On the Zariski-density of integral points on a complement of hyperplanes in \( \mathbb{P}^n \)

Aaron Levin

*Department of Mathematics, Brown University, 151 Thayer street, Providence, RI, USA*

Received 8 November 2005; revised 12 December 2006

Available online 25 May 2007

Communicated by David Goss

**Abstract**

We study the \( S \)-integral points on the complement of a union of hyperplanes in projective space, where \( S \) is a finite set of places of a number field \( k \). In the classical case where \( S \) consists of the set of archimedean places of \( k \), we completely characterize, in terms of the hyperplanes and the field \( k \), when the \((S-)integral points are not Zariski-dense.

© 2007 Elsevier Inc. All rights reserved.

**1. Introduction**

Let \( k \) be a number field and \( S \) a finite set of places of \( k \) containing the archimedean places. Let \( Z \) be a closed subset of \( \mathbb{P}^n \), defined over \( k \), that is a finite union of hyperplanes over \( \bar{k} \). We study the problem of determining when there exists a Zariski-dense set \( R \) of \( S \)-integral points on \( \mathbb{P}^n \setminus Z \). We give a complete answer to this problem when \( O_{k,S} = O_{\bar{k}} \), i.e., when \( S = S_\infty \) consists of the set of archimedean places of \( k \). For arbitrary \( S \) the problem does not appear to have a simple answer, but in the last section we discuss some partial results and reformulations of the problem.

The related problem of determining when \( R \) must be a finite set was solved by Evertse and Győry [3] once \( k \) is sufficiently large (e.g., the hyperplanes are all defined over \( k \)). In the connected topic of solutions to norm form equations, Schmidt [6,7] has given necessary and sufficient conditions for finiteness. The general problem of determining the possible dimensions of \( R \), for any \( k \), \( S \), and \( Z \), seems to be difficult.
2. Definitions

Let $k$ be a number field and $S$ a finite set of places of $k$ containing the archimedean places. Let $\mathcal{O}_{k,S}$ denote the ring of $S$-integers of $k$.

**Definition 1.** If $Z$ is a subset of $\mathbb{P}^n$ defined over $k$, we call a set $R \subset \mathbb{P}^n \setminus Z(k)$ a set of $S$-integral points on $\mathbb{P}^n \setminus Z$ if for every regular function $f$ on $\mathbb{P}^n \setminus Z$ defined over $k$ there exists $a \in k^*$ such that $af(P) \in \mathcal{O}_{k,S}$ for all $P \in R$.

For example, let $Z$ be a hypersurface in $\mathbb{P}^n$ and let $U = \mathbb{P}^n \setminus Z$. Then $R$ is a set of $S$-integral points on $U$ if and only if there exists an embedding of $U$ into an affine space such that each point of $R$ has $S$-integral coordinates.

Recall that an archimedean place $v$ of $k$ corresponds to an embedding of $k$ into the complex numbers $\sigma: k \to \mathbb{C}$. We define $v$ to be real if $\sigma(k) \subset \mathbb{R}$ and define $v$ to be complex otherwise.

With this terminology we can define the following types of fields.

**Definition 2.** Let $k$ be a number field. Then

(a) We call $k$ a totally real field if all of its archimedean places are real.
(b) We call $k$ a totally imaginary field if all of its archimedean places are complex.
(c) We call $k$ a complex multiplication (CM) field if it is a totally imaginary field that is a quadratic extension of a totally real field.
(d) We say that an extension $M$ of $k$ contains a CM subfield over $k$ if there exists a CM field $L$ with maximal real subfield $L'$ (over $\mathbb{Q}$) such that $k \subset L' \subset L \subset M$.

Note that in our terminology, if $M$ is a CM field then $M$ does not contain a CM subfield over itself because of the condition on the maximal real subfield.

3. Main theorem

Our main theorem gives a complete characterization of when there exists a Zariski-dense set of $(S_\infty)$-integral points on a complement of hyperplanes.

**Theorem 3.** Let $Z \subset \mathbb{P}^n$ be a closed subset defined over $k$ that is a geometric finite union of hyperplanes, i.e., $Z = \bigcup_{i=1}^{m} H_i$ over $\overline{k}$ where the $H_i$ are distinct hyperplanes defined over $\overline{k}$. Let $L_i$ be a linear form defining $H_i$ over its minimal field of definition $M_i$ over $k$. Let $S = S_\infty$, the set of archimedean places of $k$. Then the following are equivalent:

1. There does not exist a Zariski-dense set of $S$-integral points on $\mathbb{P}^n \setminus Z$.
2. One of the following conditions holds:
   (a) The linear forms $L_1, \ldots, L_m$ are linearly dependent.
   (b) $\mathcal{O}_{k,S}^* = \mathcal{O}_k^*$ is finite and $Z$ has more than one irreducible component over $k$.
   (c) Some $M_i$ contains a CM subfield over $k$.

**Proof.** We first prove that (2) implies (1). Suppose that (a) holds. Without loss of generality, we can extend $k$ so that each $L_i$ is defined over $k$. It suffices to prove our assertion in the case that $\{L_1, \ldots, L_m\}$ is a minimal linearly dependent set, that is no proper subset is linearly dependent.
In that case \( \sum_{i=1}^{m-1} c_i L_i = c_m L_m \) for some choice of \( c_i \in k^* \), \( i = 1, \ldots, m \). Let \( R \) be a set of \( S \)-integral points on \( \mathbb{P}^m \setminus Z \). If \( i \in \{1, \ldots, m\} \), then all of the poles of \( L_i/L_m \) lie in \( Z \) and so there exists \( a \in k^* \) such that \( af \) takes on integral values on \( R \). Since the poles of \( L_m/L_i \) also lie in \( Z \), the same reasoning applies to \( L_m/L_i \). Therefore \( L_i/L_m(R) \) is contained in the union of finitely many cosets of the group of units \( \mathcal{O}^*_k \). By enlarging \( S \) we can assume without loss of generality that \( c_i L_i (P) \) is an \( S \)-unit for all \( P \in R \) and \( i = 1, \ldots, m \). We now apply the \( S \)-unit lemma \([2, \text{Theorem 1}]\).

**Lemma 4** (\( S \)-unit lemma). Let \( k \) be a number field and \( n \) a positive integer. Let \( \Gamma \) be a finitely generated subgroup of \( k^* \). Then all but finitely many solutions of the equation

\[
u_0 + u_1 + \cdots + u_n = 1, \quad u_i \in \Gamma,
\]
satisfy an equation of the form \( \sum_{i \in I} u_i = 0 \), where \( I \) is a proper subset of \( \{0, \ldots, n\} \).

We apply the lemma with \( \Gamma = \mathcal{O}^*_k \). Since \( \sum_{i=1}^{m-1} c_i L_i (P) = 1 \) for all \( P \in R \), by the \( S \)-unit lemma it follows that each \( P \in R \) either belongs to one of the hyperplanes defined by \( \sum_{i \in I} c_i L_i = 0 \) for some subset \( I \subset \{1, \ldots, m - 1\} \) (this equation is nontrivial by the minimality of the linear dependence relation) or it belongs to a hyperplane defined by \( c_i L_i = tc_m L_m \), for some \( t \in T \), where \( T \subset \mathcal{O}^*_k \) is a finite subset containing the elements that appear in the finite number of exceptional solutions to the \( S \)-unit equation \( \sum_{i=1}^{m-1} u_i = 1 \). Thus \( R \) is contained in a finite union of hyperplanes and, in particular, \( R \) is not Zariski-dense.

Suppose that (b) holds. Let \( R \) be a set of \( S \)-integral points on \( \mathbb{P}^m \setminus Z \). Let \( Z_1 \) and \( Z_2 \) be two distinct irreducible components of \( Z \) defined over \( k \), respectively, by homogeneous polynomials \( f \) and \( g \). Let \( h = f^{\deg g}/g^{\deg f} \). Since both \( h \) and \( 1/h \) are regular on \( \mathbb{P}^m \setminus Z \), by our earlier argument \( h(R) \) is contained in the union of finitely many cosets of \( \mathcal{O}^*_k \). By our assumption on \( \mathcal{O}^*_k \), \( h(R) \) is a finite set. This implies that \( R \) is contained in the union of finitely many hypersurfaces of the form \( f^{\deg g} = a g^{\deg f} \), \( a \in k \), and so \( R \) is not Zariski-dense.

Suppose that (c) holds. It suffices to prove our assertion in the case that \( Z \) is irreducible over \( k \), \( H_1 \) has minimal field of definition \( M \) over \( k \), and \( M \) contains a CM subfield \( L \) over \( k \). From what we have already proven, we can assume that the linear forms defining the hyperplanes are linearly independent. It follows from the fact that \( Z \) is irreducible that \( [M : k] = m \). Let \( \alpha_0, \ldots, \alpha_{m-1} \in \mathcal{O}_M \) be a basis for \( M \) over \( k \). Under our assumptions, after a \( k \)-linear change of variables (a projective \( k \)-automorphism of \( \mathbb{P}^m \)), we can take \( Z \) to be defined by \( N_k^M(x_0 \alpha_0 + \cdots + x_{m-1} \alpha_{m-1}) = 0 \), where \( N_k^M \) is the norm from \( M \) to \( k \), and the embeddings of \( M \) act on each \( x_i \) trivially. From the defining equation for \( Z \), it suffices to prove the case \( n = m - 1 \).

**Lemma 5.** Let \( Z \subset \mathbb{P}^{m-1} \) be defined by \( N_k^M(x_0 \alpha_0 + \cdots + x_{m-1} \alpha_{m-1}) = 0 \). Let \( R \) be a set of \( S \)-integral points on \( \mathbb{P}^{m-1} \setminus Z \). Let \( S_M \) be the set of places of \( M \) lying above places of \( S \). There exist a finite number of elements \( \beta_1, \ldots, \beta_r \in M \) such that every \( P \in R \) has a representative \((x_0, \ldots, x_{m-1}) \in \mathcal{O}^m_{k,S_M} \) with \( \sum_{i=0}^{m-1} x_i \alpha_i \in \beta_j \mathcal{O}^*_M, S_M \) for some \( j \).

**Proof.** By the definition of \( R \) being an \( S \)-integral set of points on \( \mathbb{P}^{m-1} \setminus Z \), for any monomial \( p \) in \( x_0, \ldots, x_{m-1} \) of degree \( m \), there exists a constant \( c_p \in k^* \) such that \( c_p p / N_k^M(\sum_{i=0}^{m-1} x_i \alpha_i) \)
takes on \( S \)-integral values on \( R \). Therefore there exists a constant \( C \in k^* \) such that for all points \((x_0, \ldots, x_{m-1}) \in R,\)
\[
\left( N_k^M \left( \sum_{i=0}^{m-1} x_i \alpha_i \right) \right) | C (x_0, \ldots, x_{m-1})^m
\]
as fractional ideals of \( \mathcal{O}_{k,S} \). Since the class group of \( k \) is finite, there exists a finite set of integral ideals \( \mathfrak{A} \) such that for any point of \( R \) we can write
\[
(x_0, \ldots, x_{m-1}) = (\beta) a,
\]
where \( \beta \in k \) and \( a \in \mathfrak{A} \). So dividing (1) by \( \beta^m \) on both sides, we see that every point of \( R \) has a representative \((x_0, \ldots, x_{m-1}) \in \mathcal{O}_{k,S}^m \) such that (as \( \mathcal{O}_{k,S} \) ideals)
\[
\left( N_k^M \left( \sum_{i=0}^{m-1} x_i \alpha_i \right) \right) | b
\]
where \( b \) is some fixed ideal of \( \mathcal{O}_{k,S} \) independent of \( x_0, \ldots, x_{n-1} \). Modulo \( S_M \)-units, there are only finitely many solutions \( x = \beta_1, \ldots, \beta_r \) to
\[
\left( N_k^M (x) \right) | b, \quad x \in \mathcal{O}_{M,S_M}.
\]
The claim then follows. \( \square \)

Before continuing, we make the following convenient definition.

**Definition 6.** Let \( M \) be a finite extension of a field \( k \), \([M : k] = n\). Let \( R \) be a subset of \( M^* \). Let \( \alpha_0, \ldots, \alpha_{n-1} \) be a basis for \( M \) over \( k \). We define \( R \) to be a dense subset of \( M \) over \( k \) if the set \( \{(x_0, \ldots, x_{n-1}) \in \mathbb{P}^{n-1}(k): \sum_{j=0}^{n-1} x_j \alpha_j \in R \} \) is a Zariski-dense subset of \( \mathbb{P}^{n-1} \).

This definition is clearly independent of the basis \( \alpha_0, \ldots, \alpha_{n-1} \) that is chosen. If \( R \subset M^* \) is not a dense subset of \( M \) over \( k \) it is clear that \( \alpha R \) for \( \alpha \in M^* \) is also not a dense subset of \( M \) over \( k \), since the corresponding subsets of \( \mathbb{P}^n \) differ by a projective automorphism. Therefore, using Lemma 5, to finish our claim assuming (c) we need to show that \( \mathcal{O}_{M,S_M}^* \) is not a dense subset of \( M \) over \( k \), where \( M \) contains a CM subfield \( L \) over \( k \). Let \( L' \) be the maximal real subfield of \( L \). Since the totally imaginary field \( L \) is a quadratic extension of the totally real field \( L' \), by the Dirichlet unit theorem the unit groups of \( \mathcal{O}_L \) and \( \mathcal{O}_{L'} \) have the same free rank. It follows that there exists a positive integer \( m \) such that if \( u \in \mathcal{O}_L^* \) then \( u^m \in \mathcal{O}_{L'}^* \). Let \([L : k] = 2l\). Let \( \beta_0, \ldots, \beta_{2l-1} \) be a basis for \( L \) over \( k \) where \( \beta_0, \ldots, \beta_{l-1} \) are real (and are therefore a basis for \( L' \) over \( k \)). Let \([N_L^M (\sum_{i=0}^{n-1} x_i \alpha_i)]^m = \sum_{j=0}^{2l-1} f_i \beta_i \) where the \( f_i \) are homogeneous polynomials in \( x_0, \ldots, x_{n-1} \). Since for any \( u \in \mathcal{O}_M^* \), \( N_L^M u \in \mathcal{O}_{L'}^* \), we obtain \( (N_L^M u)^m \in \mathcal{O}_{L'}^* \). Therefore the nontrivial polynomials \( f_i \) for \( l \leq i \leq 2l - 1 \) vanish on the set associated to \( \mathcal{O}_M^* \) in this basis. So \( \mathcal{O}_M^* \) is not a dense subset of \( M \) over \( k \).

To prove the other direction of the theorem, suppose that (a)–(c) are all not satisfied. Let \( Z_1, \ldots, Z_r \) be the irreducible components of \( Z \) over \( k \). For each \( i \), let \( M_i \) be the minimal field of definition over \( k \) of some hyperplane in \( Z_i \). Let \( d_i = [M_i : k] \) and let \( s(i) = \sum_{j=1}^{i-1} d_j \). Let
\(\alpha_{0,i}, \ldots, \alpha_{d_i-1,i}\) be a basis for \(M_i\) over \(k\). Since the linear forms \(L_i\) are linearly independent, it follows that after a \(k\)-linear change of coordinates, \(Z\) can be defined by

\[
\prod_{i=1}^{r} N_k^{M_i} \left( \sum_{j=0}^{d_i-1} x_{s(i)+j} \alpha_{j,i} \right) = 0.
\]

Additionally, by assumption, \(r = 1\) if \(O_k^*\) is finite. We claim that the set

\[
R = \left\{ (x_0, \ldots, x_n) \in \mathbb{P}^n(k) : \forall i, \sum_{j=0}^{d_i-1} x_{s(i)+j} \alpha_{j,i} \in O_{M_i}^*, \forall l \geq s(r+1), x_l \in O_k \right\}
\]

is a Zariski-dense set of \(S\)-integral points on \(\mathbb{P}^n \setminus Z\). That \(R\) is a set of \(S\)-integral points on \(\mathbb{P}^n \setminus Z\) is clear from our defining equation for \(Z\), the fact that norms of units are units, and that there exists some fixed \(N \in O_k\) such that if \((x_0, \ldots, x_n) \in R\) as above then for all \(i, x_i \in \frac{1}{N} O_k\).

When \(O_k^*\) is infinite, we first give an argument to reduce our claim to the case \(r = 1\), where \(Z\) is irreducible over \(k\). Suppose that \(R\) is not Zariski-dense. Let \(P\) be a nonzero homogeneous polynomial with a minimal number of terms vanishing on \(R\). We also choose such a \(P\) with minimal degree. Since for \((x_0, \ldots, x_n) \in R, x_l\) for \(l \geq s(r+1)\) can be chosen in the infinite set \(O_k\) independently of the other \(x_j\), it is clear that \(P\) does not contain any of the variables \(x_l, l \geq s(r+1)\). After reindexing, we can assume that \(x_0\) appears in \(P\). It follows from our minimality assumptions about \(P\) and the structure of \(R\) that one can specialize the variables \(x_{d_1}, \ldots, x_n\) to obtain a nonzero polynomial \(P'(x_0, \ldots, x_{d_1-1})\) (not necessarily homogeneous) that vanishes on the set

\[
R' = \left\{ (x_0, \ldots, x_{d_1-1}) \in \mathbb{A}^{d_1}(k) : \sum_{j=0}^{d_1-1} x_j \alpha_{j,1} \in O_{M_1}^* \right\}.
\]

Write \(P' = \sum_{i=0}^{q} P'_i\), where each \(P'_i\) is homogeneous of degree \(i\). If \(u \in O_k^*\) then \(P'_u = P'(ux_0, \ldots, ux_{d_1-1}) = \sum_{i=0}^{q} u^i P'_i\) gives another polynomial that vanishes on \(R'\). Since \(O_k^*\) is infinite, we can choose \(q + 1\) distinct units \(u_1, \ldots, u_{q+1}\) of \(O_k^*\), and by the invertibility of a Vandermonde matrix, we see that for each \(i\), \(P'_i \in \text{Span}\{P'_{u_1}, \ldots, P'_{u_{q+1}}\}\). Therefore if \(R\) is not Zariski-dense, we obtain a nonzero homogeneous polynomial that vanishes on \(R'\). Showing that such a homogeneous polynomial does not exist is equivalent to the \(r = 1\) case of our original claim. In other words, we have reduced the problem, whether or not \(O_k^*\) is finite, to showing that if \(M\) does not contain a CM subfield over \(k\), \([M : k] = n\), the set

\[
R = \left\{ (x_0, \ldots, x_{n-1}) \in \mathbb{P}^{n-1}(k) : \sum_{j=0}^{n-1} x_j \alpha_{j} \in O_M^* \right\}
\]

is Zariski-dense, where \(\alpha_0, \ldots, \alpha_{n-1}\) is a basis for \(M\) over \(k\). In our terminology, we need to show that \(O_M^*\) is a dense subset of \(M\) over \(k\).

**Theorem 7.** Let \(M\) be a finite extension of a number field \(k\). The set of units \(O_M^*\) of \(O_M\) is a dense subset of \(M\) over \(k\) if and only if \(M\) does not contain a CM subfield over \(k\).
We will need the following lemma.

Lemma 8. Let $M$ be a finite extension of a number field $k$, $[M : k] = n$. Let $\sigma_1, \ldots, \sigma_n$ be the embeddings of $M$ into $\mathbb{C}$ fixing $k$. Let $G$ be a multiplicative subgroup of $M^*$. Then $G$ is not a dense subset of $M$ over $k$ if and only if there exist nonidentical sequences of nonnegative integers $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ with $\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i$ such that

$$\prod_{i=1}^{n} \sigma_i(x)^{a_i} = \prod_{i=1}^{n} \sigma_i(x)^{b_i} \tag{3}$$

for all $x \in G$.

Proof. Let $\alpha_0, \ldots, \alpha_{n-1}$ be a basis for $M$ over $k$. Let $R$ be the subset of $\mathbb{P}^{n-1}$ associated to $G$ in this basis. Suppose that there exist nonidentical sequences of nonnegative integers $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ with $\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i$ such that $\prod_{i=1}^{n} \sigma_i(x)^{a_i} = \prod_{i=1}^{n} \sigma_i(x)^{b_i}$ for all $x \in G$. Substituting $x = \sum_{i=0}^{n-1} x_i \alpha_i$ into this equation gives a homogeneous polynomial that vanishes on $R$. It remains to show that this polynomial is nonzero, or equivalently, that for some $x \in M^*$, $\prod_{i=1}^{n} \sigma_i(x)^{a_i} \neq \prod_{i=1}^{n} \sigma_i(x)^{b_i}$.

To see this, we can take for example $x = p^q$ for some $q$, where $p$ lies above a prime of $k$ that splits completely in $\tilde{M}$, the Galois closure of $M$ over $k$. Looking at the prime ideal factorization (in $\mathcal{O}_M$) of both sides shows that they are unequal. Therefore $G$ is not a dense subset of $M$ over $k$.

Suppose now that there exists a nonzero homogeneous polynomial vanishing on $R$. If $x \in G$ and $x = \sum_{i=0}^{n-1} x_i \alpha_i$, $x_i \in k$, then it follows from the fact that $\text{Tr}^M_k(xy)$ is a nondegenerate bilinear form over $k$ that each $x_i$ is a linear form, independent of $x_i$ in $\sigma_1(x), \ldots, \sigma_n(x)$. Thus, any nonzero homogeneous polynomial vanishing on $R$ gives rise to a nonzero homogeneous polynomial $P(x_0, \ldots, x_{n-1})$ such that $P(\sigma_1(x), \ldots, \sigma_n(x)) = 0$ for all $x \in G$. Let $P$ be such a polynomial with a minimal number of terms. Let $c_1 \prod_{i=1}^{n} \sigma_i(x)^{a_i} = c_1 \phi_1(x)$ and $c_2 \prod_{i=1}^{n} \sigma_i(x)^{b_i} = c_2 \phi_2(x)$ be two distinct monomials appearing in $P(\sigma_1(x), \ldots, \sigma_n(x))$. Note that $\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i$. Suppose that there exists $a \in G$ such that $\phi_1(a) \neq \phi_2(a)$. Let $Q = P(\sigma_1(a)x_0, \ldots, \sigma_n(a)x_{n-1})$. Since $\phi_1(a) \neq \phi_2(a)$, $Q$ is not a scalar multiple of $P$. Since $G$ is a group, we have

$$P(\sigma_1(a)\sigma_1(x), \ldots, \sigma_n(a)\sigma_n(x)) = P(\sigma_1(ax), \ldots, \sigma_n(ax)) = 0$$

for all $x \in G$. Taking a linear combination of $P$ and $Q$, we can find a nonzero polynomial with fewer terms than $P$ that vanishes on $\sigma_1(x), \ldots, \sigma_n(x)$, giving a contradiction. □

Proof of Theorem 7. Let $[M : k] = n$ and let $\sigma_1, \ldots, \sigma_n$ be the embeddings of $M$ into $\mathbb{C}$ fixing $k$. Let $\alpha_0, \ldots, \alpha_{n-1}$ be a basis for $M$ over $k$. Let $R$ be as in (2).

The only if direction has already been proven in the first half of our proof of Theorem 3. So suppose that there exists a nonzero homogeneous polynomial vanishing on $R$. We need to show that $M$ contains a CM subfield over $k$. By Lemma 8, there exist nonidentical sequences of nonnegative integers $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ with $\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i$ such that

$$\prod_{i=1}^{n} \sigma_i(u)^{a_i} = \prod_{i=1}^{n} \sigma_i(u)^{b_i}, \quad \forall u \in \mathcal{O}_M^*.$$
By canceling terms, we can clearly assume that either \(a_i = 0\) or \(b_i = 0\) for \(i = 1, \ldots, n\). Let \(T\) be the set of \(\sigma_i\)'s such that \(a_i \neq 0\) and let \(T'\) be the set of \(\sigma_i\)'s such that \(b_i \neq 0\). By our assumption, \(T\) and \(T'\) are disjoint. By composing both sides of (4) with some \(\sigma_j\) we can assume that the identity embedding, \(id\), is in \(T\) (having fixed an identification of \(M \subset \mathbb{C}\)). Let \(\tau\) denote complex conjugation. Let \(\sigma_i \in T\). We claim that \(\sigma_j = \tau \sigma_i\) for some \(\sigma_j \in T'\) and that \(a_i = b_j\). By the Dirichlet unit theorem, we can find a unit \(u \in \mathcal{O}_M^*\) such that \(|\sigma_i(u)|\) is very large and \(|\sigma_j(u)|\) is very small and approximately the same size for all \(\sigma_i \neq \sigma_j\). Using that \(\sum_{i=1}^{n} a_i = \sum_{i=1}^{n} b_i\), this would clearly contradict (4) unless \(\tau \sigma_i \in T'\) and \(a_i = b_j\), where \(\sigma_j = \tau \sigma_i\). Applying the same argument to \(T'\), we find that if \(\sigma \in T'\) then \(\tau \sigma \in T\). Therefore \(T' = \{\tau \sigma : \sigma \in T\}\). In particular, \(\tau \in T'\) and so \(k\) must be real. Since \(T\) and \(T'\) are disjoint, \(T\) must consist only of complex embeddings.

Let \(\bar{M}\) denote the Galois closure of \(M\) over \(k\). Let \(G = \text{Gal}(\bar{M}/k)\) and \(H = \text{Gal}(\bar{M}/M)\). Lift each \(\sigma_i\) to an element \(\tilde{\sigma}_i \in G\) such that \(\tilde{\sigma}_i|_M = \sigma_i\). Let \(\tilde{T} = TH = \{\tilde{\sigma}_i h : h \in H, \ i = 1, \ldots, n\}\). Similarly, let \(\tilde{T}' = T'H\). These definitions clearly do not depend on the liftings \(\tilde{\sigma}_i\). Note that \(\text{id}_M \in \tilde{T}\), \(\tau \in \tilde{T}'\), and \(\tilde{T}\) and \(\tilde{T}'\) are disjoint. Let \(\Sigma_{\bar{M}}\) be the embeddings of \(\bar{M}\) into \(\mathbb{C}\) (not necessarily fixing \(k\)). Let \(\phi \in \Sigma_{\bar{M}}\). Conjugating (4) by \(\phi\), we obtain

\[
\prod_{\tilde{\sigma}_i \in \tilde{T}} \left[ \phi \sigma_i \phi^{-1}(u) \right]^{a_i} = \prod_{\tilde{\sigma}_i \in \tilde{T}'} \left[ \phi \sigma_i \phi^{-1}(u) \right]^{b_i} = \prod_{\sigma_i \in T} \left[ \phi \tau \sigma_i \phi^{-1}(u) \right]^{a_i}, \quad \forall u \in \mathcal{O}_\phi^*(M),
\]

where the second equality follows from our earlier observations. Note that each \(\phi \sigma_i \phi^{-1}\) and \(\phi \tau \sigma_i \phi^{-1}\) is an embedding of \(\phi(M)\) into \(\mathbb{C}\) over \(\phi(k)\). Therefore, applying our previous reasoning to \(\phi(M)\) and \(\phi(k)\), we find that \(\phi(k)\) is real (so \(k\) is totally real) and that if \(\sigma_i \in T\), then

\[
\phi \sigma_i \phi^{-1} = \tau \phi \sigma_j \phi^{-1}
\]

on \(\phi(M)\) for some \(\sigma_j \in T\). Since \(\phi(\bar{M})\) is Galois over \(\phi(k)\) and \(\phi(k)\) is real, \(\tau \phi \bar{M} = \phi(\bar{M})\). It then makes sense to apply \(\tau \phi^{-1}\) to the left of each side of (5) to obtain \(\tau \phi^{-1} \tau \phi \tilde{\sigma}_i \in \tilde{\sigma}_j H \subset \tilde{T}\).

So we see that

\[
\tau \phi^{-1} \tau \phi \tilde{T} = \tilde{T}, \quad \forall \phi \in \Sigma_{\bar{M}}.
\]

Let \(N = \langle \tau \phi^{-1} \tau \phi : \phi \in \Sigma_{\bar{M}} \rangle\) be the subgroup of \(G\) generated by the \(\tau \phi^{-1} \tau \phi\)'s. Since \(H\) is in \(\tilde{T}\), we have in particular that \(NH \subset \tilde{T}\). Let \(N' = \langle \tau \rangle \cdot N\).

**Lemma 9.** \(N\) and \(N'\) are normal subgroups of \(G\).

**Proof.** Let \(g \in G\) and \(\phi \in \Sigma_{\bar{M}}\). By the definition of \(N\) we see that

\[
\tau \left( g^{-1} \tau \right)^{-1} \tau g^{-1} \tau = g \tau g^{-1} \tau \in N \quad \text{and} \quad \tau \left( \phi \tau^{-1} \right)^{-1} \tau \phi \tau^{-1} \in N.
\]

Multiplying these two elements gives \(g (\tau \phi^{-1} \tau \phi) g^{-1} \in N\) and therefore \(N\) is a normal subgroup of \(G\). This implies \(N'\) is actually a group, and as it is generated by \(N\) and elements of the form \(\phi^{-1} \tau \phi\), it is clearly a normal subgroup of \(G\). \(\square\)

Therefore \(NH \subset \tilde{T}\) and \(N' H\) are subgroups of \(G\). Let \(L = \bar{M}^{NH}\) be the fixed field of \(NH\) and \(L' = \bar{M}^{N'H}\). Since \(M\) is the fixed field of \(H\), we get inclusions \(k \subset L' \subset L \subset M\).
Lemma 10. L is a CM field and $L'$ is its maximal real subfield.

Proof. Showing that $L$ is totally imaginary is equivalent to showing that for all $\phi \in \Sigma_M$, $\phi^{-1}\tau\phi \notin NH$. If $\phi^{-1}\tau\phi \in NH$, then $\tau \in NH \subset \tilde{T}$, but since $\tau \notin \tilde{T}$, and $\tilde{T}$ and $\tilde{T}'$ are disjoint, we would have a contradiction. Therefore $L$ is totally imaginary. We now show that $L'$ is totally real. This is equivalent to showing that $\phi^{-1}\tau\phi \in N'H$, $\forall \phi \in \Sigma_M$, which is trivial from the definition of $N'$. Since we clearly have $[N'H : NH] = 2$, we see that $L$ is a quadratic extension of $L'$. Therefore $L$ is a CM field and $L'$ is its maximal real subfield.

So we see that if $O^*_M$ is not a dense subset of $M$ over $k$ then $M$ contains a CM subfield over $k$, and so the proofs of Theorems 3 and 7 are complete.

In fact, the field $L$ in Lemma 10 is the maximal CM subfield of $M$ over $k$.

Lemma 11. Let $M$ be a finite extension of a number field $k$. Suppose that $M$ contains a CM subfield over $k$. Then there exists a (unique) maximal CM subfield $L$ of $M$ over $k$, i.e., for any CM subfield $K$ of $M$ over $k$, $K \subset L$.

Proof. Let $\tilde{M}$ be the Galois closure of $M$ over $k$. Let $G = \text{Gal}(\tilde{M}/k)$ and let $H = \text{Gal}(\tilde{M}/M)$. Let $\Sigma_M$ be the embeddings of $M$ into $\mathbb{C}$. Let $K$ be a CM subfield of $M$ over $k$ with maximal real subfield $K'$. Let $\phi \in \Sigma_M$. Let $\tau$ denote complex conjugation. Then $\phi^{-1}\tau\phi$ gives an automorphism of $K$ over $K'$ since $K$ is a CM field. Since $K$ is totally imaginary, this automorphism cannot be the identity on $K$. Therefore it is complex conjugation, and so $\tau\phi^{-1}\tau\phi$ fixes $K$, that is $\tau\phi^{-1}\tau\phi \in \text{Gal}(\tilde{M}/K)$. Let $N \subset G$ be the group generated by the $\tau\phi^{-1}\tau\phi$'s. Since $H \subset \text{Gal}(\tilde{M}/K)$, we have $NH \subset \text{Gal}(\tilde{M}/K)$. Since $K$ is complex, $\tau \notin NH$. But then the proof of Lemma 10 shows that the fixed field of $NH$, $L$, is a CM subfield of $M$ over $k$, and by Galois theory $K \subset L$. So $L$ is the maximal CM subfield of $M$ over $k$.

4. Non-archimedean places

We now consider the general case, where $S$ may contain non-archimedean places. It is trivial that the implication $(1) \Rightarrow (2)$ of Theorem 3 extends from $S = S_\infty$ to arbitrary $S$ (containing $S_\infty$). Furthermore, the proof that (a) implies (1) works for arbitrary $S$, and condition (b) does not occur if $S$ contains non-archimedean places. The real difficulty arises when condition (c) of Theorem 3 occurs and $S$ is larger than $S_\infty$.

Assuming that neither (a) nor (b) of Theorem 3 holds and that (c) is satisfied, we easily reduce, as before, to considering the case where $Z \subset \mathbb{P}^{m-1}$ is irreducible over $k$ defined by $N^M_k(x_0\alpha_0 + \cdots + x_m-1\alpha_{m-1}) = 0$, where $M$ contains $L$, the maximal CM subfield of $M$ over $k$. Using Lemma 5, determining if (1) of Theorem 3 holds in this situation is equivalent to determining if $O^*_{M,SM}$ is a dense subset of $M$ over $k$, where $SM$ is the set of places of $M$ lying over places of $S$. Thus, we are in a position to apply Lemma 8. Paying careful attention to the proof of Theorem 3, we see that if (3) holds for all $x \in O^*_{M,SM}$, then the identity must be of the form

$$\prod_{i=1}^{l} \tau \sigma_i N^M_L(x)^{a_i} = \prod_{i=1}^{l} \tau \sigma_i N^M_L(x)^{a_i}, \quad \forall x \in O^*_{M,SM}.$$
where $\tau$ denotes complex conjugation and $\sigma_1, \ldots, \sigma_l$ are the embeddings of $L$ into $\mathbb{C}$ fixing $k$. Since $N^M_L(\mathcal{O}^*_M, \mathcal{S}_M)$ is a finite index subgroup of $\mathcal{O}^*_{L, \mathcal{S}_L}$, we can reduce to the problem of determining whether there is a nontrivial identity

$$\prod_{i=1}^l (\sigma_i x)^{a_i} = \prod_{i=1}^l (\tau \sigma_i x)^{a_i} \quad (6)$$

for all $x \in \mathcal{O}^*_{L, \mathcal{S}_L}$. Without loss of generality, by raising both sides of (6) to an appropriate power, we can assume that $a_i$ is divisible by $[\mathcal{O}^*_{L, \mathcal{S}_L} : \mathcal{O}^*_{L, \mathcal{S}_L}']$ for all $i$, where $L'$ is the maximal real subfield of $L$. In that case, (6) is true for all $x \in \mathcal{O}^*_{L, \mathcal{S}_L}$ and any appropriate choice of the $a_i$. So we can essentially reduce to studying $\mathcal{O}^*_{L, \mathcal{S}_L}/\mathcal{O}^*_L$. Assume now that $L/k$ is Galois with Galois group $G = \text{Gal}(L/k)$. If one can compute a minimal set of generators for the free abelian group $\mathcal{O}^*_{L, \mathcal{S}_L}/\mathcal{O}^*_L$ and the action of $G$ on it in terms of those generators, then determining the existence of a solution to (6) becomes elementary linear algebra. So, at least in the case the appropriate field extensions are Galois, the problem of determining whether there exists a Zariski-dense set of $\mathcal{S}$-integral points on a complement of hyperplanes is reduced to being able to do certain computations with the non-archimedean part of the $\mathcal{S}$-unit group in particular CM fields.

Of course, the action of $G$ on $\mathcal{O}^*_{L, \mathcal{S}_L}/\mathcal{O}^*_L$ is closely related to how the non-archimedean places in $\mathcal{S}$ split in $L$. For instance (still assuming $L/k$ Galois), if some place of $\mathcal{S}$ splits completely in $L$, then $\mathcal{O}^*_{L, \mathcal{S}_L}$ is a dense subset of $L$ over $k$ (see the proof of Lemma 8). On the other hand, if no place of $\mathcal{S}_L'$ splits in $L$, then $\mathcal{O}^*_{L, \mathcal{S}_L}$ is not a dense subset of $L$ over $k$. More generally, let $D$ be the set of decomposition fields of the non-archimedean places of $\mathcal{S}_L$. Then it is easily shown that if $L'^* \prod_{F \in D} F^*$ is not a dense subset of $L$ over $k$, then $\mathcal{O}^*_{L, \mathcal{S}_L}$ is not a dense subset of $L$ over $k$. This leads to the following natural question.

**Question 12.** Let $L$ be a finite extension of a number field $k$. Let $\mathcal{F}$ be a set of subfields of $L$ over $k$. Can one simply characterize when $\prod_{F \in \mathcal{F}} F^*$ is a dense subset of $L$ over $k$?

While this question does not seem to have been studied before, the related problems of determining when $\prod_{F \in \mathcal{F}} F^* = L^*$ and, more generally, determining the group structure of $L^*/\prod_{F \in \mathcal{F}} F^*$ have been studied in [1,4,5]. It would be interesting to connect this work to Question 12.

**References**


