The Minus Conjecture revisited

C. Greither and R. Kučera

Abstract

In an earlier paper we proved some results concerning Gross’s conjecture on tori. This conjecture, which we call the Minus Conjecture, is closely related to a conjecture of Burns, which is now known to hold generally in the absolutely abelian setting; however Burns’ conjecture does not directly imply the Minus Conjecture. The result proved in the earlier paper was concerned with imaginary absolutely abelian extensions $K/\mathbb{Q}$ of the form $K = FK^+$, with $F$ imaginary quadratic and $K^+ / \mathbb{Q}$ being tame, $l$-elementary and ramified at most at two primes. In the present paper we complement these results by proving the Minus Conjecture for extensions $K / \mathbb{Q}$ as above but without any restriction on the number $s$ of ramified primes. The price we have to pay for this generality is that our proof only works if the odd prime $l$ is large enough, more precisely if $l \geq 3(s + 1)$. There is one more restriction, namely $l \nmid h_F$. (A similar restriction was already needed in our previous paper.)

Introduction

There is a variety of interrelated conjectures in algebraic number theory, due to (and named after) Stark, Gross, and Rubin among others. A few years ago, two remarkable additions appeared. The first of these new conjectures was formulated by Burns in a preliminary version of [1] and incorporates both a conjecture of Gross and one of Rubin. The other new conjecture, which is the subject of the present paper, was formulated in work of Hayward [4]; we call it the Minus Conjecture (MC). Actually it already appeared in slightly different form in work of Gross [3], where it was called a “conjecture on tori”.

To keep this introduction short, we will not explain the history and the relations of all these conjectures but only give a rough idea what the Minus Conjecture says. We take a field $K$ of the form $K = FK^+$ where $F$ is imaginary quadratic and $K^+$ is a real abelian extension of $\mathbb{Q}$ with Galois group $G$. Hence complex conjugation acts on all arithmetical data attached to the complex field $K$. The Minus Conjecture postulates a congruence between two elements in $\mathbb{Z}[G]$ (one will see the formal similarity to other conjectures). One of them is the product of a class number factor by a
regulator. This regulator is associated to the group of “S-units of F in the minus part” for a suitable finite set S of prime numbers; a little more precisely it is a determinant of a matrix whose coefficients are of the shape $r_v(u) - 1$; here $r_v$ is a local Artin map, $v$ runs over a set of representatives of the split places of F above S modulo complex conjugation, and $u$ runs over a basis of the minus part of the S-unit group of F modulo roots of unity. The second element is, in very vague terms, an “L-value in the minus part”; more precisely it is a slightly adapted Stickelberger element attached to the field K. The conjecture postulates that these two elements are congruent modulo the $|S| + 1$st power of the augmentation ideal $I_G$, if all primes in $S$ split in F. Since in that case the regulator is visibly in $I_G^{[S]}$, the conjecture affirms in particular that the adapted Stickelberger element lies in the same power of $I_G$; it turns out that this is already a nontrivial statement.

In this paper (and also in the paper [2]) we only consider a fairly special class of fields $K^+$ for the sake of simplicity. To wit, we fix an odd prime number $l$; we assume that $K^+/\mathbb{Q}$ is $l$-elementary and tamely ramified. Hence $K^+$ is ramified exactly in $s$ primes $p_1, \ldots, p_s$, all of which are congruent to 1 modulo $l$. We also make the (not essential but practical) hypothesis that all these $p_i$ are split in F. Let $f$ and $h_F$ denote the conductor and the class number of F respectively. In the paper [2] we showed: (1) For $s = 1$ and $l \nmid f$, (MC) holds. (This is essentially a consequence of work of Hayward [5], but we gave an independent “elementary” proof.) (2) (MC) holds for $s = 2$ and $l \nmid fh_F$ under the following extra hypothesis: $K^+$ is cyclic; or $p_1$ is congruent to an $l$-th power modulo $p_2$. (See Theorems 8.8 and 8.9 in [2].) It is clear that $p_1$ and $p_2$ may also be exchanged in the last condition. The proof of (2) is quite involved, using complicated elementary lemmas and the Gross-Koblitz formula. Therefore it seems unlikely that the methods of [2] can be extended to $s \geq 3$ without unreasonable technical expense. However we succeeded in proving the weaker statement which says that the adapted Stickelberger element lies in $I_G^s$ fairly generally.

The purpose of the present paper is to prove (MC) (in the above setting) for all $s$ under rather weak assumptions by a different method. The most constraining of the assumptions we need to make is that the prime $l$ is not too small (for details see Theorem 3.7); in particular the main results of [2] are not fully recovered. The main idea is to deduce (MC) by a so-called “division argument” (for more of this we have to refer to §2 of [2]), which reduces it to a conjecture of Burns previously proved by Hayward in [4] and [5] (and recently much more generally by Burns himself in [1]). As pointed out in [2] already, the division argument frequently does not apply (roughly speaking because one would have to divide zero by zero). The main trick of
the present approach consists in enlarging the field $K$ in such a way that the division argument becomes applicable; we have to show that this is always possible, and that we may descend to $K$ again.

In §1 we give the precise formulation of the Minus Conjecture and also of Burns’ conjecture; and we recall some results and constructions from [2] which will be used. §2 is occupied by lemmas from linear and commutative algebra and a preparatory proposition based on Chebotarev’s Theorem. In §3 we prove our results on (MC), in particular the abovementioned main result Theorem 3.7.

**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. Both authors would like to thank the referee for several useful remarks.

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

The setup explained in this section can already be found in [2]; we only repeat it here for the readers’ convenience.

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 [4]) 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 $G = \text{Gal}(K/k)$ is $l$-elementary. Let $S$ be a nonempty finite set of finite places of $k$ including all places that ramify in $K/k$, and let $s$ denote the number of primes of $k$ that ramify in $K$.

We assume $s > 0$ throughout the paper. Since we are only interested in the rank 1 case, we further suppose that no place in $S$ splits completely in $K/k$. 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 [4] or [6]. 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 [4], 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 \( T \) has a simplifying effect. Moreover
we will assume that \( S \) is minimal, that is, \( S \) consists exactly of the primes
that ramify in \( K/k \).

There is a linear map

\[
\text{Reg}_{K/k,S} : \bigwedge_{\mathbb{Z}}^s U_S(k) \to I_G^{s-1}/I_G^s,
\]

\[
u_1 \wedge \ldots \wedge u_{s-1} \mapsto \det \left( r_v(u_i) - 1 \right)_{1 \leq i \leq s-1; v \in S^*}.
\]

Here \( r_v \) is the local reciprocity map \( x \mapsto (x, K_w/k_v) \in G_v \subset G \), (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 \( \varphi \in \text{Hom}_{\mathbb{Z}[G]}(X, \mathbb{Z}[G]) \), let \( \varphi^1 \in \text{Hom}_\mathbb{Z}(X^G, \mathbb{Z}) \) be defined by the property that \( \varphi(u) = \varphi^1(u) \cdot \sum_{\sigma \in G} \sigma \) for
all \( u \in X^G \). Then \( \varphi^1 \) canonically induces a linear map \( \bigwedge_{\mathbb{Z}}^s X^G \to \bigwedge_{\mathbb{Z}}^{s-1} X^G \)
which will again be written \( \varphi^1 \), 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 \( U_S(k)/(U_S(k))_{\text{tor}} \) and we define

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

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

There are two points to deal with before we state Burns’s conjecture.

The first is a mere technicality. Since we do not want to worry about
denominators, we will let \( I_G \) denote, from now on, the augmentation ideal
in \( \mathbb{Z}[G] \) (where \( \mathbb{Z}_l \) denotes the \( l \)-adic integers). The augmentation quotients
\( I_G^{s-1}/I_G^s \) for \( s \geq 2 \) remain the same under this adjustment, since \( G \) is \( l \)-
elementary. This permits denominators which are prime to \( l \).

The second is more subtle: fixing the sign of the regulator. 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 valuation at $v_i$. A basis $u_1, \ldots, u_s$ of $U_S(k)/U_S(k)_{tor}$ 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 $\varphi \in \text{Hom}_{\mathbb{Z}[G]}(U_S(K), \mathbb{Z}[G])$ one has

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

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

The prediction about the sign comes from [1] and is also explained in [5]. The above statement is formally a little different from the version in [5] and [1]; but as explained in §1 of [2], the statements are compatible with each other.

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 $G = \text{Gal}(K/F)$ may be identified with $\text{Gal}(K^+/\mathbb{Q})$. Let $\tau$ always stand for complex conjugation. Then both $\text{Gal}(K/K^+)$ and $\text{Gal}(F/\mathbb{Q})$ 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 $F$. Both parts of the following theorem are due to Hayward; precise references and some comments concerning the signs are given in [2], see the proofs of Theorems 1.1 and 1.2 in loc.cit.

**Theorem 1.1.** Under the above assumptions:

(a) Conjecture (B) is true for $K^+/\mathbb{Q}$ with $S = \{p_1, \ldots, p_s\}$ (the minimal possible choice of $S$).
(b) 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 $S$).

We now turn to the Minus Conjecture (MC). To state it, we have to introduce certain Stickelberger elements. Now we will also consider sets $S$ which are not minimal. More precisely: $S = \{p_1, \ldots, p_t\}$ with $t \geq s$, all $p_i$ split in $F$ and none of them is equal to $l$. Let $m_S$ stand for the product $p_1 \cdots p_t$; so $m_S$ is a multiple of the conductor $m$ of $K^+$.

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

$$\Theta_{K,S} = \frac{1}{fm_S} \sum_{a \mod \ast \setminus fm_S} \left( a - \frac{fm_S}{2} \right) \sigma_a^{-1} \in \mathbb{Q}[\text{Gal}(K/\mathbb{Q})].$$

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

$$\Theta_{K,S} = (1 - \tau) \tilde{\Theta}_{K,S}, \quad \tilde{\Theta}_{K,S} = \frac{1}{fm_S} \sum_{\sigma_a \mid p \, \ast \setminus 1} \left( a - \frac{fm_S}{2} \right) \sigma_a^{-1}.$$

Note that $\tilde{\Theta}_{K,S}$ is now in $\mathbb{Q}[\text{Gal}(K/F)]$.

We also need a regulator built from minus-units. For each $i \in \{1, \ldots, t\}$ pick a prime ideal $p_i$ above $p_i$ in $F$. Let $S'$ be the ordered set $(p_1, \ldots, p_t)$. The abelian group $\left( \frac{U_S(F)}{(U_S(F))_{tor}} \right)^{1-\tau}$ is free of rank $t$. We choose an ordered basis for it, $\left( u_i^{1-\tau}, \ldots, u_t^{1-\tau} \right)$ say. We again have a notion of well-orientedness as follows. For each $i$ we choose a positive power of $p_i$ which is principal and a generator $x_i$ of it. Then the family $x_1^{1-\tau}, \ldots, x_t^{1-\tau}$ is a $\mathbb{Q}$-basis of $\mathbb{Q} \otimes \left( \frac{U_S(F)}{(U_S(F))_{tor}} \right)^{1-\tau}$ (an analog of the “adapted systems” we used before), and we decree that $(u_1^{1-\tau}, \ldots, u_t^{1-\tau})$ is well-oriented with respect to the ordered set $S'$ if $x_1^{1-\tau}, \ldots, x_t^{1-\tau}$ can be obtained by a $\mathbb{Q}$-linear transformation with positive determinant from the ordered set $(u_1^{1-\tau}, \ldots, u_t^{1-\tau})$. All this simplifies a lot when $h_F = 1$. Then one takes $u_i$ to be a generator of $p_i$.

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

$$\text{Reg}_{K,S} = \det(r_w(u_i^{1-\tau}) - 1)_{1 \leq i \leq t, w \in S'} \in I_G^t/I_G^{t+1}.$$  

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 $K^+$, $S$ contains these ramified primes, and all the primes in $S$ are split in $F$ and distinct from $l$.

**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

$$\tilde{\Theta}_{K,S} \equiv -\frac{h_{F,S}}{w_F} \text{Reg}_{K,S}^- \pmod{I_G^{\lvert S \rvert+1}}.$$ 

We will call this the “Minus Conjecture” (MC) in the sequel. (Recall that we are assuming that $s > 0$; but notice that (MC) as stated makes sense for $s = 0$ (i.e. $K = F$) as well, and the resulting statement is true, as a direct consequence of the analytic class number formula for $F$.)

The following important consequence of (MC) is much easier to state, and was proved as Theorem 4.4 in [2]:

**Theorem 1.2.** Under the same assumptions as above on $K$ and if $S$ is minimal (i.e. $s = \lvert S \rvert$), the element $\tilde{\Theta}_K$ lies in the $s$-th power of the augmentation ideal $I_G$.

We next recall some constructions and one more result from [2] which will be needed in the sequel.

We look at the case that $K^+/\mathbb{Q}$ is cyclic (hence cyclic of order $l$). Let $\sigma$ 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 $\sigma_i$ of $G_i = \text{Gal}(K_i/\mathbb{Q})$ for each $i$, by the prescription that the extension of $\sigma_i$ by the identity map on the other $K_j$ restricts to $\sigma$ on $K_i$. We define an $s \times s$ matrix $A = (a_{ij})$ (let us call it the *reciprocity matrix attached to $K^+$*) 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 automorphism of $p_i$ in $K_j$. Let $A_i$ denote the $(i,i)$-minor of $A$ for $i = 1, \ldots, s$; note that $A$ and $A_i$ are only uniquely determined modulo $l$. The following result was shown as Theorem 2.5 in [2]:

**Theorem 1.3.** If $K^+/\mathbb{Q}$ is cyclic, $l$ does not divide $h_F$, $S$ is minimal, and at least one of the minors $A_1, \ldots, A_s$ is not zero modulo $l$, then the Minus Conjecture holds for $K/F$.

Very roughly speaking, this was obtained in [2] by dividing the statement in part (b) of Theorem 1.1 (see above) by the statement in part (a). Therefore one might call this result the “Division Theorem”.
§2. General lemmas

We begin with an easy result concerning square matrices over an arbitrary field $\mathbb{F}$. For this, we need an odd bit of terminology: An open $n \times n$-matrix $A$ over $\mathbb{F}$ is an array $(a_{ij})$ with entries in $\mathbb{F}$, where $i$ and $j$ run from 1 to $n$, but the diagonal entries $a_{ii}$ are undefined. Filling in an open matrix just means: giving values to the diagonal entries. There is one distinguished way of filling in an open matrix, namely the way dictated by the condition that all row sums of the full matrix become zero. This particular filling process will be called completing the matrix. This is undefined for $n = 1$, and for $n > 1$ it always results in a singular matrix. The following lemma is about filling in, not about completing.

**Lemma 2.1.** Every open $n \times n$-matrix $A$ over $\mathbb{F}$ can be filled in so as to make its determinant nonzero.

**Proof:** Let $a_{ij}$ denote the coefficients of $A$ ($i \neq j$), and put independent variables $x_1, \ldots, x_n$ in the diagonal positions. The determinant of the resulting matrix is a polynomial $f(x_1, \ldots, x_n) \in \mathbb{F}[x_1, \ldots, x_n]$. It is easy to see that

$$f(x_1, \ldots, x_n) = \sum_{I \subseteq \{1, \ldots, n\}} f_I \prod_{i \in I} x_i$$

for suitable $f_I \in \mathbb{F}$. We show that there exist $a_{11}, \ldots, a_{nn} \in \mathbb{F}$ such that $f(a_{11}, \ldots, a_{nn}) \neq 0$. We assume the contrary and show by induction over $|I|$ that $f_I = 0$. This will be a contradiction since $f_{\{1, \ldots, n\}} = 1$. Indeed, if $I = \emptyset$ then $f_I = f(0, \ldots, 0) = 0$. Now let $|I| = j > 0$ and assume that $f_J = 0$ for all $J \subseteq \{1, \ldots, n\}$ with $|J| < j$. Let $a_{ii} = 1$ for $i \in I$ and $a_{ii} = 0$ otherwise. Then $0 = f(a_{11}, \ldots, a_{nn}) = \sum_{I \subseteq \emptyset} f_I = f_I$. This proves our claim. QED

For the next lemma and the sequel, it is practical to denote the completion of an open matrix $A$ by $\bar{A}$. For any square matrix $C$, we denote by $C_1$ its uppermost principal minor, that is, the determinant of the matrix gotten from $C$ by omitting the last row and column. (Caution: in standard terminology that minor is written $C_{n,n}$ if $C$ has $n$ rows and columns.)

**Lemma 2.2.** Let $A$ be an open $n \times n$-matrix. Then $A$ can be enlarged by an $(n + 1)$st row and an $(n + 1)$st column to an open $(n + 1) \times (n + 1)$-matrix $B$ in such a way that the completion $\bar{B}$ has nonzero first principal minor $(\bar{B})_1$. Moreover the $(n + 1)$st row of $B$ can be chosen arbitrarily.

**Proof:** We write $a_{ij}$ for the coefficients of $A$ and also of $B$. By choosing $a_{i,n+1}$ appropriately, we may give any value whatsoever to the $(i, i)$-entry of the completion $\bar{B}$ of $B$, for $i = 1, \ldots, n$. By Lemma 2.1, there exists a choice
of diagonal entries $a_{ii}$ such that $(a_{ij})_{1 \leq i,j \leq n}$ has nonzero determinant. This proves the main statement of 2.2, and the new bottom row did not play any role. QED

Now we prove a very simple-minded bound on the number of points of hypersurfaces defined over a base field $\mathbb{F}$ which is now assumed to be finite, with $l$ elements. We will assume that $l$ is an odd prime, to conform with the rest of the paper (but the lemma would also work for prime powers $l$).

Lemma 2.3. Let $g \in \mathbb{F}[X_1, \ldots, X_n]$ be a nonzero polynomial of degree $d$ and $V_g$ the hypersurface defined by $g$. Then

$$|V_g(\mathbb{F})| \leq dl^{n-1}.$$  

(Note that for $n = 2, d = 3$ and not too small $l$ this is much weaker than the Hasse-Weil bound for elliptic curves; the reason is that we have to admit reducible hypersurfaces as well, and they tend to have more points than irreducible ones.)

Proof: The case $n = 1$ is clear, and so is the case $d = 0$ (where $f$ is a nonzero constant). We proceed by induction over $n + d$ and distinguish two cases:

1. For some $c \in \mathbb{F}$, $g$ is divisible by $X_n - c$, so $g = (X_n - c)h$ where $h$ has degree $d - 1$. Then $V_g(\mathbb{F}) \subset V_h(\mathbb{F}) \cup H_c$, where $H_c$ is the set of all vectors $x \in \mathbb{F}^n$ with last component $c$, so by induction we get our claim.

2. The complementary case: here for every $c \in \mathbb{F}$, the image $g_c$ of $g$ under the reduction map $X_n \mapsto c : \mathbb{F}[X_1, \ldots, X_n] \to \mathbb{F}[X_1, \ldots, X_{n-1}]$ is not the zero polynomial. Hence we may apply the induction hypothesis to every $g_c$. Thus there are at most $dl^{n-2}$ vectors $x \in \mathbb{F}^n$ with last component $c$ such that $g(x) = g_c(x_1, \ldots, x_{n-1}) = 0$; by summing over $c \in \mathbb{F}$, we again see the validity of our bound. QED

We now combine this with the process of completing open matrices.

Proposition 2.4. Let $\mathbb{F}$ be a field with $l$ elements, $A$ an open $n \times n$-matrix over $\mathbb{F}$ with $n > 1$, and suppose that $(\bar{A})_1 \neq 0$. (Notation explained before Lemma 2.2.) For any vector $\lambda = (\lambda_1, \ldots, \lambda_{n-1})$ we let $A(\lambda)$ be the matrix obtained from $A$ via multiplying the $j$-th column by $\lambda_j$, for $j = 1, \ldots, n-1$. (The last column is left unchanged intentionally.) Let

$$D = \{ \lambda \in (\mathbb{F} \setminus 0)^{n-1} \mid (A(\lambda))_1 \neq 0 \}.$$  

Then

$$|D| \geq (l-1)^{n-1} - (n-2)l^{n-2}.$$
\textbf{Proof:} By definition, \( D = (\mathbb{F} \setminus 0)^{n-1} \setminus V_{g}(\mathbb{F}) \), where \( g \) is the polynomial in \( \lambda_{1}, \ldots, \lambda_{n-1} \) given as the determinant of the following matrix:

\[
\begin{pmatrix}
-\lambda_{2}a_{12} - \cdots - \lambda_{n-1}a_{1,n-1} - a_{1n} & \lambda_{2}a_{12} & \lambda_{3}a_{13} & \cdots & \lambda_{n-1}a_{1,n-1} \\
\lambda_{1}a_{21} & -\lambda_{1}a_{21} - \lambda_{3}a_{23} - \cdots - a_{2,n} & \lambda_{3}a_{23} & \cdots & \lambda_{n-1}a_{2,n-1} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\lambda_{1}a_{n-1,1} & \lambda_{2}a_{n-1,2} & \lambda_{3}a_{n-1,3} & \cdots & \cdots
\end{pmatrix}
\]

Certainly \( g \) is a polynomial of total degree at most \( n - 1 \). However we can see that its degree is at most \( n - 2 \) as follows. The homogeneous part of degree \( n - 1 \) is obtained by deleting \( a_{1n}, \ldots, a_{n-1,n} \) wherever they occur. But when we do that, we get a matrix with all row sums equal to zero, that is: with determinant zero. Thus the homogeneous part of degree \( n - 1 \) is the zero polynomial.

The polynomial \( g \) is not zero itself since \( g(1, \ldots, 1) \neq 0 \) by hypothesis. From Lemma 2.3 we infer that \( V_{g}(\mathbb{F}) \) has at most \((n - 2)l^{n-2}\) elements; note that \( n - 1 \) in the present proof corresponds to \( n \) in 2.3. QED

We conclude this section with two more, rather unconnected, auxiliary results. The latter of them is a fairly standard application of the Čebotarev theorem, and the former is a presumably well-known statement about the augmentation filtration of a group ring. Recall that \( l \) is a fixed odd prime.

\textbf{Lemma 2.5.} Let \( G \) be elementary abelian of order \( l^{m} \) with fixed generators \( \sigma_{1}, \ldots, \sigma_{m} \). Let \( s_{i} = \sigma_{i} - 1 \in \mathbb{Z}[G], \mathbb{F} = \mathbb{Z}/l\mathbb{Z} \), and let \( R \) be the polynomial ring \( \mathbb{Z}[t_{1}, \ldots, t_{m}] \) in \( m \) indeterminates. The maximal ideal \( (t_{1}, \ldots, t_{m}) \) of \( R/lR = \mathbb{F}[t_{1}, \ldots, t_{m}] \) is denoted by \( M \). Then the ring homomorphism \( R \to \mathbb{Z}_{l}[G] \) given by \( t_{i} \mapsto s_{i} \) induces, for any positive integer \( n < l \), an isomorphism

\[
M^{n}/M^{n+1} \to I_{G}^{n}/I_{G}^{n+1}.
\]

\textbf{Proof:} Let overbar denote reduction modulo \( l \), so \( \bar{I}_{G} \) is the augmentation ideal (and the unique maximal ideal) in \( \mathbb{F}[G] \). As a first step one checks that \( U_{G} \subset \bar{I}_{G}^{l} \). (It is sufficient to show this for \( G \) cyclic, and in that case it can be checked by calculation.) Second step: As a consequence one has \( l\mathbb{Z}[G] \cap \bar{I}_{G}^{n} = U_{G} \cap \bar{I}_{G}^{n} = U_{G} \) for \( 0 < n \leq l \). From a diagram chase one then obtains isomorphisms \( I_{G}^{n}/I_{G}^{n+1} \cong \bar{I}_{G}^{n}/\bar{I}_{G}^{n+1} \) for \( 0 < n < l \). The prescription \( t_{i} \mapsto s_{i} \) yields a surjective ring homomorphism \( \varphi: R/lR = \mathbb{F}[t_{1}, \ldots, t_{m}] \to \mathbb{F}[G] \), which induces a surjection \( \varphi_{n}: M^{n}/M^{n+1} \to \bar{I}_{G}^{n}/\bar{I}_{G}^{n+1} \). The point is to see that the latter is bijective. Now \( \mathbb{F}[G] \cong \mathbb{F}[t_{1}, \ldots, t_{m}]/(t_{1}^{l}, \ldots, t_{m}^{l}) \), and \( \bar{I}_{G} \) is the maximal ideal of \( \mathbb{F}[G] \). The kernel of \( \varphi \) is contained in \( M^{l} \), as follows.
from the description of $F[G]$ just given. Therefore $\varphi_n$ is bijective as long as $n + 1 \leq l$. QED

Remark: The quotient $M^n/M^{n+1}$ can be identified with the $n$th symmetric power of the $F$-vectorspace with basis $t_1, \ldots, t_m$. This point of view will be useful at a later point.

Proposition 2.6. Let $p_1, \ldots, p_s$ be distinct primes congruent to 1 modulo $l$, and $K_i$ the degree $l$ field of conductor $p_i$ for $i = 1, \ldots, s$. We fix generators $\sigma_i$ of $\text{Gal}(K_i/Q)$. Suppose that $b_1, \ldots, b_s, c_1, \ldots, c_s \in \mathbb{Z}/l\mathbb{Z}$ are arbitrarily given, and let $F$ be any imaginary quadratic field. Then:

There exist infinitely many primes $q \equiv 1$ modulo $l$ which split in $F$ such that

(i) $(q, K_j/Q) = \sigma_j^{b_j}$ for $j = 1, \ldots, s$,

and there exists a generator $\tilde{\sigma}$ of $\text{Gal}(K(q)/Q)$ with

(ii) $(p_i, K(q)/Q) = \tilde{\sigma}^{c_i}$ for $i = 1, \ldots, s$.

Here $K(q)$ is the degree $l$ field of conductor $q$.

Proof: We only treat the case where at least one $c_i \neq 0$. The case where all $c_i = 0$ is similar and actually easier. We may of course assume $c_1 \neq 0$.

Since we can change $\tilde{\sigma}$ at the end, we may replace all $c_i$ by $c_i/c_1$, in other words we can assume $c_1 = 1$.

We need various fields:

$L_1 = \mathbb{Q}(\zeta_l)(p_1^{1/l})$,
$L' = \mathbb{Q}(\zeta_l)((p_2p_1^{-c_2})^{1/l}, \ldots, (p_sp_1^{-c_s})^{1/l})$,
$F$,
$K^+ = K_1 \cdots K_s$.

Condition (i) above can be equivalently expressed by prescribing the Frobenius automorphism of $q$ on $K^+$. We require that $q$ is split in $F$, that is, its Frobenius on $F$ is trivial.

Since $L_1$ and $L'$ are linearly disjoint over $\mathbb{Q}(\zeta_l)$, there is an automorphism $\eta$ of $L_1L'/\mathbb{Q}(\zeta_l)$ which is nontrivial on $L_1$ but trivial on $L'$. Consider any prime $q$ whose Frobenius on $L_1L'$ is conjugate to $\eta$. Then $q$ is not totally split in $L_1$, so $p_1$ is not an $l$-th power modulo $q$, so $\tilde{\sigma} = (p_1, K(q)/Q)$ generates $\text{Gal}(K(q)/Q)$. On the other hand, $p_ip_1^{-c_i}$ is an $l$-th power modulo $q$ since $q$ splits in $L'$. This implies $(p_i, K(q)/Q) = (p_1, K(q)/Q)^{c_i}$, which gives Condition (ii). To conclude the argument, one checks by the usual methods: $L_1L'$ and $K^+$ are linearly disjoint over $\mathbb{Q}$, and the intersection $F \cap (L_1L'K^+)$ is $\mathbb{Q}$ or $F$, the latter happening only when $F \subset \mathbb{Q}(\zeta_l)$. In the former case it
is immediately clear that the various conditions imposed on \( q \) can be realized (infinitely often) simultaneously, by the theorem of Čebotarev. In the latter case, the various conditions on \( q \) are still compatible, since the requirement concerning \( F \) is that \( q \) splits in \( F \), and from its behaviour in \( L_1L'K^+ \) we even know \( q \) to be totally split in \( \mathbb{Q}(\zeta_l) \).

§3. **Proof of the Minus Conjecture for large \( l \)**

The goal of this part is a proof of the Minus Conjecture, based on Theorem 1.3 (the “Division Theorem”). It will become clear that the argument does not work for all primes \( l \); there are always small exceptional primes which cannot be covered. We make the **blanket assumption** that \( l \) does not divide \( w_Fh_F \). But note that the hypothesis that \( l \) is not too small in our main result will force that \( l \nmid w_F \), so just the assumption \( l \nmid h_F \) has to be made there.

Recall that (MC) was formulated for sets \( S \) which are not necessarily minimal. This will now be very helpful, because it makes downward changes of fields easier.

For given \( K/F \) and \( S \), denote by \( \Delta(K/F, S) \) the difference of the two sides in the Minus Conjecture in the appropriate filtration quotient factor ring, that is:

\[
\Delta(K/F, S) = \tilde{\Theta}_{K,S} + \frac{h_{FS}}{w_F} \text{Reg}_{K,S} \in \mathbb{Z}[G]/I_{G}^{S+1},
\]

where \( G = \text{Gal}(K/F) \) is identified with \( \text{Gal}(K^+/\mathbb{Q}) \). We will prove shortly that \( \Delta(K/F, S) \) actually lies in the expected filtration quotient \( I_{G}^{S}/I_{G}^{S+1} \).

**Proposition 3.1.** If \( K' \) is a field between \( K \) and \( F \), and \( G' = \text{Gal}(K'/F) \), then the restriction map \( \pi : \mathbb{Z}[G] \to \mathbb{Z}[G'] \) takes \( \Delta(K/F, S) \) to \( \Delta(K'/F, S) \).

**Proof:** The restriction takes the minus regulator attached to \( K \) to the minus regulator attached to \( K' \), since the Artin symbol behaves well under the change from \( K \) to \( K' \). The basis of the minus-units, and the numerical factors on the right hand side of the Minus Conjecture do not even depend on \( K \). The term \( \tilde{\Theta}_{K,S} \) behaves correctly just as well. Note that it is quite important here to work with the same set \( S \) throughout. Even if \( S \) is minimal for \( K/F \), it may well be non-minimal for \( K'/F \). QED

We now discuss what happens when \( S \) is enlarged, tacitly assuming that \( S \) fits the hypotheses of the Minus Conjecture. This is well known from Hayward’s work and we only include it for convenience.
Proposition 3.2. Let \( p \neq l \) be a rational prime not in \( S \), split in \( F \). By the notation \( \{ p \} \cup S \) we also indicate that \( p \) comes first in the ordering of the union set, and the elements \( \{ p_1, \ldots, p_t \} \) of \( S \) are ordered as before. 

1. \( \Delta(K/F, \{ p \} \cup S) = ((p, K^+/\mathbb{Q}) - 1) \cdot \Delta(K/F, S) \).

2. Both summands of \( \Delta(K/F, S) \) (see the definition) lie in \( I_G^{[S]} / I_G^{[S] + 1} \).

3. The Minus Conjecture for \( S \) implies the Minus Conjecture for \( \{ p \} \cup S \), and the converse holds if \( l \geq |S| + 2 \) and the Frobenius \( (p, K^+/\mathbb{Q}) \) is not the identity.

Proof: We shall prove (1) and (2) together by induction over the size of \( S \).

First step: (2) holds for the minimal choice of \( S \), because visibly \( \text{Reg}_{K, S} \in I_G^{[S]} \), and \( \Theta_{K, S} \in I_G^{[S]} \) by Theorem 1.2.

Second step: Let us show that (2) for \( S \) implies (1) for \( S \) and \( p \), and (2) for \( \{ p \} \cup S \) instead of \( S \). Let \( p \) be a prime of \( F \) above \( p \); let \( S = \{ p_1, \ldots, p_t \} \), \( p_i \) a prime of \( F \) above \( p_i \), \( S' = \{ p_1, \ldots, p_t \} \), and let \( u_1^{1-\tau}, \ldots, u_t^{1-\tau} \) be an ordered well-oriented basis of \( (U_S(F)/\mathcal{U}_S(F)_{\text{tor}})^{1-\tau} \). Let \( a = h_{F,S}/h_{F,p}\cup S \). Then one can check that the quotient \( U_{p,\cup S}^{1-\tau}/U_S^{1-\tau} \) is free rank one, generated by an element \( u^{1-\tau} \) such that \( u \) is a \( \{ p \} \cup S \)-unit whose valuation is \( a \) at \( p \) and 0 at \( p' \). Then \( u^{1-\tau}, u_1^{1-\tau}, \ldots, u_t^{1-\tau} \) is well-oriented with respect to \( \{ p \} \cup S \), so we may use it for calculating the minus regulator \( \text{Reg}_{K, \{p\} \cup S} \).

Now \( p \) is unramified in \( K/F \), since \( S \) already contains all the places rami-

fied in \( K^+/\mathbb{Q} \). Therefore \( r_p(u_i^{1-\tau}) = 1 \) for \( i = 1, \ldots, s \), and the matrix whose determinant is \( \text{Reg}_{K, \{p\} \cup S} \) has vanishing first column with the exception of the top left entry, which is \( r_p(u^{1-\tau}) - 1 \). Again since \( p \) is unramified, this is simply the \( a \)-th power of the Frobenius of \( p \) in \( K/F \), and this Frobenius equals the Frobenius of \( p \) in \( K^+/\mathbb{Q} \) under our identification of \( \text{Gal}(K/F) \) with \( \text{Gal}(K^+/\mathbb{Q}) \). This gives the Euler factor \( (p, K^+/\mathbb{Q}) - 1 \), and the determinant of the matrix that remains after removal of the first row and column gives the minus regulator for the set \( S \). By an easy calculation we get that \( \Theta_{K, \{p\} \cup S} = (1 - (p, K^+/\mathbb{Q})^{-1}) \Theta_{K, S} \) (note the Euler factor is slightly different here), and (2) for \( S \cup \{ p \} \) is proved. Since the \( G \)-module \( I_G^{[S]} / I_G^{[S] + 1} \) has trivial \( G \)-action, multiplying by either of the two Euler factors has the same effect, and (1) follows as well. (It is no problem that we assumed in (1) that the new place is in the first position in the enlarged set: it is always possible to permute \( S \) and the basis of minus units simultaneously.)

(3) The first statement is an immediate consequence of (1); the other is a little more difficult to see.

Let \( c = |S| \). Lemma 2.5 gives that \( I_G^{c} / I_G^{c+1} \) is canonically isomorphic to \( M^c/M^{c+1} \), where \( M \) is the maximal ideal \( (t_1, \ldots, t_m) \) in \( (\mathbb{Z}/l\mathbb{Z})[t_1, \ldots, t_m] \).
and \( m \) is determined by \([K : F] = l^m\); the same holds with \( c \) replaced by \( c + 1 \) (note we are assuming \( c + 2 \leq l \)), or by 1. The product of a nonzero homogeneous linear polynomial and a nonzero homogeneous polynomial of degree \( c \) over any integral domain is nonzero homogeneous of degree \( c + 1 \). This shows that for every nonzero \( x \in M/M^2 \) the multiplication by \( x \) is an injection from \( M^c/M^{c+1} \) to \( M^{c+1}/M^{c+2} \). We conclude that for every \( \sigma \in G \) which is not the identity, multiplication by \( \sigma - 1 \) is an injective map from \( I^c_G/I^{c+1}_G \) to \( I^{c+1}_G/I^{c+2}_G \). Therefore property (3) follows from property (1). QED

As our next step, we have to take a closer look at the cyclic subfields of a given \( l \)-elementary genus field. We fix an integer \( n > 1 \) (which will later be put equal to \( s + 1 \)), and for all \( 1 \leq i \leq n \) we take \( K_i \) to be cyclic of degree \( l \) and conductor \( p_i \) (hence \( K_i \) is real). Here \( p_1, \ldots, p_n \) are distinct primes all congruent to 1 modulo \( l \). We also fix a generator \( \sigma_i \) of \( \text{Gal}(K_i/Q) \).

A vector \( \lambda = (\lambda_1, \ldots, \lambda_{n-1}, 1) \) with coefficients in the set \( \{1, \ldots, l-1\} \) will be called admissible. Note that the last entry \( \lambda_n \) of \( \lambda \) is 1 per design. For every admissible vector \( \lambda \) we consider the cyclic (degree \( l \)) subfield \( K^+(\lambda) \) of \( K_1 \cdots K_n \) defined as follows:

The Galois group \( G \) of \( K_1 \cdots K_n/Q \) is \( l \)-elementary of order \( l^n \) with generators \( \sigma_1, \ldots, \sigma_n \). Let \( \langle \sigma \rangle \) denote a group of order \( l \), and let \( \Gamma \) be the kernel of \( \pi : G \to \langle \sigma \rangle \), \( \pi(\sigma_i) = \sigma^{\lambda_i} \). Let \( K^+(\lambda) \) be the fixed field of \( \Gamma \).

Then (because no \( \lambda_i \) is zero) the cyclic field \( K^+(\lambda) \) is still ramified at all primes \( p_1, \ldots, p_n \). Let us resume the “reciprocity matrices” attached to cyclic fields as explained just before Theorem 1.3. For this we start with the \( n \times n \)-matrix \( A \) whose diagonal entries are undefined, and the other entries \( a_{ij} \) are given by the rule that the Frobenius of \( p_i \) on \( K_j \) is \( \sigma_i^{\lambda_j} \). (We called such matrices “open matrices” in §2.) The matrix \( A \) will be called the \textbf{basic matrix} attached to the \( s \)-tuple \( p_1, \ldots, p_s \). (Of course \( A \) depends implicitly on the choice of the \( \sigma_i \).

If \( A(\lambda) \) denotes the matrix obtained from \( A \) by multiplying the \( j \)-th column by \( \lambda_j \) (the \( n \)-th column remains unchanged), then \( A(\lambda) \) coincides, off the diagonal, with the reciprocity matrix attached to the cyclic field \( K^+(\lambda) \).

Note that \( \text{Gal}(K^+(\lambda)/Q) \) identifies with \( \langle \sigma \rangle \), and each \( \sigma_i \) maps to \( \sigma^{\lambda_i} \), so in the construction in the paragraph before Theorem 1.3 one has to adjust \( \sigma_i \) by an exponent \( 1/\lambda_i \). We can now formulate a key result, which shows how to test the Minus Conjecture on cyclic subfields.

**Theorem 3.3.** Let \( K^+ = K_1 \cdots K_n \) as above, \( K = K^+F \); we also assume that all \( p_i \) split in \( F \), and we let \( S = \{p_1, \ldots, p_n\} \). Assume that \( l > n \), and that there exist at least \( nl^{n-2} + 1 \) admissible vectors \( \lambda \) such that \( K^+(\lambda)F/F \)
and $S$ satisfy the Minus Conjecture. Then the Minus Conjecture holds for $K/F$ and $S$.

**Proof:** We write $G = \text{Gal}(K/F) = \langle \sigma_1, \ldots, \sigma_n \rangle$ as before. By Lemma 2.5 we may consider the element $\Delta(K/F, S) \in I^G_n/I^{n+1}_G$ as a homogeneous polynomial $h$ of degree $n$ in the indeterminates $t_1, \ldots, t_n$ over the field $F = \mathbb{Z}/l\mathbb{Z}$. In the same manner, $\Delta(K^+(\lambda)F/F, S) \in I^{n+1}_{(\sigma)}/I^{n+1}_{(\sigma)}$ can be regarded as a degree $n$ monomial in the variable $t$ (with $\sigma - 1$ corresponding to $t$). We recall that $M^n/M^{n+1}$ (see Lemma 2.5) is canonically isomorphic to $\text{Sym}^n_F(Ft_1 \oplus \cdots \oplus Ft_n)$. It is not hard to check that the following diagram commutes:

$$
\begin{array}{ccc}
I^G_n/I^{n+1}_G & \overset{\cong}{\to} & \text{Sym}^n_F(Ft_1 \oplus \cdots \oplus Ft_n) \\
\downarrow \pi & & \downarrow t_i \mapsto \lambda_i t \\
I^{n+1}_{(\sigma)}/I^{n+1}_{(\sigma)} & \overset{\cong}{\to} & \text{Sym}^n_F(Ft) = Ft^n.
\end{array}
$$

Therefore $\pi(\Delta(K/F, S)) = 0$ iff $h(\lambda_1, \ldots, \lambda_{n-1}, 1) = 0$. But by our assumption and Proposition 3.1, $\pi(\Delta(K/F, S)) = \Delta(K^+(\lambda)F/F, S) = 0$ for at least $n!^{n-2} + 1$ vectors $\lambda$; hence the polynomial $g = h(-, \ldots, -, 1)$ of degree at most $n$ has at least that number of zeros in $F^{n-1}$. By Lemma 2.3 this is only possible if $g$ is zero. Since $h$ is homogeneous of degree $n$, $h$ must be zero as well; this proves the theorem. QED

Next, we discuss situations where the hypothesis on the existence of many admissible $\lambda$’s in 3.3 is satisfied. Recall that the completion $\bar{A}$ of an open square matrix $A$ is obtained by assigning values to the diagonal so that all row sums of $\bar{A}$ are zero. Let now $\bar{A}$ denote the basic $n \times n$ matrix attached to $p_1, \ldots, p_n$ as explained before Theorem 3.3.

**Proposition 3.4.** (a) Assume the upper $(n-1) \times (n-1)$ minor of $\bar{A}$ (this was denoted $\bar{A}_{11}$) is not zero. Then there exist at least $(l-1)^{n-1} - (n-2)!^{n-2}$ admissible vectors $\lambda$ such that $(\bar{A}(\lambda))_1$ is again nonzero.

(b) For all $\lambda$ as in the last sentence, the Minus Conjecture holds for the cyclic extension $K^+(\lambda)F/F$.

**Proof:** (a) This is just a rephrasing of Proposition 2.4.

(b) Since $\bar{A}(\lambda)$ is the reciprocity matrix attached to $K^+(\lambda)$, the assertion follows from Theorem 1.3. QED

The next step is, naturally, to confront 3.3 and 3.4 and see what happens. This part of the argument is completely elementary.
Theorem 3.5. Let $K$ be as before. If the basic $n \times n$ matrix $A$ has nonvanishing minor $(A)_1$ as above, and if $l \geq 3n$, then the Minus Conjecture holds for $K/F$ and $S = \{p_1, \ldots, p_n\}$. (Actually the last condition may be weakened a little, see following Remarks.)

Proof: By looking at 3.3 and 3.4, we see that it is enough to establish the inequality

$$(l - 1)^{n-1} - (n - 2)l^{n-2} \geq n!^{n-2} + 1 \quad (*)$$

under the hypothesis $l \geq 3n$. Condition (*) is equivalent to the following inequality for which we let $m = n - 1$:

$$(l - 1)^m > 2ml^{m-1}.$$ 

Taking logarithms we get that this is tantamount to

$$\log \frac{l}{2m} > m \cdot \log \frac{l}{l - 1}.$$ 

This in turn is implied by the slightly stronger formula

$$\log \frac{l}{2m} > \frac{m}{l - 1},$$

which is easily seen to be true:

$$\log \frac{l}{2m} \geq \log \frac{3n}{2n - 2} > \log \frac{3}{2} > \frac{1}{3} \geq \frac{3n - 1}{3(l - 1)} > \frac{m}{l - 1}.$$ 

QED

Remarks: (a) For every given $n$, the least prime value $l(n)$ of $l$ making formula (*) hold can be easily found. Here are the first few pairs $(n, l(n))$, excluding the uninteresting case $n = 1$: $(2,5)$, $(3,7)$, $(4,11)$, $(5,13)$, $(6,17)$. Thus it appears that the bound $l \geq 3n$ might be tightened. This is indeed so:

(b) An analysis of the proof of 3.5 shows: (*) still holds if $m \leq (l - 1)/c$ with $c$ the unique solution of $\log 2 - \log c + c^{-1} = 0$ in the interval $[2,3]$. In other words: it suffices that

$$l \geq 2.843059872 (n - 1) + 1.$$ 

(c) By an extension of the argument which also permits that some $\lambda_i$ are zero (with the consequence that fewer primes ramify in the cyclic field $K^+(\lambda)$), one can show using Proposition 3.2 that Theorem 3.5 already holds
with \( n = 2 \) and \( l \geq 3 \), provided \( l \nmid f \). We indicate some details, resuming the notation of the proof of Theorem 3.3. Since \( n = 2 \), the polynomial \( h(\lambda_1, 1) \) is of degree at most two, and its nullity is equivalent to (MC) for \( K \). For \( \lambda_1 = 1 \) or 2, the reciprocity matrix attached to \( K^+(\lambda) \) has the same top right entry as \( A \), and this is nonzero by hypothesis. So (MC) holds for these two fields, and this means that \( h(1, 1) = h(2, 1) = 0 \). The point is now that we can find a third zero of \( h(-, 1) \), and this will force \( h \) to be zero. Indeed, we look at the subfield \( FK_2 \subset K \) and the restriction map \( \mathbb{Z}[\text{Gal}(K/F)] \rightarrow \mathbb{Z}[\text{Gal}(FK_2/F)] \). Under this map, \( h(t_1, t_2) \) is sent to \( h(0, t_2) \). Since we know that (MC) holds for \( FK_2/F \) and \( S \) by Theorem 3.9 of [2] and Proposition 3.2 (note that now \( S \) is no longer minimal!), we obtain that \( h(0, t_2) = 0 \) as claimed.

We may go a little further: The condition \((\bar{A})_1 \neq 0\) just says that the top right entry of the open \( 2 \times 2 \)-matrix \( A \) is nonzero. By symmetry, it suffices that \( A \) is not the zero matrix. If \( A \) is the zero matrix, then by definition \( p_2 \) is an \( l \)-th power modulo \( p_1 \). Since the Minus Conjecture was proved for \( s = 2 \) assuming exactly the latter condition and \( l \nmid h_F \) (see Theorem 8.8 in [2]), we now have established:

**Corollary 3.6.** The Minus Conjecture is true for \( s = 2 \), under no other assumptions than \( l \nmid h_F \).

We should point out that this corollary follows at once from what was said above in the case where \( K^+ = K_1K_2 \) is the full genus field; its validity for any cyclic extension \( K^+ \) of degree \( l \) which is ramified exactly in \( p_1 \) and \( p_2 \) is then a purely formal consequence, via descent to subfields (see Proposition 3.1). We also note that we have reproved Theorem 8.9 of [2]. A last comment: We will see that in case \( l \geq 5 \), the assumption \( l \nmid f h_F \) can be relaxed to \( l \nmid h_F \), see Remark (b) following Theorem 3.7.

The final result can now be proved. We repeat all hypotheses for clarity.

**Theorem 3.7.** Assume \( K^+ \) is tame and \( l \)-elementary over \( \mathbb{Q} \) such that the set of primes that ramify in \( K^+ \) is exactly \( S = \{p_1, \ldots, p_s\} \), and let \( K = FK^+ \); here \( F \) is an imaginary quadratic field where all \( p_1, \ldots, p_s \) split. Suppose moreover that \( l \geq 3(s+1) \) and \( l \nmid h_F \). Then the Minus Conjecture holds for \( K/F \) and \( S \).

**Proof:** Recall that \( K_i \) denotes the absolutely abelian field of degree \( l \) and conductor \( p_i \) for \( i = 1, \ldots, s \). Then \( \overline{K^+} = K_1 \cdots K_n \) is the genus field of \( K^+ \); in particular it contains \( K^+ \), and the set of primes that ramify is again \( S \). By Proposition 3.1, the validity of the Minus Conjecture for \( FK^+/F \) and \( S \) implies the validity of the Minus Conjecture for \( K/F \). We may and will therefore assume that \( K^+ = \overline{K^+} \) in the rest of the argument.
Let $A$ be the basic matrix attached to $p_1, \ldots, p_s$. This is an open $s \times s$-matrix. By Lemma 2.2 $A$ can be enlarged to an $(s + 1) \times (s + 1)$-open matrix $B$ in such a way that the first principal minor $(\bar{B})_1$ of the completed matrix $B$ is not zero. Moreover we can choose the bottom row in $B$ as we like. Let us write $a_{ij}$ for the coefficients of $B$; we take $a_{s+1,1} = 1$ and $a_{s+1,2} = \ldots = a_{s+1,s} = 0$.

By Proposition 2.6 there exists a new prime $p$, split in $F$, congruent to 1 mod $l$, plus a generator $\sigma$ of $\text{Gal}(K_{s+1}/\mathbb{Q})$ (with $K_{s+1}$ the degree $l$ field of conductor $p$), such that: the Frobenius of $p_i$ on $K_{s+1}$ is $\sigma^{a_{si,s+1}}$ for $i = 1, \ldots, s$; the Frobenius of $p$ on $K_j$ is $\sigma_1$ for $j = 1$ and the identity map for $j = 2, \ldots, s$.

We write $p_{s+1}$ for $p$, $\sigma_{s+1}$ for $\sigma$. With these choices, $B$ is the basic matrix attached to the $s+1$-tuple $p_1, \ldots, p_s, p_{s+1}$. Let $\hat{K}^+ = K_1 \cdots K_s K_{s+1}$. From Theorem 3.5 (with $n = s+1$) and our hypothesis $l \geq 3(s+1)$ we infer that the Minus Conjecture is true for $\hat{K}^+ F/F$ and the (minimal) set $\hat{S} = S \cup \{p_{s+1}\}$.

Hence the conjecture also holds (according to Proposition 3.1) for $K/F$ and $\hat{S}$. We can reorder $\hat{S}$ (and the involved basis of minus-units) so as to get $p_{s+1}$ in the first place, without affecting the statement of the conjecture. By part (3) of Proposition 3.2, we now may deduce that the Minus Conjecture is already true for $S$, since the Frobenius of $p_{s+1}$ on $K^+$ is by construction exactly $\sigma_1$, in particular nontrivial. QED

Remarks: (a) Similarly as in the last Remarks, one can check that the condition $l \geq 3(s+1)$ can be weakened to $l \geq 2.843059872 s + 1$.

(b) We look at the case $s = 2$ and $l \geq 5$. It turns out that our method proves (MC) in this case as well. To wit: If the basic matrix $A$ has a nonzero entry, we are done by part (a) of the previous Remarks. So we suppose there are only zero entries in it. We use an extension field $\hat{K}^+$ with $s = 3$ exactly as in the proof of 3.7, and we want to show that the polynomial $h(t_1, t_2, 1)$, which has degree at most three, is the zero polynomial. We now explicitly specify the enlarged matrix $B = (a_{ij})_{1 \leq i, j \leq 3}$ by saying that $a_{1,3} = a_{2,3} = 1$. Then for all $\lambda_1, \lambda_2 \neq 0$ we have $\det(B(\lambda_1, \lambda_2, 1))_1 = 1$ (the minor happens to be independent of $\lambda_1, \lambda_2$). So $h(\lambda_1, \lambda_2, 1) = 0$ for all $\lambda_1, \lambda_2 \neq 0$, that is, $h$ has at least $(l-1)^2$ zeros. From Lemma 2.3 and $l \geq 5$ we conclude that $h$ is zero.

(c) The case $s = 2$ and $l = 3$ is not amenable to this method. In fact if we are in the case where the detour via $s = 3$ is necessary, there are at best nine cyclic cubic fields to test with, even if cyclic subfields of lower conductor are allowed; on the other hand there exist nonzero cubic polynomials in two variables which vanish everywhere on $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
References:


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