Linear forms on Sinnott's module

Cornelius Greither [a], Radan Kučera [b,*,1]

[a] *Institut für Theoretische Informatik, Mathematik und OR, Fakultät für Informatik, Universität der Bundeswehr München, 85577 Neubiberg, Germany*
[b] *Faculty of Science, Masaryk University, 611 37 Brno, Czech Republic*

A R T I C L E   I N F O

A B S T R A C T

This paper proves a result concerning linear forms on the Sinnott module. This is perhaps of intrinsic interest, and it is needed in another paper of the same authors. We obtain a congruence which can be interpreted as a strengthening of a congruence of Anthony Hayward.

© 2014 Elsevier Inc. All rights reserved.

0. Introduction

We shall study $\mathbb{Z}[G]$-linear forms on a modified Sinnott module U defined in [11]. The Sinnott module U can be defined in abstract terms, only using the Galois group G, the inertia subgroups T_i and Frobenius elements, without referring to a concrete abelian number field. It is fundamental in the study of units and of the Stickelberger ideal as it describes the algebraic aspects of these modules while the arithmetical aspects are governed by values of L-functions. Even though the Sinnott module has a difficult

* Corresponding author.
 E-mail addresses: cornelius.greither@unibw.de (C. Greither), kucera@math.muni.cz (R. Kučera).

structure, it is useful since it is completely explicit and allows to understand the structure of the original module.

We should explain why linear forms are important in the subject. On the one hand they appear explicitly in the statement of the Rubin–Stark conjectures where they measure the integrality of the Stark unit. On the other hand they can be used to prove divisibility of elements in a module of Stark units by an element of the group ring (see [5]), for the simple reason that linear forms transfer the divisibility question from the module to the group ring itself, making it much easier.

The main motivation to write this paper was the fact that we need its main result in [6], in order to be able to extract some nontrivial roots of circular units which are necessary for the arithmetical problem considered in that paper. But we also think that the result offers some interest on its own.

Let us conclude this short introduction by giving a little background and discussing related research. If we set our group G to be equal to the absolute Galois group of the n-th cyclotomic field $\mathbb{Q}(\zeta_n)$ (and the subgroups T_i correspond to inertia subgroups and the elements λ_i correspond to the Frobenius automorphisms of ramified primes) then our modules $(1+j)U'$ and $(1+j)U$, where j means the complex conjugation, are not identical to, but closely related to certain modules called the universal even distribution A_n^+ and the universal punctured even distribution $(A_n^0)^+$, for the definitions see §12.3 of [13]. The importance of $(A_n^0)^+$ is that this module comes with a canonical surjection to the group of circular numbers (modulo roots of unity) of $\mathbb{Q}(\zeta_n)$. An unpublished conjecture of Milnor stated that this surjection is an isomorphism modulo torsion. This conjecture was in fact proven by Bass [1]; Ennola [4] found later on that the (torsion) kernel may be a nontrivial 2-elementary finite group.

A very important contribution is due to Sinnott [10], who in contrast with Bass and Ennola did not use A_n^+, which is a quotient of free group modulo the obvious relations, but introduced instead a new module U (corresponding to U' in the setting of this paper) which is a submodule of the rational group ring $\mathbb{Q}[G]$. In the subsequent paper [11] he generalized the construction of U to any abelian number field. Going a step further, Solomon [12] has found a system of generators and relations of several different groups of circular units and circular numbers of any abelian number field as a Galois module, showing that the quotient of the group of all relations modulo the subgroup of obvious relations is always finite. There is also an extension into a different direction: Yin in [14] generalized the notion of distributions to ray class fields over any global field. An analog of Sinnott's module U for an abelian extension of an imaginary quadratic field is studied by Oukhaba [9], and in a more general setting by Belliard and Oukhaba [2].

After this very brief tour of work on explicit modules that are "close" to groups of circular numbers and units, let us come back to our own situation. Starting with an abelian number field K, which is its own genus field in narrow sense, we consider the module U which maps surjectively to the group of circular numbers of this field modulo roots of unity, the top generator of U being mapped to the circular number $\eta \in K$ of the conductor level. Then we study the image of this top generator in any equivariant

linear map to the group ring $\mathbb{Z}[G]$, where $G = \operatorname{Gal}(K/\mathbb{Q})$. The knowledge of the possible *images* of this top generator of U under all these maps can then be used, for a suitable subfield L of K, to construct a nontrivial root of $N_{K/L}(\eta)$ in K which turns out to be useful in applications (see [6] and [7]). We are not aware of earlier work in this direction, besides Proposition 5.5 in [8] (see our comments comparing this proposition with our results in Remarks 1.2 and 4.2).

We would like to thank the referee, who encouraged us to include a little more information on background and context and provided precious suggestions as to what we might say in this respect.

1. The Sinnott modules U' and U

As mentioned in the introduction, the structure of the Sinnott module is very complicated in general. It is defined in [11] for any abelian field K, so there is a possibility to study Sinnott's module assuming only that $G = \operatorname{Gal}(K/\mathbb{Q})$ is a quotient of the direct product $T_1 \times \cdots \times T_v$, where the T_i are the inertia groups of ramified primes. But in this paper we shall assume that G equals this direct product, in other words that K is equal to its genus field in the narrow sense. Nevertheless Corollary 1.7 gives a result which can be useful for any abelian field whose genus field is K.

In fact, no field K will appear explicitly in this paper, since our approach is entirely algebraic. We describe the Sinnott module U' and the modified Sinnott module U in an abstract way as follows:

Let $T_1, \ldots, T_v$ be finite abelian groups written multiplicatively, $v \geqslant 1$, and let

$$G = T_1 \times \cdots \times T_v$$

be their direct product. For any $N \subseteq I = \{1, \ldots, v\}$ let $T_N = \prod_{i \in N} T_i \subseteq G$, so $T_I = G$ and $T_\emptyset = \{1\}$ by definition. For any $i \in I$ we fix some element $\lambda_i \in T_{I-\{i\}}$, denote $t_i = |T_i|$, and define

$$I_i = \ker\big(\mathbb{Z}[G] \to \mathbb{Z}\big[G/\langle \lambda_i, T_i \rangle\big]\big),$$

the ideal of $\mathbb{Z}[G]$ generated by $1 - \lambda_i$ and $1 - g$ for all $g \in T_i$. Let $e_1, \ldots, e_v$ be the usual basis of the $\mathbb{Z}[G]$-module $\mathbb{Z}^v$ which has trivial action of G, i.e. e_i is the v-tuple having all zeros but one 1 in the i-th position. For any $H \subseteq G$ let $s(H) = \sum_{h \in H} h \in \mathbb{Z}[G]$ and for any $N \subseteq I$ define $\rho_N \in \mathbb{Q}[G] \oplus \mathbb{Z}^v$ as follows

$$\rho_N = \begin{cases} s(T_N) \cdot \prod_{i \in I-N}(1 - t_i^{-1} \lambda_i^{-1} s(T_i)), & \text{if } |I - N| \neq 1, \\ s(T_N) \cdot (1 - t_j^{-1} \lambda_j^{-1} s(T_j)) + e_j, & \text{if } I - N = \{j\}. \end{cases}$$

Note that $\rho_N = s(T_N) \cdot (1 - t_j^{-1} s(T_j)) + e_j$ if $I - N = \{j\}$. The modified Sinnott module U is defined as the $\mathbb{Z}[G]$-submodule of $\mathbb{Q}[G] \oplus \mathbb{Z}^v$ generated by all ρ_N, $N \subseteq I$.

We have the projection to the first coordinate $\pi : \mathbb{Q}[G] \oplus \mathbb{Z}^v \to \mathbb{Q}[G]$; we define the Sinnott module U' by $U' = \pi(U)$. In explicit terms, U' is the $\mathbb{Z}[G]$-submodule of $\mathbb{Q}[G]$ generated by ρ'_N for all $N \subseteq I$, where

$$\rho'_N = \pi(\rho_N) = s(T_N) \cdot \prod_{i \in I-N} \left(1 - t_i^{-1}\lambda_i^{-1}s(T_i)\right) \in \mathbb{Q}[G]. \tag{1.1}$$

We remark that our module U' corresponds to U in Sinnott's notation in [11].

For each $i \in I$ we define the projection $\mathrm{pr}_i : G \to T_i$ by the condition $g = \prod_{i=1}^v \mathrm{pr}_i(g)$ for each $g \in G$. For each $i, j \in I$ let $g_{ij} = \mathrm{pr}_i(\lambda_j)$, then $g_{ij} \in T_i$, $g_{jj} = 1$ and

$$\lambda_j = \prod_{i \in I} g_{ij}. \tag{1.2}$$

We are going to prove the following

Theorem 1.1.

(i) *Every $\psi \in \mathrm{Hom}_{\mathbb{Z}[G]}(U', \mathbb{Z}[G])$ satisfies $\psi(\rho'_\emptyset) \in \prod_{i=1}^v I_i$.*
(ii) *Every $\psi \in \mathrm{Hom}_{\mathbb{Z}[G]}(U, \mathbb{Z}[G])$ satisfies*

$$\psi(\rho_\emptyset) \equiv \sum_{j=1}^v c_j \psi^1(t_j e_j) \quad \left(\mathrm{mod} \prod_{i=1}^v I_i\right), \tag{1.3}$$

where $\psi^1(t_j e_j) \in \mathbb{Z}$ is determined by $\psi(t_j e_j) = \psi^1(t_j e_j)s(G)$ and

$$c_j \in \prod_{i \in I-\{j\}} I_i \subseteq \mathbb{Z}[G].$$

More precisely, if $v = 1$ then $c_1 = 1$, and if $v > 1$ then

$$c_j = \sum_{\emptyset=R_0 \subsetneq R_1 \subsetneq \cdots \subsetneq R_r=I-\{j\}} (-1)^{r+v-1} \cdot \prod_{c=1}^r \prod_{k \in R_c - R_{c-1}} \left(1 - \lambda_k^{-1} \prod_{i \in R_c} g_{ki}\right)$$

$$= \sum_{\emptyset=R_0 \subsetneq R_1 \subsetneq \cdots \subsetneq R_r=I-\{j\}} (-1)^{r+v-1} \cdot \prod_{c=1}^r \prod_{k \in R_c - R_{c-1}} \left(1 - \lambda_k^{-1} \prod_{i \in R_c} g_{ik}\right).$$

The first part of the previous theorem is a kind of divisibility statement, and we repeat that we use it in [6] to obtain divisibility statements for circular units.

Remark 1.2. Formula (1.3) in Theorem 1.1(ii) looks very similar to the formula in Proposition 5.5 of [8]. But in fact we prove a sharper congruence for a wider class of linear forms, since our modulus $\prod_{i=1}^v I_i$ is usually smaller than Hayward's. Our terms c_i are

not identical to Hayward's terms A_i^B. Indeed, in Section 4 we explain the exact relationship between Hayward's result and ours, which can in fact be seen as a strengthening. Our modulus is more closely related to the modulus $I_H^{S,T}$ defined by Burns in [3] by formula (8) and used in his main result Theorem 3.1, but still $I_H^{S,T}$ is in general bigger than our modulus.

Remark 1.3. Let us show that part (i) of Theorem 1.1 is optimal in the following sense: for any $x \in \prod_{i=1}^{v} I_i$ there is $\psi \in \mathrm{Hom}_{\mathbb{Z}[G]}(U', \mathbb{Z}[G])$ satisfying $\psi(\rho'_\emptyset) = x$. It is enough to show this for x of the form $x = \prod_{i=1}^{v} x_i$, where $x_i \in I_i$ for all $i \in I$. Since $s(T_i)I_i = s(T_i)(1 - \lambda_i^{-1})\mathbb{Z}[G]$, for each $i \in I$ we can choose $y_i \in \mathbb{Z}[G]$ satisfying

$$s(T_i)x_i = s(T_i)\big(1 - \lambda_i^{-1}\big)y_i. \tag{1.4}$$

We define

$$\psi\big(\rho'_N\big) = \left(\prod_{i \in N} s(T_i)y_i\right) \cdot \prod_{i \in I - N} x_i \tag{1.5}$$

for each $N \subseteq I$. We will see in Corollary 1.6(i) below that $\psi \in \mathrm{Hom}_{\mathbb{Z}[G]}(U', \mathbb{Z}[G])$ is well-defined by the above equations if and only if the right-hand terms satisfy the relations (1.7) and (1.8), that is

$$g \cdot \psi\big(\rho'_N\big) = \psi\big(\rho'_N\big) \quad \text{for each } N \subsetneq I, \ g \in T_N$$

and

$$s(T_i) \cdot \psi\big(\rho'_N\big) = \big(1 - \lambda_i^{-1}\big) \cdot \psi\big(\rho'_{N \cup \{i\}}\big) \quad \text{for each } N \subsetneq I, \ i \in I - N.$$

But this easily follows from (1.4) and (1.5).

Remark 1.4. The definition (1.1) gives

$$|G| = \prod_{i=1}^{v} \big(t_i - \lambda_i^{-1}s(T_i) + \lambda_i^{-1}s(T_i)\big)$$

$$= \sum_{N \subseteq I} \left(\prod_{i \in N} \big(\lambda_i^{-1}s(T_i)\big)\right) \cdot \left(\prod_{i \in I - N} \big(t_i - \lambda_i^{-1}s(T_i)\big)\right)$$

$$= \sum_{N \subseteq I} \left(\prod_{i \in N} \lambda_i^{-1}\right) \cdot \left(\prod_{i \in I - N} t_i\right) \cdot \rho'_N \in U'$$

and

$$|G| \cdot \rho'_\emptyset = \prod_{i=1}^{v} \big(t_i - \lambda_i^{-1}s(T_i)\big) = \prod_{i=1}^{v} \sum_{g \in T_i} \big(1 - \lambda_i^{-1}g\big) \in \prod_{i=1}^{v} I_i.$$

Similarly $|G| \cdot \rho'_N \in \mathbb{Z}[G]$ for each $N \subseteq I$. For every $\psi \in \mathrm{Hom}_{\mathbb{Z}[G]}(U', \mathbb{Z}[G])$ this immediately gives

$$|G|^2 \cdot \psi(\rho'_\emptyset) = \left(\prod_{i=1}^{v} \sum_{g \in T_i} \left(1 - \lambda_i^{-1} g\right) \right) \psi(|G|) \in \prod_{i=1}^{v} I_i.$$

But this falls short of proving part (i) of Theorem 1.1 as $|G|$ can be a zero divisor in the quotient ring $\mathbb{Z}[G]/\prod_{i=1}^{v} I_i$. Nevertheless $|G| \in U'$ and $|G| \cdot U' \subseteq \mathbb{Z}[G]$ imply at least that the $\mathbb{Z}$-rank of U' is $|G|$. For each $j \in I$ we have $t_j e_j = s(T_j) \cdot \rho_{I-\{j\}} \in U \cap \ker \pi$, hence the $\mathbb{Z}$-rank of $U \cap \ker \pi$ is v and so the $\mathbb{Z}$-rank of U is $|G| + v$ because $U' = \pi(U)$.

The following lemma describes the additive structure of both U' and U completely.

Lemma 1.5.

(i) *The system*

$$\rho'_N \cdot \prod_{i \in I-N} g_i, \tag{1.6}$$

where N runs over the set of all subsets of I and each g_i runs over $T_i - \{1\}$, forms a $\mathbb{Z}$-basis of U'.

(ii) *The system $t_1 e_1, \ldots, t_v e_v$ and*

$$\rho_N \cdot \prod_{i \in I-N} g_i,$$

where N runs over the set of all subsets of I and each g_i runs over $T_i - \{1\}$, forms a $\mathbb{Z}$-basis of U.

Proof. (i) The number of elements mentioned in the statement of the lemma is equal to

$$\sum_{N \subseteq I} \prod_{i \in I-N} (t_i - 1) = |G|,$$

which is the $\mathbb{Z}$-rank of U' due to Remark 1.4. So it is enough to show that they generate U', which is – as an additive group – generated by $\rho'_N \cdot \prod_{i \in I-N} g_i$, where $N \subseteq I$ and $g_i \in T_i$ because

$$g \cdot \rho'_N = \rho'_N \quad \text{for each } N \subsetneqq I, \ g \in T_N. \tag{1.7}$$

Using the relation

$$s(T_i) \cdot \rho'_N = \left(1 - \lambda_i^{-1}\right) \cdot \rho'_{N \cup \{i\}} \quad \text{for each } N \subsetneqq I, \ i \in I-N, \tag{1.8}$$

we shall show that each of these generators is a $\mathbb{Z}$-linear combination of the elements mentioned in (1.6) by means of a double induction: with respect to $|N|$, and for a fixed N with respect to the number of i's with $g_i = 1$. Indeed, if $|N| = v$ then $N = I$ and ρ'_I belongs to the elements (1.6). So suppose that $|N| < v$ and that for all $L \subseteq I$, $|L| > |N|$, we know that $h \cdot \rho'_L$ is a $\mathbb{Z}$-linear combination of the elements (1.6) for any $h \in G$. For any $g = \prod_{i \in I-N} g_i$, where $g_i \in T_i$, let $R(g)$ denote the set of all i's with $g_i = 1$. If $R(g) = \emptyset$ then $g \cdot \rho'_N$ belongs to the elements (1.6). So suppose that $R(g) \neq \emptyset$ and that for all $h \in T_{I-N}$ with $|R(h)| < |R(g)|$ we already know that $h \cdot \rho'_N$ is a $\mathbb{Z}$-linear combination of the elements (1.6) for any $h \in G$. Fixing $i \in R(g)$ and multiplying (1.8) by g we obtain

$$g \cdot \rho'_N = g \cdot \left(1 - \lambda_i^{-1}\right) \cdot \rho'_{N \cup \{i\}} - \sum_{k \in T_i - \{1\}} kg \cdot \rho'_N$$

and we can use our induction hypotheses since $|N \cup \{i\}| > |N|$ and also $|R(kg)| < |R(g)|$ to finish the proof.

(ii) This can be proved in the same way; the number of elements is equal to $|G| + v$, which is the $\mathbb{Z}$-rank of U. We have again

$$g \cdot \rho_N = \rho_N \quad \text{for each } N \subsetneq I, \ g \in T_N. \tag{1.9}$$

Instead of (1.8) one uses the relations

$$s(T_i) \cdot \rho_N = \left(1 - \lambda_i^{-1}\right) \cdot \rho_{N \cup \{i\}} \quad \text{for each } N \subsetneq I, \ \{i\} \subsetneq I - N, \tag{1.10}$$

and

$$s(T_j) \cdot \rho_{I-\{j\}} = t_j e_j \quad \text{for each } j \in I, \tag{1.11}$$

by the same double induction. $\quad \square$

Corollary 1.6. *(i) The set of generators $\{\rho'_N; \ N \subseteq I\}$ together with the relations (1.7) and (1.8) defines a presentation of the module U' over $\mathbb{Z}[G]$.*

(ii) The set of generators $\{\rho_N; \ N \subseteq I\}$ together with the relations (1.9) and (1.10) defines a presentation of the module U over $\mathbb{Z}[G]$.

Proof. This was in fact established in the proof of Lemma 1.5. $\quad \square$

Let us postpone the proof of Theorem 1.1 and give a corollary first. (We are using it in [7].) Let H be a subgroup of G and consider the usual $\mathbb{Z}[G]$-module homomorphisms

$$\text{res}: \quad \mathbb{Q}[G] \to \mathbb{Q}[G/H],$$
$$\text{cor}: \quad \mathbb{Q}[G/H] \to \mathbb{Q}[G].$$

Then for any $x \in \mathbb{Q}[G/H]$ and $y \in \mathbb{Q}[G]$ we have $\operatorname{res}\operatorname{cor} x = [G : H]x$ and $\operatorname{cor}\operatorname{res} y = s(H)y$.

Corollary 1.7. *Let H be a subgroup of G and $\varphi \in \operatorname{Hom}_{\mathbb{Z}[G/H]}(U^H, \mathbb{Z}[G/H])$.*

(i) *There is $\psi \in \operatorname{Hom}_{\mathbb{Z}[G]}(U, \mathbb{Z}[G])$ such that $\psi|_{U^H} = \operatorname{cor} \circ \varphi$.*
(ii) *We have*

$$\varphi\big(s(H)\rho_\emptyset\big) \equiv \sum_{j=1}^{v} \varphi^1(t_j e_j)\operatorname{res} c_j \quad \left(\bmod \operatorname{res}\prod_{i=1}^{v} I_i\right),$$

where $\varphi^1(t_j e_j) \in \mathbb{Z}$ is determined by $\varphi(t_j e_j) = \varphi^1(t_j e_j)\sum_{\tau \in G/H}\tau$ and the elements c_j are defined in [Theorem 1.1](#).

Proof. This is just what is called the "lowering the top field" argument in [8] and [5]. Let $\nu : \mathbb{Z}[G/H] \to \mathbb{Z}$ be determined by $\nu(\sum_{\tau \in G/H} a_\tau \tau) = a_H$, i.e. ν computes the coefficient of the identity in G/H. The given φ then produces $\nu \circ \varphi \in \operatorname{Hom}_{\mathbb{Z}}(U^H, \mathbb{Z})$. Since U is a free $\mathbb{Z}$-module, U/U^H has no $\mathbb{Z}$-torsion and there is $\varphi_1 \in \operatorname{Hom}_{\mathbb{Z}}(U, \mathbb{Z})$ such that $\varphi_1|_{U^H} = \nu \circ \varphi$. Then we define $\psi \in \operatorname{Hom}_{\mathbb{Z}[G]}(U, \mathbb{Z}[G])$ by

$$\psi(x) = \sum_{\tau \in G} \varphi_1(\tau x)\tau^{-1}$$

for each $x \in U$ and we see that $\psi|_{U^H} = \operatorname{cor} \circ \varphi$. Then

$$\operatorname{cor}\operatorname{res}\psi(\rho_\emptyset) = s(H)\psi(\rho_\emptyset) = \psi\big(s(H)\rho_\emptyset\big) = \operatorname{cor}\varphi\big(s(H)\rho_\emptyset\big).$$

This means $\varphi(s(H)\rho_\emptyset) = \operatorname{res}\psi(\rho_\emptyset)$ because cor is injective. Part (ii) of [Theorem 1.1](#) states the congruence [(1.3)](#) and so

$$\varphi\big(s(H)\rho_\emptyset\big) = \operatorname{res}\psi(\rho_\emptyset) \equiv \operatorname{res}\sum_{j=1}^{s} c_j\psi^1(t_j e_j) \quad \left(\bmod \operatorname{res}\prod_{i=1}^{s} I_i\right).$$

Since $\psi(t_j e_j) = \operatorname{cor}\varphi(t_j e_j)$, we have $\psi^1(t_j e_j) = \varphi^1(t_j e_j)$. $\square$

2. Auxiliary polynomials and isotone maps

This section is devoted to some preparations that are necessary for the proof of [Theorem 1.1](#) in the next section.

Let us fix a nonempty subset $J \subseteq I$. Let $\operatorname{Chain}(J)$ mean the set of all subchains of the ordered set $(2^J, \subseteq)$ containing both $\emptyset$ and J. For any $R \in \operatorname{Chain}(J)$ and any $j \in J$ we define $M(R, j) = \min\{U \in R \mid j \in U\}$.

We define polynomials F_J, $\widehat{F}_J$ with integral coefficients in $|J|^2$ indeterminates l_i, $i \in J$, and y_{ij}, $i, j \in J$, $i \neq j$. To wit, F_J is given by

$$F_J = \sum_{R \in \text{Chain}(J)} (-1)^{|R|} \cdot \prod_{j \in J} \left(1 - l_j \cdot \prod_{i \in M(R,j)-\{j\}} y_{ij}\right), \tag{2.1}$$

and $\widehat{F}_J$ is obtained from F_J by the exchange $y_{ij} \leftrightarrow y_{ji}$, i.e.

$$\widehat{F}_J = \sum_{R \in \text{Chain}(J)} (-1)^{|R|} \cdot \prod_{j \in J} \left(1 - l_j \cdot \prod_{i \in M(R,j)-\{j\}} y_{ji}\right).$$

For example, if $J = \{1, 2\}$, the definition of F_J gives

$$F_J = (1 - l_1 y_{21}) \cdot (1 - l_2 y_{12}) - (1 - l_1) \cdot (1 - l_2 y_{12}) - (1 - l_1 y_{21}) \cdot (1 - l_2).$$

After simplification we get

$$F_J = -1 + l_1 + l_2 + l_1 l_2 (y_{12} y_{21} - y_{12} - y_{21}),$$

which clearly shows that F_J is invariant under $y_{ij} \leftrightarrow y_{ji}$. This symmetry holds in general:

Proposition 2.1. *For each $\emptyset \neq J \subseteq I$ we have $\widehat{F}_J = F_J$.*

Proof. Let us introduce new indeterminates: for each $i, j \in J$, $i \neq j$, we put $x_{ij} = y_{ij} - 1$. Then $y_{ij} = x_{ij} + 1$ and we have

$$F_J = \sum_{R \in \text{Chain}(J)} (-1)^{|R|} \cdot \prod_{j \in J} \left((1 - l_j) - l_j \cdot \sum_{\emptyset \neq N \subseteq M(R,j)-\{j\}} \prod_{i \in N} x_{ij}\right) \tag{2.2}$$

and $\widehat{F}_J$ is again obtained from F_J by the exchange $x_{ij} \leftrightarrow x_{ji}$. It is clear that both polynomials F_J and $\widehat{F}_J$ are linear in each of the variables, so to prove the lemma it is enough to show that they have the same values if each of l_i, $i \in J$, equals either 0 or 1. Let us fix any subset $Z \subseteq J$ and put

$$h_i(Z) = \begin{cases} 0 & \text{if } i \in Z, \\ 1 & \text{if } i \in J - Z. \end{cases} \tag{2.3}$$

Then the value of F_J for $l_i = h_i(Z)$ determined by (2.3) is a sum where each summand is up to a sign equal to

$$X(A) = \prod_{(i \to j) \in A} x_{ij} \tag{2.4}$$

for an oriented graph $A \in \mathrm{OrGr}(J)$, where $\mathrm{OrGr}(J)$ means the set of all oriented graphs (without loops) on the set of vertices J and $(i \to j) \in A$ denotes that A contains the arrow going from i to j. It is clear that each summand appearing in this value of F_J corresponds to an $A \in \mathrm{OrGr}(J)$ whose set $Z(A)$ of all vertices with in-degree zero is equal to Z, but we need to compute the total contribution of A. Let us fix an $A \in \mathrm{OrGr}(J)$ with $Z(A) = Z$, this A gives a summand for exactly those $R \in \mathrm{Chain}(J)$ which satisfy $M(R, i) \subseteq M(R, j)$ for each $(i \to j) \in A$. Therefore the value of F_J for $l_i = h_i(Z)$ determined by (2.3) is

$$F_J\big(l_i := h_i(Z);\ i \in J\big) = -(-1)^{|J-Z|} \sum_{\substack{A \in \mathrm{OrGr}(J) \\ Z(A)=Z}} n_A X(A), \qquad (2.5)$$

where

$$n_A = - \sum_{\substack{R \in \mathrm{Chain}(J) \\ \forall (i \to j) \in A:\ M(R,i) \subseteq M(R,j)}} (-1)^{|R|}.$$

Similarly

$$\widehat{F}_J\big(l_i := h_i(Z);\ i \in J\big) = -(-1)^{|J-Z|} \sum_{\substack{A \in \mathrm{OrGr}(J) \\ Z(\widehat{A})=Z}} n_{\widehat{A}} X(A), \qquad (2.6)$$

where $\widehat{A}$ means the dual graph to A, i.e. for each $i, j \in J$, $i \neq j$, we have $(i \to j) \in \widehat{A}$ if and only if $(j \to i) \in A$.

There is a one-to-one correspondence between $\mathrm{Chain}(J)$ and the set of all surjective mappings $J \to \{1, 2, \ldots, r\}$ for some positive integer $r \leqslant |J|$ as follows: a chain $R \in \mathrm{Chain}(J)$ of the form

$$\emptyset = R_0 \subsetneqq R_1 \subsetneqq R_2 \subsetneqq \cdots \subsetneqq R_r = J$$

corresponds to the mapping $f_R : J \to \{1, 2, \ldots, r\}$ determined by

$$f_R(i) = \min\{a \mid i \in R_a\}$$

for any $i \in J$. It is clear that $|R| = r + 1 = |f_R(J)| + 1$. Having fixed the oriented graph A, we need to compute $n_A = \sum_f (-1)^{|f(J)|}$ where f runs over the set of all surjective mappings $J \to \{1, 2, \ldots, r\}$ such that $f(i) \leqslant f(j)$ for each $(i \to j) \in A$. Let $\preccurlyeq$ be the coarsest preordering on J containing A, i.e. we have $i \preccurlyeq j$ if and only if $i = j$ or there is an oriented path in A going from i to j. Such a preordering can be viewed as a partially ordered decomposition $(D_A, \preccurlyeq)$ on J: any $i, j \in J$ belong to the same coset $[i] = [j] \in D_A$ if and only if both $i \preccurlyeq j$ and $j \preccurlyeq i$; we have $[i] \preccurlyeq [j]$ if and only if $i \preccurlyeq j$. So we are computing $n_A = \sum_f (-1)^{|f(D_A)|}$ for f running over the set of all surjective isotone mappings $(D_A, \preccurlyeq) \to (\{1, 2, \ldots, r\}, \leqslant)$. We shall use the following

Lemma 2.2. *For any finite non-empty ordered set $(D, \preccurlyeq)$ let*

$$n_{(D, \preccurlyeq)} = \sum_f (-1)^{|f(D)|}$$

where f runs over the set of all surjective isotone mappings

$$(D, \preccurlyeq) \to \big(\{1, 2, \dots, r\}, \leqslant\big)$$

for all r. Then

$$n_{(D, \preccurlyeq)} = \begin{cases} (-1)^{|D|} & \text{if } (D, \preccurlyeq) \text{ is an antichain, i.e. } \preccurlyeq \text{ is equality,} \\ 0 & \text{otherwise.} \end{cases}$$

We postpone the proof of Lemma 2.2 to finish the proof of Proposition 2.1 first. Lemma 2.2 implies $n_{\widehat{A}} = n_A$. Moreover, $(D_A, \preccurlyeq)$ is an antichain if and only if the coarsest preordering on J containing A is an equivalence, which is the case if and only if there is no arrow in A between vertices belonging to different components of A (by a component of A we mean a maximal connected subgraph of A, so a subgraph having a path from any vertex to any other vertex). In this case any $i \in J$ has in-degree zero if and only if it is the only vertex in its component, which appears if and only if its out-degree is zero. Lemma 2.2 together with (2.5) and (2.6) imply $F_J(l_i = h_i(Z);$ $i \in J) = \widehat{F}_J(l_i = h_i(Z);\ i \in J)$ and Proposition 2.1 follows. $\quad\square$

Proof of Lemma 2.2. We shall use induction with respect to the number a of maximal elements in $(D, \preccurlyeq)$. At first let us assume $a = 1$ and let m denote the only maximal element. The statement is clear if $D = \{m\}$, so we can assume that $|D| > 1$. Consider any surjective isotone mapping $f : D \to \{1, 2, \dots, r\}$. We have $m \in f^{-1}(r)$. On the one hand, if $f^{-1}(r) = \{m\}$ we define $\tilde{f} : D \to \{1, 2, \dots, r - 1\}$ by

$$\tilde{f}(u) = \begin{cases} f(u) & \text{if } u \neq m, \\ r - 1 & \text{if } u = m. \end{cases}$$

On the other hand, if $f^{-1}(r) \neq \{m\}$ we define $\tilde{f} : D \to \{1, 2, \dots, r + 1\}$ by

$$\tilde{f}(u) = \begin{cases} f(u) & \text{if } u \neq m, \\ r + 1 & \text{if } u = m. \end{cases}$$

Then $f \mapsto \tilde{f}$ is a parity-changing involution on our set of all surjective isotone mappings $f : D \to \{1, 2, \dots, r\}$ and the lemma follows for $a = 1$.

Let us now assume that $a > 1$ and that the lemma has been proved for any finite ordered set whose number of maximal elements is smaller than a. Let us choose maximal elements $m_1 \neq m_2 \in D$. We define a new ordering $\preccurlyeq_1$ on D enlarging $\preccurlyeq$ by relations $d \preccurlyeq_1 m_1$ for all $d \in D$, $d \preccurlyeq m_2$. Similarly a new ordering $\preccurlyeq_2$ on D is obtained by enlarging

$\preccurlyeq$ by relations $d \preccurlyeq_2 m_2$ for all $d \in D$, $d \preccurlyeq m_1$. Finally, let the ordered set $(D', \preccurlyeq_3)$ be obtained from $(D, \preccurlyeq)$ as follows: we amalgamate the two elements m_1 and m_2 into a new element m, so $D' = \{m\} \cup D - \{m_1, m_2\}$, and modify $\preccurlyeq$ by adding relations $d \preccurlyeq_3 m$ if and only if $d \preccurlyeq m_1$ or $d \preccurlyeq m_2$.

A surjective mapping $f : D \to \{1, 2, \ldots, r\}$ is isotone with respect to $(D, \preccurlyeq_1)$ if and only if it is isotone with respect to $(D, \preccurlyeq)$ and satisfies $f(m_1) \geqslant f(m_2)$. Similarly f is isotone with respect to $(D, \preccurlyeq_2)$ if and only if it is isotone with respect to $(D, \preccurlyeq)$ and satisfies $f(m_1) \leqslant f(m_2)$. Moreover there is a one-to-one correspondence between the set of all surjective mappings $f' : D' \to \{1, 2, \ldots, r\}$ which are isotone with respect to $(D', \preccurlyeq_3)$ and the set of all surjective mappings $f : D \to \{1, 2, \ldots, r\}$ which are isotone with respect to $(D, \preccurlyeq)$ and satisfy $f(m_1) = f(m_2)$. Therefore

$$n_{(D, \preccurlyeq)} = n_{(D, \preccurlyeq_1)} + n_{(D, \preccurlyeq_2)} - n_{(D', \preccurlyeq_3)}$$

and the lemma follows from the induction hypothesis as the number of maximal elements in any of the three involved ordered sets equals $a - 1$, noticing that neither $(D, \preccurlyeq_1)$ nor $(D, \preccurlyeq_2)$ is an antichain, and $(D', \preccurlyeq_3)$ is an antichain if and only $(D, \preccurlyeq)$ is. $\quad\square$

3. Proof of the main result

Now we can use the result of the previous section to start the proof of Theorem 1.1. Recall that for each $i \in I$ we have defined the projection $\mathrm{pr}_i : G \to T_i$ by the condition $g = \prod_{i=1}^v \mathrm{pr}_i(g)$ for each $g \in G$ and that $g_{ij} = \mathrm{pr}_i(\lambda_j)$ for each $i, j \in I$, so $\lambda_j = \prod_{i \in I} g_{ij}$, see (1.2).

Proof of Theorem 1.1. Recall that $U' = \pi(U)$, where $\pi : \mathbb{Q}[G] \oplus \mathbb{Z}^v \to \mathbb{Q}[G]$ is the projection to the first coordinate. So the restriction $\tilde{\pi} : U \to U'$ is surjective and satisfies $\tilde{\pi}(\rho_J) = \rho'_J$ for each $J \subseteq I$. Since

$$\ker \tilde{\pi} = U \cap \mathbb{Z}^v = \langle t_1 e_1, \ldots, t_v e_v \rangle$$

due to part (ii) of Lemma 1.5, this gives a bijection

$$\mathrm{Hom}_{\mathbb{Z}[G]}\bigl(U', \mathbb{Z}[G]\bigr) \to \bigl\{\psi \in \mathrm{Hom}_{\mathbb{Z}[G]}\bigl(U, \mathbb{Z}[G]\bigr); \ \forall j \in I\colon \psi(t_j e_j) = 0\bigr\}$$

determined by sending φ to $\varphi \circ \tilde{\pi}$ for each $\varphi \in \mathrm{Hom}_{\mathbb{Z}[G]}(U', \mathbb{Z}[G])$. Therefore part (i) of Theorem 1.1 is a consequence of part (ii).

To prove part (ii), let us fix some $\psi \in \mathrm{Hom}_{\mathbb{Z}[G]}(U, \mathbb{Z}[G])$. For any $N \subseteq I$ and any $h \in T_N$, we infer from (1.9) that $h \cdot \psi(\rho_N) = \psi(h \cdot \rho_N) = \psi(\rho_N)$ and so

$$\psi(\rho_N) = s(T_N) \cdot \sum_{h \in T_{I-N}} a_h^N \cdot h \tag{3.1}$$

for suitable $a_h^N \in \mathbb{Z}$. For any M, J such that $M \subseteq J \subseteq I$ and $|J| > 1$ we have

$$s(T_M) \cdot \rho_{I-J} = s(T_{(I-J)\cup M}) \cdot \prod_{i\in J}\left(1 - t_i^{-1}\lambda_i^{-1}s(T_i)\right) = \rho_{I-(J-M)} \cdot \prod_{j\in M}\left(1 - \lambda_j^{-1}\right)$$

and so

$$s(T_M) \cdot \psi(\rho_{I-J}) = \psi(\rho_{I-(J-M)}) \cdot \prod_{j\in M}\left(1 - \lambda_j^{-1}\right).$$

This gives (always assuming $|J| > 1$)

$$s(T_M) \cdot s(T_{I-J}) \cdot \sum_{h\in T_{J-M}}\sum_{g\in T_M} a_{gh}^{I-J} \cdot h$$

$$= \left(\prod_{j\in M}\left(1 - \lambda_j^{-1}\right)\right) \cdot s(T_{I-(J-M)}) \cdot \sum_{h\in T_{J-M}} a_h^{I-(J-M)} \cdot h$$

$$= s(T_M) \cdot s(T_{I-J}) \cdot \left(\prod_{j\in M}\left(1 - \lambda_j^{-1}\prod_{i\in I-(J-M)} g_{ij}\right)\right) \cdot \sum_{h\in T_{J-M}} a_h^{I-(J-M)} \cdot h.$$

Since $\lambda_j^{-1}\prod_{i\in I-(J-M)} g_{ij} = \prod_{i\in J-M} g_{ij}^{-1} \in T_{J-M}$, we have (for $|J| > 1$)

$$\sum_{h\in T_{J-M}}\sum_{g\in T_M} a_{gh}^{I-J} \cdot h = \left(\prod_{j\in M}\left(1 - \lambda_j^{-1}\prod_{i\in I-(J-M)} g_{ij}\right)\right) \cdot \sum_{h\in T_{J-M}} a_h^{I-(J-M)} \cdot h. \quad (3.2)$$

The analogous formula for the case $M = J = \{j\}$ follows from (1.11) in the same way and reads

$$\sum_{g\in T_j} a_g^{I-\{j\}} = \psi^1(t_j e_j). \quad (3.3)$$

For each $N \subseteq I$ we define $\pi_N : T_N \to \mathbb{Z}[T_N]$ by

$$\pi_N(g) = \prod_{i\in N}\left(\mathrm{pr}_i(g) - 1\right)$$

for any $g \in T_N$. Moreover, let

$$\alpha_N = \sum_{g\in T_N} a_g^{I-N} \cdot g \quad \text{and} \quad \omega_N = \sum_{g\in T_N} a_g^{I-N} \cdot \pi_N(g).$$

Therefore (3.1) gives $\psi(\rho_N) = s(T_N) \cdot \alpha_{I-N}$. Since $\pi_N(g) \in \prod_{i\in N} I_i$ we have $\omega_N \in \prod_{i\in N} I_i$, too. Finally, to formulate the following lemma we need to define

$$\omega_N' = \begin{cases} \omega_N, & \text{if } N \subseteq I, |N| \neq 1, \\ \omega_{\{j\}} + \psi^1(t_j e_j), & \text{if } N = \{j\}. \end{cases} \quad (3.4)$$

Lemma 3.1. *For each* $\emptyset \neq J \subseteq I$ *we have*

$$\alpha_J = \omega'_J + \sum_{\emptyset \neq N \subsetneq J} \omega'_N \cdot (-1)^{|J-N|}$$

$$\cdot \sum_{\emptyset = R_0 \subsetneq R_1 \subsetneq \cdots \subsetneq R_r = J-N} (-1)^r \cdot \left(\prod_{c=1}^{r} \prod_{j \in R_c - R_{c-1}} \left(1 - \lambda_j^{-1} \prod_{i \in I-(J-R_c)} g_{ij} \right) \right). \quad (3.5)$$

Let us finish the proof of Theorem 1.1 and prove Lemma 3.1 afterwards. For the special case $J = I$, (3.5) states

$$\alpha_I = \omega'_I + \sum_{\emptyset \neq N \subsetneq I} \omega'_N \cdot (-1)^{|I-N|}$$

$$\cdot \sum_{\emptyset = R_0 \subsetneq R_1 \subsetneq \cdots \subsetneq R_r = I-N} (-1)^r \cdot \left(\prod_{c=1}^{r} \prod_{j \in R_c - R_{c-1}} \left(1 - \lambda_j^{-1} \prod_{i \in R_c} g_{ij} \right) \right). \quad (3.6)$$

Let us fix N such that $\emptyset \neq N \subsetneq I$. Proposition 2.1 gives the equality of polynomials $F_{I-N} = \widehat{F}_{I-N}$, where

$$F_{I-N} = \sum_{\emptyset = R_0 \subsetneq R_1 \subsetneq \cdots \subsetneq R_r = I-N} (-1)^{r+1} \cdot \left(\prod_{c=1}^{r} \prod_{j \in R_c - R_{c-1}} \left(1 - l_j \prod_{i \in R_c - \{j\}} y_{ij} \right) \right)$$

and $\widehat{F}_{I-N}$ is obtained from F_{I-N} by the exchange $y_{ij} \leftrightarrow y_{ji}$. Therefore the two polynomials have the same values if we set the indeterminates y_{ij} to be equal to $g_{ij} \in T_i$ defined by (1.2) and $l_j = \lambda_j^{-1}$. Noticing that $g_{jj} = 1$ for each $j \in I$, this equality for each $\emptyset \neq N \subsetneq I$ leads to the following variant of (3.6):

$$\alpha_I = \omega'_I + \sum_{\emptyset \neq N \subsetneq I} \omega'_N \cdot (-1)^{|I-N|}$$

$$\cdot \sum_{\emptyset = R_0 \subsetneq R_1 \subsetneq \cdots \subsetneq R_r = I-N} (-1)^r \cdot \left(\prod_{c=1}^{r} \prod_{j \in R_c - R_{c-1}} \left(1 - \lambda_j^{-1} \prod_{i \in R_c} g_{ji} \right) \right). \quad (3.7)$$

We have $\psi(\rho_\emptyset) = \alpha_I$. If $v = 1$ then

$$\psi(\rho_\emptyset) = \alpha_{\{1\}} = \omega'_{\{1\}} = \omega_{\{1\}} + \psi^1(t_1 e_1) \equiv \psi^1(t_1 e_1) \pmod{I_1}.$$

Let us assume $v > 1$ now. We have $\prod_{i \in R_c} g_{ji} \in T_j$, which gives

$$1 - \lambda_j^{-1} \prod_{i \in R_c} g_{ji} \in I_j,$$

and $\omega_N \in \prod_{i \in N} I_i$. The theorem now follows from (3.7) using (3.4) and Proposition 2.1 again. $\quad \square$

Proof of Lemma 3.1. For any $g \in T_J$ we have $g = \prod_{i \in J} \mathrm{pr}_i(g)$ and

$$\pi_J(g) = \prod_{i \in J}(\mathrm{pr}_i(g) - 1) = \sum_{M \subseteq J}(-1)^{|M|} \prod_{i \in J-M} \mathrm{pr}_i(g).$$

Hence

$$\alpha_J = \sum_{g \in T_J} a_g^{I-J} \cdot \left(\pi_J(g) - \sum_{\emptyset \neq M \subseteq J}(-1)^{|M|} \prod_{i \in J-M} \mathrm{pr}_i(g)\right),$$

so

$$\alpha_J = \omega_J - \sum_{\emptyset \neq M \subseteq J}(-1)^{|M|} \sum_{h \in T_{J-M}} \sum_{g \in T_M} a_{gh}^{I-J} \cdot h \tag{3.8}$$

and, on the one hand, if $|J| > 1$ then (3.2) gives

$$\alpha_J = \omega_J' - \sum_{\emptyset \neq M \subseteq J}(-1)^{|M|}\left(\prod_{j \in M}\left(1 - \lambda_j^{-1} \prod_{i \in I-(J-M)} g_{ij}\right)\right) \cdot \alpha_{J-M}. \tag{3.9}$$

On the other hand, if $J = \{j\}$, then we obtain by (3.8) and (3.3)

$$\alpha_J = \omega_J + \sum_{g \in T_j} a_g^{I-\{j\}} = \omega_J + \psi^1(t_j e_j) = \omega_J'. \tag{3.10}$$

But this means that (3.9) holds true also for $J = \{j\}$ because

$$1 - \lambda_j^{-1} \prod_{i \in I} g_{ij} = 0. \tag{3.11}$$

We shall prove by induction with respect to $|J| \geqslant 1$ that the recurrence relation (3.9) implies the explicit relation (3.5). Indeed, if $J = \{j\}$ then (3.5) is given by (3.10). Let us fix any $N \subseteq I$ such that $|N| > 1$ and let us suppose that the formula (3.5) has been proved for any $\emptyset \neq J \subsetneq N$. Using (3.9) and (3.11) we have

$$\alpha_N = \omega_N' - \sum_{\emptyset \neq J \subsetneq N}(-1)^{|N-J|}\left(\prod_{j \in N-J}\left(1 - \lambda_j^{-1} \prod_{i \in I-J} g_{ij}\right)\right) \cdot \alpha_J.$$

The induction hypothesis gives

$$\alpha_N = \omega_N' - \sum_{\emptyset \neq J \subsetneq N}(-1)^{|N-J|}\left(\prod_{j \in N-J}\left(1 - \lambda_j^{-1} \prod_{i \in I-J} g_{ij}\right)\right)$$

$$\cdot \left(\omega_J' + \sum_{\emptyset \neq M \subsetneq J} \omega_M' \cdot (-1)^{|J-M|} \cdot \sum_{\emptyset = R_0 \subsetneq R_1 \subsetneq \cdots \subsetneq R_r = J-M}(-1)^r\right.$$

$$\cdot \left(\prod_{c=1}^{r} \prod_{j \in R_c - R_{c-1}} \left(1 - \lambda_j^{-1} \prod_{i \in I - (J - R_c)} g_{ij} \right) \right). \tag{3.12}$$

For the set N that was fixed previously let us define the following set of indices

$$X = \left\{ (T, R_1, \ldots, R_r) \mid \emptyset \neq T \subsetneq N, \ r > 0, \ \emptyset \neq R_1 \subsetneq \cdots \subsetneq R_r = N - T \right\}.$$

The formula (3.5) for N will be proved if we show that

$$\alpha_N = \omega'_N + \sum_{(T, R_1, \ldots, R_r) \in X} \omega'_T \cdot (-1)^{|N-T|+r}$$

$$\cdot \prod_{c=1}^{r} \prod_{j \in R_c - R_{c-1}} \left(1 - \lambda_j^{-1} \prod_{i \in I - (N - R_c)} g_{ij} \right), \tag{3.13}$$

where $R_0 = \emptyset$. Similarly, we define

$$Y = \left\{ (J, M, R_1, \ldots, R_r) \mid \emptyset \neq M \subseteq J \subsetneq N, \ r \geqslant 0, \ \emptyset \neq R_1 \subsetneq \cdots \subsetneq R_r = J - M \right\},$$

where the case $r = 0$ gives $(J, J) \in Y$ for any $\emptyset \neq J \subsetneq N$. Then (3.12) can be written as

$$\alpha_N = \omega'_N - \sum_{(J, M, R_1, \ldots, R_r) \in Y} \omega'_M \cdot (-1)^{|N-M|+r} \left(\prod_{j \in N - J} \left(1 - \lambda_j^{-1} \prod_{i \in I - J} g_{ij} \right) \right)$$

$$\cdot \prod_{c=1}^{r} \prod_{j \in R_c - R_{c-1}} \left(1 - \lambda_j^{-1} \prod_{i \in I - (J - R_c)} g_{ij} \right), \tag{3.14}$$

where again $R_0 = \emptyset$. We can define a mapping $Y \to X$ as follows: the image of $(J, J) \in Y$ is $(J, N - J) \in X$ and $(J, M, R_1, \ldots, R_r) \in Y$ with $r > 0$ is mapped to $(M, N - J, R_1 \cup (N - J), \ldots, R_r \cup (N - J)) \in X$. One can see that this is a bijection which matches up the summands in the two expressions for α_N just given, see (3.13) and (3.14). The lemma follows. $\square$

4. Another description of the coefficients c_k

To be able to describe the coefficients c_k, $k \in I$, appearing on the right hand side of (1.3) in another way, let $\mathrm{OrGr}(k, I)$ be the set of all graphs $B \in \mathrm{OrGr}(I)$ such that the in-degree of the vertex k is zero and that for each vertex $i \in I$, $i \neq k$, there is at least one oriented path going from k to i.

Proposition 4.1. *For any $k \in I$ we have*

$$c_k \prod_{i \in I - \{k\}} \lambda_i = \sum_{B \in \mathrm{OrGr}(k, I)} X'(B), \tag{4.1}$$

where

$$X'(B) = \prod_{(i \to j) \in B} (g_{ij} - 1).$$

Proof. Let $J = I - \{k\}$. Theorem 1.1 and the definition of the polynomial F_J (see (2.1) and (2.2)) give

$$c_k = (-1)^v \cdot F_J\big(l_i := \lambda_i^{-1};\ y_{ij} := g_{ij}\big) = (-1)^v \cdot F_J\big(l_i := \lambda_i^{-1};\ x_{ij} := g_{ij} - 1\big).$$

Since F_J is a linear polynomial in each variable l_j, we have the equality

$$F_J = \sum_{Z \subseteq J} \left(\prod_{i \in Z} (1 - l_i) \right) \left(\prod_{i \in J - Z} l_i \right) F_J\big(l_i := h_i(Z)\big),$$

where $h_i(Z)$ are determined by (2.3), because this holds true if each l_i is either 0 or 1. Let $\mathrm{OrGr}'(J)$ be the set all graphs $A \in \mathrm{OrGr}(J)$ such that there is no arrow in A between vertices belonging to different components of A. Equalities (2.4) and (2.5) and Lemma 2.2 give

$$F_J = - \sum_{Z \subseteq J} \left(\prod_{i \in Z} (1 - l_i) \right) \left(\prod_{i \in J - Z} l_i \right) (-1)^{|J-Z|} \sum_{\substack{A \in \mathrm{OrGr}'(J) \\ Z(A) = Z}} (-1)^{\mathrm{comp}(A)} X(A)$$

$$= (-1)^v \sum_{A \in \mathrm{OrGr}'(J)} \left(\prod_{i \in Z(A)} (1 - l_i) \right) \left(\prod_{i \in J - Z(A)} l_i \right) (-1)^{\mathrm{comp}(A) - |Z(A)|} X(A),$$

where $\mathrm{comp}(A)$ means the number of components of A. Hence

$$c_k \prod_{i \in J} \lambda_i = \sum_{A \in \mathrm{OrGr}'(J)} \left(\prod_{i \in Z(A)} (\lambda_i - 1) \right) (-1)^{\mathrm{comp}(A) - |Z(A)|} X'(A).$$

Due to (1.2) we have

$$\lambda_j - 1 = -1 + \prod_{i \in I} g_{ij} = \sum_{\emptyset \neq L \subseteq I - \{j\}} \prod_{i \in L} (g_{ij} - 1)$$

and so

$$c_k \prod_{i \in J} \lambda_i = \sum_{A \in \mathrm{OrGr}'(J)} (-1)^{\mathrm{comp}_2(A)} X'(A) \prod_{j \in Z(A)} \sum_{\emptyset \neq L_j \subseteq I - \{j\}} \prod_{i \in L_j} (g_{ij} - 1), \qquad (4.2)$$

where $\mathrm{comp}_2(A) = \mathrm{comp}(A) - |Z(A)|$ is the number of components of A consisting of at least two vertices. Let us call a graph $B \in \mathrm{OrGr}(I)$ a completion of the graph $A \in \mathrm{OrGr}'(J)$ if B is obtained from A by adding a new vertex k and by adding arrows

ending in elements of $Z(A)$ such that every $j \in Z(A)$ is the end point of at least one (new) arrow. (Note that such arrow can start at k or at $j' \in Z(A)$, $j' \neq j$, or in $J - Z(A)$.) Such a graph B satisfies that the in-degree of k is zero while the in-degree of any other vertex is positive and that there is no arrow going from any vertex in $Z(A) \cup \{k\}$ to any vertex in $J - Z(A)$. Then we have

$$X'(A) \prod_{j \in Z(A)} \sum_{\emptyset \neq L_j \subseteq I - \{j\}} \prod_{i \in L_j} (g_{ij} - 1) = \sum_{B \in \mathrm{Compl}(A)} X'(B),$$

where $\mathrm{Compl}(A)$ means the set of all completions of A.

Let $\mathrm{OrGr}'(k, I)$ be the set of all graphs $B \in \mathrm{OrGr}(I)$ such that the in-degree of k is zero while the in-degree of any other vertex is positive. Then the equality (4.2) can be rewritten as

$$c_k \prod_{i \in J} \lambda_i = \sum_{B \in \mathrm{OrGr}'(k, I)} X'(B) \sum_{\substack{A \in \mathrm{OrGr}'(J) \\ B \in \mathrm{Compl}(A)}} (-1)^{\mathrm{comp}_2(A)}. \tag{4.3}$$

Let us fix $B \in \mathrm{OrGr}'(k, I)$. To understand the last sum in the previous equation, we need to know which graphs $A \in \mathrm{OrGr}'(J)$ have B as their completion. Let $U(B)$ be the set of all vertices $i \in J$ which cannot be reached from the vertex k by a path in B. So there is no arrow in B going from any vertex in $I - U(B)$ to any vertex in $U(B)$.

On the one hand, suppose that $U(B) = \emptyset$, which means that $B \in \mathrm{OrGr}(k, I)$. If B is a completion of $A \in \mathrm{OrGr}'(J)$, then $Z(A) = J$ so A has no arrows. Hence there is only one such A and the contribution to (4.3) is $X'(B)$.

On the other hand, suppose that $U(B) \neq \emptyset$, which means $B \notin \mathrm{OrGr}(k, I)$. Let us decompose the subgraph $U(B)$ into its components. The set of these components can be understood again as an oriented graph: there is an arrow between two components if and only if there is at least one arrow in $U(B)$ between vertices in these components. Let $C_1, \ldots, C_n$ be the components which are roots of this acyclic graph on components of $U(B)$; it is clear that $n \geqslant 1$ because $U(B)$ is finite and nonempty, and also that each component C_r has at least two vertices because the in-degree of each its vertex is positive. Recalling that graphs $A \in \mathrm{OrGr}'(J)$ have no arrows between components, it is clear that B can be a completion of A if and only if $J - Z(A)$ is a union of any number of components $C_1, \ldots, C_n$. Then A has no other arrows, but the arrows given by the chosen components $C_1, \ldots, C_n$, and $\mathrm{comp}_2(A)$ equals the number of these components. Therefore the total contribution of these A's in formula (4.3) is

$$X'(B) \sum_{Y \subseteq \{C_1, \ldots, C_n\}} (-1)^{|Y|} = 0$$

and the proposition follows, because $\mathrm{OrGr}(k, I)$ is just the set of all $B \in \mathrm{OrGr}'(J)$ satisfying $U(B) = \emptyset$. $\quad\square$

Remark 4.2. Note that each $B \in \mathrm{OrGr}(k, I)$ which is not a tree has at least v arrows and that all factors $g_{ij} - 1$ belong to the augmentation ideal I_G of G. Therefore the right hand side of (4.1) is congruent modulo I_G^v to the analogous sum, $S(k, I)$ say, taken over all *trees* $B \in \mathrm{OrGr}(k, I)$. We also see that the left hand side of (4.1) is congruent modulo I_G^v to c_k since $c_k \in I_G^{v-1}$. Using the Kirchhoff–Tutte theorem, the sum $S(k, I)$ can be written as the (k, k)th minor of the matrix with zero row sums whose nondiagonal entries are $1 - g_{ji}$ (where i is the row index as usual). Modulo the vth power of the augmentation ideal, this is congruent to the (k, k)th minor of the matrix with zero row sums whose nondiagonal entries are $g_{ji}^{-1} - 1$. This is exactly the description of the coefficients used in Proposition 5.5 of [8] (see also page 114 and Lemma 5.4 of loc. cit.).

Remark 4.3. It should be noted that the right hand side of (4.1) has very many summands, much more than the sum $S(k, I)$ involving trees and also than the sums in the formulae for c_j in Theorem 1.1. To be a little more concrete, for $v = 3$, we have $|\mathrm{OrGr}(k, I)| = 8$, whereas there are only 3 trees with root k and 3 chains. For $v = 4$, the corresponding numbers are 304, 16, and 13. The number of trees is v^{v-2} due to the well-known formula, but we do not know any counting formulae for the other two objects, the number of chains or the number of graphs in $\mathrm{OrGr}(k, I)$. We have an upper bound (and conjectural asymptotic formula) for the number of chains and this shows that the ratio of the number of chains to the number of trees goes to zero for $|I| \to \infty$.

References

[1] H. Bass, Generators and relations for cyclotomic units, Nagoya Math. J. 27 (1966) 401–407.
[2] J.-R. Belliard, H. Oukhaba, Sur la torsion de la distribution ordinaire universelle attaché à un corps de nombres, Manuscripta Math. 106 (2001) 117–130.
[3] D. Burns, Congruences between derivatives of abelian L-functions at $s = 0$, Invent. Math. 169 (2007) 451–499.
[4] V. Ennola, On relations between cyclotomic units, J. Number Theory 4 (1972) 236–247.
[5] C. Greither, R. Kučera, Annihilators for the class group of a cyclic field of prime power degree II, Canad. J. Math. 58 (2006) 580–599.
[6] C. Greither, R. Kučera, Eigenspaces of the ideal class group, Ann. Inst. Fourier (Grenoble) 64 (2014), in press.
[7] C. Greither, R. Kučera, Annihilators for the class group of a cyclic field of prime power degree III, preprint.
[8] A. Hayward, A class number formula for higher derivatives of abelian L-functions, Compos. Math. 140 (2004) 99–129.
[9] H. Oukhaba, Index formulas for ramified elliptic units, Compos. Math. 137 (1) (2003) 1–22.
[10] W. Sinnott, On the Stickelberger ideal and the circular units of a cyclotomic field, Ann. of Math. 108 (1978) 107–134.
[11] W. Sinnott, On the Stickelberger ideal and the circular units of an abelian field, Invent. Math. 62 (1980) 181–234.
[12] D. Solomon, Galois relations for cyclotomic numbers and p-units, J. Number Theory 46 (1994) 158–178.
[13] L. Washington, Introduction to Cyclotomic Fields, Grad. Texts in Math., vol. 83, Springer, New York, 1997.
[14] L. Yin, Distributions on a global field, J. Number Theory 80 (2000) 154–167.