FIRST ORDER DECIDABILITY AND DEFINABILITY OF INTEGERS IN INFINITE ALGEBRAIC EXTENSIONS OF RATIONAL NUMBERS

ALEXANDRA SHLAPENTOKH

Abstract. We extend results of Videla and Fukuzaki to define algebraic integers in large classes of infinite algebraic extensions of $\mathbb{Q}$ and use these definitions for some of the fields to show first-order undecidability. In particular, we show that the following propositions hold. (1) For any rational prime $q$ and any positive rational integer $m$, algebraic integers are definable in any Galois extension of $\mathbb{Q}$ where the degree of any finite subextension is not divisible by $q^m$. (2) Given a prime $q$, and an integer $m > 0$, algebraic integers are definable in a cyclotomic extension (and any of its subfields) generated by any set $\{\zeta_p | \ell \in \mathbb{Z}_{>0}, p \neq q \text{ is any prime such that } q^m + 1 \not| (p−1)\}$. (3) The first-order theory of any abelian extension of $\mathbb{Q}$ with finitely many ramified rational primes is undecidable.

1. Introduction

The purpose of this paper is to consider the following problems of definability and decidability for an infinite algebraic extension $K_{\text{inf}}$ of $\mathbb{Q}$.

Question 1.1. Is the ring of integers of $K_{\text{inf}}$ first-order definable over $K_{\text{inf}}$?

Question 1.2. Is the first-order theory of $K_{\text{inf}}$ decidable?

The questions of this type have a long history, especially as applied to number fields and in connection to generalizations of Hilbert’s Tenth Problem. We will not attempt to give a full accounting of the work done in the subject here but will limit ourselves to pointing out some surveys as well as results specifically relevant to this paper.

Perhaps a good place to start is results of Julia Robinson who proved in [25] and [20] that in any number field the ring of integers of the number field as well as the ring of rational integers are first-order definable in the language of rings, and therefore the first-order theory of these fields (in the language of rings) is undecidable. In the process of proving these results Julia Robinson also proved that integrality at a prime of a number field is existentially definable in the language of rings over a number field. Robert Rumely in [30] improved Julia Robinson’s result making the definition of the ring of integers uniform across number fields. More recently, Bjorn Poonen in [22] and Jochen Koenigsmann in [12] updated Julia Robinson’s definition of integers by reducing the number of universal quantifiers used in these definitions, Poonen to two and Koenigsmann to one.

Date: May 2, 2014.

2000 Mathematics Subject Classification. Primary 11U05; Secondary 11G05.

Key words and phrases. Hilbert’s Tenth Problem, Diophantine definition, First-Order Definition.

The research for this paper has been partially supported by NSF grants DMS-0650927 and DMS-1161456, and a grant from John Templeton Foundation.
The desire to reduce the number of universal quantifiers is motivated to large extent by the interest in extending Hilbert’s Tenth Problem to $\mathbb{Q}$. This would be accomplished by a purely existential definition of $\mathbb{Z}$ over $\mathbb{Q}$. Unfortunately there are serious doubts as to whether such a definition exists. See [6], [33], and [21] for surveys on Hilbert’s Tenth Problem and related questions of definability.

A lot of work aiming to prove the decidability of the first-order theory has centered around various infinite extensions of $\mathbb{Q}$. (See [6] for a survey of these results.) One of the more influential results was arguably due to Robert Rumely in [31], where he showed that Hilbert’s Tenth Problem is decidable over the ring of all algebraic integers. This result was strengthened by Van der Dries proving in [39] that the first-order theory of this ring was decidable. Another remarkable result is due to Michael Fried, Dan Haran and Helmut Völklein in [10], where it is shown that the first-order theory of the field of all totally real algebraic numbers is decidable. This field constitutes a boundary of sorts between the “decidable” and “undecidable”, since Julia Robinson showed in [27] that the first-order theory of the ring of all totally real integers is undecidable. In the same paper, she also proved that the first-order theory of a family of totally real rings of integers is undecidable and produced a “blueprint” for such proofs over rings of integers which are not necessarily totally real.

Using an elaboration of Julia Robinson’s “blueprint” by C. Ward Henson (see page 199 of [39]) and Rumely’s method for defining integrality at a prime, Carlos Videla produced the first-order undecidability result for a family of infinite algebraic extensions of $\mathbb{Q}$ in [10] and [11]. More specifically, Videla showed that the first-order theory of any infinite cyclotomic extension with a single ramified prime and some infinite cyclotomic extensions with finitely many ramified primes is undecidable. Videla also produced the first result concerning definability of the ring integers over an infinite algebraic extension of $\mathbb{Q}$ by generalizing a technique of Rumely: he showed that if all finite subextensions are of degree equal to a product of powers of a fixed (for the field) finite set of primes, then the ring of integers is first-order definable over the field.

In a very recent paper [11], Kenji Fukuzaki, generalizing further Rumley’s method, proved that a ring of integers is definable over an infinite Galois extension of the rationals such that every finite subextension has odd degree over the rationals and its prime ideals dividing 2 are unramified. He then used one of the results of Julia Robinson to show that a large family of totally real fields contained in cyclotomics (with infinitely many ramified primes) has an undecidable first-order theory.

In this paper we generalize results of Videla and Fukuzaki to show that algebraic integers are definable in a much larger class of infinite algebraic extensions of $\mathbb{Q}$ including a large class of cyclotomics with infinitely many ramified primes. (This result does not follow from results of Fukuzaki since cyclotomics with infinitely many ramified primes have finite subextension of degree which is an arbitrarily high power of 2. Further, we can also include cyclotomics where dyadic ideals are ramified since we don’t have to treat prime 2 in any special way.) We call the fields to which we can apply our definability results “$q$-bounded”, with $q$ ranging over the set of rational prime numbers. We define the fields of this type in Definition 3.2. Essentially we need the relative and ramification degrees (or alternatively the local degrees) not to be uniformly divisible by arbitrarily high powers of $q$ as we progress through the extension. In the case of an infinite Galois extension this often amounts to not having cyclic subextensions of degrees divisible by arbitrarily high powers of $q$ and a similar condition...
on ramification degrees, but in the case extensions are not Galois many other examples are possible, as we describe in Section 5. The general definability results are in Theorems 4.10–4.13.

As Fukuzaki we obtain first-order undecidability results using results of Julia Robinson for totally real fields. However we are also able to use existential undecidability results previously obtained by the author to show that the first order theory of fields and rings of integers of any abelian extension with finitely many ramified primes is undecidable, thus extending results of Videla. The undecidability results are in Theorems 6.6 and 6.8 and Corollary 6.10.

To obtain our main definability results we use a modification of Rumely’s method of norm equations. Ultimately our approach is based on defining “divisibility of order”. In other words, indirectly, one gives a definition of the set of algebraic numbers with the order of every pole divisible by a fixed prime number $q$.

We also consider the issue of defining integrality at a single prime in an infinite extension and the use of finitely generated elliptic curves (see Theorem 7.5) to get first-order undecidability of the field. As a result of this discussion one observes that if the first-order theory of a field is decidable and there exists at least one rational prime which is completely $q$-bounded for some $q$, then any elliptic curve defined over the field either has rank 0 or is not finitely generated. We give an example of such a field in Section 7.

The paper is structured in the following manner. In Section 2 we describe most of the algebraic number theory necessary to establish our results. In Section 3 we discuss the conditions on primes we need to carry out our proofs over infinite extension. This is where we introduce the notion of a field being “$q$-bounded”. Section 4 completes the construction of first-order definitions of the rings of algebraic integers in specified infinite algebraic extensions of $\mathbb{Q}$, and Section 5 contains various example of fields satisfying the requirements for our definitions. Section 6 uses definitions of integers to produce undecidability results for the fields. Finally, Section 7 explains how to use finitely generated elliptic curves to obtain definitions of rational integers.

2. Some Algebraic Number Theory

In this section we show how to define a set of elements of a number field containing all integers and such that all non-integers in the set have negative orders (poles) of order divisible by a given prime number $q$ only. We start with a set of notation.

**Notation and Assumptions 2.1.** The following notation are used throughout the rest of the paper.

- Let $q$ be a rational prime number.
- Let $\xi_q$ be a primitive $q$-th root of unity.
- Let $K,F,G,L$ denote algebraic extensions of $\mathbb{Q}$.
- For a number field $G$, let $p_G, q_G, t_G, a_G$ be distinct non-archimedean primes of $G$.
- If $L$ is any finite extension of a number field $G$, then $p_L, q_L, t_L, a_L$ denote primes above $p_G, q_G, t_G, a_G$ respectively.
- For $L$ and $G$ as above, let $\mathcal{C}_L(p_G)$ denote the set of all $L$-primes above $p_G$.
- If $K$ is a number field and $x \in K$ (or any other number field) and $\text{ord}_{p_K} x > 0$, we say by analogy with function fields that $x$ has a zero at $p_K$. Similarly, if $\text{ord}_{p_K} x < 0$, we say that $x$ has a pole at $p_K$. 


If $\mathcal{S}_K$ is a set of non-archimedean primes of $K$, then we let $O_{K,\mathcal{S}_K}$ denote a subring of $K$ containing all the elements of $K$ without any poles at primes outside $\mathcal{S}_K$.

For $x, b, z \in K \setminus \{0\}$, $c \in K$ let

$$M_x(K, q) = K(\sqrt{1 + z^{-1}}),$$

$$N_{x,b,z}(K, q) = M_x(K, q)(\sqrt{1 + (bx^i + b^q)^{-1}}),$$

$$L_{c,x,b,z}(K, q) = N_{x,b,z}(K, q)(\sqrt{1 + (c + c^{-1})z^{-1}}),$$

Let $\bar{Q}$ be the algebraic closure of $Q$.

If $K$ is a number field, then for any prime $p_K$, let $K_{p_K}$ be the completion of $K$ under the $p_K$-adic topology.

The next lemma is a variation on a theme from [1].

**Lemma 2.2.** If $H$ is any algebraic extension of $Q$ with finitely many embeddings into $\bar{Q} \cap \mathbb{R}$, and $\sigma$ is any such embedding, then the set $\{u \in H : \sigma(u) \geq 0\}$ is Diophantine over $H$.

*Proof.* If $\sigma_1, \ldots, \sigma_k$ are all the distinct embeddings of $H$ into $\bar{Q} \cap \mathbb{R}$, then for any pair $\sigma_i \neq \sigma_j$ for some $x_{i,j} \in H$, it is the case that $\sigma_i(x_{i,j}) \neq \sigma_j(x_{i,j})$. Let $M = Q(x_{i,j}, i \neq j \in \{1, \ldots, k\})$, and observe that $M \subset H$. For any $i \in \{1, \ldots, k\}$, let $\hat{\sigma}_i$ be the restriction of $\sigma_i$ to $M$ and note that $\hat{\sigma}_i \neq \hat{\sigma}_j$ and each $\hat{\sigma}_i$ has only one extension to $H$. For every $i \in \{1, \ldots, k\}$, by the Weak Approximation Theorem we can find an algebraic integer $c_i \in M$ such that $\sigma_i(c_i) = \hat{\sigma}_i(c_i) > 0$ and $\sigma_j(c_i) = \hat{\sigma}_j(c_i) < 0$, $j \neq i$. Now by Hasse-Minkowskii Theorem and the fact that over a local field a quaternion form is universal, we see that

$$\{x \in H|\sigma_i(x) \geq 0\} = \{x \in L|x = x_1^2 + x_2^2 + c_i x_3^2 + x_4^2\}.$$ 

$\square$

If we are interested in elements whose images under real embeddings are always non-negative, we do not need an assumption on the finite number of real embeddings. The proof of the lemma below, as above, follows from Hasse-Minkowskii Theorem and the fact that over a local field a quaternion form is universal.

**Lemma 2.3.** If $H$ is any algebraic extension of $Q$, then the set $\{x \in H|x = x_1^2 + x_2^2 + x_3^2 + x_4^2\}$ is exactly the set of all elements of $H$ such that for any embedding $\sigma$ of $H$ into $Q$ with $\sigma(H) \subset \mathbb{R} \cap \bar{Q}$ we have that $\sigma(x) \geq 0$.

We now add to our notation list.

**Notation 2.4.** Let $\Omega_2(K)$ be the set of all the elements $c$ of $K$ such that for any embedding $\sigma$ of $K$ into $\bar{Q}$ we have that $\sigma(K) \subset \mathbb{R} \cap \bar{Q}$ implies $\sigma(x) \geq 0$. For $q > 2$, let $\Omega_q(K) = K$.

**Remark 2.5.** If $K/M$ is an algebraic extension and $c \in \Omega_2(M)$, then $c \in \Omega_2(K)$. However, $\Omega_2(K) \cap M \neq \Omega_2(M)$ in all cases, since there can be an embedding of $K$ into $\bar{Q}$ which is not real but the restriction to the image of $M$ is real. At the same time, if $K_{\text{inf}}$ is an infinite algebraic extension of $M$ and $c \in \Omega_2(K_{\text{inf}}) \cap M$, then for some finite extension $N$ of $M$ with $N \subset K_{\text{inf}}$, for all $K$ such that $N \subseteq K \subset K_{\text{inf}}$, we have $c \in \Omega_2(K)$.

Next we state Hensel’s lemma and its corollary which play an important role.
Lemma 2.6. If $K$ is a number field, $f(X) \in K_{pk}[X]$ has coefficients integral at $p_K$ and for some $\alpha \in K_{pk}$ integral at $p_K$ we have that $\text{ord}_{p_K} f(\alpha) > 2 \text{ord}_{p_K} f'(\alpha)$, then $f(X)$ has a root in $K_{pk}$. (See [14]/Proposition 2, Section 2, Chapter II.)

Corollary 2.7. If $K$ is a number field, and $x \equiv 1 \mod q^3$, and $q_K$ is any prime of $K$ dividing $q$, then $x$ is a $q$-th power in $K_{q_K}$.

Proof. Let $f(X) = X^q - x$ and observe that by our assumption on $x$ we have the following:

$$\text{ord}_{q_K} f(1) = \text{ord}_{q_K} (1 - x) = 3e(q_K/q).$$

At the same time $\text{ord}_{q_K} f'(1) = \text{ord}_{q_K} q = e(q_K/q)$ and therefore $\text{ord}_{q_K} f(1) > 2 \text{ord}_{q_K} f'(1)$.

Hence, by Hensel’s lemma $f(x)$ has a root in $K_{q_K}$, making $x$ a $q$-th power. □

The two lemmas below, stated without a proof, list some basic number-theoretic facts.

Lemma 2.8. If $F$ is a number field containing $\xi_q$, $b \in F$ and $b$ is not a $q$-th power in $F$, then the following statements are true.

1. If $\text{ord}_{p_F} q = \text{ord}_{p_F} b = 0$, then $p_F$ does not ramify in the extension $F(\sqrt[q]{b})/F$.
2. If $b$ is not a $q$-th power mod $p_F$, $\text{ord}_{p_F} b = 0$ and $p_F$ does not divide $q$, then $p_F$ does not split (i.e. has only one prime above it) in the extension $F(\sqrt[q]{b})/F$.
3. If $b$ is a $q$-th power mod $p_F$, and $\text{ord}_{p_F} b = 0$, then $p_F$ splits in the extension $F(\sqrt[q]{b})/F$.
4. If $\text{ord}_{p_F} b \neq 0 \mod q$, then $p_F$ ramifies completely in the extension $F(\sqrt[q]{b})/F$.

The second lemma deals with norms and primes in cyclic extensions of degree $q$.

Lemma 2.9. Let $G/F$ be a cyclic extension of degree $q$ of number fields. If $p_F$ is not ramified in the extension, then either it splits completely (in other words into $q$ distinct factors) or it does not split at all. Further if $w = N_{G/F}(z)$ for some $z \in G$, and $p_F$ does not split in the extension, then $\text{ord}_{p_F} w \equiv 0 \mod q$.

The following lemma provides a way to avoid ramification of factors of $q$ while taking $q$-th root.

Lemma 2.10. If $K$ is a number field containing $\xi_q$, a $K$-prime $q_K$ is a factor of $q$ and

$$\text{ord}_{q_K} (c - 1) \geq 3 \text{ord}_{q_K} q,$$

then $q_K$ splits completely in the extension $K(\sqrt[q]{c})/K$.

Proof. By Corollary 2.7 the polynomial $X^q - c$ has a root in $q_K$-adic completion of $K$, and since the field contains the primitive $q$-th root of unity, the polynomial has $q$ distinct roots. Thus, the local degree is one for all the factors above $q_K$. □

We add to our notation list.

Notation 2.11. If $K$ is a number field, and

$$\mathcal{I}_K = \{p_{1,K}, \ldots, p_{l,K}\}$$

is a finite set of primes of $K$, then let $\Theta_q(K, \mathcal{I}_K)$ denote the set of all elements $c$ of $K$ such that the numerator of the divisor of $c - 1$ is divisible by the divisor $\prod_{i=1}^{l} p_{i,K}$ in the semigroup of the integral divisors of $K$. If $\mathcal{I}_K = \emptyset$, then set $\Theta_q(K, \mathcal{I}_K) = K$. Let $\Phi_q(K)$ denote the set of all elements $c$ of $K$ such that the numerator of the divisor of $c - 1$ is divisible by $q^3$. 

5
If $K$ is an infinite extension of $\mathbb{Q}$, and $\mathcal{S}_K$ is a set of valuations of $K$ lying above finitely many primes of $\mathbb{Q}$, then a $K$-element $c$ is in $\Theta_q(K, \mathcal{S}_K)$ if and only if for some number field $M \subset K$ and the set $\mathcal{S}_M$ of primes of $M$ below valuations of $\mathcal{S}_K$ we have that $c \in \Theta_q(M, \mathcal{S}_M)$. Similarly a $K$-element $c \in \Phi_q(K)$ if and only if $c \in \Phi_q(\mathbb{Q}(e))$.

The next two propositions explain the purpose of introducing extensions

$$M_x(K, q), N_{x,b,z}(K, q), L_{c,x,b,z}(K, q) :$$

(1) ramifying all zeros of $x$ and $bx^q + b^q$; (2) ramifying zeros and poles of $c$; (3) avoiding ramifying primes in the cyclic extension where we are going solve norm equations; (4) making sure that zeros of $x$ do not have any influence on whether the norm equation has solutions.

**Proposition 2.12.** If $K$ is a number field containing $\xi_q$, and for some elements $b, c \in K$ and some $K$-prime $p_K$ the following assumptions are true:

1. $p_K$ is not a factor of $q$,
2. $c$ is not a $q$-th power modulo $p_K$ (note that this assumption includes the assumption that $\text{ord}_{p_K} c = 0$),
3. $\text{ord}_{p_K} x < 0$,
4. $\text{ord}_{p_K} b \not\equiv 0 \mod q$,
5. $q \text{ord}_{p_K} x < (q - 1) \text{ord}_{p_K} b$,

then for every prime factor $p_{L_{c,x,b,z}(K,q)}$ of $p_K$ in $L_{c,x,b,z}(K, q)$ we have that

1. $\text{ord}_{p_{L_{c,x,b,z}(K,q)}} x < 0$,
2. $c$ is not a $q$-th power modulo $p_{L_{c,x,b,z}(K,q)}$ and thus not a $q$-th power in $L_{c,x,b,z}(K, q)$,
3. $\text{ord}_{p_{L_{c,x,b,z}(K,q)}} (bx^q + b^q) \not\equiv 0 \mod q$.

**Proof.** First of all we note that

$$L_{c,x,b,z}(K, q) = K(\sqrt[1]{1 + x^{-1}}, \sqrt[1]{1 + (bx^q + b^q)^{-1}}, \sqrt[1]{1 + (c + c^{-1})x^{-1}}).$$

Next, by properties of primes and Assumption 3 we have that $\text{ord}_{p_{L_{c,x,b,z}(K,q)}} x < 0$. By Assumption 4 we have that $\text{ord}_{p_K} b \not\equiv 0 \mod q$. Next we note that

$$\text{ord}_{p_K}(x^{-1}) > 0$$

and therefore by Lemma 2.8 Part 3 we have that $p_K$ splits completely into distinct factors in the extension $M_x(K, q)/K$. (We remind the reader that $M_x(K, q) = K(\sqrt[1]{1 + x^{-1}})$. Thus, in $M_x(K, q)$ we have that $\text{ord}_{p_{M_x(K,q)}} x < 0$, $\text{ord}_{p_{M_x(K,q)}} b \not\equiv 0 \mod q$, and $c$ is not a $q$-th power modulo $p_{M_x(K,q)}$. We now note that by Assumption 5 we have that

$$q \text{ord}_{p_K} x + \text{ord}_{p_K} b < q \text{ord}_{p_K} b,$$

and therefore

$$\text{ord}_{p_{M_x(K,q)}} (bx^q + b^q) = \text{ord}_{p_{M_x(K,q)}} b + q \text{ord}_{p_{M_x(K,q)}} x < 0.$$

Further, by Assumption 4 we have that $\text{ord}_{p_{M_x(K,q)}} (bx^q + b^q) \not\equiv 0 \mod q$. Applying Lemma 2.8 Part 3 again, this time over the field $N_{x,b,z}(K, q) = M_x(K, q)(\sqrt[1]{1 + (bx^q + b^q)^{-1}})$, we see

$$6$$
that in the extension $N_{x,b,x}(K,q)/M_x(K,q)$, the $M_x(K,q)$-prime $p_{M_x(K,q)}$ splits completely into distinct factors and thus $c$ is not a $q$-th power modulo any $p_{N_{x,b,x}(K,q)}$, while
\[
\text{ord}_{p_{N_{x,b,x}(K,q)}}(bx^q + b^q) \equiv 0 \mod q
\]
and
\[
\text{ord}_{p_{N_{x,b,x}(K,q)}}(bx^q + b^q) < 0.
\]
Since, by assumption, $\text{ord}_{p_K} c = 0$ and therefore $\text{ord}_{p_{N_{x,b,x}(K,q)}} c = 0$, by Lemma 2.8 Part 3 one more time, $p_{N_{x,b,x}(K,q)}$ will split completely into distinct factors in the extension $L_{c,x,b,x}(K,q)/N_{x,b,x}(K,q)$, and, as before, this would imply that $c$ is not a $q$-th power in $L_{c,x,b,x}(K,q)$ or modulo any of $p_{L_{c,x,b,x}(K,q)}$ above $p_K$. Here we remind the reader that
\[
L_{c,x,b,x}(K,q) = N_{x,b,x}(K,q)(\sqrt[1]{1 + (c + c^{-1})x^{-1}}).
\]
Finally, we also have
\[
\text{ord}_{p_{L_{c,x,b,x}(K,q)}}(bx^q + b^q) \equiv 0 \mod q.
\]

**Proposition 2.13.** If $K$ is a number field containing $\xi_q$, and $x,c,b \in K$ are as in Proposition 2.12 then for any $L_{c,x,b,x}(K,q)$-prime $a_{L_{c,x,b,x}(K,q)}$ that is not a factor of $q$ and is not a pole of $x$, the following statements hold:

1. \(\text{ord}_{a_{L_{c,x,b,x}(K,q)}} c \equiv 0 \mod q\);
2. \(\text{ord}_{a_{L_{c,x,b,x}(K,q)}} bx^q + b^q \equiv 0 \mod q\);
3. \(\text{ord}_{a_{L_{c,x,b,x}(K,q)}} x \equiv 0 \mod q\).

**Proof.** We again proceed by applying Lemma 2.8 three times. In the extension $M_x(K,q)/K$, where $M_x(K,q) = K(\sqrt[1]{1 + x^{-1}})$, all the zeros of $x$ that are not of order divisible by $q$ are ramified by Lemma 2.8 Part 4, since for any $K$-prime $a_k$ such that $\text{ord}_{a_k} x > 0$ we have that $\text{ord}_{a_k}(1 + x^{-1}) = \text{ord}_{a_k}(x^{-1}) < 0$.

In the extension $N_{x,b,x}(K,q)/M_x(K,q)$, where $N_{x,b,x}(K,q) = M_x(K,q)(\sqrt[1]{1 + (bx^q + b^q)^{-1}})$, as before, we ramify all the primes $a_{M_x(K,q)}$ such that $\text{ord}_{a_{M_x(K,q)}}(bx^q + b^q) > 0$ and
\[
\text{ord}_{a_{M_x(K,q)}}(bx^q + b^q) \not\equiv 0 \mod q.
\]
Further, if $a_{M_x(K,q)}$ is a pole of $bx^q + b^q$ but not a pole of $x$, then it is a pole of $b$ and therefore $\text{ord}_{a_{M_x(K,q)}}(bx^q + b^q) = q \text{ord}_{a_{M_x(K,q)}} b$.

Finally, $(c + c^{-1})x^{-1}$ has poles at all primes occurring in the divisor of $c$ and not poles of $x$. Since in $M_x(K,q)$, and therefore in $N_{x,b,x}(K,q)$, all zeros of $x$ are of order divisible by $q$, if $c$ has a pole or a zero of degree not divisible by $q$, and the prime in question is not a pole of $x$, it follows that $(c + c^{-1})x^{-1}$ has a pole of degree not divisible by $q$ at this prime, forcing it to ramify in the extension $N_{x,b,x}(K,q)(\sqrt[1]{1 + (c + c^{-1})x^{-1}})/N_{x,b,x}(K,q)$. Thus, $\text{ord}_{a_{L_{c,x,b,x}(K,q)}} c \equiv 0 \mod q$ for any prime $a_{L_{c,x,b,x}(K,q)}$ not dividing $q$ and not a pole of $x$. □

We now consider what happens to factors of $q$ under cyclic extensions of degree $q$.

**Proposition 2.14.** If for some elements $x,d,a$ of a number field $K$ containing $\xi_q$ and some $K$-prime $q_K$ the following assumptions are true:
then for every prime factor \( q \) of \( q_K \) in \( L_{a,x,d,d}(K, q) \) we have that
(1) \( \text{ord}_{q_K} x < 0 \),
(2) \( q_K \) does not split in the extension \( K(\sqrt[d]{a})/K \),
(3) \( \text{ord}_{q_K} x < 0 \),
(4) \( \text{ord}_{q_K} d \neq 0 \mod q \),
(5) \( \text{ord}_{q_K} d \leq -3 \text{ord}_{q_K} q \),
(6) \( \text{ord}_{q_K} a = 0 \),
(7) \( q \text{ord}_{q_K} x < (q-1) \text{ord}_{q_K} d \).

then for every prime factor \( q \) of \( q_K \) in \( L_{a,x,d,d}(K, q) \) we have that
(1) \( \text{ord}_{q_{L_{a,x,d,d}(K, q)}} x < 0 \),
(2) \( q_{L_{a,x,d,d}(K, q)} \) does not split in the extension \( L_{a,x,d,d}(K, q)(\sqrt[d]{a})/L_{a,x,d,d}(K, q) \), and
(3) \( \text{ord}_{q_{L_{a,x,d,d}(K, q)}} (dx^a + d^q) \neq 0 \mod q \).

Proof. First of all we note that
\[
L_{a,x,d,d}(K, q) = K(\sqrt[1+d-1]{a}, \sqrt[1+(a+d^{-1})^{-1}]{a}, \sqrt[1+(a+a^{-1})d^{-1}]{a}).
\]

Next we observe that over the \( q_K \)-adic completion \( K_{q_K} \) of \( K \), a \( q \)-th root of \( a \) generates an unramified extension of degree \( q \). Further, if \( F/K \) is a finite extension, where \( q_K \) has a local degree one (i.e. \( e = f = 1 \)) factor \( q_F \), then \( F_{q_F} \cong K_{p_K} \), and a \( q \)-th root of \( a \) generates an unramified extension of degree \( q \) over \( F_{q_F} \), where \( q_F \) does not split.

Now note that by Assumption 6 we have that
\[
\text{ord}_{q_K} d \leq -3 \text{ord}_{q_K} q
\]
and therefore by Corollary 2.7 we have that \( q_K \) splits completely into distinct factors in the extension \( M_{d}(K, q)/K \). (We remind the reader that \( M_{d}(K, q) = K(\sqrt[1+d-1]{a}) \).) Thus, in \( M_{d}(K, q) \) we have that \( \text{ord}_{q_{M_{d}(K, q)}} x < 0 \), \( \text{ord}_{q_{M_{d}(K, q)}} d \neq 0 \mod q \) and \( q_{M_{d}(K, q)} \) has a factor of relative degree \( q \) in the extension generated by adjoining \( \sqrt[d]{a} \) to \( M_{d}(K, q) \) for any \( q_{M_{d}(K, q)} \in \mathcal{G}_{M_{d}(K, q)}(q_K) \). Further, by Assumption 7
\[
q \text{ord}_{q_K} x + \text{ord}_{q_K} d < q \text{ord}_{q_K} d \leq -3q \text{ord}_{q_K} q,
\]
and therefore
\[
\text{ord}_{q_{M_{d}(K, q)}} (dx^a + d^q) = \text{ord}_{q_{M_{d}(K, q)}} d + q \text{ord}_{q_{M_{d}(K, q)}} x < -3q \text{ord}_{q_K} q < 0.
\]

Further, by Assumption 7 we have that \( \text{ord}_{q_{M_{d}(K, q)}} (dx^a + d^q) \neq 0 \mod q \). Applying Corollary 2.7 again, this time over the field \( N_{x,d,d}(K, q) = M_{d}(K, q)(\sqrt[1+d-1]{a}) \), we see that in the extension \( N_{x,d,d}(K, q)/M_{d}(K, q) \), the \( M_{d}(K, q) \)- prime \( q_{M_{d}(K, q)} \) splits completely into distinct factors. Consequently, any \( q_{N_{x,d,d}(K, q)} \) has a factor of relative degree \( q \) in the extension generated by adjoining \( \sqrt[d]{a} \) to \( N_{x,d,d}(K, q) \), while
\[
\text{ord}_{q_{N_{x,d,d}(K, q)}} (dx^a + d^q) \neq 0 \mod q
\]
and
\[
\text{ord}_{q_{N_{x,d,d}(K, q)}} (dx^a + d^q) < 0.
\]

Since, by assumption, \( \text{ord}_{q_K} a = 0 \) and therefore \( \text{ord}_{q_{N_{x,d,d}(K, q)}} a = 0 \), by Corollary 2.7 one more time, \( q_{N_{x,d,d}(K, q)} \) will split completely into distinct factors in the extension
\[
L_{a,x,d,d}(K, q)/N_{x,d,d}(K, q).
\]
(here we remind the reader that \( L_{a,x,d,d}(K, q) = N_{x,d,d}(K, q)(\sqrt[\varphi]{1 + (a + a^{-1})d^{-1}}) \) and, as before, this would imply that any \( q_{L_{a,x,d,d}(K, q)} \) will have a factor of relative degree \( q \) in the extension generated by adjoining \( \sqrt[\varphi]{a} \) to \( L_{a,x,d,d}(K, q) \), while
\[
\text{ord}_{a_{L_{a,x,d,d}(K, q)}}(dx^a + d^q) \not\equiv 0 \mod q.
\]
So in particular, \( a \) is not a \( q \)-th power in \( L_{a,x,d,d}(K, q) \).

\[\square\]

Now a \( q \)-“analog” of Proposition 2.13.

**Proposition 2.15.** Under assumptions of Lemma 2.14, for any \( L_{a,x,d,d}(K, q) \)-prime \( a_{L_{a,x,d,d}(K, q)} \) that is not a pole of \( d \) and is not a pole of \( x \), the following statements hold:

1. \( \text{ord}_{a_{L_{a,x,d,d}(K, q)}} d \equiv 0 \mod q \);
2. \( \text{ord}_{a_{L_{a,x,d,d}(K, q)}} a \equiv 0 \mod q \);
3. \( \text{ord}_{a_{L_{a,x,d,d}(K, q)}}(dx^a + d^q) \equiv 0 \mod q \).

**Proof.** We again proceed by applying Lemma 2.8 three times. In the extension \( M_d(K, q)/K \), where \( M_d(K, q) = K(\sqrt[\varphi]{1 + d^{-1}}) \), all the zeros of \( d \) that are not of order divisible by \( q \) are ramified by Lemma 2.8 Part 4, since for any \( K \)-prime \( a_K \) such that \( \text{ord}_{a_K} d > 0 \) we have that \( \text{ord}_{a_K}(1 + d^{-1}) < 0 \).

In the extension \( N_{x,d,d}(K, q)/M_d(K, q) \), where \( N_{x,d,d}(K, q) = M_d(K, q)(\sqrt[\varphi]{1 + (dx^a + d^q)^{-1}}) \), as before, we ramify all the primes \( a_{M_d(K, q)} \) such that \( \text{ord}_{a_{M_d(K, q)}}(dx^a + d^q) > 0 \) and
\[
\text{ord}_{a_{M_d(K, q)}}(dx^a + d^q) \not\equiv 0 \mod q.
\]

Further, if \( a_K \) is a pole of \( dx^a + d^q \) but \( a_K \) is not a pole of \( d \), then \( \text{ord}_{a_K}(dx^a + d^q) = q \text{ord}_{a_K} x \), and if for some pole \( q_{a_K} \) of \( d \) we have that \( \text{ord}_{q_{a_K}} x > 0 \), then \( \text{ord}_{q_{a_K}}(dx^a + d^q) = q \text{ord}_{q_{a_K}} d \).

Finally, \((a + a^{-1})d^{-1} \) has poles at all primes occurring in the divisor of \( a \), and zeros of \( d \). Further in \( N_{x,d,d} \) all zeros of \( d \) are of orders divisible by \( q \). Thus if \( a \) has a pole or a zero of degree not divisible by \( q \), it follows that \((a + a^{-1})d^{-1} \) has a pole of degree not divisible by \( q \) at this prime, forcing it to ramify in the extension \( N_{x,d,d}(K, q)/(\sqrt[\varphi]{1 + (a + a^{-1})d^{-1}})/N_{x,d,d}(K, q) \). Thus, \( \text{ord}_{a_{L_{a,x,d,d}(K, q)}} c \equiv 0 \mod q \) for any prime \( a_{L_{a,x,d,d}(K, q)} \) as described in the statement of the proposition. \[\square\]

The lemma below considers some archimedean completions of a number field.

**Lemma 2.16.** If \( c \in \Omega_2(K) \) and \( M = K(\sqrt{c}) \), then any archimedean completion of \( M \) is isomorphic to the corresponding archimedean completion of \( K \).

**Proof.** Let \( \sigma \) be an embedding of \( M \) into \( \bar{Q} \). If \( \sigma(M) \subset \bar{Q} \cap \mathbb{R} \), then the archimedean completion of \( \sigma(M) \) is isomorphic to \( \mathbb{R} \), and the completion is isomorphic to \( \mathbb{C} \) otherwise. Therefore to prove the lemma, it is enough to show that whenever \( \sigma(K) \subset \bar{Q} \cap \mathbb{R} \), we also have \( \sigma(M) \subset \bar{Q} \cap \mathbb{R} \). This implication follows from the fact that whenever \( \sigma(K) \subset \bar{Q} \cap \mathbb{R} \), we have \( \sigma(c) > 0 \) and therefore \( \sqrt{\sigma(c)} \in \mathbb{R} \). \[\square\]

We will need the two lemmas below when analyzing what happens to factors of \( q \) in number field extensions of degree \( q \).
Lemma 2.17. If $U/K$ is a Galois extension of number fields, $F/U$ is a cyclic number field extension, and the extension $F/K$ is Galois, then there are infinitely many primes of $U$ not splitting in the extension $F/U$ and lying above a prime of $K$ splitting completely in $U$.

Proof. If $\sigma$ is a generator of $\text{Gal}(F/U)$, then any prime of $F$ whose Frobenius over $K$ is

$$\sigma \in \text{Gal}(F/U) \subset \text{Gal}(F/K)$$

will have the desired property. Now Tchebotarev Density Theorem tells us that there are infinitely many such primes. □

Lemma 2.18. Let $F/U$ be a cyclic extension of number number fields such that for some rational prime $q$ we have that $[F : U] \equiv 0 \mod q^m$. Let $N$ be the unique subfield of $F$ containing $U$ such that $[N : U] = q^m$. Let $p_F$ be a prime of $F$ and let $p_U$ be the $U$-prime below it. If $\sigma$ is the Frobenius automorphism of $p_F$ and $\sigma$ is not a $q$-th power in $\text{Gal}(F/U)$, then $p_U$ does not split in the extension $N/U$.

Proof. If $H = \text{Gal}(F/N)$, then $H$ is the set of all elements of the Galois group that are $q^m$-th powers. Thus, since $\sigma$ is not a $q$-th power in $\text{Gal}(F/U)$, we must have that $q^m$ is the smallest positive power $r$ of $\sigma$ such that $\sigma^r \in H$. Therefore, we have that $\sigma | N$ has order $q^m$ and thus generates the Galois group of $N$ over $U$. Hence, the decomposition group of $p_F \cap N = p_N$ is the Galois group of $N/U$, and $p_U$ does not split in the extension $N/U$. □

We now construct a cyclic extension of degree equal to a power of $q$ where $q$ can have an arbitrarily high relative degree and no ramified factors.

Lemma 2.19. If $q$ is a rational prime, $m \in \mathbb{Z}_{>0}$, then there exists a totally real cyclic extension of $\mathbb{Q}$ of degree $q^m$ where $q$ does not split.

Proof. Let $\ell$ be a rational prime satisfying the following conditions:

1. $\ell$ splits completely in $\mathbb{Q}(\xi_{q^m})/\mathbb{Q}$.
2. Factors of $\ell$ in $\mathbb{Q}(\xi_{q^m})$ do not split in the extension $\mathbb{Q}(\xi_{q^m}, \sqrt[q]{q})/\mathbb{Q}(\xi_{q^m})$.

(Observe that by Lemma 2.17, there are infinitely many such $\ell$‘s.) It follows that $\ell \equiv 1 \mod q^m$, but $q$ is not a $q$-th power mod $\ell$. Indeed, since both bases $\{1, \xi_q, \ldots, \xi_q^{(q-1)q^{m-1}}\}$ and $\{1, \sqrt[q]{q}, \ldots, \sqrt[q]{q^{q^{m-1}}}\}$ are integral bases with respect to $\ell$ and all of its factors, the factorization of $\ell$ and its factors in the extensions $\mathbb{Q}(\xi_{q^m})/\mathbb{Q}$ and $\mathbb{Q}(\xi_{q^m}, \sqrt[q]{q})/\mathbb{Q}(\xi_q)$ corresponds to the factorization of the respective minimal polynomials modulo $\ell$, implying that $\mathbb{Z}/\ell$ contains a $q^m$-th root of unity, so that $q^m | (\ell - 1)$, and the polynomial $T^q - q$ has no roots modulo any factors $\ell$ in $\mathbb{Q}(\xi_q)$.

Now consider the extension $\mathbb{Q}(\xi_\ell)/\mathbb{Q}$ and note that it is of degree divisible by $q^m$. If $\tau$ is the Frobenius of $q$, then $\tau(\xi_\ell) = \xi_\ell^{q^m}$ and $\tau$ is not a $q$-th power in $\text{Gal}(\mathbb{Q}(\xi_\ell)/\mathbb{Q})$. Indeed, suppose $\tau = \sigma^q$ for some $\sigma \in \text{Gal}(\mathbb{Q}(\xi_\ell)/\mathbb{Q})$. Let $r$ be a positive integer such that $\sigma(\xi_\ell) = \xi_\ell^r$ and therefore $\xi_\ell^q = \tau(\xi_\ell) = \sigma^q(\xi_\ell) = \xi_\ell^{r^q}$ implying $q \equiv r^q \mod \ell$ in contradiction of our assumption on $\ell$ and $q$. Therefore, by Lemma 2.18 we conclude that $q$ will not split in the unique degree $q^m$ extension of $\mathbb{Q}$ contained in $\mathbb{Q}(\xi_q)$. □

We now use the lemma above to construct a cyclic extension of a number field where $q$ will have relative degree $q$. We do this in two steps. The first step is the lemma below.

Lemma 2.20. If $G$ is algebraic over $\mathbb{Q}$, $F$ a number field with $F/\mathbb{Q}$ cyclic, then $GF/G$ is cyclic with $[GF : G][F : \mathbb{Q}]$. 

10
**Proof.** If $M = G \cap F$, then, since $F/\mathbb{Q}$ is Galois, $[F : M] = [GF : G]$ and thus
\[ [GF : G][F : \mathbb{Q}]. \]
Indeed, let $\alpha \in F$ generate $F$ over $\mathbb{Q}$ and therefore also $F$ over $M$, and let $a_0 + a_1 T + \ldots + T^r$ be the monic irreducible polynomial of $\alpha$ over $G$. Since all the conjugates of $\alpha$ over $\mathbb{Q}$ are in $F$, all the conjugates of $\alpha$ over $G$ are in $F$, and thus $a_0, \ldots, a_{r-1} \in F$ and hence in $M$. So the degree of $\alpha$ over $G$ is at least as large as the degree of $\alpha$ over $M$. Since $M \subseteq G$, these degrees must be equal.

Further $F/M$ is again a cyclic extension, and all the the conjugates of $\alpha$ over $M$ and over $G$ are the same. Hence, $\text{Gal}(GF/G) \cong \text{Gal}(F/M)$ and we can conclude that the extension $GF/G$ is cyclic. \hfill \Box

This is the second step of our construction.

**Lemma 2.21.** Let $G$ be a number field such that for some prime $p_G$ of $G$ lying above a rational prime $p_\mathbb{Q}$ we have that $\text{ord}_q(f(p_G/p_\mathbb{Q})) = m$. Suppose now that $F$ is a cyclic extension of $\mathbb{Q}$ of degree $q^r$ with $r > m$, where $p_\mathbb{Q}$ does not split. Let $GF$ be the field compositum of $G$ and $F$ inside the algebraic closure of $\mathbb{Q}$. Under these assumptions, there exists a field $\hat{G}$ such that $G \subseteq \hat{G} \subset GF$ and $GF/\hat{G}$ is a cyclic extension of degree $q$ where no factor of $p_G$ splits.

**Proof.** Consider the following field diagram
\[
\begin{array}{c}
p_{GF} \in GF \\
| \\
p_F \in F \\
| \\
p_{pQ} \in \mathbb{Q}
\end{array} 
\begin{array}{c}
p_{GF} \in GF \\
| \\
p_G \in G \\
| \\
p_F \in F \\
| \\
p_{pQ} \in \mathbb{Q}
\end{array}
\]
and observe that $f(p_{GF}/p_\mathbb{Q}) \geq q^r$, while $\text{ord}_q(f(p_G/p_\mathbb{Q})) = m < r$. Consequently,
\[ \text{ord}_q(f(p_{GF}/p_G)) > 1 \]
and thus $f(p_{GF}/p_G) > 1$. By Lemma 2.20, the extension $GF/G$ is cyclic of degree that is a power of $q$. Further, by Proposition 8, of Chapter II, §4 of [14], $GF/G$ is unramified at all the factors of $p_G$. Let $\sigma$ be a generator of the $\text{Gal}(GF/G)$ and observe that for some positive integer $i$, the Frobenius automorphism of any factor $p_{GF}$ of $p_G$ over $G$ is $\sigma^i \neq \text{id}$ and must be of order divisible by $q$. Now, if $\hat{G} \neq GF$ is the fixed field of $\sigma^{\text{ord}_q(q^i/q)}$, we have that any factor $p_G$ of $p_G$ in $\hat{G}$ will not split in the extension $GF/\hat{G}$ and $[GF : \hat{G}] = q$. \hfill \Box

Since for any $G$ and $F$ as above, the field $\hat{G}$ satisfying $G \subseteq \hat{G} \subset GF$ and $[GF : \hat{G}] = q$ is unique, we have the following corollary.

**Corollary 2.22.** Let $G, F$ be as in Lemma 2.21, and assume additionally that for any $G$-prime $p_G$ lying above a rational prime $p_\mathbb{Q}$ we have that $\text{ord}_q f(p_G/p_\mathbb{Q}) < [F : \mathbb{Q}]$. Let $\hat{G}$ be a subfield of $GF$ such that $G \subset \hat{G}$ and $[GF : \hat{G}] = q$. In this case no $\hat{G}$-factor of $p_\mathbb{Q}$ splits in the extension $GF/\hat{G}$.

We now consider the case when $q = 2$ and examine generators of $GF$ over $\hat{G}$.
Lemma 2.23. Let $G, \hat{G}, F$ be as in Corollary 2.22, let $q = 2$, and assume $F$ is totally real. Suppose $FG = \hat{G}(\sqrt{a}), a \in \hat{G}$. In this case, if $\sigma : \hat{G} \to \bar{\mathbb{Q}} \cap \mathbb{R}$ is an embedding of $\hat{G}$, then $\sigma(a) > 0$.

Proof. Since $F$ is totally real, for any embedding $\sigma : FG \to \bar{\mathbb{Q}}$, we have that $\sigma(FG) \subseteq \mathbb{R} \iff \sigma(G) \subseteq \mathbb{R}$. If $\sigma(\hat{G}) \subseteq \mathbb{R}$, then $\sigma(G) \subseteq \mathbb{R}$ and $\sigma(FG) \subseteq \mathbb{R}$ implying $\sqrt{\sigma(a)} \in \mathbb{R}$ and $\sigma(a) \geq 0$. □

3. Local degree in infinite extensions.

Before proceeding with definitions of integers and “small rings” in infinite algebraic extensions of $\mathbb{Q}$, we would like to discuss and clarify the conditions we will use. We start with adding notation.

Notation 3.1. (1) Let $K_{inf}$ be an infinite algebraic extension of a number field $G$.
(2) Let $I_G = I(G, K_{inf}) = \{K\mid K$ is a number field such that $G \subseteq K \subseteq K_{inf}\}$.
(3) For any $M \in I_G$, let $I_M = I_M(G, K_{inf}) = \{K\mid K$ is a number field such that $G \subseteq M \subseteq K \subseteq K_{inf}\}$.
(4) For any $M \in I_G$, let $J_M(G, K_{inf})$ be an ordered by inclusion subset of $I_M$ such that the union of all the fields in $J_M$ is $K_{inf}$. If $p_M$ is a prime of $M$, then prime factors of $p_M$ in the fields of $J_M$ generate a tree. A path in such a tree corresponds to a prime ideal of $O_{K_{inf}}$—the ring of integers of $K_{inf}$. We will refer to $J_M$ as a field path from $M$ to $K_{inf}$.
(5) If $M \in I_G$ and $\mathcal{P}_M$ is a set of primes of $M$, then let $O_{K_{inf}, \mathcal{P}_M}$ denote the integral closure of $O_M, \mathcal{P}_M$ in $K_{inf}$. As mentioned above, $O_{K_{inf}}$ will denote the ring of algebraic integers of $K_{inf}$.
(6) If $M$ is a number field, $p_M$ is a prime of $M$, and $K \in I_M$, then let $\mathcal{C}_K(p_M)$, as above, denote the set of all prime factors of $p_K$ in $M$. Let $\mathcal{C}_{inf}(p_M) = \bigcup_{K \in I_M} \mathcal{C}_K(p_M)$.

We now define the primes that will and will not “work” in the definitions we are describing in this paper.

A diagram for $q$-unbounded primes

\[
\begin{array}{cccccc}
G & \to & M & \rightarrow & K & \rightarrow \cdots & K_{inf} \\
\downarrow & & \downarrow & & \downarrow & & \\
p_G & \to & p_M & \rightarrow & p_K & \\
\end{array}
\]

A diagram for completely $q$-bounded primes

\[
\begin{array}{cccccc}
G & \to & M & \rightarrow & K & \rightarrow \cdots & K_{inf} \\
\downarrow & & \downarrow & & \downarrow & & \\
p_G & \to & p_M & \rightarrow & p_K & \\
\end{array}
\]
Definition 3.2 (q-unbounded and q-bounded primes). Let $q$ be a rational prime and let $p_G$ be a prime of $G$ satisfying the following condition: for any $M \in I_G$ there exists $K \in I_M$ such that for any $p_M \in C_M(p_G)$ and any $p_K$ in $C_K(p_M)$ we have that
\[
d(p_K/p_M) = e(p_K/p_M)f(p_K/p_M) \equiv 0 \mod q,
\]
where as usual $e(p_K/p_M)$ is the ramification degree of $p_K$ over $p_M$, $f(p_K/p_M)$ is the relative degree of $p_K$ over $p_M$, and $d(p_K/p_M)$ is the local degree of $p_K$ over $p_M$. In this case we call $p_G$ q-unbounded. (See the diagram above.)

If there exists $M \in I_G$ such that for any $K \in I_M$, for any $p_M \in C_M(p_G)$, and any $p_K$ in $C_K(p_M)$ we have that $\text{ord}_q d(p_K/p_M) = 0$, we call $p_G$ completely q-bounded. (See a diagram above.)

If $p_G$ is not q-unbounded, we call $p_G$ q-bounded. If every prime in $C_{\text{inf}}(p_G)$ is q-bounded, we call $p_G$ hereditarily q-bounded.

If every prime of $G$ is hereditarily q-bounded in $K_{\text{inf}}$, and all the factors of $q$ are completely q-bounded, then we will call $K_{\text{inf}}$ itself q-bounded.

Observe that if a prime is completely q-bounded, it is hereditarily q-bounded. As is shown below, we need all the primes of $G$ to be hereditarily q-bounded, and we need $q$ to be completely q-bounded for our definition method to work for the ring of integers. At the same time the unbounded primes can be used to define “big subrings”.

Remark 3.3. One can rephrase the definition of a q-unbounded prime as follows. A prime $p_G$ of $G$ is unbounded if for every $n \in \mathbb{Z}_{>0}$ there exists a field $M \in I_G$ such that for any $p_M \in C_M(p_G)$ we have that $e(p_M/p_G)f(p_M/p_G) = d(p_M/p_G) = 0 \mod q^n$, where $d(p_M/p_G)$ as above is the local degree $[M_{p_M} : G_{p_G}]$.

We also need the following definition.

Definition 3.4. Given a $G$-prime $p_G$ and a field path $J_G = \{G - M_1 - M_2 \ldots \}$ from $G$ to $K_{\text{inf}}$, as described in Notation 3.1 Part 4, call a path $\mathcal{P} = \{p_G - p_{M_1} - p_{M_2} \ldots \}$ through the tree of $p_G$-factors q-bounded if there exists $i \in \mathbb{Z}_{>0}$ such that for all integer $j \geq i$ we have that $\text{ord}_q(d(p_{M_i}/p_G)) = \text{ord}_q(d(p_{M_j}/p_G)) = n_i$. Also call $M_i$ a q-bounding field and call $n_i$ a q-bounding order.

Remark 3.5. A q-bounding field and a q-bounding order also “work” off the field path where they were defined. Indeed, let $M$ and $n$ be a q-bounding field and order defined along some field path $J_G$, and let $N \in I_G$. In this case for some $p_N \in C_N(p_G)$ it is true that $\text{ord}_q(d(p_N/p_G)) \leq n$. Indeed, some field $L$ along the field path $J_G$ contains $M$ and $N$ and for some $p_L \in C_L(p_G)$ we have that $\text{ord}_q(d(p_L/p_G)) = n$. Thus, for $p_N = p_L \cap N \in C_N(p_G)$ it is the case that $\text{ord}_q(d(p_N/p_G)) \leq \text{ord}_q(d(p_L/p_G)) = n$. Similarly, for any $L \in I_M$ we have that for some $p_L \in C_L(p_M)$ it is the case that $\text{ord}_q(d(p_L/p_M)) = 0$.

Lemma 3.6. Choose any field path $J_G$ as in Notation 3.1 Part 4 and consider the corresponding tree of factors for some prime $p_G$ of $G$. We claim that $p_G$ is q-bounded if and only if it lies along a q-bounded path.

Proof. Indeed, suppose $p_G$ is q-bounded and let $n \in \mathbb{Z}_{>0}$ be such that for any $M \in J_G$ for some $p_M \in C_M(p_G)$ we have that $d(p_M/p_G) \neq 0 \mod q^n$. From the tree of $p_G$ factors corresponding to $J_G$ remove all the “nodes” (i.e. factors of $p_G$) with the local degree with respect to $p_G$ divisible by $q^n$. Note that if a node survives removal, all of its predecessors
must survive too. Thus, the tree structure is preserved under the removal of the nodes with the local degree with respect to \( p_G \) divisible by \( q^a \). This tree will have arbitrarily long paths and thus by König’s Lemma an infinite path. Since the order at \( q \) of the local degree along this path is bounded, after some point the degree can grow only by factors prime to \( q \).

Conversely, along a \( q \)-bounded path the order of the local degree at \( q \) will be bounded and therefore we cannot have arbitrarily large powers of \( q \) divide the local degree for all the factors of a prime on such a path. □

In the case a prime \( p_G \) is completely \( q \)-bounded, by definition, there is a \( q \)-bounding field and a \( q \)-bounding order which work along all paths through the factor tree.

**Definition 3.7.** Let \( p_G \) be a completely \( q \)-bounded prime and let \( M \in I_G \) be such that for any \( K \in I_M \), for any \( p_M \in \mathcal{C}_M(p_G) \), and any \( p_K \in \mathcal{C}_K(p_M) \) we have that \( \text{ord}_q d(p_K/p_M) = 0 \). In this case call \( M \) a completely \( q \)-bounding field (for \( p_G \)). Call \( \max_{p_M \in \mathcal{C}_M(p_G)}(\text{ord}_q(d(p_M/p_G))) \) a completely \( q \)-bounding order (for \( p_G \)).

4. Defining Integers in the Infinite Extensions of \( \mathbb{Q} \).

Our plan is to deal with all but finitely many primes first. This is accomplished in the section below.

4.1. The main part of the definition. We will use the following notation and assumptions in this section.

**Notation and Assumptions 4.1.**

- Let \( K_{\inf} \) be an infinite algebraic extension of \( \mathbb{Q} \).
- Let \( G \subset K_{\inf} \) be a number field, and let \( \mathcal{S}_G \) be a finite, possibly empty set of primes of \( G \). Suppose all the primes of \( G \) not dividing \( q \) and not in \( \mathcal{S}_G \) are hereditarily \( q \)-bounded in \( K_{\inf} \).
- Let \( \mathcal{W}_G = \mathcal{S}_G \cup \{\text{factors of } q\} \)
- Let \( O_{K_{\inf},\mathcal{W}_K_{\inf}}, O_{K_{\inf},\mathcal{S}_K_{\inf}} \) denote the integral closure of \( O_{G,\mathcal{W}_G} \) and \( O_{G,\mathcal{S}_G} \) respectively in \( K_{\inf} \).

**Proposition 4.2.** If \( \xi_q \in G \), \( b \in K_{\inf} \),

\[
c \in \Omega_q(K_{\inf}) \cap \Phi_q(K_{\inf}) \cap \Theta_q(K,\mathcal{S}_{K_{\inf}}),
\]

and there exists \( y \in L_{c,x,b,x}(K_{\inf},q) \) such that

\[
(4.1) \quad N_{L_{c,x,b,x}(K_{\inf},q)/(\mathbb{Q})/L_{c,x,b,x}(K_{\inf},q)}(y) = bx^q + b^q,
\]

then there exists a field \( M \in I_G \) such that for any field \( K \in I_M \), for any non-archimedean prime \( p_K \) of \( K \) not in \( \mathcal{W}_K \), it is the case that one of the following conditions holds:

1. \( c \) is a \( q \)-th power mod \( p_K \), or
2. \( \text{ord}_{p_K} x \geq 0 \), or
3. \( q \text{ord}_{p_K} x \geq (q-1) \text{ord}_{p_K} b \), or
4. \( \text{ord}_{p_K} b \equiv 0 \mod q \).

At the same time, if \( x \in O_{K_{\inf},\mathcal{W}_K_{\inf}} \), then \((4.1)\) has a solution \( y \in L_{c,x,b,x}(K_{\inf},q) \).

**Proof.** Suppose that \((4.1)\) holds for some \( x, b, c, y \) as specified above. Let \( M \in I_G \) be such that

\[
(4.2) \quad x, c \in M,
\]
Further, by Lemma 2.10 and by our assumption that $c$ is isomorphic to $\mathbb{R}$ we have to worry about one possibility only: an archimedean completion of $\mathbb{C}$. Since (4.4) insure that for any $L$, $\Omega(y/L_{c,x,b,x}(\sqrt{c}))$ has no solution in $L_{c,x,b,x}(K,q)(\sqrt{c})$ contradicting our assumptions.

Observe further that locally every unit is a norm in an unramified extension (see Proposition 6, Section 2, Chapter XII of [42]), and we do not have to worry about archimedean primes, given our assumption on $c$. Indeed, if $q > 2$, then $K \not\subset \mathbb{R}$ and therefore all the archimedean completions of all the fields involved are isomorphic to $\mathbb{C}$. If $q = 2$, then we have to worry about one possibility only: an archimedean completion of $L_{c,x,b,x}(K,q)$ is isomorphic to $\mathbb{R}$, while a corresponding archimedean completion of $L_{c,x,b,x}(K,q)(\sqrt{c})$ is isomorphic to $\mathbb{C}$. However, this case is precluded by Lemma 2.16 and our assumption that $c \in \Omega_q(K)$. 

$$y \in L_{c,x,b,x}(M,q)(\sqrt{c})$$

and

$$[L_{c,x,b,x}(\text{Kinf},q)(\sqrt{c}) : L_{c,x,b,x}(\text{Kinf},q)] = [L_{c,x,b,x}(M,q)(\sqrt{c}) : L_{c,x,b,x}(M,q)].$$

In this case, for any $K \in I_M$, we also have that $x, c \in K$, $y \in L_{c,x,b,x}(K,q)(\sqrt{c})$, 

$$[L_{c,x,b,x}(\text{Kinf},q)(\sqrt{c}) : L_{c,x,b,x}(\text{Kinf},q)] = [L_{c,x,b,x}(K,q)(\sqrt{c}) : L_{c,x,b,x}(K,q)],$$

and therefore it is also the case

$$N_{L_{c,x,b,x}(\text{Kinf},q)(\sqrt{c})/L_{c,x,b,x}(\text{Kinf},q)}(y) = bx^q + b^q.$$ 

Now, if for some $K$-prime $p_K$ such that $p_K \not\in \mathfrak{p}_K$, we have that none of the Conditions 1 - 4 is satisfied, then by Proposition 2.12 we have that

$$\text{ord}_{L_{c,x,b,x}(\text{Kinf},q)}(bx^q + b^q) \not\equiv 0 \mod q$$

and $c$ is not $q$-th power modulo $p_{L_{c,x,b,x}(\text{Kinf},q)}$. Hence by Lemma 2.9 we conclude that the norm equation (4.4) has no solution in $L_{c,x,b,x}(K,q)(\sqrt{c})$, contradicting our assumptions.

Suppose now that $x \in O_{K_{\text{inf}},\mathfrak{w}_{\text{inf}}}$, let $M \in I_G$ satisfy assumptions (1), (2), and be such that $c \in \Omega_q(M) \cap \Phi_q(M) \cap \Theta_q(M, \mathcal{S}_M)$. (We can find $M$ satisfying $c \in \Omega_q(M)$ by Remark 2.5.) We now choose any $K \in I_M$ and show that (4.5) has a solution $y \in L_{c,x,b,x}(K,q)(\sqrt{c})$. Since (4.4) insures that for any $y \in L_{c,x,b,x}(K,q)(\sqrt{c})$, it is the case that

$$N_{L_{c,x,b,x}(K,q)(\sqrt{c})/L_{c,x,b,x}(\text{Kinf},q)(\sqrt{c})/L_{c,x,b,x}(\text{Kinf},q)}(y) = N_{L_{c,x,b,x}(\text{Kinf},q)(\sqrt{c})/L_{c,x,b,x}(\text{Kinf},q)}(y),$$

we need to solve $N_{L_{c,x,b,x}(K,q)(\sqrt{c})/L_{c,x,b,x}(\text{Kinf},q)(\sqrt{c})/L_{c,x,b,x}(\text{Kinf},q)}(y) = bx^q + b^q$ only.

Since $y \in O_{K_{\text{inf}},\mathfrak{w}_{\text{inf}}}$, we have that $y \in O_{K,\mathfrak{w}_K}$. Further, we also have that

$$c \in \Omega_q(K) \cap \Phi_q(K) \cap \Theta_q(K, \mathcal{S}_K),$$

by definition of these sets and Remark 2.5. In this case by Proposition 2.13 for every prime $a_{L_{c,x,b,x}(\text{Kinf},q)}$, not dividing $q$ or any prime in $\mathcal{S}_K$, we have the following:

- $\text{ord}_{a_{L_{c,x,b,x}(\text{Kinf},q)}}(bx^q + b^q) \equiv 0 \mod q$, and
- $\text{ord}_{a_{L_{c,x,b,x}(\text{Kinf},q)}}(c) \equiv 0 \mod q$.

Further, by Lemma 2.10 and by our assumption that $c \in \Phi_q(K)$, we know that factors of $q$ are not ramified in the extension $L_{c,x,b,x}(K,q)(\sqrt{c})/L_{c,x,b,x}(K,q)$, and since the divisor of $c$ is a $q$-th power in $L_{c,x,b,x}(K,q)$, the extension $L_{c,x,b,x}(K,q)(\sqrt{c})/L_{c,x,b,x}(K,q)$ is unramified at all primes by Lemma 2.8.

By the Hasse’s Norm Principle (see Theorem 32.9 of [42]) this norm equations has solutions globally (i.e. in $L_{c,x,b,x}(K,q)(\sqrt{c})$) if and only if it has a solution locally (i.e. in every completion).

Observe further that locally every unit is a norm in an unramified extension (see Proposition 6, Section 2, Chapter XII of [42]), and we do not have to worry about archimedean primes, given our assumption on $c$. Indeed, if $q > 2$, then $K \not\subset \mathbb{R}$ and therefore all the archimedean completions of all the fields involved are isomorphic to $\mathbb{C}$. If $q = 2$, then we have to worry about one possibility only: an archimedean completion of $L_{c,x,b,x}(K,q)$ is isomorphic to $\mathbb{R}$, while a corresponding archimedean completion of $L_{c,x,b,x}(K,q)(\sqrt{c})$ is isomorphic to $\mathbb{C}$. However, this case is precluded by Lemma 2.16 and our assumption that $c \in \Omega_q(K)$. 

15
Next we observe that since \( L_{c,x,b,x}(K,q)(\sqrt{c})/L_{c,x,b,x}(K,q) \) is a cyclic extension of prime degree, by Lemma 2.9 every unramified prime either splits completely or does not split at all. If a prime splits completely, then the local degree is one and every element of the field below is automatically a norm locally at this prime. So the only primes where we might have elements which are not local norms are the primes which do not split, or, in other words, the primes where the local degree is \( q \). (Note that any factor of \( q \) and any factor of a prime in \( \mathcal{S}_K \) split completely in the extension \( L_{c,x,b,x}(K,q)(\sqrt{c})/L_{c,x,b,x}(K,q) \) by our assumptions on \( c \) and Lemmas 2.8 and 2.10.)

So let \( \mathfrak{r}_{L_{c,x,b,x}(K,q)} \) be a prime of local degree \( q \) not in \( \mathcal{W}_{L_{c,x,b,x}(K,q)} \). By the argument above we have that \( \text{ord}_{L_{c,x,b,x}(K,q)}(bx^q + b^q) \equiv 0 \mod q \). In this case, by the Weak Approximation Theorem, there exists \( u \in L_{c,x,b,x}(K,q) \) such that \( \text{ord}_{L_{c,x,b,x}(K,q)} u = 1 \) and therefore for some integer \( m \) it is the case that \( u^m(bx^q + b^q) \) has order 0 at \( \mathfrak{r}_{L_{c,x,b,x}(K,q)} \) or in other words \( u^m(bx^q + b^q) \) is a unit at \( \mathfrak{r}_{L_{c,x,b,x}(K,q)} \).

As any \( q \)-th power of an \( L_{c,x,b,x}(K,q) \)-element, \( u^m \) is a norm locally since the degree of the local extension is \( q \) by our assumption. Therefore, \( u^m(bx^q + b^q) \) is a norm at \( \mathfrak{r}_{L_{c,x,b,x}} \) if and only if \( (bx^q + b^q) \) is a norm at \( \mathfrak{r}_{L_{c,x,b,x}} \). But \( u^m(bx^q + b^q) \) is a norm at \( \mathfrak{r}_{L_{c,x,b,x}(K,q)} \) and therefore is a norm. Hence \( bx^q + b^q \) is a norm.

**Corollary 4.3.** If \( \xi_q \in G \) then

\[
(4.7) \quad \text{ord}_{p_{G(x)}} x < 0,
\]

and \( p_{G} \) is hereditarily \( q \)-bounded in \( K_{\text{inf}} \). Thus, \( p_{G(x)} \) is \( q \)-bounded in \( K_{\text{inf}} \). Let \( M \in I_{G(x)} \) be a \( q \)-bounding field for \( p_{G(x)} \) and note that by the Strong Approximation Theorem there exists \( c \in \Theta_q(M, \mathcal{S}_M) \cap \Phi_q(M) \cap \Omega_q(M) \subset \Theta_q(K_{\text{inf}}, \mathcal{S}_{K_{\text{inf}}}) \cap \Phi_q(K_{\text{inf}}) \cap \Omega_q(K_{\text{inf}}) \) such that \( c \) is not a \( q \)-th power modulo \( p_M \), where \( p_M \in \mathcal{C}_M(p_{G(x)}) \) lies along the \( q \)-bounded path for which \( M \) is a \( q \)-bounding field. Further, let \( b \in G(x) \) such that \( \text{ord}_{p_{G(x)}} b = -1 \) and thus \( q \text{ord}_{p_M} x < (q - 1) \text{ord}_{p_M} b \). Observe further that for any \( K \in I_M \) we also have that

1. \( c \in \Omega_q(K) \cap \Phi_q(K) \cap \Theta_q(K, \mathcal{S}_K) \), by definition of sets \( \Omega_q(K), \Phi_q(K), \) and \( \Theta_q(K, \mathcal{S}_K) \),
2. for at least one \( p_K \in \mathcal{C}_K(p_M) \) we have that \( d(p_K/p_M) \) and therefore \( f(p_K/p_M) \) are not divisible by \( q \) by definition of a \( q \)-bounding field, and therefore \( c \) is not a \( q \)-th power modulo at least one \( p_K \in \mathcal{C}_K(p_M) \),
3. for the same \( p_K \) as in (2) we also have that \( e(p_K/p_M) \) is not divisible by \( q \), and therefore \( \text{ord}_{p_K} b \neq 0 \mod q \) while \( q \text{ord}_{p_K} x < (q - 1) \text{ord}_{p_K} b \).

Thus none of Conditions 1-4 of Proposition 1.2 is satisfied, and hence (4.11) has no solution \( y \in L_{c,x,b,x}(K_{\text{inf}}, q) \).

\( \square \)
4.2. **Integrality at finitely many primes using complete p-boundedness for** \( p \neq q \).

We now consider definitions of integrality at finitely many primes to define \( \Theta_q(K_{\text{inf}}, \mathcal{F}_{K_{\text{inf}}}) \), \( \Phi_q(K_{\text{inf}}) \) and their complements. One way to do this is to use a bit of “circular reasoning” by introducing another rational prime \( p \) into the picture and making additional assumptions about our field. (Here “circular reasoning” refers to the fact that we use \( q \) to define integrality at factors of \( p \), and we use \( p \) to define integrality at factors of \( q \).)

**Notation and Assumptions 4.4.**

- Let \( p \neq q \) (with \( q \) as above) be a rational prime.
- Assume \( \xi_p \in G \).
- Assume factors of \( q \) and primes in \( \mathcal{S}_G \) are completely \( p \)-bounded in \( K_{\text{inf}} \).
- Let \( \mathcal{W}_G = \mathcal{S}_G \cup \{ \text{factors of } q \text{ in } G \} \), as above.
- Let \( M_p \in I_G \) be a completely \( p \)-bounding field for all primes in \( \mathcal{W}_G \). (Even though completely bounding fields were defined for a single prime, clearly any finite collection of completely bounded primes has a common completely bounding field, a field that contains a completely bounding field for each prime in the set.)

**Proposition 4.5.** Let \( d \in M_p \) be such that the denominator of its divisor is divisible by every prime of \( \mathcal{S}_{M_p} \) and by \( q^a \), and \( d \) has no other poles. Assume further that for any \( p_{M_p} \in \mathcal{W}_{M_p} \) it is the case that \( \text{ord}_{p_{M_p}} d \neq 0 \mod p \). (Note that such an element \( d \in M_p \) exists by the Strong Approximation Theorem.) Let \( a \in \Phi_{p}(M_p) \cap \Omega_{p}(M_p) \), and let \( a \) be equivalent to a non-\( p \)-th power element of the residue field modulo any prime of \( \mathcal{W}_{M_p} \). (Existence of \( a \) is also guaranteed by the Strong Approximation Theorem.) Now let

\[
B(K_{\text{inf}}, p, a, d) =
\{ x \in K_{\text{inf}} | \exists y \in L_{a,x,d,d}(K_{\text{inf}}, p)(\sqrt[1]{a}) : N_{L_{a,x,d,d}(K_{\text{inf}}, p)}(\sqrt[1]{a})/L_{a,x,d,d}(K_{\text{inf}}, p)(y) = dx^p + dp \}.
\]

We claim \( B(K_{\text{inf}}, p, a, d) = \{ x \in K_{\text{inf}} | \forall K \in I_{M_p} \forall p_K \in \mathcal{W}_K : \text{ord}_{p_K} x > \frac{p-1}{p} \text{ord}_{p_K} d \} \).

**Proof.** The proof of the proposition is almost identical to the proof of Proposition 4.2. One should only point out the following two adjustments and remind the reader that

\[
L_{a,x,d,d}(K_{\text{inf}}, p) = K_{\text{inf}}(\sqrt[1]{1 + d^{-1}}, \sqrt[1]{1 + (dx^p + dp)^{-1}}, \sqrt[1]{1 + (a + a^{-1})d^{-1}}).
\]

(1) By construction no pole of \( d \) in any \( K \in I_{M_p} \) occurs in the divisor of \( a \), since \( a \) is not a \( p \)-th power modulo primes of \( \mathcal{W}_K \). Thus, \( (a + a^{-1})d^{-1} \) has poles at all the primes occurring in the divisor of \( a \). Also, all zeros of \( d \) of orders not divisible by \( p \) in \( K \) are ramified with ramification degree \( p \) before we adjoin \( \sqrt[1]{1 + (a + a^{-1})d^{-1}} \), and therefore in \( L_{a,x,d,d}(K, p) \) all zeros and poles of \( a \) have order divisible by \( p \).

(2) For any prime \( p_K \in \mathcal{W}_K \) we have that

\[
\text{ord}_{p_K} (dx^p) \neq \text{ord}_{p_K} (dp^p),
\]

since the left order is not equivalent to \( 0 \mod p \) and the right one is. Thus under these circumstances, \( \text{ord}_{p_K} (dx^p + dp) \equiv 0 \mod p \) implies that \( \text{ord}_{p_K} (dx^p + dp) = \text{ord}_{p_K} (dp^p) \) and

\[
\text{ord}_{p_K} x > \frac{p-1}{p} \text{ord}_{p_K} d > \text{ord}_{p_K} d.
\]

Conversely, if for some \( K \in I_{M_p(x)} \) we have that (4.8) holds for all \( K \)-primes above primes of \( \mathcal{W}_G \), then \( \text{ord}_{p_K} (dx^p + dp) \equiv 0 \mod p \) and \( x \in B(K_{\text{inf}}, p, a, d) \).
We now use this definition of $B(K_{\inf}, p, a, d)$ to obtain a definition of $R_{K_{\inf}, \mathcal{W}_{\inf}}$ — the ring of elements of $K_{\inf}$ integral with respect to primes of $\mathcal{W}_{G}$. To do this we note the following.

**Lemma 4.6.** $R_{K_{\inf}, \mathcal{W}_{\inf}} = \{ x \in B(K_{\inf}, p, a, d) | \forall y \in B(K_{\inf}, p, a, d) : xy \in B(K_{\inf}, p, a, d) \}$.

**Proof.** First assume that $x \in R_{K_{\inf}, \mathcal{W}_{\inf}} \subset B(K_{\inf}, p, a, d)$ and note that in this case $x$ has non-negative order at all primes of $\mathcal{W}_{G}(x)$. Thus, if for some field $K \in I_{G}$ and some $K$-prime $p_{K}$ above a prime of $\mathcal{W}_{G}$ we have that $\text{ord}_{p_{K}} y > \frac{p-1}{p} \text{ord}_{p_{K}} d$, then

$$\text{ord}_{p_{K}} x y \geq \text{ord}_{p_{K}} y > \frac{p-1}{p} \text{ord}_{p_{K}} d.$$ 

Conversely, suppose that $x \in B(K_{\inf}, p, a, d) \setminus R_{K_{\inf}, \mathcal{W}_{\inf}}$ and note that in $K = M_{p}(x)$ we must have for some $K$-prime $p_{K}$ above a prime of $\mathcal{W}_{G}$ that

$$\frac{p-1}{p} \text{ord}_{p_{K}} d < \text{ord}_{p} x < 0.$$ 

Therefore there exists an $r \in \mathbb{Z}_{\geq 1}$ such that $x^{r} \in B(K_{\inf}, p, a, d)$ but $x^{r+1} \notin B(K_{\inf}, p, a, d)$. Hence if we set $y = x^{r}$, we see that $y \in B(K_{\inf}, p, a, d)$ but $xy \notin B(K_{\inf}, p, a, d)$. \hfill $\square$

### 4.3. Defining Integrality at finitely many primes using complete $q$-boundedness.

Our next step is to show that we can get away using $q$-boundedness only (without introducing $p$-boundedness for an additional prime $p$). The integrality at primes of $\mathcal{S}_{K_{\inf}}$ can be handeled with complete $q$-boundedness only using sets $B(K_{\inf}, q, a, d)$ for appropriately selected $a$ and $d$ as above, since the primes of $\mathcal{S}_{K}$ are not factors of $q$. Thus we need to make special arrangements for factors of $q$ only. Since we are going to use $q$-boundedness exclusively, we now drop Assumptions and Notation 4.4 and introduce the following assumptions and notation.

**Notation and Assumptions 4.7.** We will use the following notation and assumptions.

- Assume all the primes of $\mathcal{W}_{G}$ are completely $q$-bounded.
- Let $M_{q}$ be a completely $q$-bounding field for all primes in $\mathcal{W}_{G}$.
- Assume $\xi_{q} \in G$.
- Let $\mathcal{Q}_{G}$ be the set of all the factors of $q$ in $G$.
- Let $f_{q} = \max_{qM_{q} \in \mathcal{Q}_{G}} \{ f(qM_{q}/q) \}$.
- Let $F/\mathbb{Q}$ be a totally real cyclic extension of degree $q^{f_{q}+1}$, where $q$ does not split. (Such an extension exists by Lemma 2.19)

Now consider a cyclic extension $FK_{\inf}/K_{\inf}$ of degree $q^{r}$ (this extension is cyclic of degree equal to a power of $q$ by Lemma 2.20), where $0 \leq r \leq f_{q} + 1$. We claim that in fact $r > 0$. Assume the opposite. In this case for some $K \in I_{M_{q}}$ we have that $F \subseteq K$. But the relative degree of any factor of $q$ in $K$ is at most $f_{q}$, while the relative degree of all the factors of $q$ in $FK$ is bigger than $f_{q}$. Thus, $r > 0$.

Now let $E_{\inf}$ be the unique subfield of $FK_{\inf}$ such that $[FK_{\inf} : E_{\inf}] = q$ and $K_{\inf} \subset E_{\inf}$. Since $\xi_{q} \in E_{\inf}$, we must have $FK_{\inf} = E_{\inf}(\sqrt[k]{a})$ for some $a \in E_{\inf}$ (this is so by Theorem 6.2, page 288 of [15]). Let $b \in E_{\inf}$ generate $E_{\inf}$ over $K_{\inf}$. Now let $N \in I_{M_{q}}$ be such that $F \subset N(\sqrt[q]{a}, b)$, $a \in N(b)$, and $b$ is of the same degree over $N$ as over $K_{\inf}$. Let $K \in I_{N}$ and note that $b$ is of the same degree over $K$ as over $N$, $a \in K(b)$, and $F \subset K(\sqrt[q]{a}, b)$. 


Further, $KF = K(\sqrt[q]{a}, b)/K$ is a cyclic extension of degree $q^r$ for some $r > 0$, no factor of $q$ ramifies in this extension (by Proposition 8 of Chapter II, §4 of [14]), and no factor of $q$ splits in the extension $K(\sqrt[q]{a}, b)/K(b)$ by Lemma 2.21. By Lemma 2.23 we can also assume $a \in \Omega_q(K(b))$.

Since factors of $q$ in $N(b)$ do not ramify in the extension $N(b, \sqrt[q]{a})/N(b)$, if for some factor $\mathfrak{q}_{N(b)}$ of $q$ in $N(b)$ we have that ord$_{\mathfrak{q}_{N(b)}} a \neq 0$, we also must have ord$_{\mathfrak{q}_{N(b)}} a \equiv 0 \mod q$. Thus without loss of generality (multiplying $a$ by $q$-th powers of some elements of $N(b)$, if necessary), we can assume that $a$ has no occurrences of factors of $q$ in its divisor. Note that if $q = 2$, we would only be multiplying $a$ by squares and thus not changing the fact that $a \in \Omega_2(N(b))$.

Now let $\mathcal{A}_{N(b)} \subseteq \mathcal{C}_{N(b)}(q) = \mathcal{Q}_{N(b)}$ and let $d \in N(b)$ be such that for all primes $\mathfrak{q}_{N(b)} \in \mathcal{A}_{N(b)}$ we have that ord$_{\mathfrak{q}_{N(b)}} a \equiv 0 \mod q$. (As above, such a $d$ exists by the Strong Approximation Theorem.) The proposition below lets us bound the order of the poles the elements of our field can have at factors of $q$ in $\mathcal{A}_{N(b)}$.

Proposition 4.8. Let

$$C(E_{\text{inf}}, a, d, q) = \{ x \in K_{\text{inf}} \mid \exists y \in L_{a,x,d}(E_{\text{inf}}, q)(\sqrt[q]{a}) : N_{L_{a,x,d}(E_{\text{inf}}, q)(\sqrt[q]{a})/L_{a,x,d}(E_{\text{inf}}, q)}(y) = dx^q + d^q\}.$$  

We claim $C(E_{\text{inf}}, a, d, q) = \{ x \in K_{\text{inf}} \mid \forall K \in I_{N(b), \mathcal{A}} \forall \mathfrak{q}_K \in \mathcal{A}_K : \text{ord}_{\mathfrak{q}_K, x} x > \frac{1}{q} \text{ord}_{\mathfrak{q}_K} d \}$.

Proof. The proof of this proposition is almost identical to the proof of Proposition 4.3 except that it relies on Proposition 2.14 and Proposition 2.15 in lieu of Proposition 2.12 and Proposition 2.13.

As above we can use the definition of $C(E_{\text{inf}}, a, d, q)$ to obtain a definition $R_{K_{\text{inf}}, \mathcal{A}_{\text{inf}}}$. With the definition of $R_{K_{\text{inf}}, \mathcal{A}_{\text{inf}}}$ in mind, we now modify slightly the definition in Corollary 4.3 to replace $\Phi_q(K_{\text{inf}}, \mathcal{A}_{\text{inf}}) \cap \Phi_q(K_{\text{inf}})$ with an expression involving $R_{K_{\text{inf}}, \mathcal{A}_{\text{inf}}}$. Let $w \in G$ be such that ord$_{\mathfrak{q}_G} w = 3$ ord$_{\mathfrak{q}_G} q$ for any $\mathfrak{q}_G \in \mathcal{G}(q)$, ord$_{\mathfrak{q}_G} w = 1$ for any $\mathfrak{p}_G \in \mathcal{G}$, and $w$ has no other zeros. (As above such a $w$ exists by the Strong Approximation Theorem.)

Corollary 4.9.

$$x \in O_{K_{\text{inf}}, \mathcal{W}_{K_{\text{inf}}}}$$

$$\forall c \text{ such that } \left( \frac{(c-1)}{w} \right) R_{K_{\text{inf}}, \mathcal{W}_{K_{\text{inf}}}} \wedge c \in \Omega_q(K_{\text{inf}}) \right) \forall b \in K_{\text{inf}} \exists y \in L_{c,x,b,x}(K_{\text{inf}}, q)(\sqrt[q]{c}) : N_{L_{c,x,b,x}(K_{\text{inf}}, q)(\sqrt[q]{c})/L_{c,x,b,x}(K_{\text{inf}}, q)}(y) = bx^q + b^q.$$  

Proof. It is enough to observe the following. In any $K \in I_N$ the numerator of the divisor of $c-1$ is divisible by the numerator of the divisor of $q^3$ and by every $\mathfrak{p}_K$ in $\mathcal{G}_K$. Thus $c \in \Theta_q(K, \mathcal{A}_K) \cap \Phi_q(K)$. Conversely, if $c \in \Theta_q(K, \mathcal{A}_K) \cap \Phi_q(K)$, then the divisor $c-1$ is divisible by the numerator of the divisor of $q^3$ and by every $\mathfrak{p}_K$ in $\mathcal{G}_K$ and therefore $\frac{c-1}{w}$ does not have any poles at primes of $\mathcal{W}_K$, so that $\frac{(c-1)}{w} \in R_{K_{\text{inf}}, \mathcal{W}_{\text{inf}}}$. 

Since we have definitions of integrality at finitely many primes, the definition above can be converted to a definition of $O_{K_{\text{inf}}, \mathcal{W}_{\text{inf}}}$ in general and $O_{K_{\text{inf}}}$, in particular. We are now ready for our main definability theorem.
Theorem 4.10. Let $p, q$ be rational prime numbers, not necessarily distinct. Let $H$ be a number field, and let $H_{\inf}$ be an algebraic extension of $H$. Let $\mathcal{O}_H$ be a finite, possibly empty, set of primes of $H$. Assume all primes of $H$ not in $\mathcal{O}_H$ are hereditarily $q$-bounded in $H_{\inf}$, and primes in $\mathcal{O}_H$ and factors of $q$ are completely $p$-bounded in $H_{\inf}$. In this case, the integral closure of $O_H, \mathcal{O}_H$ in $H_{\inf}$ is first-order definable over $H_{\inf}$.

Proof. Given an arbitrary number field $H$ and an algebraic extension $H_{\inf}$ of $H$, not necessarily containing any roots of unity required above, we have to show that the norm equations we have been using in our definitions can be rewritten as polynomial equations with relevant solutions in $H_{\inf}$. Below we present an informal outline of this rewriting process. For a more general and formal discussion of the rewriting techniques we refer the reader to the section on coordinate polynomials in [34]. Let $G = H(\xi, \zeta)$, $K_{\inf} = H_{\inf}(\xi, \zeta)$.

We start with rewriting the norm equation itself. If $F$ is any field of characteristic 0 and $c \in F \setminus F^q$, $u_1, \ldots, u_q, z \in F$, $y = \sum_{i=1}^{q} a_i \sqrt[q]{c^{(i-1)}}$, then

$$N_F(\psi/F(y) - c = \prod_{j=0}^{q-1} \sum_{i=1}^{q} u_i \xi^{(i-1)j} \sqrt[q]{c^{(i-1)}} - z = N(u_1, \ldots, u_q, c, z) \in \mathbb{Z}[U_1, \ldots, U_q, C, Z],$$

and the coefficients of $N(U_1, \ldots, U_q, C, Z)$ depend on $q$ only.

If $c, w \in F, c = w^q$, then for any $z \in F$ the equation $N(U_1, \ldots, U_q, c, z) = 0$ has solutions $a_1, \ldots, a_q \in F(\xi)$. Indeed, consider the following system of equations:

$$\begin{cases} \sum_{i=0}^{q-1} a_i w^i = z, \\ \sum_{i=0}^{q-1} a_i \xi^{ij} w^i = 1, j = 1, \ldots, q - 1 \end{cases}$$

This is a nonsingular system with a matrix $(\xi^{ij} w^i), i = 0, \ldots, q - 1, j = 0, \ldots, q - 1$ having all of its entries in $F(\xi)$. Since the vector $(z, 1, \ldots, 1)$ also has all of its entries in $F(\xi)$, we conclude that the system has a unique solution in $F(\xi)$. So if we, for example, consider $N_{L_{c,x,b,x}(K_{\inf}, q)}(\psi/F(\xi)) = bx^q + b^q$ with potential solutions $y$ ranging over $L_{c,x,b,x}(K_{\inf}, q)(\sqrt[q]{c})$, then we can conclude that this norm equation is equivalent to a polynomial equation

$$N(u_1, \ldots, u_q, c, bx^q + b^q) = 0$$

with coefficients in $\mathbb{Z}$ and potential solutions

$$u_1, \ldots, u_q \in L_{c,x,b,x}(K_{\inf}, q) = N_{x,b,x}(K_{\inf}, q)(\sqrt[q]{1 + (c + c^{-1})x^{-1}}).$$

We now would like to replace (4.10) by an equivalent equation but with solutions in $N_{x,b,x}(K_{\inf}, q)$. We have to consider two options: either there exists $\gamma \in N_{x,b,x}(K_{\inf}, q)$ such that

$$\gamma^q = 1 + (c + c^{-1})x^{-1}$$

and in this case all the solutions $u_1, \ldots, u_q \in N_{x,b,x}(K_{\inf}, q)$, or $1 + (c + c^{-1})x^{-1}$ is not a $q$-th power in $N_{x,b,x}(K_{\inf}, q)$ so that $u_i = \sum_{j=0}^{q-1} u_{i,j} \gamma^j$, where $\gamma$ is as in (4.11) and $u_{i,j} \in N_{x,b,x}(K_{\inf}, q)$. In the latter case we can rewrite (4.11) first as

$$N(\sum_{j=0}^{q-1} u_{1,j} \gamma^j, \ldots, \sum_{j=0}^{q-1} u_{q,j} \gamma^j, c, bx^q + b^q) = 0,$$
and then a system of equations over \( N_{x,b,x}(K_{\text{inf}}, q) \) using the fact that the first \( q \) powers of \( \gamma \) are linearly independent over \( N_{x,b,x}(K_{\text{inf}}, q) \). Thus for any \( c,b,x \in K_{\text{inf}} \) we can conclude that (4.10) has solutions \( u_1, \ldots, u_q \in L_{c,x,b,x}(K_{\text{inf}}, q) \) if and only if either there exists \( \gamma \in N_{x,b,x}(K_{\text{inf}}, q) \) satisfying (4.11) and there exists \( u_1, \ldots, u_q \in N_{x,b,x}(K_{\text{inf}}, q) \) satisfying (4.10) or there exist \( u_{1,0}, \ldots, u_{q,q-1} \in N_{x,b,x}(K_{\text{inf}}, q) \) satisfying (4.12) rewritten as a system of equations with coefficients in \( N_{x,b,x}(K_{\text{inf}}, q) \) under the assumption that \( 1, \gamma, \ldots, \gamma^{q-1} \) are linearly independent over \( N_{x,b,x}(K_{\text{inf}}, q) \).

Proceeding in the same fashion we can eventually obtain an equivalent system of equations with potential solutions in \( K_{\text{inf}} \). Now if a given field \( H_{\text{inf}} \) does not contain \( \xi_q \) or \( \xi_p \), then we can rewrite all the equations one more time so that the final system has solutions and coefficients in \( H_{\text{inf}} \).

We can also separate out results concerning integrality at finitely many primes.

**Theorem 4.11.** The following statements are true.

1. If a \( G \)-prime \( p_G \) is completely \( q \)-bounded, \( M \) is a \( q \)-bounding field for \( p_G \), \( b \in K_{\text{inf}} \) is such that for some \( p_{M(b)} \in \mathcal{C}_{M(b)}(p_G) \) we have that \( \text{ord}_{p_{M(b)}} b \neq 0 \mod q \) \( \land \) \( \text{ord}_{p_{M(b)}} b < 0 \), and \( b \) has no other poles, then the set of all elements \( x \in K_{\text{inf}} \) such that \( \text{ord}_{p_{M(x,b)}} x \geq \frac{q-1}{q} \text{ord}_{p_{M(x,b)}} b \) for all \( p_{M(x,b)} \in \mathcal{C}_{M(b,x)}(p_{M(b)}) \) is existentially definable.

   (For future reference in Section 7 denote this set by \( \text{Int}(b, p_{M(b)}, q) \).)

2. If ramification degrees over \( G \) of all factors of \( p_G \) in number fields contained in \( I_G \) are uniformly bounded, then the integral closure of the valuation ring of \( p_G \) in \( K_{\text{inf}} \) is existentially definable.

We now make use of unbounded primes.

**Theorem 4.12.** Let \( \mathcal{S}_G \cup \{ \text{factors of } q \} \) be a completely \( q \)-bounded in \( K_{\text{inf}} \) finite set of primes of \( G \), and let \( R_{\text{inf}, \mathcal{S}_G} \) be a subring of \( K_{\text{inf}} \) such that \( x \in R_{\text{inf}, \mathcal{S}_G} \) if and only if in \( G(x) \) the poles of \( x \) are either factors of \( q \) or primes of \( \mathcal{S}_G \), or are at primes that are \( q \)-unbounded. In this case \( R_{\text{inf}, \mathcal{S}_G} \) is first-order definable over \( K_{\text{inf}} \).

**Proof.** It is enough to consider what happens to the solvability of the norm equation below for \( c \) chosen so that factors of \( q \) and primes in \( \mathcal{S}_G \) split and \( x \) has poles only at the primes described in the statement of the theorem. So let \( K \in I_G \) and consider

\[
N_{L_{c,x,b,x}(K,q)(\sqrt[K]{q})/L_{c,x,b,x}(K,q)}(y) = b x^q + b^q.
\]

As above, since factors of \( q \) and primes in \( \mathcal{S}_G \) split, this equation will be solvable locally at these primes. Now as far as unbounded primes are concerned, we can always consider the norm equation over \( K \) large enough so that factors of the unbounded primes ramify with ramification degree divisible by \( q \) or their relative degree goes up by a factor divisible by \( q \). Over this \( K \), either these factors split completely when we adjoin the \( q \)-th root of \( c \) or the right side of the norm equation has order divisible by \( q \) at the factors of these \( q \)-unbounded primes. Thus, in any case of large enough \( K \), the norm equation is solvable at all the factors of unbounded primes.

One can prove a few more variations of the results above. The theorem below is an example of such results. Its proof is completely analogous to the proofs above.
Theorem 4.13. Let \( \{p_1, \ldots, p_k\} \) be a finite set of rational primes such that each prime of \( G \) is hereditarily \( p_i \)-bounded in \( K_{inf} \) with respect to some \( p_i \), and each \( p_i \) is completely \( p_j \)-bounded for some \( p_j \). In this case \( O_{K_{inf}} \) is first-order definable over \( K_{inf} \).

5. Examples of Infinite Extensions of \( \mathbb{Q} \) Where the Ring of Integers Is First-Order Definable

In this section we describe some examples to which our methods apply. Some of these examples will be pretty straightforward while others are more esoteric. We start with the more straightforward examples.

Example 5.1 (Fields with Uniformly Bounded Local Degrees). Perhaps the simplest example of a \( q \)-bounded infinite extension of rationals is an infinite extension where the local degrees of all primes are uniformly bounded. In such a field every prime is completely \( q \)-bounded for any prime \( q \). An example of such an extension is an infinite Galois extension generated by all extensions of degree \( p \) (for a fixed prime \( p \)) of \( \mathbb{Q} \) contained in cyclotomics. More examples of such fields can be found in [1]. Most of such examples where the field is Galois over \( \mathbb{Q} \) were already covered by definability results of Videla with respect to the ring of integers. However, one can construct many non-Galois examples of such fields. It is enough to take a collection \( \{K_i\} \) of number fields which are Galois but not abelian over \( \mathbb{Q} \), linearly disjoint over \( \mathbb{Q} \), of degree less or equal to some fixed \( n \) over \( \mathbb{Q} \), and consider a collection of number fields \( \{N_i\} \), where \( N_i \subset K_i \) and \( N_i \) is not Galois over \( \mathbb{Q} \). Now let \( N_{inf} \) be the compositum of all \( N_i \) inside \( \mathbb{Q} \). If \( K_{inf} \) is the compositum of all \( K_i \) inside \( \mathbb{Q} \), then \( N_{inf} \subset K_{inf} \) and \( [K_{inf} : N_{inf}] = \infty \). Thus, while Videla’s results give us a first-order definition of \( O_{K_{inf}} \) over \( K_{inf} \), they do not give us a first-order definition of \( O_{N_{inf}} \) over \( N_{inf} \), obtainable by our methods. Further our methodology also produces the first-order definition of the integral closures of small rings of rational numbers in \( K_{inf} \) and \( N_{inf} \) over \( K_{inf} \) and \( N_{inf} \) respectively.

Example 5.2 (Galois extensions without cyclic subextensions of degree divisible by arbitrarily high powers of \( q \)). If \( K_{inf} \) is a Galois extension of a number field \( G \) such that for any Galois \( K \in I_G \), we have that \( [K : G] \neq 0 \mod q \), then \( O_{K_{inf}} \) and any small subring of \( K_{inf} \) is first-order definable over \( K_{inf} \).

It is not hard to see that in this case ramification and relative degrees in all finite subextensions are prime to \( q \) and thus all the primes are completely \( q \)-bounded. This example covers cyclotomic extensions with finitely many ramified primes, i.e. extensions of the form \( \mathbb{Q}(\xi_{p_1}, \ldots, \xi_{p_k}, \ell \in \mathbb{Z}_{>0}) \), where \( p_1, \ldots, p_k \) are rational primes, and all their subfields that include all abelian extensions with finitely many ramified primes. (The definability of rings of integers in these extensions follows from Videla’s results.)

Given a prime \( q \), and an integer \( m > 0 \), our method also applies to the case of a cyclotomic extension (and any of its subfields) generated by the set

\[
\{\xi_p|\ell \in \mathbb{Z}_{>0}, p \neq q \text{ is any prime such that } q^{n+1} \not| (p - 1)\}.
\]

(In other words we need to omit primes occurring in the arithmetic sequence \( kq^{n+1} + 1, k \in \mathbb{Z}_{>0}, \) and by increasing \( m \), we can make the density of the omitted primes arbitrary small.) This example generalizes an example of Fukuzaki where he defined integers over the field \( \mathbb{Q}(\{\cos(2\pi/\ell^n) : \ell \in \Delta, n \in \mathbb{Z}_{>0}\}) \) and any of its Galois subextensions, and where \( \Delta \) is the set of all the prime integers which are congruent to 1 modulo 4.
On top of such a cyclotomic field we can also add a field generated by any subset of $p$-th roots of algebraic numbers contained in this cyclotomic field, with $p$ as above not equivalent to 1 modulo $q^{m+1}$. Clearly, many more examples of Galois extensions of this sort can be generated.

As we pointed above, being Galois is not required for our method to work. Thus we have some obvious examples of non-Galois extensions where we can define integers.

**Example 5.3** (Extensions that are not necessarily Galois). If $K_{\text{inf}}$ is a tower of finite extensions of degree less than some positive integer $m$, then $O_{K_{\text{inf}}}$ and any small subring of $K_{\text{inf}}$ are first-order definable over $K_{\text{inf}}$. Observe that a field of this sort can have primes of arbitrarily large or infinite local degree, and thus this example is a non-trivial generalization of the first example.

If the extension is Galois, we are looking at a field discussed in the second example. So the new cases will come from extensions that are not Galois. Observe, that in such a field for any $q > m$ all the primes are completely $q$-bounded.

It is more difficult to describe examples where primes are not necessarily completely $q$-bounded.

**Example 5.4** (Less natural fields). Let $q$ be a rational prime and let $\{p_1, \ldots\}$ be a listing of all rational primes omitting $q$. Let $\pi_i = \prod_{j=1}^i p_j$. Let $G$ be any number field and let $\{p_1, \ldots\}$ be a listing of all primes of $G$ not lying above $q$. We construct a tower of fields starting with $G$ where all factors of $q$ are completely $q$-bounded, all the other primes of $G$ and any finite extension of $G$ are $q$-bounded but not completely $q$-bounded and are $p$-unbounded for any other prime $p$. Let $K_0 = G$ and assume we have constructed $K_1, \ldots, K_n$ for some $n \geq 0$. We now construct $K_{n+1}$ in three steps.

First we construct an extension $M_{n,1}$ of $K_n$ of degree $\pi_n$, where all the primes above $p_1, \ldots, p_n$ will have ramification degrees divisible by $\pi_n$ and all the primes above $q$ split completely. (Such an extension always exist. For example take an element $a$ of $O_{K_n}$ such that $\text{ord}_p a = 1$ for $i = 1, \ldots, n$ and $a \equiv 1 \mod q$ and adjoin $\sqrt[n]{a}$ to $K_n$.) This step insures that the ramification degree of factors of any prime of $G$ not dividing $q$ will eventually be divisible by arbitrarily high powers of rational primes distinct from $q$.

We now construct a non-trivial extension $M_{n,2}$ of $M_{n,1}$ where all the factors of $p_1, \ldots, p_n$ and $q$ in $M_{n,1}$ split completely into distinct factors. (For example we can adjoin $\sqrt[n]{b}$, where $p$ is prime to $p_1, \ldots, p_n$ and $q$ and $b \equiv 1 \mod (q p_1 \ldots p_n)$.) This step allows us to produce $q$-bounded and $q$-unbounded paths above every prime.

Finally $K_{n+1}$ is an extension of $M_{n,2}$ of degree $q$ satisfying the following requirements:

1. All the factors of $q$ split completely.
2. For each $i = 1, \ldots, n$ and each $t_i$ that is a factor of some $p_i$ in $M_{n,1}$, if $t_{i,1}, \ldots, t_{i,k}$ are factors of $t_i$ in $M_{n,2}$ under some ordering, then $t_{i,1}$ splits completely into distinct factors and $t_{i,2}, \ldots, t_{i,k}$ do not split in the extension $K_{n+1}/M_{n,2}$.

To construct such an extension, by Lemma [2.10] we can take a $q$-th root of an algebraic integer of $M_{n,2}$ such that it is equivalent to 1 mod $q^3$ and modulo $t_{i,1}$, and to a non-$q$-th power modulo $t_{i,j}$, $j \geq 2$. In this step we construct the next level of $q$-bounded and $q$-unbounded paths. At the “end” of the construction every prime of any $K_n$ not dividing $q$, will lie along the “left-most” $q$-bounded path, and the “right-most” $q$-unbounded path. (In
fact, every prime not dividing \(q\) will lie along infinitely many \(q\)-bounded and \(q\)-unbounded paths.)

We now let \(K_{\text{inf}} = \bigcup_{i=1}^{\infty} K_i\).

It is easy to see that for all \(K \in I_G\) every factor of \(q\) is unramified and of relative degree 1. At the same time, for any \(p \neq q\), any positive integer \(m\), and any \(p_i\) prime to \(q\), there is a field \(K \in I_G\) where all the factors of \(p_i\) have a ramification degree over \(p_i\) divisible by \(p^m\).

Further, for \(i \in \mathbb{Z}_{>0}\), let \(d_i = \max_{p_{K_{i+1}} \in G_{K_{i+1}}(p_i)} \{\text{ord}_q(d(p_{K_{i+1}}/p_i))\}\), and note that for any \(p_i\), for any \(K \in I_G\) there exists a \(K\)-factor \(p_K\) of \(p_i\) such that \(\text{ord}_q(d(p_K/p_i)) \leq d_i\), while at the same time for any \(m \in \mathbb{Z}_{>0}\), there exist a field \(M \in I_G\) and an \(M\)-factor \(p_M\) of \(p_i\) such that \(f(p_K/p_M) \equiv 0 \mod q^m\).

We can also produce an example where one would need Theorem 4.13. The construction is similar to the one above and, in particular, the existence of extensions we need can be justified by similar arguments.

**Example 5.5** (Also not very natural fields). Let \(Q = \{q_1, \ldots, q_m\}\) be a finite collection of rational primes. Let \(\{p_1, \ldots\}\) be a listing of all rational primes excluding the primes in \(Q\). Let \(\pi_i = \prod_j p_j\). Let \(G\) be any number field and divide all the primes of \(G\) not lying above any prime of \(Q\) into \(m\) classes with \(\{p_{ij}, i = 1, \ldots, m, j \in \mathbb{Z}_{>0}\}\). We now construct a tower of fields \(\{K_i\}\) with \(K_{\text{inf}}\), as above, being the union of the tower. Let \(K_0 = G\) and assume that \(K_n\) for some \(n \geq 0\) has been constructed. We construct \(K_{n+1}\) in \(m+1\) steps. First let \(M_{0,n}/K\) be an extension of degree \(\pi_{n+1}\) such that

1. All the primes above \(Q\) split completely.
2. All the primes in the set \(\{p_{ij}, i = 1, \ldots, m, j = 1, \ldots, n+1\}\) ramify totally.

Next we construct \(M_{i,n}/M_{i-1,n}\) for \(i = 1, \ldots, m\). First of all, the degree of the extension will be \(q_i\). Secondly, all the primes above the primes of \(Q\) and all the primes above the primes in the set \(\{p_{ij}, j = 1, \ldots, n+1\}\) split completely. Thirdly, all the primes in the set \(\{p_{i,j}, r = 1, \ldots, m, r \neq i, j = 1, \ldots, n+1\}\) remain prime. Finally, \(K_{n+1} = M_{m,n}\).

It is not hard to see that for each \(i = 1, \ldots, m\) the primes \(\{p_{ij}, j = 1, \ldots, \}\) of \(G\) are completely \(q_i\)-bounded and these primes are \(p\)-unbounded for any prime \(p \neq q\). Further, all the primes above \(Q\) are completely \(q\)-bounded for any prime \(q\). Thus we need to use Theorem 4.13 here to get the desired definitions.

We should finish this section with a listing of some obvious fields which are **not** \(q\)-bounded: \(\bar{Q}\), the maximal abelian extension of \(Q\), the field of all totally real integers. In general examples of such fields are also not hard to generate. Observe that one would expect the field of all totally real integers not to be \(q\)-bounded since, as has been noted above, the first-order theory of the field of all totally real integers is decidable, while this is not the case for the ring of integers of this field. Thus, the ring of integers of the field of all totally real integers does not have a first-order definition over it fraction field.

### 6. From Undecidability of Rings to Undecidability of Fields

We start with reviewing results we are going to use due to Krönecker, Julia Robinson and the author of this paper. We start with reviewing the results of Julia Robinson from [27].
Theorem 6.1 (JR). If a family of finite sets including all finite initial segments of the natural numbers is arithmetically definable in an algebraic integer ring $R$, then the set of natural numbers $\mathbb{N}$ is arithmetically definable in $R$, and $R$ is undecidable.

Theorem 6.2 (JR). If a family $\mathcal{F}$ of sets of a totally real algebraic integer ring $R$ containing arbitrarily large finite sets can be arithmetically defined in $R$, then the natural numbers can be defined arithmetically in $R$. Hence $R$ is undecidable.

Corollary 6.3 (JR). The natural numbers can be defined arithmetically in any totally real algebraic integer ring $R$ such that there is a smallest interval $(0, s)$, $s$ real or $\infty$, which contains infinitely many sets of conjugates of numbers of $R$, i.e., infinitely many $x \in R$ with all the conjugates (over $\mathbb{Q}$) in $(0, s)$.

For the case of non totally real rings we have a weaker theorem, elaboration of which by Henson was used by Videla in [41] to prove the undecidability in some cyclotomic rings of integers.

Theorem 6.4 (JR). A model of the arithmetic of natural numbers can be defined arithmetically in any algebraic integer ring $R$ such that a family $\mathcal{F}$ of finite sets containing arbitrarily large finite sets is arithmetically definable in $R$.

Julia Robinson [27] and Fukuzaki [11] makes use of the following proposition which is a consequence of a result by Kronecker from [13].

Proposition 6.5 (Kronecker). The interval $(0, 4)$ contains infinitely many sets of conjugates of totally real algebraic integers and no sub-interval of $(0, 4)$ does.

An immediate consequence of Theorems 6.3 and 6.5 is that any ring of totally real integers containing a set of the form $\{\cos(2\pi/m), m \in \mathcal{I}\}$ with $\mathcal{I}$ infinite, one can give a first-order definition of integers. Thus extending results of Fukuzaki we now have the following theorems.

Theorem 6.6. Let $q$ be a rational prime, let $m > 0$ be an integer and let

$$K_{\text{inf}} = \mathbb{Q}(\cos(2\pi/n), n = \prod_{i=1}^{s} p_i^{\ell_i}, p_i \not\equiv 1 \mod q^m, s, \ell_1, \ldots, \ell_s \in \mathbb{Z}_{>0}),$$

where $p_i$ range over all primes satisfying the condition $p \not\equiv 1 \mod q^m$. In this case the first-order theory of $K_{\text{inf}}$ is undecidable and $\mathbb{Z}$ is first-order definable $K_{\text{inf}}$.

Since the ring of all totally real integers is undecidable, every ring of totally real integers is trivially contained in an undecidable ring. However, this is not automatically clear for the fields, since the first-order theory of the field of all totally real numbers is decidable. While we cannot show that the first-order theory of any $q$-bounded totally real field is undecidable, we can show the following.

Theorem 6.7. Any $q$-bounded totally real field is contained in a totally real field that has a first-order definition of rational integers and thus has an undecidable first-order theory. Alternatively, any maximal totally real $q$-bounded field has a first-order definition of rational integers and an undecidable first-order theory.

Proof. Let $K_{\text{inf}}$ be a $q$-bounded field and observe that $K_{\text{inf}}(\cos(2\pi/p^k), k \in \mathbb{Z}_{>0})$ for some $p \not\equiv q$ is also $q$-bounded, since we will introduce at most a finite number of subextensions
of degree divisible by \(q\). (In other words, the increase in divisibility by \(q\) of relative or ramification degrees can come only from adding the extension \(\mathbb{Q}(\cos 2\pi/p)\) of degree \((p-1)/2\) over \(\mathbb{Q}\).) But the ring of integers of the extended field is now undecidable and has a first-order definition of the rational integers, by the discussion above. Thus, since the extended field is still \(q\)-bounded, we have that the extended field has a first-order definition of rational integers and an undecidable first-order theory.

A maximal totally real \(q\)-bounded extension must contain a set \(\{\cos(2\pi/p^k), k \in \mathbb{Z}_{>0}\}\) and thus the argument above applies.

We now turn our attention to non-real fields. In \([40]\), Videla showed that the ring of integers is definable in infinite Galois algebraic extensions of \(\mathbb{Q}\) where every finite subextension is a power of a fixed prime \(p\). (Such a field is \(q\)-bounded for any \(q \neq p\).) Further, as mentioned above, in \([41]\), Videla proved using Theorem 6.4 of Julia Robinson that the ring of integers of \(\mathbb{Q}(\xi_{p^r}, r \in \mathbb{Z}_{>0})\) is undecidable. Combining the two results, he also obtained the first-order undecidability of \(\mathbb{Q}(\xi_{p^r}, r \in \mathbb{Z}_{>0})\).

Below we prove the following proposition.

**Theorem 6.8.** Rational integers are first-order definable in any abelian extension of \(\mathbb{Q}\) with finitely many ramified primes, and therefore the first-order theory of such fields is undecidable.

Rather than relying on the result of Julia Robinson, we use existential definability and undecidability results from \([35]\) and \([32]\), where the following result was proven.

**Theorem 6.9.** Let \(A_{\text{inf}}\) be an abelian (possibly infinite) extension of \(\mathbb{Q}\) with finitely many ramified primes. Then for any number field \(A \subseteq A_{\text{inf}}\) and any finite non-empty set \(\mathcal{P}_A\) of its primes, we have that \(\mathbb{Z}\) is existentially definable in the integral closure of \(O_A, \mathcal{P}_A\) in \(A_{\text{inf}}\).

Now Theorem 6.8 follows from the fact that any abelian extension with finitely many ramified primes must by Kronecker’s Theorem be a subfield of a cyclotomic extension with finitely many ramified primes, i.e. an extension where prime divisors of the degrees of all finite subextensions come from a finite set of primes. Such an extension is \(q\)-bounded for any odd \(q\) not occurring in the above mentioned finite set of primes, by Example 5.2. Further, all the primes of \(\mathbb{Q}\) are completely \(q\)-bounded for such a \(q\). Thus, any small subring is first order definable over any abelian extension of \(\mathbb{Q}\) with finitely many ramified primes, and therefore by Theorem 6.9 we conclude that rational integers are first-order definable over any abelian extension of \(\mathbb{Q}\) with finitely many ramified primes. Since the set of non-zero integers is definable over any ring of algebraic integers, we can “simulate” the field over the ring of integers, and therefore obtain the following corollary:

**Corollary 6.10.** Rational integers are first-order definable in the ring of integers of any abelian extension of \(\mathbb{Q}\) with finitely many ramified primes, and therefore the first-order theory of such a ring is undecidable.

### 7. Using Elliptic Curves with Finitely Generated Groups

In this section we show that over the fields with finitely generated elliptic curves, assuming one completely \(q\)-bounded prime, we can define \(\mathbb{Z}\) and conclude that the first-order theory is undecidable.
The use of elliptic curves to investigate definability and decidability has a long history. Perhaps the first mention of elliptic curves in the context of the first-order definability belongs to Raphael Robinson in [28] and in the context of existential definability to Denef in [4]. Using elliptic curves Bjorn Poonen has shown in [19] that if for a number field extension $M/K$ we have an elliptic curve $E$ defined over $K$, of rank one over $K$, such that the rank of $E$ over $M$ is also one, then $O_K$ (the ring of integers of $K$) is Diophantine over $O_M$. Cornelissen, Pheidas and Zahidi weakened somewhat assumptions of Poonen’s theorem. Instead of requiring a rank 1 curve retaining its rank in the extension, they require existence of a rank 1 elliptic curve over the bigger field and an abelian variety over the smaller field retaining its positive rank in the extension (see [2]). Further, Poonen and the author have independently shown that the conditions of Poonen’s theorem can be weakened to remove the assumption that the rank is one and require only that the rank in the extension is positive and the same as the rank over the ground field (see [30] and [18]). In [3] Cornelissen and the author of this paper used elliptic curves to define a subfield of a number field using one universal and existential quantifiers.

Elliptic curve specifically of rank 1 have been used in several papers in connection to discussions of definability and decidability over big subrings of number fields. See [20], [23], [7], [17], [8] and [38].

Following Denef in [5], as has been mentioned above, the author also considered the situations where elliptic curves had finite rank in infinite extensions and showed that when this happens in a totally real field one can existentially define $\mathbb{Z}$ over the ring of integers of this field and the ring of integers of any extension of degree 2 of such a field (see [37]).

Recently, in [16], Mazur and Rubin showed that if Shafarevich-Tate conjecture held over a number field $K$, then for any prime degree cyclic extension $M$ of $K$, there existed an elliptic curve of rank one over $K$, keeping its rank over $M$. Combined with Poonen’s theorem, this new result shows that Shafarevich-Tate conjecture implied HTP is undecidable over the rings of integers of any number field.

Videla also used finitely generated elliptic curves to produce undecidability results. His approach, as discussed above, was based on an elaboration by Henson of a proposition of Julia Robinson and results of Rohrlich (see [29]) concerning finitely generated elliptic curves in infinite algebraic extensions.

The main ideas for the proof below have been articulated in [3] for the number field case. Here only a minor adjustment is required. We start with reviewing two technical lemmas which can be found in [19]. Let $E$ be an elliptic curve defined over a number field $K$ and fix an affine Weierstrass equation for the curve. Let $P \in E(K)$ be a point of infinite order, let $n \in \mathbb{Z}_{\neq 0}$, and let $(x_n, y_n)$ be the coordinates corresponding to $[n]P$ under the chosen Weierstrass model. Given $x \in K$, let $\mathfrak{n}(x)$ be the integral divisor which is the numerator of the divisor of $x$ in $K$. Further let $\mathfrak{d}(x) = \mathfrak{n}(x^{-1})$.

**Lemma 7.1.** Let $\mathfrak{A}$ be any integral divisor of $K$ and let $m$ be a positive integer. Then there exists $k \in \mathbb{Z}_{>0}$ such that $\mathfrak{A}|\mathfrak{d}(x_{km})$ in the integral divisor semigroup of $K$.

**Lemma 7.2.** There exists a positive integer $m$ such that for any positive integers $k, l$,

$$\mathfrak{d}(x_{lm}) | n \left( \frac{x_{lm}}{x_{klm}} - k^2 \right)^2$$

in the integral divisor semigroup of $K$. 

27
The following proposition can be found in [3]. We include its short proof for the convenience of the reader.

**Proposition 7.3.** Let \( N/K \) be a number field extension of degree \( n \). Let \( \Omega \) be a prime of \( K \) and let \( q_1, \ldots, q_m \) be all the primes of \( N \) lying above \( \Omega \). Let \( u \in N \) be integral at \( \Omega \). Assume further there exists a sequence \( \{k_i, y_i\} \) where \( k_i \in \mathbb{Z}_{>0}, k_{i+1} > k_i, y_i \in K \) with \( \text{ord}_{q_i} \ y_i \geq 0 \) and such that for all \( i, j \) we have that \( \text{ord}_{q_j}(u - y_i) > k_i \). Then \( u \in K \).

**Proof.** Let \( \alpha \in N \) be a generator of \( N \) over \( K \) such that \( \alpha \) is integral with respect to \( \Omega \). Let \( D \) be the discriminant of the power basis of \( \alpha \). Using this power basis we can represent any \( w \in M \) in the following form:

\[
w = \sum_{r=0}^{n-1} b_r \alpha^r
\]

with \( Db_r \in K \) and integral at \( \Omega \). Note that for some \( a_0, a_1, \ldots, a_{n-1} \in K \) we have that

\[
u - y_i = (a_0 - y_i) + \sum_{r=1}^{n-1} a_r \alpha^r
\]

and

\[
\text{ord}_{q_j}(u - y_i) > k_i, j = 1, \ldots, m.
\]

Let \( \ell \) be a positive integer and choose \( i \) such that \( k_i > n(\ell + \text{ord}_\Omega D) \). In this case

\[
u - y_i \equiv 0 \mod \Omega^{\ell + \text{ord}_\Omega D}
\]

in the integral closure of the valuation ring of \( \Omega \) in \( N \). Let \( B \in K \) be such that

\[
\text{ord}_\Omega B = \ell + \text{ord}_\Omega D.
\]

Observe that \( \frac{u - y_i}{B} \) is integral at \( \Omega \), and therefore \( Db_r \) is integral at \( \Omega \) implying that \( \text{ord}_\Omega a_r \geq \ell \) for \( r = 1, \ldots, n-1 \). Since \( \ell \) can be arbitrarily large, \( a_r = 0, r = 1, \ldots, n-1 \) and \( u \in K \). \hfill \Box

We now use the our results on defining integrality at a single number field prime to obtain the following proposition.

**Theorem 7.4.** Let \( p_G \) be a completely \( q \)-bounded in \( K_{\text{inf}} \) prime of \( G \). If there exists an elliptic curve \( E \) defined over \( G \) such that \( \text{rank}(E(K_{\text{inf}})) > 0 \) and \( E(K_{\text{inf}}) = E(G) \), then \( Q \) is first-order definable over \( K_{\text{inf}} \) with only one variable in the range of the universal quantifier.

**Proof.** Fix an affine Weierstrass equation \( y^2 = x^3 + ax + c \) for \( E \) and identify non-zero points of \( E(K_{\text{inf}}) \) with pairs of solutions to the Weierstrass equations as above. Let \( b \in K_{\text{inf}} \) be such that it satisfies conditions of Theorem [4.4] Part 1 with respect to all prime factors of \( p_G \) in \( M(b) \), i.e. \( \text{ord}_{p_G(b)} b < 0 \) and \( \text{ord}_{p_G(b)} b \not\equiv 0 \mod q \) for all \( p_G(b) \in \mathcal{C}_M(b)(p_G) \), where \( M \) is a completely bounding field for \( p_G \). Let \( u \in K_{\text{inf}} \) be such that \( ub \in \text{Int}(b, p_G, q) \) and

\[
\forall z \in K_{\text{inf}} \exists (a_1, b_1), (a_2, b_2) \in E(K_{\text{inf}}):
\]

\[
\frac{b_z^2}{2a_1} \in \text{Int}(b, p_G, q) \land (u - \frac{a_1}{a_2})^2 a_1 \in \text{Int}(b, p_G, q).
\]

(7.1)
We claim that if the formula is true for some $u \in N = M(b, u)$, then, by Proposition 7.3, we have that $u \in G$. Indeed, given a $z \in N$ and $\frac{b^2}{za_2} \in Int(b, p_G, q)$, we have that for all $p_N$ lying above $p_G$, it is the case that

$$\text{ord}_{p_N} \frac{b^2}{za_1} > \left(\frac{q - 1}{q}\right) \text{ord}_{p_N} b$$

implying

$$-\text{ord}_{p_N} z + \text{ord}_{p_N} \frac{1}{a_1} > \left(\frac{q - 1}{q} - 2\right) \text{ord}_{p_N} b = \left(-1 - \frac{1}{q}\right) \text{ord}_{p_N} b > -\text{ord}_{p_N} b > 0.$$ 

So that we have

$$\text{ord}_{p_N} \frac{1}{a_1} > \text{ord}_{p_N} z - \text{ord}_{p_N} b > \text{ord}_{p_N} z.$$ 

The second part of the conjunction in (7.1) now implies

$$2 \text{ord}_{p_N} \left(u - \frac{a_1}{a_2}\right) > \frac{q - 1}{q} \text{ord}_{p_N} b + \text{ord}_{p_N} \frac{1}{a_1} > \frac{q - 1}{q} \text{ord}_{p_N} b - \text{ord}_{p_N} z > \text{ord}_{p_N} z.$$ 

Since $z$ can be any element of $N$ and $\frac{u}{a_2} \in G$, it follows at once from Proposition 7.3 that $u \in G$.

Now assume that $u = k^2$ with $k \in \mathbb{Z}$. Let $(x_1, y_1) \in E(G)$ be the affine coordinates with respect to a chosen Weierstrass equation of a point $P \in E(G)$ of infinite order, as above. Then by Lemma 7.2 there exists a positive integer $m$ such that for any positive integer $l$,

$$\mathfrak{d}(x_{lm}) \mid n \left(\frac{x_{lm}}{x_{krm}} - k^2\right)^2$$

in the integral divisor semigroup of $G$. Further, by Lemma 7.1 we have that for any positive $C$, for some $r$ it is the case that $\text{ord}_{p_N} x_{rm} < -C$. So given a $z \in K_{\inf}$, let $a_1 = x_{rm}, a_2 = x_{krm}$ with $r$ chosen so that $\mathfrak{d}(b^2) n(z) \mid \mathfrak{d}(x_{rm})$ in the integral divisor semigroup of $G(b, z)$ and observe that the first part of the Conjunction (7.1) is satisfied. Next we note that for $N = G(b, z)$, since $\text{ord}_{p_N} b < 0$ we have that $\text{ord}_{p_N} x_{rm} < 0$, and since

$$\mathfrak{d}(x_{rm}) \mid n \left(\frac{x_{rm}}{x_{krm}} - k^2\right)^2,$$

we also must have that

$$\text{ord}_{p_N} \left(\frac{x_{rm}}{x_{krm}} - k^2\right)^2 x_{rm} \geq 0,$$

and thus the second part of the conjunction (7.1) is satisfied.

Finally we note that any positive integer can be written as a sum of four squares, and any element of $G$ can be expressed as a linear combination of some basis elements with rational coefficients.

$\square$

In view of the above proposition we have the following theorem.
Theorem 7.5. Let $q$ be a rational prime and let $K_{\text{inf}}$ be an infinite algebraic extension of $\mathbb{Q}$ with at least one prime of a number field contained in $\mathbb{Q}$ completely $q$-bounded. Assume also there exist an elliptic curve defined over $K_{\text{inf}}$ such that its Mordell-Weil group has positive rank and is finitely generated. In this case $\mathbb{Z}$ is first-order definable over this field and therefore the first-order theory of this field is undecidable.

This theorem provides another way to improve results due to Videla in [41], where finitely generated elliptic curves are used over cyclotomics with one ramified rational prime to generate a model of $\mathbb{Z}$ using results of Julia Robinson. Using these elliptic curves as described above we would also get the first-order definition of $\mathbb{Z}$ as a subset.

Another example of a family of infinite extensions of $\mathbb{Q}$ where one can find finitely generated elliptic curves can be found in [37], where the curves are used to prove existential undecidability of rings of integers. One should note that the fields described in that paper are all $q$-bounded with respect to almost all rational primes and thus one could also derive the results on the first-order undecidability of these fields using the norm equation method above. In general the full strength of the elliptic curves method is unknown since we don’t have the complete picture concerning elliptic curves in infinite algebraic extensions of $\mathbb{Q}$.

One can also use Theorem 7.5 to obtain information about existence of finitely generated curves in infinite extensions. If an infinite extension of $\mathbb{Q}$ with a completely $q$-bounded prime has a decidable first-order theory, then our theorem implies that any elliptic curve over the field either has rank 0 or is not finitely generated. An example of such a field, pointed out to us by Moshe Jarden, can be found in [9]. Fix a prime number $p$ and consider the field of all algebraic numbers $\mathbb{Q}_p^{\text{alg}}$ contained in $\mathbb{Q}_p$, the $p$-adic completion of $\mathbb{Q}$. The field $\mathbb{Q}_p^{\text{alg}}$ is not fixed under conjugation and we can set $K_{\text{inf}}$ to be the intersection of all the conjugates of $\mathbb{Q}_p^{\text{alg}}$ over $\mathbb{Q}$. Ershov showed that the first-order theory of such a field is decidable. Further, $p$ splits completely in every finite extension contained in such a $K_{\text{inf}}$ and therefore it is $q$-bounded for any $q$.

References

[1] Sara Checcoli. Fields of algebraic numbers with bounded local degrees and their properties. Trans. Amer. Math. Soc., 365(4):2223–2240, 2013.
[2] Gunther Cornelissen, Thanases Pheidas, and Karim Zahidi. Division-ample sets and diophantine problem for rings of integers. Journal de Théorie des Nombres Bordeaux, 17:727–735, 2005.
[3] Gunther Cornelissen and Alexandra Shlapentokh. Defining the integers in large rings of number fields using one universal quantifier. Zapiski Nauchnykh Seminarov POMI, 358:199 – 223, 2008.
[4] Jan Denef. Diophantine sets of algebraic integers, II. Transactions of American Mathematical Society, 257(1):227–236, 1980.
[5] Jan Denef and Leonard Lipshitz. Diophantine sets over some rings of algebraic integers. Journal of London Mathematical Society, 18(2):385–391, 1978.
[6] Jan Denef, Leonard Lipshitz, Thanases Pheidas, and Jan Van Geel, editors. Hilbert’s tenth problem: relations with arithmetic and algebraic geometry, volume 270 of Contemporary Mathematics. American Mathematical Society, Providence, RI, 2000. Papers from the workshop held at Ghent University, Ghent, November 2–5, 1999.
[7] Kirsten Eisenträger and Graham Everest. Descent on elliptic curves and Hilbert’s tenth problem. Proc. Amer. Math. Soc., 137(6):1951–1959, 2009.
[8] Kirsten Eisenträger, Graham Everest, and Alexandra Shlapentokh. Hilbert’s tenth problem and Mazur’s conjectures in complementary subrings of number fields. Math. Res. Lett., 18(6):1141–1162, 2011.
[9] Yu. L. Ershov. Nice locally global fields. I. Algebra i Logika, 35(4):411–423, 497, 1996.
Michael D. Fried, Dan Haran, and Helmut Vöklein. Real Hilbertianity and the field of totally real numbers. In Arithmetic geometry (Tempe, AZ, 1993), volume 174 of Contemp. Math., pages 1–34. Amer. Math. Soc., Providence, RI, 1994.

Kenji Fukuzaki. Definability of the ring of integers in some infinite algebraic extensions of the rationals. MLQ Math. Log. Q., 58(4–5):317–332, 2012.

Jochen Koenigsmann. Defining Z in Q. Annals of Math. to appear.

Leopold Kronecker. Zwei satze tiber gleichungen mit ganzzahligen coefficienten. J. Reine Angew. Math., 53:173–175, 1857.

Serge Lang. Algebra. Springer-Verlag, New York, third edition, 2002.

Kenji Fukuzaki. Definability of the ring of integers in some infinite algebraic extensions of the rationals. MLQ Math. Log. Q., 58(4–5):317–332, 2012.

Jochen Koenigsmann. Defining Z in Q. Annals of Math. to appear.

Leopold Kronecker. Zwei satze tiber gleichungen mit ganzzahligen coefficienten. J. Reine Angew. Math., 53:173–175, 1857.

Serge Lang. Algebra, volume 211 of Graduate Texts in Mathematics. Springer-Verlag, New York, third edition, 2002.

Barry Mazur and Karl Rubin. Ranks of twists of elliptic curves and Hilbert’s Tenth Problem. Inventiones Mathematicae, 181:541–575, 2010.

Serge Lang. Algebraic Number Theory. Addison Wesley, Reading, MA, 1970.

Jochen Koenigsmann. Defining Z in Q. Annals of Math. to appear.

Leopold Kronecker. Zwei satze tiber gleichungen mit ganzzahligen coefficienten. J. Reine Angew. Math., 53:173–175, 1857.

Serge Lang. Algebra, volume 211 of Graduate Texts in Mathematics. Springer-Verlag, New York, third edition, 2002.

Barry Mazur and Karl Rubin. Ranks of twists of elliptic curves and Hilbert’s Tenth Problem. Inventiones Mathematicae, 181:541–575, 2010.

Serge Lang. Algebraic Number Theory. Addison Wesley, Reading, MA, 1970.

Jochen Koenigsmann. Defining Z in Q. Annals of Math. to appear.

Leopold Kronecker. Zwei satze tiber gleichungen mit ganzzahligen coefficienten. J. Reine Angew. Math., 53:173–175, 1857.

Serge Lang. Algebra, volume 211 of Graduate Texts in Mathematics. Springer-Verlag, New York, third edition, 2002.

Barry Mazur and Karl Rubin. Ranks of twists of elliptic curves and Hilbert’s Tenth Problem. Inventiones Mathematicae, 181:541–575, 2010.

Serge Lang. Algebraic Number Theory. Addison Wesley, Reading, MA, 1970.

Jochen Koenigsmann. Defining Z in Q. Annals of Math. to appear.

Leopold Kronecker. Zwei satze tiber gleichungen mit ganzzahligen coefficienten. J. Reine Angew. Math., 53:173–175, 1857.

Serge Lang. Algebra, volume 211 of Graduate Texts in Mathematics. Springer-Verlag, New York, third edition, 2002.

Barry Mazur and Karl Rubin. Ranks of twists of elliptic curves and Hilbert’s Tenth Problem. Inventiones Mathematicae, 181:541–575, 2010.

Serge Lang. Algebraic Number Theory. Addison Wesley, Reading, MA, 1970.

Jochen Koenigsmann. Defining Z in Q. Annals of Math. to appear.

Leopold Kronecker. Zwei satze tiber gleichungen mit ganzzahligen coefficienten. J. Reine Angew. Math., 53:173–175, 1857.

Serge Lang. Algebra, volume 211 of Graduate Texts in Mathematics. Springer-Verlag, New York, third edition, 2002.

Barry Mazur and Karl Rubin. Ranks of twists of elliptic curves and Hilbert’s Tenth Problem. Inventiones Mathematicae, 181:541–575, 2010.

Serge Lang. Algebraic Number Theory. Addison Wesley, Reading, MA, 1970.

Jochen Koenigsmann. Defining Z in Q. Annals of Math. to appear.

Leopold Kronecker. Zwei satze tiber gleichungen mit ganzzahligen coefficienten. J. Reine Angew. Math., 53:173–175, 1857.

Serge Lang. Algebra, volume 211 of Graduate Texts in Mathematics. Springer-Verlag, New York, third edition, 2002.

Barry Mazur and Karl Rubin. Ranks of twists of elliptic curves and Hilbert’s Tenth Problem. Inventiones Mathematicae, 181:541–575, 2010.

Serge Lang. Algebraic Number Theory. Addison Wesley, Reading, MA, 1970.

Jochen Koenigsmann. Defining Z in Q. Annals of Math. to appear.

Leopold Kronecker. Zwei satze tiber gleichungen mit ganzzahligen coefficienten. J. Reine Angew. Math., 53:173–175, 1857.

Serge Lang. Algebra, volume 211 of Graduate Texts in Mathematics. Springer-Verlag, New York, third edition, 2002.

Barry Mazur and Karl Rubin. Ranks of twists of elliptic curves and Hilbert’s Tenth Problem. Inventiones Mathematicae, 181:541–575, 2010.
[36] Alexandra Shlapentokh. Elliptic curves retaining their rank in finite extensions and Hilbert’s tenth problem for rings of algebraic numbers. *Trans. Amer. Math. Soc.*, 360(7):3541–3555, 2008.

[37] Alexandra Shlapentokh. Rings of algebraic numbers in infinite extensions of $\mathbb{Q}$ and elliptic curves retaining their rank. *Arch. Math. Logic*, 48(1):77–114, 2009.

[38] Alexandra Shlapentokh. Elliptic curve points and Diophantine models of $\mathbb{Z}$ in large subrings of number fields. *Int. J. Number Theory*, 8(6):1335–1365, 2012.

[39] Lou van den Dries. Elimination theory for the ring of algebraic integers. *J. Reine Angew. Math.*, 388:189–205, 1988.

[40] Carlos Videla. Definability of the ring of integers in pro-$p$ extensions of number fields. *Israel Journal of Mathematics*, 118:1–14, 2000.

[41] Carlos R. Videla. The undecidability of cyclotomic towers. *Proc. Amer. Math. Soc.*, 128(12):3671–3674, 2000.

[42] André Weil. *Basic Number Theory*. Springer Verlag, 1974.

Department of Mathematics, East Carolina University, Greenville, NC 27858

E-mail address: shlapentokha@ecu.edu

URL: www.personal.ecu.edu/shlapentokha