



ANNALES

DE

L'INSTITUT FOURIER

Cornelius GREITHER & Rádiu KUČERA

The lifted root number conjecture for fields of prime degree over the rationals: an approach via trees and Euler systems

Tome 52, n° 3 (2002), p. 735-777.

http://aif.cedram.org/item?id=AIF_2002__52_3_735_0

© Association des Annales de l'institut Fourier, 2002, tous droits réservés.

L'accès aux articles de la revue « Annales de l'institut Fourier » (<http://aif.cedram.org/>), implique l'accord avec les conditions générales d'utilisation (<http://aif.cedram.org/legal/>). Toute reproduction en tout ou partie cet article sous quelque forme que ce soit pour tout usage autre que l'utilisation à fin strictement personnelle du copiste est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

cedram

*Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
<http://www.cedram.org/>*

**THE LIFTED ROOT NUMBER CONJECTURE
FOR FIELDS OF PRIME DEGREE
OVER THE RATIONALS:
AN APPROACH VIA TREES AND EULER SYSTEMS**

by C. GREITHER and R. KUČERA

Introduction.

For any G -Galois extension K/F of number fields, Chinburg defined in [Ch] an invariant $\Omega = \Omega(3, K/F)$ in the class group of the integral group ring $\mathbb{Z}[G]$. The so-called Root Number Conjecture (RNC for short) states that Ω is the root number class; in particular Ω is conjecturally zero if G is abelian or of odd order. The invariant Ω measures, very roughly speaking, the discrepancy of Galois module structure between the unit group and the class group of K , but the actual description is much more subtle, involving the canonical class of K/F and so-called Tate sequences. Until the year 2000, the conjecture had only been proved in special cases, but not even for all K which are absolutely abelian. One problem is that the conjecture “does not localize well”.

In [GRW], a lifted invariant was presented. This new invariant, let us call it $\omega(K/F)$, exists if the Stark conjecture holds for K . It lies in a relative K -group $K_0T(\mathbb{Z}[G])$, and it maps to $\Omega(3, K/F)$ under the canonical epimorphism from the $K_0T(\mathbb{Z}[G])$ to the class group of $\mathbb{Z}[G]$. At least for absolutely abelian K , the lifted invariant exists, and the

so-called Lifted Root Number Conjecture (LRNC) states that it is zero. The lifted conjecture has the great advantage to localize well, that is, it is equivalent to a collection of local statements $\omega_p = 0$ with p running through all prime numbers. The reader may also consult the survey article [GRW1]. Burns and Flach [BF] introduced so-called equivariant Tamagawa numbers $T\Omega(\mathbb{Q}(0)_K, \mathbb{Z}[G])$, which are actually obtained from a more general construction by specializing to the motive $\mathbb{Q}(0)_K$, and Burns [Bu] has proved that $T\Omega(\mathbb{Q}(0)_K, \mathbb{Z}[G])$ agrees with $\omega(K/F)$ up to an involution of $\mathbb{Z}[G]$ when G is abelian and $\omega(K/F)$ is defined. So actually LRNC is a special case of the Equivariant Tamagawa Number Conjecture.

Ritter and Weiss [RW] proved that $\omega(K/F)$ is zero for the case that $F = \mathbb{Q}$ and K is abelian of prime degree l over \mathbb{Q} such that K/\mathbb{Q} is tame and at most 2 primes ramify in K . Our principal result (Theorem 6) removes the latter restriction: we prove LRNC for all K which are tame and abelian of odd prime degree over \mathbb{Q} , that is, we prove that $\omega(K/\mathbb{Q}) = 0$ for these fields. The tameness condition is presumably not necessary, but we have not done the extra calculations. Anyway, the only prime which might ramify wildly is l . In the whole paper we assume l to be odd, since for $l = 2$ there is no difference between the lifted and the unlifted conjecture. It should be mentioned here that in a very recent preprint [BG] of David Burns and the first-named author, a proof for LRNC up to its 2-primary part is given for *all* absolutely abelian fields K , using rather involved methods; but it is hoped that the explicit approach of the present paper retains some interest.

Unfortunately it would carry us way too far afield to develop the arithmetical interpretation of the Lifted Root Number Conjecture even in the fairly simple case that $F = \mathbb{Q}$ and K is abelian of (odd) prime degree l over \mathbb{Q} . For this, we have to refer to the paper [RW]. Suffice it to say that the unlifted conjecture is known to be true in this case since the so-called kernel group $D(\mathbb{Z}[G])$ is trivial and the Strong Stark conjecture is known for K ; and in order to pass from the unlifted to the lifted conjecture, one has to show that two integers c and c' agree modulo l .

This sounds modest, but already the definition of c and c' is not so simple. The number c is a determinant of a matrix constructed via local norm residue symbols, attached to the primes p_1, \dots, p_s which ramify in K and some auxiliary primes. The number c' , very roughly speaking, has to do with the way the classes $[\mathfrak{p}_1], \dots, [\mathfrak{p}_s]$ sit in the whole class group $cl(K)$ of K . (Here \mathfrak{p}_i denotes the unique prime of K above p_i .) Ultimately, c' will be calculated by finding the valuations at \mathfrak{p}_i of a certain λ -power root α_{s-1}

of the last element $\kappa_{s-1} \in K$ in a series of elements κ_j ($j \leq s-1$) attached to a suitable Euler system in K . Here λ denotes the element $\sigma - 1$, with σ a chosen generator of $G = \text{Gal}(K/\mathbb{Q})$, so by Hilbert 90, an element is a λ th power iff its norm is 1. The κ_i are (up to L -th powers, where L is a very high power of l) explicit circular numbers; but it is fairly complicated to extract higher λ -power roots of them, and this is made possible by the use of trees as a bookkeeping device. The main technical result is Theorem 3 in §3, which is later applied via Lemma 15. The reader who wishes to see this machinery at work in a less complicated setting is advised to skip directly to the final Section §8, whose content is explained at the end of this introduction. The construction of the Euler system, which is actually inspired by the final part of [RW], is done in §§6–7.

It perhaps requires some explanation why one goes to such lengths, only to treat a fairly limited class of fields K . The point is that if G does not have prime order, one does not even know how to start since the $\mathbb{Z}[G]$ -module $cl(K)$ defies classification. (That this works for $|G|$ prime is a bit of luck: $cl(K)$ is killed by the norm N , and $\mathbb{Z}[G]/(N)$ happens to be a Dedekind ring.) So the plan of this work was to consider a setup where the algebraic situation is amenable, and to see whether one can deal with the arithmetic. The fact that this is indeed the case if one sufficiently belabors the method of Euler systems, sheds a slightly more optimistic light on the matter than the concluding comment of the first paragraph in [RW]. Actually it seems novel that an Euler system is used in a seriously non-semisimple situation. In many previous situations one worked with an arbitrary Galois group, admitting however nonzero integral fudge factors in all annihilation statements, which is practically just as good as tensoring with \mathbb{Q} and making the situation semisimple. In the present setup we cannot afford any fudge factors.

In §8 we use our techniques in a more concrete setting in order to illustrate a generalization of the theorem of Rédei and Reichardt. Let us explain this general theorem: Assume as before that l is an odd prime. K is supposed to be a tame absolutely abelian field of degree l and conductor $p_1 \cdots p_s$, so all p_i have to be congruent to 1 modulo l . Genus theory tells us that the class number of K is divisible by l^{s-1} , more precisely: the G -coinvariants of the l -part $cl(K)_l$ form a vector space of dimension $s-1$ over $\mathbb{Z}/l\mathbb{Z}$. (This is in complete analogy with the case $l=2$ where $s-1$ equals the number of cyclic factors of the 2-primary part of the narrow class group, i.e., the number of invariants of $cl^+(K)$ divisible by 2. The classical theorem of Rédei and Reichardt determines the number of invariants divisible by 4.)

There is an $s \times s$ matrix $A = (a_{ij})$ over $\mathbb{Z}/l\mathbb{Z}$ whose non-diagonal entries are determined by the following condition: $\sigma_j^{a_{i,j}} = (K_j/\mathbb{Q}, p_i)$. Here K_j is the field of degree l and conductor p_j ; each σ_j is a generator of $\text{Gal}(K_j/\mathbb{Q})$ uniquely determined by a fixed generator σ of $G = \text{Gal}(K/\mathbb{Q})$ as explained at the beginning of Section 8; and $(K_j/\mathbb{Q}, p_i)$ is the global Artin symbol, i.e. the Frobenius of p_i on K_j . The diagonal of A is filled by the requirement that all row sums of A be zero. Then by construction, A has corank at least one, and our theorem à la Rédei-Reichardt is now:

THEOREM 7. — *The λ^2 -rank of $cl(K)$ equals $s - 1 - rk(A)$.*

(Here $\lambda = \sigma - 1$; the notion “ λ^2 -rank” is explained in full detail in §8.)

Let us mention here that the first published version [RR] of the classical theorem ($l = 2$) does not use the corank of a matrix, but a subsequent paper of Rédei [R] does, up to terminology. There is a considerable literature on this theorem, see for example the references given in [Hu].

After proving Theorem 7 by a fairly short argument from class field theory, we have another look at it from the viewpoint of cyclotomic units. Any divisibility statement concerning h_K implies existence of certain roots of cyclotomic units, via the analytic class number formula. In general, it is almost impossible to lay our hands on these roots. The point of everything following the proof of Theorem 7 is to make clear that in this very special setting, our methods allow to see perfectly well how these roots can be extracted. We even reprove a part of Theorem 7: the λ^2 -rank of $cl(K)$ is positive if and only if the rank of A is less than $s - 1$. We do not know whether our techniques allow to go further than that.

Acknowledgements. — The authors would like to thank Peter Sarnak for pointing out the existence of the Kirchhoff-Tutte theorem, and Manfred Kolster for directing us to the paper [Hu]. Some of the work of the first author was supported by a NSERC grant; the second author was supported by grant 201/97/0433 of the Grant Agency of the Czech Republic.

1. Some identities in a group ring.

Remark. — This section is technical and its details may well be skipped on the first reading.

Let $l > 1$ be an integer, and let G be the direct product of s cyclic groups of order l with generators $\sigma_1, \dots, \sigma_s$. The aim of this section is to prove a few identities in the integral group ring $\mathbb{Z}[G]$; most of these are fairly technical, and the principal results are Lemmas 5 and 7, which will be important in the sequel.

DEFINITION. — For any integer i let

$$S_t = \sum_{\substack{(j_1, \dots, j_s) \in \{0, 1, \dots, l-1\}^s \\ j_1 + \dots + j_s = t}} \prod_{i=1}^s \sigma_i^{j_i} \in \mathbb{Z}[G].$$

So $S_t = 0$ if $t < 0$ or $t > s(l - 1)$.

DEFINITION. — For any $\tau \in G$ and any integer $c \geq 0$ we define

$$\Delta_\tau^{(c)} = \sum_{i=0}^{l-1} \binom{i+c-1}{c} \tau^i$$

(where we put $\binom{-1}{0} = 1$ and $\binom{0}{1} = \binom{1}{2} = \dots = 0$). For brevity, sometimes we shall also write Δ_τ for $\Delta_\tau^{(1)}$, and N_τ for $\Delta_\tau^{(0)} = \sum_{i=0}^{l-1} \tau^i$.

LEMMA 1. — We have $(\tau - 1)N_\tau = 0$ and $(\tau - 1)\Delta_\tau = l - N_\tau$. For any integer $c \geq 2$ we have

$$(\tau - 1)\Delta_\tau^{(c)} = \binom{l+c-2}{c} - \Delta_\tau^{(c-1)}.$$

Proof. — This is done by a direct computation. □

LEMMA 2. — For any integer $c \geq 0$ we have

$$\begin{aligned} N_\tau \Delta_\tau^{(c+1)} &= \binom{l+c}{c+2} N_\tau, \\ \Delta_\tau \Delta_\tau^{(c+1)} &= \binom{l+c+1}{c+3} N_\tau + \binom{l+c}{c+2} \Delta_\tau - l \Delta_\tau^{(c+2)}. \end{aligned}$$

Proof. — The former identity is an easy consequence of

$$\sum_{i=1}^{l-1} \binom{i+c}{c+1} = \binom{l+c}{c+2}.$$

The latter identity can be obtained by the following calculation:

$$\begin{aligned}
 \Delta_\tau \Delta_\tau^{(c+1)} &= \sum_{j=0}^{l-1} j \tau^j \sum_{i=0}^{l-1} \binom{i+c}{c+1} \tau^i = \sum_{a=0}^{l-1} \tau^a \left(\sum_{i=0}^a \binom{i+c}{c+1} (a-i) + \sum_{i=a+1}^{l-1} \binom{i+c}{c+1} (a+l-i) \right) \\
 &= \sum_{a=0}^{l-1} \tau^a \sum_{i=0}^{l-1} \binom{i+c}{c+1} (a - (i+c+1) + (c+1)) + l \sum_{a=0}^{l-1} \tau^a \sum_{i=a+1}^{l-1} \binom{i+c}{c+1} \\
 &= \Delta_\tau \sum_{i=0}^{l-1} \binom{i+c}{c+1} - N_\tau \sum_{i=0}^{l-1} ((c+2) \binom{i+c+1}{c+2} - (c+1) \binom{i+c}{c+1}) \\
 &\quad + l \sum_{a=0}^{l-1} \tau^a \left(\binom{l+c}{c+2} - \binom{a+c+1}{c+2} \right) \\
 &= \Delta_\tau \binom{l+c}{c+2} - N_\tau \left((c+2) \binom{l+c+1}{c+3} - (c+1) \binom{l+c}{c+2} \right) + l N_\tau \binom{l+c}{c+2} - l \Delta_\tau^{(c+2)} \\
 &= N_\tau \binom{l+c}{c+2} (l+c+1 - (c+2) \frac{l+c+1}{c+3}) + \Delta_\tau \binom{l+c}{c+2} - l \Delta_\tau^{(c+2)} \\
 &= \binom{l+c+1}{c+3} N_\tau + \binom{l+c}{c+2} \Delta_\tau - l \Delta_\tau^{(c+2)},
 \end{aligned}$$

and the lemma is proved. □

DEFINITION. — We put $d_0 = 1$ and for any positive integer c we define

$$d_c = \sum_{i=0}^{c-1} (-l)^i \sum_{\substack{t_1, \dots, t_{c-i} \in \mathbb{N} \\ t_1 + \dots + t_{c-i} = c}} \prod_{j=1}^{c-i} \binom{l+t_j-1}{t_j+1},$$

where \mathbb{N} means the set of positive integers.

LEMMA 3. — For any positive integer c we have

$$d_c = \sum_{j=0}^{c-1} (-l)^j \binom{l+j}{j+2} d_{c-1-j}.$$

Proof. — We have

$$\begin{aligned}
 \sum_{j=0}^{c-2} (-l)^j \binom{l+j}{j+2} d_{c-j-1} &= \\
 &= \sum_{j=0}^{c-2} (-l)^j \binom{l+j}{j+2} \sum_{i=0}^{c-j-2} (-l)^i \sum_{\substack{t_1, \dots, t_{c-j-1-i} \in \mathbb{N} \\ t_1 + \dots + t_{c-j-1-i} = c-j-1}} \prod_{b=1}^{c-j-1-i} \binom{l+t_b-1}{t_b+1} \\
 &= \sum_{j=0}^{c-2} \binom{l+j}{j+2} \sum_{i=j}^{c-2} (-l)^i \sum_{\substack{t_1, \dots, t_{c-1-i} \in \mathbb{N} \\ t_1 + \dots + t_{c-1-i} = c-j-1}} \prod_{b=1}^{c-1-i} \binom{l+t_b-1}{t_b+1} \\
 &= \sum_{i=0}^{c-2} (-l)^i \sum_{j=0}^i \binom{l+j}{j+2} \sum_{\substack{t_1, \dots, t_{c-1-i} \in \mathbb{N} \\ t_1 + \dots + t_{c-1-i} = c-j-1}} \prod_{b=1}^{c-1-i} \binom{l+t_b-1}{t_b+1} \\
 &= \sum_{i=0}^{c-2} (-l)^i \sum_{t=1}^{i+1} \binom{l+t-1}{t+1} \sum_{\substack{t_1, \dots, t_{c-1-i} \in \mathbb{N} \\ t_1 + \dots + t_{c-1-i} = c-t}} \prod_{b=1}^{c-1-i} \binom{l+t_b-1}{t_b+1} \\
 &= \sum_{i=0}^{c-2} (-l)^i \sum_{\substack{t_1, \dots, t_{c-i} \in \mathbb{N} \\ t_1 + \dots + t_{c-i} = c}} \prod_{b=1}^{c-i} \binom{l+t_b-1}{t_b+1} \\
 &= d_c - (-l)^{c-1} \binom{l+c-1}{c+1},
 \end{aligned}$$

and the lemma follows. □

LEMMA 4. — *For any positive integer c and any $\tau \in G$ we have*

$$\Delta_\tau^c = -\frac{1}{l} \left(d_c - \binom{l}{2}^c \right) N_\tau + \sum_{i=1}^c (-l)^{i-1} d_{c-i} \Delta_\tau^{(i)}.$$

Proof. — We shall use induction with respect to c . If $c = 1$ there is nothing to prove. Suppose that the lemma already holds for a positive integer c . Using Lemma 2 we have

$$\begin{aligned}
\Delta_\tau^{c+1} &= -\frac{1}{l} \left(d_c - \binom{l}{2}^c \right) \binom{l}{2} N_\tau \\
&\quad + \sum_{i=1}^c (-l)^{i-1} d_{c-i} \left(-l \Delta_\tau^{(i+1)} + \binom{l+i-1}{i+1} \Delta_\tau + \binom{l+i}{i+2} N_\tau \right) \\
&= \left(\sum_{i=1}^c (-l)^i \Delta_\tau^{(i+1)} d_{c-i} \right) + \Delta_\tau \left(\sum_{i=1}^c (-l)^{i-1} \binom{l+i-1}{i+1} d_{c-i} \right) \\
&\quad - \frac{1}{l} \left(\sum_{i=0}^c (-l)^i \binom{l+i}{i+2} d_{c-i} \right) N_\tau + \frac{1}{l} \binom{l}{2}^{c+1} N_\tau \\
&= \left(\sum_{i=1}^c (-l)^i \Delta_\tau^{(i+1)} d_{c-i} \right) + \Delta_\tau d_c - \frac{1}{l} d_{c+1} N_\tau + \frac{1}{l} \binom{l}{2}^{c+1} N_\tau
\end{aligned}$$

due to Lemma 3, and the lemma follows. \square

DEFINITION. — We define

$$\Gamma_0 = \sum_{t=0}^{s-1} S_{lt}, \quad \Phi_0 = \sum_{t=0}^{s(l-1)} S_t$$

and for any positive integer c we put

$$\Gamma_c = \sum_{t=0}^{s(l-1)} S_t \sum_{r=1}^{\lfloor \frac{t}{l} \rfloor} \binom{t-rl+c-1}{c-1}, \quad \Phi_c = \sum_{t=0}^{s(l-1)} S_t \binom{t+c-1}{c}.$$

LEMMA 5. — For any integer $c \geq 0$ we have

$$\Phi_c = \sum_{\substack{c_1 \geq 0, \dots, c_s \geq 0 \\ \sum_{i=1}^s c_i = c}} \prod_{i=1}^s \Delta_{\sigma_i}^{(c_i)}.$$

Proof. — It is easy to see that

$$\Phi_c = \sum_{t=0}^{s(l-1)} S_t \binom{t+c-1}{c} = \sum_{j_1=0}^{l-1} \dots \sum_{j_s=0}^{l-1} \binom{c-1 + \sum_{i=1}^s j_i}{c} \prod_{i=1}^s \sigma_i^{j_i}.$$

But $\binom{c-1 + \sum_{i=1}^s j_i}{c}$ means the number of possibilities of distributing c balls into $\sum_{i=1}^s j_i$ holes (there can be any number of balls in any hole).

Distinguishing possibilities with c_1 balls in the first j_1 holes, c_2 balls in the next j_2 holes, etc., we obtain

$$\binom{c-1 + \sum_{i=1}^s j_i}{c} = \sum_{\substack{c_1 \geq 0, \dots, c_s \geq 0 \\ \sum_{i=1}^s c_i = c}} \prod_{i=1}^s \binom{j_i + c_i - 1}{c_i},$$

so

$$\begin{aligned} \Phi_c &= \sum_{\substack{c_1 \geq 0, \dots, c_s \geq 0 \\ \sum_{i=1}^s c_i = c}} \sum_{j_1=0}^{l-1} \dots \sum_{j_s=0}^{l-1} \prod_{i=1}^s \binom{j_i + c_i - 1}{c_i} \sigma_i^{j_i} \\ &= \sum_{\substack{c_1 \geq 0, \dots, c_s \geq 0 \\ \sum_{i=1}^s c_i = c}} \prod_{i=1}^s \sum_{j=0}^{l-1} \binom{j + c_i - 1}{c_i} \sigma_i^j, \end{aligned}$$

and the lemma is proved. □

LEMMA 6. — For any positive integer c we have

$$\Phi_c - \Gamma_0 \Delta_{\sigma_1}^{(c)} = l \Gamma_c + \sum_{i=1}^{c-1} \binom{l+i-1}{i+1} \Gamma_{c-i}.$$

Proof. — Let us fix an integer $t \geq 0$ for a moment and write $t = al + b$ with integral $a, b, 0 \leq b < l$ (so $a = \lfloor \frac{t}{l} \rfloor$ and $b = l \langle \frac{t}{l} \rangle$). We have

$$\binom{t+c-1}{c} - \binom{b+c-1}{c} = \sum_{r=1}^a \left(\binom{t-(r-1)l+c-1}{c} - \binom{t-rl+c-1}{c} \right).$$

Computing the number of possibilities of putting c balls into $(t - rl + 1) + (l - 1)$ holes (there can be any number of balls in any hole) we get the following identity:

$$\binom{t-(r-1)l+c-1}{c} = \sum_{i=0}^c \binom{t-rl+i}{i} \binom{l-2+c-i}{c-i}.$$

Hence

$$\begin{aligned} \binom{t+c-1}{c} - \binom{b+c-1}{c} &= \sum_{r=1}^a \left(\sum_{i=0}^c \binom{t-rl+i}{i} \binom{l-2+c-i}{c-i} - \binom{t-rl+c}{c} + \binom{t-rl+c-1}{c-1} \right) \\ &= \sum_{r=1}^a \left(l \cdot \binom{t-rl+c-1}{c-1} + \sum_{i=0}^{c-2} \binom{t-rl+i}{i} \binom{l-2+c-i}{c-i} \right). \end{aligned}$$

We have obtained

$$\begin{aligned} \sum_{t=0}^{s(l-1)} S_t \left(\binom{t+c-1}{c} - \binom{l\binom{t}{l}+c-1}{c} \right) &= l \sum_{t=0}^{s(l-1)} S_t \sum_{r=1}^{\lfloor \frac{t}{l} \rfloor} \binom{t-rl+c-1}{c-1} \\ &\quad + \sum_{i=0}^{c-2} \binom{l-2+c-i}{c-i} \sum_{t=0}^{s(l-1)} S_t \sum_{r=1}^{\lfloor \frac{t}{l} \rfloor} \binom{t-rl+i}{i}. \end{aligned}$$

The lemma follows using the definition of Γ_c and the following identity:

$$\Gamma_0 \Delta_{\sigma_1}^{(c)} = \sum_{t=0}^{s(l-1)} S_t \binom{l\binom{t}{l}+c-1}{c}$$

which can be easily proved by comparing the coefficients. \square

LEMMA 7. — For any positive integer c we have

$$\Gamma_0 \Delta_{\sigma_1}^c = (-l)^c \Gamma_c - \frac{1}{l} \left(d_c - \binom{l}{2}^c \right) \Phi_0 + \sum_{i=1}^c (-l)^{i-1} d_{c-i} \Phi_i.$$

Proof. — It is easy to see that $\Gamma_0 N_{\sigma_1} = \Phi_0$. Lemma 4 and Lemma 6 give

$$\Gamma_0 \Delta_{\sigma_1}^c = -\frac{1}{l} \left(d_c - \binom{l}{2}^c \right) \Phi_0 + \sum_{i=1}^c (-l)^{i-1} d_{c-i} \left(\Phi_i - l \Gamma_i - \sum_{j=1}^{i-1} \binom{l+j-1}{j+1} \Gamma_{i-j} \right)$$

We have

$$\begin{aligned} \sum_{i=1}^c (-l)^{i-1} d_{c-i} \sum_{j=1}^{i-1} \binom{l+j-1}{j+1} \Gamma_{i-j} &= \sum_{j=1}^{c-1} \binom{l+j-1}{j+1} \sum_{i=j+1}^c (-l)^{i-1} d_{c-i} \Gamma_{i-j} \\ &= \sum_{j=1}^{c-1} \binom{l+j-1}{j+1} \sum_{i=1}^{c-j} (-l)^{i+j-1} d_{c-i-j} \Gamma_i \\ &= \sum_{i=1}^{c-1} (-l)^i \Gamma_i \sum_{j=1}^{c-i} (-l)^{j-1} \binom{l+j-1}{j+1} d_{c-i-j} \\ &= \sum_{i=1}^{c-1} (-l)^i \Gamma_i d_{c-i} \end{aligned}$$

due to Lemma 3. Hence

$$\begin{aligned} \Gamma_0 \Delta_{\sigma_1}^c &= -\frac{1}{l} \left(d_c - \binom{l}{2}^c \right) \Phi_0 + \sum_{i=1}^c (-l)^{i-1} d_{c-i} \Phi_i + \\ &\quad \sum_{i=1}^c (-l)^i d_{c-i} \Gamma_i - \sum_{i=1}^{c-1} (-l)^i d_{c-i} \Gamma_i \end{aligned}$$

and the lemma follows. \square

LEMMA 8. — Let us suppose that l is a prime and let \mathbb{Z}_l mean the l -adic integers. Then for any $\tau \in G$, $\Delta_\tau^{(l-1)}$ is invertible in $\mathbb{Z}_l[G]$ and the inverse is congruent to τ^{-1} modulo l .

Proof. — It suffices to check that

$$\tau^{-1} \Delta_\tau^{(l-1)} = \sum_{i=1}^{l-1} \binom{i+l-2}{l-1} \tau^{i-1} \equiv 1 \pmod{l\mathbb{Z}[G]}. \quad \square$$

LEMMA 9. — Let us suppose that l is a prime and let ν_l mean the l -adic valuation on \mathbb{Z} (so, e.g. $\nu_l(l^i) = i$). Then we have

(a) For any integer $c \geq 0$

$$\nu_l(d_c) \geq \frac{l-2}{l-1}c.$$

(b) For any integer $i \geq 0$

$$d_{i(l-1)} \cdot l^{-i(l-2)} \equiv (-1)^i \pmod{l}.$$

Proof. — (a) We shall use induction with respect to c . The case $c = 0$ is clear. Let us suppose that $c > 0$ and the lemma has been proved for any index less than c . Lemma 3 gives

$$\begin{aligned} \nu_l(d_c) &\geq \min_{0 \leq j \leq c-1} \left(j + \nu_l \left(\binom{l+j}{l-2} \right) + \frac{l-2}{l-1}(c-1-j) \right) \\ &= \min_{0 \leq j \leq c-1} \left(\frac{j}{l-1} + \nu_l \left(\binom{l+j}{l-2} \right) \right) + \frac{l-2}{l-1}(c-1). \end{aligned}$$

It is enough to show that

$$\frac{j}{l-1} + \nu_l \left(\binom{l+j}{l-2} \right) \geq \frac{l-2}{l-1}$$

for any $0 \leq j \leq c-1$. This is clear for $j \geq l-2$. On the other hand it is easy to see that $\binom{l+j}{l-2}$ is divisible by l for any $j \in \{0, 1, \dots, l-3\}$.

(b) Lemma 3 gives

$$d_{i(l-1)} = \sum_{j=0}^{i(l-1)-1} (-l)^j \binom{l+j}{l-2} d_{i(l-1)-1-j}.$$

Using (a) we have

$$\begin{aligned} \nu_l \left((-l)^j \binom{l+j}{l-2} d_{i(l-1)-1-j} \right) &\geq j + \nu_l \left(\binom{l+j}{l-2} \right) + \frac{l-2}{l-1}(i(l-1)-1-j) \\ &= i(l-2) + \frac{j-(l-2)}{l-1} + \nu_l \left(\binom{l+j}{l-2} \right). \end{aligned}$$

So if $j > l - 2$ then

$$\nu_l \left((-l)^j \binom{l+j}{l-2} d_{i(l-1)-1-j} \right) > i(l-2).$$

If $j \in \{0, 1, \dots, l-3\}$ then $\binom{l+j}{l-2}$ is divisible by l and again

$$\nu_l \left((-l)^j \binom{l+j}{l-2} d_{i(l-1)-1-j} \right) > i(l-2).$$

Therefore

$$\begin{aligned} d_{i(l-1)} \cdot l^{-i(l-2)} &\equiv (-l)^{l-2} \binom{2l-2}{l-2} d_{(i-1)(l-1)} \cdot l^{-i(l-2)} \\ &\equiv -d_{(i-1)(l-1)} \cdot l^{-(i-1)(l-2)} \pmod{l}. \end{aligned}$$

Induction with respect to i gives the result. □

2. Circular numbers.

Let us fix an odd prime l , positive integers $s \leq s'$ and a high power L of l (we suppose that L satisfies $\nu_l(L) \geq \frac{s'}{l-1}$ where ν_l is the l -adic valuation defined in Lemma 9). Let $p_1, \dots, p_{s'}$ be different primes all congruent to 1 modulo l . We put $I = \{1, \dots, s\}$ and $I' = \{s+1, \dots, s'\}$. We assume that $p_i \equiv 1 \pmod{L}$ for each $i \in I'$. There is a reason for this non-symmetry: later on we shall apply results of this section to a situation, where primes p_1, \dots, p_s will be given, while primes $p_{s+1}, \dots, p_{s'}$ will be obtained by means of the Euler system machinery.

For any $i \in I \cup I'$ let ζ_i be a fixed p_i th primitive root of unity and K_i be the unique degree l subfield of $\mathbb{Q}(\zeta_i)$. For any subset $J \subseteq I \cup I'$ we define $\zeta_J = \prod_{i \in J} \zeta_i$. Let C be the group of circular numbers of $\mathbb{Q}(\zeta_{I \cup I'})$, i.e., the subgroup of $\mathbb{Q}(\zeta_{I \cup I'})^\times$ generated by all nonzero $1 - \zeta_{I \cup I'}^a$ with $a \in \mathbb{Z}$. (Thus the intersection of C and the group of all units of $\mathbb{Q}(\zeta_{I \cup I'})$ is the group of circular units of $\mathbb{Q}(\zeta_{I \cup I'})$.) Let $\tilde{G} = \text{Gal}(\mathbb{Q}(\zeta_{I \cup I'})/\mathbb{Q})$. For any $i \in I \cup I'$ let $\sigma_i \in \tilde{G}$ be a fixed generator of $\text{Gal}(\mathbb{Q}(\zeta_{I \cup I'})/\mathbb{Q}(\zeta_{(I \cup I') - \{i\}}))$.

For any positive integer c and any $i \in I$ we define

$$T_i = \sum_{b=1}^{(p_i-1)/l} \sigma_i^{bl} \quad \text{and} \quad D_i^{(c)} = T_i \cdot \sum_{a=1}^{l-1} \binom{a+c-1}{c} \sigma_i^a,$$

while for any $i \in I'$ we put

$$D_i^{(c)} = \sum_{a=1}^{p_i-2} \binom{a+c-1}{c} \sigma_i^a.$$

Moreover, for any $i \in I \cup I'$ we define

$$D_i^{(0)} = N_i = \sum_{a=0}^{p_i-2} \sigma_i^a.$$

It is easy to see for $i \in I$ that T_i can be understood as the norm operator from $\mathbb{Q}(\zeta_i)$ to K_i . One can also see that there is a bridge between $\Delta_{\sigma_i}^{(c)}$ from the previous section and our $D_i^{(c)}$, namely: putting $G = \text{Gal}(\prod_{i \in I} K_i/\mathbb{Q})$ and letting σ_i stand (by abuse of notation) also for the restrictions of the new σ_i 's above, we obtain

$$(1 - \zeta_J)^{D_J^{(c)}} = N_{\mathbb{Q}(\zeta_J)/K_J(\zeta_{J-\{j\}})}(1 - \zeta_J)^{\Delta_{\sigma_j}^{(c)}}$$

for any subset $J \subseteq I \cup I'$ and any $j \in J \cap I$.

We define an $s' \times s'$ matrix $A = (a_{ij})_{1 \leq i, j \leq s'}$ over $\mathbb{Z}/l\mathbb{Z}$ in the following way: the non-diagonal entries are given by the condition that the restriction of $\sigma_j^{a_{ij}}$ is the Frobenius automorphism of p_i in K_j . The diagonal entries are chosen so as the matrix A has zero row sums: $a_{ii} = -\sum_{j \neq i} a_{ij}$.

Let $J \subseteq I \cup I'$ and let T be a tree on J with root $r \in J$ (i.e., a directed graph with the set of vertices J without circuits such that the out-degree of r is 0 and out-degree of any other vertex equals 1). We denote the root r of T by \sqrt{T} and define the valency function $v_T : J \rightarrow \mathbb{N} \cup \{0\}$ by letting $v_T(i)$ be the in-degree of $i \in I$. Moreover, we define

$$A(T) = \prod_{(i,j) \in E(T)} a_{ij},$$

where (i, j) means the edge going from i to j and runs through the set $E(T)$ of all edges of T .

For any $J \subseteq I \cup I'$ and for any mapping $v : J \rightarrow \mathbb{N} \cup \{0\}$ we put

$$|v| = \sum_{i \in J} v(i) \quad \text{and} \quad D(v) = \prod_{i \in J} (D_i^{(v(i))}).$$

Moreover, let $\bar{v} : J \rightarrow \mathbb{N} \cup \{0\}$ be defined as follows:

$$\bar{v}(i) = \begin{cases} 0, & \text{if } i \in J \cap I \text{ and } v(i) = 0, \\ 1 + (l-1) \langle \frac{v(i)-1}{l-1} \rangle, & \text{if } i \in J \cap I \text{ and } v(i) \neq 0, \\ v(i), & \text{if } i \in J \cap I'. \end{cases}$$

THEOREM 1. — *Suppose that $J \subseteq I \cup I'$, that $w : J \rightarrow \mathbb{N} \cup \{0\}$ satisfies $|w| \leq |J| - 1$, and that $w(i) < l$ for each $i \in J \cap I$. Put*

$n = |J| - 1 - |w|$ and $m = \lfloor \frac{n}{l-1} \rfloor$. Then

$$(1 - \zeta_J)^{D(w)} \equiv \prod_{i \in J} p_i^{l^m E_i(w)} \pmod{C^{l^{m+1}}}$$

with

$$E_i(w) = (-1)^{m+|w|} \sum_{T \in \mathcal{T}_i(w)} A(T),$$

where T runs through the set $\mathcal{T}_i(w)$ of all trees T on J with the root i and valency function v_T satisfying $\overline{v_T} = w$.

Remark. — If any tree $T \in \mathcal{T}_i(w)$ is to exist, we must have $|v_T| = |J| - 1 \equiv |w| \pmod{l - 1}$, so $l - 1 \mid n$. Hence the theorem states in particular that $(1 - \zeta_J)^{D(w)} \in C^{l^{m+1}}$ if $l - 1 \nmid n$.

Proof. — The proof is done by means of induction over $|J|$. Notice that $J \neq \emptyset$. If $J = \{i\}$ then $|w| = n = m = 0$ and $(1 - \zeta_{\{i\}})^{N_i} = p_i$; on the other hand, there is just one tree T and for this tree $A(T)$, as an empty product, equals 1.

Let us suppose that $|J| > 1$ and that the theorem holds for any proper subset of J . Since $n \geq 0$, there is $t \in J$ such that $w(t) = 0$. Let us choose and fix one such t and put $J_0 = J - \{t\}$. Let w_0 be the restriction of w to J_0 . The well-known relation on circular units gives

$$\begin{aligned} (1 - \zeta_J)^{D(w)} &= \left((1 - \zeta_{J_0})^{D(w_0)} \right)^{\text{Frob}(p_t) - 1} \\ &= \left((1 - \zeta_{J_0})^{D(w_0)} \right)^{-1 + \prod_{j \in J_0} \sigma_j^{a_{tj}}}. \end{aligned}$$

Now, for appropriate $\tau_j \in \tilde{G}$, we also have (considering a_{tj} as its positive lift)

$$-1 + \prod_{j \in J_0} \sigma_j^{a_{tj}} = \sum_{j \in J_0} \left(\sum_{c=0}^{a_{tj}-1} \sigma_j^c \right) (\sigma_j - 1) \tau_j = \sum_{j \in J_0} a'_{tj} (\sigma_j - 1),$$

where the a'_{tj} are in $\mathbb{Z}[\tilde{G}]$ and all we require to know about them is that they go to a_{tj} under the augmentation map. Therefore

$$(1 - \zeta_J)^{D(w)} = \prod_{j \in J_0} \alpha_j^{a'_{tj}},$$

where

$$\alpha_j = (1 - \zeta_{J_0})^{D(w_0)(\sigma_j - 1)}.$$

For each $j \in J_0$, we want to show that

$$(*) \quad \alpha_j^{a'_{ij}} \equiv \prod_{i \in J_0} p_i^{(-1)^{m+|w|} l^m \sum_{T \in \mathcal{T}_i(w), (t,j) \in E(T)} A(T)} \pmod{C^{l^{m+1}}},$$

where the sum is taken over all the trees $T \in \mathcal{T}_i(w)$ containing the edge going from t to j . Since $\mathcal{T}_t(w) = \emptyset$, this will prove the theorem.

Let us distinguish three cases depending on j .

1. At first, let $w(j) = 0$. Then $(\sigma_j - 1)N_{\sigma_j} = 0$ and $\alpha_j = 1$. On the other hand, there is no tree $T \in \mathcal{T}_j(w)$ with $(t, j) \in E(T)$ in this case.

2. Now, suppose $j \in I'$ and $w(j) \geq 1$. We have $(\sigma_j - 1)D_j^{(1)} = (p_j - 1) - N_j$. If $w(j) > 1$ then $(\sigma_j - 1)D_j^{(w(j))} = \binom{p_i + w(j) - 3}{w(j)} - D_j^{(w(j) - 1)}$ and

$$\nu_l \left(\binom{p_i + w(j) - 3}{w(j)} \right) \geq \nu_l(L) - \nu_l(w(j)!) > \frac{s'}{l-1} - \frac{w(j)}{l-1} \geq \frac{|J| - |w|}{l-1} = \frac{n+1}{l-1} > m.$$

Hence both cases give $(\sigma_j - 1)D_j^{(w(j))} \equiv -D_j^{(w(j) - 1)} \pmod{l^{m+1}}$. Let $w_j : J_0 \rightarrow \mathbb{N} \cup \{0\}$ be determined by $w_j(j) = w(j) - 1$ and $w_j(i) = w(i)$ for $i \neq j$. Then we have

$$\alpha_j \equiv (1 - \zeta_{J_0})^{-D(w_j)} \pmod{C^{l^{m+1}}}.$$

Using the induction hypothesis for the right-hand side, we have $|J_0| - 1 - |w_j| = n$, so

$$\alpha_j \equiv \prod_{i \in J_0} p_i^{(-1)^{m+|w|-1} l^m \sum_{T \in \mathcal{T}_i(w_j)} A(T)} \pmod{C^{l^{m+1}}}$$

and (*) follows by means of the bijection between $\mathcal{T}_i(w_j)$ and $\{T \in \mathcal{T}_i(w); (t, j) \in E(T)\}$ defined by the following way: add the edge (t, j) to any tree from $\mathcal{T}_i(w_j)$.

3. Finally, let $j \in I$ and $w(j) \geq 1$. If $w(j) > 1$ then

$$(\sigma_j - 1)D_j^{(w(j))} = \binom{l + w(j) - 2}{l - 2} T_j - D_j^{(w(j) - 1)}.$$

Since $1 \mapsto T_j$ induces a monomorphism of $\mathbb{Z}[\langle \sigma_j \rangle]$ -modules from $\mathbb{Z}[\langle \sigma_j \rangle / \langle \sigma_j^l \rangle]$ to $\mathbb{Z}[\langle \sigma_j \rangle]$ sending $\Delta_{\sigma_j}^{(w(j) - 1)}$ to $D_j^{(w(j) - 1)}$ (in fact, this is the corestriction

map), Lemma 8 gives that there is $c \in \mathbb{Z}[\tilde{G}]$ satisfying

$$(**) \quad (\sigma_j - 1)D_j^{(w(j))} \equiv -D_j^{(w(j)-1)} + lcD_j^{(l-1)} \pmod{l^{m+1}}.$$

On the other hand, if $w(j) = 1$ then $(\sigma_j - 1)D_j^{(w(j))} = lT_j - N_j$ and we see that (**) holds true again, moreover we can suppose $c \equiv \sigma_j^{-1} \pmod{l}$ in this case due to Lemma 8. Treating both cases simultaneously, let us define two mappings $w_j, w'_j : J_0 \rightarrow \mathbb{N} \cup \{0\}$ by the following conditions: $w_j(i) = w'_j(i) = w(i)$ for any $i \neq j$, and $w_j(j) = w(j) - 1$, while $w'_j(j) = l - 1$. Then (**) implies

$$(***) \quad \alpha_j \equiv (1 - \zeta_{J_0})^{-D(w_j)} \cdot (1 - \zeta_{J_0})^{lcD(w'_j)} \pmod{C^{l^{m+1}}}.$$

Using the induction hypothesis for the first term on the right-hand side, we compute $|J_0| - 1 - |w_j| = n$, so

$$(1 - \zeta_{J_0})^{D(w_j)} \equiv \prod_{i \in J_0} p_i^{(-1)^{m+(l|w|-1)}l^m \sum_{T \in \mathcal{T}_i(w_j)} A(T)} \pmod{C^{l^{m+1}}}.$$

Doing the same for the second term on the right-hand side of (***), we have

$$n' = |J_0| - 1 - |w'_j| = n - (l - 1) + (w(j) - 1),$$

so $n - (l - 1) \leq n' \leq n - 1$ and $m' = \lfloor \frac{n'}{l-1} \rfloor \in \{m - 1, m\}$. If $n' \geq 0$ then the induction hypothesis gives

$$(1 - \zeta_{J_0})^{D(w'_j)} \equiv \prod_{i \in J_0} p_i^{(-1)^{m'+|w'_j|}l^{m'} \sum_{T \in \mathcal{T}_i(w'_j)} A(T)} \pmod{C^{l^{m'+1}}}.$$

At first, suppose $l - 1 \nmid n$. Then $\mathcal{T}_i(w) = \mathcal{T}_i(w_j) = \emptyset$ due to the remark following Theorem 1. If $0 \leq m' = m - 1$ then $m'(l - 1) = m(l - 1) - (l - 1) < n - (l - 1) \leq n'$, hence $l - 1 \nmid n'$ and $\mathcal{T}_i(w'_j) = \emptyset$, so $(1 - \zeta_{J_0})^{D(w'_j)} \in C^{l^m}$. Of course, the last holds true also for $m' = m$ and it is trivially satisfied if $m' < 0$. Therefore, we have proved that $l - 1 \nmid n$ implies (*).

Finally, consider $l - 1 \mid n$. The above mentioned remark gives that $\mathcal{T}_i(w'_j) = \emptyset$ if $w(j) > 1$. It is easy to check that the mapping $\{T \in \mathcal{T}_i(w); (t, j) \in E(T)\} \rightarrow \mathcal{T}_i(w_j) \cup \mathcal{T}_i(w'_j)$ given by “cut off the edge (t, j) ” is bijective. (If $w(j) = 1$ then trees are mapped to the first or second set depending whether the vertex j becomes a leaf or not.) Then (*) follows using the fact that $w(j) = 1$ implies $c \equiv \sigma_j^{-1} \pmod{l}$ and $n' = n - (l - 1)$, so $m' = m - 1$.

The theorem is proved. \square

Remark. — Theorem 1 treats circular units $(1 - \zeta_J)^{D(v)}$ for mappings $v : J \rightarrow \mathbb{N} \cup \{0\}$ which are “low”, i.e., satisfy $w(i) < l$ for each $i \in J \cap I$. The following Theorem 2 shows how to do the same job for the other mappings: we just transfer them to a “low” one.

THEOREM 2. — *Suppose $J \subseteq I \cup I'$, and $v : J \rightarrow \mathbb{N} \cup \{0\}$ satisfies $|v| \leq |J| - 1$. Then we define another mapping $w : J \rightarrow \mathbb{N} \cup \{0\}$ by*

$$w(i) = \begin{cases} 0, & \text{if } i \in J \cap I \text{ and } v(i) = 0, \\ l - 1, & \text{if } i \in J \cap I \text{ and } l \mid v(i) \neq 0, \\ l \langle \frac{v(i)}{l} \rangle, & \text{if } i \in J \cap I \text{ and } l \nmid v(i), \\ v(i), & \text{if } i \in J \cap I'. \end{cases}$$

Let us denote $j = \#\{i \in J \cap I; l \mid v(i) \neq 0\}$ and $m = \lceil \frac{|J|-1-|w|}{l-1} \rceil$. Then we have

$$(1 - \zeta_J)^{D(v)} \equiv (1 - \zeta_J)^{(-1)^j D(w)} \pmod{C^{l^{m+1}}}.$$

Proof. — For any $i \in I$ and any positive integers t, r such that $t \equiv r \pmod{l}$ we have

$$D_i^{(t)} = T_i \cdot \sum_{b=1}^{l-1} \binom{b+t-1}{b-1} \sigma_i^b \equiv T_i \cdot \sum_{b=1}^{l-1} \binom{b+r-1}{b-1} \sigma_i^b = D_i^{(r)} \pmod{l}$$

and

$$D_i^{(l)} = T_i \cdot \sum_{b=1}^{l-1} \binom{b+l-1}{b-1} \sigma_i^b \equiv T_i \cdot \sum_{b=1}^{l-1} \sigma_i^b = N_i - T_i \pmod{l}.$$

Let t be a positive integer and let $r = l \langle \frac{t}{l} \rangle$ be its rest upon division by l . Similarly as in the proof of Theorem 1, Lemma 8 implies that for any positive integer k there is $y \in \mathbb{Z}[\tilde{G}]$ such that

$$D_i^{(t)} \equiv (ly - \sigma_i^{-1})D_i^{(l-1)} + N_i \pmod{l^k}$$

if $r = 0$ and

$$D_i^{(t)} \equiv D_i^{(r)} + lyD_i^{(l-1)} \pmod{l^k}$$

if $r \neq 0$. Let

$$\begin{aligned} J_0 &= \{i \in J \cap I; v(i) = 0\}, \\ J_1 &= \{i \in J \cap I; l \mid v(i) \neq 0\}, \\ J_2 &= \{i \in J \cap I; l \nmid v(i)\}. \end{aligned}$$

For any $X \subseteq J_1$ and any $Y \subseteq J_2$ we define $v_{X,Y} : J \rightarrow \{0, 1, \dots, l-1\}$ by

$$v_{X,Y}(i) = \begin{cases} 0, & \text{if } i \in J_0 \cup X, \\ l \langle \frac{v(i)}{l} \rangle, & \text{if } i \in J_2 - Y, \\ l-1, & \text{if } i \in Y \cup (J_1 - X). \\ v(i), & \text{if } i \in J \cap I'. \end{cases}$$

Then due to the two congruences above for any positive integer k we have

$$(1 - \zeta_J)^{D(v)} \equiv \prod_{X \subseteq J_1} \prod_{Y \subseteq J_2} \left((1 - \zeta_J)^{D(v_{X,Y})} \right)^{\prod_{i \in J_1 - X} (ly_i - \sigma_i^{-1})} \prod_{i \in Y} (ly_i) \pmod{C^{l^k}}$$

for suitable $y_i \in \mathbb{Z}[\tilde{G}]$. We have $w = v_{\emptyset, \emptyset}$. Let us denote $n_{X,Y} = |J| - 1 - |v_{X,Y}|$ and $m_{X,Y} = \lfloor \frac{n_{X,Y}}{l-1} \rfloor$. It is easy to see that if $X \neq \emptyset$ or $Y \neq \emptyset$ then we have

$$|v_{X,Y}| - (\#Y)(l-1) < |v_{\emptyset, \emptyset}|,$$

which implies $n_{X,Y} + (\#Y)(l-1) > n_{\emptyset, \emptyset}$ and $m_{X,Y} + (\#Y) \geq m_{\emptyset, \emptyset} = m$. If $l-1 \nmid n_{X,Y} \geq 0$ then the remark following Theorem 1 gives

$$(1 - \zeta_J)^{D(v_{X,Y})} \in C^{l^{m_{X,Y}+1}},$$

which holds also true if $n_{X,Y} < 0$ since the right-hand side should be understood simply as C in this case. So

$$(*) \quad (1 - \zeta_J)^{l^{\#Y} D(v_{X,Y})} \in C^{l^{m+1}}.$$

On the other hand, if $l-1 \mid n_{X,Y} \geq 0$ then $m_{X,Y} + (\#Y) > m$ and again Theorem 1 gives (*). Hence we have

$$(1 - \zeta_J)^{D(v)} \equiv \left((1 - \zeta_J)^{D(v_{\emptyset, \emptyset})} \right)^{\prod_{i \in J_1} (ly_i - \sigma_i^{-1})} \pmod{C^{l^{m+1}}}.$$

The theorem follows since Theorem 1 gives that

$$(1 - \zeta_J)^{D(w)} = (1 - \zeta_J)^{D(v_{\emptyset, \emptyset})} \in C^{l^m}$$

is modulo $C^{l^{m+1}}$ congruent to a rational number. □

DEFINITION. — Let us define $T = \prod_{i \in I} T_i$,

$$\Gamma = \sum_{\substack{(j_1, \dots, j_s) \in \{0, 1, \dots, l-1\}^s \\ l \mid j_1 + \dots + j_s}} \prod_{i \in I} \sigma_i^{j_i}, \quad \text{and} \quad \Delta = \sum_{a=1}^{l-1} a \sigma_1^a.$$

THEOREM 3. — Suppose $s > 1$. Let $w_1 : I' \rightarrow \{1\}$ be the constant map with value 1 and let us define $\beta = (1 - \zeta_{I \cup I'})^{T\Gamma\Delta^{s-1}D(w_1)}$. Then we have

$$\beta \equiv \prod_{i \in I \cup I'} p_i^{l^{s-2}b_i} \pmod{C^{l^{s-1}}},$$

where

$$b_i = (-1)^{s'-s+1} \sum_{\substack{T \text{ a tree on } I \cup I', \sqrt{T}=i \\ \forall j \in I': v_T(j)=1}} A(T),$$

the summation running over all trees T on $I \cup I'$ with root i such that the in-degree in any $j \in I'$ equals 1.

Proof. — Let H denote the subgroup of \tilde{G} generated by $\sigma_1, \dots, \sigma_s$. For each $i \in I$ we identify $\sigma_i H^l$ in H/H^l with $\sigma_i \in G$ from the previous section, so we have $G = H/H^l$. It is easy to see that $1 \mapsto T$ induces a monomorphism of $\mathbb{Z}[H]$ -modules from $\mathbb{Z}[G]$ to $\mathbb{Z}[H]$ which satisfies $\Delta_{\sigma_1}^c \mapsto T\Delta^c$ for any positive integer c , $\Gamma_0 \mapsto T\Gamma$, and $\prod_{i \in I} \Delta_{\sigma_i}^{(v(i))} \mapsto D(v)$ for any mapping $v : I \rightarrow \mathbb{N} \cup \{0\}$. Let us consider the identity given by Lemma 7 for $c = s - 1$ and modify it by Lemma 5. Applying our monomorphism to both of its sides, we obtain

$$T\Gamma\Delta^{s-1} = (-l)^{s-1} \Gamma' + l^{-1} \binom{l}{2}^{s-1} D(v_0) + \sum_{i=0}^{s-1} (-l)^{i-1} d_{s-1-i} \sum_{\substack{v: I \rightarrow \mathbb{N} \cup \{0\} \\ |v|=i}} D(v),$$

where $v_0 : I \rightarrow \{0\}$ is the constant map with value 0 and Γ' is determined by $\Gamma_{s-1} \mapsto \Gamma'$. Then β equals $(1 - \zeta_{I \cup I'})$ raised to the right-hand side of the previous identity multiplied by $D(w_1)$. It is clear that

$$(1 - \zeta_{I \cup I'})^{(-l)^{s-1} \Gamma' D(w_1)} \in C^{l^{s-1}}.$$

For any $v : I \rightarrow \mathbb{N} \cup \{0\}$ let $\tilde{v} : I \cup I' \rightarrow \mathbb{N} \cup \{0\}$ be determined by the following conditions: $\tilde{v}(j) = v(j)$ for any $j \in I$, and $\tilde{v}(j) = 1$ for any $j \in I'$. Hence $D(\tilde{v}) = D(v)D(w_1)$ and $s - |v| = s' - |\tilde{v}|$.

Using Theorem 1 for $\alpha = (1 - \zeta_{I \cup I'})^{D(\tilde{v}_0)}$ we obtain $n = s - 1$ and $m = \lceil \frac{s-1}{l-1} \rceil$. So due to the remark following Theorem 1 either $l - 1 \nmid s - 1$ and $\alpha \in C^l$ or $l - 1 \mid s - 1$ and again $\alpha \in C^l$ since $m > 0$ in this case. Therefore

$$(1 - \zeta_{I \cup I'})^{l^{-1} \binom{l}{2}^{s-1} D(\tilde{v}_0)} = \alpha^{l^{-1} \binom{l}{2}^{s-1}} \in C^{l^{s-1}}.$$

So the first two summands are negligible; we shall concentrate on the last one. Consider any $i \in \{0, 1, \dots, s - 1\}$ and any $v : I \rightarrow \mathbb{N} \cup \{0\}$ satisfying $|v| = i$. Put $m = \lfloor \frac{s-1-i}{l-1} \rfloor$. Let us distinguish two cases.

1. Let $l - 1 \nmid s - 1 - i$ or $\max_{j \in I} v(j) \geq l$. Use \tilde{v} as input to Theorem 2, in order to make w . Then $|w| \leq |\tilde{v}|$, and even $|w| < |\tilde{v}|$ if $\max_{j \in I} v(j) \geq l$. Hence $m' = \lfloor \frac{s'-1-|w|}{l-1} \rfloor \geq m$. Moreover, if $l - 1 \mid s' - 1 - |w|$ then $m' > m$. Theorem 2 gives

$$(1 - \zeta_{I \cup I'})^{D(\tilde{v})} \equiv (1 - \zeta_{I \cup I'})^{\pm D(w)} \pmod{C^{l^{m'+1}}}.$$

Since $\max_{j \in I} w(j) < l$, Theorem 1 implies $(1 - \zeta_{I \cup I'})^{D(w)} \in C^{l^{m+1}}$. Finally, due to Lemma 9 we have

$$\nu_l(l^{i-1}d_{s-1-i}) + (m+1) \geq i-1 + \frac{l-2}{l-1}(s-1-i) + \frac{s-1-i}{l-1} - \frac{l-2}{l-1} + 1 = s-1 - \frac{l-2}{l-1}.$$

But there is an integer on the left-hand side, so $\nu_l(l^{i-1}d_{s-1-i}) + (m+1) \geq s - 1$ and

$$(1 - \zeta_{I \cup I'})^{(-l)^{i-1}d_{s-1-i}, D(\tilde{v})} \in C^{l^{s-1}}.$$

2. Let $l - 1 \mid s - 1 - i$ and $\max_{j \in I} v(j) < l$. So $s - 1 - i = m(l - 1)$ and Lemma 9 implies $\nu_l(d_{s-1-i}) = m(l - 2)$ and

$$d_{s-1-i} \cdot l^{-m(l-2)} \equiv (-1)^m \pmod{l}.$$

Theorem 1 gives

$$(1 - \zeta_{I \cup I'})^{D(\tilde{v})} \equiv \prod_{j \in I \cup I'} p_j^{l^m E_j(\tilde{v})} \pmod{C^{l^{m+1}}},$$

where

$$E_j(\tilde{v}) = (-1)^{m+i+s'-s} \sum_{T \in \mathcal{T}_j(\tilde{v})} A(T).$$

Therefore

$$(1 - \zeta_{I \cup I'})^{(-l)^{i-1}d_{s-1-i}, D(\tilde{v})} \equiv \prod_{j \in I \cup I'} p_j^{(-1)^{i-1+m}l^{s-2}E_j(\tilde{v})} \pmod{C^{l^{s-1}}}.$$

Putting everything together we need only to show that

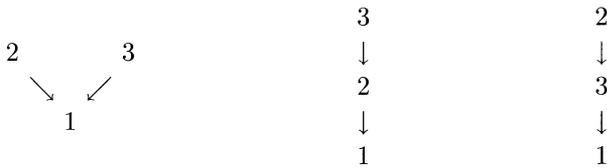
$$\sum_{\substack{i=0,1,\dots,s-1 \\ l-1 \mid s-1-i}} \sum_{\substack{v: I \rightarrow \mathbb{N} \cup \{0\}, |v|=i \\ \max_{t \in I} w(t) < l}} (-1)^{i-1+m} E_j(\tilde{v}) = b_j$$

for any $j \in I \cup I'$. But this is easy to see and the theorem follows. □

Example. — Assuming $s' = s$, Theorem 3 gives for any $s \geq 2$ that

$$(1 - \zeta_I)^{T\Gamma\Delta^{s-1}} \equiv \prod_{i \in I} p_i^{-l^{s-2}} \sum_{T \text{ a tree on } I, \sqrt{T}=i} A(T) \pmod{C^{l^{s-1}}}.$$

For example, for $s = 3$ we have obtained the following result: let K be a cyclic field of odd prime degree l , where precisely three primes p_1, p_2, p_3 ramify, assume $l \nmid p_1 p_2 p_3$, and put $\eta = N_{\mathbb{Q}(\zeta_{\{1,2,3\}})/K}(1 - \zeta_{\{1,2,3\}})$. Then $\eta^{\Delta^2} \equiv r^{-l} \pmod{C^{l^2}}$, where r is defined by means of root-trees on three vertices 1, 2, 3. For example, with 1 being a root we have the following three root-trees:



Hence r is given by

$$r = p_1^{a_{21}a_{31} + a_{32}a_{21} + a_{23}a_{31}} \cdot p_2^{a_{12}a_{32} + a_{13}a_{32} + a_{31}a_{12}} \cdot p_3^{a_{13}a_{23} + a_{12}a_{23} + a_{21}a_{13}}.$$

3. Trees and determinants.

Consider the complete symmetric digraph Γ on the set of vertices $I = \{1, \dots, s\}$ (i.e., there is exactly one edge from every vertex to every other vertex — see [Deo], p. 197). In this section, $A = (a_{ij})$ will be supposed to be an $s \times s$ matrix over \mathbb{Z} whose row sums are zero. (For later applications we remark that any $s \times s$ matrix over $\mathbb{Z}/l\mathbb{Z}$ whose row sums are zero can be lifted to a matrix over \mathbb{Z} whose row sums is zero.)

Following Tutte (see [Tu], 3.1 on p. 468), we declare the edge (i, j) going from i to j to have conductance a_{ij} . Then the Kirchhoff-Tutte matrix $(c_{ij})_{1 \leq i, j \leq s}$ constructed by Tutte (loc. cit.) satisfies $(c_{ij}) = -A$. The theorem of Kirchhoff and Tutte (see [Tu], 3.6 on p. 470) states that the sum of $A(T)$, where T runs over all subtrees of Γ converging to a fixed vertex t (i.e., with root t), equals the (t, t) minor of (c_{ij}) . For easier reference later on we are stating it directly for the matrix A here:

THEOREM 4 (Kirchhoff-Tutte). — The (t, t) minor A_t of A is given by the following formula:

$$(*) \quad A_t = (-1)^{s-1} \sum_{\substack{T \text{ a tree on } I \\ \sqrt{T}=t}} A(T).$$

Proof. — The proof in [Tu] is rather difficult to understand, so we include a sketch of proof based on ideas of Kasteleyn (see [Ka], p. 79). It is easy to see that both sides of (*) do not depend on the t -th row of A at all and that they both are multilinear in the other $s-1$ rows. Hence it is enough to prove (*) for matrices of the following shape: the t -th row is zero, every other row has 1 at the diagonal position, one other entry -1 , and all the remaining entries zero. Now there is a one-to-one correspondence between the set of all these matrices and the set of all digraphs (without self-loops) on I where the out-degree of j is 1 if $j \neq t$ and 0 if $j = t$ (the arrows of such a digraph correspond to the positions of -1 's in the matrix). If such a digraph is not a tree then it has to contain a circle and both sides of (*) equals 0 (the sum of rows corresponding to the circle is zero, so the minor is zero, on the other hand each summand on the right-hand side is zero). If such a digraph is a tree then both sides of (*) equals 1 (there is a common reordering of rows and columns which changes A into an upper-triangular matrix, while there is just one non-zero summand on the right-hand side). \square

4. More on trees, and some linear algebra.

We review some notation and introduce some more:

Let p_1, \dots, p_s be distinct primes all congruent to 1 modulo l (a fixed odd prime); let K_i be the degree l subfield of $\mathbb{Q}(\zeta_{p_i})$, \tilde{K} the compositum of all the K_i , σ_i a fixed generator of $G(K_i/\mathbb{Q})$, and $\tilde{G} = G(\tilde{K}/\mathbb{Q})$. (This cancels a previous meaning of \tilde{G} .) So with an evident abuse of notation, \tilde{G} is $\mathbb{Z}/l\mathbb{Z}$ -free with basis $\sigma_1, \dots, \sigma_s$. Let $K \subset \tilde{K}$ be the subfield fixed by the subgroup generated by $\sigma_1\sigma_2^{-1}, \dots, \sigma_{s-1}\sigma_s^{-1}$. Thus K is cyclic of degree l ; if G denotes its Galois group over \mathbb{Q} , then G is generated by σ , the common image of all σ_i in G . We set $I = \{1, \dots, s\}$.

Later on (when we use Euler systems) we shall also use auxiliary primes q_1, \dots, q_{s-1} . For notational reasons we put $q_i = p_{s+i}$ for $i = 1, \dots, s-1$; let $I' = \{s+1, \dots, 2s-1\}$.

We previously chose a generator σ_i of $\text{Gal}(K_i/\mathbb{Q})$ for all $i \in I \cup I'$ (in fact for $i \in I'$ we even had to choose a generator of $\text{Gal}(\mathbb{Q}(\zeta_{p_i})/\mathbb{Q})$, and we abuse notation in letting stand σ_i for the restriction to K_i as well), and we defined a reciprocity matrix $A = (a_{ij})$ of shape $2s - 1$ by $2s - 1$ as follows: the Frobenius of p_i in K_j is $\sigma_j^{a_{ij}}$ for $i \neq j$, and all row sums of A are equal to zero (this defines the diagonal of A).

The link with Euler systems will come from Theorem 3 above. Note that in this theorem it does not matter that A is only defined modulo l .

We have a look at the statement of Theorem 3. Let us think of the indices $i \in I$ as blue vertices and the indices $i \in I'$ as orange vertices. A blue tree will just mean a tree on I . Call a tree T on $I \cup I'$ *well-colored* if all orange vertices have valency (that is, in-degree) 1, and the root is blue. (Then the leaves are blue, too.) We have the following lemma:

LEMMA 10. — *A tree T on $I \cup I'$ whose root and leaves are blue, and which has no two orange vertices connected by an edge, is already well-colored.*

Proof. — We define a map $a : I \rightarrow I$ by sending each orange vertex to some blue vertex directly above it (this is possible since no orange vertex is a leaf). Clearly a is injective and misses the root, so it is bijective, which shows that every orange vertex has exactly one (blue) vertex directly above it. \square

We look at the exponent b_i of p_i on the right hand side in Theorem 3, but only for $i \in I$ (a blue vertex). The expression for b_i involves a sum running over all trees with root i such that the valency of every orange vertex is 1, in other words, over all well-colored trees. This will be very useful since well-colored trees also show up in the context of determinants as follows:

Let us consider a general matrix B with integer coefficients, with rows and columns indexed by $I \cup I'$. We suppose that the southeast square block indexed by $I' \times I'$ is zero and further that the all row sums are zero. Thus B is a block matrix

$$\begin{pmatrix} * & S \\ U & 0 \end{pmatrix},$$

with U an $I' \times I$ -matrix with all row sums zero, and S an $I \times I'$ -matrix. So neither U nor S are square matrices: U has an excess column and S an excess row. Let U_i (resp. S_i) denote the square matrix obtained by

deleting the i -th column from U (resp. i -th row from S). The Kirchhoff-Tutte theorem (see Theorem 4) boils down to the following:

LEMMA 11. — *Under the above hypotheses on the matrix B we have for all $i \in I$:*

$$\det(S_i) \cdot \det(U_i) = (-1)^{s-1} \sum_{\substack{\sqrt{T}=i \\ T \text{ on } IU \cup I' \text{ well-colored}}} B(T).$$

Proof. — We claim that the right hand sum is unchanged when we omit the restriction that T be well-colored. It is no problem to admit all T containing an orange-orange edge, because $B(T)$ is zero for these. A tree T with no orange-orange edge and with blue root is either already well-colored, or, by Lemma 10, it must have an orange leaf. For the rest of the proof we only deal with trees not having any orange-orange edge. Then we can show that the sum $\sum B(T)$ over all T having at least one orange leaf is zero. In fact, for any nonempty $J \subset I'$ let L_J be the set of all trees whose set of orange leaves is just J . Pick $r \in J$; then a tree $T \in L_J$ is given by a tree T' on $I \cup I' - \{r\}$ and the specification of an $i \in I$, the (blue!) vertex i just below r , and $B(T) = B(T')b_{r,i}$. Our hypothesis that the row sums of B are all zero now yields $\sum_{T \in L_J} B(T) = 0$.

Now, by Theorem 4, the full sum $\sum_{\sqrt{T}=i} B(T)$ equals $(-1)^{2s-1-1} B_i = B_i$. (For a square matrix B , B_i is the (i, i) -minor of B .) It is easy to see that the minor B_i is equal to $(-1)^{s-1} \det(S_i) \det(U_i)$. □

Now we connect this with Theorem 3. We make an assumption:

Splitting Assumption. — For all $i, j = 1, \dots, s - 1$ such that $i \neq j$, the prime q_i is (totally) split in the field of conductor q_j and degree l over \mathbb{Q} , and (totally) split in K .

The first part of this assumption is tantamount to: the $I' \times I'$ block of the reciprocity matrix A is zero off the diagonal. The second part of the assumption is easily seen to be equivalent to: the row sums of U are zero. Since the overall row sums in the whole matrix A are zero by construction, we see that under the Splitting Assumption, the entire $I' \times I'$ block of A is zero.

Under this assumption we may write $A = \begin{pmatrix} * & S \\ U & 0 \end{pmatrix}$ as we did before for B . Theorem 3 together with Lemma 11 yields (note that the factor $(-1)^{s'-s+1}$ from Theorem 3 has now become just a minus sign, because of the factor $(-1)^{s-1}$ in the last lemma and since $s' = 2s - 1$):

THEOREM 5. — *The Splitting Assumption implies that*

$$\beta \equiv (u \cdot p_1^{E_1} \cdots p_s^{E_s})^{-l^{s-2}}$$

modulo l^{s-1} -powers, where the exponents are given by

$$E_i = \det(S_i) \det(U_i),$$

and u is an integer divisible only by primes among q_1, \dots, q_{s-1} . □

To conclude this section, we put a technical result on record.

The exterior product on the vector space of column vectors $V = k^n$ (k any field whatsoever) is defined as follows: One has the canonical pairing $\langle -, - \rangle : V \times V \rightarrow k$ given by $\langle (x_1, \dots, x_n), (y_1, \dots, y_n) \rangle = x_1 y_1 + \dots + x_n y_n$. Then for any $(n - 1)$ -tuple of vectors t_1, \dots, t_{n-1} , the exterior product $T = t_1 \times \cdots \times t_{n-1}$ is the unique vector satisfying $\det(t_1, \dots, t_{n-1}, v) = \langle T, v \rangle$ for all $v \in V$. It is easy to express this by determinants: let τ be the matrix whose columns are t_1 through t_{n-1} . Then $T_i = (-1)^{n+i} \det(\tau_i)$. (Again, τ_i is obtained from τ by deleting the i -th row.) We then have the following result which we dub the Multilinear Lemma.

LEMMA 12. — *Suppose given two $(n - 1)$ -tuples w_1, \dots, w_{n-1} and t_1, \dots, t_{n-1} of column vectors in V ; let $T = t_1 \times \cdots \times t_{n-1}$. Then*

$$\det(w_1, \dots, w_{n-1}, T) = \det(\langle w_i, t_j \rangle)_{1 \leq i, j \leq n-1}.$$

Proof. — The function $\det(w_1, \dots, w_{n-1}, T)$ is linear in every w_i , and in every t_j ; moreover, it is alternating in the w 's, and alternating in the t 's. All this is just as true for the determinant on the right hand side of the statement. We may thus suppose that we are in the following special situation: The $(n - 1)$ -tuple of the w 's is the tuple obtained from the canonical basis n -tuple (e_1, \dots, e_n) by deleting exactly one entry, let us say e_k ; likewise the tuple of the t 's is obtained by deleting e_l from (e_1, \dots, e_n) . If $k \neq l$, then $T = \pm e_l$ and the left hand side in the statement vanishes. So does the right hand side: the determinant we got there is obtained by deleting row k and column l from the identity matrix of size $n \times n$, and this results in a singular matrix if $k \neq l$. We may therefore assume that $k = l$, so the string of w 's actually coincides with the string of t 's. Then the matrix $(\langle w_i, t_j \rangle)_{1 \leq i, j \leq n-1}$ is the identity matrix of rank $n - 1$, so its determinant is 1. On the left hand side we find $\det(w_1, \dots, w_{n-1}, T) = \det(t_1, \dots, t_{n-1}, T) = \langle T, T \rangle$ which is also 1 since $T = \pm e_k$. □

5. How to calculate certain valuations.

The following result provides the link between the tree calculus and the valuations that we need further on in the proof. Recall K is cyclic of degree l over \mathbb{Q} , ramified in the rational primes p_1, \dots, p_s , and $G = \langle \sigma \rangle = \text{Gal}(K/\mathbb{Q})$. Put $\lambda = \sigma - 1 \in \mathbb{Z}[G]$. As in the first section, we let $\Delta = \Delta_\sigma = \sum_{a=1}^{l-1} a\sigma^a$.

LEMMA 13. — *Let K/\mathbb{Q} be any G -Galois extension, and assume p_1, \dots, p_s (with $s > 1$) ramify (totally) in K . Denote the prime above p_i by \mathfrak{p}_i . Suppose $\eta \in K^*$ is in the kernel of N , the norm element of $\mathbb{Z}[G]$ acting on the multiplicative group K^* . Suppose further that there is a rational number r such that*

$$\eta^{\Delta^{s-1}} \equiv r \pmod{K^{*l^{s-1}}}.$$

Then

- (a) η is a λ^{s-1} -th power in K ;
- (b) Write $\eta = \alpha^{\lambda^{s-1}}$ with $\alpha \in K$. The rational number r is an l^{s-2} -th power, and if $p_i^{-l^{s-2}E_i}$ is the precise power of p_i dividing r , then $v_{\mathfrak{p}_i}(\alpha)$ is congruent to E_i modulo l .

Proof. — (a) We have $\eta^{l\Delta^{s-2}} = \eta^{(l-N)\Delta^{s-2}} = \eta^{(\sigma-1)\Delta^{s-1}}$. By our hypothesis, this last term is congruent to 1 modulo $K^{*(\sigma-1)l^{s-1}}$, that is, this last term is an l^{s-1} -th power in $P := K^{*\sigma-1}$. Thus, $\eta^{\Delta^{s-2}}$ is an l^{s-2} -th power in P . Now exponentiation by l is the same as exponentiation by $\lambda\Delta$ on P since P is killed by N ; therefore exponentiation by Δ is injective on P , because K does not contain the l -th roots of unity. From all this we may conclude that η is a λ^{s-2} -th power in P ; the definition of P now yields (a).

For (b) we calculate as follows: By the very hypothesis, $\alpha^{(\lambda\Delta)^{s-1}} \equiv r$ modulo $K^{*l^{s-1}}$. The evident equality $N^2 = lN$ gives $N(l-N) = 0$, so $(l-N)^2 = l(l-N)$, and by induction $(l-N)^i = l^{i-1}(l-N)$ for $i > 0$. This gives

$$\begin{aligned} (\lambda\Delta)^{s-1} &= (l-N)^{s-1} \\ &= l^{s-1} - N \cdot l^{s-2} \\ &\equiv -N \cdot l^{s-2} \pmod{l^{s-1}}. \end{aligned}$$

Therefore $\alpha^{-Nl^{s-2}} \equiv r$ modulo l^{s-1} -th powers. This implies that r is an l^{s-2} -th power in K , and hence also in \mathbb{Q} . Let us write $r =$

$(r'p_1^{E_1} \dots p_s^{E_s})^{-l^{s-2}}$, with r' not divisible by any p_i . Then $\alpha^N \equiv r'p_1^{E_1} \dots p_s^{E_s}$ modulo l -th powers. But α^N is rational. Again since $K^{*l} \cap \mathbb{Q} = \mathbb{Q}^{*l}$, we even have

$$\alpha^N \equiv r'p_1^{E_1} \dots p_s^{E_s} \pmod{\mathbb{Q}^{*l}}.$$

Finally, the exact exponent to which p_i divides α^N is $v_{p_i}(\alpha)$, which finishes the proof. □

It is vital in the preceding lemma to have an element η of norm one. We need another small lemma which will ensure later on that such a choice is possible in the construction of our Euler system.

LEMMA 14. — *If κ^N is an L -th power (in K or in \mathbb{Q} , this is the same thing), then there is a L/l -th power $\gamma \in K$, such that for $\kappa' = \gamma\kappa$ we obtain $\kappa'^N = 1$.*

Proof. — We can write $\kappa^N = t^L$ for some $t \in \mathbb{Q}$. Then it suffices to pose $\kappa' = t^{-L/l}\kappa$.

6. An outline of the main argument.

Here we explain how our Euler system is going to be set up, postponing some details to the next section. We also show how the Euler system once it is established will lead to the proof of the main result.

The starting point is the paper [RW]. There, an element $\alpha_\infty \in K$ is defined as the highest possible λ -power root of $N_{\mathbb{Q}(\zeta_l)/K}(1 - \zeta_l)$. We retain this element, but we will call it α_0 .

We know by genus theory (cf. [RW]) that on putting $R = \mathbb{Z}[G]/(N)$ we may write the l -part of the class group of K as follows (the isomorphism is an isomorphism of G -modules!):

$$cl(K)_l = \langle \mathbf{c}_1, \dots, \mathbf{c}_{s-1} \rangle \cong R/\lambda^{h_1} \oplus \dots \oplus R/\lambda^{h_{s-1}}.$$

Here h_1, \dots, h_{s-1} are positive integers. By this isomorphism, we do mean that the ideal class \mathbf{c}_i maps to a generator of the i -th summand of the right hand side. We then have $h_1 + \dots + h_{s-1} = h$, where l^h is the maximal power of l dividing h_K . The socle of $cl(K)_l$, that is, the maximal submodule killed by λ , is then $\mathbb{Z}/l\mathbb{Z}$ -free with basis $\mathbf{c}_1^{\lambda^{h_1-1}}, \dots, \mathbf{c}_{s-1}^{\lambda^{h_{s-1}-1}}$. We also need the obvious fact that all classes $[p_i]$ ($i = 1, \dots, s$) are in the socle.

Now, using a fairly standard Euler system, we shall successively find the following data for $i = 1, \dots, s - 1$: $\mathbf{q}_i, \kappa_i, \alpha_i$. Here \mathbf{q}_i is a prime in K

of degree one, with \mathfrak{q}_i in the class \mathfrak{c}_i , and q_i (the rational prime below \mathfrak{q}_i) is congruent to 1 modulo a high power L of l . Furthermore q_i will be an l -th power modulo q_j for all $i, j \in \{1, \dots, s-1\}$ with $i \neq j$. The elements $\kappa_i \in K$ are furnished by the Euler system as usual (we shall explain). The algebraic integers α_i are, roughly speaking, obtained from κ_i by extracting λ -power roots.

We need to specify the high l -power L : Let h^* be the smallest integer not smaller than $h/(l-1)$, and for $i = 0, \dots, s-1$ let $L_i = l^{h+1+(s-1-i)h^*}$. Thus, L_0, \dots, L_{s-1} is a sequence of l -powers with linearly decreasing exponents. We let $L = L_0$. Some more notation: If $0 \neq x, y$ are elements of a field E which is clear from the context, then $x \equiv_L y$ means that x/y is an L -th power of an element of E . If \mathfrak{b} and \mathfrak{c} are ideals in a field E which is clear from the context, then $\mathfrak{b} \equiv_L \mathfrak{c}$ means that $\mathfrak{b}/\mathfrak{c}$ is an L -th power of a (fractional) ideal in E . Thus $x \equiv_L y$ implies $(x) \equiv_L (y)$ but not vice-versa. A note to the reader: the precise choice of the l -powers in all congruences that follow is of course important, but should perhaps be ignored at first reading: think of all occurring l -powers just as “sufficiently high”.

We need to assure that the elements $\alpha_1, \dots, \alpha_{s-1}$ will have two properties, one coming from the statement of the lifted root number conjecture in [RW], and the other to make them fit our calculations. Let us state the first one:

$$(I) \quad (\alpha_i) \equiv_{L_i} \mathfrak{q}_i^{\lambda^{h_i-1}} \cdot \mathfrak{a}$$

where \mathfrak{a} is supported on the conjugates of the ideals \mathfrak{q}_j with $j < i$ and the ramified primes $\mathfrak{p}_1, \dots, \mathfrak{p}_s$. In order to see that these elements do fit in with [RW], we have to work a bit:

LEMMA 15. — *The determinant of the matrix*

$$V = \begin{pmatrix} -v_{\mathfrak{p}_1}(\alpha_0) & \cdots & -v_{\mathfrak{p}_s}(\alpha_0) \\ \vdots & & \vdots \\ -v_{\mathfrak{p}_1}(\alpha_{s-2}) & \cdots & -v_{\mathfrak{p}_s}(\alpha_{s-2}) \\ -v_{\mathfrak{p}_1}(\alpha_{s-1}) & \cdots & -v_{\mathfrak{p}_s}(\alpha_{s-1}) \end{pmatrix}$$

over $\mathbb{Z}/l\mathbb{Z}$ equals the quantity c' defined in [RW].

Proof. — We have to look at Lemma 5.1 in [RW] which mentions a quite similar matrix; let us however denote the elements in that matrix by α'_i and the matrix by V' to distinguish it from ours. We will show that V' is gotten from V by elementary operations on rows; of course this will prove $\det(V) = \det(V')$, and the latter equals c' by loc.cit.

The defining property of α'_i is $(\alpha'_i) = \mathfrak{q}_i^{\lambda^{h_i-1}} \mathbf{a}'$ with \mathbf{a}' supported on $\mathfrak{p}_1, \dots, \mathfrak{p}_s$. The element α'_i will be reached from α_i by induction over i (for $i = 0$ one takes $\alpha'_0 = \alpha_0$) and a combination of the following three operations: (1) multiply α_i by a product of conjugates of α_j 's with $j < i$; (2) multiply α_i by a rational factor; (3) multiply α_i by an l -th power in K . Then operations (2) and (3) do not even change the matrix V , and operation (1) amounts to row operations. In order to do the details, we now write

$$(\alpha_i) \equiv_{L_i} \mathfrak{q}_i^{\lambda^{h_i-1}} \mathfrak{q}_1^{x_1} \cdots \mathfrak{q}_{i-1}^{x_{i-1}} \mathbf{a}_2,$$

with \mathbf{a}_2 supported on $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ and all $x_j \in \mathbb{Z}[G]$. Then $[\mathbf{a}_2]$ is in the socle, so the product $\mathfrak{q}_1^{x_1} \cdots \mathfrak{q}_{i-1}^{x_{i-1}}$ is in the socle, and this forces that in $R := \mathbb{Z}[G]/(N)$, all exponents x_j become divisible by λ^{h_j-1} . One can therefore write $x_j = y_j \lambda^{h_j-1} + k_j N$; now \mathfrak{q}_j^N is generated by the rational prime q_j , so we can by dint of operation (2) assume that $k_j = 0$. By operation (1) one can achieve that y_1, \dots, y_{i-1} become zero. (Note here that L_i divides all L_j with $j < i$, so the congruence remains intact.) Since every L_i -th power of an ideal whose class is in $cl(K)_l$ is an l -th power of a principal ideal (we chose L_i divisible by l^{h+1}), operation (3) produces an α'_i which has the desired defining property $(\alpha'_i) = \mathfrak{q}_i^{\lambda^{h_i-1}} \mathbf{a}'$ as stated above. □

Let us now explain the second requirement. Associated to the set of primes $\mathfrak{p}_1, \dots, \mathfrak{p}_s, \mathfrak{q}_1, \dots, \mathfrak{q}_{s-1}$ we constructed a reciprocity matrix A ; one assumption made in the construction of the \mathfrak{q}_i ensures that A has the shape $\begin{pmatrix} * & S \\ U & 0 \end{pmatrix}$. The assumption is, then, that the matrix product

$$(II) \quad \begin{pmatrix} v_{\mathfrak{p}_1}(\alpha_0) & \cdots & v_{\mathfrak{p}_s}(\alpha_0) \\ \vdots & & \vdots \\ v_{\mathfrak{p}_1}(\alpha_{i-1}) & \cdots & v_{\mathfrak{p}_s}(\alpha_{i-1}) \end{pmatrix} \cdot S_{\leq i} \text{ is lower triangular with } -1 \text{ on the diagonal}$$

for $i \leq s - 1$, where $S_{\leq i}$ means the part of S having column index $\leq i$. The reader will instantly see that there is an apparent circularity in this condition, because the i -th column of S only becomes defined at the instant where \mathfrak{q}_i is chosen! This circularity will be eliminated as follows: one goes ahead and chooses the i -th row of S , just to fit (II), and then, by some happy coincidence, one is able to prove, after having chosen \mathfrak{q}_i , that this row is the right thing.

No use has yet been made of most of the previous work, that is: no valuation has yet been calculated explicitly! This is done only at the last

stage: Theorem 3 will be used to show that for $i = 1 \dots, s$ the following congruence holds modulo l :

$$(III) \quad v_{\mathfrak{p}_i}(\alpha_{s-1}) \equiv \det(S_i) \det(U_i).$$

The valuations of the α_i with $i < s - 1$ are not needed explicitly. This is not a reason for suspicion, because all these α_i are used very seriously in the making of the last one α_{s-1} .

Assuming (I)-(III), we shall now show how the Lifted Root Number Conjecture follows. Afterwards we shall supply the missing details of the construction.

Let T be the exterior product of the columns of S . Thus, $T_i = (-1)^{s+i} \det(S_i)$. Since the row sums of U are zero, we get $\det U_i = (-1)^{i-1} \det(U_1)$, so from (III) we get $v_{\mathfrak{p}_i}(\alpha_{s-1}) = (-1)^{i-1} \det(S_i) \det(U_1) = (-1)^{s-1} T_i \det(U_1)$. The Multilinear Lemma gives

$$\begin{aligned} \det \begin{pmatrix} v_{\mathfrak{p}_1}(\alpha_0) & \cdots & v_{\mathfrak{p}_s}(\alpha_0) \\ \vdots & & \vdots \\ v_{\mathfrak{p}_1}(\alpha_{s-2}) & \cdots & v_{\mathfrak{p}_s}(\alpha_{s-2}) \\ T_1 & \cdots & T_s \end{pmatrix} \\ = \det \begin{pmatrix} v_{\mathfrak{p}_1}(\alpha_0) & \cdots & v_{\mathfrak{p}_s}(\alpha_0) \\ \vdots & & \vdots \\ v_{\mathfrak{p}_1}(\alpha_{s-2}) & \cdots & v_{\mathfrak{p}_s}(\alpha_{s-2}) \end{pmatrix} \cdot S = (-1)^{s-1} \end{aligned}$$

using (II). From this we get

$$(*) \quad \det \begin{pmatrix} -v_{\mathfrak{p}_1}(\alpha_0) & \cdots & -v_{\mathfrak{p}_s}(\alpha_0) \\ \vdots & & \vdots \\ -v_{\mathfrak{p}_1}(\alpha_{s-2}) & \cdots & -v_{\mathfrak{p}_s}(\alpha_{s-2}) \\ -v_{\mathfrak{p}_1}(\alpha_{s-1}) & \cdots & -v_{\mathfrak{p}_s}(\alpha_{s-1}) \end{pmatrix} = (-1)^s \det(U_1).$$

On the left hand side, we have the determinant c' from 5.1 in [RW], by Lemma 15. Thus we must show that the right hand side is the determinant $c = \det(C)$ where $C = (c_{ij})$ is again defined in [RW]. We do this by relating C and U :

LEMMA 16. — U is obtained from C by deleting the first row of C (its index is 0, not 1), and by changing the signs of all the remaining entries.

Proof. — Let $1 \leq i \leq s - 1$. Then c_{ij} is given in [RW] by the equation $(q_i, K_{\mathfrak{p}_j} / \mathbb{Q}_{p_j}) = g_0^{c_{ij}}$. The left hand side is a local norm residue symbol, and

g_0 is in loc.cit. the chosen generator of $G = \text{Gal}(K/\mathbb{Q})$, which is σ in our notation. We recall: K_j is the degree l extension of \mathbb{Q} with conductor p_j ; σ_j is a fixed generator of $\text{Gal}(K_j/\mathbb{Q})$, extended in the obvious way to an automorphism of $\tilde{K} = K_1 \cdots K_s$, so that $\text{Gal}(\tilde{K}/\mathbb{Q})$ is the free $\mathbb{Z}/l\mathbb{Z}$ -vector space with basis $\sigma_1, \dots, \sigma_s$; and all σ_j restrict to σ . We pick a prime \mathfrak{p}_j of \tilde{K} over p_j and consider $\tau := (q_i, \tilde{K}_{\mathfrak{p}_j}/\mathbb{Q}_{p_j})$. Since the inertia group of p_j in $\text{Gal}(\tilde{K}/\mathbb{Q})$ is just $\langle \sigma_j \rangle$, we obtain $\tau = \sigma_j^a$ for some $a \in \mathbb{Z}/l\mathbb{Z}$. By looking at the restriction of τ to K_{p_j} we find $a = c_{ij}$. On the other hand we may restrict τ to $(K_j)_{\tilde{p}_j}$ where \tilde{p}_j is the prime of K_j below \mathfrak{p}_j . This gives the equality $(q_i, (K_j)_{\tilde{p}_j}/\mathbb{Q}_{p_j}) = \sigma_j^{c_{ij}}$. We now apply the product formula to the principal idèle q_i of the field \mathbb{Q} . This gives

$$1 = \prod_r (q_i, (K_j)_r/\mathbb{Q}_r).$$

Here r runs through all rational primes, and $(K_j)_r$ is short for $(K_j)_\tau$, τ a chosen extension of r . Now all terms on the right are 1 except possibly the terms for $r = p_j$ and $r = q_i$. We calculated the former; the latter equals the global Artin symbol (= Frobenius) $(\frac{K_j/\mathbb{Q}}{q_i})$ of q_i in K_j . This shows $(\frac{K_j/\mathbb{Q}}{q_i}) = \sigma_j^{-c_{ij}}$; our lemma follows, since we have by definition $(\frac{K_j/\mathbb{Q}}{q_i}) = \sigma_j^{u_{ij}}$. □

Since the sum of the first row of C is -1 (this is again shown with the product formula, and was also used in [RW] Section 7), we get

$$\begin{aligned} c = \det(C) &= -1 \det(C \text{ without row } 0, \text{ column } 1) \\ &= -\det(-U_1) = (-1)^s \det(U_1). \end{aligned}$$

This finally shows $c = c'$, so the Lifted Root Number Conjecture will be proved as soon as we shall have set up the Euler system with all required properties. This we do next.

7. Construction of the Euler system.

We already fixed a certain high power L of the prime l . The Euler system we will use is the following: to any list of primes $Q = \{q_1, \dots, q_i\}$ all congruent to 1 modulo Ll , one attaches the root of unity $\zeta_{(Q)} = \zeta_{q_1} \cdots \zeta_{q_i}$, and the element

$$\xi_Q = N_{\mathbb{Q}(\zeta_L, \zeta_{(Q)})/K(\zeta_{(Q)})}(1 - \zeta_L \zeta_{(Q)}),$$

exactly as in [RW]. The elements $\kappa_i = \kappa_Q$ are provided by the general theory; we shall recall their construction as soon as we need it. We use the following trick here: The results in [Ru] will sometimes be applied with the exponent Ll , sometimes (for instance Theorem 3.1) with the exponent L (Rubin’s notation for the exponent is always M). It is easy to see that the primes (λ in Rubin’s notation) produced by that theorem can be assumed to lie over a rational prime which is $\equiv 1$ modulo Ll , not only modulo L .

Before we start, we choose a rational prime q_0 once and for all, whose Frobenius on K is σ , as in [RW]. We shall require that in addition to condition (I) (see last section) all α_i be chosen as algebraic integers coprime to q_0 . (No problem with α_0 which is already chosen: it is supported only on the primes that ramify in K .)

Let us suppose $i \in \{1, \dots, s - 1\}$, and assume all q_j, κ_j, α_j with $j < i$ have already been constructed, such that

$$(*) \quad \alpha_j^{\lambda^{e_j}} = \kappa_j \cdot a$$

with $e_j > 0$ and a some product of conjugates of α_r ’s, $r < j$, in particular $a = 1$ for $j = 0$. For $i = 1$, we just need α_0 and κ_0 . The element α_0 has been defined already, and we let $\kappa_0 = \xi_\emptyset$. We will see that this fits into the general scheme.

The choice of the next prime q_i is governed by a certain G -homomorphism $\psi : V \rightarrow (\mathbb{Z}/L\mathbb{Z})[G]$. We choose V to be the G -submodule of $K^*/(K^*)^L$ generated by the following list $\alpha_0, \dots, \alpha_{i-1}; p_1, \dots, p_s; q_0$; and all rational primes $q \notin \{p_1, \dots, p_s\}$ which divide the norm of any α_j with $0 \leq j \leq i - 1$ (note q_0 will not be among them, but q_1, \dots, q_{i-1} will: this follows from condition (I) in §6 since α_j is an algebraic integer, so the factorisation of (α_j) must contain some conjugate of q_j and hence q_j divides the norm of α_j ; if one prefers, one may include q_1, \dots, q_{i-1} explicitly in the preceding list). The columns numbered 1 through $i - 1$ of S exist already; we pick $t_{*,i}$, the i -th column of S , to fulfil the requirements

$$\sum_{k=1}^s v_{p_k}(\alpha_j)t_{k,i} \equiv 0 \quad \text{for } 0 \leq j < i - 1;$$

$$\sum_{k=1}^s v_{p_k}(\alpha_{i-1})t_{k,i} \equiv -1.$$

The first condition is void for $i = 1$; all congruences are meant modulo L .

There are two very important things we have to say at once: (1) We announced that S is a block in the reciprocity matrix, and now we are picking a column of S almost at random! The trick is that we will prove, as soon as the induction step has been completed: $t_{k,i}$ is indeed the exponent t in $(p_k, K_{s+i}) = \sigma_{s+i}^t$. (2) The existence of the new column is not obvious and will be proved by induction over i . It is at least clear that this works for $i = 1$, since the row vector $(v_{p_k}(\alpha_0))$ is nonzero modulo l by [RW] (see Lemmas 2.1c) and 2.2(ii),(iii), or the proof of our Lemma 20).

We now can describe the map ψ we will use. Again, the proof of well-definedness is postponed. Thus, ψ is the unique G -homomorphism from V to $(\mathbb{Z}/L\mathbb{Z})[G]$ satisfying

$$\begin{aligned} \alpha_j &\mapsto 0 && \text{for } 0 \leq j < i - 1; \\ \alpha_{i-1} &\mapsto 1; \\ p_k &\mapsto -t_{k,i}N && \text{for } 1 \leq k \leq s; \\ q_0 &\mapsto N; \\ q &\mapsto 0. \end{aligned}$$

Recall that q runs over the rational primes except p_1, \dots, p_s which divide $N\alpha_j$ for some $0 \leq j \leq i - 1$. Note that for $i = 1$, the first and the last condition are void. We recall that $N = \sum_{a=0}^{l-1} \sigma^a \in \mathbb{Z}[G]$; sometimes N also denotes the norm $K \rightarrow \mathbb{Q}$, which should not lead to any confusion.

Now (assuming that ψ exists) we invoke Theorem 3.1 in [Ru] to find an unramified prime q_i in K of degree one, with the following properties:

- (i) q_i represents the class c_i ;
- (ii) q_i (the rational prime below q_i) is congruent 1 modulo $Llq_1 \cdots q_{i-1}$;
- (iii) for all $x \in V$, the q_i -adic value of x is $0 \in \mathbb{Z}/L\mathbb{Z}$, and $\varphi_{q_i}(x) = \mathfrak{q}_i^{u\psi(x)}$, for a unit u of $\mathbb{Z}/L\mathbb{Z}$. (The notation φ is again from [Ru] p.400ff.)

As in [RW] Lemma 6.1 we may achieve $u = 1$ by the device of changing the choice of generator of $\text{Gal}(\mathbb{Q}(\zeta_{q_i})/\mathbb{Q})$.

The condition $\varphi_{q_i}(q_j) = \mathfrak{q}_i^{u\psi(q_j)} = 0$ for $j < i$ entails in particular that q_j is an L -th power modulo q_i . We have as well that q_i is congruent to 1 modulo q_j by condition (ii). This will ensure our Splitting Condition and nullity of the southeast block of our reciprocity matrix A .

Now the general theory (see again [Ru]) provides an element $\kappa_i \in K$. We shall have to worry later about its actual construction, but right now

we only need the following. For all $x \in V$ we have by [Ru] Theorem 3.1 (iii):

$$\varphi_{\mathfrak{q}_i}(x) \equiv \mathfrak{q}_i^{\psi(x)}$$

modulo L -th powers of ideals. One checks from the definition and formula (*) that indeed $x = \kappa_{i-1} \in V$, and so we get by Proposition 2.4 of [Ru]:

$$(\kappa_i) \equiv \mathfrak{q}_i^{\psi(\kappa_{i-1})} \mathfrak{a}$$

modulo L -th powers of ideals, where \mathfrak{a} is supported on $\mathfrak{q}_1, \dots, \mathfrak{q}_{i-1}$. We prove right away:

LEMMA 17. — κ_i^N is an Ll -th power in \mathbb{Q} .

Proof. — We recall that all our \mathfrak{q}_j are congruent to 1 modulo Ll , not just L . Now Lemma 2.2 in [Ru] tells us that $\kappa_i = z_Q \beta$ with β an Ll -th power in $K(\zeta_{(Q)})$, where $Q = \{q_1, \dots, q_i\}$ and $z_Q = (1 - \zeta_I \zeta_{(Q)})^{D_{q_1} \cdots D_{q_i} \nu}$ where ν is the norm from $\mathbb{Q}(\zeta_I)$ to K .

It therefore suffices to show that z_Q^N is an Ll -th power in $K(\zeta_{(Q)})$. If we raise z_Q to the N , the exponent ν gets replaced by the absolute norm on $\mathbb{Q}(\zeta_I)$. Thus there exists an element γ in the augmentation ideal of $\text{Gal}(\mathbb{Q}(\zeta_{(Q)})/\mathbb{Q})$ (actually in its s -th power), such that $z_Q^N = (1 - \zeta_{(Q)})^{D_{q_1} \cdots D_{q_i} \gamma}$. It now follows as in Lemma 2.1 in [Ru] that this is an Ll -th power. (Our element $1 - \zeta_{(Q)}$ is not quite the same as Rubin’s ξ_r , but the reasoning is absolutely the same.) □

We are now in a position to apply Lemma 14 (with Ll instead of L of course), and assume that κ_i is in the kernel of the norm N from K to \mathbb{Q} without destroying the congruence $(\kappa_i) \equiv_L \mathfrak{q}_i^{\psi(\kappa_{i-1})}$.

Now define e_i as follows: it is the greatest natural number e such that the equation

$$\alpha^{\lambda^e} = \kappa_i \cdot a$$

is solvable, with $\alpha, a \in K^*$, and a a product of conjugates of α_j with $j < i$.

Let α_i be a chosen solution of this equation with $e = e_i$. (It is easy to see that the above solution cannot be solvable for arbitrarily high values of e , since λ^l is divisible by l in $\mathbb{Z}[G]$, and the term $\kappa_i \cdot a$ lies in a finitely generated multiplicative group.)

It is instantly clear from Hilbert 90 that $e_i \geq 1$ since κ_i is in the kernel of N ; thus any solution α_i may be at will multiplied by a rational number;

later on we shall use this liberty to achieve (among further properties) that α_i is an algebraic integer coprime to q_0 .

We now have a fairly long list of things which have to be proved by induction over i :

- (a) The column t_{*i} used in the above construction does exist;
- (b) $(p_k, K_{s+i}) = \sigma_{s+i}^{t_{k,i}}$ (the ex-post justification of our choice of the new column in the matrix S);
- (c) the map ψ is well-defined;
- (d) (α_i) is modulo L_i th powers of ideals supported on $\mathfrak{p}_1, \dots, \mathfrak{p}_s, \mathfrak{q}_1, \dots, \mathfrak{q}_i$;
- (e) we have the inequality $e_{i-1} - e_i \geq h_i - 1$.

Remarks. — (1) These conditions make sense from $i = 1$ onward, except (d), which makes sense, and is true, for $i = 0$ as well, by [RW], Lemma 2.2.

(2) From [RW], p.1f., we know that e_0 , the maximal exponent such that $\kappa_0 = \xi_\emptyset$ is a λ^e -th power, is exactly $h = h_1 + \dots + h_{s-1}$. (We use $s \geq 2$ implicitly, because otherwise κ_0 is not of absolute norm 1, and we need κ_0 to have absolute norm 1 to make sure that (1.3) in [RW] and our definition of e_0 agree. For $s = 1$, the Lifted Root Number Conjecture is true; see [RW].)

We now proceed to prove (a)–(e) for i , assuming of course that everything is proved for $j < i$.

Proof of (a). — It was already said that this presents no problem for $i = 1$; let us suppose $i \geq 2$. For any $x \in K^*$, let $v(x)$ stand for the vector $(v_{\mathfrak{p}_1}(x), \dots, v_{\mathfrak{p}_s}(x))$ taken modulo l . By obvious linear algebra over the field $\mathbb{Z}/l\mathbb{Z}$, the column t_{*i} fulfilling the requirements specified above exists if and only if $v(\alpha_{i-1})$ is not in the span of $v(\alpha_0), \dots, v(\alpha_{i-2})$. Just suppose the contrary; we shall obtain a contradiction with the maximality of e_{i-1} . We recall that e_{i-1} is not zero.

Thus we suppose there is a multiplicative combination ε of $\alpha_0, \dots, \alpha_{i-2}$ such that $v(\alpha_{i-1}) = v(\varepsilon)$. We look at $x = \alpha_{i-1}/\varepsilon$ and the factorisation of the ideal (x) . Then $v_{\mathfrak{p}_i}(x)$ can be written as $n_i l$ with $n_i \in \mathbb{Z}$, and we have a congruence modulo L_{i-1} -th powers of ideals:

$$(x) \equiv \mathfrak{q}_1^{\delta_1} \cdots \mathfrak{q}_{i-1}^{\delta_{i-1}} \mathfrak{p}_1^{n_1 l} \cdots \mathfrak{p}_s^{n_s l}$$

with exponents $\delta_j \in \mathbb{Z}G$. Then the $\mathfrak{p}_j^{n_j l}$ are all principal. As in the proof of Lemma 15 we see that then the image of δ_j in $R = \mathbb{Z}G/(\mathbb{N})$ must be divisible by λ for $1 \leq j \leq s - 1$; so we can write $\delta_j = (\sigma - 1)\delta'_j + k_j \mathbb{N}$ for suitable $\delta'_j \in \mathbb{Z}G$ and $k_j \in \mathbb{Z}$. If we let $r = q_1^{-k_1} \cdots q_{i-1}^{-k_{i-1}} p_1^{-n_1} \cdots p_s^{-n_s}$ and $y = xr$, then the fractional ideal $(y^{\mathbb{N}})$ is (1) modulo an L_{i-1} -th power of an ideal. If we change r suitably by a L' -th power of a rational number ($L' = L_{i-1}/l^{h+1}$), then actually $(y^{\mathbb{N}})$ becomes the unit ideal, so the rational number $y^{\mathbb{N}}$ is ± 1 , and of course we may assume it is 1. By Hilbert 90 we can find some $\gamma \in K$ with

$$xr = y = \gamma^\lambda.$$

In other words, $\alpha_{i-1} = \varepsilon r^{-1} \gamma^\lambda$. On raising this to the power $\lambda^{e_{i-1}}$ (note that $e_{i-1} > 0$) we find

$$a \kappa_{i-1} = \alpha_{i-1}^{\lambda^{e_{i-1}}} = \varepsilon^{\lambda^{e_{i-1}}} \gamma^{\lambda^{e_{i-1}+1}}$$

for some product a of conjugates of α_j 's with $j < i - 1$. Now $\varepsilon^{\lambda^{e_{i-1}}}$ is just as well a product of conjugates of α_j with $j < i - 1$, and we may stuff it into a ; thus we have achieved a contradiction with the maximality of e_{i-1} , see its definition above!

Proof of (b). — This is already proved in [RW] Lemma 6.1(iii). Their \hat{G} is our \mathbb{N} ; t is chosen to be our $-t_{k,i}$, which does fit, given our definition of the homomorphism ψ (same notation in [RW]).

Proof of (c). — (1) We claim that $\alpha_{i-1} = \beta^\lambda \cdot r \cdot A$, with A any product of conjugates of $\alpha_0, \dots, \alpha_{i-2}$, and r rational, has no solution in K . Indeed, if it did, then (since e_{i-1} is positive) we would get $\beta^{\lambda^{e_{i-1}+1}} = \kappa_{i-1} \cdot A'$, contradicting the maximality of e_{i-1} .

(2) Let V' be the submodule of V generated by the following list of rational primes: $p_1, \dots, p_s; q_0$; and all $q \notin \{p_1, \dots, p_s\}$ dividing some $\mathbb{N}\alpha_j$ with $j \leq i - 1$. Let $R = \mathbb{Z}[G]/(\mathbb{N})$. Then V/V' is an R -module since the norms of the α_j ($j < i$) are rational numbers supported on p_1, \dots, p_s , and the set of the primes q , hence belong to V' . We claim that (the classes of) $\alpha_0, \dots, \alpha_{i-1}$ constitute an R/LR -basis of V/V' . We will even show that the images of these elements are R/LR -independent in M/LM , where $M = K^*/\mathbb{Q}^*$. This goes as follows: M is a torsion-free R -module, and there is the following general lemma which is easy to prove, taking into account that R is a Dedekind ring:

LEMMA 18. — *Let M be a torsion-free R -module, $L > 1$ any l -power, $x_1, \dots, x_n \in M$. Then the images of the x_i in M/LM are independent*

over R/LR iff the images of the x_i in $M/\lambda M$ are independent over $R/\lambda = \mathbb{Z}/l\mathbb{Z}$. □

Applying this lemma to $\alpha_0, \dots, \alpha_{i-1}$ substituted for the list x_1, \dots, x_n , we are reduced to showing that there is no nontrivial dependence relation between the α 's in $M \bmod \lambda$ -th powers. In other words, there should be no product of the α 's with exponents in $\{0, \dots, l - 1\}$, not all zero, which is equal to a rational number times a λ -th power. If there is such a product, it must involve α_{i-1} , by induction. But then the existence of such a product leads to a contradiction, as explained in (1) above.

(3) The module V has an explicit presentation with two lists of generators: first, the rational primes p_1, \dots, p_s, q_0 along with the rational primes q (see above) and second α_0 through α_{i-1} . There are two types of relations: (a) the rational primes are not moved by G , and (b) the norm relations; $N(\alpha) = \prod_r r^{v_r(N(\alpha))}$, with α running through $\alpha_0, \dots, \alpha_{i-1}$, and r running through the rational primes in the first list. It is a consequence of (2) that we already have found all the relations. It is now easily checked that ψ is well-defined: it preserves all the relations. For instance $N(\alpha_{i-1}) = \prod_{j=1}^s p_j^{v_{p_j}(\alpha_{i-1})} q^*$ is a relation (q^* is a number only divisible by primes q , that is, primes in V' but different from all p_i and q_0); applying ψ gives the relation

$$N = \sum_{j=1}^s (-t_{j,i}) N_{v_{p_j}}(\alpha_{i-1})$$

which is true since $\sum_{j=1}^s t_{j,i} v_{p_j}(\alpha_{i-1}) = -1$; similarly for the other cases.

Proof of (d) and (e).— We know that the map ψ exists; at the previous step we chose α_{i-1} subject to $\alpha_{i-1}^{\lambda^{e_i-1}} = \kappa_{i-1} a$ with a some product of conjugates of $\alpha_j, j < i - 1$. It then follows immediately from the definition of ψ that

$$\psi(\kappa_{i-1}) = \lambda^{e_i-1}.$$

Consequently, by [Ru] Proposition 2.4, we get

$$(\kappa_i) \equiv_L \mathfrak{q}_i^{\lambda^{e_i-1}} \mathfrak{a}$$

with \mathfrak{a} supported on $\mathfrak{q}_1, \dots, \mathfrak{q}_{i-1}$. We recall $\alpha_i^{\lambda^{e_i}} = \kappa_i a$, with a some multiplicative combination of conjugates of the α_j for $j \leq i - 1$. Now let \mathfrak{p} be any prime of K which is totally split from \mathbb{Q} . We want to determine the \mathfrak{p} -part of the ideal (α_i) , that is, the exponent $x(\mathfrak{p}) \in \mathbb{Z}[G]$ such that

$(\alpha_i) = \mathfrak{p}^{x(\mathfrak{p})}\mathfrak{d}$, with \mathfrak{d} coprime to all conjugates of \mathfrak{p} . We need a small algebraic lemma:

LEMMA 19. — *Let n, e be positive integers. Then the annihilator of multiplication by λ^e on $\mathbb{Z}[G]/(l^n)$ is contained in the ideal generated by N and l^{n-e^*} , where e^* is the smallest integer not less than $e/(l-1)$.*

Proof. — Recall $R = \mathbb{Z}[G]/(N)$; this is a Dedekind ring. Denote the canonical map $\mathbb{Z}[G] \rightarrow R$ by an overbar. Then $\bar{\lambda}$ is a prime element of R , and $\bar{\lambda}^{l-1}$ is associated to l . Suppose $x \in \mathbb{Z}[G]/(l^n)$ is killed by the factor λ^e . Then $\bar{\lambda}^e \bar{x} = 0$ in $R/(l^n)$, which easily implies that $\bar{x} \in R/(l^n)$ is a multiple of l^{n-e^*} ; the lemma follows. \square

This is now applied as follows: Recall that $L_i = L_{i-1}/l^{h^*}$. For each $j \leq i-1$, we have α_j supported on $\mathfrak{p}_1, \dots, \mathfrak{p}_s, \mathfrak{q}_1, \dots, \mathfrak{q}_j$ modulo L_j th powers of ideals. Thus $(\kappa_i a)$ is supported on $\mathfrak{p}_1, \dots, \mathfrak{p}_s, \mathfrak{q}_1, \dots, \mathfrak{q}_i$ modulo L_{i-1} th powers of ideals. Therefore we obtain for every split prime \mathfrak{p} of K , with the help of Lemma 19: If \mathfrak{p} is not among $\mathfrak{q}_1, \dots, \mathfrak{q}_i$, then the exponent $x(\mathfrak{p})$ in the factorisation of α_i modulo L_i is a multiple of the norm; if $\mathfrak{p} = \mathfrak{q}_i$, then one first finds $e_i \leq e_{i-1}$ since $\lambda^{e_{i-1}}$ must be a multiple of λ^{e_i} in $\mathbb{Z}[G]/(N, L_{i-1})$, and we may by induction assume $e_{i-1} \leq e_0 = h$, and l^h properly divides the l -power L_{i-1} . Thus $e_i \leq h$, and the term e_i^* in Lemma 19 can be majorized by h^* . By Lemma 19 we now get $x(\mathfrak{q}_i) \equiv \lambda^{e_{i-1}-e_i}$ modulo the ideal (N, L_i) . Since the ideal \mathfrak{p}^N is generated by a rational prime, just as all inert primes of K , we get

$$(**) \quad (\alpha_i) \equiv_{L_i} r \mathfrak{q}_i^{\lambda^{e_{i-1}-e_i}} \mathfrak{a}',$$

where r is a nonzero rational number and the ideal \mathfrak{a}' is supported on the ideals $\mathfrak{p}_1, \dots, \mathfrak{p}_s$ and the conjugates of $\mathfrak{q}_1, \dots, \mathfrak{q}_{i-1}$. It is clear that it is possible to replace α_i by a rational multiple such that it becomes an algebraic integer and the multiplicative congruence $(**)$ holds with $r = 1$. Then the value $v = v_{q_0}(\alpha_i)$ is a multiple of L_i , by $(**)$, and via replacing α_i by $\alpha_i q_0^{-v}$ we achieve that α_i is coprime to q_0 , still an algebraic integer, and $(**)$ is not spoiled by this change. This proves (d).

Now we look at the structure of $cl(K)$ again. The classes $[\mathfrak{p}_j]$ ($j = 1, \dots, s$) generate the socle (=largest submodule killed by λ) of the l -part of $cl(K)$. This is proved in [RW]; actually we only need that $[\mathfrak{p}_j]$ is in the socle, and this is clear. Let us split $\mathfrak{a}' = \mathfrak{a}_1 \mathfrak{a}_2$, \mathfrak{a}_1 supported on $\mathfrak{p}_1, \dots, \mathfrak{p}_s$, and \mathfrak{a}_2 supported on the conjugates of the \mathfrak{q}_j with $j < i$. Then since l^h

divides L_i , the congruence (**) shows that the class of

$$q_i^{\lambda^{e_{i-1}-e_i}} a_2$$

must be in the socle. Since the socle is the direct sum of the cyclic modules generated by $q_j^{\lambda^{h_j-1}}$ ($j = 1, \dots, s$), we obtain the conclusion $e_{i-1} - e_i \geq h_i - 1$, as claimed. This finishes the setup of the induction.

We now proceed to prove that (I)-(III) hold. The last inequality $e_{i-1} - e_i \geq h_i - 1$, together with $e_0 = h = h_1 + \dots + h_{s-1}$ yields

$$e_i \leq i + h_{i+1} + \dots + h_{s-1}$$

for all i , so

$$e_{s-1} \leq s - 1,$$

and this inequality is strict if there is at least one i such that $e_{i-1} - e_i > h_i - 1$. We will presently show that

$$e_{s-1} \geq s - 1.$$

This will show that $e_{i-1} - e_i = h_i - 1$ always; therefore formula (**) shows that α_i satisfies requirement (I).

The final step of the argument is now the proof of formula (III), and concomitantly of the inequality $e_{s-1} \geq s - 1$. It is only at this late stage that the complicated explicit calculations of §1–§2 are brought to bear.

The element κ_{s-1} is by construction (see [Ru], Lemma 2.2) congruent modulo an L -th power to

$$x = \xi_{\{q_1, \dots, q_{s-1}\}}^{D(w_1)} = N_{\mathbb{Q}(\zeta_l, \zeta_{l'})/\bar{K}(\zeta_{l'})}(1 - \zeta_{l \cup l'})^{D(w_1)\Gamma}.$$

We recall notation: q_i is written p_{s+i} ; the notation $D(v)$ in general is defined prior to Theorem 1, and w_1 is the constant map on $\{s + 1, \dots, 2s - 1\}$ with value 1. Thus, $D(w_1)$ is the product $D_{s+1}^{(1)} \cdots D_{2s-1}^{(1)}$ (notation before Theorem 1 again). The element Γ is the norm element in the group ring $\mathbb{Z}[\text{Gal}(\bar{K}/K)]$. Finally, $\Delta = \sum_{a=1}^{l-1} a\sigma^a$ with σ a generator of $\text{Gal}(K/\mathbb{Q})$. Then $x^{\Delta^{s-1}}$ is the element β of Theorem 3 and 5. (Here $\Delta = \Delta_\sigma \in \mathbb{Z}[\text{Gal}(K/\mathbb{Q})]$.) We apply Theorem 5: this says that

$$x^{\Delta^{s-1}} \equiv_{l^{s-1}} \prod_{i \in I \cup I'} p_i^{-l^{s-2} E_i},$$

with $E_i = \det(S_i) \det(U_i)$ for $i \in I$. The same congruence then holds for $\kappa_{s-1}^{\Delta^{s-1}}$ instead of $x^{\Delta^{s-1}}$. Since we arranged for κ_{s-1} to be in the kernel of the norm N , right after the proof of Lemma 17, we now get from Lemma 13: The equation

$$\alpha^{\lambda^{s-1}} = \kappa_{s-1}$$

is solvable, and we have $v_{p_i}(\alpha) \equiv E_i$ modulo l for $i = 1, \dots, s$. This means that in the recursion just completed above, $e_{s-1} \geq s-1$, hence $e_{s-1} = s-1$, and α_{s-1} can be taken to be α . This proves (III). Since (II) holds by construction, it follows, as showed in the previous section, that $c = c'$. As proved in [RW] (see in particular the introduction, and the end of §5 (formula (LC)) of loc.cit.), the equality $c = c'$ in $(\mathbb{Z}/l\mathbb{Z})^*$ is, finally, equivalent to:

THEOREM 6. — *The Lifted Root Number Conjecture (LRNC) holds for all cyclic tame extensions of \mathbb{Q} of odd prime degree.* \square

Let us recall here that (at least for abelian extensions of \mathbb{Q}) the LRNC as formulated by Gruenberg, Ritter, and Weiss is equivalent to a special case of the Equivariant Tamagawa Number Conjecture formulated by Burns and Flach.

8. A theorem of Rédei-Reichardt type.

We resume the following setting: K/\mathbb{Q} is a tame abelian extension of odd prime degree l ; let $p_1 \cdots p_s$ be its conductor and assume $s \geq 2$. Then we have the reciprocity matrix $A = (a_{ij})$ of shape $s \times s$ over $\mathbb{Z}/l\mathbb{Z}$, defined by $\sigma_j^{a_{i,j}} = (p_i, K_j)$ for $i \neq j$, and the requirement that all row sums are zero. Here K_j is the field of degree l and conductor p_j ; each σ_j is the generator of $\text{Gal}(K_j/\mathbb{Q})$ obtained as follows: lift the fixed generator σ of $G = \text{Gal}(K/\mathbb{Q})$ to the inertia group of KK_j/\mathbb{Q} (this is uniquely possible), and restrict this lift to K_j . Moreover (p_i, K_j) is the Frobenius of p_i on K_j . Put $\tilde{K} = K_1 \cdots K_s$.

Let C denote the l -primary part of $cl(K)$. Then C is a module over $R_l = \mathbb{Z}_l[\sigma]/(N) \cong \mathbb{Z}_l[\zeta_l]$ as before. The λ^2 -rank of C is defined as the number of invariants f_i divisible by λ^2 in any direct sum decomposition $C \cong \bigoplus_i R_l/f_i R_l$; note that R_l is a discrete valuation ring with parameter λ . We have the following generalized Rédei-Reichardt theorem whose proof is surprisingly simple (it essentially also works for $l = 2$):

THEOREM 7. — *With the above notation, the λ^2 -rank of C equals $s - 1 - rk(A)$.*

Proof. — If $C[\lambda]$ denotes the submodule of elements annihilated by λ , we have the following algebraic result whose proof is immediate:

$$rk_{\lambda^2}(C) = \dim_{\mathbb{Z}/l\mathbb{Z}} \ker(\iota : C[\lambda] \rightarrow C/\lambda C),$$

with ι the map induced by the identity on C . From genus theory we use that the global Artin symbol induces an isomorphism

$$\phi : C/\lambda C \rightarrow \text{Gal}(\tilde{K}/K).$$

The group $\text{Gal}(\tilde{K}/K)$ is a subgroup of $\text{Gal}(\tilde{K}/\mathbb{Q})$ which is a $\mathbb{Z}/l\mathbb{Z}$ -vectorspace with basis $\sigma_1, \dots, \sigma_l$. We shall show:

If one identifies $\text{Gal}(\tilde{K}/\mathbb{Q})$ with $(\mathbb{Z}/l\mathbb{Z})^s$ using the basis $\sigma_1, \dots, \sigma_l$, then the image of $\phi\iota$ is precisely the row space of A .

This statement, in conjunction with the above-mentioned algebraic result, will prove the theorem, since one has the equality

$$\dim_{\mathbb{Z}_l}(\ker(\phi\iota)) = s - 1 - \dim_{\mathbb{Z}_l}(\text{im}(\phi\iota)),$$

due to $\dim_{\mathbb{Z}_l} C[\lambda] = \dim_{\mathbb{Z}_l} C/\lambda C = s - 1$.

Now we know from [RW] that $C[\lambda] = C^G$ is generated by the classes $[\mathfrak{p}_i]$ of the ramified primes. We just have to show

$$\phi\iota[\mathfrak{p}_i] = \prod_{j=1}^s \sigma_j^{a_{ij}}.$$

But this is little more than the definition! Fix $j \neq i$, and let $\tau = \phi\iota([\mathfrak{p}_i])$. Then $\tau|_{KK_j}$ is the Frobenius of \mathfrak{p}_i in the extension KK_j/K . By a standard result (see for instance [N], Proposition IV 6.4), this maps to the Frobenius of p_i in K_j/\mathbb{Q} under the canonical identification $\text{Gal}(KK_j/K) = \text{Gal}(K/\mathbb{Q})$. This shows that the exponent with which σ_j occurs in τ is precisely a_{ij} . The case $i = j$ follows, too, since $\sum_{j=1}^s a_{ij} = 0$ and since τ is in $\text{Gal}(\tilde{K}/K)$ which contains exactly all $\prod_{j=1}^s \sigma_j^{c_j}$ with $\sum_{j=1}^s c_j = 0$. This finishes the proof. \square

Now we interpret this theorem in the light of our theory. Actually our theory reproves a part of Theorem 7 by an entirely different method: the λ^2 -rank of C is positive iff A has rank less than $s - 1$. Let us show how this goes. We begin with the obvious remark that the λ^2 -rank of C is positive iff l^s divides the class number h_K . We will now examine this latter property.

Let l^h be the precise l -power dividing h_K and put $\xi = N_{\mathbb{Q}(\zeta_{p_1}, \dots, \zeta_{p_s})/K} (1 - \zeta_{p_1} \cdots \zeta_{p_s}) = (1 - \zeta_l)^{T\Gamma}$ in the notation of §2. Then by [RW], h is the maximal integer such that

$$\alpha^{\lambda^h} = \xi$$

is solvable in $\alpha \in K$. Since $h \geq s - 1$ by genus theory (see loc.cit.), the equation $\beta^{\lambda^{s-1}} = \xi$ is solvable. Again by Ritter-Weiss, β in this equation is unique up to multiplication with a rational factor; one may assume β supported on the ramified primes $\mathfrak{p}_1, \dots, \mathfrak{p}_s$. Under this extra assumption, one can achieve that $v_{\mathfrak{p}_i}(\beta)$ is in the set $\{0, \dots, l - 1\}$ for $i = 1, \dots, s$ (multiply with suitable powers of p_i), and this finally makes β unique; let us call such a β normalized.

LEMMA 20. — $\alpha^{\lambda^s} = \xi$ is solvable (that is, $h \geq s$) if and only if for the normalized β above we have $v_{\mathfrak{p}_i}(\beta) = 0$ for all $i = 1, \dots, s$.

Proof. — Suppose $\alpha^{\lambda^s} = \xi$. Then $\beta = \alpha^\lambda$ is a normalized solution of $\beta^{\lambda^{s-1}} = \xi$ in which all $v_{\mathfrak{p}_i}(\beta)$ vanish. Conversely, if all $v_{\mathfrak{p}_i}(\beta)$ vanish, then β (being normalized) is a unit, so by Hilbert 90 we can write it in the form α^λ . \square

Let us also remark that the vector $(v_{\mathfrak{p}_i}(\beta))_i$ modulo l is the same for all solutions β . We now calculate this vector using our theory. By Theorem 3 (with $s = s'$) we have

$$\xi^{\Delta^{s-1}} \equiv \prod_{i=1}^s p_i^{-l^{s-2} E_i},$$

modulo l^{s-1} th powers, where

$$E_i = \sum_{\substack{T \text{ tree on } I \\ \sqrt{T}=i}} A(T).$$

By Lemma 13, $v_{\mathfrak{p}_i}(\beta) \equiv E_i \pmod{l}$ for all i . By Theorem 4, E_i is up to sign the (i, i) minor of A . Hence all $v_{\mathfrak{p}_i}(\beta)$ vanish modulo l iff all (i, i) minors of A vanish; but since all row sums of A are zero, the latter property is tantamount with the vanishing of all (i, j) -minors of A . Of course, this in its turn is equivalent to saying that A has corank at least two. This shows, as announced: $h \geq s$ iff A has rank less than $s - 1$.

BIBLIOGRAPHY

- [Bu] D. BURNS, Equivariant Tamagawa numbers and Galois module theory I, *Compositio Math.*, 127 (2001), 304-337.
- [BF] D. BURNS and M. FLACH, Equivariant Tamagawa numbers of motives, preprint 1998.
- [BG] D. BURNS and C. GREITHER, On the equivariant Tamagawa number conjecture for Tate motives, submitted for publication.
- [Deo] N. DEO, Graph theory with applications to engineering and computer science, Prentice-Hall, Englewood Cliffs 1974.
- [GRW] K.-W. GRUENBERG, J. RITTER, and A. WEISS, A local approach to Chinburg's root number formula, *Proc. London Math. Soc.* (3), 79 (1999), 47-80.
- [GRW1] K.-W. GRUENBERG, J. RITTER, and A. WEISS, On Chinburg's root number conjecture, *Jbr. Dt. Math.-Vereinigung*, 100 (1998), 36-44.
- [Hu] J. HURRELBRINK, Circulant graphs and 4-ranks of ideal class groups, *Can. J. Math.*, 46 (1994), 169-183.
- [Ka] P. W. KASTELEYN, Graph theory and crystal physics, in: *Graph theory and theoretical physics*, edited by F. Harary, Academic Press, New York, 1967.
- [N] J. NEUKIRCH, Algebraic number theory, *Grundlehren vol. 322*, Springer Verlag, New York, 1999.
- [R] L. RÉDEI, Arithmetischer Beweis des Satzes über die Anzahl der durch 4 teilbaren Invarianten der absoluten Klassengruppe im quadratischen Zahlkörper, *J. reine angew. Math.*, 171 (1935), 55-60.
- [RR] L. RÉDEI and H. REICHARDT, Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe eines beliebigen quadratischen Zahlkörpers, *J. reine angew. Math.*, 170 (1934), 69-74.
- [RW] J. RITTER and A. WEISS, The lifted root number conjecture for some cyclic extensions of \mathbb{Q} , *Acta Arithmetica*, XC.4 (1999), 313-340.
- [Ru] K. RUBIN, The main conjecture, appendix to: *Cyclotomic fields I and II* (combined second edition), by S. Lang, GTM 121, Springer, New York, 1990.
- [Tu] W. T. TUTTE, The dissection of equilateral triangles into equilateral triangles, *Proc. Cambridge Phil. Soc.*, 44 (1948), 463-482.

Manuscrit reçu le 10 avril 2000,
 accepté le 10 janvier 2002.

Cornelius GREITHER,
 Universität der Bundeswehr München
 Institut für theoretische Informatik
 und Mathematik
 Fakultät für Informatik
 85577 Neubiberg (Allemagne).
 greither@informatik.unibw-muenchen.de
 and
 Radan KUČERA,
 Masarykova univerzita
 Přírodovědecká fakulta
 Janáčkovo nám. 2a
 663 95 Brno (République Tchèque).
 kucera@math.muni.cz