

# The second syzygy of the trivial $G$ -module, and an equivariant main conjecture

Cornelius Greither, Masato Kurihara and Hibiki Tokio

*In honor of K. Iwasawa*

## Abstract.

For a finite abelian  $p$ -extension  $K/k$  of totally real fields and the cyclotomic  $\mathbb{Z}_p$ -extension  $K_\infty/K$ , we prove a strong version of an equivariant Iwasawa main conjecture by determining completely the Fitting ideal over  $\mathbb{Z}_p[[\text{Gal}(K_\infty/k)]]$  of the classical Iwasawa module  $X_{K_\infty, S}$ , which is the Galois group of the maximal pro- $p$  abelian  $S$ -ramified extension of  $K_\infty$ , where  $S$  contains all ramified primes in  $K_\infty/k$ . To do this, we prove a conjecture which was proposed in a previous paper by the first and second author, concerning the minors of a relation matrix for the second syzygy module of the trivial module  $\mathbb{Z}$  over a suitable group ring.

## §1. Introduction

In a recent paper [2] the first two authors described the Fitting ideals of certain Iwasawa modules in terms of ideals generated by minors of a relation matrix for a second syzygy module of  $\mathbb{Z}$  over abelian group rings. Moreover, in §1 (Remark to Proposition 1.5) of that paper an explicit description of those ideals was stated, but one of the two inclusions remained conjectural. Our aim in this paper is to prove the conjectural inclusion as well. This means that these ideals of minors are now completely determined.

In §1.1 of this introduction, we explain the conjecture on the ideals of minors. Then in §1.2 we give a consequence of the conjecture (now a theorem) in Iwasawa theory. Indeed, we are now able to state and prove our equivariant Iwasawa main conjecture.

---

2010 *Mathematics Subject Classification.* 11R23, 13D02, 15A15.

*Key words and phrases.* Iwasawa module, Fitting ideal.

### 1.1. A second syzygy of $\mathbb{Z}$

Let  $G$  be a finite abelian group such that

$$G \simeq \mathbb{Z}/n_1\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/n_s\mathbb{Z},$$

where  $n_i$  is a divisor of  $n_{i+1}$  for each  $i = 1, \dots, s-1$ . Suppose that  $\sigma_i \in G$  is a generator of the  $i$ -th component of the above decomposition for each  $i$ . We put  $R = \mathbb{Z}[G]$ , which is the group ring of  $G$  over  $\mathbb{Z}$ , and consider the  $R$ -module  $\mathbb{Z}$  with trivial action of  $G$ . Using the method in [2] §1.2, we obtain a free resolution

$$R^{s(s+1)(s+2)/6} \xrightarrow{\Phi_3} R^{s(s+1)/2} \xrightarrow{\Phi_2} R^s \xrightarrow{\Phi_1} R \longrightarrow \mathbb{Z} \longrightarrow 0$$

of  $\mathbb{Z}$ . The full description of this exact sequence will be given in §2, and we just mention here that  $\Phi_1$  is defined by  $\Phi_1(x_i) = \sigma_i - 1$ , where  $(x_i)_{1 \leq i \leq s}$  is the standard basis of  $R^s$ . We put  $\Omega^2 = \text{Ker } \Phi_1$ , which is a second syzygy of  $\mathbb{Z}$ . Thus we have an exact sequence

$$R^{s(s+1)(s+2)/6} \xrightarrow{\Phi_3} R^{s(s+1)/2} \longrightarrow \Omega^2 \longrightarrow 0.$$

We denote by  $\tilde{M}_s$  the matrix which corresponds to the  $R$ -homomorphism  $\Phi_3$ , and which can be written down explicitly (see §2.1).

Put  $c = s(s+1)/2$ .

For an integer  $v$  such that  $0 \leq v \leq c$ , we define  $\mathfrak{m}_v = \text{Min}_v(\tilde{M}_s)$  to be the ideal of  $R$  generated by all  $v$ -minors of the matrix  $\tilde{M}_s$ . We note that  $\mathfrak{m}_v$  is equal to the higher Fitting ideal  $\text{Fitt}_{c-v, R}(\Omega^2)$  (concerning the definition of Fitting ideals, see [5]). The matrix  $\tilde{M}_s$  is rather sparse, but the calculation of the relevant minors is still difficult. The entries are elements of the form  $\pm\tau_i$  and  $\pm\nu_i$  where  $\tau_i = \sigma_i - 1 \in R$  and  $\nu_i = 1 + \sigma_i + \dots + \sigma_i^{n_i-1} \in R$  (recall that  $n_i$  is the order of  $\sigma_i$  in  $G$ ). We note here the important relation  $\tau_i\nu_i = 0$ .

We can easily see  $\mathfrak{m}_v = 0$  for any  $v$  such that  $s(s-1)/2 + 1 < v \leq c$ , using  $\mathfrak{m}_v = \text{Fitt}_{c-v, R}(\Omega^2)$  (see Proposition 1.5 (a) in [2]). Now we state our main theorem in which we determine all  $\mathfrak{m}_v$ .

We define  $H$  to be the ideal of  $R$  generated by  $\tau_1, \dots, \tau_s$ ; differently put,  $H$  is the augmentation ideal of  $R$ . We will define the notion ‘‘admissible monomial’’ in §2.2, and denote by  $\mathfrak{n}_d$  the ideal generated by all admissible monomials of degree  $d$ , with  $0 < d \leq s(s-1)/2$ . We also define  $\mathfrak{n}_0 = R$  and  $\mathfrak{n}_{\frac{s(s-1)}{2}+1} = 0$ . In this paper we prove the following.

**Theorem 1.1.** *For any integer  $v$  such that  $0 \leq v \leq \frac{s(s-1)}{2} + 1$ , we have*

$$\mathfrak{m}_v = \text{Fitt}_{c-v, R}(\Omega^2) = \sum_{d=0}^v H^{v-d} \mathfrak{n}_d.$$

In particular, we have

$$\mathfrak{m}_{\frac{s(s-1)}{2}+1} = H \sum_{d=0}^{s(s-1)/2} H^{\frac{s(s-1)}{2}-d} \mathfrak{n}_d = H \mathfrak{m}_{\frac{s(s-1)}{2}}.$$

In [2] Proposition 1.5 (b) we proved that the left hand side is contained in the right hand side of the above equality, and stated this equality as a conjecture. For  $s \leq 4$  we had verified the conjecture by hand, which was already a sizable calculation for  $s = 4$ . The third author checked it for  $s = 5$  in [7].

In this paper we prove the converse inclusion. To do this, we exhibit many square submatrices of  $\tilde{M}_s$  which are lower triangular; so their determinants can be evaluated at once (product of the diagonal entries), and in this way we are able to produce all monomials in the elements  $\tau_i$  and  $\nu_i$  that are required to establish the desired converse inclusion. The arguments are entirely elementary and combinatorial, but some of the details are a bit tricky. Even though the entire motivation for this work comes from [2], it is not necessary to be familiar with that paper for reading the proof of Theorem 1.1.

## 1.2. An equivariant main conjecture for $X_{K_\infty, S}$

Now we state one of the consequences in Iwasawa theory, which is a main motivation of the above theorem. Let  $K/k$  be a finite abelian extension of totally real number fields,  $p$  an odd prime, and  $K_\infty/K$  the cyclotomic  $\mathbb{Z}_p$ -extension. We consider the maximal pro- $p$  abelian extension  $M_{\infty, S}/K_\infty$  which is unramified outside  $S$ , where  $S$  is a finite set of primes of  $k$  containing all ramified primes in  $K_\infty/k$ , and hence in particular all  $p$ -adic primes. We put  $X_{K_\infty, S} = \text{Gal}(M_{\infty, S}/K_\infty)$ . It is well-known that this is a finitely generated torsion  $\Lambda_{K_\infty} = \mathbb{Z}_p[[\text{Gal}(K_\infty/k)]]$ -module.

The celebrated main conjecture in Iwasawa theory, which is a theorem of Wiles [8], states a relationship between the characteristic ideal of a character component of  $X_{K_\infty, S}$  and the  $p$ -adic  $L$ -function of Deligne-Ribet. Let  $\Theta_{K_\infty/k, S}$  be the pseudo-measure of  $\text{Gal}(K_\infty/k)$  in the sense of Serre [6], corresponding to the  $p$ -adic  $L$ -function of Deligne-Ribet, which interpolates the values  $L_S(1-n, \chi)$  of  $S$ -truncated  $L$ -functions for characters  $\chi$  of  $\text{Gal}(K/k)$ . Suppose that  $I_{K_\infty}$  is the augmentation ideal  $\text{Ker}(\Lambda_{K_\infty} = \mathbb{Z}_p[[\text{Gal}(K_\infty/k)]] \rightarrow \mathbb{Z}_p)$ ; then we know  $I_{K_\infty} \Theta_{K_\infty/k, S} \subset \Lambda_{K_\infty}$  (see [6]). Especially, if  $\gamma$  is a generator of  $\text{Gal}(K_\infty/K) \simeq \mathbb{Z}_p$  and  $T = \gamma - 1 \in \Lambda_{K_\infty}$ , then we have  $T \Theta_{K_\infty/k, S} \in \Lambda_{K_\infty}$ . For simplicity, assume  $K \cap k_\infty = k$  where  $k_\infty$  is the cyclotomic  $\mathbb{Z}_p$ -extension, put  $G = \text{Gal}(K/k)$ ,  $\Gamma = \text{Gal}(K_\infty/K)$ , and  $\mathcal{G} = \text{Gal}(K_\infty/k)$ , so  $\mathcal{G} = G \times \Gamma$ .

For any character  $\chi$  of  $G$  and any  $\mathbb{Z}_p[G]$ -module  $M$ , we define the  $\chi$ -component  $M_\chi$  by  $M_\chi = M \otimes_{\mathbb{Z}_p[G]} \mathcal{O}_\chi$ , where  $\mathcal{O}_\chi = \mathbb{Z}_p[\text{Image } \chi]$  on which  $G$  acts via  $\chi$ . If  $M$  is a  $\mathbb{Z}_p[[\mathcal{G}]]$ -module,  $M_\chi$  is an  $\mathcal{O}_\chi[[\Gamma]]$ -module. We note that  $M_\chi$  is a quotient of  $M$ . We denote the image of an element  $x \in M$  in  $M_\chi$  by  $x_\chi$ . The main conjecture asserts that for each character  $\chi$  of  $G$ , the characteristic ideal of an  $\mathcal{O}_\chi[[\Gamma]]$ -module  $(X_{K_\infty, S})_\chi$  is generated by the  $\chi$ -component  $(\Theta_{K_\infty/k, S})_\chi$  of  $\Theta_{K_\infty/k, S}$  if  $\chi$  is not the trivial character, and by  $(T\Theta_{K_\infty/k, S})_\chi$  if  $\chi$  is the trivial character.

Our goal in this paper is to establish a more refined relationship than the main conjecture between the two sides, that is  $X_{K_\infty, S}$  and  $\Theta_{K_\infty/k, S}$ , *without taking the character components*.

There exist several equivariant main conjectures, but they all use modified Iwasawa modules (e.g. cohomology groups; for example, see [1] and [4]), and there has been no equivariant theory for  $X_{K_\infty, S}$  itself before our work. The difficulty in studying  $X_{K_\infty, S}$  comes from the fact that  $X_{K_\infty, S}$  does not have projective dimension  $\leq 1$  over  $\Lambda_{K_\infty}$  when  $p$  divides the order of  $G$ .

In this paper we study the classical object  $X_{K_\infty, S}$  itself, and prove a kind of equivariant main conjecture for it. For any ring  $R$  and any  $R$ -module  $M$ , we denote the initial Fitting ideal  $\text{Fitt}_{0, R}(M)$  simply by  $\text{Fitt}_R(M)$ . We will determine the Fitting ideal  $\text{Fitt}_{\Lambda_{K_\infty}}(X_{K_\infty, S})$  completely, by which we get more information than the characteristic ideals of the character components. For example, we obtain information on the size of the  $\mathcal{O}_\chi$ -torsion submodule of  $(X_{K_\infty, S})_\chi$  from our knowledge of  $\text{Fitt}_{\Lambda_{K_\infty}}(X_{K_\infty, S})$  (see also Remark 1.4 (2) and the argument just after Remark 1.4), but first and foremost, we get *the exact relationship between the Iwasawa module  $X_{K_\infty, S}$  and the  $p$ -adic  $L$ -function  $\Theta_{K_\infty/k, S}$* .

In previous work [3] by the first two authors, we proved in Theorem 4.1 in [3] that

$$\text{Fitt}_{\Lambda_{K_\infty}}(X_{K_\infty, S}) = \mathfrak{A}\Theta_{K_\infty/k, S}$$

with a certain ideal  $\mathfrak{A}$  of  $\Lambda_{K_\infty}$ . What we do in this paper is performing further computations on the ideal  $\mathfrak{A}$  in order to describe it completely. We also note that the description given here is more general and explicit than the appendix in [2].

The essential case is that  $K/k$  is a nontrivial  $p$ -extension, so we assume it (for the general case, see [2]). We still assume that  $K \cap k_\infty = k$  and put  $G = \text{Gal}(K/k)$ . We change the notation slightly from the previous subsection, and write

$$G \simeq \mathbb{Z}/p^{n_1}\mathbb{Z} \oplus \dots \oplus \mathbb{Z}/p^{n_s}\mathbb{Z}$$

with  $0 < n_1 \leq \dots \leq n_s$  for some  $s \in \mathbb{Z}_{>0}$ . We need the auxiliary quadratic function

$$\varphi(\alpha) = \alpha(2s - \alpha - 1)/2 \quad (\text{for any } \alpha \in \mathbb{Z} \text{ such that } 0 \leq \alpha \leq s - 1).$$

This is an increasing function in the above range, and  $\varphi(0) = 0$ ,  $\varphi(1) = s - 1$ ,  $\varphi(2) = 2s - 3, \dots$ , and  $\varphi(s - 1) = s(s - 1)/2$ . We define a sequence  $(m_v)_{0 \leq v \leq s(s-1)/2}$  of integers as follows. We define  $m_0 = 0$ , and if  $v$  satisfies  $\varphi(\alpha) < v \leq \varphi(\alpha + 1)$  for some integer  $\alpha \in \mathbb{Z}$  with  $0 \leq \alpha \leq s - 2$ , then  $m_v$  is defined by

$$m_v = (s - 1)n_1 + \dots + (s - \alpha)n_\alpha + (v - \varphi(\alpha))n_{\alpha+1}.$$

In particular,  $m_v = vn_1$  for  $0 \leq v \leq s - 1$ , and

$$m_{\frac{s(s-1)}{2}} = (s - 1)n_1 + (s - 2)n_2 + \dots + n_{s-1}.$$

Recall that  $I_{K_\infty}$  is the augmentation ideal of  $\Lambda_{K_\infty} = \mathbb{Z}_p[[\mathcal{G}]]$ , with  $\mathcal{G} = \text{Gal}(K_\infty/k)$ . We define an ideal  $\mathfrak{a}_G$  of  $\Lambda_{K_\infty}$  by

$$\mathfrak{a}_G = \sum_{v=0}^{\frac{s(s-1)}{2}} p^{m_v} I_{K_\infty}^{\frac{s(s-1)}{2} - v},$$

which is determined only by the structure of  $G$  as an abelian group. Our equivariant main conjecture which we prove in this paper is

**Theorem 1.2.** *Assume that the  $\mu$ -invariant of  $k_\infty/k$  vanishes and that  $S$  contains all ramified primes in  $K_\infty/k$  (as we already mentioned). Then we have*

$$\text{Fitt}_{\Lambda_{K_\infty}}(X_{K_\infty, S}) = \mathfrak{a}_G I_{K_\infty} \Theta_{K_\infty/k, S}.$$

In order to understand the ideal  $\mathfrak{a}_G$ , let us consider simple cases. Suppose that  $G$  is homogeneous, that is,  $n_1 = \dots = n_s = n$ . Put

$$J_{K_\infty} = p^n \Lambda_{K_\infty} + I_{K_\infty}.$$

If  $n = 1$ ,  $J_{K_\infty}$  coincides with the maximal ideal  $\mathfrak{m}_{K_\infty}$  of  $\Lambda_{K_\infty}$ . It is easy to check that  $m_v = nv$  and

$$\begin{aligned} \mathfrak{a}_G &= \sum_{v=0}^{s(s-1)/2} p^{nv} I_{K_\infty}^{\frac{s(s-1)}{2} - v} = (p^n, I_{K_\infty})^{s(s-1)/2} \\ &= J_{K_\infty}^{s(s-1)/2}. \end{aligned}$$

Therefore, we get

**Corollary 1.3.** *Assume further that  $n_1 = \dots = n_s = n$ . Then we have*

$$\text{Fitt}_{\Lambda_{K_\infty}}(X_{K_\infty, S}) = J_{K_\infty}^{s(s-1)/2} I_{K_\infty} \Theta_{K_\infty/k, S}.$$

Also, if  $n = 1$ , we have

$$\text{Fitt}_{\Lambda_{K_\infty}}(X_{K_\infty, S}) = \mathfrak{m}_{K_\infty}^{s(s-1)/2} I_{K_\infty} \Theta_{K_\infty/k, S},$$

where  $\mathfrak{m}_{K_\infty}$  is the maximal ideal of  $\Lambda_{K_\infty}$ .

**Remark 1.4.** (1) At some stage, there was a guess that

$$\text{Fitt}_{\Lambda_{K_\infty}}(X_{K_\infty, S}) = I_{K_\infty} \Theta_{K_\infty/k, S}.$$

Our theorem shows that this is only true for  $s = 1$ , and the bigger  $s$  gets, the more badly it fails, because  $\mathfrak{a}_G$  becomes smaller and smaller for  $s \rightarrow \infty$ .

(2) Since the ideal  $\mathfrak{a}_G$  is of finite index in  $\Lambda_{K_\infty}$ , its image in  $\Lambda_{K_\infty, \chi}$  is also of finite index in  $\Lambda_{K_\infty, \chi}$ . Thus Theorem 1.2 implies the usual main conjecture, and in fact refines it.

Theorem 1.2 also gives information on the size of the  $\mathcal{O}_\chi$ -torsion submodule of  $(X_{K_\infty, S})_\chi$ . Suppose for simplicity that we are in the situation of Corollary 1.3, and also assume that  $\chi$  is nontrivial. Then we know that the characteristic ideal of  $(X_{K_\infty, S})_\chi$  is generated by  $(\Theta_{K_\infty/k, S})_\chi$ . This shows that

$$\chi(I_{K_\infty}) \chi(J_{K_\infty})^{s(s-1)/2} = \text{Fitt}_{\mathcal{O}_\chi[[\Gamma]]}(((X_{K_\infty, S})_\chi)_{\text{tors}})$$

where  $((X_{K_\infty, S})_\chi)_{\text{tors}}$  is the  $\mathcal{O}_\chi$ -torsion part. Since the left hand side becomes fairly small if  $s$  becomes large (see also Remark 1.4 (4) below), the above formula also shows that  $((X_{K_\infty, S})_\chi)_{\text{tors}}$  is fairly big if  $s$  is large. In this way our Theorem 1.2 also sheds light on the torsion part of Iwasawa modules.

(3) For an abelian CM-extension  $L/k$  which is unramified outside  $p$  and the cyclotomic  $\mathbb{Z}_p$ -extension  $L_\infty/L$ , we can determine the Fitting ideal of the Pontrjagin dual of the minus part of the  $p$ -part of the class group of  $L_\infty$ , using Theorem 1.2. For the details, see [2].

(4) It appears that the (finite) quotient module  $Q(G) = I_{K_\infty}/\mathfrak{a}_G I_{K_\infty}$  can quickly become very large. Arguments from commutative algebra and calculations show that for example in the homogeneous case with  $n = 1$ ,  $p = 3$  and  $s = 5$  ( $s = 6$ ), the length of  $Q(G)$  is at least 1230 (13710 respectively). It also appears that in the homogeneous case with  $n = 1$  and any  $p$ , the length of  $Q(G)$  grows at least as fast as a positive constant times  $p^s$  for  $s \rightarrow \infty$ . We will treat this question in more detail in future work.

(5) The method to get Theorem 1.2 could probably be applied to certain cohomology groups of more general  $p$ -adic representations (or of motives) satisfying suitable properties. We will come back to this problem in the future.

(6) We can prove the case  $p = 2$  of Theorem 1.2 by the same method if we can establish the usual main conjecture for each character of  $G$ , replacing  $\Theta_{K_\infty/k,S}$  by  $2^{-[k:\mathbb{Q}]}\Theta_{K_\infty/k,S}$  under the assumption that  $\mu = 0$ . And indeed, it seems that Wiles' argument in [8] implies the usual main conjecture even for the case  $p = 2$  if  $\mu = 0$ . This means that Theorem 1.2 should hold even for the case  $p = 2$ , which we hope to be able to study in future work

Let us explain in which respect our equivariant main conjecture produces information that goes beyond the usual main conjecture, which treats the characteristic ideal of the  $\chi$ -component of  $X_{K_\infty,S}$  for any character  $\chi$  of  $\text{Gal}(K/k)$ . If we denote by  $K_\chi$  the *cyclic* extension of  $k$  corresponding to  $\chi$ , the characteristic ideal of the  $\chi$ -component is determined by  $X_{K_\chi,\infty,S}$ . In other words, the usual main conjecture contains only information on  $X_{K_\infty,S}$  for cyclic  $K/k$ , without even determining it completely as a module. Our equivariant main conjecture gives more precise information.

We will explain that our equivariant main conjecture even contains information on objects attached to the finite extension  $K/k$ . Let  $M_S/K$  be the maximal abelian pro- $p$  extension which is unramified outside  $S$ . We define  $\mathcal{G}_S$  by

$$\mathcal{G}_S = \text{Ker}(\text{Gal}(M_S/K) \longrightarrow \text{Gal}(K_\infty/K)),$$

which is a  $\mathbb{Z}_p[\text{Gal}(K/k)]$ -module. Let  $\text{Res}_{K_\infty/K} : \Lambda_{K_\infty} \rightarrow \mathbb{Z}_p[\text{Gal}(K/k)]$  be the natural map induced by the restriction. Then, we get from Theorem 1.2

**Corollary 1.5.**  $\text{Fitt}_{\mathbb{Z}_p[\text{Gal}(K/k)]}(\mathcal{G}_S) = \text{Res}_{K_\infty/K}(\mathfrak{a}_G I_{K_\infty} \Theta_{K_\infty/k,S}).$

In fact, taking the Galois coinvariants of  $X_{K_\infty,S}$ , we can apply the argument of Corollary 4.1 in [2] to get the above corollary. Note also that both sides of the above equation are in principle numerically computable.

**Example.** Take  $k = \mathbb{Q}$ ,  $p = 3$ , and  $\mathbb{Q}(\ell)$  the unique cubic extension of conductor  $\ell$  for any prime  $\ell \equiv 1 \pmod{3}$ .

In general, suppose that  $G = \text{Gal}(K/k) = (\mathbb{Z}/p\mathbb{Z})^{\oplus 2}$  (so  $s = 2$ ) and write

$$\Theta_{K_\infty/k,S} = \alpha_{-1} \frac{N_G}{T} + \alpha_0 + \alpha_1 T + \alpha_2 T^2 + \dots$$

with  $\alpha_{-1} \in \mathbb{Z}_p$ , and  $\alpha_i \in \mathbb{Z}_p[G]$  for all  $i \geq 0$ , where  $N_G = \sum_{\sigma \in G} \sigma$ . In this case, we have  $\mathfrak{a}_G = \mathfrak{m}_{K_\infty}$ , which implies

$$\text{Res}_{K_\infty/K}(\mathfrak{m}_{K_\infty} I_{K_\infty} \Theta_{K_\infty/k,S}) = \alpha_{-1} p N_G \mathbb{Z}_p[G] + \mathfrak{m}_G I_G \alpha_0,$$

where  $\mathfrak{m}_G$  and  $I_G$  are the maximal ideal and the augmentation ideal of  $\mathbb{Z}_p[G]$ , respectively.

We now take  $K$  to be the composite field of  $\mathbb{Q}(7)$  and  $\mathbb{Q}(13)$ , so  $K$  is the  $(\mathbb{Z}/3\mathbb{Z})^{\oplus 2}$ -extension of conductor 91. We denote by  $\sigma$  and  $\tau$  a generator of  $\text{Gal}(\mathbb{Q}(7)/\mathbb{Q})$  and  $\text{Gal}(\mathbb{Q}(13)/\mathbb{Q})$  respectively, and regard  $\sigma, \tau$  as generators of  $G$ . (Warning: Only in the present example, we use  $\sigma, \tau$  instead of  $\sigma_1, \sigma_2$  for generators of  $G$ . Notation will change later, and the generators of an abelian  $p$ -group will be written  $\sigma_1, \dots, \sigma_s$ , so  $\sigma$  becomes  $\sigma_1$  and  $\tau$  becomes  $\sigma_2$ , and we will set  $\tau_i = \sigma_i - 1$ .) In this concrete example,  $\alpha_{-1}$  is a unit, and  $\alpha_0$  is computed as

$$\alpha_0 \equiv 48 + 42\sigma + 38\sigma^2 + 62\tau + 42\sigma\tau + 80\sigma^2\tau + 45\tau^2 + 44\sigma\tau^2 + 70\sigma^2\tau^2 \pmod{3^4}$$

up to a unit factor. Put  $x = \sigma - 1$  and  $y = \tau - 1$  (again,  $x, y$  will be  $\tau_1, \tau_2$ , later). As a result, we can compute the right hand side of Corollary 1.5 as

$$(1) \quad \text{Res}_{K_\infty/K}(\mathfrak{m}_{K_\infty} I_{K_\infty} \Theta_{K_\infty/k,S}) = (27, 9x, 3y, xy^2, 6x^2 + x^2y).$$

Note that this is an ideal of finite index, and that ideals of this kind do not usually appear in Iwasawa theory.

Now we compute the left hand side of Corollary 1.5 directly. Using PARI-GP we find that

$$\mathcal{G}_S \simeq \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/9\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z},$$

and the actions of  $\sigma$  and  $\tau$  are described by the matrices

$$\begin{pmatrix} 1 & 4 & -3 & 0 \\ 0 & -2 & 3 & 0 \\ 0 & -4 & 4 & 0 \\ 3 & 3 & 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} -2 & -3 & 3 & 0 \\ 0 & 4 & 0 & 0 \\ -3 & 3 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

respectively. This means that when we take generators  $e_1, e_2, e_3, e_4$  of  $\mathcal{G}_S$  corresponding to the above decomposition, the actions of  $\sigma$  and  $\tau$  are

$$\sigma(e_1) = e_1 + 4e_2 - 3e_3, \quad \tau(e_1) = -2e_1 - 3e_2 + 3e_3, \dots \quad \text{etc.}$$



We would like to thank J. Nomura for computing the actions for us. Then some further computations show that  $\mathcal{G}_S$  has the relation matrix

$$\begin{pmatrix} 7x^2 - 6x & 3x - 3 & 0 \\ x & x & 0 \\ 3 + 3x & 0 & -x \\ 3 + y + 3x & -3 & 0 \\ 7xy - 3x & 3y & 0 \\ 6 + 3x & -y & 0 \\ 0 & 0 & y \\ 9 & 0 & 0 \\ 0 & 9 & 0 \\ 0 & 0 & 3 \end{pmatrix}$$

as a  $\mathbb{Z}_p[G]$ -module. Thus,  $\text{Fitt}_{\mathbb{Z}_p[G]}(\mathcal{G}_S)$  is the ideal generated by all  $3 \times 3$ -minors of the above matrix. We get

$$(2) \quad \text{Fitt}_{\mathbb{Z}_p[G]}(\mathcal{G}_S) = (27, 9x, 3y, xy^2, 6x^2 + x^2y).$$

For example, the determinant of the submatrix obtained by picking the 4-th, 6-th and 7-th row gives  $3y$  times a unit. In fact,  $-3y^2 - y^3 - 3xy^2 + 18y + 9xy = 3y(7 + 3x - xy)$  since we know  $y^3 = -3y - 3y^2$ , using  $(1 + y)^3 - 1 = 0$ . In this way, we can check Corollary 1.5 numerically, using (1) and (2). It does come out correctly, and this demonstrates that our theorem contains rather delicate information on  $\mathcal{G}_S$ .

The authors would like to thank both referees for their careful reading, and are particularly indebted to one of them for a long list of helpful comments and suggestions. The third author would like to thank F. Sudo for discussions on graph theory with him. The second author and the third author are partially supported by JSPS Core-to-core program, ‘‘Foundation of a Global Research Cooperative Center in Mathematics focused on Number Theory and Geometry’’.

## §2. The matrix $\tilde{M}_s$ and the minors

### 2.1. A free resolution of $\mathbb{Z}$

We consider the group  $G$  and the group ring  $R$  as in §1.1. The free resolution of  $\mathbb{Z}$  as an  $R$ -module

$$R^{s(s+1)(s+2)/6} \xrightarrow{\Phi_3} R^{s(s+1)/2} \xrightarrow{\Phi_2} R^s \xrightarrow{\Phi_1} R \longrightarrow \mathbb{Z} \longrightarrow 0$$

constructed in [2] §1.2 from the tensor products of group rings of cyclic groups can be described in the following way. We write  $(x_i)_{1 \leq i \leq s}$  for

the standard basis of  $R^s$ ,  $(x_i x_j)_{1 \leq i \leq j \leq s}$  for a basis of  $R^{s(s+1)/2}$ , and  $(x_i x_j x_k)_{1 \leq i \leq j \leq k \leq s}$  for a basis of  $R^{s(s+1)(s+2)/6}$ . Then  $\Phi_1$  is the homomorphism such that  $\Phi_1(x_i) = \tau_i$ , and  $\Phi_2$  is defined by  $\Phi_2(x_i^2) = \nu_i x_i$  and  $\Phi_2(x_i x_j) = \tau_i x_j - \tau_j x_i$  if  $i < j$ . The homomorphism  $\Phi_3$  is defined by

$$\begin{aligned}\Phi_3(x_i^3) &= \tau_i x_i^2, \\ \Phi_3(x_i^2 x_j) &= \tau_j x_i^2 + \nu_i x_i x_j \quad \text{if } i < j, \\ \Phi_3(x_i x_j^2) &= \tau_i x_j^2 - \nu_j x_i x_j \quad \text{if } i < j,\end{aligned}$$

and

$$\Phi_3(x_i x_j x_k) = \tau_i x_j x_k - \tau_j x_i x_k + \tau_k x_i x_j \quad \text{if } i < j < k.$$

We define an  $s(s+1)(s+2)/6$  by  $s(s+1)/2$  matrix  $\tilde{M}_s$  as the matrix corresponding to  $\Phi_3$ . The rows of  $\tilde{M}_s$  are labeled by  $x_i x_j x_k$ , and the columns are labeled by  $x_\ell x_n$ . In any one row there are at most 3 nonzero entries, so  $\tilde{M}_s$  is sparse. For an example, we refer the reader to subsection 1.2 of [2], where the matrix  $\tilde{M}_3$  is written out completely (see also the beginning of §4). We will study submatrices and minors of  $\tilde{M}_s$ . As in §1.1 we use the notation  $\mathfrak{m}_v$  to denote the ideal of  $R$  generated by all  $v$ -minors of the matrix  $\tilde{M}_s$ .

## 2.2. Admissible polynomials

We consider monomials  $\nu = \nu_1^{f_1} \cdots \nu_s^{f_s}$  in  $\nu_1, \dots, \nu_s \in R$ . We say  $\nu$  is *ordered* if  $f_1 \geq \dots \geq f_s$ . Also, we say it is *ordered and admissible* if it is ordered and the inequalities

$$\sum_{j=1}^i f_j \leq \sum_{j=1}^i (s-j)$$

are satisfied for all  $i$  such that  $1 \leq i \leq s$ . The right hand side equals the quantity  $\varphi(i)$  introduced in subsection 1.2.

We say  $\nu = \nu_1^{f_1} \cdots \nu_s^{f_s}$  is *admissible* if it is obtained from an ordered admissible monomial by permuting the  $\nu_i$ . If we take  $s = 4$ , then for example  $\nu_1^3 \nu_2^2 \nu_3$  is ordered and admissible,  $\nu_1 \nu_2^3 \nu_3^2$  is admissible but not ordered, and  $\nu_2^3 \nu_3^3$  is not admissible.

Let  $\mathcal{D}$  be the set of all doubletons in  $\{1, 2, \dots, s\}$ , and let  $\phi : \mathcal{D} \rightarrow \{1, 2, \dots, s\}$  any map satisfying  $\phi(D) \in D$  for all  $D \in \mathcal{D}$ . We called every such map a *selector* in [2]. A partial selector  $\psi$  is, by definition, a map from a subset  $\mathcal{D}_\psi$  of  $\mathcal{D}$  to  $\{1, 2, \dots, s\}$ , again satisfying the condition  $\psi(D) \in D$  whenever  $\psi(D)$  is defined. We define a monomial  $\nu(\psi)$  by  $\nu(\psi) = \prod_{D \in \mathcal{D}_\psi} \nu_{\psi(D)}$ .

**Lemma 2.1.** *Suppose that  $\nu = \nu_1^{f_1} \cdots \nu_s^{f_s}$  is admissible. Then there is a partial selector  $\psi : \mathcal{D}_\psi \rightarrow \{1, 2, \dots, s\}$  such that  $\nu = \nu(\psi)$ .*

*Proof.* Since  $\nu$  is admissible, we can take an admissible monomial  $\nu'$  which is of degree  $s(s-1)/2$  and which is a multiple of  $\nu$ . By permuting the  $\nu_i$  of  $\nu'$ , we have an ordered and admissible  $\nu''$ . By [2] Proposition 1.2, we know that there is a selector  $\phi$  such that  $\nu'' = \nu(\phi)$ . This implies that there is a selector  $\phi'$  satisfying  $\nu' = \nu(\phi')$ , and that there is a partial selector  $\psi$  satisfying  $\nu = \nu(\psi)$ . Q.E.D.

We note that our definition of “admissibility” in this paper is slightly different from that we gave in [2], but they are equivalent by Lemma 2.1 (see page 950 in [2]).

By Proposition 1.4 in [2] and the above Lemma 2.1, we know that if  $\nu = \nu_1^{f_1} \cdots \nu_s^{f_s}$  is admissible, then  $\pm\nu$  appears as a minor of  $\tilde{M}_s$ .

For an integer  $0 < d \leq s(s-1)/2$ , let  $\mathfrak{n}_d$  denote the ideal of  $R$  generated by all admissible monomials in  $\nu_1, \dots, \nu_s$  of degree  $d$ . We also define  $\mathfrak{n}_0 = R$  and  $\mathfrak{n}_{s(s-1)/2+1} = 0$ . Now we have explained all the notation in §1.1.

### §3. Proof of Theorem 1.2

In this section we prove Theorem 1.2, assuming Theorem 1.1. Let  $K/k$ ,  $S$ ,  $\Lambda_{K_\infty}$ ,  $X_{K_\infty, S}$ ,  $\Theta_{K_\infty/k, S}$  be as in §1.2. We write

$$\Lambda_{K_\infty} = \mathbb{Z}_p[G][[\text{Gal}(K_\infty/K)]] = \mathbb{Z}_p[G][[T]],$$

where  $1+T$  is a generator of  $\text{Gal}(K_\infty/K)$ . Let  $\sigma_1, \dots, \sigma_s$  be generators of  $G$  corresponding to the decomposition  $G \simeq \bigoplus_{i=1}^s \mathbb{Z}/p^{n_i}\mathbb{Z}$ . We define  $\tau_i = \sigma_i - 1$ ,  $\nu_i = N_{\langle \sigma_i \rangle}$  as above, and define  $\mathfrak{m}_v$  to be the ideal of  $\mathbb{Z}_p[G]$  generated by all  $v$ -minors of the matrix  $\tilde{M}_s$ . We note that  $\mathfrak{m}_v$  is an ideal of  $\mathbb{Z}_p[G]$  (not of  $\mathbb{Z}[G]$ ) in this section. We define an ideal  $\mathfrak{A}_G$  of  $\Lambda_{K_\infty}$  by

$$\mathfrak{A}_G = (\mathfrak{m}_{\frac{s(s-1)}{2}+1} T^{s-1} + \mathfrak{m}_{\frac{s(s-1)}{2}} T^s + \dots + \mathfrak{m}_1 T^{\frac{s(s+1)}{2}-1} + T^{\frac{s(s+1)}{2}} \mathbb{Z}_p[G]) \Lambda_{K_\infty}.$$

Suppose that  $\Omega^2 = \text{Ker}(\Phi_1 : \mathbb{Z}_p[G]^s \rightarrow \mathbb{Z}_p[G])$  where  $\Phi_1$  is defined as in the previous section, and regard  $\Omega^2$  as a  $\Lambda_{K_\infty}$ -module with the trivial action of  $T$  ( $Tx = 0$  for all  $x \in \Omega^2$ ). Then the meaning of this ideal  $\mathfrak{A}_G$  is explained by  $\mathfrak{A}_G = \text{Fitt}_{\Lambda_{K_\infty}}(\Omega^2)$ .

We proved in [3] Theorem 4.1 that

$$\text{Fitt}_{\Lambda_{K_\infty}}(X_{K_\infty, S}) = T^{1-s} \mathfrak{A}_G \Theta_{K_\infty/k, S}.$$

Thus what we have to prove is the following

**Proposition 3.1.** *Theorem 1.1 implies  $T^{1-s}\mathfrak{A}_G = \mathfrak{a}_G I_{K_\infty}$ .*

Let  $H = (\tau_1, \dots, \tau_s)$  be the ideal of  $\mathbb{Z}_p[G]$  generated by all  $\tau_i = \sigma_i - 1$ , and  $m_v$  as defined in §1.2. We suppose that  $\mathfrak{n}_d$  is an ideal of  $\mathbb{Z}_p[G]$  rather than of  $\mathbb{Z}[G]$ , namely it is an ideal of  $\mathbb{Z}_p[G]$  generated by all admissible  $\nu$ -monomials of degree  $d$ . We first prove two lemmas.

**Lemma 3.2.** *Let  $\text{aug} : \mathbb{Z}_p[G] \rightarrow \mathbb{Z}_p$  be the augmentation homomorphism. Then for any  $v$  such that  $0 \leq v \leq s(s-1)/2$  we have*

$$\text{aug}(\mathfrak{n}_v) = p^{m_v} \mathbb{Z}_p.$$

*Proof.* If  $v = 0$ , this follows from  $\mathfrak{n}_0 = \mathbb{Z}_p[G]$  and  $m_0 = 0$ . We suppose  $v > 0$ . We note that for every  $1 \leq \alpha \leq s$ ,

$$\nu_\alpha = 1 + (1 + \tau_\alpha) + \dots + (1 + \tau_\alpha)^{p^{n_\alpha} - 1} = p^{n_\alpha} + \tau_\alpha \beta_\alpha$$

for some  $\beta_\alpha \in \mathbb{Z}_p[G]$ . Thus we have  $\text{aug}(\nu_\alpha) = p^{n_\alpha}$ . For  $\nu = \nu_{a_1} \dots \nu_{a_v}$ , we have  $\text{aug}(\nu) = p^{c_\nu}$  where  $c_\nu = \sum_{w=1}^v n_{a_w}$ . Thus if  $\varphi(\alpha) < v \leq \varphi(\alpha + 1)$  for some  $\alpha$  with  $0 \leq \alpha \leq s-2$  and

$$(3) \quad \nu = \nu_1^{s-1} \dots \nu_\alpha^{s-\alpha} \nu_{\alpha+1}^{v-\varphi(\alpha)},$$

then  $\text{aug}(\nu) = p^{m_v}$ . Note that the above  $\nu$  is ordered and admissible.

On the other hand, if  $\nu$  is admissible and  $\text{aug}(\nu) = p^{c_\nu}$ , it follows from the definitions of  $m_v$  and of admissibility that  $c_\nu \geq m_v$ . Thus we get Lemma 3.2. Q.E.D.

**Lemma 3.3.** *We assume Theorem 1.1. Then for any integer  $v$  such that  $0 \leq v \leq s(s-1)/2$ , we have*

$$\mathfrak{m}_v = \sum_{d=0}^v p^{m_d} H^{v-d}.$$

*Proof.* By Theorem 1.1 we have

$$\mathfrak{m}_v = \sum_{d=0}^v \mathfrak{n}_d H^{v-d}.$$

Therefore, it is enough to prove

$$(4) \quad \sum_{d=0}^v \mathfrak{n}_d H^{v-d} = \sum_{d=0}^v p^{m_d} H^{v-d}.$$

We prove this equality by induction on  $v$ . First of all, if  $v = 0$ , then both sides are trivial and we get equality. Suppose that  $\nu = \nu_{a_1} \dots \nu_{a_v}$

is admissible. Since  $\text{aug}(\nu_{a_w}) = p^{n_{a_w}}$  for any  $w$  with  $1 \leq w \leq v$  as in the last lemma, we have

$$(5) \quad \nu = \nu_{a_1} \cdots \nu_{a_v} \in \prod_{w=1}^v (p^{n_{a_w}} \mathbb{Z}_p[G] + H) \subset \sum_{d=0}^v p^{m_d} H^{v-d}$$

by the argument of the proof of Lemma 3.2. Note that the second inclusion comes from  $\text{aug}(\mathfrak{n}_d) = p^{m_d} \mathbb{Z}_p$  ( $0 \leq d \leq v$ ), which is nothing but Lemma 3.2. This shows that  $\nu$  is in the right hand side of (4). Therefore,  $\mathfrak{n}_d$  is in the right hand side of (4). We have

$$(6) \quad \sum_{d=0}^{v-1} \mathfrak{n}_d H^{v-d} = H \sum_{d=0}^{v-1} \mathfrak{n}_d H^{v-1-d} = H \sum_{d=0}^{v-1} p^{m_d} H^{v-1-d} = \sum_{d=0}^{v-1} p^{m_d} H^{v-d}$$

where we used the inductive hypothesis to get the second equality. Thus we know that the left hand side of (4) is contained in the right hand side of (4).

On the other hand, if we take  $\nu$  as in (3), then  $\text{aug}(\nu) = p^{m_v}$  and (5) together with the equation (6) show that  $p^{m_v}$  is in the left hand side of (4). This together with (6) implies that the converse inclusion also holds. This completes the proof of Lemma 3.3. Q.E.D.

Now we prove Proposition 3.1. First of all, it follows from Theorem 1.1 that  $\mathfrak{m}_{\frac{s(s-1)}{2}+1} = H \mathfrak{m}_{\frac{s(s-1)}{2}}$ . Thus by the definition of  $\mathfrak{A}_G$  and Lemma 3.3, we have

$$\begin{aligned} T^{1-s} \mathfrak{A}_G &= \left( \sum_{v=0}^{\frac{s(s-1)}{2}} \mathfrak{m}_v T^{\frac{s(s-1)}{2}+1-v} + H \mathfrak{m}_{\frac{s(s-1)}{2}} \right) \Lambda_{K_\infty} \\ &= \left( \sum_{v=0}^{\frac{s(s-1)}{2}} \sum_{d=0}^v p^{m_d} H^{v-d} T^{\frac{s(s-1)}{2}+1-v} + H \sum_{d=0}^{\frac{s(s-1)}{2}} p^{m_d} H^{\frac{s(s-1)}{2}-d} \right) \Lambda_{K_\infty}. \end{aligned}$$

Since  $I_{K_\infty}$  is generated by  $H$  and  $T$ , we have

$$\begin{aligned} T^{1-s} \mathfrak{A}_G &= T \sum_{d=0}^{\frac{s(s-1)}{2}} p^{m_d} I_{K_\infty}^{\frac{s(s-1)}{2}-d} + H \sum_{d=0}^{\frac{s(s-1)}{2}} p^{m_d} H^{\frac{s(s-1)}{2}-d} \Lambda_{K_\infty} \\ &= I_{K_\infty} \sum_{d=0}^{\frac{s(s-1)}{2}} p^{m_d} I_{K_\infty}^{\frac{s(s-1)}{2}-d} \\ &= I_{K_\infty} \mathfrak{a}_G. \end{aligned}$$

Thus we have proved Proposition 3.1 and Theorem 1.2, assuming Theorem 1.1.

#### §4. Outline of the proof of Theorem 1.1

In the rest of this paper we prove Theorem 1.1. We compute the higher Fitting ideals of  $\Omega^2$ , using the relation matrix of  $\Phi_3$ . As we mentioned in §1.1, we only have to prove  $\mathfrak{m}_v \supset \sum_{d=0}^v H^{v-d} \mathfrak{n}_d$ . To show this inclusion, for an element  $x$  of the right hand side, we construct an explicit lower triangular submatrix of the relation matrix of  $\Phi_3$ , whose determinant is  $\pm x$ . Thus we may neglect the signs of entries of the relation matrix, and think of the matrix  $\tilde{M}_s$  in the following way. The row and the column labels of  $\tilde{M}_s$  are  $x_i x_j x_k$  and  $x_\ell x_n$ , respectively, which we denote, for simplicity, by  $ijk$  and  $\ell n$ , respectively.

In the  $i^3 = i \cdot i \cdot i$ -row, there is only one nonzero entry  $\tau_i$  in the  $i^2 = i \cdot i$ -column. In the  $i^2 \cdot j = i \cdot i \cdot j$ -row with  $i \neq j$ , there are only two nonzero entries:  $\tau_j$  in the  $i^2 = i \cdot i$ -column, and  $\nu_i$  in the  $i \cdot j$ -column. In the  $i \cdot j \cdot k$ -row with  $i < j < k$ , there are only three nonzero entries:  $\tau_k$  in the  $i \cdot j$ -column,  $\tau_j$  in the  $i \cdot k$ -column, and  $\tau_i$  in the  $j \cdot k$ -column. Therefore,  $\tilde{M}_s$  is roughly of the following form:

$$\begin{array}{l} \begin{matrix} 1 \cdot 1 \cdot 1 \\ \dots \\ s \cdot s \cdot s \\ 1 \cdot 1 \cdot 2 \\ \dots \\ (s-1) \cdot s \cdot s \\ 1 \cdot 2 \cdot 3 \\ \dots \\ (s-2) \cdot (s-1) \cdot s \end{matrix} \begin{pmatrix} \begin{matrix} 1 \cdot 1 & \dots & s \cdot s & 1 \cdot 2 & 1 \cdot 3 & \dots & 2 \cdot 3 & \dots & (s-1) \cdot s \end{matrix} \\ \tau_1 & & & & & & & & \\ & \dots & & & & & & & \\ & & \tau_s & & & & & & \\ \tau_2 & & & \nu_1 & & & & & \\ & \dots & & & & \dots & & \dots & \\ & & \tau_{s-1} & & & & & & \nu_s \\ & & & \tau_3 & \tau_2 & & \tau_1 & & \\ & & & & & \dots & & \dots & \\ & & & & & & & \dots & \tau_{s-2} \end{matrix} \end{pmatrix} . \end{array}$$

In the rest of this paper we assume  $s \geq 3$ . Put

$$t = \frac{s(s-1)}{2} + 1.$$

We fix  $0 \leq v \leq t$  and consider elements  $x \in H^{v-d} \mathfrak{n}_d$  (with  $0 \leq d \leq v$ ) of the form  $x = \tau(x)\nu(x)$ , where  $\tau(x)$  is any monomial in  $\tau_1, \dots, \tau_s$  of degree  $v-d$  and  $\nu(x)$  is any admissible monomial in  $\nu_1, \dots, \nu_s$  of

degree  $d$ . Sometimes  $\tau(x)$  (and  $\nu(x)$ ) will be called the  $\tau$ -part ( $\nu$ -part respectively) of  $x$ . For the proof of Theorem 1.1, we may assume that there is no index  $i$  such that  $\tau(x)$  contains the factor  $\tau_i$  and  $\nu(x)$  contains the factor  $\nu_i$ , since then  $x$  would be zero.

For any such monomial  $x$ , it is our plan to exhibit a square submatrix  $\mathcal{M}(x)$  of  $\tilde{M}_s$  which is lower triangular and whose determinant is  $x$ . Note that then the determinant is the product of all diagonal entries; these entries are of the form  $\tau_i$  or  $\nu_j$ , and hence the size of the matrix must equal the degree  $v$  of the given monomial  $x$ . It turns out that the essential difficulty is to handle the case where  $v = t$  (the maximal possible value); it will only take one paragraph at the very end of §9 to deduce the case  $v < t$  from this.

However, handling the case  $v = t$  is an arduous task and requires a series of intermediate steps. Let us try to outline these steps. We call  $x$  a  $\tau$ -monomial if  $x = \tau(x)$  in the above notation, that is,  $\nu(x) = 1$ . Similarly,  $x$  is a  $\nu$ -monomial if  $x = \nu(x)$ . In general,  $x$  will be a  $(\tau, \nu)$ -monomial, meaning that it contains factors  $\tau_i$  as well as  $\nu_j$ .

We first explain our proof for  $\tau$ -monomials. We consider the submatrix  $C_s$  of  $\tilde{M}_s$  whose row labels are  $ijk$  such that  $i, j, k$  are all distinct, and whose column labels are  $\ell n$  with  $\ell \neq n$ . This submatrix is in a fairly large southeastern part of  $\tilde{M}_s$ . We systematically construct lower triangular submatrices of  $C_s$ , which “realize”  $\tau$ -monomials  $x$  of relatively small degree.

As a first step (§5), we will construct lower triangular submatrices  $N_{j,S_j} = N_{j,S_j}(a_1, \dots, a_m)$ , which realize  $\tau$ -monomial of degree  $m \leq s - 2$ , where  $j$  is an integer  $3 \leq j \leq s$ ,  $a_1, \dots, a_m$  are certain integers in  $\{1, \dots, j-1\}$ , and  $S_j$  is a subset of  $\{1, \dots, s\}$ . Two important properties of this matrix is that (i)  $\det N_{j,S_j}(a_1, \dots, a_m) = \tau_{a_1} \dots \tau_{a_m}$ , and (ii) the column labels are  $b_j$  for some  $b$ 's. There is one more important property of this matrix, which we do not state here, see Proposition 5.2.

Using these submatrices in §5, we will realize in §7 an arbitrary  $\tau$ -monomial  $\tau$  of degree  $(s-1)(s-2)/2$  by constructing a submatrix  $T(\tau)$  of  $C_s$  (see Theorem 7.3). By the property (ii) we mentioned in the previous paragraph, the column labels of  $N_{3,S_3}, \dots, N_{s,S_s}$  are all distinct. Noting this, we construct  $T(\tau)$  by combining  $N_{3,S_3}, \dots, N_{s,S_s}$ . In this section there are two subcases. Case I occurs when  $\tau$  does not involve every factor  $\tau_1, \dots, \tau_s$ ; then a fairly straightforward combination of the submatrices  $N_{j,S_j}$  with  $S_j$  empty, produces the desired result. Case II is the case that all  $\tau_1, \dots, \tau_s$  divide  $\tau$ . This case is much harder and we need to make a careful choice of  $S_s$  with the help of graph theory. We give no details here but refer the reader to §7 and in particular to the example given there.

Next, in §8 we are able to raise the degree to the required maximum, namely to  $t$ , constructing a submatrix  $M(\tau)$  of  $\tilde{M}_s$ . Now we use submatrices outside  $C_s$  to construct  $M(\tau)$ , but the result in §7 we mentioned above plays the most important role.

We explain our proof for a general monomial  $x$ . If  $x$  is a  $\nu$ -monomial, the conclusion was already proved in the end of §2. So we assume that  $x$  is neither a  $\tau$ -monomial nor a  $\nu$ -monomial. In §6, we first slightly modify and extend the construction of §5: here we construct a submatrix  $N'_{j,S_j} = N'_{j,S_j}(a_1, \dots, a_{m'})$  of  $\tilde{M}_s$ , which realizes a monomial whose  $\tau$ -part is as in §5, and whose  $\nu$ -part is of the form  $\nu_j^f$  for arbitrary  $j$  (as in §5) and suitable exponent  $f$ . More precisely, we get  $\det N'_{j,S_j}(a_1, \dots, a_{m'}) = \nu_j^f \tau_{a_1} \cdots \tau_{a_{m'}}$ .

Finally, in §9 we combine the outcome of §§6 and 8 to treat general  $(\tau, \nu)$ -monomials  $x$  of degree  $t$ . To construct a submatrix  $\mathcal{M}(x)$  which realizes a general monomial  $x$ , we have to combine several  $N'_{j,S_j}$  with careful choices of  $S_j$ 's,  $M(\tau)$  in §8 for some  $\tau$  dividing the  $\tau$ -part of  $x$ , and several other submatrices of  $\tilde{M}_s$ . This will then complete the proof of Theorem 1.1.

## §5. Small $\tau$ -monomials

In this section we deal with certain  $\tau$ -monomials of relatively small degree. For this, we consider the submatrix  $C_s$  of  $\tilde{M}_s$  whose row labels are  $ijk$  with  $1 \leq i < j < k \leq s$  and whose column labels are  $\ell n$  with  $1 \leq \ell < n \leq s$ . This matrix  $C_s$  has  $s(s-1)(s-2)/6$  rows and  $s(s-1)/2$  columns. It occupies a large region in the south-east of the entire matrix  $\tilde{M}_s$ , which (let us recall) has format  $s(s+1)(s+2)/6$  by  $s(s+1)/2$ .

Suppose that  $j$  is an integer such that  $3 \leq j \leq s$  and fix it in this section. Let  $S$  be a subset of  $\{1, 2, \dots, j-1\}$ . We put  $m = j - 2 - \#S$ , and assume  $m > 0$ . The subset  $S$  may be empty. We consider a sequence of integers  $a_1, \dots, a_m$ . We say in this paper that an  $m$ -tuple  $(a_\mu)_{1 \leq \mu \leq m}$  is *cautiously increasing* if it is non-decreasing and never jumps by more than one; namely  $a_{\mu+1} - a_\mu = 0$  or  $1$  for all  $1 \leq \mu \leq m-1$ . Suppose that  $(a_\mu)_{1 \leq \mu \leq m}$  is cautiously increasing,  $1 \leq a_1 \leq a_m \leq j-1$ , and  $\{a_1, \dots, a_m\} \cap S$  is empty. We will construct in this section a certain submatrix  $N_{j,S}(a_1, \dots, a_m)$  of  $C_s$  (and hence of  $\tilde{M}_s$ ), which has determinant  $\tau_{a_1} \cdots \tau_{a_m}$ .

We arrange the numbers  $1, 2, \dots, j-1$  in the following order:

$$a_1, a_1 + 1, \dots, j-1, 1, 2, \dots, a_1 - 1,$$



and remove the elements in  $S$ . Let us call the resulting sequence

$$b_0, b_1, \dots, b_m.$$

Especially,  $b_0 = a_1$  since  $a_1$  is not in  $S$ . Note that  $(b_\mu)_{1 \leq \mu \leq m}$  depends only on  $a_1$  and  $S$ . We use  $(b_\mu)_{1 \leq \mu \leq m}$  for the construction of  $N_{j,S}(a_1, \dots, a_m)$ , but not  $b_0$ . We note that by definition if  $\mu \neq \rho$ , we have  $b_\mu \neq b_\rho$ .

**Lemma 5.1.** *For any  $\mu$  and  $\rho$  such that  $1 \leq \mu \leq m$  and  $\mu \leq \rho \leq m$ , we have  $a_\mu \neq b_\rho$ .*

*Proof.* Suppose at first that  $a_1 < b_\rho \leq a_m$ . Since  $a_1, \dots, a_m$  are not in  $S$  and cautiously increasing, we have  $b_1 = a_1 + 1, b_2 = a_1 + 2, \dots, b_\rho = a_1 + \rho$ . Since  $(a_\mu)$  is cautiously increasing, we have  $a_\mu \leq a_1 + \mu - 1$ . Thus we obtain

$$a_\mu \leq a_1 + \mu - 1 \leq a_1 + \rho - 1 < a_1 + \rho = b_\rho,$$

which implies  $a_\mu \neq b_\rho$ .

Next, if  $b_\rho > a_m$ , it is clear that  $a_\mu \neq b_\rho$  because  $a_\mu \leq a_m < b_\rho$ .

Finally, suppose that  $b_\rho \leq a_1$ . Since  $\rho \neq 0$ , we know  $b_\rho \neq a_1$  and get  $b_\rho < a_1 \leq a_\mu$ . Thus we obtain the conclusion. Q.E.D.

By Lemma 5.1 we have  $a_\mu \neq b_\mu$  for all  $1 \leq \mu \leq m$ . Since  $a_\mu, b_\mu < j$ , we know  $\#\{a_\mu, b_\mu, j\} = 3$  and  $\#\{b_\mu, j\} = 2$ . Therefore, we can pick a submatrix  $N = N_{j,S}(a_1, \dots, a_m)$  of  $C_s$  by specifying the row labels  $a_1 b_{1j}, a_2 b_{2j}, \dots, a_m b_{mj}$  and the column labels  $b_{1j}, b_{2j}, \dots, b_{mj}$ , in this exact order. Then the diagonal term at position  $(a_\mu b_{\mu j}, b_{\mu j})$  is  $\tau_{a_\mu}$ , since the  $\mu$ -th row label is  $a_\mu b_{\mu j}$  and the  $\mu$ -th column label is  $b_{\mu j}$ . Thus  $N_{j,S}(a_1, \dots, a_m)$  is the matrix of the form

$$\begin{matrix} & b_{1j} & b_{2j} & \dots & b_{mj} \\ a_1 b_{1j} & \tau_{a_1} & & & 0 \\ a_2 b_{2j} & & \tau_{a_2} & & \\ \dots & & & \dots & \\ a_m b_{mj} & * & & & \tau_{a_m} \end{matrix}.$$

If  $\mu < \rho$ , the  $(a_\mu b_{\mu j}, b_{\rho j})$ -entry of  $N$  is zero, since  $b_\rho \neq b_\mu$  and  $b_\rho \neq a_\mu$  by Lemma 5.1. This shows that the matrix  $N$  is lower triangular, and the product over the diagonal is  $\tau_{a_1} \cdots \tau_{a_m}$ . Thus we have obtained

**Proposition 5.2.** *Take  $S \subset \{1, 2, \dots, j-1\}$ , and a cautiously increasing sequence  $a_1, \dots, a_m$  of elements in  $\{1, 2, \dots, j-1\} \setminus S$  such that  $m = j-2-\#S > 0$ . Then the matrix  $N_{j,S}(a_1, \dots, a_m)$  is lower triangular and*

$$\det N_{j,S}(a_1, \dots, a_m) = \prod_{\mu=1}^m \tau_{a_\mu}.$$

*This matrix has no column labels  $a_1j$ , nor  $kj$  with  $k \in S$ . In other words, the column labels of  $N_{j,S}(a_1, \dots, a_m)$  are  $b_j$  with  $b \in \{1, \dots, j-1\} \setminus (S \cup \{a_1\})$ .*

**Example.** Take  $j = 10$ ,  $S = \{1, 7\}$  and  $N_{10,S}(3, 3, 3, 4, 4, 5)$ . Then, since

$$a_1 = a_2 = a_3 = 3 < a_4 = a_5 = 4 < a_6 = 5,$$

we find

$$b_1 = 4, b_2 = 5, b_3 = 6, b_4 = 8, b_5 = 9, b_6 = 2.$$

Therefore, the matrix  $N_{10,S}(3, 3, 3, 4, 4, 5)$  is

$$\begin{array}{cccccc} & 4 \cdot 10 & 5 \cdot 10 & 6 \cdot 10 & 8 \cdot 10 & 9 \cdot 10 & 2 \cdot 10 \\ \begin{array}{l} 3 \cdot 4 \cdot 10 \\ 3 \cdot 5 \cdot 10 \\ 3 \cdot 6 \cdot 10 \\ 4 \cdot 8 \cdot 10 \\ 4 \cdot 9 \cdot 10 \\ 5 \cdot 2 \cdot 10 \end{array} & \left( \begin{array}{cccccc} \tau_3 & & & & & 0 \\ & \tau_3 & & & & \\ & & \tau_3 & & & \\ \tau_8 & & & \tau_4 & & \\ \tau_9 & & & & \tau_4 & \\ & \tau_2 & & & & \tau_5 \end{array} \right) \end{array}.$$

## §6. Introducing a power of $\nu_j$

We construct a submatrix  $N'_{j,S}(a_1, \dots, a_{m'})$  of  $\tilde{M}_s$ , which is a modification of  $N_{j,S}(a_1, \dots, a_m)$  in the previous section. Note that this is no longer a submatrix of  $C_s$  since we will now use row labels of type  $b_jj$ , that is, with repeated numbers. The column labels we use, however, will still be “square-free”. The point will be that the determinant of our submatrix is a  $\tau$ -monomial as in the previous section multiplied by a power of a single element  $\nu_j$ . This will be used later to assemble much bigger matrices whose determinant involves powers of several  $\nu_j$ .

Let  $j, S \subset \{1, 2, \dots, j-1\}$  be as in the previous section. Suppose that  $a_1, \dots, a_{m'}$  is a cautiously increasing sequence of elements in  $\{1, 2, \dots, j-1\} \setminus S$  with  $m' \leq m = j-2-\#S$ .

Using  $a_1$  and  $S$ , we define a sequence  $b_0, \dots, b_m$  as in the previous section. Recall that  $\mu \mapsto b_\mu$  is a bijection from  $\{0, 1, \dots, m\}$  to

$\{1, 2, \dots, j-1\} \setminus S$ . Put  $f = m - m' + 1$ . We consider the square matrix  $N' = N'_{j,S}(a_1, \dots, a_{m'})$  of size  $m+1$  whose column labels are  $b_0j, b_1j, \dots, b_mj$  and whose row labels are  $b_0j^2, b_1j^2, \dots, b_{f-1}j^2, a_1b_fj, a_2b_{f+1}j, \dots, a_{m'}b_mj$ , in this exact order. Note that  $f + m' - 1 = m$ . We define  $(a'_\mu)_{1 \leq \mu \leq m}$  by  $a'_\mu = a_1$  for  $\mu = 1, \dots, f$ , and  $a'_\mu = a_{\mu-f+1}$  for any  $\mu$  such that  $f < \mu \leq m$ . Then  $N'$  has row labels  $b_0j^2, b_1j^2, \dots, b_{f-1}j^2, a'_fb_fj, a'_{f+1}b_{f+1}j, \dots, a'_mb_mj$ . By definition,  $(a'_\mu)_{1 \leq \mu \leq m}$  is cautiously increasing. We have

$$a'_\mu \neq b_\rho$$

for any  $\mu$  and  $\rho$  such that  $f \leq \mu \leq \rho \leq m$  by Lemma 5.1. Therefore,  $\#\{a'_\mu, b_\mu, j\} = 3$  and  $N'$  is certainly a submatrix of  $\tilde{M}_s$ . We see that  $N'$  is of the form

$$\begin{array}{l}
 b_0j^2 \\
 b_1j^2 \\
 \dots \\
 b_{f-1}j^2 \\
 a'_fb_fj \\
 a'_{f+1}b_{f+1}j \\
 \dots \\
 a'_mb_mj
 \end{array}
 \begin{pmatrix}
 b_0j & b_1j & \dots & b_{f-1}j & b_fj & b_{f+1}j & \dots & b_mj \\
 \nu_j & & & & & & & 0 \\
 & \nu_j & & & & & & \\
 & & \dots & & & & & \\
 & & & \nu_j & & & & \\
 & & & & \tau_{a_1} & & & \\
 & & & & & \tau_{a_2} & & \\
 & & & & & & \dots & \\
 * & & & & & & & \tau_{a_{m'}}
 \end{pmatrix}.$$

In the rows having labels  $b_0j^2, b_1j^2, \dots, b_{f-1}j^2$ , there is only one nonzero entry  $\nu_j$  at the diagonal position because  $b_\mu \neq j$ . Therefore, the above inequality  $a'_\mu \neq b_\rho$  implies that  $N'$  is lower triangular. Thus we have obtained

**Proposition 6.1.** *Take  $S \subset \{1, 2, \dots, j-1\}$ , and a cautiously increasing sequence  $a_1, \dots, a_{m'}$  of elements in  $\{1, 2, \dots, j-1\} \setminus S$  with  $m' \leq m = j - 2 - \#S$ . Then the matrix  $N'_{j,S}(a_1, \dots, a_{m'})$  is lower triangular and*

$$\det N'_{j,S}(a_1, \dots, a_{m'}) = \nu_j^f \prod_{\mu=1}^{m'} \tau_{a_\mu},$$

where  $f = m - m' + 1$ . This matrix  $N'_{j,S}(a_1, \dots, a_{m'})$  has no column labels  $kj$  with  $k \in S$ .

## §7. Bigger $\tau$ -monomials

In this section we exhibit lower triangular submatrices whose determinants are  $\tau$ -monomials of much higher degree than in section 5. We

do not quite reach the necessary maximal degree  $t = s(s-1)/2 + 1$  yet, but we save some room for later, only working within the submatrix  $C_s$  introduced earlier. The matrix  $T(\tau)$  constructed in this section plays an important role in later sections. We put

$$t_0 = \frac{(s-1)(s-2)}{2}.$$

Let  $\tau$  be a monomial of degree  $t_0$  in  $\tau_1, \dots, \tau_s$ ;

$$\tau = \tau_1^{e_1} \tau_2^{e_2} \cdots \tau_s^{e_s}.$$

We will construct a submatrix of  $C_s$  which is lower triangular and whose determinant is  $\tau$ . We say  $\tau$  is ordered if  $e_1 \geq \dots \geq e_s$  is satisfied.

We may and will assume  $\tau$  is ordered. Since the degree of  $\tau$  is  $t_0$ , we have

$$(7) \quad \sum_{i=1}^s e_i = t_0 = \frac{(s-1)(s-2)}{2}.$$

For a monomial  $x = \tau_{a_1} \tau_{a_2} \cdots \tau_{a_q}$  such that  $a_1 \leq \dots \leq a_q$  is satisfied, if  $y = \tau_{a_1} \cdots \tau_{a_\mu}$  and  $z = \tau_{a_{\mu+1}} \cdots \tau_{a_q}$  for some  $\mu$  with  $1 \leq \mu \leq q$ , we say that  $x = yz$  is an *ordered decomposition*. We make the ordered decomposition

$$\tau = \tau^{(3)} \tau^{(4)} \cdots \tau^{(s)}$$

such that the degree of  $\tau^{(j)}$  is  $j-2$  for any  $j$  with  $3 \leq j \leq s$ . This means that if we write

$$\tau = \tau_{a_1} \tau_{a_2} \cdots \tau_{a_{t_0}}$$

with  $a_1 \leq a_2 \leq \dots \leq a_{t_0}$ , then  $\tau^{(3)}, \dots, \tau^{(s)}$  are defined by

$$\begin{aligned} \tau^{(3)} &= \tau_{a_1}, \quad \tau^{(4)} = \tau_{a_2} \tau_{a_3}, \dots, \\ \tau^{(j)} &= \tau_{a_{d_j+1}} \tau_{a_{d_j+2}} \cdots \tau_{a_{d_j+j-2}}, \dots, \quad \tau^{(s)} = \tau_{a_{d_s+1}} \tau_{a_{d_s+2}} \cdots \tau_{a_{t_0}} \end{aligned}$$

where  $d_j = (j-2)(j-3)/2$ . Since  $\tau$  is ordered,  $(a_{d_j+n})_{1 \leq n \leq j-2}$  is cautiously increasing for all  $j$ .

**Lemma 7.1.** *For any  $j$  such that  $3 \leq j \leq s-1$ ,  $\tau^{(j)}$  consists of  $\tau_i$ 's with  $i \leq j-1$ .*

*Proof.* It is enough to prove

$$\sum_{i=1}^{j-1} e_i \geq d_{j+1} = \sum_{i=1}^{j-2} i = \frac{(j-1)(j-2)}{2}.$$

Since  $\tau$  is ordered, it follows from (7) that

$$\begin{aligned} \sum_{i=1}^{j-1} e_i &\geq \frac{(s-1)(s-2)}{2} \cdot \frac{j-1}{s} = \frac{(s-3)(j-1)}{2} + \frac{j-1}{s} \\ &> \frac{(s-3)(j-1)}{2} \geq \frac{(j-1)(j-2)}{2}. \end{aligned}$$

This completes the proof. Q.E.D.

**Case I.** We assume  $e_s = 0$ .

For any  $j$  such that  $3 \leq j \leq s$ , suppose that

$$\tau^{(j)} = \tau_{a_{d_j+1}} \tau_{a_{d_j+2}} \cdots \tau_{a_{d_j+j-2}}$$

as above. Then by Lemma 7.1 we have  $a_{d_j+1} \leq a_{d_j+2} \leq \cdots \leq a_{d_j+j-2} \leq j-1$  if  $j \leq s-1$ . For  $j = s$ , since  $e_s = 0$  by our assumption,  $\tau^{(j)}$  consists of  $\tau_m$ 's with  $m \leq s-1$ .

Therefore, noting that  $(a_{d_j+n})_{1 \leq n \leq j-2}$  is cautiously increasing, we can construct  $N_{j,S}(a_{d_j+1}, a_{d_j+2}, \dots, a_{d_j+j-2})$  with  $S = \emptyset$  (see §5) for any  $j$  such that  $3 \leq j \leq s$ . We denote this matrix by  $N_j(\tau^{(j)})$ .

We define

$$T(\tau) = \begin{pmatrix} N_3(\tau^{(3)}) & & & 0 \\ & N_4(\tau^{(4)}) & & \\ & & \cdots & \\ * & & & N_s(\tau^{(s)}) \end{pmatrix}$$

which is a submatrix of  $C_s$ .

If  $abj$  is a row label of  $T(\tau)$  for some  $a, b < j$ , then it is a row label of  $N_j(\tau^{(j)})$ . For any  $j' > j$  and any  $k$ , the entry of  $(abj, kj')$  is zero because  $\{k, j'\} \not\subseteq \{a, b, j\}$ . This together with Proposition 5.2 shows that  $T(\tau)$  is lower triangular. It is clear from Proposition 5.2 that

$$\det T(\tau) = \tau^{(3)} \tau^{(4)} \cdots \tau^{(s)} = \tau.$$

**Case II.** We assume  $e_s > 0$ . We note that this condition together with the condition that  $\tau$  is ordered implies  $s \geq 5$ , since  $t_0 < s$  if  $s \leq 4$ . Note that no case  $s > 4$  was covered by the verifications done in [2]. By Lemma 7.1 we can define  $N_j(\tau^{(j)})$  for any  $j$  such that  $3 \leq j \leq s-1$  as in Case I.

In our arguments so far, we used row labels  $abj$  with  $a, b < j \leq s$  to produce factors  $\tau_a$  in the determinant. So this excludes  $a = s$ , which

means that in order to produce factors  $\tau_s$ , we have to resort to tricks. The row labels used for this will be  $abs$ , with corresponding column labels  $ab$ , and the pairs  $ab$  used for this have to be chosen with the utmost care, to control the interference with other rows and columns (some row labels  $abs$  have probably been used up already). We will have to use some graph theory at this point.

We put  $z = (s-2)(s-3)/2 = d_s$  and write

$$\tau^{(s)} = \tau_{a_{z+1}} \tau_{a_{z+2}} \cdots \tau_{a_{z+s-2}},$$

where  $a_{z+1}, a_{z+2}, \dots, a_{z+s-2}$  is cautiously increasing. By our assumption, we know  $a_{z+s-2} = a_{t_0} = s$ . Put  $s - \ell = a_{z+1}$  for some  $\ell \in \mathbb{Z}$ . Since  $a_{z+1}, a_{z+2}, \dots, a_{z+s-2}$  is cautiously increasing, we get

$$a_{z+1} \geq s - (s-2) + 1 = 3,$$

which implies  $\ell \leq s-3$ . Also, the inequality in the proof of Lemma 7.1 for  $j = s-1$  shows that

$$\sum_{i=1}^{s-2} e_i > \frac{(s-3)(s-2)}{2} = z,$$

which implies  $a_{z+1} \leq s-2$ . Therefore, we have  $2 \leq \ell \leq s-3$ .

Let  $m$  be the positive integer such that  $a_{z+m} = s-1$  and  $a_{z+m+1} = s$ . Since  $a_{z+m+1} = \dots = a_{z+s-2} = s$ , we have

$$(8) \quad e_s = s - 2 - m.$$

Since  $a_{z+1} = s - \ell$  and  $a_{z+m+1} = s$ , we know  $\ell = a_{z+m+1} - a_{z+1} \leq m$ , which implies

$$e_s + 1 = s - m - 1 \leq s - \ell - 1 < s - \ell.$$

Let  $j$  be an integer satisfying  $3 \leq j \leq s-1$ . We note that  $\tau^{(j)}$  begins with  $\tau_{a_{d_j+1}}$ , namely there is an ordered decomposition  $\tau^{(j)} = \tau_{a_{d_j+1}} \tau'$  for some  $\tau'$ . Then by Proposition 5.2,  $a_{d_j+1}j$  is not a column label of  $N_j(\tau^{(j)})$  for any  $j$ .

For an integer  $k$  such that  $3 \leq k \leq s-1$ , we consider an undirected graph  $G(k)$  whose vertices  $V(k)$  and edges  $E(k)$  are defined as follows:

$$V(k) = \{1, \dots, k\}, \quad E(k) = \{\{a_{d_j+1}j\} \mid 3 \leq j \leq k\} \cup \{\{12\}\}.$$

By induction on  $k$  we can show that  $G(k)$  has no closed path. Therefore, it is a *tree* and connected (see for example, [9] Theorem 3.1).

We consider the graph  $G(k)$  with  $k = s - \ell$ , namely  $G(s - \ell)$ . Using the inequality  $s - \ell > e_s + 1$  which we showed above and the fact that  $G(s - \ell)$  is connected, we can take a subgraph  $G'$  of  $G(s - \ell)$  such that

- $G'$  is a tree (hence connected),
- $s - \ell$  is a vertex of  $G'$ ,
- the set  $V(G')$  of vertices of  $G'$  consists of  $e_s + 1$  elements, and
- the set  $E(G')$  of edges of  $G'$  consists of  $e_s$  elements.

We write

$$E(G') = \{\{h_1g_1\}, \dots, \{h_{e_s}g_{e_s}\}\}.$$

**Example.** Take  $s = 7$  and  $\tau = \tau_1^3\tau_2^2\tau_3^2\tau_4^2\tau_5^2\tau_6^2\tau_7^2$ . The degree of  $\tau$  is 15. By the ordered decomposition of  $\tau$ , we have  $\tau^{(3)} = \tau_1$ ,  $\tau^{(4)} = \tau_1^2$ ,  $\tau^{(5)} = \tau_2^2\tau_3$ ,  $\tau^{(6)} = \tau_3\tau_4^2\tau_5$ , and  $\tau^{(7)} = \tau_5\tau_6^2\tau_7^2$ . Therefore,  $\ell = \#\{5, 6, 7\} - 1 = 3 - 1 = 2$ . The graph  $G(6)$  has edges

$$E(6) = \{\{12\}, \{13\}, \{14\}, \{25\}, \{36\}\}.$$

Certainly,  $G(6)$  is a tree. We consider  $G(5)$ . In this case there is a unique connected subgraph  $G'$  of  $G(5)$ , which has 3 vertices, and of which 5 is a vertex. Namely,  $G'$  has vertices  $V(G') = \{1, 2, 5\}$  and edges

$$E(G') = \{\{12\}, \{25\}\}.$$

So we can take  $h_1 = 1$ ,  $g_1 = 2$ ,  $h_2 = 2$ ,  $g_2 = 5$ .

In what follows, some of the row and column labels become a little complex. For better visibility, we sometimes put them between curly brackets  $\{ \}$ , that is, we sometimes use  $\{abc\}$ ,  $\{ab\}$  instead of  $abc$ ,  $ab$  for row and column labels.

We consider a matrix  $\mathcal{N}_{\tau,s}(G')$  whose row labels are  $\{h_\mu g_\mu s\}_{1 \leq \mu \leq e_s}$  and whose column labels are  $\{h_\mu g_\mu\}_{1 \leq \mu \leq e_s}$ . Since  $\{h_\mu g_\mu\}$  are all different, this is a submatrix of  $C_s$ . It is a diagonal matrix  $\tau_s I$  where  $I$  is the identity matrix;

$$\mathcal{N}_{\tau,s}(G') = \begin{matrix} & h_1g_1 & h_2g_2 & \dots & h_{e_s}g_{e_s} \\ \begin{matrix} h_1g_1s \\ h_2g_2s \\ \dots \\ h_{e_s}g_{e_s}s \end{matrix} & \begin{pmatrix} \tau_s & & & \\ & \tau_s & & \\ & & \dots & \\ & & & \tau_s \end{pmatrix} & \begin{matrix} \\ \\ \\ \mathbf{0} \end{matrix} \end{matrix}.$$

Next, we set  $S_{G'} = V(G') \setminus \{s - \ell\}$ . Then we have  $\#S_{G'} = e_s + 1 - 1 = e_s$ . It follows from (8) that

$$m = s - 2 - e_s = s - 2 - \#S_{G'}.$$

Therefore, we can define  $N_{s,S_{G'}}(a_{z+1}, a_{z+2}, \dots, a_{z+m})$ , which was constructed in §5 for  $j = s$  and  $S = S_{G'}$ . We put

$$N_{s,G'}(\tau^{(s)}) = N_{s,S_{G'}}(a_{z+1}, a_{z+2}, \dots, a_{z+m}).$$

**Lemma 7.2.** (i) For any  $\mu$  such that  $1 \leq \mu \leq e_s$ ,  $\{h_\mu g_\mu\}$  does not appear in the column labels of  $N_3(\tau^{(3)})$ ,  $N_4(\tau^{(4)})$ ,  $\dots$ ,  $N_{s-1}(\tau^{(s-1)})$ ,  $N_{s,G'}(\tau^{(s)})$ .

(ii) For any  $\mu$  such that  $1 \leq \mu \leq e_s$ ,  $\{h_\mu g_\mu s\}$  does not appear in the row labels of  $N_3(\tau^{(3)})$ ,  $N_4(\tau^{(4)})$ ,  $\dots$ ,  $N_{s-1}(\tau^{(s-1)})$ ,  $N_{s,G'}(\tau^{(s)})$ .

(iii) For any  $\mu$  such that  $1 \leq \mu \leq e_s$ , neither  $\{h_\mu s\}$  nor  $\{g_\mu s\}$  appears in the column labels of  $N_3(\tau^{(3)})$ ,  $N_4(\tau^{(4)})$ ,  $\dots$ ,  $N_{s-1}(\tau^{(s-1)})$ ,  $N_{s,G'}(\tau^{(s)})$ .

*Proof.* (i) By Proposition 5.2 and the definition of  $G(s-\ell)$ , no edge of  $G(s-\ell)$  appears in the column labels of  $N_3(\tau^{(3)})$ ,  $N_4(\tau^{(4)})$ ,  $\dots$ ,  $N_{s-1}(\tau^{(s-1)})$ . Since  $h_\mu, g_\mu \leq s-\ell < s$  and the column labels of  $N_{s,G'}(\tau^{(s)})$  are of the form  $\{bs\}$ ,  $\{h_\mu g_\mu\}$  is not a column label of  $N_{s,G'}(\tau^{(s)})$ . Thus we get the conclusion.

(ii) Since the row labels of  $N_j(\tau^{(j)})$  are of the form  $\{abj\}$ ,  $\{h_\mu g_\mu s\}$  cannot appear in the row labels of  $N_j(\tau^{(j)})$  for any  $j < s$ . Suppose that  $\{a_\rho b_\rho s\}$  is a row label of  $N_{s,G'}(\tau^{(s)})$ . Then by the definition of  $b_\rho$ , it is not in  $S_{G'} \cup \{s-\ell\}$ . Therefore, we have

$$(9) \quad b_\rho \notin \{h_\mu, g_\mu \mid \mu = 1, 2, \dots, e_s\}.$$

Thus we get  $\{h_\mu, g_\mu, s\} \neq \{a_\rho, b_\rho, s\}$ , which implies (ii).

(iii) Since the column labels of  $N_j(\tau^{(j)})$  are of the form  $\{bj\}$ , neither  $\{h_\mu s\}$  nor  $\{g_\mu s\}$  appears in the column labels of  $N_j(\tau^{(j)})$  for any  $j < s$ . For a column label  $\{b_\rho s\}$  of  $N_{s,G'}(\tau^{(s)})$ , by (9) we have  $h_\mu \neq b_\rho$  and  $g_\mu \neq b_\rho$  for any  $\mu$  such that  $1 \leq \mu \leq e_s$ . Thus neither  $\{h_\mu s\}$  nor  $\{g_\mu s\}$  appears in the column labels of  $N_{s,G'}(\tau^{(s)})$ . Q.E.D.

By Lemma 7.2 (i) and (ii), we can define  $T(\tau)$  by

$$T(\tau) = \begin{pmatrix} N_{\tau,s(G')} & & & & & 0 \\ & N_3(\tau^{(3)}) & & & & \\ & & N_4(\tau^{(4)}) & & & \\ & & & \dots & & \\ & & & & N_{s-1}(\tau^{(s-1)}) & \\ * & & & & & N_{s,G'}(\tau^{(s)}) \end{pmatrix},$$

which is a submatrix of  $C_s$ . It follows from Lemma 7.2 (iii) that there is only one nonzero entry in a  $h_\mu g_\mu s$ -row of the matrix  $T(\tau)$ . For  $j' > j$ ,



the  $(abj, kj')$ -entry with  $a, b < j$  is zero. Therefore, using Proposition 5.2, we know that  $T(\tau)$  is lower triangular.

Combining Cases I and II, we get

**Theorem 7.3.** *For any  $\tau$  which is a monomial in  $\tau_1, \dots, \tau_s$  of degree  $t_0 = (s-1)(s-2)/2$ , we can construct a submatrix  $T(\tau)$  of  $C_s$ , which is lower triangular and whose determinant is  $\tau$ . For the case  $\tau$  is ordered, an explicit construction of  $T(\tau)$  is given above.*

**Example.** Consider  $\tau = \tau_1^3 \tau_2^2 \tau_3^2 \tau_4^2 \tau_5^2 \tau_6^2 \tau_7^2$  for  $s = 7$  as above. Then  $T(\tau)$  is described as

$$\begin{array}{l} 1:27 \\ 2:57 \\ 1:23 \\ 1:24 \\ 1:34 \\ 2:35 \\ 2:45 \\ 3:15 \\ 3:46 \\ 4:56 \\ 4:16 \\ 5:26 \\ 5:67 \\ 6:37 \\ 6:47 \end{array} \begin{pmatrix} \tau_7 & & & & & & \\ & \tau_7 & & & & & \\ & \tau_3 & & \tau_1 & & & \\ & \tau_4 & & \tau_1 & & & \\ & & & & \tau_1 & & \\ & & \tau_3 & \tau_5 & & \tau_2 & \\ & & \tau_4 & & \tau_5 & \tau_2 & \\ & & & & & \tau_1 & \tau_3 \\ & & & & \tau_6 & & \tau_3 \\ & & & & & \tau_6 & \tau_5 & \tau_4 \\ & & & & & & \tau_1 & \tau_4 \\ & & & & & & & \tau_1 & \tau_4 \\ & \tau_6 & & & & & & \tau_2 & \tau_5 \\ & & & & & & & \tau_7 & \\ & & & & & & & & \tau_5 \\ & & & & & & & & \tau_3 & \tau_6 \\ & & & & & & & & \tau_4 & \tau_6 \end{pmatrix} \quad 0$$

### §8. The final step for $\tau$ -monomials

So far we have obtained  $\tau$ -monomials of degree  $t_0 = (s-1)(s-2)/2$ . In a final round we now consider a monomial in  $\tau_1, \dots, \tau_s$  of degree  $t$ . Recall that

$$t = \frac{s(s-1)}{2} + 1 = t_0 + s,$$

and that  $t$  is the final degree required in Theorem 1.1. We will construct a submatrix  $M(\tau)$  of  $\tilde{M}_s$  of size  $t$ , which is lower triangular and whose determinant is  $\tau$ .

As in the previous section, we may assume

$$\tau = \tau_1^{e_1} \tau_2^{e_2} \dots \tau_s^{e_s}$$

is ordered, namely  $e_1 \geq \dots \geq e_s$ . Note that we are assuming  $\sum_{i=1}^s e_i = t$ . We define  $r$  to be the positive integer such that  $e_r > 0$  and  $e_{r+1} = 0$  if  $e_s = 0$ . If  $e_s > 0$ , we define  $r = s$ . We put

$$\tau' = \tau_1^{e_1-1} \tau_2^{e_2-1} \dots \tau_r^{e_r-1},$$

which is also ordered.

At first we assume  $e_s = 0$ . Then  $r < s$  holds. We take the ordered decomposition  $\tau' = \tau(1)\tau(2)$  such that  $\tau(1)$ ,  $\tau(2)$  are monomials of degree  $t_0$ ,  $s - r$ , respectively.

We define a diagonal matrix  $A_r$  by

$$A_r = \begin{matrix} & 1 \cdot 1 & 2 \cdot 2 & \dots & r \cdot r \\ \begin{matrix} 1 \cdot 1 \cdot 1 \\ 2 \cdot 2 \cdot 2 \\ \\ r \cdot r \cdot r \end{matrix} & \left( \begin{array}{cccc} \tau_1 & & & \\ & \tau_2 & & \\ & & & \\ & & & \tau_r \end{array} \right) & \begin{matrix} \\ \\ \\ \mathbf{0} \end{matrix} \end{matrix}$$

which is a submatrix of  $\tilde{M}_s$ .

Suppose that  $\tau(2) = \tau_{a_1^{(2)}} \tau_{a_2^{(2)}} \dots \tau_{a_{s-r}^{(2)}}$ . Let us now define a diagonal matrix  $B_{r+1,s}(\tau(2)) = B_{r+1,s}(a_1^{(2)}, \dots, a_{s-r}^{(2)})$  by

$$B_{r+1,s}(\tau(2)) = \begin{matrix} & (r+1)^2 & (r+2)^2 & \dots & s^2 \\ \begin{matrix} a_1^{(2)} \cdot (r+1)^2 \\ a_2^{(2)} \cdot (r+2)^2 \\ \\ a_{s-r}^{(2)} \cdot s^2 \end{matrix} & \left( \begin{array}{cccc} \tau_{a_1^{(2)}} & & & \\ & \tau_{a_2^{(2)}} & & \\ & & & \\ & & & \tau_{a_{s-r}^{(2)}} \end{array} \right) & \begin{matrix} \\ \\ \\ \mathbf{0} \end{matrix} \end{matrix}$$

where we wrote  $j^2$  for  $j \cdot j$ . We note that  $a_n^{(2)}$  with  $1 \leq n \leq s - r$  satisfies  $a_n^{(2)} < r + 1$ , which implies that  $B_{r+1,s}(\tau(2))$  is a submatrix of  $\tilde{M}_s$ . Clearly, the determinant of  $B_{r+1,s}(\tau(2))$  is  $\tau(2)$ .

We now have

$$\tau = \tau_1 \dots \tau_r \tau(1) \tau(2)$$

with  $\deg \tau(1) = t_0$  and  $\deg \tau(2) = s - r$ . We also note that  $\tau(1)$  is ordered. Therefore, as we explained in §7, we can construct a lower triangular matrix  $T(\tau(1))$  with  $\det T(\tau(1)) = \tau(1)$ . We define  $M(\tau)$  by

$$M(\tau) = \begin{pmatrix} A_r & C_1 & C_2 \\ C_3 & T(\tau(1)) & C_4 \\ C_5 & * & B_{r+1,s}(\tau(2)) \end{pmatrix}.$$

Since the rows of  $A_r$ ,  $T(\tau(1))$ ,  $B_{r+1,s}(\tau(2))$  are all distinct and the columns of these three matrices are also all distinct,  $M(\tau)$  is a submatrix of  $\tilde{M}_s$ . Since  $\{i^2\}$  does not appear in the column labels of  $T(\tau(1))$  for any  $i$  with  $1 \leq i \leq s$ , we know  $C_1 = 0$ . If  $1 \leq i \leq r$ ,  $\{i^2\}$  does not appear in the column labels of  $B_{r+1,s}(\tau(2))$ , which implies  $C_2 = 0$ . Also, no row label of the form  $\{i^2j\}$  appears among the row labels of  $T(\tau(1))$  for any  $i, j$  with  $1 \leq i, j \leq s$ , which implies  $C_3 = 0$  and  $C_4 = 0$ . If  $1 \leq i \leq r$ , no row label of the form  $\{i^2j\}$  appears among the row labels of  $B_{r+1,s}(\tau(2))$ . This shows that  $C_5 = 0$ . It follows that  $M(\tau)$  is lower triangular, and

$$\begin{aligned} \det M(\tau) &= \det A_r \det T(\tau(1)) \det B_{r+1,s}(\tau(2)) \\ &= \tau_1 \cdots \tau_r \tau(1) \tau(2) = \tau . \end{aligned}$$

Next, we assume  $e_s > 0$ . In this case, we have  $r = s$ , and the degree of  $\tau' = \tau_1^{e_1-1} \cdots \tau_s^{e_s-1}$  is  $t_0$ . Therefore, by the method of §7 we can construct a lower triangular matrix  $T(\tau')$  with  $\det T(\tau') = \tau'$ .

We let  $A_s$  be the matrix  $A_r$  defined above with  $r = s$ , and define  $M(\tau)$  by

$$M(\tau) = \begin{pmatrix} A_s & C_1 \\ C_2 & T(\tau') \end{pmatrix},$$

which is a submatrix of  $\tilde{M}_s$ . By the same method as in the case  $e_s = 0$ , we can show that  $C_1 = 0$ ,  $C_2 = 0$ , and  $M(\tau)$  is lower triangular. Also, we have

$$\det M(\tau) = \tau_1 \cdots \tau_s \tau' = \tau.$$

For any monomial  $\tau$  in  $\tau_1, \dots, \tau_s$  of degree  $t$  without assuming it is ordered, it is clear by symmetry that we can construct a submatrix of  $\tilde{M}_s$ , which is lower triangular, and whose determinant is  $\tau$ . Thus we obtain

**Proposition 8.1.** *For any  $\tau$  which is a monomial in  $\tau_1, \dots, \tau_s$  of degree  $t = \frac{s(s-1)}{2} + 1$ , we can construct a submatrix  $M(\tau)$  of  $\tilde{M}_s$ , which is lower triangular, and whose determinant is  $\tau$ . Above, we gave an explicit method of constructing  $M(\tau)$ , assuming  $\tau$  is ordered.*

## §9. Synthesis: General $(\tau, \nu)$ -monomials

We now assemble our previous constructions, as the final step of the proof of Theorem 1.1. We now work on monomials  $x$  in  $\tau_1, \dots, \tau_s$  and  $\nu_1, \dots, \nu_s$  of degree  $t = \frac{s(s-1)}{2} + 1$ . Every such monomial  $x$  factors

uniquely as  $x = \tau(x)\nu(x)$  where  $\tau(x)$  is a product of factors  $\tau_i$  and  $\nu(x)$  is a product of factors  $\nu_j$ . We call  $\tau(x)$  and  $\nu(x)$  the  $\tau$ -part and the  $\nu$ -part of  $x$ , respectively. Recall that  $\tau_i\nu_i = 0$  for all  $i$  with  $1 \leq i \leq s$ . As said earlier, the case of monomials of degree less than  $t$  will be dealt with at the very end.

For a  $\nu$ -monomial  $\nu = \nu_1^{f_1}\nu_2^{f_2}\cdots\nu_s^{f_s}$ , we call  $\nu$  *anti-ordered admissible* if  $f_1 \leq \dots \leq f_s$  and

$$\sum_{j=i}^s f_j \leq \sum_{j=1}^{s+1-i} (s-j)$$

for all  $1 \leq i \leq s$ . Clearly, a monomial which is anti-ordered admissible is admissible.

It is our goal to construct, for every  $x$  of degree  $t$  such that  $\nu(x)$  is admissible, a lower triangular submatrix of  $\tilde{M}_s$  whose determinant is  $x$ . To achieve our goal, we may assume that both  $\tau(x)$  and  $\nu(x)$  are nontrivial, because the cases  $\nu(x) = 1$ ,  $\tau(x) = 1$  were already proved in Proposition 8.1 and in Proposition 1.4 in [2] (see also the end of §2), respectively. Also, by symmetry and  $\tau_i\nu_i = 0$ , we may assume

$$x = \tau_1^{e_1}\tau_2^{e_2}\cdots\tau_r^{e_r}\nu_g^{f_g}\nu_{g+1}^{f_{g+1}}\cdots\nu_s^{f_s}$$

with  $1 \leq r < g \leq s$ . By symmetry we may also assume

$$(10) \quad e_1 \geq e_2 \geq \dots \geq e_r > 0, \quad 0 < f_g \leq f_{g+1} \leq \dots \leq f_s,$$

and  $\nu(x) = \nu_g^{f_g}\nu_{g+1}^{f_{g+1}}\cdots\nu_s^{f_s}$  is anti-ordered admissible.

Assuming this, we will construct a submatrix  $M(x)$  of  $\tilde{M}_s$ , which is lower triangular, and whose determinant is  $x$ .

For  $\nu = \nu(x) = \nu_g^{f_g}\nu_{g+1}^{f_{g+1}}\cdots\nu_s^{f_s}$ , the existence of a partial selector for  $\nu$  implies the following lemma.

**Lemma 9.1.** *The  $\nu$ -part of  $x$  can be written as*

$$\nu = \nu(x) = \nu^{(g)}\nu^{(g+1)}\cdots\nu^{(s)}$$

such that for all  $j$  satisfying  $g \leq j \leq s$ ,

$$\deg \nu^{(j)} \leq j - 1$$

and

$$\nu^{(j)} = \nu_{a_{j1}}\nu_{a_{j2}}\cdots\nu_{a_{jr_j}}\nu_j^{f'_j}$$

for some non-negative integer  $r_j \in \mathbb{Z}_{\geq 0}$  and positive integer  $f'_j \in \mathbb{Z}_{>0}$ , and some  $(a_{jk})_{1 \leq k \leq r_j}$  such that  $g \leq a_{j1} < a_{j2} < \dots < a_{jr_j} < j$ .

*Proof.* By Lemma 2.1, there is a partial selector  $\psi : \mathcal{D}_\psi \rightarrow \{g, g+1, \dots, s\}$  corresponding to  $\nu$ . If it is needed, since  $g \geq 2$ , we can change  $\psi$  to  $\psi'$  such that  $\nu(\psi') = \nu(\psi) = \nu$  and that for any  $j$  such that  $g \leq j \leq s$ , there is  $i$  with  $1 \leq i < j$ ,  $\{i, j\} \in \mathcal{D}_{\psi'}$ , and  $\psi'(\{i, j\}) = j$ . In fact, if for some  $j$  there is no  $i$  satisfying the above, then since  $f_j > 0$  and  $\{i, j\} \in \mathcal{D}_\psi$  for some  $i$  with  $\psi(\{i, j\}) = j$ , we can take  $\psi'$  obtained from  $\psi$  by removing  $\{i, j\}$  from  $\mathcal{D}_\psi$  and adding  $\{1, j\} \in \mathcal{D}_{\psi'}$  with  $\psi'(\{1, j\}) = j$ .

For any  $j$  with  $g \leq j \leq s$ , we define

$$\nu^{(j)} = \prod_{\substack{i=1 \\ \{i, j\} \in \mathcal{D}_{\psi'}}}^{j-1} \nu_{\psi'(\{i, j\})}.$$

Then  $\nu^{(j)}$  satisfies the conditions in Lemma 9.1, in particular we have  $\deg \nu^{(j)} \leq j-1$  and  $f'_j > 0$ . Q.E.D.

**Example.** Consider  $\nu = \nu_2 \nu_3^4 \nu_4^4 \nu_5^4 \nu_6^4 \nu_7^4$  for  $s = 7$ . This  $\nu$  is admissible. For this  $\nu$ , we can decompose

$$\nu^{(2)} = \nu_2, \nu^{(3)} = \nu_3^2, \nu^{(4)} = \nu_4^3, \nu^{(5)} = \nu_5^4, \nu^{(6)} = \nu_3 \nu_6^4, \nu^{(7)} = \nu_3 \nu_4 \nu_7^4.$$

We decompose  $\nu$  as in Lemma 9.1, and put

$$m_j = j - 1 - \deg \nu^{(j)}$$

for all  $j$  such that  $g \leq j \leq s$ . Noting  $f'_j > 0$  in Lemma 9.1, we have  $\deg \nu^{(j)} > 0$ , which implies

$$0 \leq m_j \leq j - 2.$$

We put

$$\tau = \tau(x) = \tau_1^{e_1} \tau_2^{e_2} \dots \tau_r^{e_r}.$$

Then we get

$$\begin{aligned} \sum_{j=g}^s m_j &= \sum_{j=g}^s (j-1) - \deg \nu = \sum_{j=g}^s (j-1) - \left( \frac{s(s-1)}{2} + 1 - \deg \tau \right) \\ &= \deg \tau - \left( \frac{(g-1)(g-2)}{2} + 1 \right). \end{aligned}$$

Therefore, we can write down the ordered decomposition

$$\tau = \tau^{(g-1)} \tau^{(g)} \tau^{(g+1)} \dots \tau^{(s)}$$

such that  $\deg \tau^{(g-1)} = \frac{(g-1)(g-2)}{2} + 1$  and

$$\deg \tau^{(j)} = m_j$$

for any  $j$  such that  $g \leq j \leq s$ .

For each  $j$  with  $g \leq j \leq s$ , we take  $\tau^{(j)}$ ,  $\nu^{(j)}$  as above, in particular  $\nu^{(j)}$  as in Lemma 9.1;

$$\nu^{(j)} = \nu_{a_{j1}} \nu_{a_{j2}} \cdots \nu_{a_{jr_j}} \nu_j^{f'_j}.$$

We write

$$\tau^{(j)} = \tau_{n_{j1}} \tau_{n_{j2}} \cdots \tau_{n_{jm_j}}$$

with  $n_{j1} \leq \cdots \leq n_{jm_j}$ .

We define  $S_j$  by

$$S_j = \{a_{j1}, \dots, a_{jr_j}\},$$

which is a set of  $r_j$  elements. By definition, we have

$$\begin{aligned} m_j + f'_j - 1 &= j - 1 - \deg \nu^{(j)} + f'_j - 1 \\ &= j - 1 - (f'_j + r_j) + f'_j - 1 \\ &= j - 2 - \#S_j. \end{aligned}$$

Therefore,  $m_j \leq j - 2 - \#S_j$ , and we can consider  $N'_{j,S_j}(n_{j1}, \dots, n_{jm_j})$ , which is defined in §6. It is lower triangular and

$$\det N'_{j,S_j}(n_{j1}, \dots, n_{jm_j}) = \nu_j^{f'_j} \tau_{n_{j1}} \tau_{n_{j2}} \cdots \tau_{n_{jm_j}}$$

by Proposition 6.1 and  $f'_j = (j - 2 - \#S_j) - m_j + 1$ .

To the matrix  $N'_{j,S_j}(n_{j1}, \dots, n_{jm_j})$ , we now add rows labeled  $\{a_{j\mu}^2 j\}$  and also columns labeled  $\{a_{j\mu} j\}$  for  $1 \leq \mu \leq r_j$  as follows:

$$a_{j1}^2 j \begin{pmatrix} a_{j1} j & \cdots & a_{jr_j} j & & & \\ \nu_{a_{j1}} & & & & & \\ \cdots & \cdots & & & & \\ a_{jr_j}^2 j & & \nu_{a_{jr_j}} & & & \\ & & & & & \\ * & & & & N'_{j,S_j}(n_{j1}, \dots, n_{jm_j}) & \\ & & & & & & 0 \end{pmatrix}.$$

First of all, the labels  $\{a_{j1} j\}, \dots, \{a_{jr_j} j\}$  do not appear among the column labels of  $N'_{j,S_j}(n_{j1}, \dots, n_{jm_j})$ , and the labels  $\{a_{j1}^2 j\}, \dots, \{a_{jr_j}^2 j\}$  do

not appear among the row labels of  $N'_{j,S_j}(n_{j1}, \dots, n_{jm_j})$ . Therefore, the above matrix is a submatrix of  $\tilde{M}_s$ . We call this matrix  $\mathcal{M}_j(\nu^{(j)}, \tau^{(j)})$ .

In the rows with index  $\{a_{ji}^2, j\}$  the only nonzero entry sits at the diagonal position. This together with the fact that  $N'_{j,S_j}(n_{j1}, \dots, n_{jm_j})$  is lower triangular implies that  $\mathcal{M}_j(\nu^{(j)}, \tau^{(j)})$  is also lower triangular. We have

$$\begin{aligned} \det \mathcal{M}_j(\nu^{(j)}, \tau^{(j)}) &= \nu_{a_{j1}} \nu_{a_{j2}} \cdots \nu_{a_{jr_j}} \nu_j^{f'_j} \tau_{n_{j1}} \tau_{n_{j2}} \cdots \tau_{n_{jm_j}} \\ &= \nu^{(j)} \tau^{(j)}. \end{aligned}$$

Since  $\tau^{(g-1)}$  is of degree  $\frac{(g-1)(g-2)}{2} + 1$  and ordered, by Proposition 8.1 we can build a lower triangular matrix  $M(\tau^{(g-1)})$  of degree  $\frac{(g-1)(g-2)}{2} + 1$ , whose row labels are of the form  $\{abc\}$  with  $a, b, c \leq g-1$ , and whose column labels are of the form  $\{bc\}$  with  $b, c \leq g-1$ .

For  $x$  as in (10) we define  $\mathcal{M}(x)$  by

$$\mathcal{M}(x) = \begin{pmatrix} M(\tau^{(g-1)}) & & & & 0 \\ & \mathcal{M}_g(\nu^{(g)}, \tau^{(g)}) & & & \\ & & \cdots & & \\ * & & & \cdots & \\ & & & & \mathcal{M}_s(\nu^{(s)}, \tau^{(s)}) \end{pmatrix}.$$

Suppose that  $\{abc\}$  is a row label of  $M(\tau^{(g-1)})$ . Then as we explained, since  $a, b, c \leq g-1$ , we have  $j \notin \{a, b, c\}$  for any  $j$  such that  $g \leq j \leq s$ . This shows that the column labels of  $\mathcal{M}(x)$  are all distinct, and so are the row labels. Thus  $\mathcal{M}(x)$  is a submatrix of  $\tilde{M}_s$ . Also, for any row label  $\{abc\}$  of  $M(\tau^{(g-1)})$  we have  $\{n, j\} \not\subset \{a, b, c\}$  for any  $j$  such that  $g \leq j \leq s$  and any  $n$ , and so  $\mathcal{M}(x)$  is lower triangular. By the construction of  $\mathcal{M}(x)$ , we get

$$\begin{aligned} \det \mathcal{M}(x) &= \det M(\tau^{(g-1)}) \prod_{j=g}^s \det \mathcal{M}_j(\nu^{(j)}, \tau^{(j)}) \\ &= \tau^{(g-1)} \prod_{j=g}^s \nu^{(j)} \tau^{(j)} = \tau \nu = x. \end{aligned}$$

Thus we finally obtain the following theorem.

**Theorem 9.2.** *Let  $x$  be a monomial in  $\tau_1, \dots, \tau_s$  and  $\nu_1, \dots, \nu_s$  of degree  $t = \frac{s(s-1)}{2} + 1$  satisfying the condition (10). Then we can construct a submatrix  $\mathcal{M}(x)$  of  $\tilde{M}_s$ , which is lower triangular, and whose determinant is  $x$ .*

By symmetry this theorem implies that any monomial  $x$  in  $\tau_1, \dots, \tau_s$  and  $\nu_1, \dots, \nu_s$  of degree  $t$  such that the  $\nu$ -part of  $x$  is admissible, we can construct a submatrix  $\mathcal{M}(x)$  of  $\tilde{M}_s$ , which is lower triangular, and whose determinant is  $x$ . Thus we have proved that

$$\mathfrak{m}_t \supset \sum_{d=0}^t H^{t-d} \mathfrak{n}_d .$$

To finish the proof, we now discuss the case where the monomial  $x$  has degree  $v < t$ . Let  $\tau(x)$  and  $\nu(x)$  be the  $\tau$ -part and the  $\nu$ -part of  $x$  respectively as usual. Let  $d$  be the degree of  $\nu(x)$ . Then  $d \leq v \leq t-1 = s(s-1)/2$ . Let  $e = v - d$  be the degree of  $\tau(x)$ , so  $e + d = v$ . First let us note that the case  $e = 0$  need not be considered for the following reason. If  $e = 0$ , then  $x$  is a  $\nu$ -monomial, and admissible. It was already shown in Proposition 1.4 of [2] and Lemma 2.1 that all admissible  $\nu$ -monomials can be obtained as minors of  $\tilde{M}_s$  (see the end of §2). Hence we may assume that  $e > 0$ , so the  $\tau$ -part of  $x$  contains a factor  $\tau_i$ , say. We then define  $\tilde{x} = \tau_i^{t-v} \cdot x$ . This is then of degree  $t$ . (Note that  $\tilde{x}$  will not be zero since the  $\nu$ -part of  $x$  has no factor  $\nu_i$ , otherwise we would already have  $x = 0$ .) By Theorem 9.2 and the remark following it, there is a lower triangular  $t \times t$  submatrix of  $\tilde{M}_s$  whose determinant (= product over the diagonal) is  $\tilde{x}$ . Since  $x$  is a monomial of degree  $v$  dividing  $\tilde{x}$ , we can extract a  $v \times v$  matrix  $\mathcal{M}(x)$  from  $\mathcal{M}(\tilde{x})$  such that  $\det(\mathcal{M}(x)) = x$ , simply by deleting rows and columns corresponding to factors  $\tau_i$  that sit on the diagonal of  $\mathcal{M}(\tilde{x})$  and that appear in  $\tilde{x}$  but not in  $x$ . This means that we have established the inclusion  $\mathfrak{m}_v \supset \sum_{d=0}^v H^{v-d} \mathfrak{n}_d$  for any  $v \leq t$ , and this completes at last the proof of Theorem 1.1.

## References

- [1] D. Burns, M. Kurihara, T. Sano, On zeta elements for  $\mathbb{G}_m$ , *Documenta Math.* **21** (2016), 555-626.
- [2] C. Greither and M. Kurihara, Tate sequences and Fitting ideals of Iwasawa modules, “Vostokov volume”, *Algebra i Analiz* **27** (2015) 117-149, *St. Petersburg Math. J.* **27** (2016), 941-965.
- [3] C. Greither and M. Kurihara, Fitting ideals of Iwasawa modules and of the dual of class groups, “Shinoda volume”, *Tokyo Journal of Mathematics* **39** (2016), 619-642.
- [4] C. Greither and C. Popescu, An Equivariant Main Conjecture in Iwasawa Theory and Applications, *J. Algebraic Geometry*, **24** (2015), 629-692.
- [5] D. G. Northcott, *Finite free resolutions*, Cambridge Univ. Press, Cambridge New York 1976.



- [ 6 ] J.-P. Serre, Sur le résidu de la fonction zêta  $p$ -adique, *Comptes Rendus Acad. Sc. Paris*, **287** (1978), Série A, 183-188.
- [ 7 ] H. Tokio, On a conjecture of a matrix which appears in a refined Iwasawa theory (in Japanese), master's thesis, Keio University (2016).
- [ 8 ] A. Wiles, The Iwasawa conjecture for totally real fields, *Ann. Math.* **131** (1990), 493-540.
- [ 9 ] Robin J. Wilson, *Introduction to Graph Theory*, Fifth Edition, Pearson, London New York 2010

*Institut für Theoretische Informatik und Mathematik, Universität der Bundeswehr, München, 85577 Neubiberg, Germany*  
E-mail address: `cornelius.greither@unibw.de`

*Department of Mathematics, Faculty of Science and Technology, Keio University, 3-14-1 Hiyoshi, Kohoku-ku, Yokohama, 223-8522, Japan*  
E-mail address: `kurihara@math.keio.ac.jp`  
E-mail address: `tokiohibiki@a2.keio.jp`