{1,2} = \sigma_{2,1} = 1$, we have $S(G_1) \in \mathcal{I}_{-1}$ but $g_1^* \cdot S(G_1) = |G_1| g_1^* \notin \mathcal{I}_{-1}$. Indeed, in this case $\mathcal{I}_{-1}$ is the $\mathbb{Z}[G]$-submodule generated by $S(G_1)$, $S(G_1)g_2^*$, $S(G_2)$, $S(G_2)g_1^*$, $1 + j_1 j_2$, $(1 + j_2)g_1^*$, $(1 + j_1)g_2^*$, $2g_1^*g_2^*$, so each $\sum_{h\in G^*} a_h h \in \mathcal{I}_{-1}$ satisfies $a_{g_1^*} = a_{j_2 g_1^*}$.

For any non-empty $Q \subseteq P$, let $G'_Q = \bigcup_{p\in Q}(g_p^* \prod_{q\in P-Q} g_q^*)G^*$ be the set of all elements of G^* that are divisible by $g_p^* \prod_{q\in P-Q} g_q^*$ for at least one $p \in Q$. It is easy to see that $\mathbb{Z}[G'_Q]$ is the ideal of the semigroup ring $\mathbb{Z}[G^*]$ generated by $\{g_p^* \prod_{q\in P-Q} g_q^*;\ p \in Q\}$. By definition, $\mathbb{Z}[G'_\emptyset] = \{0\}$.

We shall use congruence modulo the $\mathbb{Z}[G]$-module $\mathcal{I}_\epsilon + 2\mathbb{Z}[G'_Q]$ even though it is not an ideal of $\mathbb{Z}[G^*]$; the congruence $\alpha \equiv \beta$ simply means $\alpha - \beta \in \mathcal{I}_\epsilon + 2\mathbb{Z}[G'_Q]$. The following proposition will be used to derive Theorem 2.2 which is a key tool in Section 3.

PROPOSITION 2.1. *If $Q \subseteq P$ satisfies $(-1)^{|Q|} = -\epsilon$ then for any integer $n \geq 0$ we have the following congruence modulo $\mathcal{I}_\epsilon + 2\mathbb{Z}[G'_Q]$:*

$$(2.5)\quad 2\Big(\prod_{q\in P-Q} g_q^*\Big)\prod_{w\in Q} R_{j_w} \equiv \Big(\prod_{q\in P-Q} g_q^*\Big)\sum_u\Big(\Big(\prod_{\substack{1\le i\le n\\ 2\nmid i}} j_{u(i)}\Big)\cdot\sum_p\Big(\Big(\prod_{i=1}^n g^*_{p(i)}\Big)\cdot\Big(\prod_{i=1}^n\prod_{\substack{v\in Q-(\widetilde{u}\cup\widetilde{p})\\ v<p(i)}} j_v\Big)\Big(\prod_{i=1}^n\prod_{\substack{t\in Q-\widetilde{p}\\ t<u(i)}}\sigma_{p(i),t}\Big)\Big(\prod_{i=1}^n R_{\sigma_{p(i),u(i)}}\Big)\cdot\Big(\prod_{w\in Q-(\widetilde{u}\cup\widetilde{p})} R_{j_w}\Big)\Big(1+\epsilon\prod_{x\in Q-(\widetilde{u}\cup\widetilde{p})} j_x\Big)\Big)\Big),$$

where, in the first sum, u runs through the set of all isotone injective mappings $u:\{1,\dots,n\}\to Q$ while the second sum is taken over all injective mappings $p:\{1,\dots,n\}\to Q$ such that the images $\widetilde{u}=u(\{1,\dots,n\})$ and $\widetilde{p}=p(\{1,\dots,n\})$ are disjoint.

Proof. We shall use induction on n. If $n=0$ then the right hand side of (2.5) is equal to

$$\Big(\prod_{q\in P-Q} g_q^*\Big)\Big(\prod_{w\in Q} R_{j_w}\Big)\Big(1+\epsilon\prod_{x\in Q} j_x\Big)=\Big(\prod_{q\in P-Q} g_q^*\Big)\Big(\prod_{w\in Q} R_{j_w}\Big)\Big(1+\epsilon\prod_{x\in P} j_x\Big).$$

Since

$$\Big(1+\epsilon\prod_{x\in P} j_x\Big)\Big(\prod_{q\in P-Q} g_q^*\Big)\equiv 2\Big(\prod_{q\in P-Q} g_q^*\Big)\ (\mathrm{mod}\ \mathcal{I}_\epsilon)$$

due to (2.4), the assertion is proven for $n=0$.

Now we need to show that the right hand side for any given $n\ge 0$ is congruent modulo $\mathcal{I}_\epsilon+2\mathbb{Z}[G'_Q]$ to the right hand side for $n+1$. Since $(-1)^{|Q|}=-\epsilon$ and $|\widetilde{u}\cup\widetilde{p}|=2n$, we have $(-1)^{|Q-(\widetilde{u}\cup\widetilde{p})|}=-\epsilon$ and so

$$1+\epsilon\prod_{x\in Q-(\widetilde{u}\cup\widetilde{p})} j_x=\sum_{x\in Q-(\widetilde{u}\cup\widetilde{p})}(1+j_x)\prod_{\substack{v\in Q-(\widetilde{u}\cup\widetilde{p})\\ v<x}}(-j_v).$$

We can include the sum over all x into the sum over all injective mappings p by the following procedure: enlarge the domain of p from $\{1,\dots,n\}$ to $\{1,\dots,n+1\}$ and define $p(n+1)=x$. Using $j_x(1+j_x)=1+j_x$, $(1+j_x)R_{j_x}=S(G_x)$, and $\sigma_{p(i),x}S(G_x)=S(G_x)$, we obtain on the right hand side of (2.5)

$$\Big(\prod_{q\in P-Q} g_q^*\Big)\sum_u\Big(\Big(\prod_{\substack{1\le i\le n\\ 2\nmid i}} j_{u(i)}\Big)\sum_p\Big(\prod_{i=1}^n\prod_{\substack{v\in Q-(\widetilde{u}\cup\widetilde{p})\\ v<p(i)}} j_v\Big)\Big(\prod_{\substack{v\in Q-(\widetilde{u}\cup\widetilde{p})\\ v<p(n+1)}}(-j_v)\Big)\cdot\Big(\prod_{i=1}^n g^*_{p(i)}\Big)\Big(\prod_{i=1}^n\prod_{\substack{t\in Q-\widetilde{p}\\ t<u(i)}}\sigma_{p(i),t}\Big)\Big(\prod_{i=1}^n R_{\sigma_{p(i),u(i)}}\Big)\Big(\prod_{w\in Q-(\widetilde{u}\cup\widetilde{p})} R_{j_w}\Big)S(G_{p(n+1)})\Big),$$

with the second sum taken over all injective mappings $p : \{1, \dots, n+1\} \to Q - \widetilde{u}$. Since all the other factors belong to $\mathbb{Z}[G]$, we can use the following congruence modulo $\mathcal{I}_\epsilon$ given by (2.3):

$$\Big(\prod_{q\in P-Q} g_q^*\Big)\Big(\prod_{i=1}^{n} g_{p(i)}^*\Big)S(G_{p(n+1)}) \equiv \Big(\prod_{q\in \widetilde{p}\cup(P-Q)} g_q^*\Big)\Big(1-\prod_{r\in P-\{p(n+1)\}}\sigma_{p(n+1),r}\Big).$$

It is easy to see that

$$\begin{aligned}\Big(\prod_{q\in \widetilde{p}\cup(P-Q)} g_q^*\Big)\cdot\Big(1-\prod_{r\in P-\{p(n+1)\}}\sigma_{p(n+1),r}\Big) &= \Big(\prod_{q\in \widetilde{p}\cup(P-Q)} g_q^*\Big)\cdot\Big(1-\prod_{r\in Q-\widetilde{p}}\sigma_{p(n+1),r}\Big)\\ &= \Big(\prod_{q\in \widetilde{p}\cup(P-Q)} g_q^*\Big)\cdot\sum_{r\in Q-\widetilde{p}}(1-\sigma_{p(n+1),r})\prod_{\substack{t\in Q-\widetilde{p}\\ t<r}}\sigma_{p(n+1),t}.\end{aligned}$$

Using $\prod_{q\in\widetilde{p}\cup(P-Q)} g_q^* \in \mathbb{Z}[G'_Q]$ we can modify modulo $\mathcal{I}_\epsilon + 2\mathbb{Z}[G'_Q]$ the previous version of the right hand side of (2.5) to get

$$\sum_u\Big(\Big(\prod_{\substack{1\le i\le n\\ 2\nmid i}} j_{u(i)}\Big)\sum_{r\in Q}\sum_p\Big(\prod_{q\in\widetilde{p}\cup(P-Q)} g_q^*\Big)\Big(\prod_{i=1}^{n+1}\prod_{\substack{v\in Q-(\widetilde{u}\cup\widetilde{p})\\ v<p(i)}} j_v\Big)\Big(\prod_{\substack{t\in Q-\widetilde{p}\\ t<r}}\sigma_{p(n+1),t}\Big) \cdot\Big(\prod_{i=1}^{n}\prod_{\substack{t\in Q-\widetilde{p}\\ t<u(i)}}\sigma_{p(i),t}\Big)\Big(\prod_{i=1}^{n} R_{\sigma_{p(i),u(i)}}\Big)\Big(\prod_{w\in Q-(\widetilde{u}\cup\widetilde{p})} R_{j_w}\Big)(1-\sigma_{p(n+1),r})\Big),$$

where the third sum is taken over all injective mappings $p : \{1, \dots, n+1\} \to Q - (\widetilde{u} \cup \{r\})$. If $r = u(i)$ for some i then using

$$(1-\sigma_{p(n+1),r})R_{\sigma_{p(i),u(i)}} = (1-\sigma_{p(i),r})R_{\sigma_{p(n+1),u(i)}}$$

by Lemma 1.1, we see by the symmetry $p(i) \leftrightarrow p(n+1)$ that each such summand appears twice. Due to the factor $\prod_{q\in\widetilde{p}\cup(P-Q)} g_q^* \in \mathbb{Z}[G'_Q]$ we can ignore all these summands, in other words, the sum over all $r \in Q$ is congruent modulo $\mathcal{I}_\epsilon + 2\mathbb{Z}[G'_Q]$ to the sum over all $r \in Q - \widetilde{u}$. As the product $\prod_w R_{j_w}$ contains the factor R_{j_r}, we can use the identity

$$(1-\sigma_{p(n+1),r})R_{j_r} = (1-j_r)R_{\sigma_{p(n+1),r}}$$

due to Lemma 1.1 and the identity $j_r(1-j_r) = -(1-j_r)$ allowing us to add the condition $v \ne r$ in the previous product of j_v's, again working modulo $2\mathbb{Z}[G'_Q]$.

Recall that the mapping u is isotone and injective, so $u(1) < \cdots < u(n)$ and in fact we can split the sum over all $r \in Q - \widetilde{u}$ into $n+1$ sums. Letting $s \in \{0, 1, \ldots, n\}$ we have the sum over all $r < u(1)$ for $s = 0$, the sums over all r such that $u(s) < r < u(s+1)$ for $s = 1, \ldots, n-1$, and finally the sum over all $r > u(n)$ for $s = n$. We want to enlarge the domain of u from $\{1, \ldots, n\}$ to $\{1, \ldots, n+1\}$ by introducing a new value $u(n+1) = r$. But to get an isotone mapping we must permute the values of u and p in the same way: let $u', p' : \{1, \ldots, n+1\} \to Q$ satisfy $u'(i) = u(i)$ and $p'(i) = p(i)$ if $i \le s$, and $u'(i+1) = u(i)$ and $p'(i+1) = p(i)$ if $s < i \le n$. Finally let $u'(s+1) = u(n+1)$ and $p'(s+1) = p(n+1)$.

Since $j_{u(s+1)}(1 - j_{u(s+1)}) = -(1 - j_{u(s+1)})$, working modulo $2\mathbb{Z}[G'_Q]$, the right hand side of our identity is changed into

$$\sum_u \Big(\sum_p \Big(\prod_{q \in \widetilde{p} \cup (P-Q)} g_q^* \Big) \Big(\prod_{i=1}^{n+1} \prod_{\substack{v \in Q - (\widetilde{u} \cup \widetilde{p}) \\ v < p(i)}} j_v \Big) \Big(\prod_{i=1}^{n+1} \prod_{\substack{t \in Q - \widetilde{p} \\ t < u(i)}} \sigma_{p(i),t} \Big) \cdot \Big(\prod_{i=1}^{n+1} R_{\sigma_{p(i),u(i)}} \Big) \Big(\prod_{w \in Q - (\widetilde{u} \cup \widetilde{p})} R_{j_w} \Big) \Big) \cdot \Big(\sum_{s=0}^{n} \Big(\prod_{\substack{1 \le i \le s \\ 2 \nmid i}} j_{u(i)} \Big) \Big(\prod_{\substack{s+1 \le i \le n+1 \\ 2 \mid i}} j_{u(i)} \Big) (1 - j_{u(s+1)}) \Big),$$

where the first sum is now taken over all isotone and injective mappings $u : \{1, \ldots, n+1\} \to Q$, while the second sum is over all injective mappings $p : \{1, \ldots, n+1\} \to Q - \widetilde{u}$. Using $j_{u(i)}^2 = 1$, we have

$$\begin{aligned} &\sum_{s=0}^{n} \Big(\prod_{\substack{1 \le i \le s \\ 2 \nmid i}} j_{u(i)} \Big) \cdot \Big(\prod_{\substack{s+1 \le i \le n+1 \\ 2 \mid i}} j_{u(i)} \Big) \cdot (1 - j_{u(s+1)}) \\ &\qquad = \Big(\prod_{\substack{1 \le i \le n+1 \\ 2 \nmid i}} j_{u(i)} \Big) \cdot \sum_{s=0}^{n} \Big(\Big(\prod_{i=s+1}^{n+1} j_{u(i)} \Big) (1 - j_{u(s+1)}) \Big) \\ &\qquad = \Big(\prod_{\substack{1 \le i \le n+1 \\ 2 \nmid i}} j_{u(i)} \Big) \cdot \sum_{s=0}^{n} \Big(\Big(\prod_{i=s+1}^{n+1} j_{u(i)} \Big) - \Big(\prod_{i=s+2}^{n+1} j_{u(i)} \Big) \Big) \\ &\qquad = \Big(\prod_{\substack{1 \le i \le n+1 \\ 2 \nmid i}} j_{u(i)} \Big) \cdot \Big(-1 + \prod_{i=1}^{n+1} j_{u(i)} \Big). \end{aligned}$$

Finally $2\prod_{q\in\widetilde{p}\cup(P-Q)} g_q^* \in 2\mathbb{Z}[G'_Q]$, and using (2.4) we get

$$\Big(\prod_{q\in\widetilde{p}\cup(P-Q)} g_q^*\Big)\cdot\Big(1+\prod_{w\in\widetilde{u}} j_w\Big) \equiv \Big(\prod_{q\in\widetilde{p}\cup(P-Q)} g_q^*\Big)\cdot\Big(1+\epsilon\prod_{x\in P-\widetilde{u}} j_x\Big)$$
$$= \Big(\prod_{q\in\widetilde{p}\cup(P-Q)} g_q^*\Big)\cdot\Big(1+\epsilon\prod_{x\in Q-(\widetilde{u}\cup\widetilde{p})} j_x\Big)$$

modulo $\mathcal{I}_\epsilon$, giving the right hand side of (2.5) for $n+1$. ∎

THEOREM 2.2. *For each $Q\subseteq P$ satisfying $(-1)^{|Q|}=-\epsilon$ there is $\alpha_Q\in\mathbb{Z}[G'_Q]$ such that*

$$2\alpha_Q - 2\Big(\prod_{q\in P-Q} g_q^*\Big)\prod_{p\in Q} R_{j_p}\in\mathcal{I}_\epsilon.$$

Proof. The right hand side of the formula in Proposition 2.1 is zero for any $n>\frac{1}{2}|Q|$ and so there is $\alpha_Q\in\mathbb{Z}[G'_Q]$ as desired. ∎

3. The modules $\mathcal{N}_1=\mathbb{Z}[G^*]/\mathcal{I}_1$ and $\mathcal{N}_{-1}=\mathbb{Z}[G^*]/\mathcal{I}_{-1}$. Recall that for each p in a non-empty linearly ordered finite set $(P,\leq)$ we have a finite abelian group G_p with an element $j_p\in G_p$ of order 2, and a set T_p with $1\in T_p\subseteq G_p$ and such that, for any $\sigma\in G_p$, $\sigma\in T_p$ if and only if $\sigma j_p\notin T_p$. Moreover, G_p is enlarged by a new element g_p^* to an abelian semigroup $G_p^*=G_p\cup\{g_p^*\}$, where $u\cdot g_p^*=g_p^*$, for any $u\in G_p^*$. We also have the corresponding products $G=\prod_{p\in P}G_p$ and $G^*=\prod_{p\in P}G_p^*$. For each $p\in P$ there is a projection $\pi_p: G^*\to G_p^*$, so $g=\prod_{p\in P}\pi_p(g)$ for any $g\in G^*$.

For each $g\in G^*$ we define the following subsets of P:

$$X(g)=\{p\in P;\ \pi_p(g)=g_p^*\},$$
$$U(g)=\{p\in P;\ \pi_p(g)=1\},$$
$$V(g)=\{p\in P;\ \pi_p(g)=j_p\},$$
$$W(g)=U(g)\cup V(g).$$

If $X(g)\cup W(g)\neq P$, we set

$$c(g)=\max\big(P-(X(g)\cup W(g))\big).$$

For each $\epsilon\in\{1,-1\}$ we define a subset $M_\epsilon\subseteq G^*$ as follows: for any $g\in G^*$ we declare $g\in M_\epsilon$ if and only if $V(g)=\emptyset$ and either

$$X(g)\cup W(g)=P \quad\text{and}\quad (-1)^{|U(g)|}=\epsilon,$$

or

$$X(g)\cup W(g)\neq P \quad\text{and}\quad \pi_{c(g)}(g)\in T_{c(g)}.$$

LEMMA 3.1. *We have $|M_1|=|M_{-1}|=\frac{1}{2}|G|$.*

Proof. Since $|G_p^* - \{j_p\}| = |G_p|$, the set of all $g \in G^*$ satisfying $V(g) = \emptyset$ contains exactly $|G|$ elements. This set splits into two subsets according to whether g satisfies $X(g) \cup W(g) = P$ or not. The condition $(-1)^{|U(g)|} = \epsilon$ is fulfilled by exactly half of the g satisfying both $V(g) = \emptyset$ and $X(g) \cup W(g) = P$. Similarly the condition $\pi_{c(g)}(g) \in T_{c(g)}$ is fulfilled by exactly half of the g for which both $V(g) = \emptyset$ and $X(g) \cup W(g) \neq P$, because $|T_p - \{1\}| = \frac{1}{2}|G_p - \{1, j_p\}|$. ∎

We set

$$z(g) = \begin{cases} 0 & \text{if } X(g) \cup W(g) \neq P \text{ and } \pi_{c(g)}(g) \in T_{c(g)}, \\ 1 & \text{otherwise} \end{cases}$$

and define an ordering $\preceq$ on G^* as follows: for any $g, h \in G^*$ we have $g \prec h$ if exactly one of the following four cases holds:

- $X(g) \supsetneq X(h)$;
- $X(g) = X(h)$ and $W(g) \subsetneq W(h)$;
- $X(g) = X(h)$, $W(g) = W(h)$, and $z(g) < z(h)$;
- $X(g) = X(h)$, $W(g) = W(h)$, $z(g) = z(h)$, and $V(g) \subsetneq V(h)$.

Then $g \preceq h$ means $g \prec h$ or $g = h$.

In Section 2, for any $\epsilon \in \{1, -1\}$ we have defined the $\mathbb{Z}[G]$-submodules $\mathcal{I}_\epsilon$ of $\mathbb{Z}[G^*]$ generated by (2.3) and (2.4). Let $\mathcal{N}_\epsilon = \mathbb{Z}[G^*]/\mathcal{I}_\epsilon$ and let $\mathrm{Tor}(\mathcal{N}_\epsilon)$ be the submodule of elements of finite order in $\mathcal{N}_\epsilon$. Finally, let $j = \prod_{p \in P} j_p$; we have $X(jg) = X(g)$ and $W(jg) = W(g)$ for any $g \in G^*$.

LEMMA 3.2. *Let $\epsilon \in \{1, -1\}$ and $h \in G^*$, $h \notin M_\epsilon$. Then $h + \mathcal{I}_\epsilon \in \mathcal{N}_\epsilon$ is a sum of an element belonging to $\mathrm{Tor}(\mathcal{N}_\epsilon)$ and a $\mathbb{Z}$-linear combination of elemens $g + \mathcal{I}_\epsilon$ where $g \in G^*$ with $g \prec h$.*

Proof. We shall distinguish the following four cases:

1. Assume $X(h) \cup W(h) \neq P$ and $z(h) = 0$. Since $h \notin M_\epsilon$, we have $V(h) \neq \emptyset$; denote $p = \min V(h)$. Then $p \notin X(h)$ and due to (2.3) we have

$$\Big(S(G_p) - g_p^* \cdot \Big(1 - \prod_{q \in P - \{p\}} \sigma_{p,q}\Big)\Big) \cdot h \in \mathcal{I}_\epsilon. \tag{3.1}$$

Since $X(g_p^* h) = X(g_p^* h \prod_{q \in P - \{p\}} \sigma_{p,q}) = X(h) \cup \{p\}$, we get $g_p^* h \prec h$ and $g_p^* h \prod_{q \in P - \{p\}} \sigma_{p,q} \prec h$. For any $k \in G_p$ with $1 \neq k \neq j_p$, we have $X(kh) = X(h)$ and $W(kh) = W(h) - \{p\}$, so $kh \prec h$. Moreover $X(j_p h) = X(h)$, $W(j_p h) = W(h)$, $c(j_p h) = c(h) \neq p$ and so $z(j_p h) = z(h)$, and finally $V(j_p h) = V(h) - \{p\}$. Hence $j_p h \prec h$.

2. Assume $X(h) \cup W(h) \neq P$ and $z(h) = 1$. Then $X(jh) = X(h)$, $W(jh) = W(h)$, $c(jh) = c(h)$ and so $z(jh) = 0$. This gives $jh \prec h$ and we can use $(1 - \epsilon j)h \in \mathcal{I}_\epsilon$ due to (2.4).

3. Assume $X(h) \cup W(h) = P$ and $V(h) = \emptyset$; then $h = \prod_{p \in X(h)} g_p^*$. Since $h \notin M_\epsilon$, we have $(-1)^{|U(h)|} = -\epsilon$, and Theorem 2.2 gives $\alpha_{U(h)} \in \mathbb{Z}[G'_{U(h)}]$

such that

$$\Big(\alpha_{U(h)} - h \cdot \prod_{p\in U(h)} R_{j_p}\Big) + \mathcal{I}_\epsilon \in \mathrm{Tor}(\mathcal{N}_\epsilon). \tag{3.2}$$

Then $\alpha_{U(h)}$ is a $\mathbb{Z}$-linear combination of $g \in G^*$ having $X(g) \supsetneq X(h)$; these g's satisfy $g \prec h$. It is easy to see that $h\prod_{p\in U(h)} R_{j_p}$ is the sum of all $g \in G^*$ satisfying $\pi_p(g) = g_p^*$ for each $p \in X(h)$ and $\pi_p(g) \in T_p$ for each $p \in U(h) = P - X(h)$. One of those g's equals h and the others satisfy $X(g) = X(h)$ and $W(g) \subsetneq W(h)$, which means $g \prec h$.

4. Assume $X(h) \cup W(h) = P$ and $V(h) \neq \emptyset$. Denoting $p = \min V(h)$, we can use (3.1) again. As in the first case we have $g_p^* h \prec h$, $g_p^* h \prod_{q\in P-\{p\}} \sigma_{p,q} \prec h$, and $kh \prec h$ for each $k \in G_p$ with $1 \neq k \neq j_p$. Since $X(j_p h) = X(h)$, $W(j_p h) = W(h)$, $z(j_p h) = 1 = z(h)$, and $V(j_p h) = V(h) - \{p\}$, we get $j_p h \prec h$.

The lemma follows as each h satisfies exactly one of the previous cases. ∎

Proposition 3.3. *The image of M_ϵ generates $\mathcal{N}_\epsilon/\mathrm{Tor}(\mathcal{N}_\epsilon)$ as a $\mathbb{Z}$-module.*

Proof. Lemma 3.2 implies by induction with respect to the ordering $\preceq$ that the image of any $h \in G^*$ in $\mathcal{N}_\epsilon/\mathrm{Tor}(\mathcal{N}_\epsilon)$ is generated by the image of $M_\epsilon \cap \{g \in G^*;\, g \preceq h\}$. ∎

Corollary 3.4. *For any $\epsilon \in \{1, -1\}$,*

$$\mathrm{rank}_{\mathbb{Z}}\, \mathcal{N}_\epsilon \leq \tfrac{1}{2}|G|.$$

Proof. This follows from Proposition 3.3 and Lemma 3.1. ∎

Let $\mathcal{I}_0$ be the $\mathbb{Z}[G]$-submodule of $\mathbb{Z}[G^*]$ generated by (2.3) for all $p \in P$ and all $V \subseteq P - \{p\}$, and let $\mathcal{N}_0 = \mathbb{Z}[G^*]/\mathcal{I}_0$. Moreover, let U' be the module defined in [4] for $I = P$, $T_p = G_p$, and $\lambda_p^{-1} = \prod_{q\in P-\{p\}} \sigma_{p,q}$, i.e. $U' \subseteq \mathbb{Q}[G]$ is the $\mathbb{Z}[G]$-module generated by

$$\rho'_N = S\Big(\prod_{p\in N} G_p\Big) \cdot \prod_{i\in P-N} \big(1 - |G_i|^{-1}\lambda_i^{-1} S(G_i)\big)$$

for all $N \subseteq P$.

Lemma 3.5. *Let $\gamma : \mathbb{Z}[G^*] \to U'$ be the $\mathbb{Z}[G]$-linear map determined by $\gamma(\prod_{p\in N} g_p^*) = \rho'_N$ for each $N \subseteq P$. Then γ is surjective and $\ker\gamma = \mathcal{I}_0$, hence $\mathcal{N}_0 \cong U'$ has no $\mathbb{Z}$-torsion. Moreover $\mathcal{I}_0 = \mathcal{I}_1 \cap \mathcal{I}_{-1}$, and so the natural $\mathbb{Z}[G]$-linear map $\delta : \mathcal{N}_0 \to \mathcal{N}_1 \oplus \mathcal{N}_{-1}$, determined by $\delta(\alpha + \mathcal{I}_0) = (\alpha + \mathcal{I}_1, \alpha + \mathcal{I}_{-1})$, is injective.*

Proof. The definition of ρ'_N implies that $g\rho'_N = \rho'_N$ for any $g \in \prod_{p\in N} G_p$, and (2.1) implies that γ is well-defined. For any $p \in P$ and $V \subseteq P - \{p\}$ we

have

$$\gamma\Big(S(G_p)\prod_{q\in V} g_q^* - \big(1-\prod_{q\in P-\{p\}}\sigma_{p,q}\big)\prod_{q\in V\cup\{p\}} g_q^*\Big) = S(G_p)\rho'_V - (1-\lambda_p^{-1})\rho'_{V\cup\{p\}}$$

and the presentation of U' given in [4, Corollary 1.6(i)] implies that $\mathcal{I}_0 = \ker\gamma$ and so $\mathcal{N}_0 \cong U' \subseteq \mathbb{Q}[G]$ has no $\mathbb{Z}$-torsion.

It is clear that $\mathcal{I}_0 \subseteq \mathcal{I}_1 \cap \mathcal{I}_{-1}$ and so δ is well-defined. For any $\beta \in \mathcal{I}_\epsilon$ we have $(1+\epsilon j)\beta \in \mathcal{I}_0$ because $1+\epsilon j$ kills the generators (2.4). Hence for any $\beta \in \mathcal{I}_1 \cap \mathcal{I}_{-1}$ we have $2\beta = (1+j)\beta + (1-j)\beta \in \mathcal{I}_0$ and $\ker\delta = (\mathcal{I}_1 \cap \mathcal{I}_{-1})/\mathcal{I}_0$ is 2-elementary. Since $\mathcal{N}_0$ has no $\mathbb{Z}$-torsion, δ is injective. ∎

THEOREM 3.6. *For any $\epsilon \in \{1,-1\}$, $\mathrm{Tor}(\mathcal{N}_\epsilon)$ is a 2-elementary group and the image of M_ϵ is a $\mathbb{Z}$-basis of $\mathcal{N}_\epsilon/\mathrm{Tor}(\mathcal{N}_\epsilon)$. Hence we can decompose the $\mathbb{Z}$-module $\mathcal{N}_\epsilon$ into the following direct sum of $\mathbb{Z}$-modules:*

$$\mathcal{N}_\epsilon = \mathrm{Tor}(\mathcal{N}_\epsilon) \oplus \bigoplus_{x\in M_\epsilon} (x+\mathcal{I}_\epsilon)\mathbb{Z}.$$

Proof. We have $(1-j)\mathbb{Z}[G^*] \subseteq \mathcal{I}_1$ and $(1+j)\mathbb{Z}[G^*] \subseteq \mathcal{I}_{-1}$ due to (2.4). For any $u, v \in \mathbb{Z}[G^*]$ let

$$w = (1+j)u + (1-j)v = 2u + (1-j)(v-u) = 2v + (1+j)(u-v).$$

Then $\delta(w+\mathcal{I}_0) = (2u+\mathcal{I}_1, 2v+\mathcal{I}_{-1})$. Hence if $u+\mathcal{I}_1 \in \mathrm{Tor}(\mathcal{N}_1)$ and $v+\mathcal{I}_{-1} \in \mathrm{Tor}(\mathcal{N}_{-1})$ then $(2u+\mathcal{I}_1, 2v+\mathcal{I}_{-1})$ is an element of finite order in $\delta(\mathcal{N}_0)$, which has no $\mathbb{Z}$-torsion due to Lemma 3.5. Hence $2u \in \mathcal{I}_1$ and $2v \in \mathcal{I}_{-1}$. Both $\mathrm{Tor}(\mathcal{N}_1)$ and $\mathrm{Tor}(\mathcal{N}_{-1})$ are 2-elementary. Since δ is injective,

$$\mathrm{rank}_{\mathbb{Z}}\,\mathcal{N}_1 + \mathrm{rank}_{\mathbb{Z}}\,\mathcal{N}_{-1} \geq \mathrm{rank}_{\mathbb{Z}}\,\mathbb{Z}[G^*]/\mathcal{I}_0 = \mathrm{rank}_{\mathbb{Z}}\,U' = |G| \tag{3.3}$$

by using [4, Remark 1.4], and we have equality in Corollary 3.4. The theorem follows from Lemma 3.1 and Proposition 3.3. ∎

LEMMA 3.7. *Let $\mu_1 : \mathbb{Z}[G^*] \to \mathcal{N}_1$ and $\mu_{-1} : \mathbb{Z}[G^*] \to \mathcal{N}_{-1}$ be the projections to the quotients. For any $\epsilon \in \{1,-1\}$ and any $\mathbb{Z}$-linear map $f : \mathcal{N}_\epsilon \to \mathbb{F}_2$, where $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$, there is $\tilde{f} : \mathcal{N}_{-\epsilon} \to \mathbb{F}_2$ such that $\tilde{f}\circ\mu_{-\epsilon} = f\circ\mu_\epsilon$.*

Proof. The form of the generators (2.4) implies that $2\mathbb{Z}[G^*] + \mathcal{I}_1 = 2\mathbb{Z}[G^*] + \mathcal{I}_{-1}$. Hence we have the commutative diagram

$$\begin{array}{ccccc}
\mathcal{N}_\epsilon & \xleftarrow{\mu_\epsilon} & \mathbb{Z}[G^*] & \xrightarrow{\mu_{-\epsilon}} & \mathcal{N}_{-\epsilon} \\
{\scriptstyle f}\downarrow & & \downarrow & & \downarrow \\
\mathbb{F}_2 & \leftarrow\!-\!- & \mathbb{Z}[G^*]/(2\mathbb{Z}[G^*]+\mathcal{I}_\epsilon) & \xleftarrow{\mathrm{id}} & \mathbb{Z}[G^*]/(2\mathbb{Z}[G^*]+\mathcal{I}_{-\epsilon})
\end{array}$$

where the no-name vertical arrows are the projections to the quotients. For any $\mathbb{Z}$-linear map $f : \mathcal{N}_\epsilon \to \mathbb{F}_2$ we have $2\mathbb{Z}[G^*] \subseteq \ker(f\circ\mu_\epsilon)$ and the existence of the dashed arrow follows; we obtain $\tilde{f}$ as the compositum of the given maps. ∎

For any $U \subseteq P$ we define $y_U = \prod_{p\in P-U} g_p^*$. If $\epsilon = -(-1)^{|U|}$ then $y_U \in M_{-\epsilon}$ and $y_U \notin M_\epsilon$, so Lemma 3.2 for $h = y_U$ gives (3.2) and we know that there is $\alpha_U \in \mathbb{Z}[G'_U]$ such that

$$c_U = -\alpha_U + y_U \cdot \prod_{p\in U} R_{j_p} \in \mathbb{Z}[G^*]$$

satisfies $c_U + \mathcal{I}_\epsilon \in \mathrm{Tor}(\mathcal{N}_\epsilon)$. Moreover any element of $\mathbb{Z}[G'_U]$ is a $\mathbb{Z}$-linear combination of $h \in G^*$ such that $P - U \subsetneq X(h)$, and Lemma 3.2 implies by induction with respect to $\preceq$ that

$$y_U \cdot \prod_{p\in U} R_{j_p} = c_U + \sum_{h\in M_\epsilon,\, X(h)\supsetneq P-U} a_{h,U} \cdot h \tag{3.4}$$

for suitable $a_{h,U} \in \mathbb{Z}$. Moreover the proof of Lemma 3.2 shows that the $\mathbb{Z}$-module $\mathrm{Tor}(\mathcal{N}_\epsilon)$ is generated by $\{c_U + \mathcal{I}_\epsilon;\, U \subseteq P,\, (-1)^{|U|} = -\epsilon\}$. Theorem 3.6 states that $\mathrm{Tor}(\mathcal{N}_\epsilon)$ is a vector space over $\mathbb{F}_2$. But we can say even more:

THEOREM 3.8. *For any $\epsilon \in \{1, -1\}$, the set $\{c_U + \mathcal{I}_\epsilon;\, U \subseteq P,\, (-1)^{|U|} = -\epsilon\}$ is a basis of the vector space $\mathrm{Tor}(\mathcal{N}_\epsilon)$ over $\mathbb{F}_2$. Hence $\dim_{\mathbb{F}_2} \mathrm{Tor}(\mathcal{N}_\epsilon) = 2^{|P|-1}$.*

Proof. We need to show that this set is linearly independent. So assume that there is a linear dependence, which means that there is a non-empty subset $\mathcal{R} \subseteq \{U \subseteq P;\ (-1)^{|U|} = -\epsilon\}$ such that $\sum_{W\in\mathcal{R}}(c_W + \mathcal{I}_\epsilon) = 0$ in $\mathcal{N}_\epsilon$. Let us fix a maximal $U \in \mathcal{R}$ (with respect to inclusion).

Hence $y_U \in M_{-\epsilon}$ and $y_U \notin M_\epsilon$. Theorem 3.6 implies that there is a unique $\mathbb{Z}$-linear map $f : \mathcal{N}_{-\epsilon} \to \mathbb{F}_2$ such that

$$y_U + \mathcal{I}_{-\epsilon} \notin \ker f \quad \text{and} \quad \mathrm{Tor}(\mathcal{N}_{-\epsilon}) \cup \{x + \mathcal{I}_{-\epsilon};\, x \in M_{-\epsilon},\, x \neq y_U\} \subseteq \ker f.$$

Lemma 3.7 gives $\tilde f : \mathcal{N}_\epsilon \to \mathbb{F}_2$ such that $\tilde f \circ \mu_\epsilon = f \circ \mu_{-\epsilon}$ and so

$$y_U + \mathcal{I}_\epsilon \notin \ker \tilde f \quad \text{and} \quad \{x + \mathcal{I}_\epsilon;\ x \in M_{-\epsilon},\ x \neq y_U\} \subseteq \ker \tilde f.$$

The left hand side of (3.4) is the sum of all elements $g \in G^*$ satisfying $\pi_p(g) = g_p^*$ for each $p \in P - U$ and $\pi_p(g) \in T_p$ for each $p \in U$. All these g's belong to $M_{-\epsilon}$ and one of them equals y_U. Thus

$$\tilde f\Big(\Big(y_U \cdot \prod_{p\in U} R_{j_p}\Big) + \mathcal{I}_\epsilon\Big) = 1. \tag{3.5}$$

Suppose that $h \in M_\epsilon \cup M_{-\epsilon}$ and $X(h) \not\subseteq P - U$. If $h \in M_{-\epsilon}$ then $\tilde f(h + \mathcal{I}_\epsilon) = 0$ because $h \neq y_U$. If $h \notin M_{-\epsilon}$ then $h = y_V$ for some $V \not\supseteq U$ with $(-1)^{|V|} = \epsilon$. Then (3.4) for V gives

$$y_V \cdot \prod_{p\in V} R_{j_p} = c_V + \sum_{g\in M_{-\epsilon},\, X(g)\supsetneq P-V} a_{g,V} \cdot g, \tag{3.6}$$

where $a_{g,V} \in \mathbb{Z}$ and $c_V + \mathcal{I}_{-\epsilon} \in \mathrm{Tor}(\mathcal{N}_{-\epsilon})$, so $f(c_V + \mathcal{I}_{-\epsilon}) = 0$. Then (3.6) gives $f(y_V + \mathcal{I}_{-\epsilon}) = 0$ as all the other summands on the left hand side belong

to $M_{-\epsilon}$ and are different from y_U. But $h = y_V$ and so again $\tilde{f}(h + \mathcal{I}_\epsilon) = 0$. Then (3.4) and (3.5) imply that $\tilde{f}(c_U + \mathcal{I}_\epsilon) = 1$.

Hence for all $h \in M_\epsilon \cup M_{-\epsilon}$ such that $X(h) \not\subseteq P - U$ we have obtained $\tilde{f}(h + \mathcal{I}_\epsilon) = 0$. If $W \in \mathcal{R}$ and $W \neq U$, then $W \not\supseteq U$ due to the choice of U. Thus (3.4) for W gives

$$y_W \cdot \prod_{p \in W} R_{j_p} = c_W + \sum_{g \in M_\epsilon,\, X(g) \supsetneq P - W} a_{g,W} \cdot g, \tag{3.7}$$

where each summand h on the left hand side satisfies $h \in M_{-\epsilon}$ and $X(h) = P - W \not\subseteq P - U$, and so $\tilde{f}(h + \mathcal{I}_\epsilon) = 0$. Similarly $\tilde{f}(g + \mathcal{I}_\epsilon) = 0$ for each g in the sum on the right hand side of (3.7). Hence $\tilde{f}(c_W + \mathcal{I}_\epsilon) = 0$ and we have

$$\sum_{W \in \mathcal{R}} \tilde{f}(c_W + \mathcal{I}_\epsilon) = \tilde{f}(c_U + \mathcal{I}_\epsilon) = 1,$$

which contradicts our assumption. ∎

4. Circular numbers. This section is devoted to the groups of circular units and circular numbers of an abelian field K of a special type defined below; any cyclotomic field is of this type.

Let P be a finite set of primes linearly ordered by an ordering $\leq$ (not necessarily coinciding with the usual ordering of integers). For each $p \in P$ let K_p be an imaginary abelian field which is ramified only at p, so the conductor of K_p is a power of p, say p^{e_p}. Let $K = \prod_{p \in P} K_p$ be the compositum of these fields, so $m = \prod_{p \in P} p^{e_p}$ is the conductor of K. The absolute Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ is the direct product of its inertia subgroups $G_p \cong \mathrm{Gal}(K_p/\mathbb{Q})$. Each G_p contains a distinguished element j_p of order 2 given in $\mathrm{Gal}(K_p/\mathbb{Q})$ by the complex conjugation. In the same way as in Sections 2 and 3 we enlarge each G_p to a semigroup G_p^* by adding a new element g_p^* and define G^* as the direct product of all the semigroups G_p^*. Set $g^* = \prod_{p \in P} g_p^*$ and $j = \prod_{p \in P} j_p$, so j is the complex conjugation on K.

Let $\mathcal{E}$ and W denote the group of units and the group of roots of unity of K, respectively.

For any non-empty $V \subseteq P$ let $d_V = \prod_{p \in V} p^{e_p}$, $\zeta_V = e^{2\pi i/d_V}$, $K_V = \prod_{p \in V} K_p$, and $\eta_V = \mathrm{N}_{\mathbb{Q}(\zeta_V)/K_V}(1 - \zeta_V)$, so η_V is a unit if and only if $|V| > 1$. We define the group $\mathcal{D}$ of circular numbers of K as the $\mathbb{Z}[G]$-module generated in $K^\times$ by -1 and by all η_V for $V \subseteq P$, $V \neq \emptyset$. Then the Sinnott group $\mathcal{C}$ of circular units of K is defined to be the intersection $\mathcal{C} = \mathcal{D} \cap \mathcal{E}$. It is easy to show that W is the torsion subgroup of both $\mathcal{C}$ and $\mathcal{D}$. (Sinnott [10] in fact used a module different from our $\mathcal{D}$, which however coincides with D' defined by Lettl [8]; the equality $\mathcal{C} = \mathcal{D} \cap \mathcal{E}$ is [8, Proposition 1]. Actually, Lettl used more generators: all conjugates of all

norms $\mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta)\cap K}(1-\zeta)$, where $\zeta = e^{2\pi i/n}$ for an integer $n \mid m$, $n > 1$; but $\mathrm{N}_{\mathbb{Q}(\zeta)/\mathbb{Q}(\zeta)\cap K}(1-\zeta) = \mathrm{N}_{K_V/\mathbb{Q}(\zeta)\cap K}(\eta_V)$ for the set V of all primes dividing n.)

For each $p \in P$ let ν_p be the valuation on K of a fixed prime ideal above p, so $\nu_p(\eta_{\{p\}}) = 1$ and $\nu_p(p) = [K_p : \mathbb{Q}] = |G_p|$.

We define a $\mathbb{Z}[G]$-linear map $\vartheta : \mathbb{Z}[G^*] \to \mathcal{D}$ as follows: $g^* \in \ker\vartheta$ and for each $V \subsetneq P$ let $\vartheta(\prod_{p\in V} g_p^*) = \eta_{P-V}$. This is well-defined by (2.1) because η_{P-V} is fixed by each automorphism in $\prod_{p\in V} G_p$. Let $\pi : \mathcal{D} \to \mathcal{D}^{1+j}$ be defined by $\pi(\varepsilon) = \varepsilon^{1+j}$. It is well-known that $\ker\pi = W$ (see [10, Lemma 4.1(i)]). The map $\pi\circ\vartheta$ is surjective because all generators of $\mathcal{D}^{1+j}$ are in the image. For any distinct $p, q \in P$ we fix $\sigma_{p,q} \in G_q$ in the following way: the action of $\prod_{q\in P-\{p\}} \sigma_{p,q}$ corresponds to the action of $\mathrm{Frob}(p)^{-1}$ on $K_{P-\{p\}}$, where $\mathrm{Frob}(p)$ is the Frobenius automorphism of p.

For any $p \in V \subseteq P$ we have the following well-known norm and mirror relations:

$$\prod_{\sigma\in G_p} \eta_V^\sigma = \begin{cases} \eta_{V-\{p\}}^{1-\mathrm{Frob}(p)^{-1}} & \text{if } V \neq \{p\},\\ p & \text{if } V = \{p\}, \end{cases} \tag{4.1}$$

$$\eta_V^j \equiv \eta_V \pmod{W}. \tag{4.2}$$

We have $\mathcal{D}^{1+j} \cap \mathbb{Q} = \langle P\rangle$ since each number in $\mathcal{D}^{1+j}$ is a totally positive P-unit and because for any $p \in P$ we have

$$\eta_{\{p\}}^{R_{jp}} \in \mathcal{D} \quad\text{and}\quad (\eta_{\{p\}}^{R_{jp}})^{1+j} = \eta_{\{p\}}^{R_{jp}(1+j_p)} = p \tag{4.3}$$

by (2.2) and (4.1).

Let $\psi : \mathcal{D}^{1+j} \to \mathcal{D}^{1+j}/\langle P\rangle$ be the projection to the quotient. We have the following commutative diagram with exact rows and columns (the exactness of the last row is given by the snake lemma):

$$\begin{array}{ccccccccc}
 & & 0 & & 0 & & & & \\
 & & \downarrow & & \downarrow & & & & \\
0 & \longrightarrow & \langle P\rangle & \longrightarrow & \bigoplus_{p\in P} \nu_p(p)\mathbb{Z} & \longrightarrow & 0 & & \\
 & & \downarrow{\scriptstyle\subseteq} & & \downarrow{\scriptstyle\subseteq} & & & & \\
0 & \longrightarrow & \mathcal{C}^{1+j} & \xrightarrow{\subseteq} & \mathcal{D}^{1+j} & \xrightarrow{\bigoplus_{p\in P}\nu_p} & \bigoplus_{p\in P} 2\mathbb{Z} & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow{\scriptstyle\psi} & & \downarrow & & \\
0 & \longrightarrow & \mathcal{C}^{1+j} & \longrightarrow & \mathcal{D}^{1+j}/\langle P\rangle & \longrightarrow & \bigoplus_{p\in P} \mathbb{Z}/\big(\tfrac{1}{2}\nu_p(p)\mathbb{Z}\big) & \longrightarrow & 0 \\
 & & \downarrow & & \downarrow & & \downarrow & & \\
 & & 0 & & 0 & & 0 & &
\end{array}$$

LEMMA 4.1. *The quotient $\mathcal{D}^{1+j}/\langle P\rangle$ has no $\mathbb{Z}$-torsion.*

Proof. Assume that there is $\varepsilon \in \mathcal{D}$ such that $\varepsilon^{1+j} \notin \langle P\rangle$ but for a suitable positive integer n we have $(\varepsilon^{1+j})^n \in \langle P\rangle$. Take ε with the smallest possible n. Then n is a prime. Moreover, using (4.3), we can assume that $(\varepsilon^{1+j})^n$ is a positive integer such that there is $p \in P$ satisfying $p \,|\, (\varepsilon^{1+j})^n$ and $p^2 \nmid (\varepsilon^{1+j})^n$. Since $\varepsilon \in \mathcal{D}$, we have $\varepsilon^{1-j} \in W$, and so there is a root of unity ξ such that $\varepsilon^{1-j} = \xi^2$. Then $\varepsilon\xi^{-1}$, which belongs to an abelian field, is a root of the irreducible polynomial $x^{2n} - (\varepsilon^{1+j})^n \in \mathbb{Z}[x]$. Hence this polynomial has an abelian splitting field, so $2n = 2$, which is a contradiction. ∎

THEOREM 4.2. *The set*

$$\mathcal{B} = \{\vartheta(u);\, u \in M_1,\, u \neq g^*\} \cup \Big\{\vartheta\Big(\prod_{p\in P-\{q\}} g_p^*\Big);\, q \in P\Big\}$$

is a $\mathbb{Z}$-basis of $\mathcal{D}$, i.e. $\pi(\mathcal{B})$ is a basis of the free $\mathbb{Z}$-module $\mathcal{D}^{1+j}$.

Proof. We know that $\operatorname{rank}_{\mathbb{Z}} \mathcal{E} = \frac{1}{2}|G| - 1$ and $\mathcal{C}$ is of finite index in $\mathcal{E}$ (see e.g. [11, §8.2] or [10, Theorem 4.1]). Then the last row of the diagram above gives

$$\operatorname{rank}_{\mathbb{Z}} \mathcal{D}^{1+j}/\langle P\rangle = \operatorname{rank}_{\mathbb{Z}} \mathcal{C}^{1+j} = \operatorname{rank}_{\mathbb{Z}} \mathcal{C} = \tfrac{1}{2}|G| - 1. \tag{4.4}$$

It is enough to show that $\pi(\mathcal{B})$ generates $\mathcal{D}^{1+j}$ because the middle row of the diagram, (4.4), and Lemma 3.1 together with $g^* \in M_1$ give

$$\operatorname{rank}_{\mathbb{Z}} \mathcal{D}^{1+j} = |P| + \tfrac{1}{2}|G| - 1 \geq |\mathcal{B}|.$$

Comparing (2.3) and (2.4) with (4.1) and (4.2) we obtain

$$g^*\mathbb{Z} + \mathcal{I}_1 \subseteq \ker(\psi \circ \pi \circ \vartheta),$$

hence there is a surjective mapping

$$\mathcal{N}_1 \to \mathcal{D}^{1+j}/\langle P\rangle \tag{4.5}$$

induced by $\psi \circ \pi \circ \vartheta$. Theorem 3.6, Lemma 3.1, $g^* \in M_1$, and (4.4) imply that $(\psi \circ \pi \circ \vartheta)(M_1 - \{g^*\})$ is a $\mathbb{Z}$-basis of $\mathcal{D}^{1+j}/\langle P\rangle$. By Lemma 4.1, $\psi(\pi(\mathcal{B}))$ generates $\psi(\mathcal{D}) = \mathcal{D}^{1+j}/\langle P\rangle$, and (4.3) shows that $\pi(\mathcal{B})$ generates $\ker\psi = \langle P\rangle$. ∎

The previous theorem allows us to give a basis of the group $\mathcal{C}$ of circular units. Recall that $X(u) = \{p \in P;\, \pi_p(u) = g_p^*\}$. For any $u \in G^* - \{g^*\}$ we have $\vartheta(u) = \eta^{\sigma}_{P-X(u)}$, where $\sigma = \prod_{p\in P-X(u)} \pi_p(u) \in G$. Define

$$\tilde{\vartheta}(u) = \begin{cases} \vartheta(u) = \eta^{\sigma}_{P-X(u)} & \text{if } |X(u)| < |P| - 1, \\ \vartheta(u - \prod_{p\in X(u)} g_p^*) = \eta^{\sigma^{-1}}_{P-X(u)} & \text{if } |X(u)| = |P| - 1. \end{cases}$$

COROLLARY 4.3. *The set*

$$\tilde{\mathcal{B}} = \{\tilde{\vartheta}(u);\, u \in M_1,\, u \neq g^*\}$$

is a $\mathbb{Z}$-basis of $\mathcal{C}$, i.e. $\pi(\tilde{\mathcal{B}})$ is a basis of the free $\mathbb{Z}$-module $\mathcal{C}^{1+j}$.

Proof. Theorem 4.2 implies that

$$\{\tilde{\vartheta}(u);\, u \in M_1,\, u \neq g^*\} \cup \Big\{\vartheta\Big(\prod_{p\in P-\{q\}} g_p^*\Big);\, q \in P\Big\} \tag{4.6}$$

is a $\mathbb{Z}$-basis of $\mathcal{D}$. For any $q, r \in P$ we have

$$\nu_r\Big(\vartheta\Big(\prod_{p\in P-\{q\}} g_p^*\Big)\Big) = \begin{cases} 1 & \text{if } r = q, \\ 0 & \text{if } r \neq q. \end{cases}$$

The left summand in (4.6) consists of units and so it is a $\mathbb{Z}$-basis of the kernel of $\bigoplus_{p\in P} \nu_p$ in $\mathcal{D}$. ∎

Having the surjective mapping $\pi \circ \vartheta$ we shall describe its kernel to get the following short exact sequence which gives a presentation of $\mathcal{D}^{1+j}$:

$$0 \to \ker(\pi \circ \vartheta) \xrightarrow{\subseteq} \mathbb{Z}[G^*] \xrightarrow{\pi\circ\vartheta} \mathcal{D}^{1+j} \to 0. \tag{4.7}$$

Write the module $\mathcal{I}_1$ as the sum $\mathcal{I}_2 + \mathcal{I}_3$ where $\mathcal{I}_2$ is the $\mathbb{Z}[G]$-module generated by the generators (2.3) for all $p \in P$ and $V = P - \{p\}$, and $\mathcal{I}_3$ is the $\mathbb{Z}[G]$-module generated by all the other generators (2.3) and by all the generators (2.4) with $\epsilon = 1$. So $\mathcal{I}_2 + \mathcal{I}_3 = \mathcal{I}_1$ and

$$\mathcal{I}_2 = \Big\langle \Big\{ S(G_p) \cdot \textstyle\prod_{q\in P-\{p\}} g_q^*;\, p \in P \Big\} \Big\rangle \tag{4.8}$$

is a $\mathbb{Z}[G]$-module with the trivial action of G.

Using (4.1) we see that $\ker \vartheta$ contains all elements (2.3) for $|V| < |P|-1$. The identity $(1+j)(1-j) = 0$ shows that $\ker(\pi \circ \vartheta)$ contains all elements (2.4) with $\varepsilon = 1$, hence $\mathcal{I}_3 \subseteq \ker(\pi \circ \vartheta)$. We shall need the following stronger variant of Theorem 2.2:

PROPOSITION 4.4. *For each $Q \subseteq P$ satisfying $(-1)^{|Q|} = -1$ and $|Q| > 1$ there is $\alpha_Q \in \mathbb{Z}[G'_Q]$ such that*

$$2\alpha_Q - 2\Big(\prod_{q\in P-Q} g_q^*\Big) \prod_{p\in Q} R_{j_p} \in \mathcal{I}_3.$$

Proof. Since $\mathcal{I}_2 + \mathcal{I}_3 = \mathcal{I}_1$, Theorem 2.2 and (4.8) give

$$2\Big(\prod_{q\in P-Q} g_q^*\Big) \prod_{p\in Q} R_{j_p} - \sum_{p\in P} a_p S(G_p) \cdot \prod_{q\in P-\{p\}} g_q^* \in 2\mathbb{Z}[G'_Q] + \mathcal{I}_3 \tag{4.9}$$

for suitable integers a_p. For any $p \in Q$, (2.2) implies

$$S(G_p) \cdot \prod_{q\in P-\{p\}} g_q^* = \big(2j_p R_{j_p} + (1-j_p) R_{j_p}\big) \cdot \prod_{q\in P-\{p\}} g_q^* \in 2\mathbb{Z}[G'_Q] + \mathcal{I}_3,$$

and so we can assume that $a_p = 0$. Fix $r \in P - Q$. For any element of $\mathbb{Z}[G'_Q]$ we see that the coefficient of $\prod_{P-\{r\}} g_q^*$ is zero. The same holds true for the product of $S(G_r)$ and any generator of $\mathcal{I}_3$. Hence (4.9) shows that this coefficient is zero also for

$$S(G_r) \cdot \sum_{p\in P} a_p S(G_p) \cdot \prod_{q\in P-\{p\}} g_q^* = \sum_{p\in P} |G_r| \cdot a_p S(G_p) \cdot \prod_{q\in P-\{p\}} g_q^*,$$

and so $a_r = 0$. The proposition follows. ∎

THEOREM 4.5. *The kernel* $\ker(\pi \circ \vartheta)$ *in the presentation* (4.7) *of* $\mathcal{D}^{1+j}$ *is generated, as a* $\mathbb{Z}$*-module, by* $\mathcal{I}_3$*, by* g^**, and by the elements*

$$\beta_Q = \alpha_Q - \Big(\prod_{q\in P-Q} g_q^*\Big) \prod_{p\in Q} R_{j_p}$$

for all $Q \subseteq P$ *with odd* $|Q| > 1$*, where* α_Q *is introduced in Proposition* 4.4.

Proof. Since $\mathcal{D}^{1+j}$ has no $\mathbb{Z}$-torsion, Proposition 4.4 and (4.7) imply that

$$B = \{\beta_Q;\, Q \subseteq P,\, |Q| > 1,\, (-1)^{|Q|} = -1\} \subseteq \ker(\pi \circ \vartheta).$$

Since the image of $(M_1 - \{g^*\}) \cup \{\prod_{q\in P-Q} g_q^*;\, p \in P\}$ in $\pi \circ \vartheta$ is a $\mathbb{Z}$-basis of $\mathcal{D}^{1+j}$ due to Theorem 4.2, to prove $\ker(\pi \circ \vartheta) \subseteq \mathcal{I}_3 + \langle B \cup \{g^*\}\rangle_{\mathbb{Z}}$ it is enough to show that

$$\mathbb{Z}[G^*] = \Big\langle M_1 \cup \Big\{\prod_{q\in P-\{p\}} g_q^*;\, p \in P\Big\}\Big\rangle_{\mathbb{Z}} + \mathcal{I}_3 + \langle B\rangle_{\mathbb{Z}}. \tag{4.10}$$

This can be proven exactly in the same way as Lemma 3.2, changing $\mathcal{I}_1$ to $\mathcal{I}_3$: let us go through the four cases discussed in the proof of Lemma 3.2 to see where the generators of $\mathcal{I}_2$ have been used.

1. The element in (3.1) does not belong to $\mathcal{I}_3$ only if $X(h) = P - \{p\}$. Then the other assumptions of this case give $W(h) = \emptyset$ and $V(h) = \emptyset$, a contradiction.

2. The element of $\mathcal{I}_1$ used here belongs to $\mathcal{I}_3$.

3. The element in (3.2) belongs to B unless $U(h) = \{p\}$ and $h = \prod_{q\in P-\{p\}} g_q^*$, but this h appears in (4.10).

4. The element in (3.1) does not belong to $\mathcal{I}_3$ only if $X(h) = P - \{p\}$. Then $V(h) = \{p\}$ and $h = j_p \prod_{q\in P-\{p\}} g_q^*$, so we can use $(1 - j_p)h \in \mathcal{I}_3$ since $j_p h$ appears in (4.10).

We have proved (4.10) and the theorem follows. ∎

5. Galois descent. The aim of this section is to prove the following result concerning an extension K/L of two fields satisfying the assumptions of Section 4. We shall use the previous notation just adding the appropriate

field as index, for example $\mathcal{C}_K$ and $\mathcal{C}_L$ mean the groups of circular units in K and L, respectively. The following Galois descent property has been proven for full cyclotomic fields by Gold and Kim [3].

THEOREM 5.1. *Let $L \subseteq K$ be abelian fields, each being a compositum of imaginary abelian fields ramified at one prime, i.e. $K = \prod_{p\in P_K} K_p$ and $L = \prod_{p\in P_L} L_p$, where K_p for any $p \in P_K$ and L_p for any $p \in P_L$ are imaginary abelian fields ramified only at p. Then $\mathcal{C}_L = \mathcal{C}_K \cap L$.*

Proof. It is easy to see that $\mathcal{C}_L \subseteq \mathcal{C}_K \cap L$, so we need to show the other inclusion.

We can assume that either $P_K - P_L = \{q\}$, or $P_K = P_L$ and $[K : L]$ is a prime. Indeed, after having proven these two special cases the general statement can be easily obtained by induction.

In the former case $K = LK_q$ we immediately see from the definitions that $\tilde{\vartheta}_L(u) = \tilde{\vartheta}_K(ug_q^*)$ for any $u \in G_L^*$ and $\{ug_q^*;\, u \in M_{1,L}\} \subseteq M_{1,K}$. For any $\varepsilon \in \mathcal{C}_K \cap L$ we have $\varepsilon^{[K:L]} = \mathrm{N}_{K/L}(\varepsilon) \in \mathcal{C}_L$. Corollary 4.3 for L says that there are unique $\xi \in W_L$ and $a_u \in \mathbb{Z}$ satisfying

$$\varepsilon^{[K:L]} = \xi \cdot \prod_{\substack{u\in M_{1,L}\\ u\neq g_L^*}} \tilde{\vartheta}_L(u)^{a_u} = \xi \cdot \prod_{\substack{u\in M_{1,L}\\ u\neq g_L^*}} \tilde{\vartheta}_K(ug_q^*)^{a_u}.$$

Since $\varepsilon \in \mathcal{C}_K$, Corollary 4.3 for K implies that $[K : L]$ divides a_u for each u and so there is $\xi' \in W_L$ such that

$$\varepsilon = \xi' \cdot \prod_{\substack{u\in M_{1,L}\\ u\neq g_L^*}} \tilde{\vartheta}_L(u)^{a_u/[K:L]}.$$

Hence $\varepsilon \in \mathcal{C}_L$ and the theorem follows in this case.

To finish the proof we need to show $\mathcal{C}_K \cap L \subseteq \mathcal{C}_L$ when $P_K = P_L$ and $[K : L]$ is a prime. It is enough to show that $\mathcal{D}_K \cap L \subseteq \mathcal{D}_L$. Set $H = \mathrm{Gal}(K/L)$ and $P = P_K$. Our assumption on K, L implies that there is a unique $q \in P$ such that $K_q \neq L_q$. Then $j_{q,K} \notin H \subset G_{q,K}$ and $G_{q,L} \cong G_{q,K}/H$.

We extend the restriction $\mathrm{res}_{K/L} : G_K \to G_L$ to a semigroup homomorphism $\mathrm{res}_{K/L} : G_K^* \to G_L^*$ by setting $\mathrm{res}_{K/L}\, g_{p,K}^* = g_{p,L}^*$ for each $p \in P$. On the one hand, if $[K : L]$ is odd then the construction in Lemma 1.1 gives $\mathrm{res}_{K/L}\, T_{q,K} = T_{q,L}$. On the other hand, if $[K : L] = 2$ then defining τ by $H = \{1, \tau\}$ we see that τ and $j_{q,K}$ are different elements of $G_{q,K}$ of order 2. In Lemma 1.1, the 2-Sylow subgroup of $G_{q,K}$ is written as the direct product $\langle z\rangle \times \bar{H}$, where $j_{q,K}$ is the only element of order 2 in $\langle z\rangle$ and $\bar{H}$ is a suitable subgroup. Then either $\tau \in \bar{H}$ when again $\mathrm{res}_{K/L}\, T_{q,K} = T_{q,L}$, or $\tau \notin \bar{H}$ when $j_{q,K}\tau \in \bar{H}$, which implies $\mathrm{res}_{K/L}\, T_{q,K} = G_{q,L}$.

Since we can choose any linear ordering $\leq$ on P, we can assume that q is the least element of P with respect to $\leq$. For any $u \in G_K^*$ we have

$$\vartheta_L(\mathrm{res}_{K/L}\, u) = \begin{cases} \vartheta_K(u) & \text{if } \pi_{q,K}(u) = g_{q,K}^*, \\ \prod_{h\in H} \vartheta_K(hu) & \text{if } \pi_{q,K}(u) \neq g_{q,K}^*. \end{cases} \tag{5.1}$$

Let

$$M_{1,L}^+ = (M_{1,L} - \{g_L^*\}) \cup \Big\{ \prod_{q\in P-\{p\}} g_{q,L}^*;\ p \in P \Big\}$$

be the set giving the $\mathbb{Z}$-basis of $\mathcal{D}_L$ described by Theorem 4.2, and let $M_{1,K}^+$ be defined similarly. Recall that, before Lemma 3.2, we have defined the ordering $\preceq$ on G_K^*. We shall prove that for each $h \in M_{1,L}^+$ we can choose $k_h \in M_{1,K}^+$ such that $\mathrm{res}_{K/L}\, k_h = h$ and

$$\vartheta_L(h) = \xi \cdot \vartheta_K(k_h) \cdot \rho_h, \tag{5.2}$$

where $\xi \in W_K$ and ρ_h is a multiplicative combination with integral coefficients of $\vartheta_K(l)$ for those $l \in M_{1,K}^+$, $l \neq k_h$, which satisfy either $l \prec k_h$ or $\mathrm{res}_{K/L}\, l = h$ or $\mathrm{res}_{K/L}\, l = j_{q,L}h$, the last case being possible only if $j_{q,L}h \notin M_{1,L}^+$. To prove (5.2) let us distinguish the following four cases:

1. Suppose $\pi_{q,L}(h) = g_{q,L}^*$. There is a unique $k_h \in G_K^*$ such that $\mathrm{res}_{K/L}\, k_h = h$. This k_h is in $M_{1,K}^+$ and (5.1) gives $\vartheta_L(h) = \vartheta_K(k_h)$.

2. Suppose $\pi_{q,L}(h) = 1$. We have exactly $[K : L]$ elements $k \in G_K^*$ satisfying $\mathrm{res}_{K/L}\, k = h$; we denote by k_h the only one of them with $\pi_{q,K}(k_h) = 1$. Then $k_h \in M_{1,K}^+$ and the other k satisfy $X(k) = X(h)$ and $W(k) = W(h) - \{q\}$ since $j_{q,K} \notin H$, and so $k \prec k_h$. Using (4.5) and reasoning as in the proof of Proposition 3.3 we see that (5.1) implies (5.2).

3. Suppose $\pi_{q,L}(h) \notin \{1, g_{q,L}^*\}$ and $c(h) \neq q$. Again we have exactly $[K : L]$ elements $k \in G_K^*$ satisfying $\mathrm{res}_{K/L}\, k = h$. For each of them we have $X(k) = X(h)$, $W(k) = W(h)$, so $c(k) = c(h) \neq q$. And since $\pi_{q,K}(k) \neq j_{q,K}$, we obtain $k \in M_{1,K}^+$. Choosing any of these k as k_h, we find that (5.1) implies (5.2).

4. Suppose $\pi_{q,L}(h) \notin \{1, g_{q,L}^*\}$ and $c(h) = q$. Then $X(h) \cup W(h) = P - \{q\}$ as q was chosen to be the least element of P and $j_{q,L}h \notin M_{1,L}^+$. Again we have exactly $[K : L]$ elements $k \in G_K^*$ satisfying $\mathrm{res}_{K/L}\, k = h$. For each of them we have $X(k) = X(h)$, $W(k) = W(h)$, $c(k) = c(h) = q$, and $V(k) = V(h) = \emptyset$. Since $\mathrm{res}_{K/L}\, T_{q,K}$ is either $T_{q,L}$ or $G_{q,L}$, for at least one of these k's we have $\pi_{q,K}(k) \in T_{q,K}$. Each such k belongs to $M_{1,K}^+$; we choose k_h to be one of them. Now consider any $k \in G_K^*$ satisfying $\mathrm{res}_{K/L}\, k = h$ and $\pi_{q,K}(k) \notin T_{q,K}$. Then $j_{q,K}k \in M_{1,K}^+$. Relation (4.2) gives $\vartheta_K(j_K k) \equiv \vartheta_K(k) \pmod{W_K}$. On the one hand, if $W(h) = \emptyset$ then $j_K k = j_{q,K} k$. On the other hand, if we fix any $p \in W(h)$ and set $R = \{r \in W(h);\ r < p\}$ then (4.1)

gives the following relation for $t = k \cdot \prod_{r\in R\cup\{q\}} j_{r,K}$:

$$\prod_{u\in G_{p,K}} \vartheta_K(ut) = \vartheta_K(g^*_{p,K}t)\cdot \vartheta_K(\mathrm{Frob}(p)^{-1}g^*_{p,K}t)^{-1}. \tag{5.3}$$

As $X(g^*_{p,K}t) = X(\mathrm{Frob}(p)^{-1}g^*_{p,K}t) = X(k_h)\cup\{p\}$, we have $g^*_{p,K}t \prec k_h$ and $\mathrm{Frob}(p)^{-1}g^*_{p,K}t \prec k_h$. If $u \in G_{p,K} - \{1, j_{p,K}\}$ then $X(ut) = X(k_h)$ and $W(ut) \subsetneq W(k_h)$, so $ut \prec k_h$. Hence (5.3) implies that $\vartheta_K(t)\vartheta_K(j_{p,K}t)$ is a multiplicative combination of $\vartheta_K(l)$ with $l \prec k_h$. As this holds for all $p \in W(h)$, we deduce that $\vartheta_K(j_K k)\cdot\vartheta_K(j_{q,K}k)^{\pm1}$ is such a multiplicative combination. Using (4.5) and reasoning as in the proof of Proposition 3.3, we see again that (5.1) implies (5.2).

We have proven (5.2) since each h satisfies exactly one of the previous cases. But the previous construction shows even more: we have $X(k_h) = X(h)$, $U(k_h) = U(h)$, $V(k_h) = \emptyset = V(h)$, and $z(k_h) = z(h)$, therefore for any $h_1, h_2 \in M^+_{1,L}$ we have

$$h_1 \prec h_2 \;\Leftrightarrow\; k_{h_1} \prec k_{h_2}. \tag{5.4}$$

For any $\varepsilon \in \mathcal{D}_K \cap L$ we have $\varepsilon^{[K:L]} = \mathrm{N}_{K/L}(\varepsilon) \in \mathcal{D}_L$. By Theorem 4.2 for L there are unique $\xi \in W_L$ and $a_h \in \mathbb{Z}$ satisfying

$$\varepsilon^{[K:L]} = \xi \cdot \prod_{h\in M^+_{1,L}} \vartheta_L(h)^{a_h}. \tag{5.5}$$

As above, we need to show that $[K : L]$ divides a_h for each $h \in M^+_{1,L}$. Assume the contrary, and among those $h \in M^+_{1,L}$ satisfying $[K : L] \nmid a_h$ choose a maximal h_0 with respect to $\preceq$. Hence $[K : L] \nmid a_{h_0}$, and $[K : L] \mid a_h$ for each $h \in M^+_{1,L}$ with $h \succ h_0$. Using (5.2) we obtain

$$\varepsilon^{[K:L]} = \xi' \cdot \prod_{h\in M^+_{1,L}} (\vartheta_K(k_h)\cdot\rho_h)^{a_h} \tag{5.6}$$

for a suitable $\xi' \in W_K$. Let us study the total exponent of $\vartheta_K(k_{h_0})$ appearing in the expression of the right hand side of (5.6) in the basis of Theorem 4.2. The exponent a_{h_0} is obtained for $h = h_0$. Assume that we have a power of $\vartheta_K(k_{h_0})$ coming from ρ_h for some $h \in M^+_{1,K}$, $h \neq h_0$. By the description of ρ_h this means that either $k_{h_0} \prec k_h$ or $\mathrm{res}_{K/L}\, k_{h_0} = h$ or $\mathrm{res}_{K/L}\, k_{h_0} = j_{q,L}h$, the last case being possible only if $j_{q,L}h \notin M^+_{1,L}$. But $\mathrm{res}_{K/L}\, k_{h_0} = h_0$, so $h_0 \prec h$ in view of (5.4), because the other two cases lead to a contradiction: $h_0 = h$ or $h_0 = j_{q,L}h \notin M^+_{1,L}$. Our choice of h_0 then gives $[K : L] \mid a_h$. Therefore the total exponent of $\vartheta_K(k_{h_0})$ appearing on the right hand side of (5.6) is not divisible by $[K : L]$, and (5.6) contradicts Theorem 4.2 for K. This shows that all the exponents a_h in (5.5) are divisible by $[K : L]$ and so $\varepsilon \in \mathcal{D}_L$. ∎

6. The Stickelberger ideal. Let K denote the field considered in Section 4. We shall keep the notation introduced there, so for example $G = \mathrm{Gal}(K/\mathbb{Q})$ and $j \in G$ is the complex conjugation. The Stickelberger ideal of K is the intersection $\mathcal{S} = \mathbb{Z}[G] \cap \mathcal{S}'$ where $\mathcal{S}' \subset \mathbb{Q}[G]$ is defined by means of explicit generators in [10, p. 189]. Letting $e^- = \frac{1}{2}(1-j)$, we have $\mathcal{S}' = e^-\mathcal{S}' \oplus \frac{1}{2}S(G)\mathbb{Z}$ and $e^-\mathcal{S}' = \omega e^- U'$ (see [10, Lemma 2.1 and Corollary of Proposition 2.2]), where $\omega \in \mathbb{Q}[G]$ is defined by [10, (2.6)] and U' (denoted by U in [10]) has the same meaning as in Section 3. Hence we have

LEMMA 6.1. $\mathcal{S}' = \frac{1}{2}\omega(1-j)U' \oplus \frac{1}{2}S(G)\mathbb{Z}$.

Lemma 3.5 states that $U' \cong \mathcal{N}_0$ and so $(1-j)U' \cong (1-j)\mathcal{N}_0$. Since $(1-j)\mathbb{Z}[G] \subseteq \mathcal{I}_1$ and $(1+j)\mathbb{Z}[G] \subseteq \mathcal{I}_{-1}$, the injective linear map δ defined in Lemma 3.5 satisfies $\delta((1-j)(\alpha+\mathcal{I}_0)) = (0, 2(\alpha+\mathcal{I}_{-1}))$ for any $\alpha \in \mathbb{Z}[G^*]$. Therefore the restriction of δ to $(1-j)\mathcal{N}_0$ together with Theorem 3.6 gives the following isomorphism of $\mathbb{Z}[G]$-modules:

$$(1-j)U' \cong (1-j)\mathcal{N}_0 \cong 2\mathcal{N}_{-1} \cong \mathcal{N}_{-1}/\mathrm{Tor}(\mathcal{N}_{-1}).$$

Let $\psi : \mathcal{N}_{-1}/\mathrm{Tor}(\mathcal{N}_{-1}) \to (1-j)U'$ denote this isomorphism and let $\pi : \mathbb{Z}[G^*] \to \mathcal{N}_{-1}/\mathrm{Tor}(\mathcal{N}_{-1})$ be the projection to the quotient. Theorem 3.6 implies that $\psi(\pi(M_{-1}))$ is a basis of the free $\mathbb{Z}$-module $(1-j)U'$. Therefore

$$\mathcal{B} = \{\tfrac{1}{2}\omega \cdot \psi(\pi(u));\ u \in M_{-1}\} \cup \{\tfrac{1}{2}S(G)\} \tag{6.1}$$

is a system of generators of $\mathcal{S}'$. It is well-known that $\mathrm{rank}_{\mathbb{Z}}\,\mathcal{S}' = 1 + \frac{1}{2}|G| = |\mathcal{B}|$ (see [10, Theorem 2.1]). Hence we have

THEOREM 6.2. *The set $\mathcal{B}$ defined by* (6.1) *is a basis of the free $\mathbb{Z}$-module $\mathcal{S}'$.*

The previous theorem describes a basis of $\mathcal{S}'$, but we would like to get a basis of $\mathcal{S}$. It is easy to derive such a basis from $\mathcal{B}$, but a formal description is quite cumbersome. So we only outline this procedure.

We know that there is a surjective $\mathbb{Z}[G]$-linear map $\varphi : \mathcal{S}' \to W$, where W is the group of roots of unity in K, defined as follows: for any $\theta \in \mathcal{S}'$ we have $\varphi(\theta) = e^{2\pi i a_1}$, where a_1 is the coefficient of $1 \in G$ in $\theta = \sum_{\sigma\in G} a_\sigma \sigma^{-1}$. The kernel of φ is $\mathcal{S}$, so $\mathcal{S}'/\mathcal{S} \cong W$ (see [10, Proposition 2.2]).

We can decompose the cyclic group W into the direct product of cyclic p-groups for primes $p \,|\, |W|$ (those p are in $P \cup \{2\}$). Let W_1 denote the first of those factors. Theorem 6.2 implies that we can fix $b \in \mathcal{B}$ such that the projection of $\varphi(b)$ to W_1 is a generator of W_1. By adding a suitable multiple of b to any other element of $\mathcal{B}$ (and keeping b unchanged) we can modify the basis $\mathcal{B}$ to another basis of $\mathcal{S}'$ each of whose elements except b has trivial projection to W_1 of its φ-image. Then we change b to $|W_1| \cdot b$ to obtain a basis of a subideal $\mathcal{S}_1 \subseteq \mathcal{S}$ which is the kernel of the composition of φ with

the projection to W_1. Continuing this procedure for each factor of W (so at most $|P|+1$ times) we arrive at a basis of $\mathcal{S}$.

Acknowledgments. The author thanks the anonymous referee for very useful remarks. This research was supported under Project P201/11/0276 of the Czech Science Foundation.

References

[1] M. Conrad, *Construction of bases for the group of cyclotomic units*, J. Number Theory 81 (2000), 1–15.
[2] V. Ennola, *On relations between cyclotomic units*, J. Number Theory 4 (1972), 236–247.
[3] R. Gold and J. Kim, *Bases for cyclotomic units*, Compos. Math. 71 (1989), 13–27.
[4] C. Greither and R. Kučera, *Linear forms on Sinnott's module*, J. Number Theory 141 (2014), 324–342.
[5] J. M. Kim and J. Ryu, *A note on Ennola relation*, Taiwanese J. Math. 18 (2014), 1653–1661.
[6] R. Kučera, *On bases of odd and even universal ordinary distributions*, J. Number Theory 40 (1992), 264–283.
[7] R. Kučera, *On bases of the Stickelberger ideal and of the group of circular units of a cyclotomic field*, J. Number Theory 40 (1992), 284–316.
[8] G. Lettl, *A note on Thaine's circular units*, J. Number Theory 35 (1990), 224–226.
[9] C. G. Schmidt, *Die Relationenfaktorgruppen von Stickelberger Elementen und Kreiszahlen*, J. Reine Angew. Math. 315 (1980), 60–72.
[10] W. Sinnott, *On the Stickelberger ideal and the circular units of an abelian field*, Invent. Math. 62 (1980), 181–234.
[11] L. Washington, *Introduction to Cyclotomic Fields*, Grad. Texts in Math. 83, Springer, New York, 1997.
[12] K. Yamamoto, *The gap group of multiplicative relationships of Gaussian sums*, in: Symposia Math. 15, Academic Press, London, 1975, 427–440.

Radan Kučera
Department of Mathematics and Statistics
Faculty of Science
Masaryk University
Kotlářská 2
611 37 Brno, Czech Republic
E-mail: kucera@math.muni.cz