An Existential Divisibility Lemma for Global Fields

Jeroen Demeyer* Jan Van Geel†

2004–06–16

1 Introduction

In [Phe00] Thanases Pheidas proves, what he calls, existential divisibility lemmas for $K = \mathbb{F}_q(z)$ where q is a prime congruent to 3 mod 4 and for $K = \mathbb{Q}$. Let R be the set of primes p in $\mathbb{Z}$, respectively in $\mathbb{F}_q[t]$, such that -1 is not a square in the residue field of p. The existential divisibility lemmas state the existence of an existential formula $\phi(x, y)$ such that: *if $\phi(x, y)$ holds for $x, y \in K \setminus \{0\}$ then for all primes $p \in R$ for which $v_p(x)$ is odd it follows that $v_p(xy^{-2}) > 0$.*

Actually putting extra local conditions on the elements x (conditions in the point at infinity in the function field case and in the real prime and the prime 2 in case $K = \mathbb{Q}$) the truth of $\phi(x, y)$ for $x, y \in K^*$ is equivalent to the statement: *for all primes $p \in R$ for which $v_p(x)$ is odd it follows that $v_p(xy^{-2}) > 0$.*

The formula $\phi(x, y)$ expresses "almost" that *all poles of x in R, with odd multiplicity, are poles of y.*

These existential divisibility lemmas play a role in strategies to obtain undecidability results for the existential theory of the field K. In [Phe91] Pheidas proved that the existential theory of $\mathbb{F}_{p^n}(t)$ is undecidable. His proof worked for all odd primes p. Videla ([Vid94]) extended this result to rational global function fields of characteristic 2. Shlapentokh ([Shl96]) showed

*The first author is a Research Assistant of the Fund for Scientific Research - Flanders (Belgium) (F.W.O.-Vlaanderen).

†Work partially supported by the European Community's Human Potential Programme under contract HPRN-CT-2002-00287.

that the existential theory of global function fields of characteristic not 2 is undecidable and finally in her thesis ([Eis03]) Kirsten Eisenträger completed the results by proving the same result for global function fields in characteristic 2. This is essentially the (negative) solution of Hilbert's 10th problem for global function fields.

One of the main open questions directly related to Hilbert's 10th problem is whether or not the existential theory of $\mathbb{Q}$ (or more general of any number field) is decidable or undecidable. In [Phe00] a program to come to a uniform way to attack Hilbert's 10th problem for global fields is described. This program generates a series of "possible facts" (cf. [Phe00, sections 3 and 4]), two of which are related to the existential divisibility lemma and one of them is forced into the strategy by the fact that the existential divisibility lemma as proved by Pheidas uses the set of primes p for which -1 is not a square in the residue field of p.

In view of this Thanases Pheidas and Gunther Cornelissen raised the question to what extent the existential divisibility lemma holds. *For which sets of primes does it hold? Why does the condition in the prime 2 occur? Can the lemma be generalized to all global fields?*

Together with Karim Zahidi the second author worked out a more general version of the existential divisibility lemma. Namely for $K = \mathbb{Q}$ and for a set of primes that are inert in a quadratic extension of $\mathbb{Q}$. This result was presented at the Oberwolfach meeting on Hilbert's 10th problem in January 2003 (cf. [VZ03]).

In this paper we generalize the existential divisibility lemma to all global fields K (of characteristic not 2), and for all sets of primes that are inert in a quadratic extension L of K. We first prove the direct generalisation of Pheidas' existential divisibility lemma, with conditions in the real primes and in the primes ramifying in L. In the last section we remove all these conditions and prove:

Let K be a global field and $R(L/K)$ be the set of primes which are inert in a quadratic extension L of K. Then there is an existential formula $\Omega(x,y)$ which is equivalent with the formula

$$\forall \mathfrak{r} \in R(L/K) : \big(v_{\mathfrak{r}}(x) \ \textit{odd} \ \rightarrow v_{\mathfrak{r}}(xy^{-2}) > 0\big)$$

2 Preliminaries

Our discussion of the existential divisibility lemma relies on facts about norms and norm groups of quadratic extensions of local and global fields. We use the Hasse–Minkowski local–global principle and Hilbert's reciprocity law. In this section we give a survey of these facts, for more details and proofs we refer to the literature (e.g. [O'M63]).

We start fixing terminology and notation. Throughout the paper K will be a global field of characteristic not 2, so it is either a number field or the function field of a curve over a finite field $\mathbb{F}_q$ with q odd. L will be a quadratic extension of K.

With M_K we denote the set of all "primes" $\mathfrak{p}$ of K. In the number field case the *finite* or *non-archimedean* primes correspond (one to one) to (equivalence classes of) discrete valuations of K and the *infinite* or *archimedean* primes correspond (one to one) to the different embeddings of K in the complex numbers. In the function field case all the elements of M_K correspond (one to one) to (equivalence classes of) discrete valuations on K. With every element of M_K there corresponds a normalized absolute value $|\ |_\mathfrak{p}$ on K, we let $K_\mathfrak{p}$ denote the completion of K with respect to this absolute value.

If $\mathfrak{p}$ is a non-archimedean prime, then $K_\mathfrak{p}$ is the fraction field of a complete discrete valuation ring $\mathcal{O}_\mathfrak{p}$ and its maximal ideal is a principal ideal. A generator for this ideal is called a uniformizing element. We can choose such a uniformizing element in the base field K and denote it with $\pi_\mathfrak{p}$. The quotient ring $\mathcal{O}_\mathfrak{p}/(\pi_\mathfrak{p})$ is a finite field $\mathbb{F}_\mathfrak{p}$, the residue field of the prime $\mathfrak{p}$. The discrete valuation associated with a non-archimedean prime $\mathfrak{p}$ will be denoted with $v_\mathfrak{p}$ and we normalize it by $v_\mathfrak{p}(\pi_\mathfrak{p}) = 1$. We use the analogous terminology and notation for primes $\mathfrak{P} \in M_L$.

All absolute values $|\ |_\mathfrak{p}$ extend to the quadratic extension L/K in different ways, depending on the prime $\mathfrak{p}$. The possible extensions correspond to what is called the *splitting behavior* of the prime $\mathfrak{p}$ in L. For a quadratic extension we have the following possibilities (in the number field case we distinguish between non-archimedean and archimedean primes, in the function field case points 4 and 5 are empty):

1. $\mathfrak{p}$ is a non-archimedean prime and $L \otimes_K K_\mathfrak{p} \cong K_\mathfrak{p} \times K_\mathfrak{p}$. In this case there are two primes $\mathfrak{P}_1, \mathfrak{P}_2$ in M_L lying over $\mathfrak{p}$, $L_{\mathfrak{P}_1} \cong L_{\mathfrak{P}_2} \cong K_\mathfrak{p}$ and $\mathbb{F}_{\mathfrak{P}_1} \cong \mathbb{F}_{\mathfrak{P}_2} \cong \mathbb{F}_\mathfrak{p}$. We say that the prime $\mathfrak{p}$ is *completely split* in L.

2. $\mathfrak{r}$ is a non-archimedean prime and $L \otimes_K K_\mathfrak{r}$ is a quadratic field extension $L_\mathfrak{R}$ over $K_\mathfrak{r}$ and $[\mathbb{F}_\mathfrak{R} : \mathbb{F}_\mathfrak{r}] = 2$. In this case there is only one prime $\mathfrak{R}$ in L lying over $\mathfrak{r}$, the uniformizing element $\pi_\mathfrak{r}$ of $\mathcal{O}_\mathfrak{r}$ is also a uniformizing element of $\mathcal{O}_\mathfrak{R}$. The prime $\mathfrak{r}$ is said to be *inert* in L.

3. $\mathfrak{s}$ is a non-archimedean prime and $L \otimes_K K_\mathfrak{s}$ is a quadratic field extension $L_\mathfrak{S}$ over $K_\mathfrak{s}$ and $[\mathbb{F}_\mathfrak{S} : \mathbb{F}_\mathfrak{s}] = 1$. Here we also have a unique prime $\mathfrak{S}$ in L lying over $\mathfrak{s}$, but the uniformizing element $\pi_\mathfrak{s}$ of $\mathcal{O}_\mathfrak{s}$ is not a uniformizing element of $\mathcal{O}_\mathfrak{S}$. We have $\pi_\mathfrak{S}^2 = w\pi_\mathfrak{s}$ with w a unit in $\mathcal{O}_\mathfrak{S}$. The prime $\mathfrak{s}$ is said to *ramify* in L.

4. $\mathfrak{a}$ is an archimedean prime and $L \otimes K_\mathfrak{a} \cong K_\mathfrak{a} \times K_\mathfrak{a}$, the archimedean prime $\mathfrak{a}$ is said to *split* in L.

5. $\mathfrak{c}$ is an archimedean prime and $L \otimes_K K_\mathfrak{c}$ is quadratic extension $L_\mathfrak{C}$ of $K_\mathfrak{c}$. Note that this case can only occur if $K_\mathfrak{c} \cong \mathbb{R}$ and we have $L_\mathfrak{C} \cong \mathbb{C}$, the archimedean prime $\mathfrak{c}$ *does not split* in L.

We can now partition the set of primes M_K according to the splitting behavior in the quadratic extension L:

$$\begin{aligned}
P(L/K) &= \{\mathfrak{p} \in M_K \mid \mathfrak{p} \text{ is a non-archimedean prime, completely split in } L\}\\
R(L/K) &= \{\mathfrak{r} \in M_K \mid \mathfrak{r} \text{ is a non-archimedean prime, inert in } L\}\\
S(L/K) &= \{\mathfrak{s} \in M_K \mid \mathfrak{s} \text{ is a non-archimedean prime, ramified in } L\}\\
A_\mathrm{s}(L/K) &= \{\mathfrak{a} \in M_K \mid \mathfrak{a} \text{ is an archimedean prime, split in } L\}\\
A_\mathrm{ns}(L/K) &= \{\mathfrak{c} \in M_K \mid \mathfrak{c} \text{ is an archimedean prime, not split in } L\}
\end{aligned}$$

In the number field case we sometimes need to refer to all archimedean primes therefore we define $A(L/K) = A_\mathrm{s}(L/K) \cup A_\mathrm{ns}(L/K)$. In the function field case the sets $A(L/K)$, $A_\mathrm{s}(L/K)$ and $A_\mathrm{ns}(L/K)$ are empty.

The sets $S(L/K)$, $A_\mathrm{s}(L/K)$ and $A_\mathrm{ns}(L/K)$ are finite. The sets $P(L/K)$ and $R(L/K)$ are not empty, Chebotarev's density theorem yields that these sets are infinite and both have density $\frac{1}{2}$. (An other consequence of Chebotarev's theorem states that the set of primes $P(L/K)$ that split completely determine uniquely the (Galois) extension L/K.)

The strong approximation theorem [Neu92, page 204] implies

Proposition 1. *Let T be a finite set of primes in K such that $A(L/K) \subset T$. Let $a_\mathfrak{t} \in K$ for $\mathfrak{t} \in T$. Choose a prime $\mathfrak{p}_0$ not in T. Then for all $\varepsilon > 0$ there exists an element $x \in K$ such that*

$$|x - a_\mathfrak{t}|_\mathfrak{t} < \varepsilon \text{ for all } \mathfrak{t} \in T \text{ and } |x|_\mathfrak{q} \leq 1 \text{ for all } \mathfrak{q} \in M_K \setminus (T \cup \{\mathfrak{p}_0\})$$

As an immediate consequence of this one has

Corollary 2. *Let T, $\mathfrak{p}_0 \notin T$ and $a_\mathfrak{t} \in K$ be as in the preceding proposition. Then there exists an element $a \in K$ such that*

$$\begin{aligned}
v_\mathfrak{t}(a) &= v_\mathfrak{t}(a_\mathfrak{t}) \text{ for all } \mathfrak{t} \in T \setminus A(L/K)\\
\mathrm{sign}(a) &= \mathrm{sign}(a_\mathfrak{t}) \text{ for all } \mathfrak{t} \text{ with } K_\mathfrak{t} \cong \mathbb{R}
\end{aligned}$$

and

$$v_\mathfrak{q}(a) \geq 0 \text{ for all } \mathfrak{q} \in M_K \setminus (T \cup \{\mathfrak{p}_0\})$$

Let $\sigma \in \mathrm{Gal}(L/K)$ be the non-trivial automorphism of L fixing K. The norm map $\mathrm{N}_{L/K} : L^* \to K^*; z \mapsto z\sigma(z)$ defines a quadratic form on the two dimensional vector space L over K. If $L = K(\alpha)$ then we can write this form as $x^2 + \mathrm{Tr}_{L/K}(\alpha)xy + \mathrm{N}_{L/K}(\alpha)y^2$ with respect to the basis $\{1, \alpha\}$ for L over K. Here $\mathrm{Tr}_{L/K}(z) = z + \sigma(z)$ stands for the trace map.

Facts. We will denote this quadratic form with N and we have the following facts (cf. [O'M63] and [Sch85]):

1. For all $\mathfrak{p} \in P(L/K)$ the quadratic form N has a non-trivial zero over $K_\mathfrak{p}$, it follows from this that every element of $K_\mathfrak{p}$ is represented by N.
2. For all $\mathfrak{r} \in R(L/K)$ the norm form N has no non-trivial zero over $K_\mathfrak{r}$. The elements of $K_\mathfrak{r}$ represented by N are exactly the norms of the extension $L_\mathfrak{R}/K_\mathfrak{r}$, where $\mathfrak{R}$ is the unique prime in L lying over $\mathfrak{r}$. The norm map $\mathrm{N}_{L_\mathfrak{R}/K_\mathfrak{r}}$ is surjective on units $\mathcal{U}_\mathfrak{r}$ in $\mathcal{O}_\mathfrak{r}$ and the uniformizing element $\pi_\mathfrak{r}$ is not a norm. It follows that an element $x \in K_\mathfrak{r}$ is a norm if and only if its valuation $v_\mathfrak{r}(x)$ is even (we recall that $v_\mathfrak{r}$ is the discrete valuation associated to $\mathfrak{r}$ and normalized by $v_\mathfrak{r}(\pi_\mathfrak{r}) = 1$).
3. For all $\mathfrak{s} \in S(L/K)$ the norm form N has no non-trivial zero over $K_\mathfrak{s}$. Again the elements represented by N are the norms of the extension $L_\mathfrak{S}/K_\mathfrak{s}$, where $\mathfrak{S}$ is the unique prime in L lying over $\mathfrak{s}$. The image $\mathrm{N}_{L_\mathfrak{S}/K_\mathfrak{s}}(\mathcal{U}_\mathfrak{S})$ of the group of units in $\mathcal{O}_\mathfrak{S}$ is a subgroup of index 2 in the group $\mathcal{U}_\mathfrak{s}$ of units in $\mathcal{O}_\mathfrak{s}$. It follows that $\mathrm{N}_{L_\mathfrak{S}/K_\mathfrak{s}}(L_\mathfrak{S})$ is a subgroup of index 2 in $K_\mathfrak{s}$, since $\mathrm{N}_{L_\mathfrak{S}/K_\mathfrak{s}}(\pi_\mathfrak{S}) = u\pi_\mathfrak{s}$ for some unit u in $\mathcal{O}_\mathfrak{s}$.
4. For primes $\mathfrak{a} \in A_\mathrm{s}(L/K)$ we have the same as completely split primes, namely that every element of $K_\mathfrak{a}$ is represented by N.
5. If $\mathfrak{c} \in A_\mathrm{ns}(L/K)$, the norm form N has no non-trivial zero over $K_\mathfrak{c}$. The elements represented by N are the norms of the extension $L_\mathfrak{C} = \mathbb{C}$ over $K_\mathfrak{p} = \mathbb{R}$. So these are the elements represented as sums of 2 squares in $\mathbb{R}$, which are exactly the positive elements in $\mathbb{R}$.

For inert primes $\mathfrak{r} \in R(L/K)$ we need slightly more than the fact that the norms in $K_\mathfrak{r}$ are the elements of even valuation.

Lemma 3. *Let $\mathfrak{r} \in R(L/K)$ be an inert prime and $\mathfrak{R}$ the unique prime in L lying over $\mathfrak{r}$. Let $\alpha \in \mathcal{O}_\mathfrak{R}$ be such that $\mathcal{O}_\mathfrak{R}/(\pi_\mathfrak{R}) = \mathbb{F}_\mathfrak{R} = \mathbb{F}_\mathfrak{r}[\overline{\alpha}] = \big(\mathcal{O}_\mathfrak{r}/(\pi_\mathfrak{r})\big)[\overline{\alpha}]$, with $\overline{\alpha}$ the reduction of $\alpha \bmod \mathfrak{R}$. Then*

$$v_\mathfrak{r}(\mathrm{N}_{L_\mathfrak{R}/K_\mathfrak{r}}\left(x + y\alpha)\right) = \min(v_\mathfrak{r}(x^2), v_\mathfrak{r}(y^2))$$

for $x, y \in K_\mathfrak{r}$.

Proof. Because $\mathfrak{r}$ is inert, we may replace $v_{\mathfrak{r}}$ with $v_{\mathfrak{R}}$ in the statement.

Note that $\sigma \in \mathrm{Gal}(L/K)$ extends to a generator of $\mathrm{Gal}(L_{\mathfrak{R}}/K_{\mathfrak{r}})$, so

$$v_{\mathfrak{R}}\big(\,\mathrm{N}_{L_{\mathfrak{R}}/K_{\mathfrak{r}}}(x+y\alpha)\big) = v_{\mathfrak{R}}\big((x+y\alpha)(x+y\sigma(\alpha))\big) = 2v_{\mathfrak{R}}(x+y\alpha)$$

It remains to prove that $v_{\mathfrak{R}}(x+y\alpha) = \min(v_{\mathfrak{R}}(x), v_{\mathfrak{R}}(y))$.

The hypotheses imply that $v_{\mathfrak{r}}(\alpha) = 0$, since $\overline{\alpha}$ is non-zero in $\mathbb{F}_{\mathfrak{R}}$. If $v_{\mathfrak{r}}(x) \neq v_{\mathfrak{r}}(y)$, the properties of discrete valuations immediatly give us $v_{\mathfrak{R}}(x+y\alpha) = \min(v_{\mathfrak{R}}(x), v_{\mathfrak{R}}(y))$.

Now suppose $v_{\mathfrak{R}}(x) = v_{\mathfrak{R}}(y) = m$ for a certain integer m. Then we have $x = \pi_{\mathfrak{r}}^m x_0$ and $y = \pi_{\mathfrak{r}}^m y_0$, with x_0 and y_0 elements of $\mathcal{O}_{\mathfrak{r}}$ having valuation 0.

Since $\{1, \overline{\alpha}\}$ is a basis for $\mathbb{F}_{\mathfrak{R}}$ over $\mathbb{F}_{\mathfrak{r}}$, we have that $\overline{x_0 + y_0\alpha} = \overline{x_0} + \overline{y_0}\,\overline{\alpha}$ is a non-zero element of $\mathbb{F}_{\mathfrak{R}}$, so $v_{\mathfrak{R}}(x_0+y_0\alpha) = 0$. Hence $v_{\mathfrak{R}}(x+y\alpha) = v_{\mathfrak{R}}\big(\pi_{\mathfrak{r}}^m(x_0+y_0\alpha)\big) = m = \min(v_{\mathfrak{R}}(x), v_{\mathfrak{R}}(y))$. $\square$

Information on the global norm group $\mathrm{N}_{L/K}(L^*) \subset K^*$ can be obtained from Hilbert's reciprocity law as expressed by the exact sequence (cf. [Rei75] and [O'M63])

$$0 \to {}_2\mathrm{Br}(K) \to \bigoplus_{\mathfrak{p}\in M_K} {}_2\mathrm{Br}(K_{\mathfrak{p}}) \xrightarrow{\sum \mathrm{inv}_{\mathfrak{p}}} \mathbb{Z}/2\mathbb{Z} \to 0 \tag{1}$$

Here ${}_2\mathrm{Br}(F)$ denotes the two component (the elements of exponent two) of the Brauer group of the field F. The elements of the Brauer group of F are classes of central simple algebras over F, the group law is induced by the tensor product of algebras. In the case of local and global fields (of characteristic not 2) the (non-trivial) elements of the two component of the Brauer group are given by quaternion division algebras, which in turn can be represented by symbols (a, b) with a, b non-zero elements of the field. The symbol (a, b) corresponds to the quaternion algebra with basis $\{1, i, j, k\}$ satisfying $i^2 = a, j^2 = b, ij = -ji = k = ab$. If one is not familiar with the theory of Brauer groups, it is enough to know that the subgroups of elements of exponent 2 are generated multiplicatively by these symbols modulo the following relations (cf. [Sch85])

- $(ab, c) = (a, c)(b, c)$ and $(a, bc) = (a, b)(a, c)$
- for all $a \neq 0, 1$; $(a, 1-a) = 1$.

Remark. This is true for the two component of the Brauer group of any field (of characteristic not equal to 2) by a theorem of Merkuriev. For local and global fields one has moreover that the product of symbols is equal to a symbol, this fact does not hold in general.

The following facts are important for us:

Proposition 4 ([Rei75, section 31]). *Over a local field $K_\mathfrak{p}$ there exists a unique quaternion division algebra $\mathbb{H}_\mathfrak{p}$, so ${}_2\mathrm{Br}(K_\mathfrak{p}) \cong \mathbb{Z}/2\mathbb{Z}$.*

This element $\mathbb{H}_\mathfrak{p}$ is split over any quadratic extension E of $K_\mathfrak{p}$, i.e., $\mathbb{H}_\mathfrak{p} \otimes_{K_\mathfrak{p}} E$ is a full matrix algebra over $K_\mathfrak{p}$ and is therefore trivial in $\mathrm{Br}(K_\mathfrak{p})$.

In the exact sequence (1) presenting Hilbert's reciprocity law the maps $\mathrm{inv}_\mathfrak{p} : {}_2\mathrm{Br}(K_\mathfrak{p}) \to \mathbb{Z}/2\mathbb{Z}$ are defined by $\mathrm{inv}_\mathfrak{p}(\mathbb{H}_\mathfrak{p}) = 1 \in \mathbb{Z}/2\mathbb{Z}$, proposition 4 says that $\mathrm{inv}_\mathfrak{p}$ is an isomorphism.

Proposition 5 ([Rei75, Theorem 30.4]). *Let F be a field, $\mathrm{char}(F) \neq 2$. A quaternion division algebra $\mathbb{H}$ over F is represented by a symbol of the form (a, b) with $a \in F^* \setminus F^{*2}$ if and only if $\mathbb{H} \otimes F(\sqrt{a})$ is trivial in ${}_2\mathrm{Br}(F)$. If $a \in F^* \setminus F^{*2}$ then a symbol (a, b) is trivial in ${}_2\mathrm{Br}(F)$ if and only if $b \in \mathrm{N}_{F(\sqrt{a})/F}(F(\sqrt{a})^*)$.*

The second part of this proposition together with Hilbert's reciprocity law yield the Hasse norm theorem for quadratic extensions L/K. This theorem states that an element in K is a norm of an element in L if and only if it is a norm locally everywhere. More generally the following holds for quadratic forms over global fields:

Theorem 6 (Hasse–Minkowski, [Sch85]). *A quadratic form Q over a global field K has a non-trivial zero in K if and only if it has a non-trivial zero in $K_\mathfrak{p}$ for all $\mathfrak{p} \in M_K$.*

An element x in a global field K is represented by a quadratic form Q over K if and only if x is represented by Q over $K_\mathfrak{p}$ for all $\mathfrak{p} \in M_K$.

Let ${}_2\mathrm{Br}(L/K)$ be the kernel of the natural group morphism ${}_2\mathrm{Br}(K) \to {}_2\mathrm{Br}(L)$. Clearly for any element ω in this kernel we have $\mathrm{inv}_\mathfrak{p}(\omega) \equiv 0 \bmod 2$ for $\mathfrak{p} \in P(L/K) \cup A_s(L/K)$. Hilbert's reciprocity law together with the approximation theorem allows us to give different parameterizations of the finite subgroups of ${}_2\mathrm{Br}(L/K)$. We will use this in section 4.

Let Q be a finite set of primes satisfying

$$S(L/K) \cup A_{\mathrm{ns}}(L/K) \subseteq Q \subseteq R(L/K) \cup S(L/K) \cup A_{\mathrm{ns}}(L/K)$$

Denote with ${}_2\mathrm{Br}^Q(L/K)$ the subgroup of ${}_2\mathrm{Br}(L/K)$ defined by

$${}_2\mathrm{Br}^Q(L/K) = \{\omega \in {}_2\mathrm{Br}(L/K) \mid \mathrm{inv}_\mathfrak{l}(\omega) \equiv 0 \bmod 2 \text{ for all } \mathfrak{l} \in M_K \setminus Q\}$$

Hilbert's reciprocity law gives a one-to-one correspondence between ${}_2\mathrm{Br}^Q(L/K)$ and the set $\{Q_0 \subseteq Q | \#Q_0 \text{ even}\}$. This correspondence is given by

$$\omega \mapsto Q_\omega = \{\mathfrak{q} \in M_K \mid \mathrm{inv}_\mathfrak{q}\, \omega \equiv 1 \bmod 2\}$$

The latter is a subset of Q by the definition of ${}_2\mathrm{Br}^Q(L/K)$.

Let T be a finite subset of primes in $R(L/K) \setminus Q$, and fix a $\Delta \in K^*$ for which $L = K(\sqrt{\Delta})$. Take an $\omega \in {}_2\mathrm{Br}^Q(L/K)$, then ω is of the form (Δ, λ) with $\lambda \in K^*$. We claim that we may choose λ such that $v_{\mathfrak{r}}(\lambda) \geq 0$ for all $\mathfrak{r} \in R(L/K)$ and $v_{\mathfrak{t}}(\lambda) = 0$ for all $\mathfrak{t} \in T$. To see this, we note that for $\mathfrak{t} \in T$ we have $\mathrm{inv}_{\mathfrak{t}}(\omega) \equiv 0 \bmod 2$, so λ is a norm of $L_{\mathfrak{T}}/K_{\mathfrak{t}}$ and $v_{\mathfrak{t}}(\lambda)$ is even. Now we apply the approximation theorem (corollary 2) with $\mathfrak{p}_0 \in P(L/K)$ to find an element $c \in K^*$ such that

$$v_{\mathfrak{r}}(c) \geq -\frac{v_{\mathfrak{r}}(\lambda)}{2} \qquad \text{for all } \mathfrak{r} \in R(L/K)$$
$$v_{\mathfrak{t}}(c) = -\frac{v_{\mathfrak{t}}(\lambda)}{2} \qquad \text{for all } \mathfrak{t} \in T$$

Since $\omega = (\Delta, \lambda) = (\Delta, c^2\lambda)$, we may replace λ by $c^2\lambda$ to obtain the desired conditions.

By choosing one such λ for every $\omega \in {}_2\mathrm{Br}^Q(L/K)$, we obtain a set $\Lambda_{Q,T}(L/K)$ parametrizing the elements of ${}_2\mathrm{Br}^Q(L/K)$, we have:

Lemma 7. *Let Q, T and $\Lambda_{Q,T} = \Lambda_{Q,T}(L/K)$ be as above.*

There is a one-to-one correspondence between $\Lambda_{Q,T}$ and the subsets of Q with an even number of elements, given by

$$\lambda \mapsto Q_\lambda = \{\mathfrak{q} \in Q \mid \mathrm{inv}_{\mathfrak{q}}(\Delta, \lambda) \equiv 1 \bmod 2\}$$

Conversely for every subset Q_0 of Q with $\# Q_0 \in 2\mathbb{Z}$ there is a unique $\lambda \in \Lambda_{Q,T}$ determined by the fact that λ is a norm of $L_{\mathfrak{Q}}/K_{\mathfrak{q}}$, where $\mathfrak{Q} \in M_L$ and $\mathfrak{q}$ is the prime in K lying under $\mathfrak{Q}$, if and only if $\mathfrak{q} \notin Q_0$.

Proof. Except for the last statement this follows from the contruction of the set $\Lambda_{Q,T}$. The last statement follows from the fact that $\mathrm{inv}_{\mathfrak{l}}(\Delta, \lambda) \equiv 0 \bmod 2$ for all $\mathfrak{l} \notin Q$ and that $\mathrm{inv}_{\mathfrak{q}}(\Delta, \lambda) \equiv 1 \bmod 2$ if and only if λ is not a norm from $L_{\mathfrak{Q}}/K_{\mathfrak{q}}$. □

3 Existential Divisibility Lemma

As before K is a global field (of characteristic not 2) and L is a quadratic extension of K. We fix an element $\Delta \in K^*$ such that $L = K(\sqrt{\Delta})$.

Proposition 8. *There exists an existential formula $\phi(x, y)$ such that:*

1. *Let x and y be elements of K^* for which $\phi(x,y)$ is true. If $\mathfrak{r}$ is any prime in $R(L/K)$ such that $v_{\mathfrak{r}}(x)$ is odd, then $v_{\mathfrak{r}}(xy^{-2}) > 0$.*

2. *$\phi(x,y)$ is true for all elements x and y of K^* satisfying the following conditions:*

   (a) *There exists at least one $\mathfrak{r} \in R(L/K)$ for which $v_{\mathfrak{r}}(x)$ is odd.*

   (b) *For every $\mathfrak{r} \in R(L/K)$ with $v_{\mathfrak{r}}(x)$ odd, we have $v_{\mathfrak{r}}(xy^{-2}) \geq 0$.*

   (c) *For every $\mathfrak{c} \in A_{\text{ns}}$ the element x is positive in $K_{\mathfrak{c}} \cong \mathbb{R}$.*

   (d) *For every $\mathfrak{s} \in S(L/K)$, the element x is a norm from $L_{\mathfrak{S}}$, where $\mathfrak{S}$ is the unique prime lying above $\mathfrak{s}$.*

To prove the proposition we need to use lemma 3 for all inert primes $\mathfrak{r} \in R(L/K)$. However in general it is not possible to find a primitive element $\alpha \in L$ such that $\mathbb{F}_{\mathfrak{R}} = \mathbb{F}_{\mathfrak{r}}[\overline{\alpha}]$ for all $\mathfrak{r} \in R(L/K)$. The following lemma will solve this difficulty:

Lemma 9. *Let K and L be as above. There exist elements $\alpha_0, \alpha_1 \in L^*$ such that for all $\mathfrak{r} \in R(L/K)$ either $\mathbb{F}_{\mathfrak{R}} = \mathbb{F}_{\mathfrak{r}}[\overline{\alpha_0}]$ or $\mathbb{F}_{\mathfrak{R}} = \mathbb{F}_{\mathfrak{r}}[\overline{\alpha_1}]$.*

Proof. We start by setting $\alpha_0 = \sqrt{\Delta}$. Consider a $\mathfrak{r} \in R(L/K)$ such that $v_{\mathfrak{r}}(\Delta) = 0$ and (in the number field case) $\mathfrak{r}$ is not a 2-adic prime (i.e., it is not lying above the prime 2 in $\mathbb{Q}$). Since $L_{\mathfrak{R}} = K_{\mathfrak{r}}(\sqrt{\Delta})$ is a quadratic extension of $K_{\mathfrak{r}}$, it follows from the assumptions on $\mathfrak{r}$ that $\overline{\Delta}$ is not a square in $\mathbb{F}_{\mathfrak{r}}$. This is a consequence of Hensel's lemma since for non-2-adic primes a square in the residue field lifts to a square in the completion. So for these primes $\mathfrak{r}$ we have $\mathbb{F}_{\mathfrak{R}} = \mathbb{F}_{\mathfrak{r}}(\overline{\sqrt{\Delta}})$.

The remaining primes are exactly the inert 2-adic primes or the inert primes $\mathfrak{r}$ for which $v_{\mathfrak{r}}(\Delta) \neq 0$. This set T of inert primes is finite, say $T = \{\mathfrak{r}_1, \ldots, \mathfrak{r}_n\}$. For all $i = 1, \ldots, n$, we let $\mathfrak{R}_i$ be the unique prime in L lying over $\mathfrak{r}_i$.

Consider the semi-local ring $\mathcal{O}_T = \cap_{i=1}^{n}(\mathcal{O}_{\mathfrak{r}_i} \cap K)$ and its integral closure $\widetilde{\mathcal{O}_T} = \cap_{i=1}^{n}(\mathcal{O}_{\mathfrak{R}_i} \cap L)$. The canonical morphisms

$$\mathcal{O}_T \hookrightarrow \mathcal{O}_{\mathfrak{r}_i} \text{ and } \widetilde{\mathcal{O}_T} \hookrightarrow \mathcal{O}_{\mathfrak{R}_i}$$

induce isomorphisms $\mathcal{O}_T/(\pi_{\mathfrak{r}_i}) \cong \mathcal{O}_{\mathfrak{r}_i}/(\pi_{\mathfrak{r}_i}) = \mathbb{F}_{\mathfrak{r}_i}$ and $\widetilde{\mathcal{O}_T}/(\pi_{\mathfrak{R}_i}) \cong \mathcal{O}_{\mathfrak{R}_i}/(\pi_{\mathfrak{R}_i}) = \mathbb{F}_{\mathfrak{R}_i}$. For all $i = 1, \ldots, n$ the residue fields $\mathbb{F}_{\mathfrak{R}_i}$ are degree 2 extensions of $\mathbb{F}_{\mathfrak{r}_i}$, so $\mathbb{F}_{\mathfrak{R}_i} = \mathbb{F}_{\mathfrak{r}_i}[\overline{\beta_i}]$. By the Chinese remainder theorem there exists an element $\alpha_1 \in \widetilde{\mathcal{O}_T}$ such that $\alpha_1 \equiv \overline{\beta_i} \bmod (\pi_{\mathfrak{R}_i})$. This implies $\mathbb{F}_{\mathfrak{R}_i} = \mathbb{F}_{\mathfrak{r}_i}[\overline{\alpha_1}]$ for all $i = 1, \ldots, n$. $\square$

We can now prove the proposition.

Proof. Take α_0, α_1 as in lemma 9. We define $\phi(x, y)$ as

$$\phi(x, y) \leftrightarrow \phi_0(x, y) \wedge \phi_1(x, y)$$

where $\phi_i(x, y)$ is the formula

$$\phi_i(x, y) \leftrightarrow \exists a, b, c \in K : 1 + x \,\mathrm{N}(y^{-1} + \alpha_i c) = a^2 - \Delta b^2$$

or, written in an other way

$$\phi_i(x, y) \leftrightarrow \exists a, b, c \in K : (1 + xy^{-2}) + xy^{-1} \,\mathrm{Tr}(\alpha_i) c + x \,\mathrm{N}(\alpha_i) c^2 - a^2 + \Delta b^2 = 0$$

We will prove part 1 of the theorem. For the sake of contradiction, assume that $\phi(x, y)$ holds, but $v_{\mathfrak{r}}(xy^{-2}) \leq 0$ for some prime $\mathfrak{r} \in R(L/K)$ for which $v_{\mathfrak{r}}(x)$ is odd. Since $v_{\mathfrak{r}}(xy^{-2})$ is odd, necessarily $v_{\mathfrak{r}}(xy^{-2}) < 0$.

We have $\mathbb{F}_{\mathfrak{R}} = \mathbb{F}_{\mathfrak{r}}[\alpha_i]$, with i either equal to 0 or 1. Lemma 3 implies $v_{\mathfrak{r}}\big(\mathrm{N}(y^{-1} + \alpha_i c)\big) = \min(v_{\mathfrak{r}}(y^{-2}), v_{\mathfrak{r}}(c^2)) \leq v_{\mathfrak{r}}(y^{-2})$. It follows that

$$v_{\mathfrak{r}}\big(x \,\mathrm{N}(y^{-1} + \alpha_i c)\big) \leq v_{\mathfrak{r}}(xy^{-2}) < 0$$

Thus $v_{\mathfrak{r}}\big(1 + x \,\mathrm{N}(y^{-1} + \alpha_i c)\big) = v_{\mathfrak{r}}\big(x \,\mathrm{N}(y^{-1} + \alpha_i c)\big)$, which is odd. But $\phi_i(x, y)$ states that $1 + x \,\mathrm{N}(y^{-1} + \alpha_i c)$ is equal to $a^2 - \Delta b^2$. The latter however has even valuation in $\mathfrak{r}$ since it is a norm, so we found our contradiction.

To prove part 2 of the theorem, we assume x and y satisfy all the given conditions.

We claim that $\phi_i(x, y)$ $(i = 0, 1)$ will be true if the following quadratic form is isotropic:

$$Q_i(a, b, c, d) = (1 + xy^{-2}) d^2 + xy^{-1} \,\mathrm{Tr}(\alpha_i) cd + x \,\mathrm{N}(\alpha_i) c^2 - a^2 + \Delta b^2 \tag{2}$$

Indeed, if Q_i is isotropic but $\phi_i(x, y)$ does not hold, then Q_i must have a solution with d equal to zero:

$$x \,\mathrm{N}(\alpha_i) c^2 - a^2 + \Delta b^2 = 0$$

Now choose a prime $\mathfrak{r} \in R(L/K)$ for which $v_{\mathfrak{r}}(x)$ is odd. Then $v_{\mathfrak{r}}(x \,\mathrm{N}(\alpha_i) c^2)$ will be odd, but $v_{\mathfrak{r}}(a^2 - \Delta b^2)$ is even, which gives a contradiction.

It remains to prove that Q_i $(i = 0, 1)$ is isotropic in K, or by applying the theorem of Hasse–Minkowski (cf. theorem 6) that Q_i is isotropic over every completion of K. We check this by considering all possible primes in M_K.

Case 1: $\mathfrak{a} \in A(L/K)$

$K_{\mathfrak{a}} \cong \mathbb{R}$ or $\mathbb{C}$. Set $d = 0$, $c = \frac{1}{\sqrt{x}}$ and a and b such that $\alpha_i = a + b\sqrt{\Delta}$. It follows that $Q_i(a,b,c,d) = 0$.

Case 2: $\mathfrak{p} \in P(L/K)$

Take $\mathfrak{P}$ as one of the two primes in M_L lying over $\mathfrak{p}$. Since $L = K(\sqrt{\Delta})$ and $L_{\mathfrak{P}} = K_{\mathfrak{p}}$ it follows that Δ is a square in $K_{\mathfrak{p}}$. This means that the form $\langle -1, \Delta \rangle$, which is a subform of Q_i, is isotropic in $K_{\mathfrak{p}}$. So also Q_i is isotropic in $K_{\mathfrak{p}}$.

Case 3: $\mathfrak{r} \in R(L/K)$

Suppose $v_{\mathfrak{r}}(x)$ is even. We know that $v_{\mathfrak{r}}\big(\mathrm{N}(\alpha_i)\big)$ will also be even, so we can write $x\,\mathrm{N}(\alpha_i) = \pi_{\mathfrak{r}}^{2m} u$ with $v_{\mathfrak{r}}(u) = 0$. If we set $d = 0$ and $c = \pi_{\mathfrak{r}}^{-m}$, then the first three terms of (2) will be equal to the unit u. Since every unit in $K_{\mathfrak{r}}$ is a norm of the extension $L_{\mathfrak{R}}$, there exist elements a and b in $L_{\mathfrak{R}}$ such that $u = \mathrm{N}(a + b\sqrt{\Delta})$. This proves that Q_i is isotropic.

If $v_{\mathfrak{r}}(x)$ is odd, it is given that $v_{\mathfrak{r}}(xy^{-2}) > 0$. This implies that $v_{\mathfrak{r}}(1 + xy^{-2}) = 0$, so $1 + xy^{-2}$ is a unit. If we set $c = 0$, we can conclude as above that Q_i is isotropic.

Case 4: $\mathfrak{s} \in S(L/K)$

Setting $d = 0$ and $c = 1$ in Q_i yields the equation $x\,\mathrm{N}_{L_{\mathfrak{S}}/K_{\mathfrak{s}}}(\alpha_i) = \mathrm{N}_{L_{\mathfrak{S}}/K_{\mathfrak{s}}}(a + b\sqrt{\Delta})$. If we write this as

$$x = \mathrm{N}_{L_{\mathfrak{S}}/K_{\mathfrak{s}}}\left(\frac{a + b\sqrt{\Delta}}{\alpha_i}\right)$$

we see that this will always have a solution, because by assumption x is a norm from $L_{\mathfrak{S}}$ over $K_{\mathfrak{s}}$, and $a + b\sqrt{\Delta}$ represents all elements of $L_{\mathfrak{S}} = K_{\mathfrak{s}}(\sqrt{\Delta})$.

□

Remark. Proposition 8 applied to $K = \mathbb{Q}$ and $L = \mathbb{Q}(i)$ is a direct generalistation of the existenial divisibility lemma proven by Pheidas in [Phe00]. In the ramified primes, only the prime 2 in that case, Pheidas formulates alternatives for condition 2d (x being a local norm). It would be possible to formulate such alternatives in the general case. We did not work this out explicitly since in theorem 13 all conditions in the ramified primes will be removed.

We also like to point out that condition 2a, the existence of an inert prime where x has an odd value, is not necessary. Even without this condition one can show that if the quadratic form (2) is isotropic there also is a zero (a, b, c, d) with $d = 1$. Since removing this condition would not substantially simplify the following section, we preferred to keep the formulation of the lemma analogous to that of Pheidas.

4 Removing all extra conditions

In this section we will prove a version of the existential divisibility lemma without the local conditions (2a), (2c) and (2d). from proposition 8. This way we will find a formula which is equivalent with *For all primes* $\mathfrak{r}$ *in* $R(L/K)$ *for which* $v_{\mathfrak{r}}(x)$ *is odd, it holds that* $v_{\mathfrak{r}}(xy^{-2}) > 0$.

As an application of this, we give an existential definition of the set of elements of K having non-negative valuation in a prime.

Lemma 10. *There exists a number* k *and elements* $u_1, \ldots, u_k \in K$ *with* $v_{\mathfrak{r}}(u_i) \geq 0$ *for all* $\mathfrak{r} \in R(L/K)$*, such that the following holds:*

Take any finite set $T \subset R(L/K)$ *and consider the semi-local ring* $\mathcal{O}_T = \cap_{\mathfrak{t} \in T}(\mathcal{O}_{\mathfrak{t}} \cap K)$*. Every* $x \in \mathcal{O}_T$ *can be written as*

$$x = u_1 x_1^2 + u_2 x_2^2 + \cdots + u_k x_k^2$$

with $x_i \in \mathcal{O}_T \setminus \{0\}$.

Proof. Here we need to give a different arguments for K a global function field and for K a number field.

Let K be a global function field of characteristic not 2. Let L and T be as in the statement of the theorem and let $x \in \mathcal{O}_T$. Choose $y \in \mathcal{O}_T$ such that $y \neq \pm 1$ and $x + y \neq \pm 1$ (this is possible since $\mathcal{O}_T$ is infinite). Then

$$x = \left(\frac{x+y+1}{2}\right)^2 - \left(\frac{x+y-1}{2}\right)^2 + \left(\frac{y-1}{2}\right)^2 - \left(\frac{y+1}{2}\right)^2$$

Since $\frac{1}{2} \in \mathcal{O}_T$ we see that every $x \in \mathcal{O}_T$ is equal to an alternating sum of four non-zero squares in $\mathcal{O}_T$. It follows that the lemma holds in this case with $k = 4$ and $u_1 = u_3 = 1$, $u_2 = u_4 = -1$.

To prove the lemma in the number field case we first note that every integer $x \in \mathbb{Z}$ is represented over $\mathbb{Z}$ by the quadratic form $x_1^2 - x_2^2 + x_3^2 - x_4^2$. Namely if x is odd choose $y \in \mathbb{Z}$ such that $x + 4y \neq \pm 1$ and $y \neq \pm 1$, then

$$x = \left(\frac{x+4y+1}{2}\right)^2 - \left(\frac{x+4y-1}{2}\right)^2 + (y-1)^2 - (y+1)^2 .$$

If x is even choose $y \in \mathbb{Z}$ such that y is odd, $x + y \neq \pm 1$ and $y \neq \pm 1$, then

$$x = \left(\frac{x+y+1}{2}\right)^2 - \left(\frac{x+y-1}{2}\right)^2 + \left(\frac{y-1}{2}\right)^2 - \left(\frac{y+1}{2}\right)^2 .$$

Note that in these representations of $x \in \mathbb{Z}$ all the coordinates are non-zero.

We know that the ring of integers $\mathcal{O}_K$ of K is a finitely generated $\mathbb{Z}$-module, say

$$\mathcal{O}_K = a_1\mathbb{Z} + a_2\mathbb{Z} + \cdots + a_n\mathbb{Z}.$$

Set $k = 4n$ and for the u_i's we take $a_1, -a_1, a_1, -a_1, a_2, -a_2, a_2, -a_2 \ldots, a_n, -a_n, a_n, -a_n$. Since any integer is represented with non-zero coordinates by the form $x_1^2 - x_2^2 + x_3^2 - x_4^2$ it follows that every element of $\mathcal{O}_K$ is represented with non-zero coordinates by the form $u_1x_1^2 + u_2x_2^2 + \cdots + u_{4n}x_{4n}^2$.

Now consider $\mathcal{O}_T$ with T a finite subset of $R(L/K)$. Every x in $\mathcal{O}_T$ can be written as y/z with y and z in $\mathcal{O}_K$. And since $\mathcal{O}_T$ is a principal ideal domain we may assume that $v_\mathfrak{t}(z) = 0$ for all $\mathfrak{t} \in T$. It follows from the above that $yz = u_1x_1^2 + \cdots + u_kx_k^2$, with $x_1, \ldots, x_k$ non-zero elements of $\mathcal{O}_K$. Then

$$x = \frac{yz}{z^2} = u_1\left(\frac{x_1}{z}\right)^2 + \cdots + u_k\left(\frac{x_k}{z}\right)^2$$

For all $i = 1, \ldots, k$ and $\mathfrak{t} \in T$ we have $x_i/z \neq 0$ and $v_\mathfrak{t}(x_i/z) = v_\mathfrak{t}(x_i) \geq 0$, which means that $x_i/z \in \mathcal{O}_T$. □

Definition 11. Given any subset $\Lambda \subseteq K^*$, we define the *support* of Λ to be

$$\operatorname{supp}(\Lambda) = \{\mathfrak{p} \in M_K \mid \exists\lambda \in \Lambda : |\lambda|_\mathfrak{p} \neq 1\}$$

If Λ is finite, then $\operatorname{supp}(\Lambda)$ will also be finite.

Choose four primes $\mathfrak{r}_1, \mathfrak{r}_2, \mathfrak{r}_3, \mathfrak{r}_4$ in $R(L/K)$ and define the following finite set of primes:

$$Q = \{\mathfrak{r}_1, \mathfrak{r}_2, \mathfrak{r}_3, \mathfrak{r}_4\} \cup S(L/K) \cup A_{\mathrm{ns}}(L/K)$$

Let T be any finite subset of $R(L/K) \setminus Q$ and $\Lambda_{Q,T}$ the subset of K^* parameterizing ${}_2\mathrm{Br}^Q(L/K)$ as given in lemma 7. By construction of $\Lambda_{Q,T}$ it holds that $\operatorname{supp}(\Lambda_{Q,T}) \cap T = \emptyset$.

Lemma 12. *Let $\Lambda = \Lambda_{Q,T}$ be the set as defined above. There exists an existential formula $\psi_\Lambda(x, y)$ such that:*

1. *Let x and y be elements of K^* for which $\psi_\Lambda(x, y)$ is true. If $\mathfrak{r}$ is any prime in $R(L/K) \setminus \operatorname{supp}(\Lambda)$ such that $v_\mathfrak{r}(x)$ is odd, then $v_\mathfrak{r}(xy^{-2}) > 0$.*
2. *Suppose x and y are elements of K^* such that for every $\mathfrak{r} \in R(L/K)$ with $v_\mathfrak{r}(x)$ odd, it holds that $v_\mathfrak{r}(xy^{-2}) > 0$. Then $\psi_\Lambda(x, y)$ is true.*

Proof. To construct the formula $\psi_\Lambda(x,y)$, we use the $\phi(x,y)$ obtained in lemma 8, and the u_i from lemma 10. We also set $u_0 = 1$. We define $\psi_\Lambda(x,y)$ as

$$\begin{aligned}
&\exists y_0, y_1, \ldots, y_k, z_0, z_1, \ldots, z_k \in K : \\
&\qquad (y_0 z_0 = 1) \wedge \cdots \wedge (y_k z_k = 1) \wedge \big((u_0 z_0^2 + \cdots + u_k z_k^2) y^2 = 1\big) \\
&\qquad\qquad \wedge \left(\bigvee_{\lambda\in\Lambda} \phi(\lambda x, y_0)\right) \wedge \cdots \wedge \left(\bigvee_{\lambda\in\Lambda} \phi(\lambda x, y_k)\right)
\end{aligned}$$

Note that the first two lines are equivalent with

$$\exists y_0, y_1, \ldots y_k \in K^* : \big(u_0 y_0^{-2} + \cdots + u_k y_k^{-2} = y^{-2}\big)$$

To prove part 1, assume that $\psi_\Lambda(x,y)$ holds. Take any prime $\mathfrak{r} \in R(L/K)\setminus \mathrm{supp}(\Lambda)$ for which $v_\mathfrak{r}(x)$ is odd. $\psi_\Lambda(x,y)$ implies that for all $i = 1, \ldots, k$, $\phi(\lambda_i x, y_i)$ is true for a certain $\lambda_i \in \Lambda$. Because $\mathfrak{r}$ is outside of the support of Λ, we know that $v_\mathfrak{r}(\lambda_i x) = v_\mathfrak{r}(x)$ is odd. But now $\phi(\lambda_i x, y_i)$ implies that $v_\mathfrak{r}(\lambda_i x y_i^{-2}) > 0$, and this valuation is equal to $v_\mathfrak{r}(x y_i^{-2})$. Lemma 10 gave us $v_\mathfrak{r}(u_i) \geq 0$, so we also have $v_\mathfrak{r}(x u_i y_i^{-2}) > 0$. We conclude the proof of part 1 by observing that

$$v_\mathfrak{r}(xy^{-2}) = v_\mathfrak{r}\left(x(u_0 y_0^{-2} + \cdots + u_k y_k^{-2})\right) \geq \min_{i=0}^{k} v_\mathfrak{r}(x u_i y_i^{-2}) > 0$$

For the proof of part 2, suppose we have $x, y \in K^*$ such that for every $\mathfrak{r} \in R(L/K)$ with $v_\mathfrak{r}(x)$ odd, the inequality $v_\mathfrak{r}(xy^{-2}) > 0$ holds.

We can use approximation to get a y_0^{-1} for which the following finitely many conditions are satisfied:

(I) $v_\mathfrak{r}(y_0^{-1}) > v_\mathfrak{r}(y^{-1})$ for all $\mathfrak{r} \in R(L/K) \setminus \{\mathfrak{r}_1, \mathfrak{r}_2, \mathfrak{r}_3, \mathfrak{r}_4\}$ for which $v_\mathfrak{r}(x)$ is odd.

(II) $v_{\mathfrak{r}_j}(y_0^{-1}) > -v_{\mathfrak{r}_j}(x)/2$ for $j = 1, 3$.

(III) $v_{\mathfrak{r}_j}(y_0^{-1} - y^{-1}) = -v_{\mathfrak{r}_j}(2y^{-1}) +$ an even number greater than $\max\left(-v_{\mathfrak{r}_j}(x), 2v_{\mathfrak{r}_j}(2y^{-1})\right)$, for $j = 2, 4$.

We define these sets of primes:

$$\begin{aligned}
T_0 &= \{\mathfrak{r}_1, \mathfrak{r}_3\} \cup \{\mathfrak{r} \in R(L/K) \setminus \{\mathfrak{r}_1, \mathfrak{r}_2, \mathfrak{r}_3, \mathfrak{r}_4\} \mid v_\mathfrak{r}(x) \text{ is odd}\} \\
T_1 = T_2 = \cdots = T_k &= \{\mathfrak{r}_2, \mathfrak{r}_4\} \cup \{\mathfrak{r} \in R(L/K) \setminus \{\mathfrak{r}_1, \mathfrak{r}_2, \mathfrak{r}_3, \mathfrak{r}_4\} \mid v_\mathfrak{r}(x) \text{ is odd}\}
\end{aligned}$$

Claim. *There exist* $y_0, y_1, \ldots, y_k \in K^*$ *such that* $u_0 y_0^{-2} + \cdots + u_k y_k^{-2} = y^{-2}$ *and for all* $0 \le i \le k$ *we have* $v_{\mathfrak{r}}(x y_i^{-2}) > 0$ *for all* $\mathfrak{r} \in T_i$.

Proof of claim. We have already constructed y_0. The case $i = 0$ follows easily from (I) and (II) above, together with the hypotheses of part 2.

For every $\mathfrak{r} \in T_1$ we will prove that $v_{\mathfrak{r}}(y^{-2} - y_0^{-2})$ is even, and $v_{\mathfrak{r}}(y^{-2} - y_0^{-2}) \ge -v_{\mathfrak{r}}(x)$. Set

$$a = y^{-2} - y_0^{-2} = -(y_0^{-1} - y^{-1})((y_0^{-1} - y^{-1}) + 2y^{-1})$$

If $\mathfrak{r}$ is either $\mathfrak{r}_2$ or $\mathfrak{r}_4$,then from (III) it follows that $v_{\mathfrak{r}}(y_0^{-1} - y^{-1}) > v_{\mathfrak{r}}(2y^{-1})$, so

$$v_{\mathfrak{r}}(a) = v_{\mathfrak{r}}(y_0^{-1} - y^{-1}) + v_{\mathfrak{r}}(2y^{-1}) = \text{an even number greater than } -v_{\mathfrak{r}}(x)$$

If $\mathfrak{r}$ is not $\mathfrak{r}_2$ nor $\mathfrak{r}_4$, we know that $v_{\mathfrak{r}}(x)$ is odd and the hypotheses say that $v_{\mathfrak{r}}(y^{-2}) > -v_{\mathfrak{r}}(x)$. Then (I) implies that $v_{\mathfrak{r}}(a) = v_{\mathfrak{r}}(y^{-2} - y_0^{-2}) = v_{\mathfrak{r}}(y^{-2})$ is even and $v_{\mathfrak{r}}(a) > -v_{\mathfrak{r}}(x)$.

Now we use approximation to find a $\mu \in K$ for which

$$v_{\mathfrak{r}}(\mu) = -v_{\mathfrak{r}}(a)/2 \qquad \text{for all } \mathfrak{r} \in T_1.$$

This way $\mu^2 a$ is in the ring $\mathcal{O}_{T_1}$, and by applying lemma 10 for this ring, we write $\mu^2 a$ as

$$\mu^2 a = u_1 w_1^2 + \cdots + u_k w_k^2.$$

If we set $y_i^{-1} = w_i/\mu$, then $v_{\mathfrak{r}}(y_i^{-2}) = 2v_{\mathfrak{r}}(w_i) - 2v_{\mathfrak{r}}(\mu) \ge 0 + v_{\mathfrak{r}}(a) > -v_{\mathfrak{r}}(x)$ for $\mathfrak{r} \in T_1 = T_i$.

This concludes the proof of the claim.

Using this, we will show that $\bigvee_{\lambda \in \Lambda} \phi(\lambda x, y_0)$ is true. The argument proving that $\bigvee_{\lambda \in \Lambda} \phi(\lambda x, y_i)$ is true for $i = 1, \ldots k$ is completely analogous but with the role of the pairs $\{\mathfrak{r}_1, \mathfrak{r}_3\}$ and $\{\mathfrak{r}_2, \mathfrak{r}_4\}$ exchanged.

We make a subset Q_0 of Q of even cardinality. We start by taking the primes in $\{\mathfrak{r}_2, \mathfrak{r}_4\} \cup S(L/K) \cup A_{\mathrm{ns}}(L/K)$ for which x is not a local norm. We add $\mathfrak{r}_1$ to Q_0 if x is a norm from $L_{\mathfrak{R}_1}$. If necessary, we add $\mathfrak{r}_3$ to make sure Q_0 has an even number of elements. If we take the $\lambda \in \Lambda$ such that λ is a local norm everywhere, except for the primes in Q_0, then λx will have the following properties:

- λx is a local norm for all primes in $S(L/K) \cup A_{\mathrm{ns}}(L/K)$.
- $v_{\mathfrak{r}_1}(\lambda x)$ is odd.

- $v_{\mathfrak{r}_2}(\lambda x)$ is even and $v_{\mathfrak{r}_4}(\lambda x)$ is even.
- $v_{\mathfrak{r}}(\lambda x) \equiv v_{\mathfrak{r}}(x) \mod 2$ for all $\mathfrak{r} \in R(L/K) \setminus \{\mathfrak{r}_1, \mathfrak{r}_2, \mathfrak{r}_3, \mathfrak{r}_4\}$.

We will now prove that $\phi(\lambda x, y_0)$ is true for this $\lambda \in \Lambda$. The choice of λ already implies conditions 2a, 2c and 2d for part 2 of lemma 8.

In order to prove condition 2b, take any prime $\mathfrak{r} \in R(L/K)$ for which $v_{\mathfrak{r}}(\lambda x)$ is odd. We see that $\mathfrak{r}$ cannot be $\mathfrak{r}_2$ or $\mathfrak{r}_4$. If $\mathfrak{r}$ is not $\mathfrak{r}_1$ nor $\mathfrak{r}_3$, the fact that $v_{\mathfrak{r}}(\lambda x)$ is odd implies that $v_{\mathfrak{r}}(x)$ is odd. In any case we have $\mathfrak{r} \in T_0$. Hence $v_{\mathfrak{r}}(\lambda x y_0^{-2}) \geq v_{\mathfrak{r}}(x y_0^{-2}) > 0$ by the preceding claim. □

The previous lemma is a form of the existential divisibility lemma without conditions in the real primes and ramifying primes. However, in one direction, it does not work for primes in $\operatorname{supp}(\Lambda_{Q,T})$. By applying the lemma two times for well chosen sets $\Lambda_{Q,T}$ and $\Lambda_{Q',T'}$, we can solve this problem and obtain the main theorem.

Theorem 13. *There is an existential formula $\Omega(x, y)$ which is equivalent with the formula*

$$\forall \mathfrak{r} \in R(L/K) : \big(v_{\mathfrak{r}}(x) \text{ odd } \to v_{\mathfrak{r}}(xy^{-2}) > 0\big) \tag{3}$$

Proof. Take eight different primes $\{\mathfrak{r}_1, \mathfrak{r}_2, \mathfrak{r}_3, \mathfrak{r}_4, \mathfrak{r}'_1, \mathfrak{r}'_2, \mathfrak{r}'_3, \mathfrak{r}'_4\}$ in $R(L/K)$, and define Q as $\{\mathfrak{r}_1, \mathfrak{r}_2, \mathfrak{r}_3, \mathfrak{r}_4\} \cup S(L/K) \cup A_{\text{ns}}(L/K)$. Take $T = \{\mathfrak{r}'_1, \mathfrak{r}'_2, \mathfrak{r}'_3, \mathfrak{r}'_4\}$ and let $\Lambda = \Lambda_{Q,T}$ be the corresponding set parameterizing ${}_2\mathrm{Br}^Q(L/K)$.

Let $Q' = \{\mathfrak{r}'_1, \mathfrak{r}'_2, \mathfrak{r}'_3, \mathfrak{r}'_4\} \cap S(L/K) \cap A_{\text{ns}}(L/K)$ and take $T' = \{\mathfrak{r}_1, \mathfrak{r}_2, \mathfrak{r}_3, \mathfrak{r}_4\} \cup (\operatorname{supp}(\Lambda_{Q,T}) \cap R(L/K))$. Since $T' \cap Q' = \emptyset$ by the choice of T, the parameterizing set $\Lambda' = \Lambda_{Q',T'}$ is defined. Note that the choice of T' now implies $R(L/K) \cap \operatorname{supp}(\Lambda_{Q,T}) \cap \operatorname{supp}(\Lambda_{Q',T'}) = \emptyset$.

Now we define

$$\Omega(x, y) \leftrightarrow \psi_{\Lambda}(x, y) \wedge \psi_{\Lambda'}(x, y)$$

Suppose $\Omega(x, y)$ is true. $\psi_{\Lambda}(x, y)$ says that $v_{\mathfrak{r}}(x)$ odd implies $v_{\mathfrak{r}}(xy^{-2}) > 0$ for $\mathfrak{r} \in R(L/K) \setminus \operatorname{supp}(\Lambda)$. $\psi_{\Lambda'}(x, y)$ says the same thing for $\mathfrak{r} \in R(L/K) \setminus \operatorname{supp}(\Lambda')$. Because $R(L/K) \cap \operatorname{supp}(\Lambda) \cap \operatorname{supp}(\Lambda') = \emptyset$, we have it for all $\mathfrak{r}$ in $R(L/K)$.

If (3) is satisfied, then we know by lemma 12 that $\psi_{\Lambda}(x, y)$ and $\psi_{\Lambda'}(x, y)$ are both true. □

As mentioned in the introduction our motivation for theorem 13 finds its origin in Pheidas' paper [Phe00]. The next corrolary shows that the theorem also generalises the fact that in a global field the elements integral in a prime $\mathfrak{p}$ form a diophantine set. This result in different cases is due to different authors as indicated in the introduction of chapter 5 in [Eis03], there one also finds a uniform proof for this fact based on Hilbert's reciprocity law for the Brauer group of a global field.

Corollary 14. *For every non-archimedean prime $\mathfrak{p} \in M_K$, the set $\{z \in K \mid v_\mathfrak{p}(z) \geq 0\}$ is diophantine.*

Proof. Let $\mathfrak{p} \in M_K$ be a non-archimedean prime. Choose an other non-archimedean prime $\mathfrak{q} \neq \mathfrak{p}$. Choose L/K a quadratic extension such that $\mathfrak{p} \in R(L/K)$ and $\mathfrak{q} \in S(L/K)$. To see that such an extension exists, let $K_\mathfrak{p}(\alpha_\mathfrak{p})$ be the unique quadratic unramified extension of $K_\mathfrak{p}$ and $K_\mathfrak{q}(\beta_\mathfrak{q})$ a totally ramified extension of degree two of $K_\mathfrak{q}$. Let $X^2 + a_{\mathfrak{p},1}X + a_{\mathfrak{p},2}$ be the minimal polynomial of $\alpha_\mathfrak{p}$ over $K_\mathfrak{p}$ and $X^2 + b_{\mathfrak{q},1}X + b_{\mathfrak{q},2}$ be the minimal polynomial of $\beta_\mathfrak{q}$ over $K_\mathfrak{q}$. Then lemma (33.8) in [Rei75] states that if c_1 and c_2 are taken sufficiently close to $a_{\mathfrak{p},1}$ and $b_{\mathfrak{q},1}$, respectively $a_{\mathfrak{p},2}$ and $b_{\mathfrak{q},2}$, the polynomial $f(X) = X^2 + c_1X + c_2$ is separable and irreducible over K having a root in $K_\mathfrak{p}$ and in $K_\mathfrak{q}$. It follows that $K(\gamma)$, with $f(\gamma) = 0$, is a quadratic extension of K with the desired properties.

Let $\omega \in {}_2\mathrm{Br}(K)$ such that $\mathrm{inv}_\mathfrak{p}\,\omega \equiv 1 \bmod 2$, $\mathrm{inv}_\mathfrak{q}\,\omega \equiv 1 \bmod 2$ and $\mathrm{inv}_\mathfrak{r}\,\omega \equiv 0 \bmod 2$ for all primes $\mathfrak{r} \neq \mathfrak{p}, \mathfrak{q}$. (Such an element ω exists by Hilbert's reciprocity law). By construction L is a splitting field of ω. So $\omega = (\gamma, x)$ with $L = K(\gamma)$. It follows from the choice of L and ω that $v_\mathfrak{p}(x)$ is odd and $v_\mathfrak{r}(x)$ is even for all $\mathfrak{r} \in R(L/K) \setminus \{\mathfrak{p}\}$. After multiplying x with a suitable square, we may assume that $v_\mathfrak{p}(x) = 1$. Now apply theorem 13 with this fixed x. Then $\Omega(x, y)$ is equivalent with "$v_\mathfrak{p}(xy^{-2}) > 0$", or "$v_\mathfrak{p}(y^{-1}) > -v_\mathfrak{p}(x)/2$". If we set $y = z^{-1}$ and use the fact that $v_\mathfrak{p}(x) = 1$, we find that $\Omega(x, z^{-1})$ is equivalent with "$v_\mathfrak{p}(z) \geq 0$". □

References

[Eis03] Kirsten Eisenträger, *Hilbert's tenth problem and arithmetic geometry*, Ph.D. thesis, University of California at Berkeley, 2003.

[Neu92] Jürgen Neukirch, *Algebraische zahlentheorie*, Springer, 1992.

[O'M63] Timothy O'Meara, *Introduction to quadratic forms*, Springer, 1963.

[Phe91] Thanases Pheidas, *Hilbert's tenth problem for rational function fields over finite fields*, Invent. Math. **103** (1991), 1–8.

[Phe00] ———, *An effort to prove that the existential theory of $\mathbb{Q}$ is undecidable*, Contemporary Mathematics **270** (2000), 237–252.

[Rei75] Irving Reiner, *Maximal orders*, London Academic Press, 1975.

[Sch85] Winfried Scharlau, *Quadratic and hermitian forms*, Grundlehren Math. Wiss., no. 270, Springer Berlin, 1985.

[Shl96] Alexandra Shlapentokh, *Diophantine undecidability over algebraic function fields over finite fields of constants*, J. Number Theory **58** (1996), 317–342.

[Vid94] Carlos Videla, *Hilbert's tenth problem for rational function fields in characteristic 2*, Proc. Amer. Math. Soc. **120** (1994), 249–253.

[VZ03] Jan Van Geel and Karim Zahidi, *Quadratic forms and divisibility*, Mini-Workshop: Hilbert's 10th problem, Mazur's conjecture and divisibility sequences, Oberwolfach January 19–25, 2003.