On a conjecture concerning minus parts in the style of Gross

C. Greither and R. Kučera

Abstract

This paper is devoted to Gross's conjecture on tori over the base field $\mathbb{Q}$. We call it the Minus Conjecture, since it involves a regulator built from units in the minus part. We recall and develop its relation to a conjecture of Burns, which is now known to hold generally in the absolutely abelian setting; however in many situations it is not clear at all how one should deduce the Minus Conjecture from it. We prove a somewhat weaker statement (order of vanishing) rather generally, and we give a proof of the Minus Conjecture for some specific classes of absolutely abelian extensions $K/\mathbb{Q}$, for which $K^+/\mathbb{Q}$ is l-elementary and ramified in at most two primes. The field K is assumed to be of the form FK^+ where F is an arbitrary imaginary quadratic field. Our methods involve a good deal of explicit calculation; among other things, we use p-adic Γ-functions and the Gross-Koblitz formula.

AMS Mathematics Subject Classification: 11R20

Key words: Stark units, regulators, Gross conjecture on tori

Introduction

In the eighties, B. Gross (see [5]) introduced a conjecture which is close to Stark's conjectures inasmuch as it postulates a link between L-values and regulators, but differs from Stark's conjectures in a very important aspect: the regulators are not complex numbers, arising as determinants of logarithms of certain algebraic numbers, but they lie in an appropriate quotient of the augmentation filtration of $\mathbb{Z}[G]$, where G is the Galois group of the abelian field extension K/F under consideration, and they are obtained as determinants of matrices made from certain local Artin symbols.

In a previous version of [1], David Burns formulated a conjecture which combines Stark-type and Gross-type conjectures. (Note: in the most recent version [1], this is formulated not as a conjecture but as a conditional result (Corollary 4.1) assuming the equivariant Tamagawa number conjecture for an appropriate motive. This result requires a very sophisticated proof.) We sketch Burns's conjecture for an abelian extension $K/\mathbb{Q}$ now; this involves two steps. One starts out with a Stark unit η_K (whose existence is proven in this case, not just a conjecture), and then one obtains a description of the

"position of η_K inside an appropriate exterior power of $\mathcal{O}_K^\times$" in terms of a Gross regulator. At the first stage, the Stark unit is essentially determined by a classical regulator, that is, a determinant involving the logarithms of the conjugates of η_K. At the second stage, the Gross regulator is an algebraic object living in a subquotient of an integral group ring. (The whole setup generalizes to other base fields than $\mathbb{Q}$.) For details, see §1.

In subsequent work of Hayward ([6], [7]), where Burns's conjectures are discussed and in some cases proved, another conjecture arises which may be considered as the "minus part" of Burns's conjecture for extensions K/F where F is an imaginary quadratic field and K is absolutely abelian. (The methods in Hayward's proofs are much more accessible than those of [1].) We will explain this in §1 without trying for maximum generality, so as to keep things a little simpler. This "Minus Conjecture" equates, up to explicit constant factors, the leading term of a Stickelberger element and a regulator constructed from S-units in the minus part. We hasten to mention two things: firstly our Minus Conjecture is in fact a special case of what is called "the conjecture of Gross on tori", on which not much seems to be known, and secondly we are indebted to Henri Darmon for his suggestion that we might look at leading terms of Stickelberger elements in the minus part. Let us also remark that Darmon deals with an interesting analogous situation in [3] where F is a *real* quadratic field.

The Minus Conjecture (MC) is intimately linked to the conjecture of Burns (B) for $K^+/\mathbb{Q}$ and K/F respectively: if we assume the validity of (B) for $K^+/\mathbb{Q}$, then the Minus Conjecture can be shown to imply the validity of (B) for K/F (this is a result of Hayward, aptly called "base change for conjecture (B)"), and the converse implication, which entails a kind of division argument, works under some hypotheses (Theorem 2.5). We will review Hayward's argument in detail in §2, in order to make clear just when the division argument is possible. The idea is, very crudely speaking, that (B) for $K^+/\mathbb{Q}$ is the "plus part of (B) for K/F", and the Minus Conjecture (MC) is "the minus part of (B) for K/F", and the problem is to neatly separate the plus and minus parts.

We repeat that the division argument does not always work. The problem is simply "division of zero by zero". Our main objective in the second part of this paper (§§5-8) is thus to find a direct proof of the Minus Conjecture, which appears to be deeper than (B). Hayward proved the abovementioned instances of (B) by a nice argument involving Euler systems and a Matrix-Tree theorem. As things stand, this is not always sufficient for (MC), although it does lead the way to our proof of the weaker conjecture (VOC) on the order of vanishing (see below and §4). In our direct proof of (MC),

we are only able to handle $s = 1$ and $s = 2$, but still have to use (along with a lot of calculation) the Gross-Koblitz formula in §7. The situation in [3] is somewhat similar: the order of vanishing (Theorem 4.2 in loc.cit.) is easier to obtain than the results on the leading coefficient.

Actually we impose some more hypotheses in order to simplify things: We assume K/F elementary l-abelian with l a fixed odd prime; we suppose that $K = K^+F$, and K^+ is ramified in the primes $p_1, \ldots, p_s$ that are distinct from l, and we also suppose that all p_i are split in F. Let w_F, f and h_F denote the number of roots of unity, the conductor and the class number of F, respectively. We make the blanket assumption that $l \nmid w_F$. Then we can prove (MC) for $s = 1$ and $l \nmid f$ (see §3), and for cyclic K, $s = 2$ and $l \nmid fh_F$ (Theorem 8.9). We also have a positive result for $s = 2$ and noncyclic K (Theorem 8.8), but this requires that one of p_1, p_2 is an l-th power modulo the other prime, and again $l \nmid fh_F$.

The Vanishing Order Conjecture (VOC), which is a weakened form of (MC), says that the Stickelberger element associated to K is contained in the power I_G^s, where I_G is the augmentation ideal of $\mathbb{Z}_l[G]$ and s is the number of ramified primes in $K^+/\mathbb{Q}$. We prove this under some assumptions in §4 for all s. This shows that the invariant predicted to vanish by (MC) lives in the filtration quotient I_G^s/I_G^{s+1}.

It should be said that the case $s = 1$ of (MC) can already be deduced from our Theorem 2.5 together with [7]. The latter is an unpublished Ph.D. thesis, and we decided to present our own approach anyway, since we also feel that it might be of independent arithmetic interest. Hayward's argument makes essential use of elliptic units. While this is quite natural in the setting of [7], one may argue that in our case even the top field K is abelian over $\mathbb{Q}$, so one should try to stick to the cyclotomic framework all the way, and we show that this is possible.

In a forthcoming paper [4] we will explain how to prove (MC) for an arbitrary s under the assumption that $l \geq 3(s + 1)$ and $l \nmid w_F h_F$.

Notation will be introduced in §1 and further along as needed. We only mention here that X/l means X/lX or X/X^l depending on whether the abelian group X is written additively or multiplicatively.

Acknowledgements: The second author was supported under the project MSM0021622409 of the Ministry of Education of the Czech Republic. The first author acknowledges support from the DFG.

§1. *The setup, and statement of the conjectures*

We fix an odd prime l for the entire paper. First we state Burns's conjecture (B) on abelian Galois extensions K/k in a situation which is appropriate for our setting, always assuming that $l \nmid w_k$. We only look at the case where the parameter r (see [6]) has value 1. This suggests taking $k = \mathbb{Q}$ and K real, or taking k to be an imaginary quadratic field, since these are the obvious examples of abelian extensions where exactly one infinite place is totally split. To keep things simple we also assume $G = \mathrm{Gal}(K/k)$ is l-elementary. Let S be a nonempty finite set of finite places of k including all places that ramify in K, and let s denote the cardinality of S. Stark's conjecture in its strong form for rank one is known to be true for k the rationals or imaginary quadratic, and we will write $\eta_{K/k,S}$ for the Stark unit. For more details see [6] or [11]. Note that $\eta_{K/k,S}$ depends on the choice of the set S, and also in a harmless way on the choice of a place at infinity for K. Note moreover that in general $\eta_{K/k,S}$ only belongs to $U_S(K)^{1/w_K}$, so certainly belongs to $\mathbb{Z}_l \otimes_{\mathbb{Z}} U_S(K)$. We always suppose K given as a subfield of $\mathbb{C}$, and then there is the obvious choice of the infinite place.

In the statement of the conjecture we follow [6], except that we consistently eliminate the auxiliary set T which is used in loc.cit. to make certain unit groups torsion-free. The price for this is a denominator w_k, and we pay it gladly since all our conjectures amount to equalities that take place in groups of exponent l, and the absence of T does help.

There is a linear map

$$\begin{aligned} \mathrm{Reg}_{K/k,S}: \quad \bigwedge_{\mathbb{Z}}^{s-1} U_S(k) &\to I_G^{s-1}/I_G^s, \\ u_1 \wedge \ldots \wedge u_{s-1} &\mapsto \det\Big(r_v(u_i) - 1\Big)_{1 \le i \le s-1; v \in S^*}. \end{aligned}$$

Here r_v is the *local* reciprocity map $x \mapsto (x, K_w/k_v) \in G_v \subseteq G$ (note that the choice of the place w in K above v does not matter), and S^* denotes S with any one place deleted. This regulator map is well-defined up to sign; we will specify the sign shortly, before stating the central conjecture.

We note at once that r_v is trivial on roots of unity in k, since w_k is assumed to be coprime to $|G|$.

To obtain a regulator from the regulator map, one has (in contrast with Stark's conjecture) to introduce an extra parameter running over a Hom group. For any G-module X and any $\varphi \in \mathrm{Hom}_{\mathbb{Z}[G]}(X, \mathbb{Z}[G])$, let $\varphi^1 \in \mathrm{Hom}_{\mathbb{Z}}(X^G, \mathbb{Z})$ be defined by the property that $\varphi(u) = \varphi^1(u) \cdot \sum_{\sigma \in G} \sigma$ for all $u \in X^G$. Then φ^1 canonically induces a linear map $\bigwedge_{\mathbb{Z}}^s X^G \to \bigwedge_{\mathbb{Z}}^{s-1} X^G$

which will again be written φ^1, to wit

$$\varphi^1(x_1 \wedge \cdots \wedge x_s) = \sum_{i=1}^{s} (-1)^{i+1} \varphi^1(x_i) \cdot (x_1 \wedge \cdots \wedge x_{i-1} \wedge x_{i+1} \wedge \cdots \wedge x_s).$$

We now pick any $\mathbb{Z}$-basis $u_1, \ldots, u_s$ of $U_S(k)/(U_S(k))_{\mathrm{tor}}$ and we define

$$\mathrm{Reg}^{\varphi}_{K/k,S} = \mathrm{Reg}_{K/k,S}(\varphi^1(u_1 \wedge \ldots \wedge u_s)) \in I_G^{s-1}/I_G^s$$

for all $\varphi \in \mathrm{Hom}_{\mathbb{Z}[G]}(U_S(K), \mathbb{Z}[G])$. Note that this is well-defined (independent of the choice of the basis) up to sign.

We have to fix the sign of the regulator before we state Burn's conjecture. For this we use ad hoc terminology. Let us fix an ordering $v_1, \ldots, v_s$ of the set S. (Contrary to Hayward's work, the infinite place is not counted as a member of S.) An independent system $u_1, \ldots, u_s$ of S-units is called "adapted to the given ordering of S" (or just adapted, in context), if u_i is a unit outside v_i and has positive value at v_i. A basis $u_1, \ldots, u_s$ of $U_S(k)/U_S(k)_{\mathrm{tor}}$ is called *well-oriented,* if the transition matrix from this basis to any adapted system has positive determinant. (In many cases, e.g. if $h_F = 1$, we will even be able to pick a basis which is itself adapted.) Unless otherwise stated, we always make two assumptions:

(1) S and the basis $u_1, \ldots, u_s$ are ordered so that the basis is well-oriented.

(2) In the calculation of the regulator, the *last* place in S is omitted.

We may now state:

Conjecture (B). For all $\varphi \in \mathrm{Hom}_{\mathbb{Z}[G]}(U_S(K), \mathbb{Z}[G])$ one has

$$\varphi(\eta_{K/k,S}) \equiv (-1)^{s+1} \frac{h_{k,S}}{w_k} \mathrm{Reg}^{\varphi}_{K/k,S} \pmod{I_G^s}.$$

The letter φ here stands for the extension of φ in $\mathrm{Hom}_{\mathbb{Z}_l[G]}(\mathbb{Z}_l \otimes U_S(K), \mathbb{Z}_l[G])$.

The prediction about the sign comes from [1] and is also explained in [7]. Our way of stating things is different from [7] (and a bit more explicit), so we have to show compatibility. [7] uses the $\mathrm{sign}\, \xi = (-1)^{|T|+1} \mathrm{sign}(R)$ where R is a certain real-valued regulator. Since we work with empty T, we just have to show that the sign of R is exactly $(-1)^s$ under our assumptions.

The real-valued regulator R used by Hayward is constructed as follows: one takes an ordered basis $u_1, \ldots, u_s$ as above but a slightly different set of places $v_0 := \infty, v_1, \ldots, v_{s-1}$ (unfortunately Hayward's indexing is different, starting at 1), and one considers the determinant

$$R = \det(-\log |u_i|_{v_{j-1}})_{1 \le i,j \le s}.$$

If one extends R by an $s+1$th column by letting j run up to $j = s+1$, then the resulting matrix has zero row sums. By the usual argument we have

$$R = (-1)^s \cdot \det(-\log |u_i|_{v_j})_{1 \le i,j \le s}.$$

Now if $u_1, \ldots, u_s$ is an adapted system, the matrix inside the last det is diagonal, with positive entries $a_i \log \mathrm{N}(v_i)$ (where a_i denotes the valuation of u_i at v_i). Thus the determinant is positive, and the same holds if $u_1, \ldots, u_s$ is well-oriented. This shows $\mathrm{sign}(R) = (-1)^s$ and $\xi = (-1)^{s+1}$ as claimed.

In order to show that our version conforms with Hayward's formulation on p. 104 of [6], we also have to remark the following: Hayward's formula is invariant under enlarging T, as long as $U_{S,T}(k)$ is assumed torsion-free to begin with. We put in an extra denominator $w_{k,T}$ on the right in his formula, and we claim that then the formula is invariant under changing T, without any condition. Indeed: If we replace T by $T' = T \cup \{v\}$ (v some finite place of k outside $S \cup T$), then $\eta_{K/k,S,T'} = \eta_{K/k,S,T}^{\alpha}$ with $\alpha = 1 - \mathrm{N}(v) \cdot \mathrm{Frob}_v^{-1}$, so $\varphi(\eta_{K/k,S,T'}) = \alpha\varphi(\eta_{K/k,S,T})$, and we only need to know α modulo I_G, so we just get the factor $1 - \mathrm{N}(v)$. A standard argument using Formula (3) in [6] then shows that $h_{k,S,T} \mathrm{Reg}_{K/k,S,T}^{\varphi} / w_{k,T}$ is multiplied by the factor $\mathrm{N}(v) - 1$ when T is replaced by T'. Setting $T = \emptyset$ gives our version, since of course $h_{k,S,\emptyset} = h_{k,S}$ and $w_{k,\emptyset} = w_k$.

This shows at once that our version implies Hayward's. But the converse is equally true. For this we point out that one can always take $T = \{v\}$ in Hayward's situation such that l does not divide $\mathrm{N}(v) - 1$ (here we have to use the assumption that w_k is coprime to l). This ensures that the above argument works both ways. Note in this context that the term $(-1)^{|T|}$ in Hayward's sign definition is due to the fact that the sign changes whenever an element is put into or taken out of T, as can be seen by the preceding argument.

We will be concerned with Conjecture (B) in two concrete cases which we now describe. Let F be an imaginary quadratic field of conductor f. Let h_F denote the class number of F and w_F the number of roots of unity in F. We recall that we assume $l \nmid w_F$, and we stress that this hypothesis will be in force throughout the paper. We always assume that K is absolutely abelian, contains F, and that K^+ is elementary l-abelian over $\mathbb{Q}$. Then $K = FK^+$ and $G = \mathrm{Gal}(K/F)$ may be identified with $\mathrm{Gal}(K^+/\mathbb{Q})$. Let τ always stand for complex conjugation. Then both $\mathrm{Gal}(K/K^+)$ and $\mathrm{Gal}(F/\mathbb{Q})$ can be identified with $\{1, \tau\}$. Let m be the conductor of K^+. We also assume that there is no wild ramification in $K^+/\mathbb{Q}$. Then m has the form

$m = p_1 \cdots p_s$ where the p_i are all congruent to 1 mod l. Finally, we assume all p_i are split in F.

Theorem 1.1. *Under all these assumptions, Conjecture (B) is true for $K^+/\mathbb{Q}$ with $S = \{p_1, \ldots, p_s\}$ (the minimal possible choice of S).*

PROOF: This is due to Hayward. In the published work [6], this result can be found up to sign, see Theorem 5.10 and Remark 5.11. The sharp version including the sign is only proved in Hayward's thesis, see top of page 98. We have to explain the role of the auxiliary integer b by which both sides of the conjecture are multiplied in loc.cit. It has to satisfy two conditions: b must be a multiple of w_k, and there must be a section s of the natural epimorphism $R \to cl_k$ such that s^b is a homomorphism, where R denotes the ray class group of conductor $p_1 \ldots p_s$ in k. Since $k = \mathbb{Q}$ here, the class group is trivial, and the second condition is void; so we may take $b = w_{\mathbb{Q}} = 2$, which is prime to l, and we may cancel b in Hayward's theorem on both sides. QED

We make a few comments:

(i) As a basis for $U_S(\mathbb{Q})$ modulo torsion one can take the set $\{p_1, \ldots, p_s\}$. Note this is well-oriented (with the obvious ordering of S) and even adapted.

(ii) The Stark unit comes out as $\mathrm{N}_{\mathbb{Q}(\zeta_m)/K^+}(1-\zeta_m)^{1/2}$ where $\zeta_m \mapsto e^{2\pi i/m}$ fixes the choice of place at infinity.

(iii) The factor preceding the regulator on the right is simply $h_{\mathbb{Q},S}/w_{\mathbb{Q}} = \frac{1}{2}$.

On the upper level we have:

Theorem 1.2. *If $l \nmid h_F$ then Conjecture (B) is true for K/F with $S = S_F$ the set of places above any of the p_i, $i = 1, \ldots, s$ (the minimal possible choice of S).*

PROOF: This is again due to Hayward. He actually proves much more, using elliptic units; the big field K only needs to be abelian over k, not necessarily over $\mathbb{Q}$. The requirements on the integer b have already been explained, but here $k = F$, and we have to be more careful. Let b be w_F multiplied with the greatest factor of $\prod_{i=1}^{s}(p_i - 1)$ that is prime to l. Then b annihilates the non-l-part of the kernel of $R \to cl_F$, and b is prime to l. Since we assumed h_F prime to l, there is a section $s : cl_F \to R$ with image contained in the non-l-part of R. Then s^b is a homomorphism, so Hayward's theorem (p.98 in [7]) applies again, and we may cancel b as in the proof of 1.1. QED

Again, a few comments:

(iv) Now the set S_F has cardinality $2s$, so we are looking at an equation in I_G^{2s-1}/I_G^{2s}.

(v) In the particular case that interests us in §3 and §§5-8, we will fix an explicit basis of $U_S(F)$.

(vi) One can express $\eta_{K/F,S}$ in terms of $\eta_{K^+/\mathbb{Q},S}$; this will be made precise at an appropriate later moment.

(vii) The denominator is legal since we are assuming $l \nmid w_F$.

We now turn to the Minus Conjecture (MC). To state it, we have to introduce certain Stickelberger elements.

The notation $\sum_{a \bmod^\times n}$ means that the sum runs over all $a = 1, \dots, n-1$ which are coprime to n. Let σ_a denote the automorphism $\zeta_{fm} \mapsto \zeta_{fm}^a$ for a coprime to fm. We likewise denote by σ_a the restriction of this to $K = FK^+ \subseteq \mathbb{Q}(\zeta_{fm})$. We define:

$$\Theta_K = \frac{1}{fm} \sum_{a \bmod^\times fm} \Big(a - \frac{fm}{2}\Big)\sigma_a^{-1} \in \mathbb{Q}[\mathrm{Gal}(K/\mathbb{Q})].$$

We note that $\tau \in \mathbb{Q}[\mathrm{Gal}(K/\mathbb{Q})]$ is just σ_{-1}, and comparing coefficients shows that Θ_K is a multiple of $(1-\tau)$, more precisely:

$$\Theta_K = (1-\tau)\tilde{\Theta}_K, \quad \tilde{\Theta}_K = \frac{1}{fm} \sum_{\substack{a \bmod^\times fm \\ \sigma_a|F=1}} \Big(a - \frac{fm}{2}\Big)\sigma_a^{-1}.$$

Note that $\tilde{\Theta}_K$ is now in $\mathbb{Q}[\mathrm{Gal}(K/F)]$.

We also need a regulator built from minus-units. For each $i \in \{1, \dots, s\}$ pick a prime ideal $\mathfrak{p}_i$ above p_i in F. Let S' be the ordered set $(\mathfrak{p}_1, \dots, \mathfrak{p}_s)$. The abelian group $\big(U_S(F)/(U_S(F))_{\mathrm{tor}}\big)^{1-\tau}$ is free of rank s. We choose an ordered basis for it, $(u_1^{1-\tau}, \dots, u_s^{1-\tau})$ say. We again have a notion of well-orientedness as follows. For each i we choose a positive power of $\mathfrak{p}_i$ which is principal and a generator x_i of it. Then the family $x_1^{1-\tau}, \dots, x_s^{1-\tau}$ is a $\mathbb{Q}$-basis of $\mathbb{Q} \otimes \big(U_S(F)/(U_S(F))_{\mathrm{tor}}\big)^{1-\tau}$ (an analog of the "adapted systems" we used before), and we decree that $(u_1^{1-\tau}, \dots, u_s^{1-\tau})$ is well-oriented with respect to the ordered set S' if $(x_1^{1-\tau}, \dots, x_s^{1-\tau})$ can be obtained by a $\mathbb{Q}$-linear transformation with positive determinant from the ordered set $(u_1^{1-\tau}, \dots, u_s^{1-\tau})$. All this simplifies a lot when $h_F = 1$. Then one takes u_i to be a generator of $\mathfrak{p}_i$.

No parameter φ is needed, and no place has to be omitted in the following definition:

$$\mathrm{Reg}_{K,S}^- = \det(r_w(u_i^{1-\tau}) - 1)_{1 \le i \le s, w \in S'} \in I_G^s / I_G^{s+1}.$$

This is indeed well-defined. In order to state the Minus Conjecture, we repeat our assumptions for convenience: $K = K^+F$, $l \nmid w_F$, $K^+/\mathbb{Q}$ is l-elementary

with Galois group G, exactly s rational primes ramify (tamely) in K^+, and all these primes are split in F.

Conjecture (MC). Let $(u_i^{1-\tau})_i$ be an ordered basis of the minus units as above which is well-oriented with respect to S'. Then

$$\tilde{\Theta}_K \equiv -\frac{h_{F,S}}{w_F} \operatorname{Reg}^-_{K,S} \pmod{I_G^{s+1}}.$$

We will call this the "Minus Conjecture" in the sequel.

We point out that in the notation of [6] (p.118), $\tilde{\Theta}_K = -\frac{1}{2}\Theta(0,\omega)$ (note the minus sign, which comes from the usual formula linking an L-value at 0 to a generalised Bernoulli number), so (MC) reads as $\Theta(0,\omega) \equiv \frac{2h_{F,S}}{w_F} \operatorname{Reg}^-_{K,S}$, and the constant $\frac{2h_{F,S}}{w_F}$ should be interpreted as $\frac{h_{F,S}}{w_F} \Big/ \frac{h_{\mathbb{Q}}}{w_{\mathbb{Q}}}$, which agrees with the general idea that (MC) is "the quotient of (B) for K/F by (B) for $K^+/\mathbb{Q}$." There is one intentional discrepancy with [6]:

Remark: In our minus regulator we take a basis of $\big(U_S(F)/(U_S(F))_{\text{tor}}\big)^{1-\tau}$ whereas Hayward takes a basis of the group $\big(U_S(F)/(U_S(F))_{\text{tor}}\big)^-$, which may be slightly larger. This makes our regulator larger by the index of the smaller group inside the latter; and so we get rid of the index factor which is needed in the statements of Proposition 7.2 and Conjecture 7.4 in loc.cit.

The following important consequence of the Minus Conjecture is much easier to state, and also easier to prove (see Theorem 4.4).

Conjecture (VOC). The element $\tilde{\Theta}_K$ always lies in the s-th power of the augmentation ideal I_G.

§2. *Base change for (B) and the division argument for (MC)*

In simple terms, we are going to show: If (MC) holds, then Theorem 1.2 is a direct consequence of Theorem 1.1 (it would be slightly misleading to say that the one implies the other, since both statements are true); and under specific conditions this argument can be reversed, leading to a proof of (MC). The former part of this is due to Hayward. We explain the argument in detail for the reader's convenience before discussing the question of the converse implication.

We keep all assumptions and notations from the previous section.

Proposition 2.1. (Hayward) *We have a base change property for conjecture (B), that is: Theorem 1.2 can be deduced from Theorem 1.1 and the validity of (MC).*

PROOF: The main idea is that both sides in the statement of (B) for K/F can be conveniently written as the product of two factors.

In [6] Hayward defines a twisted Stickelberger element $\Theta_{K/K^+/\mathbb{Q},S}(0,\omega)$. One can check that it equals $-2\tilde{\Theta}_K$. By the formula (13) of [6] it satisfies the product formula

$$\Theta'_{K/F,S}(0) = \Theta_{K/K^+/\mathbb{Q},S}(0,\omega) \cdot \Theta'_{K^+/\mathbb{Q},S}(0),$$

where the equivariant L-functions $\Theta_{K/F,S}(z)$ and $\Theta_{K^+/\mathbb{Q},S}(z)$ are defined for instance in [11], chapter IV, §1. Note that the idempotent $e_{\omega\chi}$ two lines below formula (13) in loc.cit. should read e_χ.

Lemma 2.2. *The Stark units satisfy* $\eta_{K/F,S} = \eta_{K^+/\mathbb{Q},S}^{-\tilde{\Theta}_K}$.

PROOF: This was proved by Hayward under the Hypothesis 7.1 in loc.cit. An argument is necessary here as we are not assuming this hypothesis.

Let ∞_1 be an infinite place of K^+; we identify this with the place of K above it. Let v be a place of K^+ above p_1 and let w be a place of K above v. By $\bar{w}$ we denote the K/K^+ conjugate of w which may or may not be equal to w.

Similarly as in [6] we deduce the following two formulas:

$$\begin{aligned} \lambda_K(\eta_{K^+/\mathbb{Q}}^{-\tilde{\Theta}_K}) &= -\Theta'_{K^+/\mathbb{Q},S}(0)\tilde{\Theta}_K \cdot (2\infty_1 - w - \bar{w}) \\ &= \Theta'_{K/F,S}(0) \cdot (\infty_1 - \tfrac{w}{2} - \tfrac{\bar{w}}{2}), \\ \lambda_K(\eta_{K/F}) &= \Theta'_{K/F,S}(0) \cdot (\infty_1 - w). \end{aligned}$$

We want to conclude that the arguments of λ_K in two preceding formulas are equal but we cannot do so directly since λ_K is not injective in general.

Let $e_K \in \mathbb{C}[G]$ be the idempotent which is the sum of all e_χ such that χ is nontrivial on all decomposition groups of primes in S. We claim that

$$e_K(\infty_1 - \tfrac{w}{2} - \tfrac{\bar{w}}{2}) = e_K(\infty_1 - w).$$

If $w = \bar{w}$, this is trivial. If not, suppose e_χ is one of the idempotents whose sum is e_K. Then χ must be nontrivial on the decomposition group of w and of $\bar{w}$. But then $e_K w = e_K \bar{w} = 0$.

Since λ_K is injective in the e_K-part, we have proved the e_K-part of the lemma. We will be done if we establish that both sides of the equality are already in the e_K-part. The support of an element x of a $\mathbb{C}[G]$-module is by definition the set of all $\chi \in \hat{G}$ with $e_\chi x \neq 0$. We know the following: $\eta_{K/F}$ has the same support as $\Theta'_{K/F,S}(0)$ and $\eta_{K^+/\mathbb{Q}}$ has the same support as

$\Theta'_{K^+/\mathbb{Q},S}(0)$. Then using the product formula stated before Lemma 2.2 we deduce that the both sides of Lemma 2.2 have the same support, in particular they are both in the e_K-part. QED

From the preceding lemma it follows that $\varphi(\eta_{K/F,S}) = -\tilde{\Theta}_K\varphi(\eta_{K^+/\mathbb{Q},S})$ for all $\varphi \in \mathrm{Hom}_{\mathbb{Z}[G]}(U_S(K), \mathbb{Z}[G])$.

We fix the ordering of the primes $p_1, \ldots, p_s$; for each i we fix a prime $\mathfrak{p}_i$ above p_i in F and we choose the ordering $(\mathfrak{p}_1, \ldots, \mathfrak{p}_s, \mathfrak{p}_1^\tau, \ldots, \mathfrak{p}_s^\tau)$ on S.

Lemma 2.3. *Recall $S' = \{\mathfrak{p}_1, \ldots, \mathfrak{p}_s\}$. If $\mathbf{u}' = (u_1, \ldots, u_s)$ is an ordered basis of $U_{S'}(F)/U_{S'}(F)_{\mathrm{tor}}$, then $\mathbf{u} = (u_1, \ldots, u_s, p_1, \ldots, p_n)$ is an ordered basis of $U_S(F)/U_S(F)_{\mathrm{tor}}$, and $\mathbf{u}$ is well-oriented with respect to S iff $\mathbf{u}'$ is well-oriented with respect to S'.*

Proof: We begin by noting that $U_S(F)/U_S(F)_{\mathrm{tor}}$ is the direct sum of $U_{S'}(F)/U_{S'}(F)_{\mathrm{tor}}$ and $U_S(\mathbb{Q})/U_S(\mathbb{Q})_{\mathrm{tor}} = \langle p_1, \ldots, p_s\rangle$. Pick $x_i \in F$ so that x_i generates a positive power of $\mathfrak{p}_i$. Then $\mathbf{x} = (x_1, \ldots, x_s, x_1^\tau, \ldots, x_s^\tau)$ is an adapted system with respect to S, and one checks that the transition from this to $(x_1, \ldots, x_s, p_1, \ldots, p_s)$ has positive determinant. Hence the transition from $\mathbf{u}$ to $\mathbf{x}$ has positive determinant iff the transition from $\mathbf{u}'$ to $(x_1, \ldots, x_n)$ has positive determinant. QED

We continue in the proof of 2.1, assuming that $S, S', u_1, \ldots, u_s$ have been chosen so that $\mathbf{u}$ is well-oriented. We write u_{s+i} for p_i $(i = 1, \ldots, s)$. We will prove below the following formula (in which the first and third equalities hold by definition):

$$\begin{aligned}
\mathrm{Reg}^{\varphi}_{K/F,S} &= \mathrm{Reg}_{K/F,S}(\varphi^1(u_1 \wedge \ldots \wedge u_{2s})) \\
&= \frac{1}{2}(-1)^s \,\mathrm{Reg}^-_{K,S} \cdot \mathrm{Reg}_{K^+/\mathbb{Q},S}(\varphi^1(u_{s+1} \wedge \ldots \wedge u_{2s})) \\
&= \frac{1}{2}(-1)^s \,\mathrm{Reg}^-_{K,S} \cdot \mathrm{Reg}^{\varphi}_{K^+/\mathbb{Q},S}\,.
\end{aligned}$$

Let us assume this for a moment. For the ensuing calculation, which takes place in the group I_G^{2s-1}/I_G^{2s}, we note that there is a canonical map $I_G^s/I_G^{s+1} \times I_G^{s-1}/I_G^s \to I_G^{2s-1}/I_G^{2s}$ induced by multiplication. We have

$$\begin{aligned}
\varphi(\eta_{K/F,S}) &= -\tilde{\Theta}_K \cdot \varphi(\eta_{K^+/\mathbb{Q},S}) \\
&= \Big(+\frac{h_{F,S}}{w_F}\,\mathrm{Reg}^-_{K,S}\Big)\Big((-1)^{s+1}\frac{1}{2}\ \mathrm{Reg}^{\varphi}_{K^+/\mathbb{Q},S}\Big) \\
&\qquad\qquad \text{(use (B) for } K^+/\mathbb{Q}\text{, and (MC))} \\
&= (-1)^{s+1}\frac{h_{F,S}}{2w_F}\,\mathrm{Reg}^-_{K,S}\,\mathrm{Reg}^{\varphi}_{K^+/\mathbb{Q},S}\,.
\end{aligned}$$

This is (B) for K/F.

To complete the proof, we need another proposition as announced. We follow Hayward's reasoning.

Proposition 2.4. *With all the previously introduced hypotheses:*

$$\mathrm{Reg}_{K/F,S}(\varphi^1(u_1\wedge\ldots\wedge u_{2s})) = \frac{1}{2}(-1)^s \,\mathrm{Reg}^-_{K,S}\cdot \mathrm{Reg}_{K^+/\mathbb{Q},S}(\varphi^1(u_{s+1}\wedge\ldots\wedge u_{2s})).$$

Proof: We have a matrix with row sums in I_G^2, whose rows are indexed by $i = 1,\ldots,2s$ and the columns are indexed as indicated:

	$\mathfrak{p}_1$	$\ldots$	$\mathfrak{p}_s$	$\mathfrak{p}_1^\tau$	$\ldots$	$\mathfrak{p}_s^\tau$
u_1		$\vdots$			$\vdots$	
$\vdots$	$\ldots$	$r_{\mathfrak{p}_j}(u_i)-1$	$\ldots$	$\ldots$	$r_{\mathfrak{p}_j^\tau}(u_i)-1$	$\ldots$
u_s		$\vdots$			$\vdots$	
u_{s+1}		$\vdots$			$\vdots$	
$\vdots$	$\ldots$	$r_{\mathfrak{p}_j}(u_i)-1$	$\ldots$	$\ldots$	$r_{\mathfrak{p}_j^\tau}(u_i)-1$	$\ldots$
u_{2s}		$\vdots$			$\vdots$	

We may use that $r_{\mathfrak{p}_j^\tau}(u_i) - 1 = r_{\mathfrak{p}_j}(u_i^\tau) - 1$ and $u_i^\tau = u_i$ if $i > s$. For any i, $s < i \le 2s$, we have $2\sum_{j=1}^s (r_{\mathfrak{p}_j}(u_i)-1) \in I_G^2$. But $I_G/I_G^2 \simeq G$ has no element of order 2 and so $\sum_{j=1}^s (r_{\mathfrak{p}_j}(u_i)-1) \in I_G^2$. We remove the last column from the matrix and call the resulting matrix A:

	$\mathfrak{p}_1$	$\ldots$	$\mathfrak{p}_{s-1}$	$\mathfrak{p}_s$	$\mathfrak{p}_1^\tau$	$\ldots$	$\mathfrak{p}_{s-1}^\tau$
u_1		$\vdots$		$\vdots$		$\vdots$	
$\vdots$	$\ldots$	$r_{\mathfrak{p}_j}(u_i)-1$	$\ldots$	$r_{\mathfrak{p}_j}(u_s)-1$	$\ldots$	$r_{\mathfrak{p}_j}(u_i^\tau)-1$	$\ldots$
u_s		$\vdots$		$\vdots$		$\vdots$	
u_{s+1}		$\vdots$		$\vdots$		$\vdots$	
$\vdots$	$\ldots$	$r_{\mathfrak{p}_j}(u_i)-1$	$\ldots$	$r_{\mathfrak{p}_j}(u_s)-1$	$\ldots$	$r_{\mathfrak{p}_j}(u_i)-1$	$\ldots$
u_{2s}		$\vdots$		$\vdots$		$\vdots$	

The left hand side of Proposition 2.4 is then $\sum_{i=1}^{2s}(-1)^{i+1}\varphi(u_i)\det(A_i)$, where A_i means A without the i-th row. Before we can compute further, we perform some column operations on A: We add all the first $s-1$ columns to the sth one and then for each $i = 1,\ldots,s-1$ we subtract the $(i+s)$th column from the ith one. All computations are done modulo I_G^2, and the outcome is as follows:

	$\mathfrak{p}_1$	$\dots$	$\mathfrak{p}_{s-1}$	$\mathfrak{p}_s$	$\mathfrak{p}_1^\tau$	$\dots$	$\mathfrak{p}_{s-1}^\tau$
u_1		$\vdots$		$\vdots$		$\vdots$	
$\vdots$	$\dots$	$r_{\mathfrak{p}_j}(u_i) - r_{\mathfrak{p}_j}(u_i^\tau)$	$\dots$	$\sum_{j=1}^{s}(r_{\mathfrak{p}_j}(u_i)-1)$	$\dots$	$r_{\mathfrak{p}_j}(u_i^\tau)-1$	$\dots$
u_s		$\vdots$		$\vdots$		$\vdots$	
u_{s+1}		$\vdots$		$\vdots$		$\vdots$	
$\vdots$	$\dots$	0	$\dots$	0	$\dots$	$r_{\mathfrak{p}_j}(u_i)-1$	$\dots$
u_{2s}		$\vdots$		$\vdots$		$\vdots$	

We need to compute the determinant of this matrix if one row is removed. If the removed row is in the upper half of the matrix, then this $(2s-1)\times(2s-1)$ matrix contains a $s \times s$ zero submatrix and so its determinant is zero. But if we remove one row in the lower half of the matrix, say row number $s+k$, then the remaining $(2s-1)\times(2s-1)$ matrix contains a $(s-1)\times s$ zero submatrix and its determinant is the product of the determinant D of the upper left $s \times s$ submatrix and the determinant D_k of the lower right $(s-1)\times(s-1)$ submatrix. Let us compute D. We multiply the sth column by 2 and then we subtract the first $s-1$ columns from the sth one. Then the ith entry of the sth column looks as follows:

$$\begin{aligned} & 2\sum_{j=1}^{s}(r_{\mathfrak{p}_j}(u_i)-1) - \sum_{j=1}^{s-1}(r_{\mathfrak{p}_j}(u_i) - r_{\mathfrak{p}_j}(u_i^\tau)) \\ & = r_{\mathfrak{p}_s}(u_i) - r_{\mathfrak{p}_s}(u_i^\tau) + \sum_{j=1}^{s}((r_{\mathfrak{p}_j}(u_i)-1) + (r_{\mathfrak{p}_j^\tau}(u_i)-1)) \\ & \equiv r_{\mathfrak{p}_s}(u_i) - r_{\mathfrak{p}_s}(u_i^\tau) \end{aligned}$$

modulo I_G^2. Therefore D is congruent to $\frac{1}{2}\det(r_{\mathfrak{p}_j}(u_i^{1-\tau})-1)_{1\le i,j\le s} = \frac{1}{2}\operatorname{Reg}^-_{K,S}$. Since p_j splits in $F/\mathbb{Q}$, we have $F_{\mathfrak{p}_j} = \mathbb{Q}_{p_j}$ and similarly the completions of K^+ and of K coincide, so $r_{\mathfrak{p}_j}(u_i) = r_{p_j}(u_i)$ and we obtain:

$$D_k = \operatorname{Reg}_{K^+/\mathbb{Q},S}(u_{s+1} \wedge \ldots \wedge u_{s+k-1} \wedge u_{s+k+1} \wedge \ldots \wedge u_{2s}).$$

From the definition of φ^1 we finally obtain

$$\operatorname{Reg}_{K/F,S}(\varphi^1(u_1 \wedge \ldots \wedge u_{2s})) = (-1)^s \cdot \tfrac{1}{2}\operatorname{Reg}^-_{K,S} \cdot \operatorname{Reg}_{K^+/\mathbb{Q},S}(\varphi^1(u_{s+1} \wedge \ldots \wedge u_{2s})).$$

The factor $(-1)^s$ comes from the alternating signs in the sum that defines φ^1 applied to an $s-1$-fold wedge, and to an $2s-1$-fold wedge: the summand number $s+k$ on the left corresponds to the k-th summand on the right. QED

This argument can be exploited further. We come back to the part of the argument immediately preceding Proposition 2.4. We let $c(\varphi) = \mathrm{Reg}^{\varphi}_{K^+/\mathbb{Q},S}$. If we assume that we can find at least one φ such that the multiplication map

$$\_ \cdot c(\varphi) : I_G^s/I_G^{s+1} \to I_G^{2s-1}/I_G^{2s}$$

is *injective,* then the same calculation works backwards. More precisely we have $\tilde{\Theta}_K \cdot \varphi(\eta_{K^+/\mathbb{Q},S}) = \tilde{\Theta}_K \cdot ((-1)^{s+1}\frac{1}{2}c(\varphi))$ because of (B) for $K^+/\mathbb{Q}$; and we have $-\tilde{\Theta}_K \cdot \varphi(\eta_{K^+/\mathbb{Q},S}) = \varphi(\eta_{K/F,S}) = (-1)^{2s+1}\frac{h_{F,S}}{w_F}\,\mathrm{Reg}^{\varphi}_{K/F,S}$ by virtue of (B) for K/F, and the last term can again be factored as $(-1)^{s+1}\frac{h_{F,S}}{2w_F}\,\mathrm{Reg}^{-}_{K,S}\,c(\varphi)$. Thus under our assumption that multiplication by $c(\varphi)$ is injective, we may simplify by $c(\varphi)$; the result is (MC).

It remains to see just when such a φ can be found.

Let us assume that $K^+/\mathbb{Q}$ is cyclic (hence cyclic of order l). Let σ be a fixed generator of G. The genus field of K^+ is the compositum $K_1 \ldots K_s$ with K_i the abelian field of conductor p_i and degree l. We also fix a generator σ_i of $G_i = \mathrm{Gal}(K_i/\mathbb{Q})$ for each i, by the prescription that the extension of σ_i by identity on the other K_j restricts to σ on K. We define an $s \times s$ matrix $A = (a_{ij})$ by the properties that it has zero row sums and for $i \neq j$, a_{ij} is an integer such that $\sigma_j^{a_{ij}}$ equals the Frobenius of p_i in K_j. Then up to sign $\mathrm{Reg}_{K^+/\mathbb{Q},S}(p_1 \wedge \ldots \wedge p_{i-1} \wedge p_{i+1} \wedge \ldots \wedge p_s)$ equals $A_i(\sigma - 1)^{s-1}$ modulo $(\sigma - 1)^s$ where A_i is the (i,i)-minor of A; see [6] Proposition 5.6. (Hayward does specify the sign, but we do not need it). Note that A and A_i are only uniquely determined modulo l. We now claim:

Theorem 2.5. *If $K^+/\mathbb{Q}$ is cyclic, l does not divide h_F, and at least one of the minors $A_1, \ldots, A_s$ is not zero modulo l, then the validity of (B) for $K^+/\mathbb{Q}$ and for K/F taken together imply the Minus Conjecture (MC) for K. Therefore (MC) holds in this situation as a consequence of Theorems 1.1 and 1.2.*

Proof: Assume that the minor A_i is not zero modulo l. Either by the theory of Gorenstein rings or by using the isomorphism

$$\mathrm{Hom}_{\mathbb{Z}[G]}(X, \mathbb{Z}[G]) \ni \varphi \mapsto \varphi^1 \in \mathrm{Hom}_{\mathbb{Z}}(X, \mathbb{Z}),$$

where $\varphi^1(x)$ is the coefficient of the identity element in $\varphi(x)$, one shows that there exists $\varphi \in \mathrm{Hom}_{\mathbb{Z}[G]}(X, \mathbb{Z}[G])$ with $\varphi^1(p_{i'}) = 1$ if $i' = i$ and 0 else. (For the existence of such a φ one has to use that quotient of $U_S(F)/U_S(F)_{\mathrm{tor}}$ modulo the subgroup spanned by $p_1, \ldots, p_s$ has no torsion. Note also that the present definition of φ^1 extends a previous definition.) Then $\mathrm{Reg}^{\varphi}_{K^+/\mathbb{Q},S}$ is up to sign just $\mathrm{Reg}_{K^+/\mathbb{Q},S}(p_1 \wedge \ldots \wedge p_{i-1} \wedge p_{i+1} \wedge \ldots \wedge p_s)$. Because of

our assumption, this has the form "l-unit times $(\sigma-1)^{s-1}$". Since for all $t>0$, I^t/I^{t+1} is cyclic of order l, generated by $(\sigma-1)^t$, we conclude that multiplication with $c(\varphi)$ is injective (as explained above) for this choice of φ. QED

An aside remark: From a heuristic viewpoint, i.e., if we regard A as a random matrix with row sums zero, it is highly probable that at least one A_i is nonzero. More precisely, there are $l^{n(n-1)}$ matrices in $(\mathbb{Z}/l)^{n,n}$ with vanishing row sums, and one can show that exactly

$$l^{n(n-1)}(1-l^{-2})(1-l^{-3})\cdots(1-l^{-n})$$

among them have the maximal possible rank $n-1$. By comparison, there are l^{n^2} matrices in $(\mathbb{Z}/l)^{n,n}$, and exactly $l^{n^2}(1-l^{-1})(1-l^{-2})(1-l^{-3})\cdots(1-l^{-n})$ among them are nonsingular; this is a visibly lower proportion.

We ran extensive tests to check on this estimate, only a small part of which will be mentioned here. We let A be the Frobenius matrix attached to a cyclic degree l field K^+ with s ramified primes $p_1,\ldots,p_s$, all congruent to 1 modulo the prime l, and we calculated the rank of A for all such fields with given s and l, under the restriction that all $p_i<1000$. For $s=3$ and $l=3$, the observed and the estimated ratios of fields with A of maximal rank $s-1$ were 0.858024 and 0.855967 respectively (a difference of about 0.2 percent). There were about 330000 fields. For $s=5$ and $l=19$, the observed and estimated ratios were 0.997086 and 0.997076, that is, very close indeed. There were about 2.2 million fields. For the case $s=3$, $l=19$, the range of fields was extended further to $p_i<10000$, with the result that the observed ratio was still closer to the estimate than it was for $p_i<1000$.

If $s=2$ the condition on minors simplifies a lot, so Theorem 2.5 reads as

Corollary 2.6. *Let $K^+/\mathbb{Q}$ be cyclic, and assume $s=2$ and $l\nmid h_F$. If at least one of p_1,p_2 is not an l-th power residue modulo the other one, then the Minus Conjecture (MC) holds for K.*

This hypothesis is satisfied for instance if $l=3$, $p_1=13,p_2=37$. It is not satisfied for instance if $l=3$, $p_1=13,p_2=229$. It is routine to show that there are (for every l) infinitely many pairs p_1,p_2 for which the hypothesis is not satisfied, and one even may fix one of the p_i.

The main aim of this paper is to give a proof of the Minus Conjecture in the case not covered by the previous corollary, so (in our opinion) in the really hard case. Consider the following

Assumption A. $s=2$ and p_2 is an l-th power modulo p_1.

Our main result will be that the Minus Conjecture is true under Assumption A. As things stand, we only can do it if $l \nmid h_F$. We repeat our other hypotheses: l is an odd prime which does not divide the conductor f of F; $K = FK^+$, and $K^+/\mathbb{Q}$ is l-elementary abelian, tamely ramified exactly in p_1 and p_2 which both split in F. By Corollary 2.6, the Minus Conjecture is then true for $s = 2$ without any restriction on p_1 and p_2, at least in the cyclic case.

We first deal with the case $s = 1$. Actually this already follows from Theorem 2.5, since the condition on the matrix minors is trivially true for $s = 1$: the determinant of an empty matrix is 1. But the proof of Theorem 2.5 heavily relies on Hayward's as yet unpublished thesis, because the sign in the conjecture is crucial. So we give a complete argument here, also as a preparation for dealing with $s = 2$. We think that there is some explicit arithmetic meaning behind this; see Theorem 3.4 below. We mention right here that this theorem has the following nontrivial congruence as a special case $f = 4$:

$$\Big(\frac{p-1}{4}\Big)!^{-8} \equiv \prod_{\substack{a \bmod^\times 4p \\ a \equiv 1(4)}} a^{2a} \pmod{p}$$

for all primes $p \equiv 1 \pmod 4$. It is actually possible here to divide the exponents by 2 and to remove the sign ambiguity. V. Trnková (work in progress) proved that the sign is a minus for all p. The authors do not know whether this could be done in Theorem 3.4.

§3. *The case $s = 1$ of the Minus Conjecture*

We start with an imaginary quadratic field F of conductor f, class number h_F and unit-root-number w_F. We let S be the singleton set $\{p\}$, with $p \equiv 1$ modulo l and p split in F, as usual. We assume $l \nmid f$, which implies $l \nmid w_F$. Using the canonical isomorphism

$$\iota : I_G/I_G^2 \to G, \quad \overline{\sigma - 1} \mapsto \sigma, \quad \sigma \in G,$$

we can rewrite the Minus Conjecture with $s = 1$ as the following statement:

$$\iota(-w_F \tilde{\Theta}_K) = r_{\mathfrak{p}}(u^{1-\tau})^{h_{F,S}} \in G.$$

We recall the notations: $\mathfrak{p}$ is a chosen prime of F over p, and $u^{1-\tau}$ is a suitably chosen generator of $(U_S(F)/U_S(F)_{\mathrm{tor}})^{1-\tau}$. We need to be more precise however. The order of $[\mathfrak{p}]$ in $Cl_F = Cl_F^-$ is $h_F/h_{F,S}$; let u be a generator of

$\mathfrak{p}^{h_F/h_{F,S}}$. Then u, p are a $\mathbb{Z}$-basis of $U_S(F)/U_S(F)_{\mathrm{tor}}$, and the basis $u^{1-\tau}$ satisfies the sign rule explained in the statement of the conjecture in §1. Inserting this in the above formula we obtain the following version:

$$\iota(-w_F\tilde{\Theta}_K) = r_{\mathfrak{p}}(\psi^{1-\tau}) \in G, \tag{1}$$

where ψ is a generator of $\mathfrak{p}^{h_F}$.

Let t be the order of p modulo f and $q = p^t$. We consider a standard Gauss sum $g_0 = g(\omega^{-(q-1)/f}, \eta) \in \mathbb{Q}(\zeta_f, \zeta_p)$, where ω is the Teichmüller character associated to a prime $\mathfrak{P}$ over $\mathfrak{p}$ in $\mathbb{Q}(\zeta_{q-1})$ and η the standard additive character. Let D be the decomposition field for p in $\mathbb{Q}(\zeta_f)/\mathbb{Q}$, so $F \subseteq D \subseteq \mathbb{Q}(\zeta_f)$ and $\mathrm{Gal}(\mathbb{Q}(\zeta_f)/D) = \langle\sigma_p\rangle$. Let g be obtained from g_0^f (which lies in D - see [12], Lemmas 6.4 and 6.5) by taking the norm from D to F.

Lemma 3.1. *There is an explicit p-power p^n such that*

$$g^2 p^n \mathcal{O}_F = \mathfrak{p}^{-2(1-\tau)fh_F/w_F},$$

and consequently g^2 equals $\psi^{-2(1-\tau)f/w_F}$ up to a power of p and a root-of-unity-factor in F.

Proof: The primes above p split in D/F and are inert in $\mathbb{Q}(\zeta_f)/D$. From this one gets that $g\mathcal{O}_F = \mathfrak{p}^\beta$, where β is the image of the Stickelberger element without denominator $f\Theta_f = \sum_{a \bmod^\times f} a\sigma_a^{-1}$ in $\mathbb{Z}[\tau]$. We exponentiate with $(1-\tau)$. Since $g^{1+\tau}$ is a p-power, this changes g to g^2 times a p-power (always modulo roots of unity). On the right hand side we get $\mathfrak{p}^{(1-\tau)\beta}$, and $(1-\tau)\beta = (1-\tau)\chi(\beta)$ with χ the quadratic character of F; finally $\chi(\beta) = fB_{1,\chi} = -2fh_F/w_F$ by [12], Theorem 4.17. This gives the first formula in the lemma, and the second statement is a direct consequence. QED

The next step is now (and this will reappear later) to consider the p-adic leading term $T(g)$ of g. This is defined as follows: identify $F_{\mathfrak{p}}^\times$ with $\mathbb{Q}_p^\times$, write $g = p^z h$ with $z \in \mathbb{Z}$ and $h \in \mathbb{Z}_p^\times$, and let $T(g)$ be the image of h in $(\mathbb{Z}/p\mathbb{Z})^\times$. For $0 \le a < q-1 = p^t - 1$ we write out a p-adically as $a = a_0 + a_1 p + \ldots + a_{t-1}p^{t-1}$ with digits a_i in the interval $[0, p-1]$, and we put

$$a!! = a_0!a_1!\ldots a_{t-1}! \qquad \text{and} \qquad s(a) = a_0 + a_1 + \cdots + a_{t-1}.$$

From [12], Remark on page 97, we obtain the following congruence for any $a \bmod^\times f$:

$$g_0^{\sigma_a} \cdot (\zeta_p - 1)^{-s(a(q-1)/f)} \equiv (a(q-1)/f)!!^{-1} \pmod{\mathfrak{P}'},$$

where $\mathfrak{P}'$ is the prime of $\mathbb{Q}(\zeta_{q-1},\zeta_p)$ above $\mathfrak{P}$. As $f\cdot s(a(q-1)/f)\equiv a(q-1)\equiv 0 \pmod{p-1}$ and $(\zeta_p-1)^{p-1}\cdot(-p)^{-1}\equiv 1 \pmod{\mathfrak{P}'}$, we obtain by means of a well-known computation of p-adic digits

$$g_0^{f\sigma_a}\cdot(-p)^{-f\cdot s(a(q-1)/f)/(p-1)}\equiv\prod_{i=0}^{t-1}\Big(p\cdot\Big\langle\frac{\langle ap^i/f\rangle(q-1)}{p}\Big\rangle\Big)!^{-f}\pmod{\mathfrak{P}'},$$

where angular brackets mean the fractional part of a rational number.

Let χ be the nontrivial Dirichlet character attached to F. Recalling that $\chi(p)=1$ by hypothesis, we see that if σ_a runs over $\mathrm{Gal}(D/F)$ then $f\cdot\langle ap^i/f\rangle$ runs over all $c \bmod^\times f$, $\chi(c)=1$, and so

$$T(g)=\pm\prod_{\substack{c \bmod^\times f\\ \chi(c)=1}}\big(p\cdot\langle c(q-1)/(pf)\rangle\big)!^{-f}.$$

From this formula and Lemma 3.1 we obtain (writing $\sigma(a)$ instead of σ_a):

Lemma 3.2. $r_{\mathfrak{p}}(\psi^{(1-\tau)})=\sigma\big(\prod_{c \bmod^\times f,\,\chi(c)=1}(p\cdot\langle c(q-1)/(pf)\rangle)!\big)^{-w_F}$.

(A comment on signs: Both Lemma 3.1 and the preceding formula for $T(g)$ have a minus sign in their exponent; these cancel on putting things together; however a new exponent -1 arises, since the local Artin map sends a to σ_a^{-1}.)

The next step is to calculate with the element $\tilde\Theta_K$. Recall K is the compositum of F and the degree l field of conductor p, and $(1-\tau)\tilde\Theta_K$ equals Θ_K as defined in §1; by the way, Θ_K just differs from the "standard" Stickelberger element attached to K by a multiple of the norm element.

Lemma 3.3. $\iota(-f\tilde\Theta_K)=\prod_{a \bmod^\times pf,\,\chi(a)=1}\sigma_a^a\in G$.

Proof: As $\chi(p)=1$, the Frobenius of p on F is trivial and so $\tilde\Theta_K$ belongs to I_G. This gives

$$2pf\tilde\Theta_K=\sum_{\substack{a \bmod^\times pf\\ \chi(a)=1}}(2a-pf)\sigma_a^{-1}=\sum_{\substack{a \bmod^\times pf\\ \chi(a)=1}}(2a-pf)(\sigma_a^{-1}-1)$$

and the lemma follows using the fact that $\prod_a\sigma_a=1\in G$. QED

Our task is to show formula (1), which is, by means of Lemmas 3.2 and 3.3, equivalent to

$$\sigma\Big(\prod_{\substack{c \bmod^\times f\\ \chi(c)=1}}\Big(p\cdot\Big\langle\frac{c(q-1)}{pf}\Big\rangle\Big)!\Big)^{-f}=\prod_{\substack{a \bmod^\times pf\\ \chi(a)=1}}\sigma_a^a\in G,$$

and this in turn is equivalent to

$$\prod_{\substack{c \bmod^\times f \\ \chi(c)=1}} \Big(p \cdot \Big\langle \frac{c(q-1)}{pf} \Big\rangle\Big)!^{-f} \equiv_l \prod_{\substack{a \bmod^\times pf \\ \chi(a)=1}} a^a \in (\mathbb{Z}/p\mathbb{Z})^\times,$$

where $\equiv_l$ means equality up to a factor which is an l-th power. In fact we will prove the above formula up to 4-torsion in the multiplicative group $(\mathbb{Z}/p\mathbb{Z})^\times$. We will prove the following congruence modulo p (where one can even show that the sign is always "+" if f is even):

Theorem 3.4.

$$\prod_{\substack{c \bmod^\times f \\ \chi(c)=1}} \Big(p \cdot \Big\langle \frac{c(q-1)}{pf} \Big\rangle\Big)!^{-2f} \equiv \pm \prod_{\substack{a \bmod^\times pf \\ \chi(a)=1}} a^{2a} \pmod p.$$

We shall see that Theorem 3.4 can be obtained as a consequence of the still sharper results that follows, namely of Theorems 3.5 and 3.8. The integers $v(c)$ are defined later on.

Theorem 3.5. *For all $0 < c < f$ with $\chi(c) = 1$ we have*

$$\Big(p \cdot \Big\langle \frac{c(q-1)}{pf} \Big\rangle\Big)!^{-2f} \equiv \pm f^{-fv(c)} \cdot \prod_{\substack{a \bmod^\times pf \\ a \equiv c \pmod f}} a^{2a} \pmod p.$$

PROOF: Let x_c denote the product on the right hand side. Let y_c denotes a similar product with p being replaced by $q = p^t$, namely

$$y_c = \prod_{\substack{a \bmod^\times qf \\ a \equiv c \pmod f}} a^{2a}.$$

Lemma 3.6. $x_c \equiv y_c \pmod p$.

PROOF: We fix $a \in \{1, \dots, fp\}$ coprime to fp. We can write down the set of all $\alpha \in \{1, \dots, fq\}$ coprime to fq that map to a modulo fp: this is simply the set $I = \{a + ipf \mid i = 0, \dots, p^{t-1} - 1\}$. From this we find

$$\prod_{\substack{\alpha \bmod^\times qf \\ \alpha \mapsto a}} \alpha^{2\alpha} \equiv a^{2s} \pmod p,$$

where the exponent s is given as the sum of all elements in the set I. This sum has the value $p^{t-1}a + \frac{1}{2}p^{t-1}(p^{t-1}-1)pf$. In particular $2s$ is congruent to $2a$ modulo $p-1$; hence $a^{2s} \equiv a^{2a} \pmod{p}$. Since this argument works for all choices of a, the lemma follows. QED

We continue in the proof of 3.5.

The next step is to calculate y_c by a certain trick (symmetry). We define

$$I_c = \{a = 1, \ldots, fq-1 \mid (a, fq) = 1;\ a \equiv c \pmod{f}\}.$$

Then the set I_c carries an involution ε, which induces identity modulo f and multiplication by -1 modulo q. In more explicit terms, using the least nonnegative residue $j(c) = \langle \frac{2c}{f} \rangle \cdot f$ of $2c$ modulo f:

$$\varepsilon(a) = \begin{cases} -a + j(c)q & : \quad a < j(c)q, \\ -a + j(c)q + fq & : \quad a > j(c)q. \end{cases}$$

It is easily checked that $\prod_{a \in I_c} a$ maps to -1 modulo p (Wilson's theorem). We put $I_c' = \{a \in I_c \mid a > j(c)q\}$ (the set corresponding to the second case in the above description of ε) and we calculate mod p:

$$\begin{aligned} y_c &\equiv \prod_{a \in I_c} a^a \varepsilon(a)^{\varepsilon(a)} \\ &\equiv \pm \prod_{a \in I_c} a^{a+\varepsilon(a)} \\ &\equiv \pm \prod_{a \in I_c'} a^{fq} \cdot \prod_{a \in I_c} a^{j(c)q} \\ &\equiv \pm z_c^f, \end{aligned}$$

where we have put $z_c = \prod_{a \in I_c'} a$, and used again that $\prod_{a \in I_c} a \equiv -1 \pmod{p}$.

We need a better description of I_c'. Taking the residue modulo q gives the natural map $\nu \colon I_c \to \{i = 1, \ldots, q-1 \mid (p,i) = 1\}$, which is bijective.

Lemma 3.7. *(a) If $c < f/2$, then*

$$\nu(I_c') = \{d = 1, \ldots, q-1 \mid (p,d) = 1;\ \tfrac{c}{f} < \langle \tfrac{d}{f} \rangle \leq 1 - \tfrac{c}{f}\}.$$

(b) If $c > f/2$, then

$$\nu(I_c') = \{d = 1, \ldots, q-1 \mid (p,d) = 1;\ \langle \tfrac{d}{f} \rangle \leq \tfrac{\hat{c}}{f} \ \text{ or } \ 1 - \tfrac{\hat{c}}{f} < \langle \tfrac{d}{f} \rangle\},$$

where $\hat{c} = f - c$. Note that the condition on d is exactly the logical complement of the analogous condition in part (a), with c replaced by $\hat{c}$.

PROOF: Let d be prime to p and in the set $\{1, \ldots, q-1\}$. The preimage $\nu^{-1}(d) \in I_c$ has the form $d + iq$, $0 \leq i < f$. We can get at the number i by noting that $q \equiv 1 (\mathrm{mod}\ f)$, so $d + i \equiv c (\mathrm{mod}\ f)$, that is, i is the least nonnegative residue of $c - d$ modulo f. Moreover $\nu^{-1}(d) \in I'_c$ iff $i \geq j(c)$.

We now first treat case (a), that is $c < f/2$. Then $j(c) = 2c$, and $i \geq j(c)$ happens iff $c - d$ is congruent to $2c$, $2c + 1$, ..., $f - 1$ modulo f, which translates to $d \equiv c + 1, c + 2, \ldots, f - c \ (\mathrm{mod}\ f)$.

In case (b) we have $c > f/2$, and $j(c) = 2c - f$. Then $i \geq j(c)$ iff $c - d$ is congruent to $2c - f$, $2c - f + 1$, ..., $f - 1$ modulo f; this happens iff d is congruent to $c + 1, c + 2, \ldots, f - 1, 0, 1, \ldots, f - c$ modulo f. The latter condition translates to: either $d \equiv 0, \ldots, \hat{c} (\mathrm{mod}\ f)$ or $d \equiv f - \hat{c} + 1, \ldots, f - 1$ $(\mathrm{mod}\ f)$. This proves the lemma. QED

We turn to the final part of the proof of 3.5 now, which consists in an explicit calculation of z_c.

We first assume $c < f/2$ and put $u(c) = |I'_c|$. The last lemma gives

$$z_c \equiv \prod_{i=c+1}^{f-c} \prod_{\substack{d \bmod^\times q \\ d \equiv i \pmod f}} d = f^{u(c)} \prod_{i=c+1}^{f-c} \prod_{\substack{d \bmod^\times q \\ d \equiv i \pmod f}} \frac{d}{f} \pmod p.$$

The inner product can be simplified using the p-adic Gamma function:

$$\begin{aligned} \prod_{\substack{d \bmod^\times q \\ d \equiv i \pmod f}} \frac{d}{f} &= \prod_{j=1}^{(q-1)/f} -\frac{\Gamma_p((i+jf)/f)}{\Gamma_p((i-f+jf)/f)} \\ &= \pm \frac{\Gamma_p((i+q-1)/f)}{\Gamma_p(i/f)} \equiv \pm \frac{\Gamma_p((i-1)/f)}{\Gamma_p(i/f)} \pmod p \end{aligned}$$

as Γ_p preserves congruences modulo p. Therefore

$$z_c \equiv \pm f^{u(c)} \prod_{i=c+1}^{f-c} \frac{\Gamma_p((i-1)/f)}{\Gamma_p(i/f)} = \pm f^{u(c)} \frac{\Gamma_p(c/f)}{\Gamma_p((f-c)/f)} \pmod p.$$

Lemma 3.7 gives that

$$z_c \cdot z_{f-c} \equiv \prod_{d \bmod^\times q} d \equiv -1 \pmod p$$

and so

$$z_{f-c} \equiv -z_c^{-1} \equiv \pm f^{-u(c)} \frac{\Gamma_p((f-c)/f)}{\Gamma_p(c/f)} \pmod p.$$

Therefore we no longer have to distinguish whether $c < f/2$ or not. Setting $v(c) = u(c)$ for $c < f/2$ and $v(c) = -u(f-c)$ for $c > f/2$, in both cases we have

$$z_c \equiv \pm f^{v(c)} \frac{\Gamma_p(c/f)}{\Gamma_p((f-c)/f)} \pmod{p}.$$

In the next step we use the functional equation:

$$\begin{aligned} z_c &\equiv \pm f^{v(c)} \Gamma_p(1-c/f)^{-2} \\ &\equiv \pm f^{v(c)} \Gamma_p(1+c(q-1)/f)^{-2} \\ &\equiv \pm f^{v(c)} \Gamma_p(1+p\langle c(q-1)/(pf)\rangle)^{-2} \\ &= \pm f^{v(c)} (p\langle c(q-1)/(pf)\rangle)!^{-2} \pmod{p}. \end{aligned}$$

It follows that

$$y_c \equiv \pm z_c^f \equiv \pm f^{fv(c)} (p\langle c(q-1)/(pf)\rangle)!^{-2f} \pmod{p}$$

and Theorem 3.5 follows. QED

It remains to prove the following result which shows that all the f-powers which we picked up in Theorem 3.5 to prove Theorem 3.4 do not matter in the end.

Let us define an integer V by

$$V = f \cdot \sum_{\substack{c \bmod^\times f \\ \chi(c)=1}} v(c).$$

We then have the following result:

Theorem 3.8. *There is an equality*

$$V = (p-1)p^{t-1} \frac{2fh_F}{w_F};$$

in particular V is divisible by $p-1$, and so $f^V \equiv 1 \pmod{p}$.

PROOF: We first remark that we did not find a simple argument showing just $(p-1) \mid V$; apparently we have to calculate the exact value and use $w_F \mid 2f$.

We recall, slightly adapting our notation:

$$v(c) = \epsilon_c \cdot |\{d \bmod^\times q,\ \tfrac{\hat{c}}{f} < \langle \tfrac{d}{f} \rangle \leq 1 - \tfrac{\hat{c}}{f}\}|,$$

where ϵ_c is $+1$ or -1, and $\hat{c}$ is either c or $f-c$, both according to whether $c < f/2$ or $c > f/2$.

Via the involution $c \mapsto f - c$, the residues $c > f/2$ with $\chi(c) = 1$ correspond bijectively to the residues $c < f/2$ with $\chi(c) = -1$, because of $\chi(-1) = -1$. Hence we can rewrite the sum as follows:

$$V = f \cdot \sum_{\substack{c \bmod^\times f \\ c<f/2}} \left(\chi(c) \cdot \sum_{\substack{d \bmod^\times q \\ \frac{c}{f} < \langle \frac{d}{f} \rangle \leq 1 - \frac{c}{f}}} 1 \right) = f \cdot \sum_{d \bmod^\times q} \sum_{\substack{c \bmod^\times f \\ c<f/2 \\ \frac{c}{f} < \langle \frac{d}{f} \rangle \leq 1 - \frac{c}{f}}} \chi(c).$$

We define $\beta(r) = \sum_{c=1}^{r-1} \chi(c)$ for any positive integer r. Then $\beta(r)$ depends only on the residue of r modulo f because $\sum_{c=1}^{f} \chi(c) = 0$.

We shall show that the inner sum over c in the last displayed formula equals $\beta(d)$. Let $\frac{d'}{f} = \langle \frac{d}{f} \rangle$. If $d' < f/2$ then the inner sum in question is simply $\beta(d')$. For the complementary case $d' > f/2$, the condition $c < d' \leq f - c$ is tantamount to $c \leq f - d'$. By the change of variables $c \mapsto f - c$ we obtain

$$\sum_{c=1}^{f-d'} \chi(c) = \sum_{c=d'}^{f-1} \chi(f-c) = -\sum_{c=d'}^{f-1} \chi(c) = -(\beta(f) - \beta(d')) = \beta(d').$$

So we end up with $\beta(d') = \beta(d)$ in both cases. Therefore

$$V = f \cdot \sum_{d \bmod^\times q} \beta(d) = f \cdot (V' - V''),$$

where

$$V' = \sum_{d=1}^{q} \beta(d) \qquad \text{and} \qquad V'' = \sum_{d=1}^{q/p} \beta(pd).$$

The analytic class number formula gives

$$\begin{aligned} \sum_{d=1}^{f} \beta(d) &= \sum_{d=1}^{f} \sum_{c=1}^{d-1} \chi(c) = \sum_{c=1}^{f-1} \sum_{d=c+1}^{f} \chi(c) = \sum_{c \bmod^\times f} (f-c) \cdot \chi(c) \\ &= -\sum_{c \bmod^\times f} c \cdot \chi(c) = \frac{2 f h_F}{w_F}. \end{aligned}$$

From this we get (recalling that $q = p^t \equiv 1$ modulo f):

$$V' = \frac{q-1}{f} \cdot \sum_{d=1}^{f} \beta(d) = (q-1) \cdot \frac{2 h_F}{w_F}.$$

This takes care of V'. We shall concentrate on V'' now:

$$V'' = \sum_{d=1}^{q/p} \beta(pd) = \sum_{d=1}^{q/p} \beta(f \cdot \langle \tfrac{pd}{f} \rangle) = \sum_{d=1}^{q/p} \sum_{c=1}^{f\langle pd/f\rangle - 1} \chi(c) = \sum_{c=1}^{f-1} r_c \chi(c),$$

where r_c means the number of $d = 1, 2, \ldots, p^{t-1}$ satisfying $c < f \cdot \langle \frac{pd}{f} \rangle$. So r_c is the number of pairs (d, e) with $1 \le d \le p^{t-1}$ and $1 \le e \le f-c-1$ such that $pd \equiv f-e \pmod f$, i.e. $d \equiv -ep^{t-1} \pmod f$, which means $f \mid ep^{t-1}+d$. But $ep^{t-1}+d$ runs throught $p^{t-1}+1, p^{t-1}+2, \ldots, (f-c)p^{t-1}$ without repetitions. So

$$\begin{aligned} r_c &= \Big[\frac{(f-c)p^{t-1}}{f}\Big] - \Big[\frac{p^{t-1}}{f}\Big] = p^{t-1} - \Big[\frac{p^{t-1}}{f}\Big] + \Big[-\frac{cp^{t-1}}{f}\Big] \\ &= p^{t-1} - \Big[\frac{p^{t-1}}{f}\Big] - 1 - \Big[\frac{cp^{t-1}}{f}\Big], \end{aligned}$$

where we have used $f \nmid cp^{t-1}$. Thus, considering χ also as a ring homomorphism $\mathbb{Q}[\mathrm{Gal}(\mathbb{Q}(\zeta_f)/\mathbb{Q})] \to \mathbb{Q}$, we have

$$\begin{aligned} V'' &= -\sum_{c=1}^{f-1} \Big[\frac{cp^{t-1}}{f}\Big]\chi(c) = -\chi\Big(\sum_{c \bmod^\times f} \Big[\frac{cp^{t-1}}{f}\Big]\sigma_c^{-1}\Big) \\ &= -\chi\Big((p^{t-1} - \sigma_{p^{t-1}}) \sum_{c \bmod^\times f} \frac{c}{f}\,\sigma_c^{-1}\Big) = (p^{t-1}-1)\frac{2h_F}{w_F}, \end{aligned}$$

because $\chi(p) = 1$. This gives $V' - V'' = (q - p^{t-1})\frac{2h_F}{w_F}$ and Theorem 3.8 follows. QED

We now see at once that Theorem 3.4 follows from Theorems 3.5 and 3.8. Since Theorem 3.4 implies formula (1), which in turn is equivalent to the Minus Conjecture, we have proved:

Theorem 3.9. *The Minus Conjecture is true in case $s = 1$ and $l \nmid f$. (The notation and the setup are explained at the beginning of this section.)*

§4. *Transformation of $\tilde{\Theta}_K$ and the Vanishing Order Conjecture*

In this section we allow all imaginary fields F (the conductor is written f) and all values $s \ge 1$, as in §§1-2. We repeat that $l \nmid w_F$ and we also suppose until further notice that K^+ equals its own genus field $K_1 \cdots K_s$ (recall K_i is the degree l conductor p_i field). Recall that all primes $p_1, \ldots, p_s$ split in F.

Before starting the proof of the Minus Conjecture it is necessary to process the quantity $\tilde{\Theta}_K$. As a byproduct we will obtain that it is always in I_G^s (so conjecture (VOC) holds). The expression we are going to get for $\tilde{\Theta}_K$ looks complicated, but for $s = 2$ it will fit quite well into the Minus Conjecture since on the regulator side the same structure will appear.

Some notation is required. For all $T \subseteq \{1, \ldots, s\}$ let K_T denote the compositum of all K_i with $i \in T$; here $K_\emptyset = \mathbb{Q}$. Let $G_T = \mathrm{Gal}(K_T/\mathbb{Q})$ which is always tacitly identified with the product of the $G_{\{i\}} = G_i$ for $i \in T$. Note that $K_{\{1,\ldots,s\}} = K^+$. We also need matrices of Frobenius symbols, related to the matrix A of §2 but with entries in I_G. To begin with, let α_{ij} be the Frobenius of p_i in K_j $(i \neq j)$. For $V \subsetneq U \subseteq \{1, \ldots, s\}$ define a matrix $\tilde{M}_V^U = (\tilde{m}_{ij}^U)_{i,j \in U-V}$ over I_{G_U} as follows: for $i \neq j$, we set $\tilde{m}_{ij}^U = \alpha_{ij}^{-1} - 1$. For $i = j$ we set

$$\tilde{m}_{ii}^U = \prod_{j \in U, j \neq i} \alpha_{ij} \ - 1.$$

It is easy to see that the row sums of each matrix $\tilde{M}_\emptyset^U$ are zero modulo I_G^2. Finally let $\tilde{A}_V^U = \det \tilde{M}_V^U$. For $V = U$ this has to be interpreted as 1 (the determinant of the empty matrix).

For each $T \subseteq \{1, \ldots, s\}$ we set $m_T = \prod_{i \in T} p_i$ (this is the conductor of K_T), and we have a Stickelberger element Θ_T attached to FK_T the same way as Θ_K was attached to K:

$$\Theta_T = (1 - \tau)\tilde{\Theta}_T, \quad \tilde{\Theta}_T = \sum_{\lambda \in G_T} a^T(\lambda)\, \lambda^{-1},$$

with

$$a^T(\lambda) = \sum_{\substack{t \bmod^\times f m_T \\ \sigma_t|F=1 \\ \sigma_t|K_T=\lambda}} \Big(\frac{t}{f m_T} - \frac{1}{2}\Big).$$

Next we associate to every $T \neq \emptyset$ a term $\tilde{R}_T$ which will later give a contribution towards the leading term of $\tilde{\Theta}_K$.

Definition: The map $\tilde{g}_T : G_T \to I_G^{|T|}$ is given by

$$\tilde{g}_T\Big(\prod_{i \in T} \gamma_i\Big) = \prod_{i \in T} (\gamma_i - 1) \qquad (\text{where } \gamma_i \in G_i \text{ for all } i \in T).$$

Now let, for $\emptyset \neq T \subseteq \{1, \ldots, s\}$,

$$\tilde{R}_T = \sum_{\lambda \in G_T} a^T(\lambda)\, \tilde{g}_T(\lambda^{-1}).$$

If life were simple, $\tilde{R}_{\{1,\ldots,s\}}$ would be equal to $\tilde{\Theta}_K$. This is not the case. We will see that $\tilde{R}_{\{1,\ldots,s\}}$ is only "the principal term" in a representation of $\tilde{\Theta}_K$ as a sum with many terms.

Proposition 4.1. *We have for any nonempty subset U of $\{1,\ldots,s\}$:*

$$\tilde{\Theta}_U \equiv \sum_{\emptyset \neq T \subseteq U} \tilde{A}_T^U \cdot \tilde{R}_T \pmod{I_{G_U}^{|U|+1}}.$$

PROOF: We have to begin with a lemma.

Lemma 4.2. *For any sets $V \subseteq U \subseteq \{1,\ldots,s\}$ and any $\lambda \in G_{U-V}$ we have*

$$\sum_{\mu \in G_V} a^U(\lambda\mu) = \sum_{J \subseteq V} (-1)^{|J|} a^{U-V}\left(\lambda \prod_{u \in J} \mathrm{Frob}_{U-V}(p_u)^{-1}\right),$$

where $\mathrm{Frob}_T(q)$ means Frobenius of q in $\mathrm{Gal}(K_T/\mathbb{Q}) = G_T$.

PROOF: It is easy to see that our Θ_U is equal to $e^{-}\theta'_{fm_U}(-1)$ in the notation of Sinnott (see [10]). Using well-known norm relations (see Lemma 12 in [9] for example) we obtain

$$\begin{aligned}
\mathrm{res}_{FK_U/FK_{U-V}}\,\Theta_U &= \Theta_{U-V} \prod_{u \in V} (1 - \mathrm{Frob}_{U-V}(p_u)^{-1}) \\
&= (1-\tau) \sum_{\lambda \in G_{U-V}} a^{U-V}(\lambda)\,\lambda^{-1} \sum_{J \subseteq V} \prod_{u \in J} (-\mathrm{Frob}_{U-V}(p_u)^{-1}) \\
&= (1-\tau) \sum_{\lambda \in G_{U-V}} \lambda^{-1} \sum_{J \subseteq V} (-1)^{|J|} a^{U-V}\left(\lambda \prod_{u \in J} \mathrm{Frob}_{U-V}(p_u)^{-1}\right).
\end{aligned}$$

On the other hand, from the fact that we can decompose G_U into a direct product $G_U = G_V \times G_{U-V}$, we obtain

$$\mathrm{res}_{FK_U/FK_{U-V}}\,\Theta_U = (1-\tau) \sum_{\lambda \in G_{U-V}} \sum_{\mu \in G_V} a^U(\lambda\mu)\,\lambda^{-1}.$$

Comparing coefficients gives the lemma. QED

Continuing in the proof of 4.1, we note that l does not divide the number of roots of unity in $FK_{\{1,\ldots,s\}}$ (since $l \nmid w_F$). Proposition 2.1 in [10] implies that $a^T(\lambda)$ is l-integral for any $T \subseteq \{1,\ldots,s\}$, and so $\tilde{R}_T \in I_{G_T}^{|T|}$. We shall use induction with respect to $|U|$.

If $|U| = 1$ then from the definition and the fact that the coefficients $a^U(\lambda)$ sum to zero (see Lemma 4.2 for $V = U$) we obtain at once that $\tilde{\Theta}_U = \tilde{R}_U$. Since we have set $\tilde{A}_U^U = 1$, the proposition holds true in this case.

Let us suppose $|U| > 1$ and that the proposition has been proved for all smaller nonempty sets. Using again the fact that for any $T \subseteq U$ we can decompose G_U into a direct product $G_U = G_T \times G_{U-T}$, the definition of $\tilde{g}_U$ gives, by multiplying out, that:

$$\tilde{R}_U = \sum_{T \subseteq U} (-1)^{|U-T|} \sum_{\lambda \in G_T} \sum_{\mu \in G_{U-T}} a^U(\lambda\mu) \cdot \lambda^{-1}.$$

Lemma 4.2 implies

$$\begin{aligned}
\tilde{R}_U &= \sum_{T \subseteq U} (-1)^{|U-T|} \sum_{\lambda \in G_T} \lambda^{-1} \cdot \sum_{J \subseteq U-T} (-1)^{|J|} a^T \left(\lambda \prod_{u \in J} \mathrm{Frob}_T(p_u)^{-1} \right) \\
&= \sum_{T \subseteq U} \sum_{\lambda \in G_T} \lambda^{-1} \cdot \sum_{J \subseteq U-T} (-1)^{|U-T-J|} \left(\prod_{u \in J} \mathrm{Frob}_T(p_u)^{-1} \right) a^T(\lambda) \\
&= \sum_{T \subseteq U} \sum_{J \subseteq U-T} (-1)^{|U-T-J|} \left(\prod_{u \in J} \mathrm{Frob}_T(p_u)^{-1} \right) \tilde{\Theta}_T \\
&= \sum_{T \subseteq U} \tilde{\Theta}_T \prod_{u \in U-T} \big(\mathrm{Frob}_T(p_u)^{-1} - 1 \big).
\end{aligned}$$

Using the induction hypothesis we get (the congruence is modulo $I_U^{|U|+1}$):

$$\begin{aligned}
\tilde{R}_U - \tilde{\Theta}_U &= \sum_{\emptyset \neq J \subseteq U} \tilde{\Theta}_{U-J} \prod_{u \in J} \big(\mathrm{Frob}_{U-J}(p_u)^{-1} - 1 \big) \\
&\equiv \sum_{\emptyset \neq J \subseteq U} \left(\prod_{u \in J} \big(\mathrm{Frob}_{U-J}(p_u)^{-1} - 1 \big) \right) \sum_{\emptyset \neq T \subseteq U-J} \tilde{A}_T^{U-J} \tilde{R}_T \\
&= \sum_{\emptyset \neq T \subsetneq U} \tilde{R}_T \sum_{\emptyset \neq J \subseteq U-T} \tilde{A}_T^{U-J} \prod_{u \in J} \big(\mathrm{Frob}_{U-J}(p_u)^{-1} - 1 \big).
\end{aligned}$$

Since

$$\mathrm{Frob}_{U-J}(p_u)^{-1} - 1 = \prod_{j \in U-J} \alpha_{uj}^{-1} - 1 \equiv \sum_{j \in U-J} (\alpha_{uj}^{-1} - 1) \pmod{I_{U-J}^2},$$

we have

$$\tilde{R}_U - \tilde{\Theta}_U \equiv \sum_{\emptyset \neq T \subsetneq U} \tilde{R}_T \sum_{\emptyset \neq J \subseteq U-T} \tilde{A}_T^{U-J} \prod_{u \in J} \sum_{j \in U-J} (\alpha_{uj}^{-1} - 1) \pmod{I_U^{|U|+1}}.$$

At this point we need to modify the matrix $\tilde{M}_T^{U-J}$ slightly, in order to work with a matrix that has all row sums equal to zero. Define for $V \subsetneq U \subseteq \{1,\dots,s\}$ a new matrix $\bar{M}_V^U$. First, $\bar{M}_\emptyset^U$ has the same entries as $\tilde{M}_\emptyset^U$ off the diagonal, and we fill the diagonal in such a way that all row sums become zero. Second, $\bar{M}_V^U$ is obtained from $\tilde{M}_\emptyset^U$ simply by omitting rows and columns belonging to indices in V. Then $\bar{M}_V^U$ and $\tilde{M}_V^U$ are congruent modulo I_U^2. We also let $\bar{A}_V^U = \det \bar{M}_V^U$. The right hand side in the last formula will stay the same modulo $I_U^{|U|+1}$ if $\tilde{A}$ is replaced by $\bar{A}$. The proposition will thus be proved if we can show that

$$\sum_{J\subseteq U-T} \bar{A}_T^{U-J} \prod_{u\in J} \sum_{j\in U-J} (\alpha_{uj}^{-1} - 1) = 0 \tag{2}$$

for any $\emptyset \neq T \subsetneq U$. To show this, we use the following very convenient theorem of Chaiken and Kleitman [2] on matrices and trees.

Theorem 4.3. *Let $M = (m_{ij})_{i,j\in\{1,\dots,n\}}$ be a matrix over any commutative ring with zero row sums. For any forest L on $\{1,\dots,n\}$ we put*

$$M(L) = \prod_{(i\to j) \text{ is an edge in } L} (-m_{ij}).$$

Then for any $T \subseteq \{1,\dots,n\}$ we have

$$\det(m_{ij})_{i,j\in\{1,\dots,n\}-T} = \sum_L M(L),$$

where L runs over the set of all forests on $\{1,\dots,n\}$ whose set of roots is T.

In our case, we fix $J \subseteq U - T$ and obtain

$$\bar{A}_T^{U-J} = \sum_{\substack{L \text{ is a forest on } U-J \\ \sqrt{L}=T}} \bar{M}_\emptyset^{U-J}(L),$$

where the sum is taken over all forests on the set of vertices $U - J$ and the set of roots T. Since $\bar{M}_\emptyset^{U-J}$ and the corresponding submatrix of $\bar{M}_\emptyset^U$ have the same entries off the diagonal, we get

$$\bar{A}_T^{U-J} \prod_{u\in J} \sum_{j\in U-J} \big(-(\alpha_{uj}^{-1} - 1)\big) = \sum_{\substack{L \text{ is a forest on } U \\ \sqrt{L}=T \\ J\subseteq \ell(L)}} \bar{M}_\emptyset^U(L),$$

where the sum is taken over all forests L on the set of vertices U and the set of roots T, whose set of leaves $\ell(L)$ contains J. So the left hand side of (2) equals

$$\sum_{J\subseteq U-T}(-1)^{|J|}\sum_{\substack{L \text{ is a forest on } U\\ \sqrt{L}=T\\ J\subseteq\ell(L)}}\bar{M}^U_\emptyset(L) =$$

$$\sum_{\substack{L \text{ is a forest on } U\\ \sqrt{L}=T}}\bar{M}^U_\emptyset(L)\sum_{J\subseteq(U-T)\cap\ell(L)}(-1)^{|J|}=0,$$

because $U-T\neq\emptyset$ and so $(U-T)\cap\ell(L)\neq\emptyset$, too. Proposition 4.1 is now proved. QED

Since each term $\tilde{A}^U_T$ is the determinant of a matrix of size $|U|-|T|$ with entries in I_U and each term $\tilde{R}_T$ is visibly in $I_T^{|T|}$, we obtain at once that $\tilde{\Theta}_U$ is in $I_U^{|U|}$. On setting $U=\{1,\ldots,s\}$ we now obtain that (VOC) is true, that is, we have:

Theorem 4.4. *Under the assumptions stated at the beginning of the section, the element $\tilde{\Theta}_K=\tilde{\Theta}_{\{1,\ldots,s\}}$ lies in I^s_G. In other words: The congruence in (MC) is at least true modulo I^s_G and just says $0\equiv 0$.*

§5. *Simplification of the Minus Conjecture for* $s=2$

Until Theorem 8.9 at the very end of the paper we assume from now on that $s=2$, $S=\{p_1,p_2\}$ and that K^+ is its own genus field, that is, $K^+=K_1K_2$.

In the proof of Proposition 4.1 we showed that for $|U|=1$ the equality $\tilde{R}_U=\tilde{\Theta}_U$ does hold, and we write $\tilde{\Theta}_i$ for $\tilde{\Theta}_{\{i\}}$. We will now spell out Proposition 4.1 for the case $s=2$. Let α_{ij} be defined as in §4, i.e. α_{ij} is the Frobenius of p_i in K_j for $i\neq j$, and set $\alpha_{11}=\alpha_{12}^{-1}$, $\alpha_{22}=\alpha_{21}^{-1}$. Then

$$\tilde{M}^{1,2}_\emptyset=\begin{pmatrix}\alpha_{11}^{-1}-1 & \alpha_{12}^{-1}-1\\ \alpha_{21}^{-1}-1 & \alpha_{22}^{-1}-1\end{pmatrix}.$$

The quantities $\tilde{A}^{\{1,2\}}_{\{i\}}$ are obtained by deleting the i-th row and column from this matrix and taking the determinant ($i=1,2$). Therefore Proposition 4.1 amounts to:

$$\begin{aligned}\tilde{\Theta}_K &\equiv \tilde{R}_{1,2}+(\alpha_{11}^{-1}-1)\tilde{R}_2+(\alpha_{22}^{-1}-1)\tilde{R}_1\\ &\equiv \tilde{R}_{1,2}+(\alpha_{11}^{-1}-1)\tilde{\Theta}_2+(\alpha_{22}^{-1}-1)\tilde{\Theta}_1 \pmod{I_G^3}. \qquad (3)\end{aligned}$$

We now show that the minus-unit regulator has a very similar decomposition. Let $\mathfrak{p}_1$ and $\mathfrak{p}_2$ be prime ideals in F above p_1 and p_2, respectively.

Let us denote $t_1 = \frac{h_F}{h_{F,\{p_1\}}}$, $t_2 = \frac{h_F}{h_{F,\{p_2\}}}$, $t_3 = \frac{h_F h_{F,S}}{h_{F,\{p_1\}} h_{F,\{p_2\}}}$, $t_1' = \frac{h_{F,\{p_1\}}}{h_{F,S}} = \frac{t_2}{t_3}$, $t_2' = \frac{h_{F,\{p_2\}}}{h_{F,S}} = \frac{t_1}{t_3}$. Then t_2 is the smallest positive integer such that $\mathfrak{p}_2^{t_2} = (u_2)$ is principal. Similarly t_2' is the smallest positive integer for which there is an integer t such that $\mathfrak{p}_1^{t_2'}\mathfrak{p}_2^{t} = (u_1)$ is principal. Then u_1, u_2, p_1, p_2 is a basis of $U_S(F)/U_S(F)_{\rm tor}$ and $u_1^{1-\tau}, u_2^{1-\tau}$ is a basis of $\big(U_S(F)/U_S(F)_{\rm tor}\big)^{1-\tau}$ and it is well-oriented with respect to $\mathfrak{p}_1, \mathfrak{p}_2$.

With this choice we get $\mathrm{Reg}^-_{K,S} = \det(r_{\mathfrak{p}_j}(u_i^{1-\tau}) - 1)_{i,j=1,2}$, with $r_{\mathfrak{p}_j}(x)$ denoting the local Artin symbol $(x, K_{\mathfrak{p}_j}/F_{\mathfrak{p}_j})$. Note that (here and elsewhere) this is a harmless abuse of notation for $(x, K_{\mathfrak{P}}/F_{\mathfrak{p}_j})$ with $\mathfrak{P}$ being a prime above $\mathfrak{p}_j$ in K.

Let $\beta_{ij} = (u_i^{1-\tau}, (FK_j)_{\mathfrak{p}_j}/F_{\mathfrak{p}_j}) \in G_j \subseteq G$, for *all* $i, j \in \{1, 2\}$ (including $i = j$). Let $\tilde{M}^- = (\beta_{ij} - 1)_{i,j=1,2}$.

Proposition 5.1. *The following congruence holds modulo I_G^2:*

$$(r_{\mathfrak{p}_j}(u_i^{1-\tau}) - 1)_{i,j=1,2} \;\equiv\; \tilde{M}^- + \begin{pmatrix} t_2'(\alpha_{11}^{-1} - 1) & t(\alpha_{22}^{-1} - 1) \\ 0 & t_2(\alpha_{22}^{-1} - 1) \end{pmatrix}$$

Proof: We have

$$r_{\mathfrak{p}_1}(u_1^{1-\tau}) = (u_1^{1-\tau}, (FK_1)_{\mathfrak{p}_1}/F_{\mathfrak{p}_1})(u_1^{1-\tau}, (FK_2)_{\mathfrak{p}_1}/F_{\mathfrak{p}_1}) = \beta_{11}\alpha_{12}^{t_2'},$$

because $(FK_2)_{\mathfrak{p}_1}/F_{\mathfrak{p}_1}$ is unramified and the $\mathfrak{p}_1$-valuation of $u_1^{1-\tau}$ is t_2'. Similarly

$$\begin{aligned} r_{\mathfrak{p}_1}(u_2^{1-\tau}) &= (u_2^{1-\tau}, (FK_1)_{\mathfrak{p}_1}/F_{\mathfrak{p}_1})(u_2^{1-\tau}, (FK_2)_{\mathfrak{p}_1}/F_{\mathfrak{p}_1}) = \beta_{21}, \\ r_{\mathfrak{p}_2}(u_1^{1-\tau}) &= (u_1^{1-\tau}, (FK_1)_{\mathfrak{p}_2}/F_{\mathfrak{p}_2})(u_1^{1-\tau}, (FK_2)_{\mathfrak{p}_2}/F_{\mathfrak{p}_2}) = \alpha_{21}^{t}\beta_{12}, \\ r_{\mathfrak{p}_2}(u_2^{1-\tau}) &= (u_2^{1-\tau}, (FK_1)_{\mathfrak{p}_2}/F_{\mathfrak{p}_2})(u_2^{1-\tau}, (FK_2)_{\mathfrak{p}_2}/F_{\mathfrak{p}_2}) = \alpha_{21}^{t_2}\beta_{22}. \end{aligned}$$

The proposition follows using the canonical isomorphism $I_G/I_G^2 \cong G$. QED

On taking determinants in Proposition 5.1 we find:

Corollary 5.2. *The following congruence holds modulo I_G^3:*

$$\begin{aligned} \mathrm{Reg}^-_{K,S} \equiv \det(\tilde{M}^-) &+ t_2'(\alpha_{11}^{-1} - 1)(\beta_{22} - 1) + t_2(\alpha_{22}^{-1} - 1)(\beta_{11} - 1) \\ &+ t_2 t_2'(\alpha_{11}^{-1} - 1)(\alpha_{22}^{-1} - 1) - t(\alpha_{22}^{-1} - 1)(\beta_{21} - 1). \end{aligned}$$

It is easy to see that $u_2^{1-\tau}$ is a basis of $\big(U_{p_2}(F)/U_{p_2}(F)_{\rm tor}\big)^{1-\tau}$ and so the definition of the regulator in case $s = 1$ gives $\mathrm{Reg}^-_{FK_2,S} = \beta_{22} - 1$.

Writing the principal ideal $\mathfrak{p}_1^{t_1}$ in the form $\mathfrak{p}_1^{t_3t_2'} = ((u_1)\cdot\mathfrak{p}_2^{-t})^{t_3}$ gives that $t_2 \mid tt_3$ and $\mathfrak{p}_1^{t_1} = (u_1^{t_3}u_2^{t'})$ with $t' = -tt_3/t_2$. Then $(u_1^{t_3}u_2^{t'})^{1-\tau}$ is a basis of $\big(U_{p_1}(F)/U_{p_1}(F)_{\mathrm{tor}}\big)^{1-\tau}$ and

$$\begin{aligned}((u_1^{t_3}u_2^{t'})^{1-\tau}, (FK_1)_{\mathfrak{p}_1}/F_{\mathfrak{p}_1}) &= (u_1^{1-\tau}, (FK_1)_{\mathfrak{p}_1}/F_{\mathfrak{p}_1})^{t_3}(u_2^{1-\tau}, (FK_1)_{\mathfrak{p}_1}/F_{\mathfrak{p}_1})^{t'}\\ &= \beta_{11}^{t_3}\beta_{21}^{t'},\end{aligned}$$

hence

$$\mathrm{Reg}^-_{FK_1,S} \equiv t_3(\beta_{11}-1) - \frac{tt_3}{t_2}(\beta_{21}-1) \pmod{I_{G_1}^2}. \tag{4}$$

Therefore substituting $t_2(\beta_{11}-1) \equiv t(\beta_{21}-1) + \frac{t_2}{t_3}\mathrm{Reg}^-_{FK_1,S}$ into the congruence of Corollary 5.2 gives

$$\begin{aligned}\mathrm{Reg}^-_{K,S} \equiv \det(\tilde{M}^-) &+ t_2'(\alpha_{11}^{-1}-1)\,\mathrm{Reg}^-_{FK_2,S} + (\alpha_{22}^{-1}-1)\big(t(\beta_{21}-1) + t_1'\,\mathrm{Reg}^-_{FK_1,S}\big)\\ &+ t_2t_2'(\alpha_{11}^{-1}-1)(\alpha_{22}^{-1}-1) - t(\alpha_{22}^{-1}-1)(\beta_{21}-1).\end{aligned}$$

After rearrangement and simplification this gives

Corollary 5.3. *Modulo I_G^3 we have*

$$\begin{aligned}\mathrm{Reg}^-_{K,S} \equiv \det(\tilde{M}^-) &+ \frac{h_{F,\{p_2\}}}{h_{F,S}}(\alpha_{11}^{-1}-1)\,\mathrm{Reg}^-_{FK_2,S} + \frac{h_{F,\{p_1\}}}{h_{F,S}}(\alpha_{22}^{-1}-1)\,\mathrm{Reg}^-_{FK_1,S}\\ &+ \frac{h_F}{h_{F,S}}(\alpha_{11}^{-1}-1)(\alpha_{22}^{-1}-1).\end{aligned}$$

We now turn back to formula (3). Since (MC) is proved for $s=1$, we may replace the theta terms by minus regulators as follows:

$$\tilde{\Theta}_K \equiv \tilde{R}_{1,2} - \frac{h_{F,\{p_2\}}}{w_F}(\alpha_{11}^{-1}-1)\,\mathrm{Reg}^-_{FK_2,S} - \frac{h_{F,\{p_1\}}}{w_F}(\alpha_{22}^{-1}-1)\,\mathrm{Reg}^-_{FK_1,S} \pmod{I_G^3}.$$

On comparing this with Corollary 5.3 we see that $\tilde{\Theta}_K \equiv -\frac{h_{F,S}}{w_F}\mathrm{Reg}^-_{K,S}$ if and only if

$$\tilde{R}_{1,2} \equiv -\frac{h_{F,S}}{w_F}\det(\tilde{M}^-) - \frac{h_F}{w_F}(\alpha_{11}^{-1}-1)(\alpha_{22}^{-1}-1) \pmod{I_G^3}.$$

Under Assumption (A), the automorphism α_{21} and hence also α_{11} is identity. In any case $l(\alpha_{11}^{-1}-1)(\alpha_{22}^{-1}-1) \in I_G^3$. So we have proved:

Corollary 5.4. *Under Assumption (A), or if $l \mid h_F$, the Minus Conjecture (MC) for $s=2$ is equivalent to the following congruence:*

$$\tilde{R}_{1,2} \equiv -\frac{h_{F,S}}{w_F}\det(\tilde{M}^-) \pmod{I_G^3}.$$

Actually both sides of this congruence are in the submodule $I_{G_1}I_{G_2}$ of I_G^2. This will further simplify our task. It is easily verified that the canonical map

$$I_{G_1}/I_{G_1}^2 \otimes_{\mathbb{Z}} I_{G_2}/I_{G_2}^2 \to I_G^2/I_G^3$$

is well-defined and injective. (Indeed, both $I_{G_1}/I_{G_1}^2$ and $I_{G_2}/I_{G_2}^2$ are copies of $\mathbb{Z}/l\mathbb{Z}$, so it suffices to see that the map is not zero.) Putting together the canonical isomorphisms $\iota_j : I_{G_j}/I_{G_j}^2 \to G_j$, we get a canonical isomorphism

$$\iota = \iota_{1,2} : I_{G_1}/I_{G_1}^2 \otimes_{\mathbb{Z}} I_{G_2}/I_{G_2}^2 \to G_1 \otimes_{\mathbb{Z}} G_2.$$

It is our intention to consider the formula in 5.4 above as an equality (to be proven) in $G_1 \otimes_{\mathbb{Z}} G_2$. We want to avoid working with chosen generators of G_1 and G_2 as long as possible. In other words, we would like to keep the argument "coordinate-free" as long as feasible. However, a quaint little problem of notation comes up. The groups G_j are naturally multiplicative groups, but one should rather work with additively written groups when looking at tensor products over $\mathbb{Z}$. On the other hand, additive notation for G_j would look awful (try it!). For lack of a better idea we introduce, for any multiplicative abelian group Γ, an additive group $\lg\Gamma$, which is just a copy of Γ. The symbol lg is just formal (reminiscent of a logarithm), and

$$\lg\Gamma = \{\lg\gamma | \gamma \in \Gamma\}, \quad \lg\gamma + \lg\delta = \lg(\gamma\delta) \quad \forall \gamma, \delta \in \Gamma.$$

Now we put $R_{1,2} = \iota_{1,2}(\tilde{R}_{1,2})$. We note that

$$\iota_{1,2}\tilde{g}_{1,2}(\gamma_1\gamma_2) = \lg\gamma_1 \otimes \lg\gamma_2$$

and that

$$\iota_{1,2}\det(\tilde{M}^-) = \lg\beta_{11} \otimes \lg\beta_{22} - \lg\beta_{21} \otimes \lg\beta_{12}.$$

Thus,

$$\begin{aligned} R_{1,2} &= \sum_{\gamma_1 \in G_1} \sum_{\gamma_2 \in G_2} a^{1,2}(\gamma_1\gamma_2) \cdot \lg(\gamma_1^{-1}) \otimes \lg(\gamma_2^{-1}) \\ &= \sum_{\gamma_1 \in G_1} \sum_{\gamma_2 \in G_2} a^{1,2}(\gamma_1\gamma_2) \cdot (-\lg\gamma_1) \otimes (-\lg\gamma_2) \\ &= \sum_{\gamma_1 \in G_1} \sum_{\gamma_2 \in G_2} a^{1,2}(\gamma_1\gamma_2) \cdot \lg\gamma_1 \otimes \lg\gamma_2 \end{aligned}$$

and the formula of Corollary 5.4 can be rewritten as follows.

Corollary 5.5. *(Assumptions as in Corollary 5.4.) The Minus Conjecture is equivalent to the following* **equality** *in* $\lg G_1 \otimes_{\mathbb{Z}} \lg G_2$*:*

$$\sum_{\gamma_1 \in G_1} \sum_{\gamma_2 \in G_2} a^{1,2}(\gamma_1\gamma_2) \cdot \lg \gamma_1 \otimes \lg \gamma_2 = -\frac{h_{F,S}}{w_F}\Big(\lg \beta_{11} \otimes \lg \beta_{22} - \lg \beta_{21} \otimes \lg \beta_{12}\Big). \quad (5)$$

§6. *A formula for* $R_{1,2}$

In this section we shall continue to assume $s = 2$. For convenience, we will very often write p for p_1 and q for p_2. (Thus, q will never denote a p-power.) To explain the outcome of this section we need some notation (slightly different from earlier notations): For $u \in (\mathbb{Z}/p\mathbb{Z})^\times$ let $\sigma_u \in G_1 = \mathrm{Gal}(FK_1/F)$ be given by the condition that σ_u is the restriction of $\zeta_p \mapsto \zeta_p^u$ on K_1 and identity on F. We define $\tau_v \in G_2 = \mathrm{Gal}(FK_2/F)$ similarly for $v \in (\mathbb{Z}/q\mathbb{Z})^\times$. (No relation with $\tau =$ complex conjugation.) Recall that χ is the nontrivial Dirichlet character attached to F and that f is the conductor of F (and so also of χ).

Theorem 6.1. *If* $\gamma(u)$ *stands for* $\Gamma_q(\frac{u}{fp})$*, then*

$$R_{1,2} = \sum_{\substack{a \bmod^\times pf \\ \chi(a)=1}} \lg \sigma_a \otimes \lg \tau_{\gamma(a)}.$$

Since this formula is probably not very enlightening at first sight, we give a numerical example. Take $l = 3$, $f = 4$, $p = 13$, and omit the lg symbols for simplicity. Then (the dependence on q is hidden in γ):

$$\begin{aligned} R_{1,2} \;=\; & \sigma_5 \otimes \tau_{\gamma(5)} + \sigma_9 \otimes \tau_{\gamma(9)} + \sigma_4 \otimes \tau_{\gamma(17)} + \sigma_8 \otimes \tau_{\gamma(21)} \\ & + \sigma_{12} \otimes \tau_{\gamma(25)} + \sigma_3 \otimes \tau_{\gamma(29)} + \sigma_7 \otimes \tau_{\gamma(33)} + \sigma_{11} \otimes \tau_{\gamma(37)} \\ & + \sigma_2 \otimes \tau_{\gamma(41)} + \sigma_6 \otimes \tau_{\gamma(45)} + \sigma_{10} \otimes \tau_{\gamma(49)} \in G_1 \otimes G_2 \cong \mathbb{Z}/3\mathbb{Z}. \end{aligned}$$

Note that we omitted $\sigma_1 \otimes \tau_{\gamma(1)}$ since $\lg \sigma_1 \otimes \lg \tau_{\gamma(1)}$ is the zero element of $\lg G_1 \otimes \lg G_2$.

Before we enter the proof of Theorem 6.1, let us mention that it arose as the result of at least two successive generalisations, which make it very technical and unfortunately not very enlightening. However, we think we would lose more by abandoning generality than we would gain. The strange-looking Lemma 6.3 (which was also seriously tested by computer, to minimise

error probability) has the purpose of eliminating an ungainly obstruction term, which unavoidably appears in the main part of the proof. Proposition 6.2 is just a preparation for this important lemma. It is recommended to skip over 6.2 and 6.3 at the first reading (going directly to the not so long proof of 6.1) and refer back to them later.

For any integer a we define non-negative integers $r(a) < fpq$, $h(a) < fp$ by the following conditions:

$$\begin{aligned} r(a) &\equiv h(a) \equiv 2a \pmod f, \\ r(a) &\equiv h(a) \equiv 0 \pmod p, \\ r(a) &\equiv pf \pmod q. \end{aligned}$$

Notice that both $r(a)$ and $h(a)$ only depend on a modulo f. The following proposition holds true for any odd quadratic Dirichlet character χ of conductor f and any primes p, q such that $p \neq q$ and $\chi(p) = \chi(q) = 1$:

Proposition 6.2. *Let $u = \#\{t \bmod^\times f \mid \chi(t) = 1, \langle \frac{2t}{f} \rangle < \frac{1}{q}\}$ (so in particular $u = 0$ for $f \leq 4$). Let $v = q^{(p-1)/3}$ if $f = 3$, $v = q^{(p-1)/2}$ if $f = 4$, and $v = (-1)^u$ if $f > 4$. Then we have*

$$\prod_{\substack{0<a<r(a)\\ \chi(a)=-1\\ q|a,\, p\nmid a}} a \equiv v \cdot \prod_{\substack{0<a<pf\\ \chi(a)=1\\ q|a,\, p\nmid a}} a \cdot \prod_{\substack{h(a)<a<pf\\ \chi(a)=1\\ p\nmid a}} a \pmod p. \tag{6}$$

Proof: Let n_1, n_2, n_3 be the number of factors in the three products above. By means of the substitution $b = a + pqt$, where t is determined by $-pqt \equiv a \pmod f$, we obtain

$$\begin{aligned} n_1 &= \sum_{\substack{t \bmod^\times f\\ \chi(t)=1}} \#\{b \mid pqt < b < r(-pqt) + pqt,\ qf|b,\ p \nmid b\} \\ &= \sum_{\substack{t \bmod^\times f\\ \chi(t)=1}} \Big(\big[\tfrac{r(-pqt)+pqt}{qf}\big] - \big[\tfrac{pqt}{qf}\big] - \big[\tfrac{r(-pqt)+pqt}{pqf}\big] + \big[\tfrac{pqt}{pqf}\big] \Big). \end{aligned}$$

It is easy to check that $r(-pqt) \equiv -2pqt + pf \pmod{pqf}$ and so $r(-pqt) = pqf\langle -\frac{2t}{f} + \frac{1}{q} \rangle = -2pqt + pf - pqf[-\frac{2t}{f} + \frac{1}{q}]$, which gives

$$\begin{aligned} n_1 &= \sum_{\substack{t \bmod^\times f\\ \chi(t)=1}} \Big(\big[-\tfrac{pt}{f} + \tfrac{p}{q} - p[-\tfrac{2t}{f} + \tfrac{1}{q}]\big] - \big[\tfrac{pt}{f}\big] - \big[-\tfrac{t}{f} + \tfrac{1}{q} - \big[-\tfrac{2t}{f} + \tfrac{1}{q}\big]\big] + \big[\tfrac{t}{f}\big] \Big) \\ &\equiv \sum_{\substack{t \bmod^\times f\\ \chi(t)=1}} \Big(\big[-\tfrac{pt}{f} + \tfrac{p}{q}\big] - \big[\tfrac{pt}{f}\big] - \big[-\tfrac{t}{f} + \tfrac{1}{q}\big] + \big[\tfrac{t}{f}\big] \Big) \pmod{p-1}. \end{aligned}$$

Therefore the first product in (6)

$$\prod_{\substack{0<a<r(a)\\ \chi(a)=-1\\ q|a,\,p\nmid a}} a \equiv (fq)^{n_1} \prod_{\substack{t \bmod^\times f\\ \chi(t)=1}} \prod_{\substack{pqt<b<r(-pqt)+pqt\\ qf|b,\ p\nmid b}} \tfrac{b}{fq} \pmod p$$

$$= (fq)^{n_1}(-1)^{c_1} \prod_{\substack{t \bmod^\times f\\ \chi(t)=1}} \Gamma_p\big(1+[-\tfrac{pt}{f}+\tfrac{p}{q}]-p[-\tfrac{2t}{f}+\tfrac{1}{q}]\big)\Gamma_p\big(1+[\tfrac{pt}{f}]\big)^{-1}$$

$$\equiv (fq)^{n_1}(-1)^{c_1} \prod_{\substack{t \bmod^\times f\\ \chi(t)=1}} \Gamma_p\big(1+[-\tfrac{pt}{f}+\tfrac{p}{q}]\big)\Gamma_p\big(1+[\tfrac{pt}{f}]\big)^{-1} \pmod p,$$

where $c_1 = \sum_{t \bmod^\times f,\,\chi(t)=1}\big([-\frac{pt}{f}+\frac{p}{q}]-p[-\frac{2t}{f}+\frac{1}{q}]-[\frac{pt}{f}]\big)$.

The second product in (6) can be treated by means of the substitution $b = a - pqt$, where t is determined by $pqt \equiv a \pmod f$. We obtain

$$n_2 = \sum_{\substack{t \bmod^\times f\\ \chi(t)=1}} \#\{b \mid -pqt < b < pf - pqt,\ qf|b,\ p\nmid b\}$$

$$= \sum_{\substack{t \bmod^\times f\\ \chi(t)=1}} \big([\tfrac{pf-pqt}{qf}]-[\tfrac{-pqt}{qf}]-[\tfrac{pf-pqt}{pqf}]+[\tfrac{-pqt}{pqf}]\big)$$

$$= \sum_{\substack{t \bmod^\times f\\ \chi(t)=1}} \big([-\tfrac{pt}{f}+\tfrac{p}{q}]-[-\tfrac{pt}{f}]-[-\tfrac{t}{f}+\tfrac{1}{q}]+[-\tfrac{t}{f}]\big)$$

and

$$\prod_{\substack{0<a<pf\\ \chi(a)=1\\ q|a,\,p\nmid a}} a \equiv (fq)^{n_2} \prod_{\substack{t \bmod^\times f\\ \chi(t)=1}} \prod_{\substack{-pqt<b<pf-pqt\\ qf|b,\ p\nmid b}} \tfrac{b}{fq} \pmod p$$

$$= (fq)^{n_2}(-1)^{c_2} \prod_{\substack{t \bmod^\times f\\ \chi(t)=1}} \Gamma_p\big(1+[-\tfrac{pt}{f}+\tfrac{p}{q}]\big)\Gamma_p\big(1+[-\tfrac{pt}{f}]\big)^{-1},$$

where $c_2 = \sum_{t \bmod^\times f,\,\chi(t)=1}\big([-\frac{pt}{f}+\frac{p}{q}]-[-\frac{pt}{f}]\big)$.

Similarly by means of the substitution $b = a - pt$, where t is determined by $pt \equiv a \pmod f$, we obtain

$$n_3 = \sum_{\substack{t \bmod^\times f\\ \chi(t)=1}} \#\{b \mid h(pt) - pt < b < pf - pt,\ f|b,\ p\nmid b\}$$

$$= \sum_{\substack{t \bmod^\times f\\ \chi(t)=1}} \big([\tfrac{pf-pt}{f}]-[\tfrac{h(pt)-pt}{f}]-[\tfrac{pf-pt}{pf}]+[\tfrac{h(pt)-pt}{pf}]\big).$$

It is easy to check that $h(pt) \equiv 2pt \pmod{pf}$ and so $h(pt) = pf\langle\frac{2t}{f}\rangle = 2pt - pf[\frac{2t}{f}]$, which gives

$$\begin{aligned} n_3 &= \sum_{\substack{t \bmod^\times f \\ \chi(t)=1}} \big([p - \tfrac{pt}{f}] - \big[\tfrac{pt}{f} - p[\tfrac{2t}{f}]\big] - [1 - \tfrac{t}{f}] + \big[\tfrac{t}{f} - [\tfrac{2t}{f}]\big]\big) \\ &\equiv \sum_{\substack{t \bmod^\times f \\ \chi(t)=1}} \big([-\tfrac{pt}{f}] - [\tfrac{pt}{f}] - [-\tfrac{t}{f}] + [\tfrac{t}{f}]\big) \pmod{p-1}. \end{aligned}$$

Thus the third product in (6)

$$\begin{aligned} \prod_{\substack{h(a)<a<pf \\ \chi(a)=1 \\ p\nmid a}} a &\equiv f^{n_3} \prod_{\substack{t \bmod^\times f \\ \chi(t)=1}} \prod_{\substack{h(pt)-pt<b<pf-pt \\ f\mid b,\ p\nmid b}} \tfrac{b}{f} \pmod{p} \\ &= f^{n_3}(-1)^{c_3} \prod_{\substack{t \bmod^\times f \\ \chi(t)=1}} \Gamma_p\big(1+p+[-\tfrac{pt}{f}]\big)\Gamma_p\big(1+[\tfrac{pt}{f}]-p[\tfrac{2t}{f}]\big)^{-1} \\ &\equiv f^{n_3}(-1)^{c_3} \prod_{\substack{t \bmod^\times f \\ \chi(t)=1}} \Gamma_p\big(1+[-\tfrac{pt}{f}]\big)\Gamma_p\big(1+[\tfrac{pt}{f}]\big)^{-1} \pmod{p}, \end{aligned}$$

where $c_3 = \sum_{t \bmod^\times f,\, \chi(t)=1} \big(p + [-\frac{pt}{f}] - [\frac{pt}{f}] + p[\frac{2t}{f}]\big)$.

Putting these results together we see that $n_1 - n_2 - n_3 \equiv 0 \pmod{p-1}$ and that

$$\prod_{\substack{0<a<r(a) \\ \chi(a)=-1 \\ q\mid a,\, p\nmid a}} a \cdot \prod_{\substack{0<a<pf \\ \chi(a)=1 \\ q\mid a,\, p\nmid a}} a^{-1} \cdot \prod_{\substack{h(a)<a<pf \\ \chi(a)=1 \\ p\nmid a}} a^{-1} \equiv q^{n_3}(-1)^{c_1-c_2-c_3} \pmod{p}.$$

The proposition will be proved if we show that the right hand side of the previous congruence is congruent to v. If $p = 2$ then the parity of $c_1 - c_2 - c_3$ is not important, if p is odd then

$$c_1 - c_2 - c_3 \equiv \sum_{\substack{t \bmod^\times f \\ \chi(t)=1}} \big(1 + [\tfrac{2t}{f}] + [-\tfrac{2t}{f} + \tfrac{1}{q}]\big) \equiv \sum_{\substack{t \bmod^\times f \\ \chi(t)=1}} \big([\tfrac{2t}{f}] - [\tfrac{2t}{f} - \tfrac{1}{q}]\big) \equiv u \pmod{2}.$$

We have the following congruence modulo $p-1$:

$$\begin{aligned} n_3 &\equiv 2 \sum_{\substack{t \bmod^\times f \\ \chi(t)=1}} \big([\tfrac{t}{f}] - [\tfrac{pt}{f}]\big) = 2 \sum_{\substack{t \bmod^\times f \\ \chi(t)=1}} \big(\tfrac{t}{f} - \tfrac{pt}{f} - \langle\tfrac{t}{f}\rangle + \langle\tfrac{pt}{f}\rangle\big) = \tfrac{2(1-p)}{f} \sum_{\substack{t \bmod^\times f \\ \chi(t)=1}} t \\ &= \tfrac{(1-p)}{f} \sum_{t \bmod^\times f} (1+\chi(t))t = (1-p) \sum_{t \bmod^\times f} \big(\tfrac{\varphi(f)}{2} - \tfrac{2h_F}{w_F}\big) \pmod{p-1}. \end{aligned}$$

If $f=3$ then $n_3 \equiv (1-p)(1-\frac{1}{3}) \equiv \frac{1}{3}(p-1)$, if $f=4$ then $n_3 \equiv (1-p)(1-\frac{1}{2}) \equiv \frac{1}{2}(p-1)$. Finally, if $f>4$ then $n_3 \equiv 0$. In all cases $q^{n_3}(-1)^{c_1-c_2-c_3} \equiv v \pmod p$ and the proposition is proved. QED

Lemma 6.3. *Let d be any integer satisfying $pfd \equiv 1 \pmod q$. Then the integer*

$$n = \prod_{\substack{a \bmod^{\times} pf \\ q\nmid a,\ \chi(a)=1}} a^{q\langle \frac{da}{q}\rangle - 1}$$

is an l-th power modulo p.

Proof: Since $0 < fp - h(a) + fpq\langle \frac{dh(a)}{q}\rangle < fpq$ and

$$fp - h(a) + fpq\langle \frac{dh(a)}{q}\rangle \equiv \begin{cases} fp(1+dh(a)) - h(a) \equiv pf \pmod q, \\ -h(a) \equiv 0 \pmod p, \\ -h(a) \equiv -2a \pmod f, \end{cases}$$

we have $r(-a) = fp - h(a) + fpq\langle \frac{dh(a)}{q}\rangle$. The left hand side of (6)

$$\prod_{\substack{0<a<r(a)\\ \chi(a)=-1\\ q|a,\,p\nmid a}} a = \prod_{\substack{0<-a<r(-a)\\ \chi(a)=1\\ q|a,\,p\nmid a}} (-a) = \prod_{\substack{0>a>h(a)-fp-fpq\langle \frac{dh(a)}{q}\rangle\\ \chi(a)=1\\ q|a,\,p\nmid a}} (-a)$$

$$= (-1)^{n_1} \prod_{y=0}^{q-1} \Big(\Big(\prod_{\substack{-fpy>a>h(a)-fp-fpy\\ \chi(a)=1,\ y\equiv dh(a) \pmod q\\ q|a,\,p\nmid a}} a \Big) \cdot \prod_{\substack{0>a>-fpy\\ \chi(a)=1,\ y\equiv dh(a) \pmod q\\ q|a,\,p\nmid a}} a \Big),$$

where n_1 again means the number of factors of this product. By means of the substitution $b = a + fp(y+1)$ for the former inner product and of the substitution $b = a + fpx$, $x = 1, 2, \ldots, y$, for the latter one we obtain the following congruence modulo p:

$$\prod_{\substack{0<a<r(a)\\ \chi(a)=-1\\ q|a,\,p\nmid a}} a \equiv (-1)^{n_1} \prod_{y=0}^{q-1} \Big(\Big(\prod_{\substack{h(b)<b<fp\\ \chi(b)=1,\ y\equiv dh(b) \pmod q\\ p\nmid b,\ db\equiv y+1 \pmod q}} b \Big) \cdot \prod_{x=1}^{y} \prod_{\substack{0<b<fp\\ \chi(b)=1,\ y\equiv dh(b) \pmod q\\ p\nmid b,\ db\equiv x \pmod q}} b \Big)$$

$$= (-1)^{n_1} \Big(\prod_{\substack{h(b)<b<fp\\ \chi(b)=1,\ p\nmid b\\ db\equiv dh(b)+1 \pmod q}} b \Big) \cdot \prod_{\substack{0<b<fp\\ \chi(b)=1,\ p\nmid b\\ 0<\langle \frac{db}{q}\rangle \le \langle \frac{dh(b)}{q}\rangle}} b \pmod p.$$

Let us consider the following partition on the set $I = \{a \bmod^{\times} fp \mid \chi(a) = 1\}$:

$$
\begin{aligned}
I_1 &= \{a \in I,\, q|a,\, a < h(a)\},\\
I_2 &= \{a \in I,\, q|a,\, a > h(a),\, dh(a) \equiv -1 \pmod q\},\\
I_3 &= \{a \in I,\, q|a,\, a > h(a),\, dh(a) \not\equiv -1 \pmod q\},\\
I_4 &= \{a \in I,\, q \nmid a,\, a < h(a),\, \left\langle \tfrac{da}{q} \right\rangle \le \left\langle \tfrac{dh(a)}{q} \right\rangle\},\\
I_5 &= \{a \in I,\, q \nmid a,\, a < h(a),\, \left\langle \tfrac{da}{q} \right\rangle > \left\langle \tfrac{dh(a)}{q} \right\rangle\},\\
I_6 &= \{a \in I,\, q \nmid a,\, a > h(a),\, dh(a) \equiv -1 \pmod q\},\\
I_7 &= \{a \in I,\, q \nmid a,\, a > h(a),\, dh(a) \not\equiv -1 \pmod q,\, \left\langle \tfrac{da}{q} \right\rangle \le \left\langle \tfrac{1+dh(a)}{q} \right\rangle\},\\
I_8 &= \{a \in I,\, q \nmid a,\, a > h(a),\, dh(a) \not\equiv -1 \pmod q,\, \left\langle \tfrac{da}{q} \right\rangle > \left\langle \tfrac{1+dh(a)}{q} \right\rangle\}.
\end{aligned}
$$

Tedious evaluation of all possibilities gives that Proposition 6.2 can be stated also in the following form:

$$(-1)^{n_1} v \cdot \prod_{a \in I_3} a^2 \prod_{a \in I_1 \cup I_2 \cup I_8} a \cdot \prod_{a \in I_4} a^{-1} \equiv 1 \pmod p. \tag{7}$$

Let us consider the involution ε on the set I such that $\varepsilon(a) \equiv a \pmod f$ and $\varepsilon(a) \equiv -a \pmod p$. Then

$$n^2 \equiv \pm \prod_{\substack{a \bmod^{\times} fp \\ q|a,\ \chi(a)=1}} a^2 \cdot \prod_{\substack{a \bmod^{\times} fp \\ \chi(a)=1}} a^{q\langle \frac{da}{q} \rangle + q\langle \frac{d\varepsilon(a)}{q} \rangle - 2} \pmod p.$$

Wilson's theorem implies

$$\prod_{\substack{a \bmod^{\times} fp \\ \chi(a)=1}} a^{q\langle \frac{dh(a)}{q} \rangle - 1} = \prod_{\substack{t \bmod^{\times} f \\ \chi(t)=1}} \Big(\prod_{\substack{a \bmod^{\times} fp \\ a \equiv t \pmod f}} a \Big)^{q\langle \frac{dh(t)}{q} \rangle - 1} \equiv \pm 1 \pmod p.$$

Therefore

$$n^2 \equiv \pm \prod_{\substack{a \bmod^{\times} fp \\ q|a,\ \chi(a)=1}} a^2 \cdot \prod_{\substack{a \bmod^{\times} fp \\ \chi(a)=1}} a^{q(\langle \frac{da}{q} \rangle + \langle \frac{d\varepsilon(a)}{q} \rangle - \langle \frac{dh(a)}{q} \rangle) - 1} \pmod p. \tag{8}$$

It is easy to see that

$$a + \varepsilon(a) = \begin{cases} h(a) & \text{if } a < h(a), \\ h(a) + fp & \text{otherwise,} \end{cases}$$

and so

$$\langle \tfrac{d(a+\varepsilon(a))}{q} \rangle = \begin{cases} \langle \tfrac{dh(a)}{q} \rangle & \text{if } a < h(a), \\ \langle \tfrac{1+dh(a)}{q} \rangle & \text{otherwise.} \end{cases}$$

Moreover

$$\langle \tfrac{da}{q} \rangle + \langle \tfrac{d\varepsilon(a)}{q} \rangle = \begin{cases} \langle \tfrac{d(a+\varepsilon(a))}{q} \rangle & \text{if } \langle \tfrac{da}{q} \rangle \le \langle \tfrac{d(a+\varepsilon(a))}{q} \rangle, \\ \langle \tfrac{d(a+\varepsilon(a))}{q} \rangle + 1 & \text{otherwise,} \end{cases}$$

and

$$\langle \tfrac{1+dh(a)}{q} \rangle - \langle \tfrac{dh(a)}{q} \rangle = \begin{cases} \frac{1}{q} & \text{if } dh(a) \not\equiv -1 \pmod q, \\ \frac{1-q}{q} & \text{otherwise.} \end{cases}$$

If we go again through all eight cases, we find

$$q\big(\langle \tfrac{da}{q} \rangle + \langle \tfrac{d\varepsilon(a)}{q} \rangle - \langle \tfrac{dh(a)}{q} \rangle\big) - 1 = \begin{cases} -1 & \text{if } a \in I_1 \cup I_4, \\ 0 & \text{if } a \in I_3 \cup I_6 \cup I_7, \\ -q & \text{if } a \in I_2, \\ q-1 & \text{if } a \in I_5, \\ q & \text{if } a \in I_8, \end{cases}$$

and (8) gives the following congruence modulo lth powers

$$n^2 \equiv_l \pm \prod_{\substack{a \bmod^\times fp \\ q|a,\ \chi(a)=1}} a^2 \cdot \prod_{a \in I_1 \cup I_2 \cup I_4} a^{-1} \cdot \prod_{a \in I_8} a \pmod p.$$

The lemma follows from (7) and the fact that both -1 and v are lth powers modulo p. QED

Proof of Theorem 6.1: As a first step, we define $a(u,v)$ to be the integer between 0 and $fpq-1$ which is congruent to u modulo fp, and congruent to v modulo q. Then by definition

$$fpqR_{1,2} = \sum_{u \in I} \sum_{v=1}^{q-1} \big(a(u,v) - \tfrac{1}{2}fpq\big) \cdot \lg \sigma_u \otimes \lg \tau_v,$$

where $I = \{u \bmod^\times fp \mid \chi(u) = 1\}$. For any $u \in I$ and any positive integer $v < q$ let $b(u,v) = \frac{a(u,v)-u}{fp}$. It is easy to see that $b(u,v)$ is an integer and that $0 \le b(u,v) < q$. Moreover $fp \cdot b(u,v) \equiv v - u \pmod q$. Recall that the integer d satisfies $fpd \equiv 1 \pmod q$, so $b(u,v) \equiv d(v-u) \pmod q$, which gives

$$b(u,v) = q\langle \tfrac{d(v-u)}{q} \rangle = d(v-u) - q[\tfrac{d(v-u)}{q}] = d(v-u) - q\big([\tfrac{dv}{q}] + [-\tfrac{du}{q}] + \alpha_{u,v}\big),$$

where $\alpha_{u,v} = 1$ if $\left\langle \frac{dv}{q} \right\rangle + \left\langle -\frac{du}{q} \right\rangle \geq 1$ and $\alpha_{u,v} = 0$ otherwise. Therefore

$$a(u,v) = u + fp \cdot b(u,v) = fp\big(dv - q[\tfrac{dv}{q}]\big) - fp\big(du + q[-\tfrac{du}{q}]\big) + u - fpq\alpha_{u,v}.$$

Wilson's theorem gives that $\sum_{v=1}^{q-1} \lg \tau_v = \lg \tau_{-1} = 0$ and $\sum_{u \in I} \lg \sigma_u = \lg \sigma_{-1} = 0$. Consequently, any sum of the form $\sum_{u \in I} \sum_{v=1}^{q-1} c(u,v) \lg \sigma_u \otimes \lg \tau_v$ where the function $c(u,v)$ is independent of u or independent of v will be zero. This shows, given the above expression for $a(u,v)$, that

$$R_{1,2} = -\sum_{u \in I} \sum_{v=1}^{q-1} \alpha_{u,v} \cdot \lg \sigma_u \otimes \lg \tau_v = \sum_{v=1}^{q-1} \sum_{u \in I} (1 - \alpha_{u,v}) \cdot \lg \sigma_u \otimes \lg \tau_v.$$

Since $\alpha_{u,v} = 0$ if and only if $\left\langle \frac{dv}{q} \right\rangle < 1 - \left\langle -\frac{du}{q} \right\rangle$, which is the case if and only if either $q \mid u$ or $\left\langle \frac{dv}{q} \right\rangle < \left\langle \frac{du}{q} \right\rangle$, we obtain

$$\begin{aligned} R_{1,2} &= \sum_{v=1}^{q-1} \Big(\sum_{\substack{u \in I \\ q \mid u}} \lg \sigma_u + \sum_{\substack{u \in I \\ \langle \frac{du}{q} \rangle > \langle \frac{dv}{q} \rangle}} \lg \sigma_u \Big) \otimes \lg \tau_v \\ &= \sum_{b=1}^{q-2} \sum_{\substack{u \in I \\ \langle \frac{du}{q} \rangle > \frac{b}{q}}} \lg \sigma_u \otimes \lg \tau_{fpb}, \end{aligned}$$

where we have used the identity $\sum_{v=1}^{q-1} \lg \tau_v = 0$ and the substitution $v = fpb$. Since $\gamma(u) = \Gamma_q\big(\frac{u}{fp}\big) \equiv \Gamma_q(du) \pmod q$ and $\Gamma_q(a) = (-1)^a (a-1)!$ for any $a \in \{1, 2, \ldots, q\}$, the right hand side of Theorem 6.1 equals

$$\begin{aligned} \sum_{u \in I} \lg \sigma_u \otimes \lg \tau_{\gamma(u)} &= \sum_{a=1}^{q-1} \sum_{\substack{u \in I \\ du \equiv a \,(\mathrm{mod}\ q)}} \lg \sigma_u \otimes \lg \tau_{(a-1)!} \\ &= \sum_{a=1}^{q-1} \sum_{b=1}^{a-1} \sum_{\substack{u \in I \\ du \equiv a \,(\mathrm{mod}\ q)}} \lg \sigma_u \otimes \lg \tau_b \\ &= \sum_{b=1}^{q-2} \sum_{a=b+1}^{q-1} \sum_{\substack{u \in I \\ du \equiv a \,(\mathrm{mod}\ q)}} \lg \sigma_u \otimes \lg \tau_b \\ &= \sum_{b=1}^{q-2} \sum_{\substack{u \in I \\ \langle \frac{du}{q} \rangle > \frac{b}{q}}} \lg \sigma_u \otimes \lg \tau_b. \end{aligned}$$

We have $\lg \tau_{fpb} = \lg \tau_b + \lg \tau_{fp}$, so to prove Theorem 6.1 we need to show that

$$\Big(\sum_{b=1}^{q-2} \sum_{\substack{u\in I \\ \langle \frac{du}{q}\rangle > \frac{b}{q}}} \lg \sigma_u\Big) \otimes \lg \tau_{fp} = 0.$$

It is easy to see that

$$\sum_{b=1}^{q-2} \sum_{\substack{u\in I \\ \langle \frac{du}{q}\rangle > \frac{b}{q}}} \lg \sigma_u = \sum_{u\in I,\, q\nmid u} (q\big\langle \tfrac{du}{q}\big\rangle - 1) \lg \sigma_u.$$

We shall show that this sum is zero. In multiplicative notation this amounts to proving that $\prod_{u\in I,\, q\nmid u} u^{q\langle \frac{du}{q}\rangle - 1}$ is an lth power modulo p; but this is exactly the statement of Lemma 6.3. QED

We return to our numerical example $l = 3$, $f = 4$, $p = 13$. (It is not necessary to specify q; the dependence on q is hidden in γ.) Let us identify $G_1 = (\mathbb{Z}/13\mathbb{Z})^\times/3$ with $\mathbb{Z}/3\mathbb{Z}$ via the following isomorphism κ: ± 1 and ± 5 (the cubes modulo 13) map to $\bar{0}$ under κ, $\pm 2, \pm 10$ map to $\bar{1}$, and $\pm 4, \pm 6$ map to $\bar{2} = \overline{-1}$. Thus $G_1 \otimes G_2$ becomes identified with G_2, and we can do without the lg notation. Then $R_{1,2}$, or rather its image in $G_2 = (\mathbb{Z}/q\mathbb{Z})^\times/3$, comes out as

$$\gamma(9)^{-1}\,\gamma(17)^{-1}\,\gamma(29)\,\gamma(33)^{-1}\,\gamma(37)\,\gamma(41)\,\gamma(45)^{-1}\,\gamma(49).$$

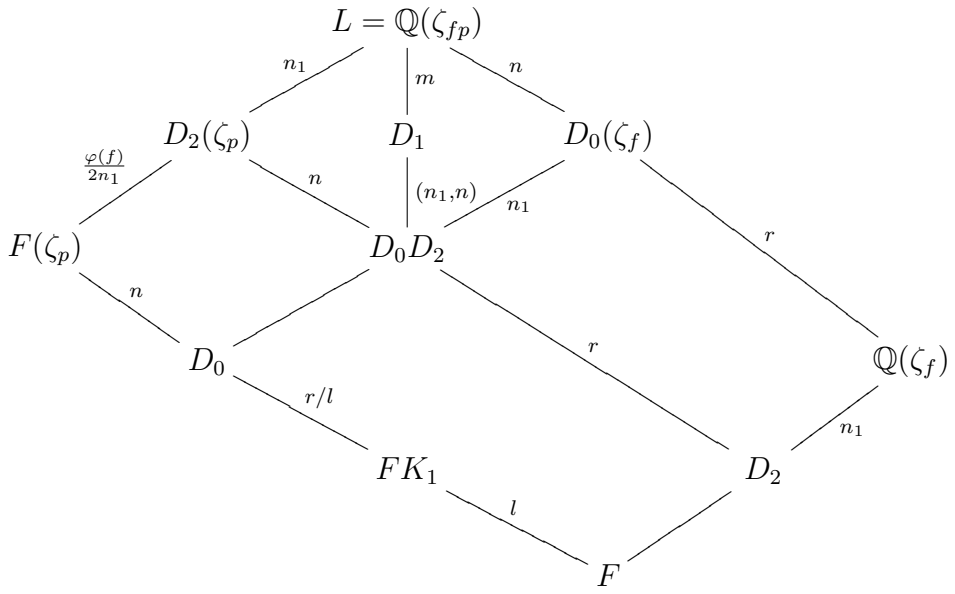
Again we do not pretend that this is very enlightening yet. The picture will become clearer in the next section.

§7. *Establishing the connection with a Gauss sum*

In this section we shall assume Assumption A: $s = 2$ and $q = p_2$ is an l-th power modulo $p = p_1$. Let n be the order of q modulo p. Assumption A is equivalent to $l \mid r := \frac{p-1}{n}$. Let σ_q be the Frobenius of q in $L = \mathbb{Q}(\zeta_{fp})$.

Let $D_0 \subseteq F(\zeta_p)$ be the decomposition subfield of q, i.e. $\mathrm{Gal}(F(\zeta_p)/D_0) = \langle \sigma_q|_{F(\zeta_p)}\rangle$. Assumption A gives $FK_1 \subseteq D_0$. From this point onwards it seems necessary to fix a generator $\tilde{\sigma}$ of the group $\mathrm{Gal}(F(\zeta_p)/F)$ and we shall do it in such a way that $\sigma_q|_{F(\zeta_p)} = \tilde{\sigma}^r$. Then the restriction σ_0 of $\tilde{\sigma}$ to K_1 is a generator of G_1, and this choice of generator induces identifications $\lg G_1 \cong \mathbb{Z}/l\mathbb{Z}$ and $\lg G_1 \otimes \lg G_2 \cong \lg G_2$, which we will both denote by ι'. The lg symbol will sometimes be omitted again (switching back to multiplicative notation when

possible), and G_2 will then be identified with $(\mathbb{Z}/q\mathbb{Z})^\times$ modulo l-th powers, often tacitly.



Let n_1 be the order of q modulo f and let $D_2 \subseteq \mathbb{Q}(\zeta_f)$ be the decomposition subfield of q. Let m be the order of q modulo fp, and let $D_1 \subseteq L$ be the decomposition subfield of q. So $D_0D_2 \subseteq D_1$ and m is the least common multiple of n and n_1. Then $[D_1 : D_0] = u := \frac{\varphi(f)n}{2m}$. The prime q is totally split in D_1 and we fix a prime $\mathfrak{q}_1$ above q in D_1. Since $\mathfrak{q}_1$ stays inert in L/D_1, we can view $\mathfrak{q}_1$ also as a prime in L. Let ψ be the additive character on $\mathbb{Z}/q\mathbb{Z}$ sending $\bar{1}$ to ζ_q, where the q-th primitive root of unity is chosen once and for all. Let $\rho = \omega^{(q^m-1)/(fp)}$ where $\omega : \mathbb{F}_{q^m}^\times \to \mu_{q^m-1}$ is the Teichmüller character attached to a prime in $L(\zeta_{q^m-1}) = \mathbb{Q}(\zeta_{q^m-1})$ above $\mathfrak{q}_1$. All we need to know is that the values of ρ belong to L and that $\rho(x \bmod \mathfrak{q}_1) \equiv x^{(q^m-1)/(fp)} \pmod{\mathfrak{q}_1}$ for all $x \in \mathcal{O}_L$. We shall also need the conjugate characters $\rho_v(x) = \rho(x)^v$ for v running $\bmod^\times fp$. Let $g(\rho_v) = g(\rho_v, \psi \circ \mathrm{Tr}) \in L(\zeta_q)$ be the resulting Gauss sums (see e.g. [8] p. 56). According to [12] (p. 97, Lemmas 6.4 and 6.5), $g(\rho_v) \in D_1(\zeta_q)$ and $g(\rho_v)^{fp} \in D_1$.

For any integer t relatively prime to f let $\nu_t \in \mathrm{Gal}(L/\mathbb{Q}(\zeta_p))$ be determined by $\nu_t(\zeta_f) = \zeta_f^t$. Then $\mathrm{Gal}(L/F(\zeta_p)) = \{\nu_t \mid t \bmod^\times f,\ \chi(t) = 1\}$ and $\mathrm{Gal}(L/D_1(\zeta_p)) = \{\nu_{q^{ni}} \mid i = 1, \ldots, \frac{m}{n}\}$. Let us choose and fix a system of integers $v_1, \ldots, v_u$ all congruent to 1 modulo p such that

$$\mathrm{Gal}(D_1(\zeta_p)/F(\zeta_p)) = \{\nu_{v_i}|_{D_1(\zeta_p)} \mid i = 1, \ldots, u\}.$$

As $D_1 \cap F(\zeta_p) = D_0$, we have $\mathrm{Gal}(D_1/D_0) \cong \mathrm{Gal}(D_1(\zeta_p)/F(\zeta_p))$ via restric-

tion. A key role in the forthcoming Theorem 7.1 is played by

$$g = \mathrm{N}_{D_1(\zeta_q)/D_0(\zeta_q)}(g(\rho)) = \prod_{i=1}^{u} g(\rho_{v_i}).$$

The choice of ψ we made entails the choice of a solution $\pi \in \mathbb{Q}_q(\zeta_q)$ of the equation $\pi^{q-1} = -q$, as in [8] p. 71. We may and will identify the local field $\mathbb{Q}_q(\zeta_q)$ with $(D_1)_{\mathfrak{q}_1}(\zeta_q)$. Let $T : \mathbb{Q}_q(\zeta_q)^\times \to \mathcal{O}^\times_{\mathbb{Q}_q(\zeta_q)}$ be the "leading term homomorphism" given by $T(x) = x \cdot \pi^{-val_\pi(x)}$. Let $a \equiv_l b \in X$ mean that a/b is an l-th power in the multiplicative abelian group X. Often X will be clear from the context and not be mentioned.

We finally define, considering $\tilde{\sigma}$ as an element of $\mathrm{Gal}(D_0(\zeta_q)/F(\zeta_q))$ in the obvious way (i.e. $\zeta_q^{\tilde{\sigma}} = \zeta_q$):

$$\Delta = \sum_{i=0}^{r-1} i\tilde{\sigma}^i \in \mathbb{Z}[\mathrm{Gal}(D_0(\zeta_q)/F(\zeta_q))].$$

(Note: This type of element is frequently used in the theory of Euler systems and points to an impending application of Hilbert's Theorem 90.) Our next goal is the following result.

Theorem 7.1. *Under Assumption A, if the residue map $\mathcal{O}_{\mathbb{Q}_q(\zeta_q)} \to \mathbb{Z}/q\mathbb{Z}$ is written by an overbar, then*

$$\iota'(R_{1,2}) \equiv_l \overline{T(g^{-\Delta})} \in (\mathbb{Z}/q\mathbb{Z})^\times.$$

Proof: In order to prove this we need the Gross-Koblitz formula, see p. 82 in [8]. Let us point out right away that our q (which is a prime!) and q^m correspond to p and q in loc.cit.

The Gross-Koblitz formula states the following equality in $\mathbb{Q}_q(\zeta_q)$, where S means the sum of q-adic digits:

$$g(\rho_v) = \pi^{(q-1)m - S(\langle \frac{v}{fp} \rangle (q^m-1))} \cdot \prod_{i=0}^{m-1} \Gamma_q\big(1 - \big\langle \tfrac{q^i v}{fp} \big\rangle\big)$$

and so by means of the functional equation

$$T(g(\rho_v)) = \pm \prod_{i=0}^{m-1} \Gamma_q\big(\big\langle \tfrac{q^i v}{fp} \big\rangle\big)^{-1}. \tag{9}$$

Let $h \equiv 1 \pmod f$ be such that $\tilde{\sigma}(\zeta_p) = \zeta_p^h$ (so h is a primitive root modulo p and $h^r \equiv q \pmod p$). Let $v(a)$ be the smallest positive residue of

a modulo fp. We now look at $\iota'(R_{1,2})$ in $\lg G_2$. From Theorem 6.1 we have, replacing a by $v(h^i t)$ and noting that $\iota'(\sigma_{h^i t}) = i$:

$$\iota'(R_{1,2}) = \sum_{\substack{t \bmod^\times fp \\ \chi(t)=1,\, t\equiv 1 \pmod p}} \sum_{i=0}^{p-2} i \cdot \lg \tau_{\gamma(v(h^i t))},$$

where $\gamma(v) = \Gamma_q\big(\frac{v}{fp}\big)$ from §6. If we identify G_2 with $(\mathbb{Z}/q\mathbb{Z})^\times/l$ and revert to multiplicative notation, this gives

$$\iota'(R_{1,2}) \equiv_l \prod_{\substack{t \bmod^\times fp \\ \chi(t)=1,\, t\equiv 1 \pmod p}} \overline{\prod_{i=0}^{p-2} \Gamma_q\big(\big\langle \tfrac{h^i t}{fp} \big\rangle\big)^i} \in (\mathbb{Z}/q\mathbb{Z})^\times.$$

We now calculate the right hand side of Theorem 7.1 using (9)

$$\begin{aligned}
T\big(g^{-\Delta}\big) &= \prod_{i=1}^{u}\prod_{j=0}^{r-1} T(g(\rho_{v_i h^j}))^{-j} \\
&= \pm \prod_{i=1}^{u}\prod_{j=0}^{r-1}\prod_{a=0}^{n-1}\prod_{b=0}^{m/n-1} \Gamma_q\big(\big\langle \tfrac{q^{bn+a} v_i h^j}{fp} \big\rangle\big)^j \\
&= \pm \prod_{\substack{t \bmod^\times fp \\ \chi(t)=1,\, t\equiv 1 \pmod p}} \prod_{j=0}^{r-1}\prod_{a=0}^{n-1} \Gamma_q\big(\big\langle \tfrac{q^a h^j t}{fp} \big\rangle\big)^j \\
&= \pm \prod_{\substack{t \bmod^\times fp \\ \chi(t)=1,\, t\equiv 1 \pmod p}} \prod_{j=0}^{r-1}\prod_{a=0}^{n-1} \Gamma_q\big(\big\langle \tfrac{h^{ra+j} t}{fp} \big\rangle\big)^j
\end{aligned}$$

We have $l \mid r$ and $-1 \equiv_l 1$, so if we put $k = ra + j$ and note that then $k \equiv j$ modulo l, we obtain

$$\overline{T\big(g^{-\Delta}\big)} \equiv_l \overline{\prod_{\substack{t \bmod^\times fp \\ \chi(t)=1,\, t\equiv 1 \pmod p}} \prod_{k=0}^{p-2} \Gamma_q\big(\big\langle \tfrac{h^k t}{fp} \big\rangle\big)^k} \in (\mathbb{Z}/q\mathbb{Z})^\times,$$

and the theorem follows.

§8. *The final calculation*

In this section we assemble our earlier results and prove the formula given in Corollary 5.5 by an application of Hilbert's Theorem 90. We assume Assumption A and we keep all the notations like L, D_0, D_1, g, Δ from the preceding section. As in §3 we impose that $l \nmid f$, which is slightly stronger than the blanket assumption $l \nmid w_F$.

The main technical task is to describe the element $y := g^{-2fpw_F\Delta} \in D_0$ as explicitly as possible. Actually we will work with the slightly modified element $y_1 = g^{-fpw_F(1-\tau)\Delta} \in D_0$.

Lemma 8.1. $T(y_1) = T(y)$.

Proof: From the well-known fact $g(\rho)^{1+\tau} = q^m$ we deduce that $g^{1+\tau} = q^{mu}$ and that

$$y_1/y = (g^{-1+\tau}/g^{-2})^{fpw_F\Delta} = (q^{mu})^{fpw_F\Delta} = (-q)^{mufpw_F\Delta}.$$

The lemma follows from $-q = \pi^{q-1}$. QED

We will show that y_1 can be written as an l-th power times an element y_2 of F, and we will determine the prime factorisation of the ideal (y_2), which will turn out to be (modulo the lth power of an ideal of F) an ideal supported only on prime ideals dividing p and q. Now for the details.

We have mentioned that $g(\rho)^{fp}$ lies in D_1 and by Stickelberger's theorem the principal ideal $\big(g(\rho)^{fp}\big)$ has the following prime factorisation in L (or in D_1):

$$\big(g(\rho)^{fp}\big) = \mathfrak{q}_1^{fp(\nu - \Theta(L/\mathbb{Q}))},$$

where ν is the norm element of $\mathrm{Gal}(L/\mathbb{Q})$ and $fp\,\Theta(L/\mathbb{Q}) = \sum_{a \bmod^\times fp} a\sigma_a^{-1}$; σ_a being the automorphim of L sending each root of unity to its a-th power. (The reason for the minus sign in the exponent and the presence of ν is that in [12], where the exponent is simply $fp\,\Theta(L/\mathbb{Q})$, one takes negative powers of the Teichmüller character, and we take positive powers. Alternatively, consult the Gross-Koblitz formula in [8].)

Therefore

$$\big(g(\rho)^{fp(1-\tau)}\big) = \mathfrak{q}_1^{-2fp(1-\tau)\tilde{\Theta}_{D_1}},$$

with

$$\tilde{\Theta}_{D_1} = \sum_{\substack{a \bmod^\times fp \\ \chi(a)=1}} \left(\tfrac{a}{fp} - \tfrac{1}{2}\right) (\sigma_a|_{D_1})^{-1} \in \mathbb{Q}[\mathrm{Gal}(D_1/F)].$$

Let $\mathfrak{q}_0$ be the prime in D_0 below $\mathfrak{q}_1$. As $g^{fp} = \mathrm{N}_{D_1/D_0}(g(\rho)^{fp})$, the previous decomposition gives

$$\left(g^{fp(1-\tau)}\right) = \mathfrak{q}_0^{-2fp(1-\tau)\tilde{\Theta}_{D_0}}, \tag{10}$$

with

$$\tilde{\Theta}_{D_0} = \mathrm{res}_{D_1/D_0}\,\tilde{\Theta}_{D_1} = \sum_{\substack{a \bmod^{\times} fp \\ \chi(a)=1}} \left(\tfrac{a}{fp} - \tfrac{1}{2}\right)(\sigma_a|_{D_0})^{-1} \in \mathbb{Q}[\mathrm{Gal}(D_0/F)].$$

Then $\tilde{\Theta}_{D_0}$ is a preimage in $\mathbb{Q}[\mathrm{Gal}(D_0/F)]$ of $\tilde{\Theta}_{FK_1} \in \mathbb{Q}[\mathrm{Gal}(FK_1/F)]$, which was introduced in §1. We can easily check that $\tilde{\Theta}_{D_0}$ is divisible by $\tilde{\sigma} - 1$, and we can write

$$2fp\,\tilde{\Theta}_{D_0} \equiv i_1 \cdot (\tilde{\sigma} - 1) \pmod{(\tilde{\sigma} - 1)^2}$$

in $\mathbb{Z}[\mathrm{Gal}(D_0/F)]$. This implies that

$$2fp\,\tilde{\Theta}_{FK_1} \equiv i_1 \cdot (\sigma_0 - 1) \equiv \sigma_0^{i_1} - 1 \pmod{(\sigma_0 - 1)^2}.$$

Thus $\iota(2fp\,\tilde{\Theta}_{FK_1}) = \sigma_0^{i_1}$ (recall ι is the canonical isomorphism $I_{G_1}/I_{G_1}^2 \to G_1$), and hence

$$\iota'\iota(2fp\,\tilde{\Theta}_{FK_1}) = i_1 \in \mathbb{Z}/l\mathbb{Z}. \tag{11}$$

Thus, up to identifications and multiplying by $2fp$, i_1 is the "leading term" of the minus Stickelberger element attached to FK_1.

The following simple fact is well-known and easily checked.

Lemma 8.2. *$(\tilde{\sigma} - 1)\Delta = r - \mathrm{N}_{\tilde{\sigma}} \in \mathbb{Z}[\mathrm{Gal}(D_0/F)]$, where $\mathrm{N}_{\tilde{\sigma}} = \sum_{i=0}^{r-1} \tilde{\sigma}^i$.*

From formula (10) and the fact that the exponent to which $\mathfrak{q}_0$ is raised is divisible by $\tilde{\sigma} - 1$, we see that $\mathrm{N}_{\tilde{\sigma}}(g^{fp(1-\tau)})$ is a unit of F, that is, a w_F-th root of unity. From this and Hilbert's Theorem 90 applied to $g^{fpw_F(1-\tau)}$ we obtain:

Proposition 8.3. *There exists z_0 in $D_0^{\times}$ such that $z_0^{\tilde{\sigma}-1} = g^{fpw_F(1-\tau)}$.*

Our aim is to compute $\iota'(R_{1,2})$. Theorem 7.1 and Lemma 8.1 give

$$\iota'(R_{1,2})^{2fpw_F} \equiv_l \overline{T(y_1)} \in (\mathbb{Z}/q\mathbb{Z})^{\times}.$$

From Proposition 8.3 and Lemma 8.2 we get:

$$y_1 = g^{-fpw_F(1-\tau)\Delta} = \left(z_0^{\tilde{\sigma}-1}\right)^{-\Delta} = z_0^{\mathrm{N}_{\tilde{\sigma}} - r}$$

and $l|r$ gives $\overline{T(y_1)} \equiv_l \overline{T(z_0^{\mathrm{N}_{\tilde{\sigma}}})} \in (\mathbb{Z}/q\mathbb{Z})^\times$. We have proved

Corollary 8.4. *Let $y_2 = z_0^{\mathrm{N}_{\tilde{\sigma}}} = \mathrm{N}_{D_0/F}(z_0) \in F^\times$. Then we have*

$$\iota'(R_{1,2})^{2fpw_F} \equiv_l \overline{T(y_2)} \in (\mathbb{Z}/q\mathbb{Z})^\times.$$

To obtain $\overline{T(y_2)}$ we now have a look at the prime factorisation of (y_2). It is easily seen from (10) that the principal ideal (z_0) is the product of the lift of an ideal in F and of an ideal in D_0 supported only on prime ideals above p and q. Therefore the principal ideal $(y_2) = (\mathrm{N}_{D_0/F}(z_0))$ is equal (up to l-th powers of ideals in F) to an ideal in F supported only on prime ideals above p and q.

It is possible to write $2fp(1-\tau)\tilde{\Theta}_{D_0} = (1-\tau)(\tilde{\sigma}-1)(i_1+\beta)$ with $\beta \in (\tilde{\sigma}-1)\mathbb{Z}[\mathrm{Gal}(D_0/F)]$. If the above-$q$-part of the principal ideal (z_0) is written $\mathfrak{q}_0^\delta$ with some $\delta \in \mathbb{Z}[\mathrm{Gal}(D_0/\mathbb{Q})]$ then we must have $(\tilde{\sigma}-1)\delta = -2fpw_F(1-\tau)\tilde{\Theta}_{D_0}$, and this implies

$$\delta \equiv -w_F(1-\tau)(i_1+\beta) \pmod{\mathrm{N}_{\tilde{\sigma}}\,\mathbb{Z}[\langle\tau\rangle]}$$

and so

$$\delta\,\mathrm{N}_{\tilde{\sigma}} \equiv -w_F(1-\tau)i_1\,\mathrm{N}_{\tilde{\sigma}} \pmod{l\,\mathrm{N}_{\tilde{\sigma}}\,\mathbb{Z}[\langle\tau\rangle]}.$$

Let $\mathfrak{p}_2$ be the ideal of F below $\mathfrak{q}_0$. (The notation $\mathfrak{p}_2$ is consistent with the notation in the statement of the Minus Conjecture in §1; recall q is just another name for p_2.) Then the above-q-part of (y_2) is (letting $\equiv_l$ likewise denote equality of ideals up to l-th powers of ideals in F):

$$(y_2)_q \equiv_l \mathfrak{p}_2^{-w_F(1-\tau)i_1}. \tag{12}$$

We shall now concentrate on the above-p-part of the ideal (y_2) modulo l-th powers. The following result is well-known to experts.

Lemma 8.5. *Let the map $\kappa : \mathbb{Q}_p(\zeta_p)^\times \to (\mathbb{Z}/p\mathbb{Z})^\times$ be given by $\kappa(x) = \overline{x^{\tilde{\sigma}-1}}$. Then the kernel of κ is $\mathcal{O}^\times_{\mathbb{Q}_p(\zeta_p)} \cdot p^{\mathbb{Z}}$, and the following diagram commutes with $\tilde{\iota}(\tilde{\sigma}) = \bar{1}$, and the left hand vertical map induced by the valuation:*

$$\begin{array}{ccc}
\mathbb{Q}_p(\zeta_p)^\times & \xrightarrow{\kappa} & (\mathbb{Z}/p\mathbb{Z})^\times \\
\Big\downarrow{\scriptstyle \mathrm{val}} & & \Big\downarrow{\scriptstyle \cong} \\
\mathbb{Z}/(p-1)\mathbb{Z} & \xleftarrow{\tilde{\iota}} & \mathrm{Gal}(\mathbb{Q}_p(\zeta_p)/\mathbb{Q}_p)
\end{array}$$

PROOF: Recall that $\tilde{\sigma}$ corresponds to the primitive root h modulo p. We have $\kappa(\zeta_p - 1) = \overline{(\zeta_p - 1)^{\tilde{\sigma}-1}} = \overline{(\zeta_p^h - 1)/(\zeta_p - 1)} = \overline{\zeta_p^{h-1} + \cdots + \zeta_p + 1} = \bar{h}$, and $\mathrm{val}(\zeta_p - 1) = 1$, so the diagram does commute. The other claims of the lemma follow easily. QED

In order to get at the above-p-part of the principal ideal (z_0) we need another auxiliary result. Recall that $\rho = \omega^{(q^m-1)/(fp)}$, where $\omega : \mathbb{F}_{q^m}^\times \to \mu_{q^m-1}$ is the Teichmüller character attached to a prime $\mathfrak{Q}$ in $\mathbb{Q}(\zeta_{q^m-1})$ above $\mathfrak{q}_1$, and that n_1 is the order of q modulo f. Then $\overline{\omega} = \omega|_{\mathbb{F}_{q^{n_1}}^\times}$ is the Teichmüller character attached to the prime below $\mathfrak{Q}$ in $\mathbb{Q}(\zeta_{q^{n_1}-1})$. Let $\overline{\rho} = \overline{\omega}^{(q^{n_1}-1)/f}$ and let $g(\overline{\rho})$ be the Gauss sum (using the same additive character ψ as in the definition of $g(\rho)$). The relation between these two Gauss sums is described in the following lemma, where σ' is the automorphism of $\mathbb{Q}(\zeta_{fpq})$ determined by $\zeta_f^{\sigma'} = \zeta_f^p$ and $\zeta_{pq}^{\sigma'} = \zeta_{pq}$. Recall also the notation of §3: we have fixed $u_2 \in F$ such that the prime $\mathfrak{p}_2$ below $\mathfrak{Q}$ in F satisfies $\mathfrak{p}_2^{h_F/h_{F,\{p_2\}}} = (u_2)$.

Lemma 8.6. *(a)* $g(\rho)^{\sigma'} \equiv g(\overline{\rho})^{m/n_1}$ *modulo all primes dividing* p *in* $D_1(\zeta_q)$.

(b) $z_0^{\tilde{\sigma}-1} \equiv u_2^{(1-\tau)2nfph_{F,\{p_2\}}}$ *modulo all primes dividing* p *in* D_0.

PROOF: (a) As $\rho(x)^p = \overline{\rho}\big(\mathrm{N}_{\mathbb{F}_{q^m}/\mathbb{F}_{q^{n_1}}}(x)\big)$ for any $x \in \mathbb{F}_{q^m}^\times$, the Davenport-Hasse relation gives $g(\rho^p) = g(\overline{\rho})^{m/n_1}$ (e.g., see [12], Ex. 6.4, p. 111). Let us decompose $\rho = \varkappa_p\varkappa_f$ where the characters $\varkappa_p$, $\varkappa_f$ satisfy $\varkappa_p^p = \varkappa_f^f = 1$. Then $\rho^p(x) = \varkappa_f(x)^p = (\varkappa_f(x))^{\sigma'} \equiv (\rho(x))^{\sigma'} \pmod{\zeta_p - 1}$ and so $g(\rho^p) \equiv g(\rho)^{\sigma'} \pmod{\zeta_p - 1}$.

(b) We have $g(\rho)^{fp} \in D_1$ and $g(\overline{\rho})^f \in D_2$. It is easy to see that $[D_1 : D_0D_2] \cdot m = nn_1$. Thus (a) gives $\mathrm{N}_{D_1/D_0D_2}(g(\rho)^{fp})^{\sigma'} \equiv g(\overline{\rho})^{nfp}$ modulo all primes dividing p in D_0D_2. Therefore $g^{fp} = g^{fp\sigma'} \equiv \mathrm{N}_{D_2/F}(g(\overline{\rho})^f)^{np}$ modulo all primes dividing p in D_0. Stickelberger's theorem gives the factorization

$$(\mathrm{N}_{D_2/F}(g(\overline{\rho})^f)) = \mathfrak{p}_2^{f((1+\tau)\varphi(f)/2-\Theta_F)},$$

where $f\Theta_F = \big(\sum_{t \bmod^\times f,\, \chi(t)=1} t\big) + \big(\sum_{t \bmod^\times f,\, \chi(t)=-1} t\big)\tau$ and so $(1-\tau)f\Theta_F = (1-\tau)\sum_{t \bmod^\times f} t\chi(t) = -(1-\tau)2fh_F/w_F$. Hence

$$(\mathrm{N}_{D_2/F}(g(\overline{\rho})^f)^{(1-\tau)}) = \mathfrak{p}_2^{(1-\tau)2fh_F/w_F} = (u_2)^{(1-\tau)2fh_{F,\{p_2\}}/w_F},$$

so the two generators of these principal ideals are equal up to a unit in F, i.e. up to a w_F-th root of unity. We have obtained

$$\mathrm{N}_{D_2/F}(g(\overline{\rho})^f)^{w_F(1-\tau)} = u_2^{(1-\tau)2fh_{F,\{p_2\}}}.$$

Therefore, by Proposition 8.3

$$z_0^{\tilde{\sigma}-1} = g^{fpw_F(1-\tau)} \equiv \mathrm{N}_{D_2/F}(g(\overline{\rho})^f)^{npw_F(1-\tau)} = u_2^{(1-\tau)2nfph_{F,\{p_2\}}}$$

modulo all primes dividing p in D_0. QED

Let $\mathfrak{P}_1$ and $\mathfrak{P}_1'$ denote the primes of D_0 and $F(\zeta_p)$ above $\mathfrak{p}_1$, respectively. The extension $F(\zeta_p)/F$ is totally ramified at the primes above p and so

$$\mathrm{val}_{\mathfrak{p}_1}(y_2) = \mathrm{val}_{\mathfrak{p}_1}(\mathrm{N}_{D_0/F}(z_0)) = \mathrm{val}_{\mathfrak{P}_1}(z_0) = \tfrac{1}{n}\,\mathrm{val}_{\mathfrak{P}_1'}(z_0).$$

Lemma 8.5 gives

$$\mathrm{val}_{\mathfrak{p}_1}(y_2) \equiv \tfrac{1}{n}\tilde{\iota}\big(\overline{z_0^{\tilde{\sigma}-1}}\big) \pmod{\tfrac{p-1}{n}},$$

and using Lemma 8.6(b) we obtain

$$\mathrm{val}_{\mathfrak{p}_1}(y_2) \equiv \tfrac{1}{n}\tilde{\iota}\big(\big(\overline{u_2^{1-\tau}}\big)^{2nfph_{F,\{p_2\}}}\big) \equiv 2fph_{F,\{p_2\}}\tilde{\iota}\big(\overline{u_2^{1-\tau}}\big) \pmod{\tfrac{p-1}{n}}.$$

The definition of z_0 in Proposition 8.3 gives that $z_0^{(1+\tau)(\tilde{\sigma}-1)} = 1$ and so $z_0^{(1+\tau)} \in F$ which means $z_0^{(1+\tau)} \in \mathbb{Q}$; hence $y_2^{(1+\tau)} = (z_0^{(1+\tau)})^{(p-1)/n}$ is an l-th power of a rational number. Therefore the above-p-part of (y_2) is

$$(y_2)_p \equiv_l \mathfrak{p}_1^{2fph_{F,\{p_2\}}(1-\tau)\tilde{\iota}(\overline{u_2^{1-\tau}})}. \tag{13}$$

When writing $\tilde{\iota}(u)$ we tacitly identify $(\mathbb{Z}/p\mathbb{Z})^\times$ and $\mathrm{Gal}(F(\zeta_p)/F)$. Since we now work modulo l-th powers we actually can write $\iota'(u)$ as well (now identifying $(\mathbb{Z}/p\mathbb{Z})^\times/l$ and $\mathrm{Gal}(FK_1/F)$). Finally (12) and (13) give together the following factorization of the principal ideal (y_2) modulo l-th powers of ideals in F:

$$(y_2) \equiv_l \mathfrak{p}_1^{2fph_{F,\{p_2\}}(1-\tau)\iota'(\overline{u_2^{1-\tau}})} \cdot \mathfrak{p}_2^{-w_F(1-\tau)i_1}.$$

We shall use the notation t_1, t_2, t_3, t_1', t_2', and $\beta_{ij} = (u_i^{1-\tau}, (FK_j)_{\mathfrak{p}_j}/F_{\mathfrak{p}_j}) \in G_j$ introduced in §5. For example, $(u_2) = \mathfrak{p}_2^{t_2}$, hence $u_2^{1-\tau}$ is a unit in $F_{\mathfrak{p}_1}$ and the extension $(FK_1)_{\mathfrak{p}_1}/F_{\mathfrak{p}_1}$ is totally ramified, thus $\beta_{21}^{-1} = \overline{u_2^{1-\tau}}$. Now (11) and (MC) for $s = 1$ give

$$-w_F i_1 = \iota'\iota(-2fpw_F\,\tilde{\Theta}_{FK_1}) = \iota'\iota(2fph_{F,\{p_1\}}\,\mathrm{Reg}^-_{FK_1,S})$$

and using (4) we obtain

$$\begin{aligned} -w_F i_1 &= \iota'\iota(2fph_{F,S}(t_2(\beta_{11}-1) - t(\beta_{21}-1))) \\ &= 2fph_{F,S}(t_2\iota'(\beta_{11}) - t\iota'(\beta_{21})). \end{aligned}$$

Putting things together, we finally arrive at

$$\begin{aligned} (y_2) &\equiv_l \mathfrak{p}_1^{-2fph_{F,S}(1-\tau)t_2'\iota'(\beta_{21})} \cdot \mathfrak{p}_2^{2fph_{F,S}(1-\tau)(t_2\iota'(\beta_{11})-t\iota'(\beta_{21}))} \\ &\equiv_l (\mathfrak{p}_1^{t_2'}\mathfrak{p}_2^{t})^{-2fph_{F,S}(1-\tau)\iota'(\beta_{21})} \cdot (\mathfrak{p}_2^{t_2})^{2fph_{F,S}(1-\tau)\iota'(\beta_{11})} \\ &= (u_1^{1-\tau})^{-2fph_{F,S}\iota'(\beta_{21})} \cdot (u_2^{1-\tau})^{2fph_{F,S}\iota'(\beta_{11})}. \end{aligned}$$

Proposition 8.7. *If $l \nmid h_F$ then (taking lifts of $\iota'(\beta_{11})$ and $\iota'(\beta_{21})$)*

$$y_2 \equiv_l \left(u_1^{-(1-\tau)\iota'(\beta_{21})} \cdot u_2^{(1-\tau)\iota'(\beta_{11})}\right)^{2fph_{F,S}} \in F^\times.$$

PROOF: We know that there is an ideal I in F such that

$$(y_2) = I^l \cdot (u_1^{1-\tau})^{-2fph_{F,S}\iota'(\beta_{21})} \cdot (u_2^{1-\tau})^{2fph_{F,S}\iota'(\beta_{11})}.$$

Since $l \nmid h_F$ and I^l is principal, $I = (\alpha)$ is principal, too[1]. Then

$$y_2 \cdot \alpha^{-l} \cdot (u_1^{1-\tau})^{2fph_{F,S}\iota'(\beta_{21})} \cdot (u_2^{1-\tau})^{-2fph_{F,S}\iota'(\beta_{11})}$$

is a unit in F, so a w_F-th root of unity, which is an l-th power in F because $l \nmid w_F$. The proposition is proved. QED

Let us come back to the formula (5) (see Corollary 5.5), which we want to prove. When we apply ι' to it and switch to multiplicative notation, it takes the shape

$$\iota'(R_{1,2}) = \left(\beta_{22}^{\iota'(\beta_{11})} \cdot \beta_{12}^{-\iota'(\beta_{21})}\right)^{-h_{F,S}/w_F} \in (\mathbb{Z}/q\mathbb{Z})^\times/l = G_2. \qquad (14)$$

Now q is a norm in $(FK_2)_{\mathfrak{p}_2}/F_{\mathfrak{p}_2}$ and so

$$\beta_{22} = (u_2^{1-\tau}, (FK_2)_{\mathfrak{p}_2}/F_{\mathfrak{p}_2}) = (u_2^{1-\tau}q^{-t_2}, (FK_2)_{\mathfrak{p}_2}/F_{\mathfrak{p}_2}) \in G_2.$$

Moreover $(u_2) = \mathfrak{p}_2^{t_2}$, hence $u_2^{1-\tau}q^{-t_2}$ is a unit in $F_{\mathfrak{p}_2}$ and the extension $(FK_2)_{\mathfrak{p}_2}/F_{\mathfrak{p}_2}$ is totally ramified. Thus $\beta_{22} = \left(\overline{u_2^{1-\tau}q^{-t_2}}\right)^{-1}$. Recall that the "leading term homomorphism" T was defined as follows: take out the appropriate π-power from an element of $\mathbb{Q}_q(\zeta_q)$ to obtain a unit. As $\pi^{q-1} = -q$, in $\mathbb{Q}_q \cong F_{\mathfrak{p}_2}$ we are taking out a power of $-q$ to get a unit, so $\beta_{22} = \overline{\pm T(u_2^{1-\tau})^{-1}}$. Similarly we have

$$\begin{aligned}\beta_{12} &= (u_1^{1-\tau}, (FK_2)_{\mathfrak{p}_2}/F_{\mathfrak{p}_2}) = (u_1^{1-\tau}q^{-t}, (FK_2)_{\mathfrak{p}_2}/F_{\mathfrak{p}_2}) = \left(\overline{u_1^{1-\tau}q^{-t}}\right)^{-1} \\ &= \overline{\pm T(u_1^{1-\tau})^{-1}}.\end{aligned}$$

Therefore (14) is equivalent to

$$\iota'(R_{1,2}) = \left(\overline{T\left(u_2^{(1-\tau)\iota'(\beta_{11})} \cdot u_1^{-(1-\tau)\iota'(\beta_{21})}\right)}\right)^{h_{F,S}/w_F} \in (\mathbb{Z}/q\mathbb{Z})^\times/l = G_2.$$

Since $l \nmid 2fpw_F$, this equality follows from Proposition 8.7 and Corollary 8.4. We have proved

[1]This is the only point in §8 where we are using $l \nmid h_F$.

Theorem 8.8. *Suppose $s = 2$, K^+ is a genus field (that is, $K^+ = K_1K_2$), p_2 is an l-th power modulo p_1 and $l \nmid fh_F$. Then the Minus Conjecture (MC) is true for K.*

Remark: It follows immediately that Theorem 8.8 remains true if K^+ is any subfield of K_1K_2 with conductor p_1p_2, since the constructions of both the Stickelberger element and the minus reciprocity matrix are compatible, in an obvious sense, with a lowering of the top field, as long as the set of ramified primes does not get any smaller. (This compatibility with lowering of the base field is likewise true for Conjecture (B), but certainly less obvious, since one has to deal with the parameter φ.)

In conclusion, we obtain from Theorem 8.8, the previous remark, and Corollary 2.6:

Theorem 8.9. *Suppose $s = 2$, K^+ is cyclic (that is, a subfield of degree l of K_1K_2 different from K_1 and K_2), and $l \nmid fh_F$. Then (MC) holds for K.*

References:

[1] D. Burns, *Congruences between derivatives of abelian L-functions at $s = 0$,* preprint 2006, http://www.mth.kcl.ac.uk/staff/dj_burns/dburns-revised.ps

[2] S. Chaiken, D. J. Kleitman, *Matrix tree theorems*, J. Combinatorial Theory Ser. A **24** (1978), 377–381.

[3] H. Darmon, *Thaine's method for circular units and a conjecture of Gross*, Can. J. Math. **47** (1995), 302–317.

[4] C. Greither, R. Kučera, *The Minus Conjecture revisited*, preprint.

[5] B. Gross, *On the values of abelian L-functions at $s = 0$*, J. Fac. Sci. Univ. Tokyo, Sect. 1A, Math. **35** (1988), 177–197.

[6] A. Hayward, *A class number formula for higher derivatives of abelian L-functions*, Compositio Math. 140 (2004), 99–129.

[7] A. Hayward, *Congruences satisfied by Stark units,* Ph. D. Thesis, King's College London 2004.

[8] N. Koblitz, *p-adic Analysis: a Short Course on Recent Work*, LMS Lecture Note Series **46**, Cambridge University Press, 1980.

[9] R. Kučera, *On the Stickelberger ideal and circular units of a compositum of quadratic fields*, J. Number Theory **56** (1996), 139–166.

[10] W. Sinnott, *On the Stickelberger ideal and the circular units of an abelian*

field, Invent. math. **62** (1980), 181–234.

[11] J. Tate, *Les conjectures de Stark sur les fonctions L d'Artin en s = 0*, Notes d'un cours à Orsay rédigées par D. Bernardi et N. Schappacher, Birkhäuser-Verlag 1984.

[12] L. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics **83**, Springer, New York 1982.

Cornelius Greither
Institut für theoretische Informatik und Mathematik
Fakultät für Informatik
Universität der Bundeswehr München
85577 Neubiberg, Germany
cornelius.greither@unibw.de

Radan Kučera
Přírodovědecká fakulta
Masarykova univerzita
Janáčkovo nám. 2a
602 00 Brno, Czech Republic
kucera@math.muni.cz