The Monogeneity of Radical Extensions

HANSON SMITH

Abstract. Let L be a number field. We give necessary and sufficient conditions for a radical extension $L(\sqrt[n]{\alpha})$ to be monogenic over L with $\sqrt[n]{\alpha}$ as a generator, i.e., for $\sqrt[n]{\alpha}$ to generate a power $\mathcal{O}_L$-basis for the ring of integers $\mathcal{O}_{L(\sqrt[n]{\alpha})}$. We also give sufficient conditions for a Kummer extension of the form $\mathbb{Q}(\zeta_n, \sqrt[n]{\alpha})$ to be non-monogenic over $\mathbb{Q}$ and establish a general criterion relating ramification and relative monogeneity. Using this criterion, we find a necessary and sufficient condition for a relative cyclotomic extension of degree $\phi(n)$ to have ζ_n as a monogenic generator.

1. Results and Previous Work

Let L be a number field. We will always denote the ring of integers by $\mathcal{O}_L$. Suppose M is a finite extension of L. If $\mathcal{O}_M = \mathcal{O}_L[\theta]$ for an algebraic integer $\theta \in M$, then we say M *is monogenic over* L or $\mathcal{O}_M$ has a *power* $\mathcal{O}_L$*-basis.* We note that in general $\mathcal{O}_M$ may not be free over $\mathcal{O}_L$; however, monogeneity[1] implies freeness. When L is $\mathbb{Q}$ we will simply say M is *monogenic* or $\mathcal{O}_M$ has a *power integral basis.*

Suppose for the moment that L is a number field containing a primitive n^{th} root of unity, ζ_n. A *Kummer extension of degree* n is an extension of the form $L(\sqrt[n]{\alpha})$, where $x^n - \alpha$ is irreducible over L. The Kummer extensions of L of degree n are exactly the cyclic extensions of L of order n. When $L = \mathbb{Q}(\zeta_n)$, a Kummer extension will be denoted by K. If L is an arbitrary number field (not necessarily containing the n^{th} roots of unity), we call an extension of the form $L(\sqrt[n]{\alpha})$ a *radical extension*[2]. Letting L again be arbitrary, when $n = 2k$ with k odd, one has $L(\zeta_n) = L(\zeta_k)$. For this reason, when we speak of the n^{th} cyclotomic field or an n^{th} root of unity, it is often assumed that $n \not\equiv 2 \bmod 4$. Context will make our intent clear.

The main result of this paper is Theorem 6.1, where we describe necessary and sufficient conditions for the ring of integers of the radical extension $L(\sqrt[n]{\alpha})$ to have a power $\mathcal{O}_L$-basis generated by $\sqrt[n]{\alpha}$. This result can be illustrated by the important special case of Kummer extensions, which we state below for n an odd prime. In our investigation of Kummer

2020 *Mathematics Subject Classification.* 11R04, 11R18, 11R20.

Key words and phrases. Monogenic, Power integral basis, Relative integral basis, Kummer extension, Radical extension.

[1]'Monogenicity' would be more correct, but we employ 'monogeneity' because it is more common in the literature.

[2]Radical number fields are also known as 'pure.'

extensions, we also obtain sufficient conditions for when K is not monogenic over $\mathbb{Q}$; this is stated below as well.

$$\begin{array}{c} K := \mathbb{Q}(\zeta_n)(\sqrt[n]{\alpha}) \\ \Big| \\ \mathbb{Z}/n\mathbb{Z} \\ \Big| \\ \mathbb{Q}(\zeta_n) \\ \Big| \\ (\mathbb{Z}/n\mathbb{Z})^* \\ \Big| \\ \mathbb{Q} \end{array}$$

FIGURE 1. Kummer extensions we consider

Theorem 1.1. *Let p be an odd, rational prime, and note $(1-\zeta_p)$ is the unique prime ideal of $\mathbb{Z}[\zeta_p]$ above p. Let $\alpha \in \mathbb{Z}[\zeta_p]$ and suppose that $x^p - \alpha$ is irreducible in $\mathbb{Z}[\zeta_p][x]$. The ring of integers $\mathcal{O}_{\mathbb{Q}(\zeta_p, \sqrt[p]{\alpha})}$ is $\mathbb{Z}[\zeta_p][\sqrt[p]{\alpha}]$ if and only if (α) is a square-free ideal[3] of $\mathbb{Z}[\zeta_p]$ and the congruence*

$$\alpha^p \equiv \alpha \bmod (1-\zeta_p)^2 \tag{1.1}$$

is not satisfied.

Theorem 1.2. *Suppose there exists a rational prime l such that $l \equiv 1 \bmod n$ and $l < n \cdot \phi(n)$. Let $\alpha \in \mathbb{Z}[\zeta_n]$ be relatively prime to l. Suppose further that α is an n^{th} power residue modulo some prime of $\mathbb{Z}[\zeta_n]$ above l and that $x^n - \alpha$ is irreducible in $\mathbb{Z}[\zeta_n][x]$. Then $K = \mathbb{Q}(\zeta_n, \sqrt[n]{\alpha})$ is not monogenic over $\mathbb{Q}$. Moreover, l is a common index divisor, i.e., l divides $[\mathcal{O}_K : \mathbb{Z}[\theta]]$ for every integer θ such that $\mathbb{Q}(\theta) = K$.*

Theorem 1.1 stands in marked contrast to the situation over $\mathbb{Q}$. Gras [25] shows that the only monogenic abelian extensions of $\mathbb{Q}$ of prime degree ≥ 5 are maximal real subfields of cyclotomic fields. In order to obtain a single monogenic abelian extension of prime degree $p \geq 5$, we must have $p = \frac{\phi(n)}{2}$, where ϕ is Euler's phi function. Over $\mathbb{Q}(\zeta_p)$, however, we are able to construct infinitely many monogenic abelian extensions of prime degree p.

In addition to the theorems mentioned above, we give a more general criterion relating ramification to relative monogeneity, Proposition 3.1. The proof of Proposition 3.1 serves to highlight our methods. This proposition is then applied to prove Corollary 3.2: For an arbitrary number field L in which the n^{th} cyclotomic polynomial is irreducible, the ring of integers $\mathcal{O}_{L(\zeta_n)} = \mathcal{O}_L[\zeta_n]$ if and only if $\gcd(n, \Delta_L) = 1$. We use the classical strategy of Dedekind to prove Theorem 1.2, while our other results are established using a generalization, by Kumar and Khanduja, of Dedekind's index criterion to relative extensions (Theorem 2.5).

[3]Note that the unit ideal is square-free.

The outline of the paper is as follows. At the end of this section we will briefly survey the literature regarding the monogeneity of abelian extensions, relative monogeneity, and the monogeneity of radical extensions. Section 2 recalls the necessary tools that we will use. With Section 3, we state and prove our proposition relating relative monogeneity and ramification. Section 4 is concerned with the proof of Theorem 1.1. This section also serves to illustrate how we will approach the proof of Theorem 6.1. In Section 5, we prove Theorem 1.2. Finally, Section 6 states and establishes our main result on the monogeneity of radical extensions.

The literature regarding monogenic fields is extensive: For a nice treatise on monogeneity that focuses on using index form equations, see Gaál's book [14]. With the inclusion of numerous references, this book is likely the most modern and thorough survey of the subject. For another bibliography of monogeneity, see Narkiewicz's text [40, pages 79-81]. Narkiewicz also considers monogeneity in [41]. Though unpublished and written as a final paper for a number theory course taught by William Stein, Zhang's brief survey [51] is a nice overview.

Investigations into the monogeneity of abelian number fields are classical. For example, the monogeneity of quadratic fields is immediate and the monogeneity of cyclotomic fields was established very early. As mentioned above, Gras [25] has shown that, with the exception of the maximal real subfields of cyclotomic fields, abelian extensions of $\mathbb{Q}$ of prime degree greater than or equal to 5 are not monogenic. Generally, Gras [24] has shown that almost all abelian extensions of $\mathbb{Q}$ with degree coprime to 6 are not monogenic. The extensions of $\mathbb{Q}$ we show are non-monogenic in this paper generally have degree divisible by 2. Previous to Gras, Payan [42] found necessary conditions for monogeneity of certain cyclic extensions. Cougnard [7] builds on the ideas of Payan and establishes more stringent conditions for an imaginary quadratic field to have a monogenic cyclic extension of prime degree. Ichimura [31] establishes the equivalence of a certain unramified Kummer extension being monogenic over its base field and the Kummer extension being given by the p^{th} root of a unit of a specified shape. Khan, Katayama, Nakahara, and Uehara [35] study the monogeneity of the compositum of a cyclotomic field, with odd conductor $n \geq 3$ or even conductor $n \geq 8$ with $4 \mid n$, and a totally real number field, distinct from $\mathbb{Q}$ and with discriminant coprime to the discriminant of the cyclotomic field. They show that no such compositum is monogenic. The monogeneity of the compositum of a real abelian field and an imaginary quadratic field is studied by Motoda, Nakahara, and Shah [39]. When the conductors are relatively prime and the imaginary quadratic field is not $\mathbb{Q}(i)$, they establish that monogeneity is not possible. Shah and Nakahara [44] show the monogeneity of certain imaginary index 2 subfields of cyclotomic fields. They also prove a criterion for non-monogeneity in Galois extensions based on the ramification and inertia of a small prime. Jung, Koo, and Shin [34] use Weierstrass units to build relative monogenic generators for the composita of certain ray class fields of imaginary quadratic fields. Motoda and Nakahara [38] show that if the Galois

group of L is elementary 2-abelian and L has degree ≥ 16, then L is not monogenic over $\mathbb{Q}$. They also establish partial results in the case that $[L : \mathbb{Q}] = 8$. Chang [4] completely describes the monogeneity of the Kummer extension K when $[K : \mathbb{Q}] = 6$. Gaál and Remete [19] investigate $[K : \mathbb{Q}] = 8$. Though we do not outline it further here, there is a wealth of literature on monogenic abelian extensions of a fixed degree. The interested reader should consult the surveys mentioned earlier.

Gaál, Remete, and Szabó [21] study the relation between absolute monogeneity, i.e. monogeneity over $\mathbb{Q}$, and relative monogeneity. Suppose L is a number field, $\mathcal{O}_L = \mathbb{Z}[\theta]$, and R is an order of a subfield of L. They establish that θ can always be used to construct a power R-integral basis for $\mathcal{O}_L$. Relative power integral bases are also studied in [13], [15], [16], [20], and [22].

Radical extensions are also a classical object of study. In 1910, Westlund [49] computed the discriminant and an integral basis for the radical extensions $\mathbb{Q}\left(\sqrt[p]{\alpha}\right)$ over $\mathbb{Q}$, where $\alpha \in \mathbb{Z}$ and p is a prime. Westlund also identified when $\sqrt[p]{\alpha}$ yields a power integral basis for $\mathbb{Q}\left(\sqrt[p]{\alpha}\right)$. Using Dedekind's index criterion (Theorem 2.4) and the Montes algorithm, Gassert [23] gives necessary and sufficient conditions for the ring of integers of $\mathbb{Q}\left(\sqrt[n]{\alpha}\right)$ to be $\mathbb{Z}\left[\sqrt[n]{\alpha}\right]$. Having $\sqrt[n]{\alpha}$ generate a power integral basis is dependent on the congruence

$$\alpha^p \equiv \alpha \bmod p^2, \tag{1.2}$$

where p divides n. Loosely speaking, non-zero solutions to Congruence (1.2) are obstructions to $\sqrt[n]{\alpha}$ generating a power integral basis. A prime p for which Congruence (1.2) has a solution is called a *Wieferich prime*[4] *to the base* α. See Conrad's expository note [6] for background on $\mathbb{Z}$-power bases of radical extensions and the history of Wieferich primes.

The monogeneity of radical extensions of a given degree has been studied extensively. The radical quartic case is investigated by Funakura, who finds infinitely many monogenic fields [12]. Gaál and Remete [17], characterize the only power integral bases of a number of infinite families of radical quartic fields using binomial Thue equations and extensive calculations on a supercomputer. In [1] and [2] degree six is studied. Degree eight is considered in [28] and [29]. Degree equal to a power of 2 is also studied in [29]. For degree n with $3 \leq n \leq 9$, Gaál and Remete [18] establish a periodic characterization of integral bases. Very recently this was generalized in [32].

One can also ask about the extent to which monogeneity can fail. First a few definitions: A quantity related to monogeneity is the field index. The *field index* is defined to be the pairwise greatest common divisor $\gcd_{\alpha \in \mathcal{O}_K} [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Note that K can have field index 1 and still not be monogenic; see Example 2.3. Define the *minimal index* to be $\min_{\alpha \in \mathcal{O}_K} [\mathcal{O}_K : \mathbb{Z}[\alpha]]$. Monogeneity is equivalent to having minimal index equal to 1. An early result of Hall [27] shows that there exist cubic fields with arbitrarily large minimal indices. In [46], this is

[4]Wieferich [50] studied these primes, with $\alpha = 2$, in relation to Fermat's Last Theorem.

generalized to show that every cube-free integer occurs as the minimal index of infinitely many radical cubic fields. Monogeneity is equivalent to requiring exactly one ring generator; Pleasants [43] shows that the number of generators needed for the ring of integers of a number field of degree n is less than $\ln(n)/\ln(2)+1$, and, if 2 splits completely, the minimal number of generators is $\lfloor \ln(n)/\ln(2)+1 \rfloor$.

2. Background and Necessary Lemmas

Notation: An overline always denotes reduction modulo a prime. Discriminants will be denoted by Δ, often decorated with a subscript to indicate the object whose discriminant we are considering. A subscript is also used to indicate localization. For example, $(\mathcal{O}_L)_{\mathfrak{p}}$ is $\mathcal{O}_L$ with every element not in the prime ideal $\mathfrak{p}$ inverted. A choice of uniformizer, i.e., a generator of the maximal ideal of the local ring we are considering, is indicated by π with the ideal of localization in the subscript. In the aforementioned context, $\pi_{\mathfrak{p}}$ denotes our choice of generator for $\mathfrak{p} \subset (\mathcal{O}_L)_{\mathfrak{p}}$. The valuation associated with a prime ideal $\mathfrak{p}$ is denoted by $v_{\mathfrak{p}}$; here we normalize so that $v_{\mathfrak{p}}(\pi_{\mathfrak{p}}) = 1$.

We start with some ideas of Dedekind based on work of Kummer. The following is often called Dedekind's criterion and first appeared in [8]. Since we have two criteria due to Dedekind, we will call the following Dedekind's criterion for splitting.

Theorem 2.1 (Dedekind's criterion for splitting)**.** *Let $f(x) \in \mathbb{Z}[x]$ be monic and irreducible, let θ be a root, and let $L = \mathbb{Q}(\theta)$ be the number field generated by θ. If $p \in \mathbb{Z}$ is a prime that does not divide $[\mathcal{O}_L : \mathbb{Z}[\theta]]$, then the factorization of p in $\mathcal{O}_L$ mirrors the factorization of $f(x)$ modulo p. That is, if*

$$f(x) \equiv \varphi_1(x)^{e_1} \cdots \varphi_r(x)^{e_r} \bmod p$$

is a factorization of $\overline{f(x)}$ into irreducibles in $\mathbb{F}_p[x]$, then p factors into primes in $\mathcal{O}_L$ as

$$p = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_r^{e_r}.$$

Moreover, the residue class degree of $\mathfrak{p}_i$ is equal to the degree of φ_i.

An expository proof can be found in many algebraic number theory texts. For example, see [40, Proposition 4.33]. We note there is a natural generalization to relative extensions of number fields. See [33, Chapter I, Theorem 7.4].

Using this criterion, Dedekind was the first to demonstrate a number field that was not monogenic. Dedekind considered the cubic field generated by a root of $x^3 - x^2 - 2x - 8$. He showed that the prime 2 splits completely. If there were a possible power integral basis, then one would be able to find a cubic polynomial, generating the same number field, that splits completely into distinct linear factors modulo 2. Since there are only two distinct linear polynomials in $\mathbb{F}_2[x]$, this is impossible. Hence the number field cannot be monogenic. More generally, if a prime $p < n$ splits completely in an extension $L/\mathbb{Q}$ of degree n, then L is not

monogenic. We will use the same strategy as Dedekind to construct non-monogenic fields. Hensel [30] built on these ideas to show the following.

Theorem 2.2. *Fix a prime p. The prime p divides $[\mathcal{O}_L : \mathbb{Z}[\theta]]$ for every algebraic integer θ generating L over $\mathbb{Q}$ if and only if there is an integer f such that the number of prime ideal factors of $p\mathcal{O}_L$ with inertia degree f is greater than the number of monic irreducibles of degree f in $\mathbb{F}_p[x]$.*

Any p satisfying Theorem 2.2 is called a *common index divisor*[5]. It turns out that common index divisors are not the only obstruction to monogeneity:

Example 2.3. [40, Chapter 2.2.6] Consider the number field given by $L = \mathbb{Q}\left(\sqrt[3]{7 \cdot 5^2}\right) = \mathbb{Q}\left(\sqrt[3]{5 \cdot 7^2}\right)$. The elements $\left\{1, \sqrt[3]{7 \cdot 5^2}, \sqrt[3]{7^2 \cdot 5}\right\}$ form an integral basis of L. For any fixed prime p, one can find $\theta \in \mathcal{O}_L$ such that $[\mathcal{O}_L : \mathbb{Z}[\theta]]$ is not divisible by p; however, L is not monogenic.

We will use another criterion of Dedekind, which we will call Dedekind's index criterion, to establish monogeneity. First, we state the version Dedekind proved, with $\mathbb{Q}$ as the base field.

Theorem 2.4 (Dedekind's index criterion)**.** *Let $f(x)$ be a monic, irreducible polynomial in $\mathbb{Z}[x]$, θ a root of f, and $L = \mathbb{Q}(\theta)$. If p is a rational prime, we have*

$$f(x) \equiv \prod_{i=1}^{r} f_i(x)^{e_i} \bmod p,$$

where the $f_i(x)$ are monic lifts of the irreducible factors of $\overline{f(x)}$ to $\mathbb{Z}[x]$. Define

$$d(x) := \frac{f(x) - \prod_{i=1}^{r} f_i(x)^{e_i}}{p}.$$

Then p divides $[\mathcal{O}_L : \mathbb{Z}[\theta]]$ if and only if $\gcd\left(\overline{f_i(x)}^{e_i - 1}, \overline{d(x)}\right) \neq 1$ for some i, where we are taking the greatest common divisor in $\mathbb{F}_p[x]$.

Recently, Kumar and Khanduja, using completely different methods from those of Dedekind, have proved a generalization of Dedekind's index criterion to relative extensions. This generalization will be very useful to us.

Theorem 2.5. *[36, Theorem 1.1] Let R be a Dedekind domain with quotient field L, and let $f(x)$ be a monic, irreducible polynomial in $R[x]$ with θ a root. Define $M = L(\theta)$, and suppose $\mathfrak{p}$ is a prime of R. We have*

$$f(x) \equiv \prod_{i=1}^{r} f_i(x)^{e_i} \bmod \mathfrak{p},$$

[5]The terms 'essential discriminant divisor' and 'inessential discriminant divisor' also appear in the literature.

where the $f_i(x)$ are monic lifts of the irreducible factors of $\overline{f(x)}$ to $R[x]$. Note the integral closure of $R_\mathfrak{p}$ in M is $(\mathcal{O}_M)_\mathfrak{p}$. Define the polynomial $d(x) \in R_\mathfrak{p}[x]$ to be

$$d(x) := \frac{f(x) - \prod_{i=1}^{r} f_i(x)^{e_i}}{\pi_\mathfrak{p}}.$$

Then $(\mathcal{O}_M)_\mathfrak{p} = R_\mathfrak{p}[\theta]$ if and only if $\overline{f_i(x)}^{e_i - 1}$ is coprime to $\overline{d(x)}$ for each i.

With Equation (2.2), we will see that the conclusion of Theorem 2.5 is exactly what we need to study $[\mathcal{O}_M : \mathcal{O}_L[\theta]]$. The interested reader should consult [48] for a nice discussion of and comparison between three different criteria for monogeneity: Dedekind's index criterion, a theorem of Uchida [47], and a theorem of Lüneburg [37]. For other, similar generalizations of Dedekind's index criterion see [5], [10], and, for the greatest generality, [9].

In addition to the work of Dedekind, we will need a few facts about cyclotomic, radical, and Kummer extensions. First, we recall the following well-known formula relating polynomial discriminants and field discriminants. Let f be a monic, irreducible polynomial of degree $n > 1$, let θ be a root, and write $L = \mathbb{Q}(\theta)$, then

$$\Delta_f = \Delta_L [\mathcal{O}_L : \mathbb{Z}[\theta]]^2. \tag{2.1}$$

Equation (2.1) admits a generalization to relative extensions. We will specialize [11, Chapter III, Equation 2.4] for our purposes. Let L be a number field, and let M be a finite extension of L generated by a root, θ, of a monic, irreducible polynomial $f(x) \in \mathcal{O}_L[x]$. As ideals, we have the equality

$$(\Delta_f) = \left(\Delta_{M/L}\right) \left([\mathcal{O}_M : \mathcal{O}_L[\theta]]\right)^2. \tag{2.2}$$

Thus, in studying monogeneity, we need only consider the prime factors of (Δ_f).

Suppose M and N are two finite extensions of a number field L. We call M and N *arithmetically disjoint* (over L) if they are linearly disjoint and, as ideals, $\gcd\left(\left(\Delta_{M/L}\right), \left(\Delta_{N/L}\right)\right) = \mathcal{O}_L$. The following is Proposition III.2.13 of [11].

Proposition 2.6. *If M and N are arithmetically disjoint over L, then $\mathcal{O}_{MN} = \mathcal{O}_M \cdot \mathcal{O}_N$ as $\mathcal{O}_L$-modules.*

Proposition 2.6 will be useful in studying the monogeneity of relative cyclotomic extensions.

Turning to cyclotomic extensions of $\mathbb{Q}$, the following is Lemma 6 of Chapter III of [3].

Lemma 2.7. *The discriminant of $\mathbb{Q}(\zeta_n)$ over $\mathbb{Q}$ is*

$$\Delta_{\mathbb{Q}(\zeta_n)/\mathbb{Q}} = n^{\phi(n)} \Big/ \prod_{p|n} p^{\frac{\phi(n)}{p-1}},$$

where ϕ denotes Euler's phi function. Further, an integral basis for $\mathcal{O}_{\mathbb{Q}(\zeta_n)}$ is given by 1 and the powers ζ_n^k with $1 \leq k \leq \phi(n) - 1$.

Lemma 2.7 and Equation (2.1) yield the following corollary.

Corollary 2.8. *The cyclotomic polynomial $\phi_n(x)$ has discriminant*

$$\Delta_{\phi_n} = n^{\phi(n)} \Big/ \prod_{p|n} p^{\frac{\phi(n)}{p-1}}.$$

It is useful to understand the splitting of primes in cyclotomic extensions.

Lemma 2.9. *[3, III.1 Lemma 4]: If p is a prime not dividing n, then it is unramified in $\mathbb{Q}(\zeta_n)$ and its residue class degree is the least positive integer f such that $p^f \equiv 1 \bmod n$.*

Bringing our attention to radical and Kummer extensions, consider the polynomial $x^n - \alpha$. One computes

$$\Delta_{x^n-\alpha} = (-1)^{\frac{n^2-n}{2}} n^n (-\alpha)^{n-1}. \tag{2.3}$$

One can also derive this by specializing Theorem 4 of [26].

The following describes splitting in Kummer extensions.

Lemma 2.10. *[3, III.2 Lemma 5]: The discriminant of $K = \mathbb{Q}(\zeta_n, \sqrt[n]{\alpha})$ over $\mathbb{Q}(\zeta_n)$ divides $n^n \alpha^{n-1}$. A prime $\mathfrak{p}$ of $\mathbb{Z}[\zeta_n]$ is unramified in K if $\mathfrak{p} \nmid n\alpha$. In this case, the residue class degree of $\mathfrak{p}$ is the least positive integer f such that $\alpha^f \equiv x^n \bmod \mathfrak{p}$ is solvable.*

3. Monogeneity and Ramification

In this section we present a proposition relating monogeneity and ramification. The result is likely classical, but we include it here to highlight our methods.

Proposition 3.1. *Let L be a number field, $h(x)$ a monic, irreducible polynomial in $\mathcal{O}_L[x]$, and η a root of $h(x)$. Suppose $\mathfrak{p}$ is a prime of L above the rational prime p such that $\mathfrak{p} \mid \Delta_h$. Let M be an extension of L such that $h(x)$ is irreducible in $\mathcal{O}_M[x]$. If $\mathfrak{p}$ is ramified in M, then $p \mid [\mathcal{O}_{M(\eta)} : \mathcal{O}_M[\eta]]$.*

The setup of Proposition 3.1 is summarized in Figure 2.

Proof. We will use Theorem 2.5 to show that p divides $\left[\mathcal{O}_{M(\eta)} : \mathcal{O}_M[\eta]\right]$. Reducing $h(x)$ modulo $\mathfrak{p}$ and choosing lifts of the irreducible factors to $\mathcal{O}_L[x]$, we have

$$h(x) \equiv h_0(x)^{e_0} h_1(x) \bmod \mathfrak{p}, \tag{3.1}$$

where $e_0 > 1$. Such an h_0 exists since $\mathfrak{p} \mid \Delta_h$.

Let $\mathfrak{p}$ be a prime of M that is ramified above $\mathfrak{p}$. Consider the element of $(\mathcal{O}_M)_{\mathfrak{p}}[x]$ given by

$$d(x) = \frac{h(x) - h_0(x)^{e_0} h_1(x)}{\pi_{\mathfrak{p}}}.$$

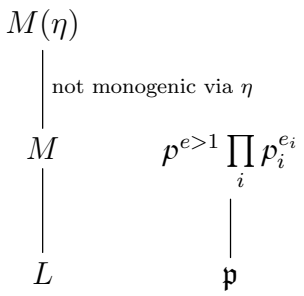

FIGURE 2. Diagram for Proposition 3.1

Let η_0 be a root of h_0 in some extension of $(\mathcal{O}_M)_p$. For η to yield a power $\mathcal{O}_M$-basis, it is necessary that $d(\eta_0) \not\equiv 0 \bmod \pi_p^2$. Equation (3.1) shows that $d(\eta_0) \equiv 0 \bmod \pi_{\mathfrak{p}}$. Since $\pi_p^2 \mid \pi_{\mathfrak{p}}$, we see $d(\eta_0) \equiv 0 \bmod \pi_p^2$ and $p \mid \left[\mathcal{O}_{M(\eta)} : \mathcal{O}_M[\eta]\right]$. □

Proposition 3.1 sheds some light on the monogeneity of cyclotomic relative extensions:

Corollary 3.2. *Let L be a number field in which the n^{th} cyclotomic polynomial is irreducible, where $n > 2$ is any integer not congruent to 2 modulo 4. Then $\mathcal{O}_L[\zeta_n] = \mathcal{O}_{L(\zeta_n)}$ if and only if $\gcd(n, \Delta_L) = 1$.*

Proof. If $\gcd(n, \Delta_L) \neq 1$, then some prime dividing n is ramified in L. Hence Proposition 3.1 shows that $\mathcal{O}_L[\zeta_n] \neq \mathcal{O}_{L(\zeta_n)}$.

Conversely, if $\gcd(n, \Delta_L) = 1$, then L and $\mathbb{Q}(\zeta_n)$ are arithmetically disjoint over $\mathbb{Q}$, and the result follows from Proposition 2.6. One can also prove this direction via a computation with Theorem 2.5. □

We can contrast the above Proposition 3.1 to the following example.

Example 3.3. Let $k, m \in \mathbb{Z}$ with $\gcd(k, m) = 1$, k and m square-free, $m \equiv 1 \bmod 4$, and $k \equiv 2, 3 \bmod 4$. One can use Theorem 2.5 to show that a $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$-basis of $\mathcal{O}_{\mathbb{Q}(\sqrt{m},\sqrt{k})}$ is given by 1 and $\sqrt{k}$. Thus, in this case, a root of a polynomial in $\mathbb{Z}[x]$ yields a power $\mathbb{Z}\left[\frac{1+\sqrt{m}}{2}\right]$-basis for $\mathcal{O}_{\mathbb{Q}(\sqrt{m},\sqrt{k})} = \mathbb{Z}\left[\frac{1+\sqrt{m}}{2}, \sqrt{k}\right]$. The interested reader should consult [45] for an in-depth study of relative integral bases of quartic fields with quadratic subfields.

4. Monogeneity of K over $\mathbb{Q}(\zeta_p)$

We wish to establish Theorem 1.1: *Let p be an odd, rational prime, and note $(1-\zeta_p)$ is the unique prime ideal of $\mathbb{Z}[\zeta_p]$ above p. Let $\alpha \in \mathbb{Z}[\zeta_p]$ and suppose that $x^p - \alpha$ is irreducible in $\mathbb{Z}[\zeta_p][x]$. The ring of integers $\mathcal{O}_{\mathbb{Q}(\zeta_p, \sqrt[p]{\alpha})}$ is $\mathbb{Z}[\zeta_p][\sqrt[p]{\alpha}]$ if and only if (α) is a square-free ideal of $\mathbb{Z}[\zeta_p]$ and the congruence*

$$\alpha^p \equiv \alpha \bmod (1-\zeta_p)^2 \tag{4.1}$$

is not satisfied.

Note that Congruence (4.1) is exactly the Wieferich congruence, Congruence (1.2), but with respect to the prime $(1-\zeta_p)$. We will see that the analogue of Congruence (1.2) in Theorem 6.1 is a bit more complicated. This is due to the potential for higher powers of a prime to divide n and the need to accommodate arbitrary residue class degrees.

Proof. Recall that $\Delta_{x^p-\alpha} = (-1)^{\frac{p^2-p}{2}} p^p(-\alpha)^{p-1}$. Equation 2.2 and the discussion afterwards show that for questions of monogeneity, we need only consider the prime divisors of $\Delta_{x^p-\alpha}$. We will contend with the prime divisors of α, then we will contend with $\mathfrak{p} := (1-\zeta_p)$. In both cases, we will use Theorem 2.5.

Suppose $\mathfrak{l}$ is a prime of $\mathbb{Z}[\zeta_p]$ dividing α. The reduction of $x^p-\alpha$ modulo $\mathfrak{l}$ is $\overline{x}^p$. Hence, in the notation of Theorem 2.5, we have

$$d(x) = \frac{x^p - \alpha - x^p}{\pi_{\mathfrak{l}}} = \frac{-\alpha}{\pi_{\mathfrak{l}}}.$$

Now $v_{\mathfrak{l}}\left(\frac{-\alpha}{\pi_{\mathfrak{l}}}\right) = 0$ if and only if $v_{\mathfrak{l}}(\alpha) = 1$. If $v_{\mathfrak{l}}(\alpha) = 1$, the reduction $\overline{\frac{-\alpha}{\pi_{\mathfrak{l}}}}$ generates the unit ideal. In particular, $\overline{\frac{-\alpha}{\pi_{\mathfrak{l}}}}$ is relatively prime to $\overline{x}^{p-1}$. Conversely, if $v_{\mathfrak{l}}(\alpha) > 1$, then $\overline{\frac{-\alpha}{\pi_{\mathfrak{l}}}} = 0$ and is not relatively prime to $\overline{x}^{p-1}$. With Theorem 2.5, we see

$$(\mathcal{O}_K)_{\mathfrak{l}} = (\mathbb{Z}[\zeta_p])_{\mathfrak{l}}\left[\sqrt[p]{\alpha}\right]$$

if and only if $v_{\mathfrak{l}}(\alpha) = 1$.

Next, we contend with $\mathfrak{p}$. We localize $\mathbb{Z}[\zeta_p]$ at $\mathfrak{p}$ and choose $1-\zeta_p$ to be the uniformizer. The reduction of $x^p-\alpha$ modulo $\mathfrak{p}$ is $(\overline{x-\alpha})^p$. We have

$$d(x) = \frac{x^p - \alpha - (x-\alpha)^p}{1-\zeta_p}.$$

Evaluating at α, we see that $\overline{d(x)}$ is relatively prime to $\overline{x-\alpha}$ if and only if

$$\alpha^p \not\equiv \alpha \bmod (1-\zeta_p)^2.$$

Applying Theorem 2.5, our result follows. Note that our argument here does not depend on whether or not $\mathfrak{p}$ divides α. □

5. Non-monogeneity of K over $\mathbb{Q}$

In this section, we will prove Theorem 1.2: *Suppose there exists a rational prime l such that $l \equiv 1 \bmod n$ and $l < n\cdot\phi(n)$. Let $\alpha \in \mathbb{Z}[\zeta_n]$ be relatively prime to l. Suppose further that α is an n^{th} power residue modulo some prime of $\mathbb{Z}[\zeta_n]$ above l and that $x^n-\alpha$ is irreducible in $\mathbb{Z}[\zeta_n][x]$. Then $K = \mathbb{Q}(\zeta_n, \sqrt[n]{\alpha})$ is not monogenic over $\mathbb{Q}$. Moreover, l is a common index divisor.*

Proof. We will use Dedekind's method for proving a number field is not monogenic. From Lemmas 2.9 and 2.10, we see that l splits completely in K. If K is monogenic over $\mathbb{Q}$, then Theorem 2.1 shows that the factorization of l in K is mirrored by the factorization

of a degree $n \cdot \phi(n)$ polynomial modulo l. Thus there is a degree $n \cdot \phi(n)$ polynomial that generates K over $\mathbb{Q}$ and factors into distinct linear factors modulo l. Since $l < n \cdot \phi(n)$, we see this is impossible. Thus K is not monogenic over $\mathbb{Q}$. Applying Theorem 2.2, we see l is in fact a common index divisor. □

Remark 5.1. If k denotes the multiplicative order of l modulo n, the number of irreducible polynomials in $\mathbb{F}_l[x]$ of degree k is $\frac{1}{k}\sum_{d|k}\mu\left(\frac{k}{d}\right)l^d$. If

$$\frac{1}{k}\sum_{d|k}\mu\left(\frac{k}{d}\right)l^d < \frac{n\cdot\phi(n)}{k}$$

and the requirements on α remain the same, then K is not monogenic over $\mathbb{Q}$ by the same methods used above. One can also obtain weakened hypotheses on α via these ideas.

Example 5.2. Consider $n = 5$ and $l = 11$. We see $11 < 5 \cdot 4$. Since $11 \equiv 1 \bmod 5$, the prime 11 splits completely in $\mathbb{Q}(\zeta_5)$. For 11 to split completely in $\mathbb{Q}\left(\zeta_5, \sqrt[5]{\alpha}\right)$, we need α to be a 5^{th} power in $\mathbb{F}_{11}$. This is satisfied by rational integers congruent to $\pm 1 \bmod 11$. Hence all rational integers $\alpha \equiv \pm 1 \bmod 11$ for which $x^5 - \alpha$ is irreducible in $\mathbb{Z}(\zeta_5)[x]$ yield non-monogenic K.

6. General Radical Extensions

In this section we consider an arbitrary number field L and an element $\alpha \in \mathcal{O}_L$ such that $x^n - \alpha$ is irreducible over L. To avoid trivialities, we assume $n \geq 2$. For a prime ideal $\mathfrak{p}$ of $\mathcal{O}_L$ dividing n, we write p for the residue characteristic and f for the residue class degree. If $\mathfrak{p}$ divides n, we factor $n = p^e m$ with $\gcd(m, p) = 1$. Let ε be congruent to e modulo f with $1 \leq \varepsilon \leq f$, and define β to be α to the power $p^{f-\varepsilon}$. By construction β is the p^e-th root of α modulo $\mathfrak{p}$. The Wieferich congruence, Congruence (1.2), generalizes to

$$\alpha^{p^{f-\varepsilon+e}} = \beta^{p^e} \equiv \alpha \bmod \mathfrak{p}^2. \tag{6.1}$$

In the case where $e \leq f$, this is simply

$$\alpha^{p^f} \equiv \alpha \bmod \mathfrak{p}^2.$$

Theorem 6.1. *The ring of integers of $L\left(\sqrt[n]{\alpha}\right)$ is $\mathcal{O}_L\left[\sqrt[n]{\alpha}\right]$ if and only if (α) is a square-free ideal of $\mathcal{O}_L$ and every prime $\mathfrak{p}$ dividing n does not satisfy Congruence (6.1).*

Proof. We need only consider the prime divisors of $\Delta_{x^n-\alpha} = (-1)^{\frac{n^2-n}{2}} n^n (-\alpha)^{n-1}$. For any primes dividing α, the argument is straightforward and essentially the same as in the proof of Theorem 1.1.

Maintaining the notation outlined above, let $\mathfrak{p}$ be a prime ideal of $\mathcal{O}_L$ dividing n, but not α. Noting $\beta^{p^e} \equiv \alpha \bmod \mathfrak{p}$, we have

$$x^n - \alpha \equiv \left(x^m - \beta\right)^{p^e} \bmod \mathfrak{p}.$$

With the notation of Theorem 2.5,

$$d(x) = \frac{x^n - \alpha - (x^m - \beta + a\pi_{\mathfrak{p}})^{p^e}}{\pi_{\mathfrak{p}}},$$

where a is some element of $(\mathcal{O}_L)_{\mathfrak{p}}$ so that the term $a\pi_{\mathfrak{p}}$ accommodates possible further factorization of $x^m - \beta$ modulo $\mathfrak{p}$.

The relative primality of $\overline{d(x)}$ and the factors of $\overline{x^m - \beta}$ does not change upon extension, so it suffices to work in $(\mathcal{O}_L)_{\mathfrak{p}}\left(\sqrt[m]{\beta}, \zeta_m\right)$ and $(\mathcal{O}_L)_{\mathfrak{p}}\left(\sqrt[m]{\beta}, \zeta_m\right)$ modulo $(\pi_{\mathfrak{p}})$. With Theorem 2.5 in mind, we wish to show that $\overline{d(x)}$ does not have $\overline{\zeta_m^k \sqrt[m]{\beta}}$ as a root for any k. Evaluating,

$$d\left(\zeta_m^k \sqrt[m]{\beta}\right) = \frac{\beta^{p^e} - \alpha - (\beta - \beta + a\pi_{\mathfrak{p}})^{p^e}}{\pi_{\mathfrak{p}}} = \frac{\beta^{p^e} - \alpha + (a\pi_{\mathfrak{p}})^{p^e}}{\pi_{\mathfrak{p}}}.$$

Clearly, $d\left(\zeta_m^k \sqrt[m]{\beta}\right) \equiv 0 \bmod \pi_{\mathfrak{p}}$ if and only if

$$\beta^{p^e} - \alpha = \alpha^{p^{f-\varepsilon+e}} - \alpha \equiv 0 \bmod \pi_{\mathfrak{p}}^2.$$

Our result follows. □

Combining the above proof with the generalization of Dedekind's criterion for splitting, [33, Chapter I, Theorem 7.4], we obtain

Corollary 6.2. *As above, suppose $x^n - \alpha \in \mathcal{O}_L[x]$ is irreducible with (α) square-free. Let $\mathfrak{p}$ be a prime ideal of L that does not divide n. Then the splitting of $\mathfrak{p}$ in $L\left(\sqrt[n]{\alpha}\right)$ is mirrored by the splitting of $\overline{x^n - \alpha}$ in $\mathcal{O}_L/\mathfrak{p}[x]$, as in Theorem 2.1. In particular, $\mathfrak{p}$ splits completely if and only if $\overline{\alpha} \neq 0$ is an n^{th} root in $\mathcal{O}_L/\mathfrak{p}$. Moreover, if Congruence (6.1) holds, we can remove the restriction that $\mathfrak{p} \nmid n$.*

Acknowledgments

The author would like to thank Sebastian Bozlee, Keith Conrad, and Katherine Stange. The author is especially grateful to Keith for the idea to look into more general radical extensions. The author would also like to thank Anuj Jakhar for pointing out a mistake in the original proof of Theorem 6.1 and the anonymous referee for the helpful and constructive comments. This research was partially supported by NSF-CAREER CNS-1652238 under the supervision of PI Dr. Katherine E. Stange.

References

[1] S. Ahmad, T. Nakahara, and A. Hameed. On certain pure sextic fields related to a problem of Hasse. *Internat. J. Algebra Comput.*, 26(3):577–583, 2016.

[2] S. Ahmad, T. Nakahara, and S. M. Husnine. Power integral bases for certain pure sextic fields. *Int. J. Number Theory*, 10(8):2257–2265, 2014.

[3] J. W. S. Cassels and A. Fröhlich, editors. *Algebraic number theory*. London Mathematical Society, London, 2010. Papers from the conference held at the University of Sussex, Brighton, September 1–17, 1965, Including a list of errata.

[4] M.-L. Chang. Non-monogeneity in a family of sextic fields. *J. Number Theory*, 97(2):252–268, 2002.

[5] M. E. Charkani and A. Deajim. Generating a power basis over a Dedekind ring. *J. Number Theory*, 132(10):2267–2276, 2012.

[6] K. Conrad. The ring of integers in a radical extension. https://kconrad.math.uconn.edu/blurbs/gradnumthy/integersradical.pdf.

[7] J. Cougnard. Conditions nécessaires de monogénéité. Application aux extensions cycliques de degré premier $l \geq 5$ d'un corps quadratique imaginaire. *J. London Math. Soc. (2)*, 37(1):73–87, 1988.

[8] R. Dedekind. Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen. *Gött. Abhandlungen*, pages 1–23, 1878.

[9] L. El Fadil, M. Boulagouaz, and A. Deajim. A Dedekind's Criterion over Valued Fields. *arXiv e-prints*, page arXiv:1908.06365, Aug. 2019.

[10] Y. L. Ershov. The Dedekind criterion for arbitrary valuation rings. *Dokl. Akad. Nauk*, 410(2):158–160, 2006.

[11] A. Fröhlich and M. J. Taylor. *Algebraic number theory*, volume 27 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1993.

[12] T. Funakura. On integral bases of pure quartic fields. *Math. J. Okayama Univ.*, 26:27–41, 1984.

[13] I. Gaál. Power integral bases in cubic relative extensions. *Experiment. Math.*, 10(1):133–139, 2001.

[14] I. Gaál. *Diophantine equations and power integral bases*. Birkhäuser/Springer, Cham, 2019. Theory and algorithms, Second edition of [MR1896601].

[15] I. Gaál and M. Pohst. Computing power integral bases in quartic relative extensions. *J. Number Theory*, 85(2):201–219, 2000.

[16] I. Gaál and L. Remete. Power integral bases in cubic and quartic extensions of real quadratic fields. to appear in *Acta Scientiarum Mathematicarum*.

[17] I. Gaál and L. Remete. Binomial thue equations and power integral bases in pure quartic fields. *JP J. Algebra Number Theory Appl.*, 32:49–61, 02 2014.

[18] I. Gaál and L. Remete. Integral bases and monogenity of pure fields. *J. Number Theory*, 173:129–146, 2017.

[19] I. Gaál and L. Remete. Non-monogenity in a family of octic fields. *Rocky Mountain J. Math.*, 47(3):817–824, 2017.

[20] I. Gaál and L. Remete. Integral bases and monogenity of composite fields. *Exp. Math.*, 28(2):209–222, 2019.

[21] I. Gaál, L. Remete, and T. Szabó. Calculating power integral bases by using relative power integral bases. *Funct. Approx. Comment. Math.*, 54(2):141–149, 2016.

[22] I. Gaál and T. Szabó. Relative power integral bases in infinite families of quartic extensions of quadratic fields. *JP J. Algebra Number Theory Appl.*, 29(1):31–43, 2013.

[23] T. A. Gassert. A note on the monogeneity of power maps. *Albanian J. Math.*, 11(1):3–12, 2017.

[24] M.-N. Gras. Condition nécessaire de monogénéité de l'anneau des entiers d'une extension abélienne de $\mathbf{Q}$. In *Séminaire de théorie des nombres, Paris 1984–85*, volume 63 of *Progr. Math.*, pages 97–107. Birkhäuser Boston, Boston, MA, 1986.

[25] M.-N. Gras. Non monogénéité de l'anneau des entiers des extensions cycliques de $\mathbf{Q}$ de degré premier $l \geq 5$. *J. Number Theory*, 23(3):347–353, 1986.

[26] G. R. Greenfield and D. Drucker. On the discriminant of a trinomial. *Linear Algebra Appl.*, 62:105–112, 1984.

[27] M. Hall. Indices in cubic fields. *Bull. Amer. Math. Soc.*, 43(2):104–108, 1937.

[28] A. Hameed and T. Nakahara. Integral bases and relative monogenity of pure octic fields. *Bull. Math. Soc. Sci. Math. Roumanie (N.S.)*, 58(106)(4):419–433, 2015.

[29] A. Hameed, T. Nakahara, S. M. Husnine, and S. Ahmad. On existence of canonical number system in certain classes of pure algebraic number fields. *J. Prime Res. Math.*, 7:19–24, 2011.

[30] K. Hensel. Arithmetische Untersuchungen über die gemeinsamen ausserwesentlichen Discriminantentheiler einer Gattung. *J. Reine Angew. Math.*, 113:128–160, 1894.

[31] H. Ichimura. On power integral bases of unramified cyclic extensions of prime degree. *J. Algebra*, 235(1):104–112, 2001.

[32] A. Jakhar, S. K. Khanduja, and N. Sangwan. On integral basis of pure number fields. *arXiv e-prints*, page arXiv:2005.01915, May 2020.

[33] G. J. Janusz. *Algebraic number fields*, volume 7 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, second edition, 1996.

[34] H. Y. Jung, J. K. Koo, and D. H. Shin. Application of Weierstrass units to relative power integral bases. *Rev. Mat. Iberoam.*, 30(4):1489–1498, 2014.

[35] N. Khan, S.-i. Katayama, T. Nakahara, and T. Uehara. Monogenity of totally real algebraic extension fields over a cyclotomic field. *J. Number Theory*, 158:348–355, 2016.

[36] M. Kumar and S. K. Khanduja. A generalization of Dedekind criterion. *Comm. Algebra*, 35(5):1479–1486, 2007.

[37] H. Lüneburg. Resultanten von Kreisteilungspolynomen. *Arch. Math. (Basel)*, 42(2):139–144, 1984.

[38] Y. Motoda and T. Nakahara. Power integral bases in algebraic number fields whose Galois groups are 2-elementary abelian. *Arch. Math. (Basel)*, 83(4):309–316, 2004.

[39] Y. Motoda, T. Nakahara, and S. I. A. Shah. On a problem of Hasse for certain imaginary abelian fields. *J. Number Theory*, 96(2):326–334, 2002.

[40] W. Narkiewicz. *Elementary and analytic theory of algebraic numbers*. Springer Monographs in Mathematics. Springer-Verlag, Berlin, third edition, 2004.

[41] W. Narkiewicz. *The story of algebraic numbers in the first half of the 20th century: From Hilbert to Tate*. Springer Monographs in Mathematics. Springer, Cham, 2018.

[42] J. J. Payan. Sur les classes ambiges et les ordres monogenes d'une extension cyclique de degré premier impair sur Q ou sur un corps quadratique imaginaire. *Ark. Mat.*, 11:239–244, 1973.

[43] P. A. B. Pleasants. The number of generators of the integers of a number field. *Mathematika*, 21:160–167, 1974.

[44] S. I. A. Shah and T. Nakahara. Monogenesis of the rings of integers in certain imaginary abelian fields. *Nagoya Math. J.*, 168:85–92, 2002.

[45] B. K. Spearman and K. S. Williams. Relative integral bases for quartic fields over quadratic subfields. *Acta Math. Hungar.*, 70(3):185–192, 1996.

[46] B. K. Spearman, Q. Yang, and J. Yoo. Minimal indices of pure cubic fields. *Arch. Math. (Basel)*, 106(1):35–40, 2016.

[47] K. Uchida. When is $Z[\alpha]$ the ring of the integers? *Osaka Math. J.*, 14(1):155–157, 1977.

[48] X. Vidaux and C. R. Videla. Dedekind's criterion for the monogenicity of a number field versus Uchida's and Lüneburg's. *arXiv e-prints*, page arXiv:1809.04122, Sept. 2018.

[49] J. Westlund. On the fundamental number of the algebraic number-field $k(\sqrt[p]{m})$. *Trans. Amer. Math. Soc.*, 11(4):388–392, 1910.

[50] A. Wieferich. Zum letzten Fermatschen Theorem. *J. Reine Angew. Math.*, 136:293–302, 1909.

[51] Y. Zhang. On power bases in number fields. *Constructed for a Harvard number theory course taught by William Stein*, March 2005. https://pdfs.semanticscholar.org/0ba0/a35b7976153f610803e19bee074b90ef37fe.pdf.

Department of Mathematics, University of Connecticut, 341 Mansfield Road U1009 Storrs, CT 06269-1009 USA

Email address: hanson.smith@uconn.edu