RATIONAL SEPARABILITY OF THE INTEGRAL CLOSURE.

ALEXANDRA SHLAPENTOKH

Abstract

We investigate the following question. Let K be a global field, i.e. a number field or an algebraic function field of one variable over a finite field of constants. Let $\mathscr{W}_K$ be a set of primes of K, possibly infinite, such that in some fixed finite separable extension L of K, all the primes of $\mathscr{W}_K$ do not have factors of relative degree 1. Let M be a finite extension of K and let $\mathscr{W}_M$ be the set of all the M-primes above the primes of $\mathscr{W}_K$. Then does $\mathscr{W}_M$ have the same property? The answer is "always" for one variable algebraic function fields over finite fields of constants and "not always" for number fields. In this paper we give a complete descriptions of the conditions under which $\mathscr{W}_M$ inherits and does not inherit the above described property.

1. Introduction.

The question raised in this paper came out of an investigation of some logical properties of subrings of global fields (number fields and function fields over finite fields of constants). More specifically the prime sets which are investigated in this paper play a role in a study of weak presentations of these rings, as well as in the investigation of the first-order definability over global fields. We start with defining the sets of primes in question.

Definition 1.1. Let K be a global field. Let $\mathscr{W}_K$ be a set of primes of K such that there exists a finite extension M of K where each prime of $\mathscr{W}_K$ has no factors of relative degree 1 over K. Then $\mathscr{W}_K$ will be called a *K-separable* set of primes.

It is not hard to show that for a global field K being K-separable is equivalent to existence of a polynomial $P(X) \in K[x]$ such that for all $a \in K$, all $\mathfrak{p} \in \mathscr{W}_K$ we have that $\mathrm{ord}_{\mathfrak{p}} P(a) \leq 0$. The Logic applications are based on this fact. For example, if we have a weak presentation of K (a map from K into $\mathbb{N}$ translating all the field operations by recursive functions), then for any K-separable prime set $\mathscr{W}_K$, the ring where the *complement* of $\mathscr{W}_K$ (denoted by $\overline{\mathscr{W}}_K$) is inverted,

$$O_{K,\overline{\mathscr{W}}_K} = \{x \in K : \mathrm{ord}_{\mathfrak{p}} x \geq 0 \, \forall \mathfrak{p} \in \mathscr{W}_K\},$$

will have a Turing degree which is equal to the Turing degree of the field. This is so, because for any $a \in K$ we have that $\frac{1}{P(a)} \in O_{K,\overline{\mathscr{W}}_K}$. (See [5], [9], [10], [11] for more details concerning weak presentations). We say that the ring $O_{K,\overline{\mathscr{W}}_K}$ is "inseparable" from K by analogy with a similar relation between a pair of fields, and thus we call the set of primes $\mathscr{W}_K$ and the ring $O_{K,\mathscr{W}_K}$ "separable" (from the field K).

Date: July 6, 2008.

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

The research for this paper has been partially supported by NSF grants DMS-9988620 and DMS-0650927.

The applications to the existential definability have to do with the fact that using a polynomial like $P(x)$ we can say something about integrality at infinitely many primes. Further, rings $O_{K,\mathscr{W}_K}$ are precisely the subrings of global fields where we have successfully defined existentially all the elements of a subfield contained in the ring. (See [12], [14], [13], [15], [16].)

In view of the above it is natural to ask whether these logical/algebraic properties carry over under extensions if we consider prime sets containing all the factors of the primes in the original set. To make this question more precise we need another definition.

Definition 1.2. Let K and $\mathscr{W}_K$ be as in Definition 1.1. Suppose further that the following conditions are also satisfied.

(1) For *any* finite extension M of K, the set $\mathscr{W}_M$ of M-primes above the primes of $\mathscr{W}_K$ is M-separable.
(2) For *any* finite subextension E of K, the set of all E-primes such that all of their factors in K are in $\mathscr{W}_K$, is E-separable.

Then $\mathscr{W}_K$ will be called *separable*.

In this paper we would like to answer the following question.

Question 1.3. ***Given a global field K and a K-prime set W_K, is being K-separable the same as being separable*?**

In [11] we made the following easy observations which provide a partial answer to the question.

Proposition 1.4. *Let M/K be a finite extension of global fields. Let $\mathscr{W}_K$ be a set of primes of K and let $\mathscr{W}_M$ be the set of primes of M above the primes of $\mathscr{W}_K$. Then the following statements are true.*

- *If $\mathscr{W}_M$ is M-separable, then $\mathscr{W}_K$ is K-separable.*
- *If all primes of $\mathscr{W}_M$ are of relative degree one over the corresponding primes of $\mathscr{W}_K$ and $\mathscr{W}_K$ is K-separable, then $\mathscr{W}_M$ is M-separable.*

In this paper we complete the answer. Before we state the main results of the paper we need to introduce more definitions.

Definition 1.5. Let M/K be a Galois extension of number fields. Let $\mathscr{W}_K$ be the set of all primes of K without relative degree one factors in M. Then $\mathscr{W}_K$ will be called *maximal* K-separable. (Theorem 7.4 will establish the relationship between the separable sets and maximal K-separable sets.)

The following remark accounts for the usefulness of our definition.

Remark 1.6. Let K be a number field. Then there is a one-to-one correspondence between the maximal K-separable sets of K and finite Galois extensions of K in the following sense. If $\mathscr{W}_K$ is a maximal K-separable set, M is the corresponding Galois extension, and L is another Galois extension of K such that $\mathscr{W}_K$ primes do not have relative degree one factors in L, then $M \subseteq L$. (The reverse inclusion is obvious.)

Proof. Let $\mathscr{P}(K)$ be the set of all the non-archimedean primes of K. Let $\bar{\mathscr{W}}_K = \mathscr{P}(K) \setminus \mathscr{W}_K$ be the set of K-primes splitting completely in the extension M/K. Let $\bar{\mathscr{V}}_K$ be the set of K primes splitting completely in the extension L/K. Then $\bar{\mathscr{V}}_K \subseteq \bar{\mathscr{W}}_K$, and by Corollary 5.5, page 136 of [4], we have that $M \subseteq L$. □

Definition 1.7. Let F/E be an extension of number fields with the following property. *If* $\bar{E} \subset F$, $[F : \bar{E}] = 2$, *and* $E \subset \bar{E}$, *then for any embedding* $\sigma : F \longrightarrow \tilde{\mathbb{Q}}$, *the algebraic closure of* $\mathbb{Q}$, *we have that* $\sigma(\bar{E}) \subset \mathbb{R} \Rightarrow \sigma(F) \subset \mathbb{R}$. Then we will say that the extension F/E satisfies the *weak real embeddings* condition. *If for any embedding* $\sigma : F \longrightarrow \tilde{\mathbb{Q}}$, *we have that* $\sigma(E) \subset \mathbb{R} \Rightarrow \sigma(F) \subset \mathbb{R}$, we will say that the extension F/E satisfies the *strong real embeddings condition*. (For extensions of degree 2, both conditions are clearly equivalent.)

We now state the main results of the paper.

Main Theorem 1. **[Theorem 7.4]** Let K be a number field. Let $\mathscr{W}_K$ be a maximal K-separable set. Then $\mathscr{W}_K$ is separable if and only if the corresponding Galois extension M/K satisfies the weak real embeddings condition.

Main Theorem 2. **[Theorem 7.5]** Let M/K be a finite extension (not necessarily Galois) of number fields such that in the extension M^G/K, where M^G is the Galois closure of M over K, subextensions of degree 2, M^G/M_i, $i = 1, \ldots, k$ are all the subextensions of degree 2 which do not satisfy the real embeddings condition. Let $\mathscr{W}_K$ be the set of all K-primes without relative degree 1 one factors in M. Then $\mathscr{W}_K$ is separable if and only if

$$\forall i = 1, \ldots, k, \text{ we have that } \sigma_i \in \bigcup_{\tau \in G} \tau \mathrm{Gal}(M^G/M)\tau^{-1},$$

where σ_i is the generator of $\mathrm{Gal}(M^G/M_i)$, $i = 1, \ldots, k$ and $G = \mathrm{Gal}(M^G/K)$.

Main Theorem 3. **[Theorem 7.6]** Let K be a one-variable algebraic function field over a finite field of constants. Let $\mathscr{W}_K$ be a set of K-separable primes. Then $\mathscr{W}_K$ is a separable set of primes.

Finally, these results can be restated in terms of Galois groups of the corresponding extensions.

Main Theorem 4. **[Theorem 7.7]** Let M/K be a Galois extension of number fields satisfying the weak real embeddings condition or a Galois extension of function fields over a finite fields of constants. Then there exists an extension L of M with the following property. If $\sigma \in \mathrm{Gal}(M/K)$ is of order $n = \prod p_i^{a_i}$, where all p_i's are distinct, then any $\bar{\sigma} \in \mathrm{Gal}(L/K)$ extending σ will have order $\bar{n} = \prod p_i^{b_i} q_j^{c_j}$, where $b_i > a_i$, $p_i \neq q_j$.

Before proceeding with the proofs we remark on the following. One way to look at the question we have raised is to note that it belongs to a very well known variety of number theoretic questions which ask whether a certain property of a subring of a global field survives under the integral closure in an extension. The answer is often "yes" and easily obtainable, but there are certainly exceptions to this rule. The question of Diophantine decidability of the rings of algebraic integers of number fields is one example where the problem seems quite

hard. The difficulties are often caused by archimedean valuations, which is the case for our question. Over function fields where all the valuations are non-archimedean things progress much more smoothly, though, as usual, one has to take special care of inseparable extensions and extensions where the degree is not prime to the characteristic.

We also would like to make a remark concerning finite prime sets. Let M be a global field and let $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ be a finite set of its non-archimedean primes. Then it is not difficult to construct an extension L of M where none of $\mathfrak{P}_i$, $i = 1, \ldots, r$ would have a factor of relative degree 1. Indeed, let l be a rational prime number greater than then the size of the residue field of any of the primes in the set, different from the characteristic of the field and not equal to the characteristic of the residue field of any of the primes. Then ξ_l – an l-th primitive root of unity is not an element of any of the residue fields. Consider the extension $M(\xi_l)/M$. The power basis of ξ_l is an integral basis for the extension with respect to any non-archimedean prime of M. Since the minimal polynomial of ξ_l over M does not have linear factors modulo $\mathfrak{P}_i$ and the power basis of ξ_l is an integral basis with respect to $\mathfrak{P}_i$, by Proposition 25, page 27 of [6], we know that $\mathfrak{P}_i$ does not have any relative degree 1 factors in the extension $M(\xi_l)/M$. Therefore, if $\mathscr{W}_M$ is an infinite set of primes of M and F is a finite extension of M such that all but finitely many primes $\mathfrak{P}_1, \ldots, \mathfrak{P}_r$ of $\mathscr{W}_M$ have no relative degree one factors in F, then in the extension $F(\xi_l)/M$, no prime of $\mathscr{W}_M$ will have a relative degree 1 factor.

We finish this section with a description of some notational conventions.

Notation 1.8. We will use the following notation and terminology throughout the paper.

- Let K be a global field. Then $\mathscr{P}(K)$ will denote the set of all non-archimedean primes of K.
- If $\mathscr{A}_K \subset \mathscr{P}(K)$ and M is a finite extension of K, then $\mathscr{A}_M$ will denote the set of all primes of M above primes of $\mathscr{A}_K$.
- For a natural number $n \neq 0$, we let ξ_n denote a primitive n-th root of unity.
- Let M/K be a finite extension of global fields. Let $\mathfrak{P}_M$ be a prime of M and let $\mathfrak{P}_K$ be a prime of K below $\mathfrak{P}_M$. Then $e(\mathfrak{P}_M/\mathfrak{P}_K)$, $f(\mathfrak{P}_M/\mathfrak{P}_K)$ will denote the ramification and relative degree respectively of $\mathfrak{P}_M$ over $\mathfrak{P}_K$.
- O_K will denote the ring of integers of K if K is a number field.
- If M/K is Galois, then $\mathrm{Gal}(M/K)$ will denote the Galois group of M over K.
- If M/K is Galois and $\mathfrak{P}_M$ is a prime of M, then we will denote by $G_{M/K}(\mathfrak{P}_M)$ the decomposition group of $\mathfrak{P}_M$.
- If $\mathfrak{P}_K$ is a non-archimedean prime of K, then let $R_{\mathfrak{P}_K}$ be the valuation ring of $\mathfrak{P}_K$.
- We will fix and algebraic closure $\widetilde{\mathbb{Q}}$ of $\mathbb{Q}$, and for each $p > 0$ we will fix an algebraic closure $\widetilde{\mathbb{F}_p(t)}$ of a rational function field with coefficients in a finite field of p elements.
- Given two number fields (function fields) M and E, we will often form a field compositum ME denoting the smallest field inside the fixed above algebraic closure which contains both M and E.

2. Overview of the Proof.

In order to prove the main theorems (Theorem 7.4 and Theorem 7.6) we first go through a series of reductions.

- If $\mathscr{W}_K$ is a K-separable set, then it is not hard to see that separability of $\mathscr{W}_K$ is equivalent to the following condition. For all $n \in \mathbb{Z}_{>0}$ there exists a finite extension K_n of K such that every prime $\mathfrak{p} \in \mathscr{W}_K$ has all of its K_n-factors of relative degree greater or equal to n. (See the proof of Theorem 7.4 for the argument for the non-trivial direction of the statement.)
- It is enough to consider the maximal K-separable sets corresponding to the cyclic extensions of prime degree. (See the Proposition 7.1.)
- If a K-maximal separable set $\mathscr{W}_K$ corresponds to an extension of degree 2 not satisfying the weak real embedding condition, then $\mathscr{W}_K$ is *not* separable. (See Lemma 7.2.)

Next we solve the problem for the cyclic extensions. The process goes through the steps listed below.

(1) Given a K-maximal K-separable set $\mathscr{W}_K$ corresponding to a cyclic extension M/K of degree p, it is enough to be able to produce for any $n \in \mathbb{Z}_{>0}$, a tower of fields $K_0 = K \subset K_1 = M \subset \ldots \subset K_n$ such that for $n-2 \geq i \geq 0, K_{i+2}/K_i$ is a Galois extension of degree p^2. In particular, it is enough to be able to produce for any n the cyclic extension K_n/K of degree p^n with $K \subset M \subset K_n$. (See Section 3 in general and more specifically Lemma 3.4.) Unfortunately, given an arbitrary cyclic extension M/K of prime degree p and satisfying the weak real embedding condition, a tower of extensions as described above does not always exist even for $n = 2$. The necessary and sufficient condition for the existence of the tower $K - M - K_2$ is solvability of a certain norm equation over M. (See Lemma 5.1.)

(2) In the case of $p > 2$ for number fields and in the case of algebraic function fields when the characteristic is different from p, there is a relatively easy construction, adding the p^2-th roots of unity to K if necessary, which makes the norm equation solvable and produces the required tower of extensions of degree p. (See Section 4 in general and specifically Proposition 4.5 and Proposition 4.6 for the number field case, and see Section 6 in general and Proposition 6.1 in particular for the function field case.) In the case of a function field case when the characteristic is equal to p, the required tower always exists (see Lemma 6.2).

(3) The only difficult case is the case of number fields when $p = 2$. This case requires several constructions carried out in Section 5. Here we are forced to analyze the obstruction to the solvability of the norm equation for producing a tower of cyclic extensions of height 2. We do this using Hasse Norm Principle to reduce the problem to the behavior of a finite set of primes, both finite and infinite. The problem with finite primes is solved by constructing an extension where the residue fields are extended to solve the norm equation locally. The problem with archimedean primes is resolved using the weak real embedding assumption. More details are provided at the beginning of Section 5.

3. Towers of Cyclic Extensions and Primes that Do not Split.

In this section we work out the details of Step 1. Essentially, in this section we want to answer the following question. Given two Galois extensions of global fields: $K \subset M \subset L$, what are the necessary and sufficient conditions insuring that every prime not splitting completely in the first extension, also does not split in the second extension? The conditions we seek turn out to be related to the orders of the Frobenius automorphisms. The first lemma states a necessary and sufficient condition for the prime of the field in the middle to split completely in the second extension, in terms of the Frobenius of its factors.

Lemma 3.1. *Let $K \subset M \subset L$ be a tower of extensions of global fields with all of the three extensions being Galois. Let $\sigma \in Gal(L/K)$ and let $\mathfrak{P}_L$ be a prime of L, unramified over K, such that σ is the Frobenius automorphism of $\mathfrak{P}_L$. Then $\mathfrak{P}_L$ lies above an M-prime which splits completely in the extension L/M if and only if the L/K-decomposition group $G_{L/K}(\mathfrak{P}_L)$ of $\mathfrak{P}_L$, i.e. the cyclic group generated by σ in $Gal(L/K)$, has no elements in $Gal(L/M)$ except for identity. In other words, $<\sigma> \cap Gal(L/M) = \{id\}$.*

Proof. Note that the decomposition group of $\mathfrak{P}_L$ over M (denoted by $G_{L/M}(\mathfrak{P}_L)$) is equal to $\mathrm{Gal}(L/M) \cap G_{L/K}(\mathfrak{P}_L)$. Therefore, if this intersection is trivial, $\mathfrak{P}_M$, the M-prime below $\mathfrak{P}_L$, splits completely in the extension L/M. Conversely, if the intersection is not trivial, then the Frobenius automorphism of $\mathfrak{P}_L$ over M is not the identity and therefore $\mathfrak{P}_M$ will not split completely in the extension L/M. □

The lemma below reinterprets the lemma above in terms of orders of Frobenius automorphisms involved.

Lemma 3.2. *Let $K \subset M \subset L$ be a tower of extensions of global fields with all of the three extensions being Galois. Let $\sigma \in Gal(M/K)$ and assume that $\sigma \neq id$ has an extension $\hat{\sigma}$ in $Gal(L/K)$ such that the order of $\hat{\sigma}$ is the same as the order of σ. Then the infinitely many primes of K whose M-factors have σ as their Frobenius automorphism over K will not split completely in M, but their M-factors will split completely in L.*

Proof. Let $\sigma \in \mathrm{Gal}(M/K)$ be as described in the statement of the lemma. Let $\hat{\sigma}$ be an extension of σ in $\mathrm{Gal}(L/K)$. If $l \in \mathbb{Z}_{>0}$ is such that $\hat{\sigma}^l \in \mathrm{Gal}(L/M)$, then $\sigma^l = \mathrm{id}$. Thus if σ has the order $m > 0$, then $\hat{\sigma}^m$ is the smallest positive power of $\hat{\sigma}$ that belongs to $\mathrm{Gal}(L/M)$. At the same time by assumption $\hat{\sigma}^m = \mathrm{id}$ also and we can conclude that $<\hat{\sigma}> \cap \mathrm{Gal}(L/M) = \{\mathrm{id}\}$. Therefore if $\mathfrak{P}_L$ is a prime of L whose Frobenius in $\mathrm{Gal}(L/K)$ is $\hat{\sigma}$, then Frobenius of $\mathfrak{P}_L$ in $\mathrm{Gal}(L/M)$ is id, and thus $\mathfrak{P}_M = \mathfrak{P}_L \cap M$ splits completely in the extension L/M by Lemma 3.1. At the same time the Frobenius of $\mathfrak{P}_M$ is σ. Indeed, $\forall x \in R_{\mathfrak{P}_L}$, we have that

$$\hat{\sigma}(x) \equiv x^{N\mathfrak{P}_L} \mod \mathfrak{P}_L,$$

where $N\mathfrak{P}_L$ is the norm of $\mathfrak{P}_L$. Therefore, $\forall x \in R_{\mathfrak{P}_M}$ we have that

$$\hat{\sigma}(x) \equiv x^{N\mathfrak{P}_L} \mod \mathfrak{P}_M,$$

because $x \in M$ implies $\hat{\sigma}(x) \in M$, and thus $(\hat{\sigma}(x) - x^{N\mathfrak{P}_L}) \in M$. But since $\mathfrak{P}_M$ splits completely in the extension L/M, we have that $N\mathfrak{P}_L = N\mathfrak{P}_M$. Hence, $\sigma = \hat{\sigma}_{|M}$ is the Frobenius

automorphism of $\mathfrak{P}_M$. Finally, since by assumption $\sigma \neq \mathrm{id}$, we have that $\mathfrak{P}_K = \mathfrak{P}_M \cap K$ does not split completely in M. $\square$

We now specialize our discussion of a Galois tower of two extensions to cyclic extensions, where the necessary and sufficient condition for the primes not to split completely in both extensions has a particularly simple form.

Lemma 3.3. *Let $K \subset M \subset L$ be a cyclic extension of global fields. Let $\mathscr{W}_K$ be the set of all primes of K not ramified in the extension L/K and not splitting completely in the extension M/K. Let $\mathscr{W}_M$ be the set of all the primes of M lying above the primes of $\mathscr{W}_K$. Then none of the primes of $\mathscr{W}_M$ split completely in the extension L/M if and only if for every rational prime q, we have that*

$$ord_q|Gal(M/K)| > 0 \Rightarrow ord_q|Gal(L/M)| > 0.$$

Proof. Suppose

$$|\mathrm{Gal}(M/K)| = \prod q_i^{a_i},$$

$$|\mathrm{Gal}(L/M)| = \prod q_i^{b_i} \prod t_j^{c_j},$$

where for all i, j, we have that q_i, t_j are distinct rational prime numbers and a_i, b_i, c_j are positive integers. This of course implies that

$$|\mathrm{Gal}(L/K)| = \prod q_i^{a_i+b_i} \prod t_j^{c_j}.$$

Let $\sigma \in \mathrm{Gal}(L/K)$ be a generator. Then $\sigma^{\prod q_i^{a_i}}$ generates $\mathrm{Gal}(L/M)$. Let $\tau = \sigma^{\prod q_i^{m_i} \prod t_j^{n_j}}$, where $m_i, n_j \in \mathbb{Z}_{\geq 0}$, and

$$0 \leq m_i < a_i + b_i,$$

$$0 \leq n_j < c_j.$$

Let $l_i = \max(0, a_i - m_i)$. Then $\tau^{\prod q_i^{l_i}} \in \mathrm{Gal}(L/M)$. Suppose now that $\tau^{\prod q_i^{l_i}} = \mathrm{id}$. This implies $n_j = 0$ for all j and $l_i + m_i = b_i + a_i$ for all i, since l_i and m_i cannot be zero at the same time. Thus, $\max(0, a_i - m_i) + m_i = b_i + a_i$ for all i. We have to consider two cases: $m_i \geq a_i$ and $m_i < a_i$. In the first case, $l_i = 0$ and $m_i = a_i + b_i$. In the second case, $l_i = a_i - m_i$ and $l_i + m_i = a_i < a_i + b_i$. Since by assumption $0 \leq m_i < a_i + b_i$, neither case can occur and therefore for any element $\tau \neq \mathrm{id}$ of $\mathrm{Gal}(L/K)$, the intersection of $< \tau >$ and $\mathrm{Gal}(L/M)$ is non-trivial. Hence, every prime of K not splitting completely in M will have all of its M-factors not splitting completely in L.

Suppose now that for some rational prime q, we have that

$$q \Big| |\mathrm{Gal}(M/K)| \text{ and } q \not| |\mathrm{Gal}(L/M)|.$$

Then by Sylow Theorems, $\mathrm{Gal}(L/K)$ has an element τ of order q such that

$$< \tau > \cap \mathrm{Gal}(L/M) = \{\mathrm{id}\},$$

while $\tau_{|M} \neq \mathrm{id}$. Thus, there are infinitely many primes of K not splitting completely in the extension M/K with some factors splitting completely in the extension L/M. $\square$

We now extend the results of Lemma 3.3 to cyclic towers of arbitrary height and determine that to obtain prime factors of arbitrary high relative degree it is enough to construct cyclic towers, where each pair of adjacent fields produces an extension of the same (prime) degree and *every subtower of length two is itself cyclic*.

Lemma 3.4. *Let p be a rational prime. Consider the following tower of number fields:*

$$K_1 \subset K_2 \subset \ldots \subset K_n,$$

where for $2 \leq i+1 \leq n$, we have that

$$[K_{i+1} : K_i] = p,$$

and for $1 \leq i < n-1$, it is the case that K_{i+2}/K_i is a cyclic extension. Let $\mathscr{W}_{K_1}$ be a set of K_1 primes not splitting in the extension K_2/K_1 and not ramified in the extension K_n/K_1. Then no prime of $\mathscr{W}_{K_1}$ splits in the extension K_n/K_1 and consequently all the K_n-factors of $\mathscr{W}_{K_1}$-primes have relative degree p^{n-1} over K_1.

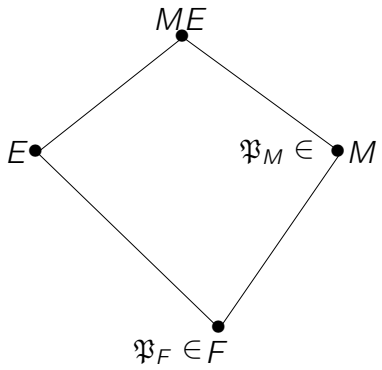
Proof. We use induction on n to prove the lemma. The base case, i.e. the case for $n = 3$ holds by Lemma 3.3. So assume the statement of the lemma holds for $n = m-1$. For $n \geq 0$ let $\mathscr{W}_{K_n}$ be the set of all the factors of primes of $\mathscr{W}_{K_1}$ in K_n. Then by induction hypothesis, all the primes of $\mathscr{W}_{K_1}$ do not split in the extension K_{m-1}/K_1 and consequently all the primes of $\mathscr{W}_{K_{m-2}}$ do not split in the extension K_{m-1}/K_{m-2}. However, by Lemma 3.3, all the primes of K_{m-2} which do not split in the extension K_{m-1}/K_{m-2} have K_{m-1} factors not splitting in the extension K_m/K_{m-1}. Therefore, primes of $\mathscr{W}_{K_1}$ will not split in the extension K_m/K_1. □

4. Cyclic extensions of odd prime degree over number fields.

In the last section we established that we would like to construct cyclic towers, where each pair of adjacent fields produces an extension of the same (prime) degree and *every subtower of length two is itself cyclic*. In this section we execute such a construction starting with a cyclic extension of degree $p > 2$ of number fields. The prime 2 will be dealt with separately and will cause many more difficulties. This section is Step 2 of the overview for number fields.

We start with a series of technical propositions describing prime splitting under linearly disjoint Galois extensions. (For a definition and a discussion of properties of linearly disjoint fields see [3].) We consider the situation first assuming the degrees of the extensions in question are relatively prime.

Lemma 4.1. *Consider the following diagram, where E/F is a cyclic extension of global fields, M/F is a Galois extension of global fields, $[M : F]$ is prime to $[E : F]$.*



Let $\mathfrak{P}_M$ be any prime of M. Then $\mathfrak{P}_M$ does not split in the extension ME/M if and only if the prime $\mathfrak{P}_F$ below it in F does not split in the extension E/F.

Proof. Let $G_M, G_E, G_{ME/M}, G_{ME/E}, G_{ME/F}$ be the Galois groups of extensions M/F, E/F, ME/M, ME/E, and ME/F respectively. Then the assumptions of the lemma imply the following.

$$G_{ME/M} \cong G_E, G_{ME/E} \cong G_M,$$

$$G_{ME/F} = G_{ME/E} \times G_{ME/M} \cong G_M \times G_E,$$

and every element of $G_{ME/F}$ is of the form $\tau\sigma = \sigma\tau$, where $\tau \in G_{ME/M}, \sigma \in G_{ME/E}$. Let $\mathfrak{P}_M$ be a prime of M. Then $\mathfrak{P}_M$ does not split in the extension EM/M if and only if some factor $\mathfrak{P}_{ME}$ of $\mathfrak{P}_M$ in ME, has a Frobenius automorphism σ that is a generator of $G_{ME/M}$. This implies that $\sigma|_E$, a generator of G_E, will not move $\mathfrak{P}_{ME} \cap E = \mathfrak{P}_E$ and therefore the decomposition group of $\mathfrak{P}_E$ is G_E. The last assertion however is equivalent to the statement that $\mathfrak{P}_F = \mathfrak{P}_E \cap F$ does not split in the extension E/F.

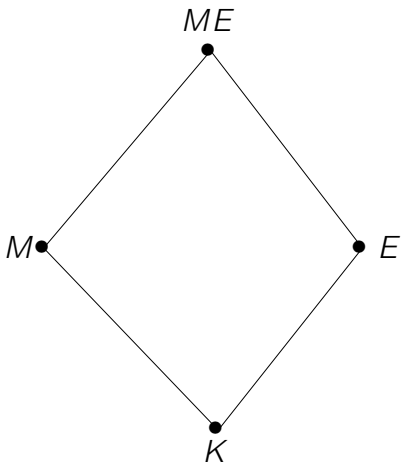
Suppose now that an F-prime $\mathfrak{P}_F$ does not split in the extension E/F. Since

$$([E : F], [M : F]) = 1 = ([E : F], [ME : E]),$$

the number of factors of $\mathfrak{P}_F$ in ME is prime to $[E : F]$. Since $[E : F] = [ME : M]$, this implies that the primes above $\mathfrak{P}_F$ in M do not split in the extension ME/M. □

The next lemma considers the linearly disjoint extensions of the same prime degree.

Lemma 4.2. *Let $M/K, E/K$ be two cyclic extensions of prime degree p of global fields such that $M \cap E = K$. Then all the primes of K not ramifying in the extension ME/K can be divided into four disjoint classes described in the following table and field diagram.*



Prime class	*M/K*	*E/K*	*ME/E*	*ME/M*
1	*split completely*	*split completely*	*E-factors split completely*	*M-factors split completely*
2	*split completely*	*do not split*	*E-factors split completely*	*M-factors do not split*
3	*do not split*	*split completely*	*E-factors do not split*	*M-factors split completely*
4	*do not split*	*do not split*	*E-factors split completely*	*M-factors split completely*

Proof. Since E/K and M/K are linearly disjoint over K, we have that

$$\mathrm{Gal}(ME/K) \cong \mathrm{Gal}(E/K) \times \mathrm{Gal}(M/K) \cong \mathbb{Z}/p \times \mathbb{Z}/p.$$

Further, since the Galois group of ME/K is abelian, all factors of a prime of K without ramified factors in ME have the same Frobenius automorphism over K. Let σ_E, σ_M be generators of $\mathrm{Gal}(ME/M)$ and $\mathrm{Gal}(ME/E)$ respectively. Then the primes in the first class are all the primes which split completely in the extension ME/K or the ones whose factors have identity as their ME-Frobenius automorphism. The primes in the second class have factors with $\sigma_E^l, (l, p) = 1$ as their ME-Frobenius automorphism. The primes in the third class have factors with $\sigma_M^l, (l, p) = 1$ as their ME-Frobenius. Finally, the primes in the fourth class have factors with $\sigma_M^{l_1}\sigma_E^{l_2}, (l_i, p) = 1, i = 1, 2$ as their ME-Frobenius automorphism. $\square$

The next two lemmas are obvious and we state them without proof.

Lemma 4.3. *Let E/F be any cyclic extension of number fields of prime degree p. Then one of the following options holds.*

- *F contains ξ_p.*
- *F does not contain ξ_p and E and $F(\xi_p)$ are linearly disjoint over F.*

Lemma 4.4. *Let $A, B \in \mathbb{Z}, k \in \mathbb{Z}_{>0}, p \neq 2$ – a rational prime. Assume $A \doteq B \mod p^k$ or in other words $A \equiv B \mod p^k$ but $A \not\equiv B \mod p^{k+1}$. Then $A^p \doteq B^p \mod p^{k+1}$. (See Lemma 6.3.1, page 206 of [8].)*

We now get to the business of constructing our tower, first under the assumption that the ground field has a primitive p-th root of unity.

Proposition 4.5. *Let M/K be a cyclic extension of number fields of prime degree $p > 2$. Assume further that $\xi_p \in K$. Let $n \in \mathbb{Z}_{>0}$ be given. Then there exists a number field $L \supset M \supset K$ satisfying the following condition. Let $\mathfrak{p}_K$ be a K-prime not splitting in the*

extension M/K and not ramifying in the extension L/K. Let $\mathfrak{p}_M$ be its M-factor. Let $\mathfrak{p}_{L,1}, \ldots, \mathfrak{p}_{L,k}$ be all the L primes above $\mathfrak{p}_M$. Then for all j, we have that $f(\mathfrak{p}_{L,j}/\mathfrak{p}_M) > n$.

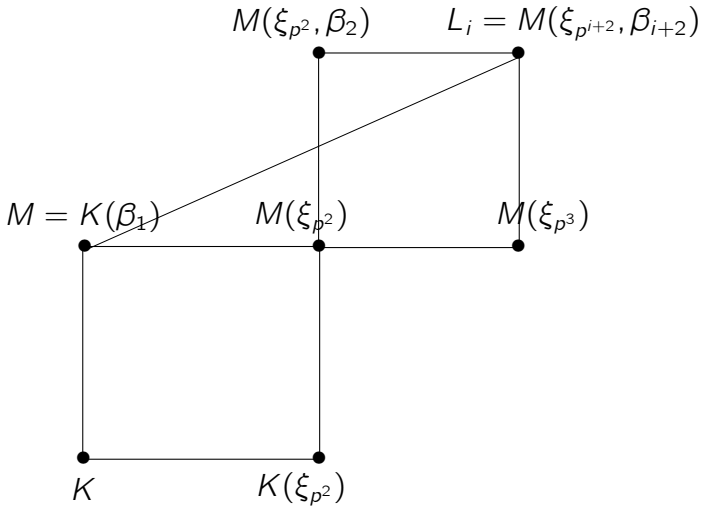
Proof. First of all, if M contains ξ_{p^2}, then there exists the following tower of number fields:

$$K_1 = K \subset K_2 = M \subset \ldots \subset K_n,$$

where for $1 \leq i < n$ we have that $[K_{i+1} : K_i] = p$ and for $1 \leq i < n-2$, it is the case that K_{i+2}/K_i is a cyclic extension. Indeed, first assume that $\xi_{p^2} \in K$. Then $M = K(\alpha)$, where $\alpha^p = a \in K$ by Theorem 10, page 214 of [7]. Consider now the following set of numbers in our fixed algebraic closure of $\mathbb{Q}$: $\{\alpha_1 = a, \alpha_i^p = \alpha_{i-1}, i > 1\}$. Let $K_i = K_{i-1}(\alpha_i), i > 1$. Then the presence of ξ_{p^2} in K_i insures that K_{i+2}/K_i is a cyclic extension of degree p^2.

Suppose now that $\xi_{p^2} \in M \setminus K$. Then $M = K(\xi_{p^2})$. Thus we can set $K_i = K(\xi_{p^i}), i \geq 2$ and the assertion concerning the tower follows.

Next assume that $\xi_{p^2} \notin M$. Then M and $K(\xi_{p^2})$ are linearly disjoint over K. Consider now the following picture, where $M = K(\beta_1)$, with $\beta_1^p \in K$ by Theorem 10, page 214 of [7] again, and $\beta_2^p = \beta_1, \beta_i^p = \beta_{i-1}$ for $i > 1$.



Let $\mathfrak{P}_K$ be a K prime not splitting in the extension M/K and not ramifying in the extension L_i/K. Next we consider two cases. In the first case we assume that $\mathfrak{P}_K$ splits completely in the extension $K(\xi_{p^2})/K$. Since $K(\xi_{p^2})$ and M are disjoint over K, and

$$\mathrm{Gal}(M(\xi_{p^2})/K) = \mathrm{Gal}(M/K) \times \mathrm{Gal}(K(\xi_{p^2})/K) \cong \mathbb{Z}/p \times \mathbb{Z}/p,$$

we must conclude that in this case $\mathfrak{P}_{K(\xi_{p^2})}$ – any $K(\xi_{p^2})$-prime lying above $\mathfrak{P}_K$, does not split in the extension $M(\xi_{p^2})/K(\xi_{p^2})$, by Lemma 4.2. Note further that the extension $M(\xi_{p^2}, \beta_2)/K(\xi_{p^2})$ is cyclic of degree p^2 and provides the foundation of the tower as in Lemma 3.4, where

$$K_1 = K(\xi_{p^2}), K_2 = M(\xi_{p^2}), K_3 = M(\xi_{p^2}, \beta_2), K_{i+1} = M(\xi_{p^2}, \beta_i),$$

and $\beta_i^p = \beta_{i-1}$. By Lemma 3.4, we know that $\mathfrak{P}_{K(\xi_{p^2})}$ will not split in the extension K_i/K_1. If $\mathfrak{P}_{K_i}$ is a factor of $\mathfrak{P}_K$ in K_i, then for $i \geq 3$, we have that $f(\mathfrak{P}_{K_i}/\mathfrak{P}_{K_1}) = p^{i-1}$ and $f(\mathfrak{P}_{K_i}/\mathfrak{P}_M) = p^{i-2}$.

Suppose now that $\mathfrak{P}_K$ does not split in the extension $K(\xi_{p^2})/K$. Note that the power basis of ξ_{p^2} is an integral basis for the extension. Thus if $\mathfrak{P}_K$ does not split in the extension, this implies that the monic irreducible polynomial of ξ_{p^2} over K has no roots modulo $\mathfrak{P}_K$. Therefore, the residue field of $\mathfrak{P}_K$ is of size q, where $q-1$ is divisible by p but not by p^2. Further, again since $K(\xi_{p^2})$ and M are linearly disjoint over K, it is the case that $\mathfrak{P}_{K(\xi_{p^2})}$, the $K(\xi_{p^2})$-factor of $\mathfrak{P}_K$, splits completely in the extension $M(\xi_{p^2})/K(\xi_{p^2})$. (See Lemma 4.2 again.) Let $\mathfrak{P}_{M(\xi_{p^2})}$ be an $M(\xi_{p^2})$-factor of $\mathfrak{P}_K$. Then

$$f(\mathfrak{P}_{M(\xi_{p^2})}/\mathfrak{P}_K) = f(\mathfrak{P}_{M(\xi_{p^2})}/\mathfrak{P}_{K(\xi_{p^2})})f(\mathfrak{P}_{K(\xi_{p^2})}/\mathfrak{P}_K) = p.$$

Thus, the residue field of $\mathfrak{P}_{M(\xi_{p^2})}$ is of size q^p. By Lemma 4.4 we now have

$$p^2 | q^p - 1 \text{ but } p^3 \nmid q^p - 1.$$

Hence, the monic irreducible polynomial of ξ_{p^3} over $M(\xi_{p^2})$ will have no solutions modulo $\mathfrak{P}_{M(\xi_{p^2})}$. Therefore, $\mathfrak{P}_{M(\xi_{p^2})}$ will not split in the extension $M(\xi_{p^3})/M(\xi_{p^2})$. We can now set

$$K_1 = M(\xi_{p^2}),$$

$$K_i = M(\xi_{p^{i+1}})$$

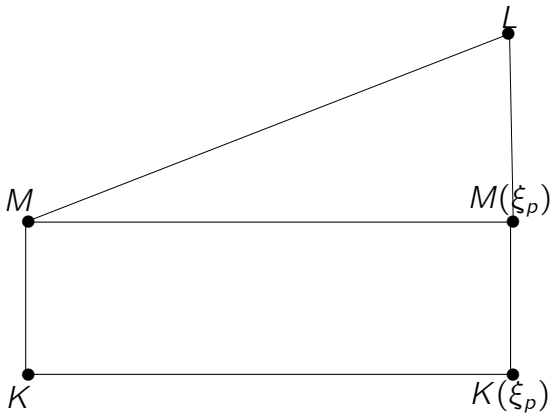
and use Lemma 3.4 to claim that $\mathfrak{P}_{M(\xi_{p^2})}$ will not split in the extension K_i/K_1. Let $\mathfrak{P}_{K_i}$ be a factor of $\mathfrak{P}_M$ in K_i. Then, $f(\mathfrak{P}_{K_{i+2}}/\mathfrak{P}_M) = p^i$.

Now let $\mathfrak{P}_{L_i}$ be any L_i-factor of $\mathfrak{P}_M$. Then, from the discussion above it follows that $f(\mathfrak{P}_{L_i}/\mathfrak{P}_M) \geq p^i$. □

We now remove the assumption that the ground field K has a p-th root of unity and prove the main result of this section.

Proposition 4.6. *Let M/K be a cyclic extension of number fields of degree $p > 2$. Let $n \in \mathbb{Z}_{>0}$ be given. Then there exists a number field $L \supset M \supset K$ satisfying the following condition. Let $\mathfrak{p}_K$ be a K-prime not splitting in the extension M/K and not ramifying in the extension L/K. Let $\mathfrak{p}_M$ be its M-factor. Let $\mathfrak{p}_{L,1}, \ldots, \mathfrak{p}_{L,k}$ be all the L-primes above $\mathfrak{p}_M$. Then for all j, we have that $f(\mathfrak{p}_{L,j}/\mathfrak{p}_M) > n$.*

Proof. If K contains ξ_p, then we are done by Proposition 4.5. Then assume $\xi_p \notin K$ and consider the following diagram, where L is the extension of $M(\xi_p)$ with the property that every prime of $M(\xi_p)$ of relative degree p over $K(\xi_p)$ and lying over a $K(\xi_p)$-prime not ramifying in the extension $L/K(\xi_p)$, will have all of its factors in L of relative degree higher than n. (Such an L exists by Proposition 4.5.)



Note that by Lemma 4.1 and due to the fact that $(p, [K(\xi_p) : K]) = 1$, a K-prime $\mathfrak{P}_K$, not ramified in the extension $M(\xi_p)/K$, does not split in the extension M/K if and only if every prime above it in the extension $K(\xi_p)$ does not split in the extension $M(\xi_p)/K(\xi_p)$. Let $\mathfrak{P}_L$ be a prime of L lying above a prime $\mathfrak{P}_M$ in M of relative degree p over K. Let $\mathfrak{P}_{M(\xi_p)}, \mathfrak{P}_{K(\xi_p)}, \mathfrak{P}_K$ be the primes below $\mathfrak{P}_L$ in $M(\xi_p), K(\xi_p)$ and K respectively with $\mathfrak{P}_K$ not ramified in the extension L/K. Then

$$f(\mathfrak{P}_L/\mathfrak{P}_M) = \frac{1}{p} f(\mathfrak{P}_L/\mathfrak{P}_K) = \frac{1}{p} f(\mathfrak{P}_L/\mathfrak{P}_{M(\xi_p)}) p f(\mathfrak{P}_{K(\xi_p)}/\mathfrak{P}_K) \geq f(\mathfrak{P}_L/\mathfrak{P}_{M(\xi_p)}) \geq n.$$

□

5. Extensions of degree two of number fields.

In the preceding section it was fairly easy, starting with a cyclic extension M/K of degree $p > 2$, to construct a cyclic extension L/M of degree p so that L/K is cyclic of degree p^2. This two-tower then served as a foundation for a tower of arbitrary length where the factors of the primes not splitting in the extension M/K would have arbitrarily high relative degrees over K. Unfortunately, it is much harder to execute the same plan for $p = 2$. We are forced to look at a problem in much greater detail and first in much greater generality. The crucial issue turns out to be the presence or absence of $i = \sqrt{-1}$ in the dyadic completions of the field in question. Initially we will assume that the dyadic completions of the fields we consider do have i and later remove this assumption. We start however, with a rather general proposition about making towers of height two of cyclic extensions. In the first lemma we show that the existences of a cyclic extension $K \subset M \subset L$ of degree p^2 for any prime p is equivalent to solvability of a norm equation over M.

Lemma 5.1. *Let $K \subset M$ be a cyclic field extension of prime degree p distinct from the characteristic of the field. Assume that $\xi_p \in K$. Then there exists a field L such that $K \subset M \subset L$ is a cyclic extension of degree p^2 if and only if $M = K(\mu)$, where $\mathbf{N}_{M/K}(\mu) = \xi_p$.*

Further, if $M = K(\mu)$ with $\mathbf{N}_{M/K}(\mu) = \xi_p$, then $L = M(\gamma)$, where $\gamma^p = \beta \in M$ and $\mu^p = \beta/\bar{\beta}$, with $\bar{\beta}$ – a conjugate of β over K.

Proof. First suppose that M contains an element μ as described in the statement of the lemma. Note that $\mu \neq \xi_p^i, i = 0, \ldots, p-1$, since M/K is a non-trivial extension and K has

p-th roots of unity. Further $\mathbf{N}_{M/K}(\mu^p) = 1$ and by Hilbert's Theorem 90 (see [7], page 213),

$$\mu^p = \beta/\sigma(\beta), \tag{5.1}$$

where $\sigma \in \mathrm{Gal}(M/K) \setminus \{\mathrm{id}\}$ and $\beta \in M \setminus K$. Let $\gamma \in \tilde{K}$, the algebraic closure of K, be such that $\gamma^p = \beta$. Then let $L = M(\gamma)$. We claim that L/K is a cyclic extension of degree p^2. First we show that the extension L/K is Galois. Indeed, any K conjugate γ_i of γ satisfies the equation $\gamma_i^p = \beta_i$ where for $i = 1, \ldots, p$, we have that $\beta_i = \sigma^{i-1}(\beta)$. However, from (5.1) it follows that $\beta_i = \nu_i^p \beta$, where $\nu_i \in M$. Indeed,

$$\frac{\beta_i}{\beta} = \frac{\beta_i}{\beta_{i-1}} \ldots \frac{\beta_2}{\beta} = \mu_i^{-p} \ldots \mu_1^{-p} = \nu_i^p,$$

where for $i = 1, \ldots, p$, we have that $\mu_i = \sigma^{i-1}(\mu)$. Thus, in L, it is the case that β_i is a p-th power and since $\xi_p \in K$, we can deduce that β_i has all of its p-th roots in L. Hence, $\gamma_i \in L$.

Next we show that L/K is cyclic. To accomplish this, it is enough to produce an automorphism τ of L over K such that $\tau^p \neq \mathrm{id}$. Let $\tau \in \mathrm{Gal}(L/K)$ be such that

$$\tau_{|M} = \sigma \in \mathrm{Gal}(M/K).$$

Then $\tau(\gamma) = \xi_p^j \mu^{-1} \gamma$, for some $j = 0, \ldots, p-1$. Indeed, we have that $\gamma^p = \beta$, and therefore, $\tau(\gamma^p)/\gamma^p = \sigma(\beta)/\beta = \mu^p$. Thus, $\tau(\gamma)/\gamma = \xi_p^j \mu$, for some $j = 0, \ldots, p-1$. Further,

$$\tau^2(\gamma) = \xi_p^{2j} \mu^{-1} \sigma(\mu^{-1}) \gamma,$$

$$\ldots,$$

$$\tau^p(\gamma) = \xi_p^{jp} \mu^{-1} \sigma(\mu^{-1}) \ldots \sigma^{p-1}(\mu^{-1}) \gamma = \mathbf{N}_{M/K}(\mu^{-1}) \gamma = \xi_p^{p-1} \gamma \neq \gamma.$$

Suppose now that $K \subset M \subset L$ is a cyclic extension. Then by Theorem 10, page 214 of [7], we have that

$$M = K(\alpha) \text{ with } \alpha^p = a \in K,$$

$$L = M(\gamma) \text{ with } \gamma^p = \beta \in M.$$

Let $\tau \in \mathrm{Gal}(L/K) \setminus \mathrm{Gal}(L/M)$ and consider $\gamma/\tau(\gamma)$. We claim that $\gamma/\tau(\gamma) \in M$. Indeed, let $\phi \in \mathrm{Gal}(L/M)$. Then $\phi(\gamma) = \xi_p^i \gamma$. At the same time, since the extension is abelian and ξ_p is not moved by elements of $\mathrm{Gal}(L/K)$, we have that

$$\phi(\tau(\gamma)) = \tau(\phi(\gamma)) = \tau(\xi_p^i \gamma) = \xi_p^i \tau(\gamma).$$

Thus, $\phi(\gamma/\tau(\gamma)) = \gamma/\tau(\gamma)$. Let $\mu = \gamma/\tau(\gamma)$. Then $\mu^p = \beta/\sigma(\beta)$, where $\tau_{|M} = \sigma$. Hence, $\mathbf{N}_{M/K}(\mu^p) = 1$. At the same time, since $\tau \notin \mathrm{Gal}(L/M)$, we have that $\mathrm{ord}\tau = p^2$ and $\tau^p(\gamma) \neq \gamma$. So $\tau^p(\gamma) = \mathbf{N}_{M/K}(\mu^{-1})\gamma \neq \gamma$. Therefore, $\mathbf{N}_{M/K}(\mu) = \xi_p^i$, for some $i = 1, \ldots, p-1$. Let $j \cong i^{-1} \mod p$. Then $\mathbf{N}_{M/K}(\mu^j) = \xi_p$. □

We now specialize the situation above to the case of $p = 2$ with an added twist. We will show that if -1 is a norm the cyclic tower we construct will also satisfy the strong real embeddings condition.

Corollary 5.2. *Let M/K be an extension of degree 2 of number fields such that -1 is a K-norm of some element of M. Then there exists an extension U of degree 2 over M such that U/K is cyclic and satisfies the strong real embeddings condition.*

Proof. Using Lemma 5.1, we can generate U by adjoining any $\alpha \in \widetilde{\mathbb{Q}}$ to M, with

$$\alpha^2 = \beta \in M,$$

where $\beta = x^2\bar{\beta}$, for some $x \in M \setminus \{0\}$ with K-norm equal to -1, and $\bar{\beta}$ is a conjugate of β over K. An arbitrary β however does not insure that the strong embeddings condition is satisfied. To make sure that it is, given a β as above, we construct β'. Let $y \in K$ be such that all the real conjugates of $y(\beta + \bar{\beta})$ are positive. (Such a y exists by the Approximation Theorem). Now let $\beta' = y\beta$. Let $\alpha' \in \widetilde{\mathbb{Q}}$ be such that $\alpha'^2 = \beta'$ and $U = M(\alpha')$.

Now let $\sigma(M) \subset \mathbb{R}$ for some $\sigma : U \longrightarrow \widetilde{\mathbb{Q}}$. Then

$$\sigma(\beta') + \sigma(\bar{\beta}') > 0, \tag{5.2}$$

$$\sigma(x)^2 > 0, \tag{5.3}$$

$$\sigma(\beta') = \sigma(x^2)\sigma(\beta). \tag{5.4}$$

From (5.3) and (5.4) we conclude that $\sigma(\beta)$ and $\sigma(\beta')$ have the same sign, and (5.2) forces this sign to be positive. Thus $\sigma(\beta') > 0$ and consequently $\sigma(U) \subset \mathbb{R}$. Consequently, the extension U/K satisfies the weak real embeddings condition.

Note also that if -1 is the K-norm of an element of M, then M/K must satisfy the real embeddings condition. Indeed, suppose for some $\sigma : M \longrightarrow \widetilde{\mathbb{Q}}$, we have that $\sigma(K) \subset \mathbb{R}$, while $\sigma(M) \not\subset \mathbb{R}$. Since $M = \sqrt{d}$, with $d \in K$, we must conclude that $\sigma(d) < 0$. Thus, we have real solutions to the equation:

$$\sigma(x^2) - \sigma(d)\sigma(y^2) = -1,$$

where $\sigma(d)$ is negative. This is of course impossible. Finally, suppose that for some $\sigma : U \longrightarrow \widetilde{\mathbb{Q}}$, we have that $\sigma(K) \subset \mathbb{R}$. Then $\sigma(M) \subset \mathbb{R}$ and consequently $\sigma(U) \subset \mathbb{R}$. □

We have now established that to build our tower extending a given extension of degree 2 we must have -1 as a norm. Unfortunately, this is not always the case in an arbitrary extension of number fields of degree 2. In the next lemma we identify *all* the possible causes preventing -1 from being a norm.

Lemma 5.3. *Suppose M/K is an extension of degree 2 of number fields and -1 is not the K-norm of any element from M. Then at least one of the following is true.*

1. *Extension M/K does not satisfy the real embeddings condition.*
2. *For some prime $\mathfrak{P}_K \nmid 2$ with a ramified factor in the extension M/K, we have that -1 is not a square modulo $\mathfrak{P}_K$.*
3. *For some prime $\mathfrak{P}_K | 2$ with a ramified factor in the extension M/K, we have that -1 is not a square in $K_{\mathfrak{P}_K}$ – completion of K at $\mathfrak{P}_K$.*

Proof. We will assume that all the statements above are false and show that -1 is an M-norm in K. By the Strong Hasse Norm Principle (see Theorem 4.5, page 156 of [4]), -1 is a norm globally if and only if it is a norm at all the primes. Observe that a unit is a norm locally at all the finite unramified primes. (See Proposition 3.11, page 153 of [4].) Thus we have to worry only about infinite and finite ramified primes. First suppose that for every embedding $\sigma : M \longrightarrow \widetilde{\mathbb{Q}}$, either both $\sigma(K), \sigma(M)$ are real or both non-real. Let d be such that $M = K(\sqrt{d})$. It is enough to consider the case of $\sigma = \mathrm{id}$. (Other cases of σ are analogous.) If M, K are both real, then their completion at the usual absolute value is $\mathbb{R}$, the local degree is 1 and -1 is automatically an M-norm. Similarly, if M, K are both non-real, then the completion at the usual absolute value is $\mathbb{C}$ in both cases and -1 is a norm again.

We now turn our attention to the finite ramified primes. Assume $\mathfrak{P}_K \nmid 2$ and has a ramified factor in the extension M/K. If -1 is a square mod $\mathfrak{P}_K$, then the equation $x^2 + 1 = 0$ has a root modulo $\mathfrak{P}_K$. Since $\mathfrak{P}_K \nmid 2$, we conclude that $x^2 + 1 = 0$ has a root in $K_{\mathfrak{P}_K}$ by Hensel's Lemma. Further, since the local degree is 2, any square of $K_{\mathfrak{P}_K}$ is a norm in the extension $M_{\mathfrak{P}_M}/K_{\mathfrak{P}_K}$.

Finally, if a factor of 2 is ramified, then we assume that -1 is a square in the corresponding completion and thus -1 is a norm at this prime also. □

Now that we know all the causes of our problems, we will attempt to fix what can be fixed. If the extension does not satisfy the real embeddings condition, then there is nothing to be done. In fact, the tower we seek does not exist, and as we will see in the last section of the paper, there is no way of keeping factors of all the primes not splitting in this extension from splitting in any other extension. At the same time the other two conditions can be "cured" by extending the fields. The lemmas below will lay out a "cure". We will handle one problem at a time, initially assuming that -1 is a square in every dyadic completion of the ground field. Before we proceed with the technical details however, we state without a proof a few obvious properties of extensions satisfying the strong real embeddings conditions that we will need later.

Lemma 5.4. *Let K be a number field. Then the following statements are true.*

(1) *Let $K \subset M \subset L$ be a finite extension such that extensions M/K and L/M satisfy the strong real embeddings condition. Then the extension L/K satisfies the strong real embeddings condition.*
(2) *Let M/K and L/K be finite extensions satisfying the strong real embeddings condition. Then ML/K satisfies the strong real embeddings condition.*
(3) *Let α be an algebraic number all of whose conjugates over $\mathbb{Q}$ are real. Then the extension $K(\alpha)/K$ satisfies the strong real embeddings condition.*

We now start our treatment under the assumption that -1 is a square in all the dyadic completions of the ground field. This assumption will finally be removed in Lemmas 5.9-5.11. In the lemma below we construct the base of our tower which previously consisted of just two extensions for $p > 2$ but becomes more complicated now. Given primes not splitting in an extension M/K of degree 2, rather than constructing a single extension of M of degree 2 where factors of non-splitting primes do not split, we will construct, after extending M and

K to make -1 a norm, if necessary, *two* extensions of degree 2 each taking care of a part of the relevant prime set.

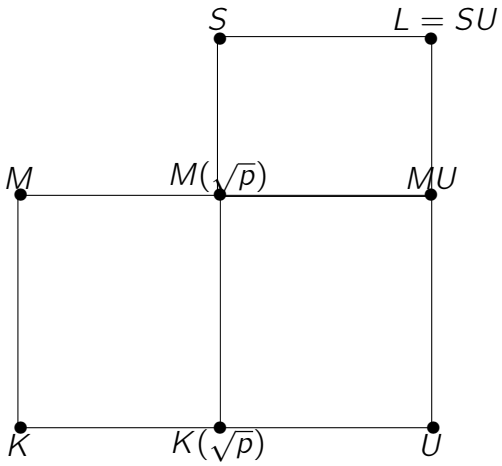
Lemma 5.5. *Let K be a number field such that every dyadic completion of K contains roots of polynomial x^2+1. Let M/K be an extension of degree 2 satisfying the real embeddings condition. Then there exists L, a finite extension of M of degree less or equal to 8, with the following properties.*

- *There exist number fields L_1, L_2 such that $M \subset L_1 \subseteq L_2 \subseteq L$, with all the extensions being of degree 2 or less.*
- *Every prime of M, lying above a prime of K not splitting in the extension M/K and not ramified in the extension L/K, will not have factors of relative degree one in the extension L/M.*
- *The extension L/K satisfies the strong real embeddings condition.*

Proof. We have to consider two cases. First assume that M contains an element with K-norm equal to -1. In this case, by Lemma 5.1 and Corollary 5.2, we can let L be an extension of degree 2 of M such that L/K is cyclic and satisfies the strong real embeddings condition. So assume now that -1 is not a K-norm of any element of M. Given our assumptions on archimedean and dyadic completions, we must conclude that for some non-dyadic primes $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_r$ of K, ramifying in the extension M/K, we have that x^2+1 does not factor in the corresponding completions of K. For each i, let q_i be the rational prime below $\mathfrak{Q}_i$. Let p be a rational prime not ramified in the extension $M/\mathbb{Q}$ and such that

$$p \cong -1 \mod \prod q_i,$$
$$p \cong 1 \mod 4.$$

Next consider below the diagram of field extensions, where U and S are constructed in the following fashion. First examine the extension $K(\sqrt{p})/K$. Since p is a positive integer, the extension $K(\sqrt{p})/K$ satisfies the real embeddings condition by Lemma 5.4. Further, the only primes possibly ramified in this extension are factors of p and factors of 2. Now, by assumption, the dyadic completions of K posses the roots of x^2+1 and therefore -1 is a norm at all the dyadics. Further, -1 is a square modulo p and since p is an odd prime, x^2+1 splits in $\mathbb{Q}_p$. Thus, completions of K at factors of p will have square roots of -1. Therefore, by Lemma 5.3 we have that -1 is a K-norm of an element of $K(\sqrt{p})$. Hence, by Lemma 5.1 and Corollary 5.2, there exists U, an extension of degree 2 of $K(\sqrt{p})$ such that U/K is cyclic and satisfies the strong real embeddings condition. Next consider the extension $M(\sqrt{p})/K(\sqrt{p})$. Note that by Lemma 5.4, the extension $M(\sqrt{p})/K$ satisfies the strong real embeddings conditions and therefore the extension $M(\sqrt{p})/K(\sqrt{p})$ satisfies the real embeddings condition. As in the case of the extension M/K, the only primes possibly ramified in this extension are dyadic primes and primes above $\mathfrak{Q}_1, \ldots, \mathfrak{Q}_r$. Note that by construction of p, it is the case that $\mathfrak{Q}_i$ does not split in the extension $K(\sqrt{p})/K$ and -1 is a square modulo the factor of $\mathfrak{Q}_i$ in $K(\sqrt{p})$ for all $i = 1, \ldots . r$. Thus, as above, there exists an extension S of degree 2 over $M(\sqrt{p})$ such that $S/K(\sqrt{p})$ is cyclic and satisfies the strong real embeddings condition. Let $L = SU$. Then by Lemma 5.4, the extensions S/K and L/K satisfy the strong real embeddings condition.



Next consider all the primes of K not splitting in the extension M/K and not ramified in the extension L/K, and divide them into two groups. If $\mathfrak{P}_K$ is such a prime of K not splitting in the extension M/K but splitting in the extension $K(\sqrt{p})/K$ then its factors in $K(\sqrt{p})$ will not split in the extension $M(\sqrt{p})/K(\sqrt{p})$, by Lemma 4.2. Therefore, the factors of such a $\mathfrak{P}_K$ will not split in the extension $S/K(\sqrt{p})$. Thus, every factor of $\mathfrak{P}_K$ in L will have relative degree at least 4. Hence, if $\mathfrak{P}_M$ lies above $\mathfrak{P}_K$ in M, all the factors of $\mathfrak{P}_M$ in L must have relative degree at least 2.

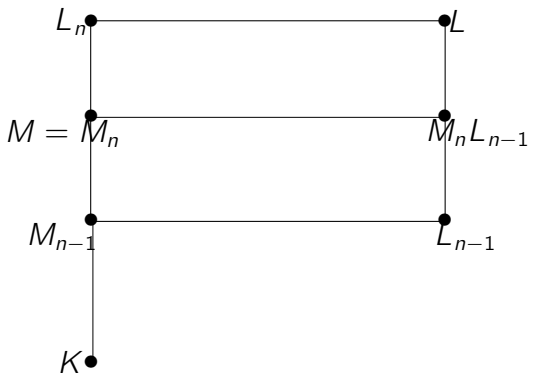
Now consider $\mathfrak{P}_K$, as described above, not splitting in both extensions M/K and $K(\sqrt{p})/K$, and not ramifying in the extension L/K. Since this $\mathfrak{P}_K$ is not splitting in the extension $K(\sqrt{p})/K$, it will not split in the extension U/K. Thus in L, all the factors of this $\mathfrak{P}_K$ will have relative degree at least 4. Hence the M-prime $\mathfrak{P}_M$ lying above this $\mathfrak{P}_K$ in M will have all of its L-factors of relative degree at least two each. □

Next we generalize somewhat the lemma above by replacing the assumption that M/K is of degree 2 by the assumption that M/K is a tower of degree 2 extensions. We will need this generalization to get the desired conclusion on relative degrees.

Corollary 5.6. *Consider the following field diagram, where K is a number field such that every dyadic completion of K contains roots of the polynomial x^2+1, M/K is a number field extension satisfying the strong real embeddings condition and such that there exist finitely many fields $M_2, \ldots, M_{n-1}$ satisfying*

$$K = M_1 \subset \ldots \subset M_{n-1} \subset M_n = M$$

with M_i/M_{i-1} being an extension of degree 2.



Then there exist an extension L of M satisfying the following conditions.

- *There exist number fields*

$$L^{(1)} \subset \ldots \subset L^{(s)} = L$$

such that

$$M \subset L^{(1)} \subset \ldots \subset L^{(s)} = L,$$

with all the extensions being of degree 2.
- *Every prime of M, of relative degree higher than 1 over K and lying above a K-prime not ramifying in the extension L/K, will have all of its L-factors with relative degrees higher than 1 over M.*
- *The extension L/K satisfies the strong real embeddings condition.*

Proof. We will proceed by induction on n. The case of $n = 2$ follows from Lemma 5.5. Suppose now that the proposition holds with for $k = n - 1$. Let $\mathscr{W}_M$ be the set of all primes of M of relative degree higher than 1 over K. Then $\mathscr{W}_M = \mathscr{W}_n \cup \mathscr{W}_{n-1}$, where $\mathscr{W}_n$ consists of $\mathscr{W}_M$-primes of degree higher than 1 over M_{n-1} and $\mathscr{W}_{n-1}$ consists of $\mathscr{W}_M$-primes of relative degree 1 over M_{n-1}. By the case of $n = 2$, there exists a field L_n such that

- There exist number fields

$$L_n^{(1)} \subset \ldots \subset L_n^{(s_n)} = L_n$$

such that

$$M \subset L_n^{(1)} \subset \ldots \subset L_n^{(s_n)} = L_n,$$

with all the extensions being of degree 2.
- Every prime of M, of relative degree higher than 1 over M_{n-1} and lying above a K-prime not ramified in the extension L_n/K, will have all of its L_n-factors with relative degrees higher than 1 over M.
- The extension L_n/M satisfies the strong real embeddings condition.

Next we consider the set $\mathscr{W}_{n-1}$. If $\mathscr{W}_{n-1}$ is empty, then we set $L = L_n$ and we are done. Otherwise, let $\mathscr{V}_{n-1}$ be the set of M_{n-1}-primes below primes of $\mathscr{W}_{n-1}$. Given our assumptions on primes of $\mathscr{W}_{n-1}$ we must conclude that primes of $\mathscr{V}_{n-1}$ are of degree higher than 1 over K. Then, by induction hypothesis, there exists a field L_{n-1} satisfying the following conditions.

- There exist number fields
$$L_{n-1}^{(1)} \subset \ldots \subset L_{n-1}^{(s_{n-1})} = L_{n-1}$$
such that
$$M_{n-1} \subset L_{n-1}^{(1)} \subset \ldots \subset L_{n-1}^{(s_{n-1})} = L_{n-1},$$
with all the extensions being of degree 2.
- Every prime of M_{n-1}, of relative degree higher than 1 over K and lying above a K-prime not ramified in the extension L_{n-1}/K, will have L_{n-1}-factors with relative degrees higher than 1 over M_{n-1}.
- The extension L_{n-1}/K satisfies the real embeddings condition.

Let $L = L_n L_{n-1}$ and consider the extension ML_{n-1}/M. Let $\mathfrak{P}_M \in \mathscr{W}_{n-1}$. Let $\mathfrak{P}_K, \mathfrak{P}_{M_{n-1}}$ be the primes below $\mathfrak{P}_M$ in K and M_{n-1} respectively with $\mathfrak{P}_K$ not ramified in the extension L/K. Let $\mathfrak{P}_{ML_{n-1}} = \mathfrak{P}_{M_n L_{n-1}}$ be a prime above $\mathfrak{P}_M$ in ML_{n-1}, and let $\mathfrak{P}_{L_{n-1}}$ be the prime below $\mathfrak{P}_{ML_{n-1}}$ in L_{n-1}. Then, on the one hand, we have
$$f(\mathfrak{P}_{ML_{n-1}}/\mathfrak{P}_K) = f(\mathfrak{P}_{ML_{n-1}}/\mathfrak{P}_M) f(\mathfrak{P}_M/\mathfrak{P}_K) = f(\mathfrak{P}_{ML_{n-1}}/\mathfrak{P}_M) f(\mathfrak{P}_{M_{n-1}}/\mathfrak{P}_K).$$
On the other hand,
$$f(\mathfrak{P}_{ML_{n-1}}/\mathfrak{P}_K) = f(\mathfrak{P}_{ML_{n-1}}/\mathfrak{P}_{L_{n-1}}) f(\mathfrak{P}_{L_{n-1}}/\mathfrak{P}_{M_{n-1}}) f(\mathfrak{P}_{M_{n-1}}/\mathfrak{P}_K).$$
Thus,
$$f(\mathfrak{P}_{ML_{n-1}}/\mathfrak{P}_M) = f(\mathfrak{P}_{ML_{n-1}}/\mathfrak{P}_{L_{n-1}}) f(\mathfrak{P}_{L_{n-1}}/\mathfrak{P}_{M_{n-1}}) \geq f(\mathfrak{P}_{L_{n-1}}/\mathfrak{P}_{M_{n-1}}) > 1.$$

Let $\mathfrak{P}_L$ lie in L above a prime $\mathfrak{P}_M \in \mathscr{W}_n$ and let $\mathfrak{P}_K$ be as above. Then
$$f(\mathfrak{P}_L/\mathfrak{P}_M) \geq f(\mathfrak{P}_{L_n}/\mathfrak{P}_M) > 1.$$
Further, if $\mathfrak{P}_M \in \mathscr{W}_{n-1}$ then
$$f(\mathfrak{P}_L/\mathfrak{P}_M) \geq f(\mathfrak{P}_{ML_{n-1}}/\mathfrak{P}_M) > 1.$$
Finally, the extension L/M was obtained by merging two towers of degree two extensions over M. Such a merge results in a tower of degree two extensions. Finally, it is clear that by Lemma 5.4, the extensions ML_{n-1}/K and L/K satisfy the strong real embeddings condition. □

We now return to the assumption that M/K is of degree two to establish that Lemma 5.5 and Corollary 5.6 allow us to produce arbitrarily high relative degrees for the factors of primes not splitting in the extension M/K.

Corollary 5.7. *Let M/K be an extension of degree 2 of number fields and let $n \in \mathbb{Z}_{>0}$. Assume also that the extension M/K satisfies the strong real embeddings condition and all dyadic completions of K contain roots of the polynomial $x^2 + 1$. Then there exists an extension L_n of M such that every prime of M of relative degree higher than one over K and lying above a K-prime not ramified in the extension L_n/K, has all of its L_n-factors of relative degree higher than 2^n over M, and the extension L_n/K satisfies the strong real embeddings condition.*

Proof. We will prove this proposition by induction. The case of $n = 1$ follows from Lemma 5.5. Note also that we can assume that the resulting extension L_1/M is a tower of extensions of degree 2 and the extension L_1/K satisfies the strong real embeddings condition. Further L_1/K is also a tower of extensions of degree 2. Assume now that we have constructed L_{n-1} satisfying the following conditions.

- Let $\mathfrak{P}_{n-1}$ be a prime of L_{n-1}. Let $\mathfrak{P}_M, \mathfrak{P}_K$ be the primes below $\mathfrak{P}_{n-1}$ in M and K respectively, with $\mathfrak{P}_K$ not ramified in the extension L_{n-1}/K. Then

$$f(\mathfrak{P}_M/\mathfrak{P}_K) > 1 \Rightarrow f(\mathfrak{P}_{n-1}/\mathfrak{P}_M) > 2^{n-1}.$$

- Extensions L_{n-1}/M and L_{n-1}/K are towers of extensions of degree 2.
- The extension L_{n-1}/K satisfies the strong real embeddings condition.

Now by Corollary 5.6 there exists an extension L_n of L_{n-1} satisfying the following conditions.

- Let $\mathfrak{P}_n$ be a prime of L_n. Let $\mathfrak{P}_{n-1}, \mathfrak{P}_K$ be the primes below $\mathfrak{P}_n$ in L_{n-1} and K respectively with $\mathfrak{P}_K$ not ramified in the extension L_n/K. Then $f(\mathfrak{P}_{n-1}/\mathfrak{P}_K) > 1$ implies $f(\mathfrak{P}_n/\mathfrak{P}_{n-1}) > 1$.
- L_n/L_{n-1} is a tower of extensions of degree 2.
- The extension L_n/L_{n-1} satisfies the strong real embeddings condition.

Let $\mathfrak{P}_M$ be a prime of M, $\mathfrak{P}_K$ a K-prime below it and suppose now that $f(\mathfrak{P}_M/\mathfrak{P}_K) > 1$ while $\mathfrak{P}_K$ is not ramified in the extension L_n/K. Then, if $\mathfrak{P}_{n-1}$ is an L_{n-1} prime above $\mathfrak{P}_M$, by induction hypothesis, $f(\mathfrak{P}_{n-1}/\mathfrak{P}_M) > 2^{n-1} > 1$ and therefore, if $\mathfrak{P}_n$ is an L_n-prime above $\mathfrak{P}_{n-1}$, by construction of L_n, we have that $f(\mathfrak{P}_n/\mathfrak{P}_{n-1}) \geq 2$. Thus, $f(\mathfrak{P}_n/\mathfrak{P}_M) > 2^n$. Further, since extensions L_{n-1}/M and L_n/L_{n-1} are towers of extensions of degree 2, we conclude that L_n/M is a tower of extensions of degree 2. Finally, by Lemma 5.4, the extension L_n/K satisfies the strong real embeddings condition. □

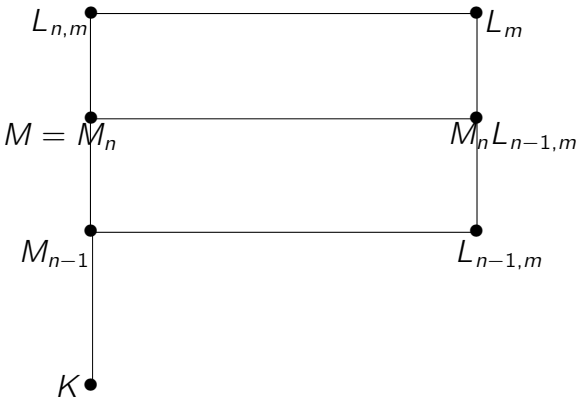
We now generalize Corollary 5.7 to the case of M/K being a tower of extensions of degree 2. We will need this case when we remove the assumptions on the dyadic completions of K.

Corollary 5.8. *Let K be a number field such that every dyadic completion of K contains roots of the polynomial $x^2 + 1$. Let M/K be a number field extension such that there exist finitely many fields satisfying*

$$K = M_1 \subset \ldots \subset M_{n-1} \subset M_n = M$$

with M_i/M_{i-1} being an extension of degree 2. Further, assume that the extension M/K satisfies the strong real embeddings condition. Then for any $m \in \mathbb{Z}_{>0}$ there exist an extension L_m of M such that every prime of M of relative degree higher than 1 over K and lying above a K-prime not ramifying in the extension L_m/K, has all of its L_m factors of relative degree greater than m over M.

Proof. The proof of this corollary is similar to the proof of Corollary 5.6. We again proceed by induction on n and consider the following diagram:



The case of $n = 2$ follows from Corollary 5.7. Suppose now that the proposition holds with for $k = n - 1$. Let $\mathscr{W}_M$ be the set of all primes of M of relative degree higher than 1 over K. Then $\mathscr{W}_M = \mathscr{W}_n \cup \mathscr{W}_{n-1}$, where $\mathscr{W}_n$ consists of M-primes of degree higher than 1 over M_{n-1} and $\mathscr{W}_{n-1}$ consists of M-primes of relative degree 1 over M_{n-1}. By the case of $n = 2$, there exists a field $L_{n,m}$ such that all primes of M, of relative degree higher than 1 over M_{n-1} and lying above K-primes unramified in the extension $L_{n,m}/K$, will have all of their $L_{n,m}$-factors with relative degrees higher than m over M. Further, the extension $L_{n,m}/M$ will satisfy the strong real embeddings condition.

Next we consider the set $\mathscr{W}_{n-1}$. If $\mathscr{W}_{n-1}$ is empty, then we set $L_m = L_{m,n}$ and we are done. Otherwise, let $\mathscr{V}_{n-1}$ be the set of M_{n-1} primes below primes of $\mathscr{W}_{n-1}$. Given our assumptions on the primes of $\mathscr{W}_{n-1}$ we must conclude that primes of $\mathscr{V}_{n-1}$ are of degree higher than 1 over K. Then, by induction hypothesis, there exists a field $L_{m,n-1}$ satisfying the following condition. Every prime of M_{n-1}, of relative degree higher than 1 over K and lying above a K-prime unramified in the extension $L_{m,n-1}/K$, will have all of its $L_{m,n-1}$-factors with relative degrees higher than m over M_{n-1}, and the extension $L_{m,n-1}/K$ will satisfy the strong real embeddings condition.

Let $L_m = L_{m,n}L_{m,n-1}$ and consider the extension $ML_{n-1,m}/M$. Let $\mathfrak{P}_M \in \mathscr{W}_{n-1}$. Let $\mathfrak{P}_K, \mathfrak{P}_{M_{n-1}}$ be the primes below $\mathfrak{P}_M$ in K and M_{n-1} respectively with $\mathfrak{P}_K$ unramified in the extension L_m/K. Let $\mathfrak{P}_{ML_{m,n-1}}$ be a prime above $\mathfrak{P}_M$ in $ML_{m,n-1}$, and let $\mathfrak{P}_{L_{m,n-1}}$ be the prime below $\mathfrak{P}_{ML_{m,n-1}}$ in $L_{m,n-1}$. Then we have the following. On the one hand,

$$f(\mathfrak{P}_{ML_{m,n-1}}/\mathfrak{P}_K) = f(\mathfrak{P}_{ML_{m,n-1}}/\mathfrak{P}_M)f(\mathfrak{P}_M/\mathfrak{P}_K) = f(\mathfrak{P}_{ML_{m,n-1}}/\mathfrak{P}_M)f(\mathfrak{P}_{M_{n-1}}/\mathfrak{P}_K).$$

On the other hand,

$$f(\mathfrak{P}_{ML_{m,n-1}}/\mathfrak{P}_K) = f(\mathfrak{P}_{ML_{m,n-1}}/\mathfrak{P}_{L_{m,n-1}})f(\mathfrak{P}_{L_{m,n-1}}/\mathfrak{P}_{M_{n-1}})f(\mathfrak{P}_{M_{n-1}}/\mathfrak{P}_K).$$

Thus,

$$f(\mathfrak{P}_{ML_{m,n-1}}/\mathfrak{P}_M) = f(\mathfrak{P}_{ML_{m,n-1}}/\mathfrak{P}_{L_{m,n-1}})f(\mathfrak{P}_{L_{m,n-1}}/\mathfrak{P}_{M_{n-1}}) \geq f(\mathfrak{P}_{L_{m,n-1}}/\mathfrak{P}_{M_{n-1}}) > m.$$

Let $\mathfrak{P}_{L_m}$ lie above a prime $\mathfrak{P}_M \in \mathscr{W}_n$ in L_m with $\mathfrak{P}_K$ as above. Then

$$f(\mathfrak{P}_{L_m}/\mathfrak{P}_M) \geq f(\mathfrak{P}_{L_{m,n}}/\mathfrak{P}_M) > m.$$

And if $\mathfrak{P}_M \in \mathscr{W}_{n-1}$. Then

$$f(\mathfrak{P}_{L_m}/\mathfrak{P}_M) \geq f(\mathfrak{P}_{ML_{m,n-1}}/\mathfrak{P}_M) > m.$$

Finally, by Lemma 5.4, the extension L_m/K satisfies the strong real embeddings condition. □

We are now ready to consider the cases of the fields which have dyadic completions not containing i. We start with an obvious assertion we will need later. Its proof is a direct consequence of Hensel's lemma.

Lemma 5.9. *Let K be a number field such that K contains $\sqrt{15}$. Then every dyadic completion of K contains roots of the polynomial x^2+1.*

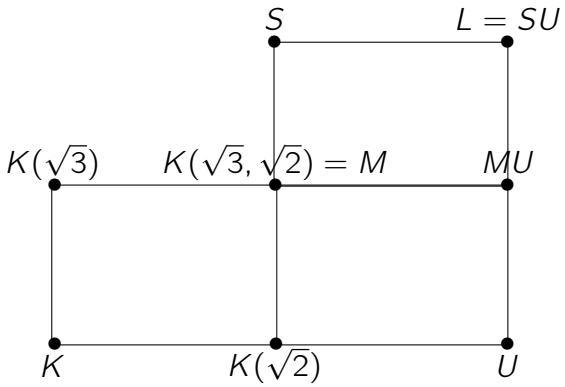
The following lemma is similar to Lemma 5.5. It will also construct a foundation of a tower, but on top of the constructed tower -1 will be a square at all the dyadic completions.

Lemma 5.10. *Let K be a number field containing neither $\sqrt{3}$, nor $\sqrt{2}$. Then there exists an extension L of $M = K(\sqrt{3},\sqrt{2})$ such that for every prime of M of relative degree greater than one over K and lying above a K-prime not ramified in the extension L/K, all of its L-factors will be of relative degree greater than 1 over M, and L/M is Galois of degree 4 with the Galois group isomorphic to $\mathbb{Z}/2\times\mathbb{Z}/2$. Further, the extension L/K will satisfy the strong real embeddings condition.*

Proof. Consider the field diagram below, where fields U and S are obtained in the following fashion. First of all observe that $K(\sqrt{2})$ has an element with K-norm equal to -1, i.e. $1-\sqrt{2}$. Thus by Lemma 5.1 and Corollary 5.2, there exists an extension U of $K(\sqrt{2})$ such that U/K is cyclic of degree 4 and the extension U/K satisfies the strong real embeddings condition. (For future reference we note that since $(1-\frac{\sqrt{2}}{2}) = (1-\sqrt{2})^2(1+\frac{\sqrt{2}}{2})$, by Lemma 5.1, we can take $U = K(\sqrt{2},\sqrt{1-\frac{\sqrt{2}}{2}})$.)

Further, $K(\sqrt{2},\sqrt{3})$ has an element whose $K(\sqrt{2})$-norm is -1, that is $\sqrt{2}-\sqrt{3}$. Thus, again by Lemma 5.1 and Corollary 5.2, it follows that $M = K(\sqrt{3},\sqrt{2})$ has an extension S of degree 2, such that $S/K(\sqrt{2})$ is a cyclic extension of degree 4 and the extension $S/K(\sqrt{2})$ satisfies the strong real embeddings condition. (Again for future reference, note that $(1-\frac{\sqrt{2}}{\sqrt{3}}) = (\sqrt{2}-\sqrt{3})^2(1+\frac{\sqrt{2}}{\sqrt{3}})$. Thus by Lemma 5.1, we can take $S = K(\sqrt{2},\sqrt{3},\sqrt{1-\frac{\sqrt{2}}{\sqrt{3}}})$.)

Note also that $[MU : M] = [MU : U] = 2$. Otherwise, $M = U$ contradicting the fact that the extension U/K is cyclic of degree 4 and the Galois group of M/K is isomorphic to $\mathbb{Z}/2\times\mathbb{Z}/2$. Note further that the extension $MU/K(\sqrt{3})$ is a cyclic extension of degree 4.



Next we analyze prime splitting in the extension L/K, where $L = SU$. Let $\mathfrak{P}_M$ be a prime of M of relative degree greater than 1 over K. Let $\mathfrak{P}_K$ be the prime below $\mathfrak{P}_M$ in K such that $\mathfrak{P}_K$ is not ramified in the extension L/K. Then we have to consider three cases.

Case 1: $\mathfrak{P}_K$ does not split in the extension $K(\sqrt{3})/K$ but splits in the extension $K(\sqrt{2})/K$. Then, by Lemma 4.2, we have that $\mathfrak{P}_M$ lies above a non-splitting prime from the extension $M/K(\sqrt{2})$ and therefore $\mathfrak{P}_M$ does not split in the extension S/M by Lemma 3.3.

Case 2: $\mathfrak{P}_K$ splits in the extension $K(\sqrt{3})/K$ but not in the extension $K(\sqrt{2})/K$. By Lemma 4.2 again, $\mathfrak{P}_M$ lies above a non-splitting prime in the extension $M/K(\sqrt{3})$ and therefore, $\mathfrak{P}_M$ will not split in the extension MU/M by Lemma 3.3.

Case 3: $\mathfrak{P}_K$ splits in neither $K(\sqrt{2})/K$, nor in $K(\sqrt{3})/K$. Let $\mathfrak{P}_{K(\sqrt{2})}$ be the prime above $\mathfrak{P}_K$ in $K(\sqrt{2})$. Then $\mathfrak{P}_{K(\sqrt{2})}$ splits completely in the extension $M/K(\sqrt{2})$ and does not split in the extension $U/K(\sqrt{2})$ yet again by Lemma 4.2 and Lemma 3.3. Thus, in this case $\mathfrak{P}_M$ does not split in the extension MU/M by Lemma 4.2 again.

Thus, in either case, $\mathfrak{P}_L$ – a factor of $\mathfrak{P}_M$ in L, will have a relative degree of at least 2 over M.

Finally, the fact that the extension L/K satisfies the strong real embeddings condition follows from the fact that

$$L = K(\sqrt{2}, \sqrt{3}, \sqrt{1 - \frac{\sqrt{2}}{\sqrt{3}}}, \sqrt{1 - \frac{\sqrt{2}}{2}}).$$

□

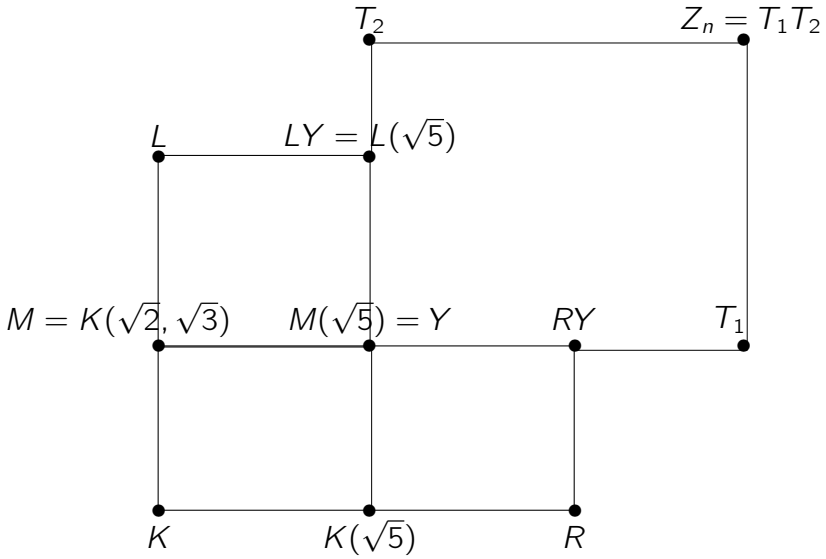
We now construct the rest of the tower for the case -1 is not a square of all dyadic completions of the ground field.

Lemma 5.11. *Let K be a number field such that the extension $Y = K(\sqrt{2}, \sqrt{3}, \sqrt{5})/K$ is not trivial. Then for any n there exists a field Z_n such that for any prime $\mathfrak{P}_Y$ of relative degree greater than 1 over K and lying above a K-prime not ramified in the extension Z_n/K, all of its Z_n-factors are of relative degree greater or equal to n over Y.*

Proof. We will assume first that K does not contain $\sqrt{2}, \sqrt{3}$, or $\sqrt{5}$. Please note that by Lemma 5.9, all the dyadic completions of Y have the roots of the polynomial $x^2 + 1$. Consider next the field extension diagram below, where fields L, T_1, T_2, R are constructed

in the following fashion. L is the extension of $M = K(\sqrt{2}, \sqrt{3})$ constructed in the Lemma 5.10. From the explicit calculations done in the proof of Lemma 5.10 it follows that L and Y are linearly disjoint over M and therefore LY is of degree 4 over Y. Since all the dyadic completions of Y have the square roots of -1, and by construction of L and Lemma 5.4, the extension LY/Y satisfies the strong real embeddings condition, by Corollary 5.8, there exists an extension T_2 of LY such that any prime of LY of relative degree higher than 1 over Y will have T_2-factors of relative degree higher than n over LY.

Next we consider the extension $K(\sqrt{5})/K$. Note that $2^2 - 5 = -1$ and therefore by Lemma 5.1 and Corollary 5.2, there exists an extension R of $K(\sqrt{5})$ such that R/K is a cyclic extension of degree 4 and the extension R/K satisfies the strong real embeddings condition. Further since M and $K(\sqrt{5})$ are linearly disjoint over K, it is the case that RY/Y is an extension of degree 2. Further, by Lemma 5.4 and construction of R and Y, the extension RY/K satisfies the strong real embeddings condition and therefore the extension RY/Y satisfies the strong real embeddings condition. Consequently, by Corollary 5.8 again, there exists an extension T_1 of RY such that any RY-prime of relative degree greater than 1 over Y will have T_1-factors of relative degree greater than n over RY. Finally, we set $Z_n = T_1T_2$.



Next let $\mathfrak{P}_Y$ be a prime of Y of relative degree higher than 1 over K. Let $\mathfrak{P}_K, \mathfrak{P}_M, \mathfrak{P}_{K(\sqrt{5})}$ be the primes below $\mathfrak{P}_Y$ in K, M and $K(\sqrt{5})$ respectively with $\mathfrak{P}_K$ not ramified in the extension Z_n/K. Let $\mathfrak{P}_{LY}$ be a prime above $\mathfrak{P}_Y$ in LY. Let $\mathfrak{P}_L$ be a prime below $\mathfrak{P}_{LY}$ in L. As in Lemma 5.10, we have to consider three cases:

(1) *The case of* $f(\mathfrak{P}_M/\mathfrak{P}_K) > 1$ *and* $f(\mathfrak{P}_{K(\sqrt{5})}/\mathfrak{P}_K) = 1$*:*
In this case, $f(\mathfrak{P}_L/\mathfrak{P}_M) > 1$ by construction of L. Note that on the one hand,

$$f(\mathfrak{P}_{LY}/\mathfrak{P}_K) = f(\mathfrak{P}_{LY}/\mathfrak{P}_Y)f(\mathfrak{P}_Y/\mathfrak{P}_{K(\sqrt{5})}f(\mathfrak{P}_{K(\sqrt{5})}/\mathfrak{P}_K) = f(\mathfrak{P}_{LY}/\mathfrak{P}_Y)f(\mathfrak{P}_Y/\mathfrak{P}_{K(\sqrt{5})}),$$

On the other hand,

$$f(\mathfrak{P}_{LY}/\mathfrak{P}_K) = f(\mathfrak{P}_{LY}/\mathfrak{P}_L)f(\mathfrak{P}_L/\mathfrak{P}_M)f(\mathfrak{P}_M/\mathfrak{P}_K).$$

Since $\mathfrak{P}_K$ splits completely in the extension $K(\sqrt{5})/K$, the prime $\mathfrak{P}_L$ above $\mathfrak{P}_K$ in L splits completely in the extension $LY/L = L(\sqrt{5})/L$ by the repeated application of Lemma 4.1. Consequently, $f(\mathfrak{P}_{LY}/\mathfrak{P}_L) = 1$. Thus,

$$f(\mathfrak{P}_{LY}/\mathfrak{P}_K) = f(\mathfrak{P}_L/\mathfrak{P}_M)f(\mathfrak{P}_M/\mathfrak{P}_K).$$

Therefore,

$$f(\mathfrak{P}_L/\mathfrak{P}_M)f(\mathfrak{P}_M/\mathfrak{P}_K) = f(\mathfrak{P}_{LY}/\mathfrak{P}_Y)f(\mathfrak{P}_Y/\mathfrak{P}_{K(\sqrt{5})}),$$

Further,

$$f(\mathfrak{P}_M/\mathfrak{P}_K) = f(\mathfrak{P}_Y/\mathfrak{P}_{K(\sqrt{5})}),$$

since the relative degree is 1 from K to $K(\sqrt{5})$ at $\mathfrak{P}_K$ and thus $f(\mathfrak{P}_Y/\mathfrak{P}_M) = 1$ by Lemma 4.1. Consequently,

$$1 < f(\mathfrak{P}_L/\mathfrak{P}_M) = f(\mathfrak{P}_{LY}/\mathfrak{P}_Y).$$

In this case by construction of T_2, for any prime $\mathfrak{P}_{T_2}$ above $\mathfrak{P}_{LY}$, we have that $f(\mathfrak{P}_{T_2}/\mathfrak{P}_{LY}) > n$. Hence, $f(\mathfrak{P}_{T_2}/\mathfrak{P}_Y) > n$. Finally if $\mathfrak{P}_{Z_n}$ is any prime above $\mathfrak{P}_Y$ in Z_n, then clearly $f(\mathfrak{P}_{Z_n}/\mathfrak{P}_Y) > n$.

(2) *The case of* $f(\mathfrak{P}_M/\mathfrak{P}_K) = 1$ *and* $f(\mathfrak{P}_{K(\sqrt{5})}/\mathfrak{P}_K) > 1$*:*
In this case, by a double application of Lemma 4.2, we have that

$$f(\mathfrak{P}_Y/\mathfrak{P}_{K(\sqrt{5})}) = 1,$$

$$f(\mathfrak{P}_Y/\mathfrak{P}_M) = f(\mathfrak{P}_{K(\sqrt{5})}/\mathfrak{P}_K) = 2.$$

Indeed, let $\mathfrak{P}_{K(\sqrt{2})}$ be the primes below $\mathfrak{P}_M$ in $K(\sqrt{2})$. Let $\mathfrak{P}_{K(\sqrt{2},\sqrt{5})}$ be the prime above $\mathfrak{P}_{K(\sqrt{2})}$ in $K(\sqrt{2},\sqrt{5})$. Then by assumption we have that

$$f(\mathfrak{P}_{K\sqrt{2}}/\mathfrak{P}_K) = f(\mathfrak{P}_M/\mathfrak{P}_{K\sqrt{2}}) = 1,$$

and by Lemma 4.2 applied two times (to $K(\sqrt{2},\sqrt{5})/K$ and to $Y/K(\sqrt{2})$), it follows that

$$f(\mathfrak{P}_{K(\sqrt{2},\sqrt{5})}/\mathfrak{P}_{K(\sqrt{2})}) = f(\mathfrak{P}_Y/\mathfrak{P}_M) = 2,$$

Further, extension RY/M is a cyclic extension of degree 4. Therefore, if $\mathfrak{P}_{RY}$ is a prime above $\mathfrak{P}_Y$ in RY, then, by Lemma 3.3, $f(\mathfrak{P}_{RY}/\mathfrak{P}_Y) = 2$. Further, by construction of T_1, if $\mathfrak{P}_{T_1}$ is any prime above $\mathfrak{P}_Y$ in T_1, we conclude that $f(\mathfrak{P}_{T_1}/\mathfrak{P}_{RY}) > n$. Consequently, $f(\mathfrak{P}_{T_1}/\mathfrak{P}_Y) > n$ and $f(\mathfrak{P}_{Z_n}/\mathfrak{P}_Y) > n$.

(3) *The case of* $f(\mathfrak{P}_M/\mathfrak{P}_K) > 1$ *and* $f(\mathfrak{P}_{K(\sqrt{5})}/\mathfrak{P}_K) > 1$*:*
In this case, by two applications of Lemmas 4.2 again, and by construction of R, we have

$$f(\mathfrak{P}_Y/\mathfrak{P}_{K(\sqrt{5})}) = f(\mathfrak{P}_{RY}/\mathfrak{P}_R) = 1,$$

$$f(\mathfrak{P}_{RY}/\mathfrak{P}_Y) = f(\mathfrak{P}_R/\mathfrak{P}_{K(\sqrt{5})}) = 2.$$

Indeed, let $\mathfrak{P}_{K(\sqrt{2})}, \mathfrak{P}_{K(\sqrt{3})}$ be the primes below $\mathfrak{P}_M$ in $K(\sqrt{2})$ and $K(\sqrt{3})$ respectively. Let $\mathfrak{P}_{K(\sqrt{2},\sqrt{5})}$ be the prime below $\mathfrak{P}_Y$ in $K(\sqrt{2},\sqrt{5})$. By Lemma 4.2, either $f(\mathfrak{P}_M/\mathfrak{P}_{K(\sqrt{2})}) = 1$ or $f(\mathfrak{P}_M/\mathfrak{P}_{K(\sqrt{3})}) = 1$ (since M/K is of degree 4 and not a cyclic

extension). Without loss of generality assume that $f(\mathfrak{P}_M/\mathfrak{P}_{K(\sqrt{2})}) = 1$. Therefore, given our assumptions,

$$f(\mathfrak{P}_{K(\sqrt{2})}/\mathfrak{P}_K) = 2.$$

Then applying Lemma 4.2 to the extension $K(\sqrt{2}, \sqrt{5})/K$, we conclude that

$$f(\mathfrak{P}_{K(\sqrt{2},\sqrt{5})}/\mathfrak{P}_{K(\sqrt{5})}) = 1.$$

Applying Lemma 4.2 to the extension $Y/K(\sqrt{2})$, we now conclude that

$$f(\mathfrak{P}_Y/\mathfrak{P}_{K(\sqrt{2},\sqrt{5})}) = 1.$$

Thus,

$$f(\mathfrak{P}_Y/\mathfrak{P}_{K(\sqrt{5})}) = 1.$$

Now applying Lemma 4.2 twice to the extension $RY/K(\sqrt{5})$, we conclude that $f(\mathfrak{P}_{RY}/\mathfrak{P}_R) = 1$. Further, the comparison of relative degrees gives

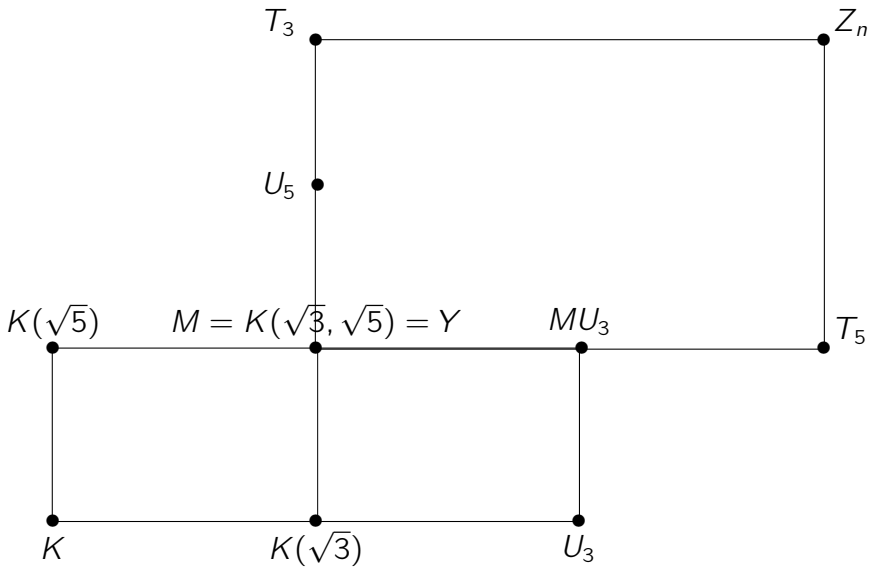
$$f(\mathfrak{P}_{RY}/\mathfrak{P}_Y) = f(\mathfrak{P}_R/\mathfrak{P}_{K(\sqrt{5})}),$$

where by construction of R, we know that $f(\mathfrak{P}_R/\mathfrak{P}_{K(\sqrt{5})}) = 2$. Consequently, as above, by construction of T_1, we have that $f(\mathfrak{P}_{T_1}/\mathfrak{P}_Y) > n$ and $f(\mathfrak{P}_{Z_n}/\mathfrak{P}_Y) > n$.

We still have to consider the cases where K contains exactly one of $\sqrt{2}, \sqrt{3}, \sqrt{5}$ and the cases when K contains exactly two of $\sqrt{2}, \sqrt{3}, \sqrt{5}$. These are cases handled in a manner similar to the one used above. We will go over them briefly.

Assume that K contains $\sqrt{5}$ but not $\sqrt{2}$ or $\sqrt{3}$. This case can proceed pretty much as the proof of Lemma 5.10. The only difference will come at the end when we have constructed the extension L/M. We can note that M contains $\sqrt{2}, \sqrt{3}$, and $\sqrt{5}$. Thus, by Lemma 5.9, all dyadic completions of M will have roots of the polynomial $x^2 + 1$. Hence by Corollary 5.8, we can construct an extension Z_n of L such that every L-prime of relative degree higher than one over M has all of its Z_n-factors of relative degree higher than n over M. But by construction of L, every M-prime of degree higher than one over K, has all of its L factors of relative degree higher than one over M. Therefore, Z_n will have the required properties.

Assume now that K contains $\sqrt{2}$ but not $\sqrt{3}$ or $\sqrt{5}$. Then this case can be handled by the following diagram, where $U_5/K(\sqrt{3})$ is a cyclic extension of degree 4 satisfying the strong real embeddings condition, T_3 is an extension of U_5 such that every U_5-prime of relative degree greater than 1 over M has all of its T_3-factors of relative degree higher than n over M, extensions U_3/K, $MU_3/K(\sqrt{5})$ are cyclic of degree 4 satisfying the strong real embeddings condition, T_5 is an extension of MU_3 such that every MU_3-prime of relative degree greater than 1 over M has all of its T_5 factors of relative degree higher than n over M. The existence of all of these extensions is justified the same way as in the arguments above.



The case of K containing $\sqrt{3}$ but not $\sqrt{2}$ or $\sqrt{5}$ is handled in almost identical fashion with $K(\sqrt{3})$ replaced by $K(\sqrt{2})$, since $1+\sqrt{2}$ is a $K(\sqrt{2})$-element of K-norm equal to -1.

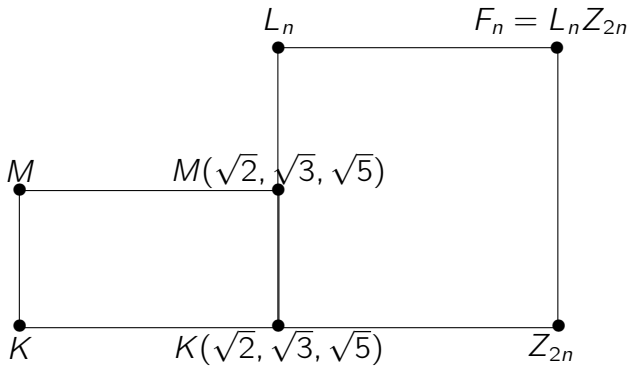
Finally, we consider *the cases of K containing exactly two of the three roots*. If K contains $\sqrt{5}$ and $\sqrt{3}$, then all the dyadic completions of K have square root of -1 as above and the extension $K(\sqrt{2})/K$ can be handled by Corollary 5.7. If K contains $\sqrt{2}$ and $\sqrt{5}$. Then $K(\sqrt{3})$ has an extension U_3 such that U_3/K is cyclic of degree 4 satisfying the strong real embeddings condition. From this point we proceed as above. The case of K containing $\sqrt{3}, \sqrt{2}$ but not $\sqrt{5}$ is identical to the preceding case. □

We now state an prove the main proposition of this section which summarizes the above discussion of extensions of degree 2.

Proposition 5.12. *Let M/K be an extension of number fields of degree 2 satisfying the real embeddings condition. Then for any $n \in \mathbb{Z}_{>0}$ there exists an extension F_n of M such that any prime of M of relative degree 2 over K and lying above a K-prime unramified in the extension F_n/K, will have all of its F_n-factors of relative degree greater than n over M.*

Proof. If all the dyadic completions of K have square root of -1, then we are done by Corollary 5.8. If this is not the case, then the extension $K(\sqrt{3}, \sqrt{5})/K$ is non-trivial. If $M \subseteq K(\sqrt{2}, \sqrt{3}, \sqrt{5})$, then we are done by Lemma 5.11. Otherwise, $K(\sqrt{2}, \sqrt{3}, \sqrt{5})$ and M are linearly disjoint over K. So assume $M \not\subseteq K(\sqrt{2}, \sqrt{3}, \sqrt{5})$ and consider the following diagram, where L_n is such that any prime of $M(\sqrt{2}, \sqrt{3}, \sqrt{5})$ of relative degree greater than one over $K(\sqrt{2}, \sqrt{3}, \sqrt{5})$ and lying above $K(\sqrt{2}, \sqrt{3}, \sqrt{5})$-prime unramified in the extension $L_n/K(\sqrt{2}, \sqrt{3}, \sqrt{5})$, will have all of its L_n factors of relative degree higher than n over $M(\sqrt{2}, \sqrt{3}, \sqrt{5})$. L_n exists by Corollary 5.8, since all the dyadic completions of $K(\sqrt{2}, \sqrt{3}, \sqrt{5})$ have square root of -1 and the real embeddings condition is satisfied by the extension $M(\sqrt{2}, \sqrt{3}, \sqrt{5})/K(\sqrt{2}, \sqrt{3}, \sqrt{5})$ by Lemma 5.4. Further, Z_{2n} is an extension of $K(\sqrt{2}, \sqrt{3}, \sqrt{5})$ such that any prime of $K(\sqrt{2}, \sqrt{3}, \sqrt{5})$ of relative degree greater than one over K and lying above a K-prime unramified in the extension Z_{2n}/K, will have all of its Z_{2n}

factors of relative degree higher than $2n$ over $K(\sqrt{2},\sqrt{3},\sqrt{5})$. Existence of Z_{2n} is guaranteed by Lemma 5.11.



Let $\mathfrak{P}_M$ be a prime of relative degree 2 over $\mathfrak{P}_K$, the prime below it in K unramified in the extension F_n/K. We will consider two cases: the case of $\mathfrak{P}_K$ splitting completely in the extension $K(\sqrt{2},\sqrt{3},\sqrt{5})/K$ and the case when this does not happen. In the first case, let $\mathfrak{P}_{M(\sqrt{2},\sqrt{3},\sqrt{5})}$ be the prime above $\mathfrak{P}_M$ in $M(\sqrt{2},\sqrt{3},\sqrt{5})$. Then $\mathfrak{P}_{M(\sqrt{2},\sqrt{3},\sqrt{5})}$ is of relative degree 2 over $K(\sqrt{2},\sqrt{3}\sqrt{5})$ since $f(\mathfrak{P}_{M(\sqrt{2},\sqrt{3},\sqrt{5})}/\mathfrak{P}_K) \geq 2$. Let $\mathfrak{P}_{F_n}$ be any prime above $\mathfrak{P}_M$ in F_n. Then we have the following.

$$f(\mathfrak{P}_{F_n}/\mathfrak{P}_M) \geq f(\mathfrak{P}_{L_n}/\mathfrak{P}_M) \geq f(\mathfrak{P}_{L_n}/\mathfrak{P}_{M(\sqrt{2},\sqrt{3},\sqrt{5})}) > n,$$

where the last inequality is true by construction of L_n and the fact that $\mathfrak{P}_{M(\sqrt{2},\sqrt{3},\sqrt{5})}$ is of relative degree 2 over $K(\sqrt{2},\sqrt{3},\sqrt{5})$. We now consider the second case, the case $\mathfrak{P}_K$ not splitting completely in the extension $K(\sqrt{2},\sqrt{3},\sqrt{5})$. Then by construction of Z_{2_n}, using the same notational scheme as above

$$f(\mathfrak{P}_{F_n}/\mathfrak{P}_K) \geq f(\mathfrak{P}_{Z_{2n}}/\mathfrak{P}_K) > 2n,$$

$$f(\mathfrak{P}_{F_n}/\mathfrak{P}_M) = \frac{1}{2} f(\mathfrak{P}_{F_n}/\mathfrak{P}_K) > n.$$

□

6. Cyclic extensions of prime degree of function fields.

In this section we consider the cyclic and totally inseparable extensions of algebraic function fields in one variable over finite fields of constants (abbreviated as "function fields" in the future). The case of cyclic extensions of these fields is very similar to the cyclic case for number fields. The main difference is that in the case of function fields we will have to consider separately not necessarily the case of extensions of degree 2 but rather the case of extensions whose degree is equal to the characteristic of the field. We start with the case when the degree of the extension is different from the characteristic.

Proposition 6.1. *Let M/K be a cyclic extension of degree q of function fields over finite field of constants of characteristic $p > 0$. Assume q is a rational prime distinct from p. Then for any $n \in \mathbb{Z}_{>0}$ there exists a finite separable extension L of M such that any prime of M of*

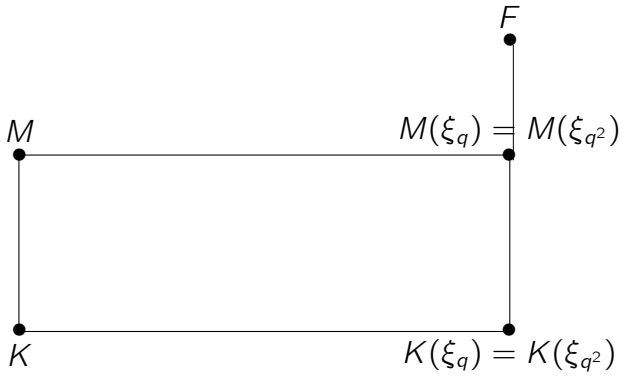
relative degree higher than 1 over K lying above a K-prime unramified in the extension L/K, will have all of its factors in L of relative degree greater than n over M.

Proof. First observe the following. If $\xi_q \in K$, then of course $[M : K] = [M(\xi_q) : K(\xi_q)]$. At the same time, if $\xi_q \notin K$, then, due to the fact that $([K(\xi_q) : K], q) = 1$, M and $K(\xi_q)$ are linearly disjoint over K, and thus we still have $[M : K] = [M(\xi_q) : K(\xi_q)]$. Further, by Lemma 4.1, a prime of $K(\xi_q)$, lying above a prime of K unramified in the extension $M(\xi_q)/K$, splits in the extension $M(\xi_q)/K(\xi_q)$ if and only if the prime below it splits completely in the extension M/K. Thus, as in some cases for number fields we can consider the extension $M(\xi_q)/K(\xi_q)$ instead of M/K. Given this simplification, we are led to consider three cases below.

(1) *The Case of $\xi_{q^2} \in K(\xi_q)$*: Consider the field diagram below, where F, a finite separable extension of $M(\xi_q)$, is such that every prime $\mathfrak{P}_{M(\xi_{q^2})}$ of $M(\xi_q)$ of relative degree higher than one over $K(\xi_q)$ and lying above a prime of $K(\xi_q)$ unramified in the extension $F/K(\xi_q)$, will have all of its F-factors of relative degree higher than n over $M(\xi_q)$. The existence of F follows from Theorem 10, page 214 of [7], the fact that $\xi_{q^2} \in K(\xi_q)$ and Lemma 3.4. Indeed, by Theorem 10, page 214 of [7] we have as in the case of number fields

$$K_1 = M(\xi_q) = K(\xi_q, \alpha_1) = K_0(\alpha_1),$$

where $K_0 = K(\xi_q)$ and $\alpha_1^q \in K_0$. Let $K_2 = K_1(\alpha_2)$, where $\alpha_2^q = \alpha_1$. Since $\xi_{q^2} \in K_0$, the extension K_2/K_0 is cyclic of degree q^2. Now we can continue as in Lemma 3.4 to construct a chain $K_0 \subset K_1 \ldots \subset K_{n+1} = F$ such that $K_{i+2}/K_i, i = 0, \ldots, n-1$ is a Galois extension of degree q^2, and the primes of K_0 not splitting in the extension K_1/K_0 do not split in the extension F/K_0. Therefore, any prime of $M(\xi_q)$ of degree greater than 1 over $K(\xi_q)$ and lying above K_0-prime not ramified in the extension F/K_0, will have all of its F-factors of degree greater than $q^n \geq n$ over $M(\xi_q)$.

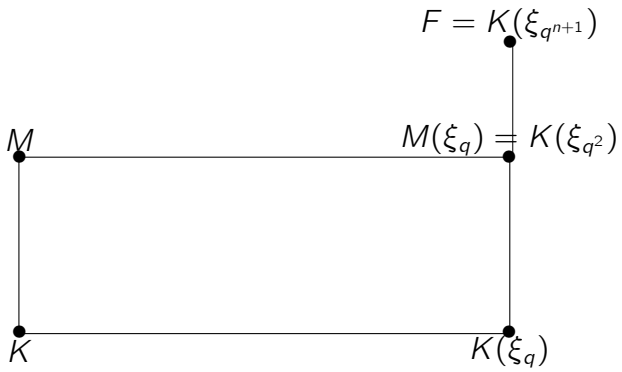


Let $\mathfrak{P}_M$ be a prime of M of relative degree greater than 1 over K. Let $\mathfrak{P}_F$ be a prime above $\mathfrak{P}_M$ in F. Let $\mathfrak{P}_{M(\xi_q)}, \mathfrak{P}_{K(\xi_q)}, \mathfrak{P}_K$ be the primes below $\mathfrak{P}_F$ in the fields $M(\xi_q), K(\xi_q)$ and K respectively with $\mathfrak{P}_K$ unramified in the extension F/K. Then, as has been noted above, $f(\mathfrak{P}_{M(\xi_q)}/\mathfrak{P}_{K(\xi_q)}) = q$ and therefore by construction of F, $f(\mathfrak{P}_F/\mathfrak{P}_{M(\xi_q)}) \geq n$. Thus,

$$f(\mathfrak{P}_F/\mathfrak{P}_M) = \frac{1}{q} f(\mathfrak{P}_F/\mathfrak{P}_K) = \frac{1}{q} f(\mathfrak{P}_F/\mathfrak{P}_{M(\xi_q)}) f(\mathfrak{P}_{M(\xi_q)}/\mathfrak{P}_{K(\xi_q)}) f(\mathfrak{P}_{K(\xi_q)}/\mathfrak{P}_K) \geq \frac{1}{q} nq = n$$

Thus we can set $L = F$.

(2) *The Case of* $\xi_{q^2} \notin K(\xi_q)$ *and* $M(\xi_q) = K(\xi_{q^2})$: Consider the following picture.



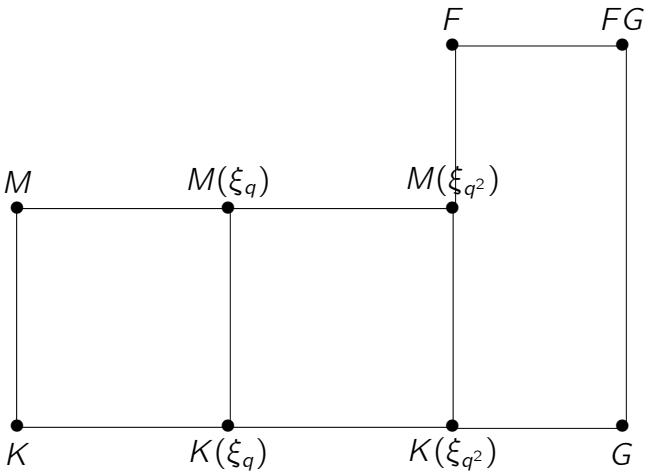
In this case we also set $L = F$ and the conclusion of the lemma follows by an argument similar to the one used in Case 1.

(3) *The Case of* $\xi_{q^2} \notin K(\xi_q)$, *and* M *and* $K(\xi_{q^2})$ *are linearly disjoint over* $K(\xi_q)$: Consider the field diagram below, where, by Theorem 10, page 214 of [7] we have that

$$M(\xi_{q^2}) = K(\xi_{q^2}, \alpha), \text{ where } \alpha^q \in K(\xi_{q^2}) \text{ and } \alpha \notin K(\xi_{q^2}).$$

Hence, in this case, as in the first case, by Lemma 3.4, there exists a finite separable extension F of $M(\xi_{q^2})$ such that every prime of $M(\xi_{q^2})$ of relative degree higher than 1 over $K(\xi_{q^2})$ and lying above a $K(\xi_{q^2})$-prime unramified in the extension $F/K(\xi_{q^2})$, has all of its F-factors of relative degree higher than nq over $M(\xi_{q^2})$.

Next let C_K be the constant field of K. Let C_n be an extension of degree $q^{n+1} > nq$ of $C(\xi_{q^2})$ – the constant field $K(\xi_{q^2})$. Such an extension exists by propositions on pages 184-186 of [7]. Then the extension $C_n/C(\xi_{q^2})$ is cyclic and so is the extension KC_n/K. Further, $[KC_n : K] = [C_n : C]$ by Theorem 11, page 280 of [1]. Let $G = KC_n$. Then we can apply Lemma 3.4 to conclude that every prime of $K(\xi_{q^2})$ of relative degree greater than one over $K(\xi_q)$ will have all of its factors in G of relative degree greater than $q^{n+1} > nq$ over $K(\xi_{q^2})$. (Note that since G/K is a separable constant field extension, no prime of K ramifies in this extension.)



Now let $\mathfrak{P}_{FG}$ be an FG-prime lying above an M-prime $\mathfrak{P}_M$ of relative degree q over K. Let $\mathfrak{P}_F$, $\mathfrak{P}_G$, $\mathfrak{P}_{M(\xi_{q^2})}$, $\mathfrak{P}_{M(\xi_q)}$, $\mathfrak{P}_{K(\xi_q)}$, $\mathfrak{P}_K$ be the primes below $\mathfrak{P}_{FG}$ in the fields $F, G, M(\xi_{q^2}), M(\xi_q), K(\xi_q), K$ respectively, with $\mathfrak{P}_K$ unramified in the extension FG/K. By Lemma 4.1, we know that $\mathfrak{P}_{K(\xi_q)}$ does not split in the extension $M(\xi_q)/K(\xi_q)$. Unfortunately, $\mathfrak{P}_{K(\xi_{q^2})}$ can split in the extension $M(\xi_{q^2})/K(\xi_{q^2})$. However, by Lemma 4.2 this will happen if and only if $\mathfrak{P}_{K(\xi_q)}$ does not split in the extension $K(\xi_{q^2})/K(\xi_q)$. Thus we consider two cases below:

(a) $\mathfrak{P}_{K(\xi_q)}$ splits in the extension $K(\xi_{q^2})/K(\xi_q)$ but its factors do not split in $M(\xi_{q^2})/K(\xi_{q^2})$. Then

$$f(\mathfrak{P}_{FG}/\mathfrak{P}_M) = \frac{1}{q} f(\mathfrak{P}_{FG}/\mathfrak{P}_K) \geq \frac{1}{q} f(\mathfrak{P}_F/\mathfrak{P}_K) \geq \frac{1}{q} f(\mathfrak{P}_F/\mathfrak{P}_{M(\xi_{q^2})}) \geq n.$$

(b) $\mathfrak{P}_{K(\xi_q)}$ does not split in the extension $K(\xi_{q^2})/K(\xi_q)$. In this case consider

$$f(\mathfrak{P}_{FG}/\mathfrak{P}_M) = \frac{1}{q} f(\mathfrak{P}_{FG}/\mathfrak{P}_K) \geq \frac{1}{q} f(\mathfrak{P}_G/\mathfrak{P}_K) \geq \frac{1}{q} f(\mathfrak{P}_G/\mathfrak{P}_{K(\xi_{q^2})}) \geq n.$$

So in this case we set $L = FG$.

□

The next lemma is in part the additive analog of Lemma 5.1. The proof relies on the additive version of Hilbert's Theorem 90.

Lemma 6.2. *Let M/K be a cyclic extension of degree $p > 0$ of function fields over finite fields of constants of characteristic p. Then there exists a finite separable extension L_n of M such that every prime of M of relative degree higher than one over K and lying above a prime of K unramified in the extension L_n/K has all of its L_n factors of relative degree higher than n over M.*

Proof. First let $\delta \in M$ be such that $\mathrm{Tr}_{M/K}(\delta) \in \{1, \ldots, p-1\}$. Then

$$\mathrm{Tr}_{M/K}(\delta^p - \delta) = 0$$

and by the additive version of Hilbert's Theorem 90, we have

$$\delta^p - \delta = b - \sigma(b),$$

for some $b \in M$ and some $\sigma \in \mathrm{Gal}(M/K)$ such that $\sigma \neq \mathrm{id}$. Note further, that

$$\sigma^i(\delta^p) - \sigma^i(\delta) = \sigma^i(b) - \sigma^{i+1}(b)$$

and for $i \geq 1$ it is the case that

$$b - \sigma^i(b) = \sum_{j=0}^{i-1}(\sigma^j(b) - \sigma^{j+1}(b)) = \sum_{j=0}^{i-1}(\sigma^j(\delta^p) - \sigma^j(\delta)).$$

Next consider a field L generated over M by the roots of

$$X^p - X - b = 0. \tag{6.1}$$

Any two roots of (6.1) differ by an element of $\mathbb{F}_p$ and therefore L is Galois over M of degree at most p. Note that if β is a root of $X^p - X - b = 0$, then

$$\beta - \sum_{j=0}^{i-1}\sigma^j(\delta)$$

is a root of

$$X^p - X - \sigma^i(b) = 0.$$

Thus, L is also Galois over K. Next let $\bar{\sigma} \in \mathrm{Gal}(L/K)$ be an extension of σ to an element $\mathrm{Gal}(L/K)$ sending β to $\beta - \delta$. Then $\bar{\sigma}^p(\beta) = \beta - Tr_{M/K}(\delta) \neq \beta$. Thus, $\bar{\sigma}$ is not of order p and hence must be of order p^2. Thus L/K is cyclic of degree p^2.

Next note that M has an element whose trace is 1. Indeed, by Artin Schreier Theorem, M is generated by an element α satisfying $X^p - X - a = 0, a \in K$. Then α^{-1} satisfies, $X^p + a^{-1}X^{p-1} - a^{-1} = 0$, i.e. has K-trace equal to $-a^{-1}$. Therefore, $\frac{a}{\alpha}$ will have trace equal to -1. Thus, there exists an extension L_1 of M such that L_1/K is cyclic of degree p^2. Applying the same reasoning to the extension L_1/M we construct a cyclic extension L_2/M of degree p^2, etc. Now the the desired conclusion follows by Lemma 3.4. □

The last lemma of this section will demonstrate that the inseparable extensions are irrelevant for our purposes.

Lemma 6.3. *Let M/K be a totally inseparable finite extension of function fields over finite fields of constants. Then all but possibly finitely many primes of K have all their M-factors of relative degree 1.*

Proof. It is sufficient to consider the case of $M = K(t^{1/p})$ for $t \in K$. Without loss of generality, we can assume that t is not a p-th power in K and therefore the extension $K/C_K(t)$, where C_K is the constant field of K, is separable. Since in $C_K(t)$ every prime corresponds to an irreducible polynomial in t or $1/t$, it is easy to see that in the extension $C_K(t^{1/p})/C_K(t)$ all the primes will be ramified with ramification degree p. Further, the extension $K(t^{1/p})/C_K(t^{1/p})$ is separable (since it will be generated by the same element as the extension $K/C_K(t)$ and therefore only finitely many primes can ramify in this extension.

If $\mathfrak{P}_{C_K(t^{1/p})}$ is a $C_K(t^{1/p})$-prime without ramified factors in $K(t^{1/p})$, then a $K(t^{1/p})$-prime $\mathfrak{P}_{K(t^{1/p})}$ above $\mathfrak{P}_{C_K(t^{1/p})}$ has the same ramification degree over K as $\mathfrak{P}_{C_K(t^{1/p})}$ does over $C_K(t)$. Therefore this ramification degree is equal to the degree of extension. Thus, by Theorem 1, page 52 of [2], all but finitely many primes have relative degree 1 in the extension M/K. □

7. Extending Rational Separability Up.

In this section we use the results from the earlier sections to prove the main theorems. As was promised in the proof overview, the first proposition of this section reduces the case of an arbitrary Galois extension of global fields to the case of a cyclic extension of prime degree.

Proposition 7.1. *Let E/F be a Galois extension of global fields. Let $n \in \mathbb{Z}_{>0}$. Let $E_1, \ldots, E_m$ be all the subextensions of E such that $F \subset E_i$ and $p_i = [E : E_i]$ is a prime number. For each $i = 1, \ldots, m$, let L_i be an extension of E such that all E-primes $\mathfrak{P}_E$ lying above any E_i-prime $\mathfrak{P}_{E_i}$ not splitting in the extension E/E_i and unramified in the extension L_i/E_i, have all of their L_i-factors of relative degree higher than n over E. Let $L = \prod_{i=1}^m L_i$. Let $\mathfrak{P}_E$ be an E-prime lying above a F-prime $\mathfrak{P}_F$ unramified in the extension L/F and with $f(\mathfrak{P}_E/\mathfrak{P}_F) > 1$. Then, $\mathfrak{P}_E$ will have all of its L-factors of relative degree higher than n over E.*

Proof. Let $\mathfrak{P}_E$ be an E-prime lying above an F-prime $\mathfrak{P}_F$ with $f = f(\mathfrak{P}_E/\mathfrak{P}_F) > 1$. Let $\sigma \in \mathrm{Gal}(E/F)$ be the Frobenius automorphism of $\mathfrak{P}_E$. Then $\sigma \neq \mathrm{id}$. Let E^σ be the fixed field of σ and let $\mathfrak{P}_{E^\sigma}$ be the prime below $\mathfrak{P}_E$ in E^σ. Then $\mathfrak{P}_{E^\sigma}$ does not split in the extension E/E^σ. Further for any $k \in \mathbb{N}$, the prime above $\mathfrak{P}_{E^\sigma}$ in E^{σ^k} does not split in the extension E/E^{σ^k}. Let $\prod_{i=1}^s q_i^{a_i}$, where $q_1, \ldots, q_s$ are prime integers, be the order of σ in $\mathrm{Gal}(M/K)$. Let $k = q_1^{a_1 - 1} \prod_{i=2}^s q_i^{a_i}$. Then σ^k has order q_1 and E^{σ^k} must be one of $E_1, \ldots, E_m$. Thus $\mathfrak{P}_E$ lies above a prime of some E_i not splitting in the extension E/E_i. Therefore, all the factors of $\mathfrak{P}_E$ in L_i and consequently in L will be of relative degree greater than n over E. □

The purpose of the next lemma is to demonstrate the necessity of the weak real embeddings condition.

Lemma 7.2. *Let M/K be a number field Galois extension not satisfying the weak real embeddings condition. Then for any extension L of M, infinitely many primes of M of relative*

degree higher than 1 over K will split completely in the extension L/M. These primes will be the primes whose Frobenius automorphism (under some embedding of M into $\mathbb{C}$) is the complex conjugation.

Proof. First of all, it is enough to show that the lemma holds for a field L such that L/K is Galois. Secondly, by replacing L and M by $\sigma(L)$ and $\sigma(M)$ if necessary for some embedding $\sigma : L \longrightarrow \widetilde{\mathbb{Q}}$, without loss of generality we can assume that some subextension M_1 of M of degree 2 is a subset of $\mathbb{R}$ while $M \not\subset \mathbb{R}$. (This of course implies that $K \subset \mathbb{R}$.) Let $\sigma \in \mathrm{Gal}(M/M_1), \sigma \neq \mathrm{id}$. Then σ must be complex conjugation. Let $\mathscr{V}_M$ be the set of all M-primes whose Frobenius automorphism over K is σ. This set is infinite. Note that $\mathrm{Gal}(L/K)$ will also contain complex conjugation which will be of order two in that group. ($\mathrm{Gal}(L/K)$ contains complex conjugation because every element of L satisfies a real coefficient polynomial over K, and therefore L is closed under the complex conjugation which keeps $K \subset \mathbb{R}$ fixed.) Thus by Corollary 3.2 all elements of $\mathscr{V}_M$ will split completely in the extension L/M. □

We are now ready to state and prove the main theorems of the paper. The first result follows immediately from Propositions 7.1, 4.6, and 5.12.

Theorem 7.3. *Let M/K be a Galois extension of number fields satisfying the weak real embeddings condition. Then for any n there exists an extension L of M such that all but finitely many M-primes of relative degree higher than 1 over K will have all of their L-factors of relative degree higher than n over M.*

We now use the arbitrarily high relative degrees from the previous theorem to show that maximal separable sets can remain separable in the extensions.

Theorem 7.4. *Let K be a number field. Let $\mathscr{W}_K$ be a maximal K-separable set. Then $\mathscr{W}_K$ is separable if and only if the corresponding Galois extension M/K satisfies the weak real embeddings condition.*

Proof. Let M/K be the Galois extension corresponding to $\mathscr{W}_K$. First assume that the extension M/K satisfies the weak real embeddings condition. Next let F/K be any finite extension of K. Let $\mathscr{W}_F$ be the set of all the F-primes lying above the primes of $\mathscr{W}_K$. Let $L \supset M \supset K$ be a finite extension such that all the primes of L lying above all but finitely many primes of $\mathscr{W}_K$, are of relative degree $n > [F : K]$ over K. Such an extension L exists by Theorem 7.3. Then consider the extension FL/F. Let $\mathfrak{P}_F$ lie above $\mathfrak{P}_K \in \mathscr{W}_K$ with all of its L factors of relative degree n over K, and let $\mathfrak{P}_{FL}$ be an FL-prime above $\mathfrak{P}_F$. Finally, let $\mathfrak{P}_L$ be the L-prime below $\mathfrak{P}_{FL}$. Then

$$f(\mathfrak{P}_{FL}/\mathfrak{P}_F) = \frac{f(\mathfrak{P}_{FL}/\mathfrak{P}_K)}{f(\mathfrak{P}_F/\mathfrak{P}_K)} \geq \frac{f(\mathfrak{P}_L/\mathfrak{P}_K)}{[F : K]} > 1,$$

by construction of L.

The case of M/K not satisfying the weak real embeddings condition follows from Lemma 7.2. In other words, $\mathscr{W}_M$ – the set of all M-primes above the primes of $\mathscr{W}_K$ is *not* M-separable. □

We now proceed to examine extensions which are not necessarily Galois and sets of primes not splitting completely in these extensions.

Theorem 7.5. *Let M/K be a finite extension (not necessarily Galois) of number fields such that in the extension M^G/K, where M^G is the Galois closure of M over K, subextensions of degree 2, $M^G/M_i, i = 1, \ldots, k$ are all the subextensions of degree 2 which do not satisfy the real embeddings condition. Let $\mathscr{W}_K$ be the set of all K-primes without relative degree 1 one factors in M. Let $G = Gal(M^G/K)$. Then $\mathscr{W}_K$ is separable if and only if*

$$\forall i = 1, \ldots, k, \text{ we have that } \sigma_i \in \bigcup_{\tau \in G} \tau\, Gal(M^G/M)\tau^{-1}, \tag{7.2}$$

for all σ_i – generators of $Gal(M/M_i)$.

Proof. Suppose Condition (7.2) is satisfied. Then if $\mathfrak{P}_{M^G}$ is a prime whose Frobenius automorphism is σ_i for some i, then by Proposition 2.8, page 101 of [4], we have that $\mathfrak{P}_K$ – the prime below $\mathfrak{P}_{M^G}$ in K, has a relative degree one factor in M and thus is not in $\mathscr{W}_K$. (This is so because $\mathrm{Gal}(M^G/M)\tau^{-1} = \mathrm{Gal}(M^G/M)\tau^{-1}\sigma_i$.) Let $N_i, i = 1, \ldots, r$ be all the cyclic subextensions of M^G of prime degree and containing M but not generated by σ_i for any i. Then every M-prime lying above a prime of $\mathscr{W}_K$ will have all of its M^G factors lie above a non-splitting prime of some N_i. Given $n \in \mathbb{Z}_{>0}$, by Propositions 4.6, and 5.12, as in Theorem 7.3, we can construct an extension L of M^G such that all but finitely many primes of M^G of relative degree greater than 1 over some N_i will have all of their L-factors of relative degree greater than n over M^G. Thus, as in Theorem 7.4 we can conclude that $\mathscr{W}_K$ is separable.

Suppose now that Condition (7.2) does not hold. Then for some σ_i, we have that

$$\sigma_i \notin \bigcup_{\tau \in G} \tau \mathrm{Gal}(M^G/M)\tau^{-1}.$$

Therefore, for any $\tau \in \mathrm{Gal}(M^G/K)$, it is that case

$$\mathrm{Gal}(M^G/M)\tau\sigma_i \neq \mathrm{Gal}(M^G/M)\tau.$$

Thus, by Proposition 2.8, page 101 of [4], for all M^G-primes $\mathfrak{P}_{M^G}$ with Frobenius automorphism equal to σ_i, the K-prime $\mathfrak{P}_K$ below $\mathfrak{P}_{M^G}$ will not have any relative degree one factors in M and therefore will be in $\mathscr{W}_K$. However, as in the proof of Lemma 7.2, in any extension L of M such that L/K is Galois, infinitely many primes of M^G with Frobenius automorphism equal to σ_i will split completely. □

We now turn our attention to the function fields.

Theorem 7.6. *Let K be a function field over a finite field of constants. Let $\mathscr{W}_K$ be a set of K-separable primes. Then $\mathscr{W}_K$ is a separable set of primes.*

Proof. Let M/K be a finite extension of K where all but finitely many primes of $\mathscr{W}_K$ do not have relative degree one factors. Then by Lemma 6.3, there exists a non-trivial extension M_s of K such that M_s/K is separable, M/M_s is completely inseparable and all but finitely many primes of $\mathscr{W}_K$, do not have relative degree one factors in M_s. Let M^G be the Galois closure of M_s over K. Then all but finitely many primes of K do not have relative degree

one factors in the extension M^G/K. Now the result follows by Proposition 6.1, Lemma 6.2 and Proposition 7.1. □

Some of the results described above can be restated in the following form.

Theorem 7.7. *Let M/K be a Galois extension of number fields satisfying the weak real embeddings condition or a Galois extension of function fields over a finite fields of constants. Then there exists a Galois extension L of M such that the extension L/K is Galois and has the following property. If $\sigma \in Gal(M/K)$ is of order*

$$n = \prod p_i^{a_i},$$

where all p_i's are distinct, then any $\bar{\sigma} \in Gal(L/K)$ extending σ will have order

$$\bar{n} = \prod p_i^{b_i} q_j^{c_j},$$

where $b_i > a_i$, $p_i \neq q_j$.

Proof. Let L be such that all but finitely many primes of M of relative degree greater than 1 over K have all of their L-factors of relative degree greater than 1 over M, and L/K is Galois. It is clear, by definition of an extension, that $b_i \geq a_i$. Thus what we have to show is that the strict inequality holds. Suppose for some p_i we have that $b_i = a_i$. Let $\bar{\tau} = \bar{\sigma}^{\bar{n}/p_i^{b_i}}, \tau = \sigma^{\bar{n}/p_i^{b_i}}$. Then $\bar{\tau}$ is an extension of τ. Further the order $\bar{\tau} = p_i^{b_i}$ and so is the order of τ. By Corollary 3.2 this would contradict our assumption on factors of M-primes of relative degree higher than one over K. □

References

[1] Emil Artin. *Algebraic Numbers and Algebraic Functions*. Gordon Breach Science Publishers, New York, 1986.

[2] Claude Chevalley. *Introduction to the theory of Algebraic Functions of One Variable*, volume 6 of *Mathematical Surveys*. AMS, Providence, RI, 1951.

[3] Michael D. Fried and Moshe Jarden. *Field arithmetic*, volume 11 of *Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics]*. Springer-Verlag, Berlin, second edition, 2005.

[4] Gerald Janusz. *Algebraic Number Fields*. Academic Press, New York, 1973.

[5] Carl Jockusch and Alexandra Shlapentokh. Weak presentations of computable fields. *Journal of Symbolic Logic*, 60:199–208, 1995.

[6] Serge Lang. *Algebraic Number Theory*. Addison Wesley, Reading, MA, 1970.

[7] Serge Lang. *Algebra*. Addison Wesley, Reading, MA, 1971.

[8] H. N. Shapiro. *Introduction to the Theory of Numbers*. John Wiley and Sons, New York, 1983.

[9] Alexandra Shlapentokh. Non-standard extensions of weak presentations. *Journal of Algebra*, 176:735–749, 1995.

[10] Alexandra Shlapentokh. Algebraic and Turing separability of rings. *Journal of Algebra*, 185:229–257, 1996.

[11] Alexandra Shlapentokh. Rational separability over global fields. *Annals of Pure and Applied Logic*, 79:93–108, 1996.

[12] Alexandra Shlapentokh. Diophantine definability over some rings of algebraic numbers with infinite number of primes allowed in the denominator. *Inventiones Mathematicae*, 129:489–507, 1997.

[13] Alexandra Shlapentokh. Diophantine definability over holomorphy rings of algebraic function fields with infinite number of primes allowed as poles. *International Journal of Mathematics*, 9(8):1041–1066, 1998.

[14] Alexandra Shlapentokh. Defining integrality at prime sets of high density in number fields. *Duke Mathematical Journal*, 101(1):117–134, 2000.
[15] Alexandra Shlapentokh. Defining integrality at prime sets of high density over function fields. *Monatshefte fuer Mathematik*, 135:59–67, 2002.
[16] Alexandra Shlapentokh. Diophantine definability and decidability in the extensions of degree 2 of totally real fields. *Journal of Algebra*, 313(2):846–896, 2007.

Department of Mathematics, East Carolina University,Greenville, NC 27858
E-mail address: shlapentokha@.ecu.edu
URL: www.personal.ecu.edu/shlapentokha