

A note on quadratic cyclotomic extensions

Sophie Marques¹  and Elizabeth Mrema² 

¹ Department of Mathematical Sciences, Stellenbosch University
Stellenbosch, 7600, South Africa
e-mail: smarques@sun.ac.za

² Department of Mathematics, University of Dar es Salaam
P.O. Box 35061, Tanzania
e-mail: mrema.elizabeth@udsm.ac.tz

Received: 11 March 2026

Revised: 7 October 2026

Accepted: 23 October 2026

Online First: 26 October 2026

Abstract: Schinzel’s classification of radical extensions relies on the structure of quadratic cyclotomic extensions, which also play an important role in the study of cyclotomic extensions over general fields. In this paper, we identify properties and invariants associated with quadratic cyclotomic extensions that are relevant to these classification problems. We determine the possible minimal polynomials of primitive roots of unity generating quadratic extensions, describe the prime-power levels at which such extensions occur, and assemble the prime-power information into a global classification of quadratic cyclotomic fields. The treatment applies in arbitrary characteristic, with the usual restriction that, in positive characteristic, the orders of the roots of unity considered are prime to the characteristic.

Keywords: Cyclotomic extensions, Field extensions, Roots of unity, Quadratic extensions, Radical extensions.

2020 Mathematics Subject Classification: 12F05, 12E05, 12E20, 12E10, 12F10.

1 Introduction

This work emerged from an effort to understand the classification of radical field extensions up to isomorphism. From Kummer theory, the relevant isomorphisms are described in [12, Corollary



Copyright © 2026 by the Authors. This is an Open Access paper distributed under the terms and conditions of the Creative Commons Attribution 4.0 International License (CC BY 4.0). <https://creativecommons.org/licenses/by/4.0/>

to Theorem 3] and [14, Theorem 2.1]. These results establish the existence of two isomorphism types, but do not by themselves characterize precisely when each type occurs. The distinction is linked to the occurrence of certain quadratic cyclotomic subextensions, in particular those generated by primitive 2^e -th roots of unity. Clarifying the cyclotomic information underlying this classification led to the present paper.

The problem belongs to a broader literature on quadratic and finite-rank algebraic structures. Quadratic extensions over rings are studied, for example, in [4, 6, 13], quadratic modules in [8], and moduli and discriminant descriptions of finite-rank or quadratic algebras in [2, 11, 15]. In the field-theoretic direction most closely related to the present work, structural questions for radical extensions and their subfields are considered in [1, 5, 10, 12, 14], while degrees of cyclotomic extensions over general base fields are studied in [16]; see also the expository account [3].

Throughout the paper, if $\text{char}(F) = r > 0$, we consider only roots of unity whose order is prime to r . Equivalently, every p -primary assertion concerns primes $p \neq r$. This convention allows the characteristic-zero and positive-characteristic cases to be treated in parallel.

A significant part of the paper is devoted to primitive p^e -th roots of unity ζ_{p^e} that generate quadratic cyclotomic extensions. For odd primes p , the situation is rigid: whenever the p -primary component is nontrivial over F , the nontrivial automorphism acts by inversion, and the corresponding minimal polynomial has the usual trace–norm form with constant term 1; see Lemma 2.1. The case $p = 2$ is more delicate. Lemma 2.2 determines the possible orders over F and the possible involutions, which give rise to three types of quadratic minimal polynomials. These prime-power calculations are assembled for an arbitrary primitive n -th root of unity in Theorem 2.1.

We then introduce the field invariants needed to organize these extensions. The property $\mathcal{C}_2$ isolates the exceptional 2-primary situation relevant to Schinzel’s classification, while the map t_F records the effective cyclotomic order entering the quadraticity criterion. The invariants $\ell_{p^\infty, F}$ and $\nu_{p^\infty, F}$ record, respectively, the p -power roots of unity already contained in F and the range of p -power levels that can give quadratic cyclotomic extensions. Theorem 3.1 gives a criterion for $F(\zeta_n)/F$ to be quadratic, and Theorem 3.2 determines the corresponding prime-power range. The 2-primary case requires a separate analysis, particularly when $\ell_{2^\infty, F} = 1$, where the upper range may be finite or infinite.

Finally, we pass from prime-power information to a global classification. For each prime that occurs in a quadratic primary cyclotomic extension, there is a unique corresponding quadratic field E_p . Two such primes are declared compatible when their quadratic p -primary fields coincide. Theorem 3.3 shows that the resulting compatibility classes are in bijection with the quadratic cyclotomic extensions of F and describes the primitive roots that generate each class.

The mathematical results presented in this article originate in the second author’s doctoral thesis [9]. The purpose of the present paper is to provide a self-contained, corrected, and streamlined journal-article treatment of this material, organized around the structure and classification of quadratic cyclotomic extensions. Related cyclicity questions for 2-power cyclotomic extensions are studied in [7].

2 Quadratic cyclotomic generators

2.1 Conventions and basic notation

Fix a field F and an algebraic closure $\overline{F}$. If $\text{char}(F) = r > 0$, every integer n occurring as the order of a primitive root of unity is assumed to satisfy $(n, r) = 1$. Likewise, throughout the paper

$$\mathbb{P}_F := \{p \text{ prime} : p \neq \text{char}(F)\}$$

when $\text{char}(F) > 0$, while $\mathbb{P}_F$ is the set of all primes in characteristic 0. Thus primitive p^e -th roots are only considered for $p \in \mathbb{P}_F$. This is the only restriction needed to treat characteristic 0 and positive characteristic in parallel.

We use $\mathbb{N} = \{1, 2, \dots\}$ and $\mathbb{N}_0 = \mathbb{N} \cup \{0\}$. We call an integer $n \geq 1$ *admissible* if every prime divisor of n belongs to $\mathbb{P}_F$. For an admissible integer $n \geq 1$, let

$$\mu_n := \{\zeta \in \overline{F} : \zeta^n = 1\}, \quad \mathcal{P}_n := \{\zeta \in \mu_n : \text{ord}(\zeta) = n\}.$$

Thus μ_n is the cyclic group of n -th roots of unity and $\mathcal{P}_n$ is the set of primitive n -th roots. We write ζ_n for an element of $\mathcal{P}_n$. Whenever divisibility relations among orders are used, the roots are chosen compatibly inside $\overline{F}$. More precisely, whenever $n = rs$ with $\gcd(r, s) = 1$, we choose primitive roots ζ_r and ζ_s compatibly with ζ_n , by which we mean that $\zeta_n = \zeta_r \zeta_s$. Such a choice is always possible. Indeed, choose integers a, b such that $as + br \equiv 1 \pmod{n}$. Then $\zeta_r := \zeta_n^{as}$, $\zeta_s := \zeta_n^{br}$ are primitive roots of orders r and s , respectively, and satisfy $\zeta_r \zeta_s = \zeta_n$.

For $\zeta_n \in \mathcal{P}_n$, define its *order over F* by

$$\text{o}_F(\zeta_n) := \min\{m \geq 1 : \zeta_n^m \in F\}.$$

The set $\{m \in \mathbb{Z} : \zeta_n^m \in F\}$ is a subgroup of $\mathbb{Z}$ containing $n\mathbb{Z}$. Hence, it is $\text{o}_F(\zeta_n)\mathbb{Z}$, and $\text{o}_F(\zeta_n) \mid n$. If $\zeta'_n = \zeta_n^u$ with $\gcd(u, n) = 1$, choose v such that $uv \equiv 1 \pmod{n}$. Then $(\zeta'_n)^m \in F$ if and only if $\zeta_n^m \in F$. Hence $\text{o}_F(\zeta_n)$ is independent of the chosen primitive n -th root. We put

$$\text{d}_F(n) := \frac{n}{\text{o}_F(\zeta_n)}.$$

Equivalently, $\text{d}_F(n)$ is the largest divisor d of n for which F contains a primitive d -th root of unity. For a prime p , $v_p(n)$ denotes the usual p -adic valuation.

If $[F(\zeta_n) : F] = 2$, let σ denote the nontrivial element of $\text{Gal}(F(\zeta_n)/F)$. There is a unique residue class $j_{\sigma, n} \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $\sigma(\zeta_n) = \zeta_n^{j_{\sigma, n}}$. Since $\sigma^2 = 1$ and $\zeta_n \sigma(\zeta_n) \in F$, we have

$$j_{\sigma, n}^2 \equiv 1 \pmod{n}, \quad \text{o}_F(\zeta_n) \mid (j_{\sigma, n} + 1). \quad (1)$$

We write $\text{minpol}(\zeta_n, F)$ for the monic minimal polynomial of ζ_n over F . It is therefore

$$\text{minpol}(\zeta_n, F) = x^2 - (\zeta_n + \zeta_n^{j_{\sigma, n}})x + \zeta_n^{j_{\sigma, n}+1}. \quad (2)$$

2.2 Odd-primary quadratic cyclotomic extensions

The following lemma will be used repeatedly below.

Lemma 2.1. *Let $[F(\zeta_n) : F] = 2$, and let p be an odd prime divisor of $\mathfrak{o}_F(\zeta_n)$. Put $a = v_p(n)$. Then, for every $1 \leq t \leq a$,*

1. $\zeta_{p^t} \notin F$ and $F(\zeta_{p^t}) = F(\zeta_n)$;
2. $\mathfrak{o}_F(\zeta_{p^t}) = p^t$, $d_F(p^t) = 1$, $v_p(\mathfrak{o}_F(\zeta_n)) = a$;
3. *if σ denotes the nontrivial element of $\text{Gal}(F(\zeta_n)/F)$, then $\sigma(\zeta_{p^t}) = \zeta_{p^t}^{-1}$. Consequently, $\text{minpol}(\zeta_{p^t}, F) = x^2 - (\zeta_{p^t} + \zeta_{p^t}^{-1})x + 1$.*

Proof. By Equation (1), $\mathfrak{o}_F(\zeta_n) \mid j_{\sigma,n} + 1$. Since $p \mid \mathfrak{o}_F(\zeta_n)$, it follows that $j_{\sigma,n} \equiv -1 \pmod{p}$. Hence, for the compatible primitive p -th root ζ_p , $\sigma(\zeta_p) = \zeta_p^{-1} \neq \zeta_p$, where the inequality follows from the fact that p is odd. Thus $\zeta_p \notin F$, and $F \subsetneq F(\zeta_p) \subseteq F(\zeta_n)$. Since $[F(\zeta_n) : F] = 2$, we obtain $F(\zeta_p) = F(\zeta_n)$.

For every $1 \leq t \leq a$, $F(\zeta_p) \subseteq F(\zeta_{p^t}) \subseteq F(\zeta_n)$, and therefore $F(\zeta_{p^t}) = F(\zeta_n)$. In particular, $\zeta_{p^t} \notin F$. This proves (1).

Now suppose that $d_F(p^t) > 1$. Since $d_F(p^t)$ is a power of p , this implies $p \mid d_F(p^t)$, and hence $\zeta_p \in F$, a contradiction. Therefore $d_F(p^t) = 1$, and $\mathfrak{o}_F(\zeta_{p^t}) = p^t$.

Similarly, $p \nmid d_F(n)$, since otherwise $\zeta_p \in F$. As $n = d_F(n) \mathfrak{o}_F(\zeta_n)$ and $a = v_p(n)$, we conclude that $v_p(\mathfrak{o}_F(\zeta_n)) = a$. This proves (2).

Finally, since $F(\zeta_{p^t}) = F(\zeta_n)$, the restriction of σ to $F(\zeta_{p^t})$ is its nontrivial F -automorphism. Applying Equation (1) to ζ_{p^t} and using $\mathfrak{o}_F(\zeta_{p^t}) = p^t$ gives $p^t \mid j_{\sigma,p^t} + 1$, and hence $j_{\sigma,p^t} \equiv -1 \pmod{p^t}$. Thus $\sigma(\zeta_{p^t}) = \zeta_{p^t}^{-1}$. Consequently,

$$\text{minpol}(\zeta_{p^t}, F) = (x - \zeta_{p^t})(x - \zeta_{p^t}^{-1}) = x^2 - (\zeta_{p^t} + \zeta_{p^t}^{-1})x + 1.$$

This proves (3). □

2.3 2-primary quadratic cyclotomic extensions

The 2-primary case is different because $-1 \in F$ whenever $2 \in \mathbb{P}_F$.

Lemma 2.2. *Let $e \geq 2$ and suppose that $[F(\zeta_{2^e}) : F] = 2$. Then $\mathfrak{o}_F(\zeta_{2^e}) \in \{2, 2^{e-1}\}$. More precisely:*

1. *If $\mathfrak{o}_F(\zeta_{2^e}) = 2$, then $j_{\sigma,2^e} \equiv 1 + 2^{e-1} \pmod{2^e}$, $\text{minpol}(\zeta_{2^e}, F) = x^2 - \zeta_{2^e}^2$. If $e > 2$, then $F(\zeta_{2^e}) \neq F(\zeta_{2^j})$ for every $j > e$.*
2. *If $\mathfrak{o}_F(\zeta_{2^e}) = 2^{e-1}$, then $F(\zeta_{2^e}) = F(\zeta_{2^e}^{2^s})$ ($1 \leq s \leq e-2$), and exactly one of the following occurs:*

(a) $j_{\sigma,2^e} \equiv 2^{e-1} - 1 \pmod{2^e}$ and

$$\text{minpol}(\zeta_{2^e}, F) = x^2 - (\zeta_{2^e} - \zeta_{2^e}^{-1})x - 1,$$

thus $\zeta_{2^e} - \zeta_{2^e}^{-1} \in F$.

(b) $j_{\sigma,2^e} \equiv -1 \pmod{2^e}$ and

$$\text{minpol}(\zeta_{2^e}, F) = x^2 - (\zeta_{2^e} + \zeta_{2^e}^{-1})x + 1,$$

thus $\zeta_{2^e} + \zeta_{2^e}^{-1} \in F$.

Proof. For $e = 2$, $\zeta_4^2 = -1 \in F$, so $o_F(\zeta_4) = 2 = 2^{e-1}$. Assume $e \geq 3$. The representatives of the solutions to $u^2 \equiv 1 \pmod{2^e}$ are $1, -1, 1 + 2^{e-1}, -1 + 2^{e-1}$. The first is excluded because σ is nontrivial.

If $j_{\sigma, 2^e} \equiv 1 + 2^{e-1}$, then using (1) and the fact that $o_F(\zeta_{2^e})$ is a nontrivial power of 2 imply $o_F(\zeta_{2^e}) = 2$.

For either of the other two involutions, σ acts by inversion on $\zeta_4 = \zeta_{2^e}^{2^{e-2}}$. Hence $\zeta_4 \notin F$. Consequently $o_F(\zeta_{2^e}) > 2^{e-2}$. Since $-1 = \zeta_{2^e}^{2^{e-1}} \in F$, the order over F is at most 2^{e-1} , so it is exactly 2^{e-1} . This proves the dichotomy.

The three displayed minimal polynomials now follow directly from (2). In the second case, $\zeta_{2^e}^{2^s} \notin F$ for $1 \leq s \leq e-2$; since it belongs to the quadratic field $F(\zeta_{2^e})$, it generates that field.

It remains to justify the last assertion in 1. Suppose $e > 2$ and $F(\zeta_{2^e}) = F(\zeta_{2^j})$ for some $j > e$. If $o_F(\zeta_{2^j}) = 2$, then $\zeta_{2^{j-1}} \in F$, hence $\zeta_{2^e} \in F$, a contradiction. Therefore the first part of the lemma gives $o_F(\zeta_{2^j}) = 2^{j-1}$. Since $\zeta_{2^e} = \zeta_{2^j}^{2^{j-e}}$,

$$o_F(\zeta_{2^e}) = \frac{2^{j-1}}{\gcd(2^{j-1}, 2^{j-e})} = 2^{e-1},$$

contradicting $o_F(\zeta_{2^e}) = 2$. □

Remark 1. Let $[F(\zeta_n) : F] = 2$. If n is odd, or if n is even and its full 2-primary root $\zeta_{2^{v_2(n)}}$ lies in F , then $\gcd(d_F(n), o_F(\zeta_n)) = 1$. Otherwise the greatest common divisor is 2. Indeed, let $d = d_F(n)$ and $o = o_F(\zeta_n)$, so that $n = do$. If an odd prime p divided both d and o , then $p \mid o$ and Lemma 2.1 would give $p \nmid d$, a contradiction. Thus no odd prime divides $\gcd(d, o)$. For the 2-primary part, if $\zeta_{2^{v_2(n)}} \in F$, then $v_2(o) = 0$. Otherwise Lemma 2.2 gives either $v_2(o) = 1$ and $v_2(d) = v_2(n) - 1$, or $v_2(o) = v_2(n) - 1$ and $v_2(d) = 1$. Hence in the nontrivial 2-primary case $v_2(\gcd(d, o)) = 1$, proving the claim.

2.4 The general quadratic minimal polynomial

We now assemble the prime-power information and express the minimal polynomial in terms of $d := d_F(n)$, $o_n := o_F(\zeta_n)$, $o_{2^e} := o_F(\zeta_{2^e})$, so that $n = do_n$. Put $e = v_2(n)$. By Remark 1,

$$\gcd(d, o_n) = \begin{cases} 1, & e = 0 \text{ or } \zeta_{2^e} \in F, \\ 2, & \zeta_{2^e} \notin F. \end{cases}$$

According to the order of the 2-primary component ζ_{2^e} over F , the factorization $n = do_n$ can therefore be rewritten as a product of coprime factors:

$$n = \begin{cases} d o_n, & e = 0 \text{ or } \zeta_{2^e} \in F, \\ (2d)(o_n/2), & o_{2^e} = 2, \\ (d/2)(2o_n), & o_{2^e} = 2^{e-1}. \end{cases}$$

In each case the two displayed factors are coprime. Hence, choosing the corresponding primitive roots compatibly with ζ_n , we may write

$$\zeta_n = \begin{cases} \zeta_d \zeta_{o_n}, & e = 0 \text{ or } \zeta_{2^e} \in F, \\ \zeta_{2d} \zeta_{o_n/2}, & o_{2^e} = 2, \\ \zeta_{d/2} \zeta_{2o_n}, & o_{2^e} = 2^{e-1}. \end{cases}$$

Theorem 2.1. Let $[F(\zeta_n) : F] = 2$, put $d = d_F(n)$, $o_n = o_F(\zeta_n)$, $o_{2^e} := o_F(\zeta_{2^e})$, and let σ be the nontrivial element of $\text{Gal}(F(\zeta_n)/F)$. Then exactly one of the following cases occurs.

(1) *The trivial 2-primary case.* If $e = 0$ or $\zeta_{2^e} \in F$, then $F(\zeta_n) = F(\zeta_{o_n})$, $\sigma(\zeta_n) = \zeta_d \zeta_{o_n}^{-1}$, and

$$\text{minpol}(\zeta_n, F) = x^2 - \zeta_d(\zeta_{o_n} + \zeta_{o_n}^{-1})x + \zeta_d^2.$$

(2) *The order-2 case.* If $o_{2^e} = 2$, equivalently $2 \parallel o_n$, then $F(\zeta_n) = F(\zeta_{2d}) = F(\zeta_{2^{e-1}o_n})$, $\sigma(\zeta_n) = -\zeta_{2d} \zeta_{o_n/2}^{-1}$, and

$$\text{minpol}(\zeta_n, F) = x^2 - \zeta_{2d}(\zeta_{o_n/2} - \zeta_{o_n/2}^{-1})x - \zeta_{2d}^2.$$

(3) *The plus-trace case.* If $e > 2$, $o_{2^e} = 2^{e-1}$, $\zeta_{2^e} + \zeta_{2^e}^{-1} \in F$, then $F(\zeta_n) = F(\zeta_{2o_n}) = F(\zeta_4)$, $\sigma(\zeta_n) = \zeta_{d/2} \zeta_{2o_n}^{-1}$, and

$$\text{minpol}(\zeta_n, F) = x^2 - \zeta_{d/2}(\zeta_{2o_n} + \zeta_{2o_n}^{-1})x + \zeta_{d/2}^2.$$

(4) *The minus-trace case.* If $e > 2$, $o_{2^e} = 2^{e-1}$, $\zeta_{2^e} - \zeta_{2^e}^{-1} \in F$, then $F(\zeta_n) = F(\zeta_{2o_n}) = F(\zeta_4)$, $\sigma(\zeta_n) = -\zeta_{d/2} \zeta_{2o_n}^{-1}$, and

$$\text{minpol}(\zeta_n, F) = x^2 - \zeta_{d/2}(\zeta_{2o_n} - \zeta_{2o_n}^{-1})x - \zeta_{d/2}^2.$$

Proof. For every odd prime p dividing o , Lemma 2.1 shows that the nontrivial automorphism acts by inversion on the corresponding p -primary component. The components belonging to d lie in F and are therefore fixed by σ . It remains only to combine this with the action on the 2-primary component given by Lemma 2.2.

In case (1), we have $\zeta_n = \zeta_d \zeta_{o_n}$, where $\zeta_d \in F$, while σ acts by inversion on ζ_{o_n} . Hence $\sigma(\zeta_n) = \zeta_d \zeta_{o_n}^{-1}$. Since $\zeta_d \in F$, we also obtain $F(\zeta_n) = F(\zeta_{o_n})$.

In case (2), we have $\zeta_n = \zeta_{2d} \zeta_{o_n/2}$. The odd-primary factors of ζ_{2d} lie in F , while Lemma 2.2(1) gives $\sigma(\zeta_{2d}) = -\zeta_{2d}$. Moreover, $o_n/2$ is odd, so Lemma 2.1 gives $\sigma(\zeta_{o_n/2}) = \zeta_{o_n/2}^{-1}$.

Therefore $\sigma(\zeta_n) = -\zeta_{2d} \zeta_{o_n/2}^{-1}$. Both ζ_{2d} and a compatible primitive $2^{e-1}o_n$ -th root lie in $F(\zeta_n) \setminus F$, and hence each generates the quadratic extension. Thus $F(\zeta_n) = F(\zeta_{2d}) = F(\zeta_{2^{e-1}o_n})$.

In cases (3) and (4), we have $\zeta_n = \zeta_{d/2} \zeta_{2o_n}$, $\zeta_{d/2} \in F$. In case (3), Lemma 2.2(2) together with Lemma 2.1 gives $\sigma(\zeta_{2o_n}) = \zeta_{2o_n}^{-1}$, whereas in case (4) it gives $\sigma(\zeta_{2o_n}) = -\zeta_{2o_n}^{-1}$. This yields the stated formulas for $\sigma(\zeta_n)$. Moreover, $\zeta_4 \in F(\zeta_n) \setminus F$, so the quadraticity of the extension implies $F(\zeta_n) = F(\zeta_{2o_n}) = F(\zeta_4)$. Finally, in every case

$$\text{minpol}(\zeta_n, F) = (x - \zeta_n)(x - \sigma(\zeta_n)).$$

Substituting the corresponding expression for $\sigma(\zeta_n)$ gives the four displayed minimal polynomials. $\square$

- Remark 2.** 1. Let $d = d_F(n)$, as defined in Theorem 2.1. The automorphism acts by inversion on ζ_n , that is, $\sigma(\zeta_n) = \zeta_n^{-1}$, if and only if $d = 1$, or $d = 2$ and $\zeta_{2^e} + \zeta_{2^e}^{-1} \in F$. Equivalently, $j_{\sigma,n} \equiv -1 \pmod{n}$ precisely in these cases.
2. Assume $\text{char}(F) \neq 2$, and let a be a root of unity such that the polynomial under consideration belongs to $F[x]$. Then $x^2 - (a + a^{-1})x + 1$ is irreducible over F if and only if $a - a^{-1} \notin F$, while $x^2 - (a - a^{-1})x - 1$ is irreducible over F if and only if $a + a^{-1} \notin F$. Indeed, their discriminants are respectively $(a - a^{-1})^2$ and $(a + a^{-1})^2$. Thus, once a cyclotomic element is known to have degree at most 2 over F , these criteria distinguish the quadratic case from the trivial one.

3 Structural invariants and classification

We now introduce the invariants that describe the prime-power structure of quadratic cyclotomic extensions. As noted in the Introduction, the material in this section originates in [9]; the definitions are formulated here so as to include both finite and infinite ranges and to apply uniformly in arbitrary characteristic.

3.1 Roots already contained in the base field

For $p \in \mathbb{P}_F$ put

$$\mu_{p^\infty} := \bigcup_{e \geq 1} \mu_{p^e}.$$

Definition 3.1. For $p \in \mathbb{P}_F$, define

$$\ell_{p^\infty, F} := \sup\{e \in \mathbb{N}_0 : \mu_{p^e} \subseteq F\} \in \mathbb{N}_0 \cup \{\infty\},$$

where $\mu_{p^0} = \{1\}$.

Remark 3. If $\ell_{p^\infty, F} < \infty$, then $\mu_{p^\infty} \cap F = \mu_{p^{\ell_{p^\infty, F}}}$. If $\ell_{p^\infty, F} = \infty$, then $\mu_{p^\infty} \subseteq F$. Thus $\mu_{p^\infty} \cap F$ is finite cyclic in the first case.

For a family of subgroups of $\overline{F}^\times$, we write $\bigvee$ for the subgroup generated by that family. Let

$$\mu_\infty := \bigvee_{p \in \mathbb{P}_F} \mu_{p^\infty}, \quad \mu_\infty(F) := \mu_\infty \cap F.$$

Every root of unity in μ_∞ is a finite product of its primary components.

3.2 The function t_F

The function below records the part of a primary root that remains nontrivial over F .

Definition 3.2. For $p \in \mathbb{P}_F$ and $e \geq 1$, define

$$t_F(p^e) = \begin{cases} p^e, & p \text{ odd and } o_F(\zeta_{p^e}) > 1, \\ 2^e, & p = 2 \text{ and } o_F(\zeta_{2^e}) > 2, \\ 2, & p = 2 \text{ and } o_F(\zeta_{2^e}) = 2, \\ 1, & o_F(\zeta_{p^e}) = 1. \end{cases}$$

For an admissible $n = \prod_{p|n} p^{v_p(n)}$, put

$$t_F(n) := \prod_{p|n} t_F(p^{v_p(n)}),$$

with the empty product equal to 1. In particular, $t_F(1) = 1$.

Lemma 3.1. *For fixed $p \in \mathbb{P}_F$ and integers $1 \leq f < e$, one has $t_F(p^f) \mid t_F(p^e)$. Moreover, if $\zeta_{t_F(p^e)} + \zeta_{t_F(p^e)}^{-1} \in F$, then $\zeta_{t_F(p^f)} + \zeta_{t_F(p^f)}^{-1} \in F$.*

Proof. Put $m_f = t_F(p^f)$ and $m_e = t_F(p^e)$. The divisibility $m_f \mid m_e$ follows from Definition 3.2 and the inclusion $F(\zeta_{p^f}) \subseteq F(\zeta_{p^e})$. Indeed, for odd p , each $t_F(p^k)$ is either 1 or p^k ; for $p = 2$, it is one of 1, 2, 2^k , and $o_F(\zeta_{2^e}) = 2$ implies $\zeta_{2^{e-1}} \in F$.

Since $m_f \mid m_e$, choose $\zeta_{m_f} = \zeta_{m_e/m_f}^{m_e/m_f}$. For every $q \geq 1$, the expression $X^q + X^{-q}$ is an integral polynomial in $X + X^{-1}$. Indeed, if $u_q = X^q + X^{-q}$, then $u_{q+1} = (X + X^{-1})u_q - u_{q-1}$, $u_0 = 2, u_1 = X + X^{-1}$. Hence, if $\zeta_{m_e} + \zeta_{m_e}^{-1} \in F$, then, taking $q = m_e/m_f$, $\zeta_{m_f} + \zeta_{m_f}^{-1} = \zeta_{m_e/m_f}^{m_e/m_f} + \zeta_{m_e/m_f}^{-m_e/m_f} \in F$. $\square$

3.3 The radical case: Roots of order 2 over F

We first isolate the quadratic cyclotomic extensions generated by roots of unity of order 2 over F .

Lemma 3.2. *Let $n = 2^e r$ be admissible, with r odd, and assume $\text{char}(F) \neq 2$. Then $o_F(\zeta_n) = 2$ if and only if $o_F(\zeta_{2^e}) = 2$ and $\zeta_r \in F$. If $\ell_{2^\infty, F} < \infty$, this is equivalent to $e = \ell_{2^\infty, F} + 1$ and $\zeta_r \in F$. If $\ell_{2^\infty, F} = \infty$, there is no root of unity of order 2 over F .*

Proof. Suppose first that $o_F(\zeta_n) = 2$. Then $\zeta_n^2 \in F$. Since r is odd, the Chinese remainder theorem gives an integer k such that

$$2k \equiv 0 \pmod{2^e}, \quad 2k \equiv 1 \pmod{r}.$$

For a compatible decomposition $\zeta_n = \zeta_{2^e} \zeta_r$, we therefore have $(\zeta_n^2)^k = \zeta_r$, so $\zeta_r \in F$. Consequently, $\zeta_{2^e} = \zeta_n \zeta_r^{-1} \notin F$, $\zeta_{2^e}^2 \in F$, and hence $o_F(\zeta_{2^e}) = 2$. Conversely, if $\zeta_r \in F$ and $o_F(\zeta_{2^e}) = 2$, then $\zeta_n \notin F$ and $\zeta_n^2 \in F$, so $o_F(\zeta_n) = 2$.

Finally, if $\ell_{2^\infty, F} < \infty$, then

$$o_F(\zeta_{2^e}) = 2 \iff e = \ell_{2^\infty, F} + 1,$$

since $\zeta_{2^{e-1}} \in F$ but $\zeta_{2^e} \notin F$. The assertion for $\ell_{2^\infty, F} = \infty$ is immediate. $\square$

Corollary 3.1. *Assume $\text{char}(F) \neq 2$. If $\ell_{2^\infty, F} < \infty$, the roots of unity of order 2 over F are precisely the products $\xi\eta$, where $\xi \in \mathcal{P}_{2^{\ell_{2^\infty, F}+1}}$ and $\eta \in F$ is a root of unity of odd order. Every such root generates the same quadratic extension, $F(\xi\eta) = F(\zeta_{2^{\ell_{2^\infty, F}+1}})$. If $\ell_{2^\infty, F} = \infty$, there are no such roots.*

3.4 The exceptional property $\mathcal{C}_2$

The only exceptional sign in the trace criterion occurs in the 2-primary case.

Definition 3.3. If $\text{char}(F) \neq 2$, an integer $e \geq 2$ has property $\mathcal{C}_2$ over F if

$$\zeta_{2^e} \notin F, \quad t_F(2^e) \neq 2, \quad \zeta_{2^e} - \zeta_{2^e}^{-1} \in F.$$

We say that F has property $\mathcal{C}_2$ if $\text{char}(F) \neq 2$ and such an e exists.

Lemma 3.3. If F has property $\mathcal{C}_2$, the corresponding exponent is unique. We denote it by $c_2(F)$. Moreover,

$$(1) \quad o_F(\zeta_{2^{c_2(F)}}) = 2^{c_2(F)-1} \text{ and } \text{minpol}(\zeta_{2^{c_2(F)}}, F) = x^2 - (\zeta_{2^{c_2(F)}} - \zeta_{2^{c_2(F)}}^{-1})x - 1;$$

$$(2) \text{ for every integer } 1 \leq f < c_2(F), \zeta_{t_F(2^f)} + \zeta_{t_F(2^f)}^{-1} \in F.$$

Proof. Let e have property $\mathcal{C}_2$. The element ζ_{2^e} is a root of $x^2 - (\zeta_{2^e} - \zeta_{2^e}^{-1})x - 1 \in F[x]$. Since $\zeta_{2^e} \notin F$, this polynomial is irreducible and $F(\zeta_{2^e})/F$ is quadratic. Because $t_F(2^e) \neq 2$, Lemma 2.2 gives the order and the displayed minimal polynomial.

Set $u = \zeta_{2^e} - \zeta_{2^e}^{-1} \in F$ and $a_f := \zeta_{2^f} + \zeta_{2^f}^{-1}$ for $1 \leq f < e$. Then

$$a_{e-1} = \zeta_{2^e}^2 + \zeta_{2^e}^{-2} = u^2 + 2 \in F, \quad a_{f-1} = a_f^2 - 2 \quad (2 \leq f < e).$$

The recurrence gives $a_f \in F$ successively for every $1 \leq f < e$. Whenever $t_F(2^f) = 2^f$, this is precisely the required assertion; if $t_F(2^f) = 1$ or 2 , the assertion is immediate. This proves (2).

For uniqueness, suppose $e < k$ both have property $\mathcal{C}_2$. Applying (2) to k gives $\zeta_{2^e} + \zeta_{2^e}^{-1} \in F$, while property $\mathcal{C}_2$ at e gives $\zeta_{2^e} - \zeta_{2^e}^{-1} \in F$. Since $\text{char}(F) \neq 2$, adding the two expressions yields $2\zeta_{2^e} \in F$, a contradiction. $\square$

3.5 A criterion for quadraticity

For an admissible n , write $n = 2^e r$ with r odd. Thus, after discarding the odd-primary factors already contained in F , the remaining odd-primary component is a primitive $t_F(r)$ -th root.

Theorem 3.1. Let $n = 2^e r$ be admissible, with r odd. Then $F(\zeta_n)/F$ is quadratic if and only if $\zeta_n \notin F$ and one of the following mutually exclusive alternatives holds:

- (1) If $e = 0$ or $\zeta_{2^e} \in F$, then $\zeta_{t_F(n)} + \zeta_{t_F(n)}^{-1} \in F$.
- (2) If $e > 0$ and $o_F(\zeta_{2^e}) = 2$, then $\zeta_{2^e}(\zeta_{t_F(r)} - \zeta_{t_F(r)}^{-1}) \in F$.
- (3) If $e > 0$ and $o_F(\zeta_{2^e}) > 2$, then
 - if F has property $\mathcal{C}_2$ and $e = c_2(F)$, $\zeta_{t_F(n)} - \zeta_{t_F(n)}^{-1} \in F$;
 - otherwise $\zeta_{t_F(n)} + \zeta_{t_F(n)}^{-1} \in F$.

Proof. Put $d := d_F(n)$, and $o_n := o_F(\zeta_n)$. Assume first that $[F(\zeta_n) : F] = 2$.

If $e = 0$ or $\zeta_{2^e} \in F$, then o_n is odd and $t_F(n) = o_n$.

By Theorem 2.1(1),

$$\text{minpol}(\zeta_n, F) = x^2 - \zeta_d(\zeta_{o_n} + \zeta_{o_n}^{-1})x + \zeta_d^2.$$

Since $\zeta_d \in F^\times$, the trace coefficient lies in F if and only if $\zeta_{t_F(n)} + \zeta_{t_F(n)}^{-1} \in F$.

If $e > 0$ and $\circ_F(\zeta_{2^e}) = 2$, then $2||_{o_n}$ and $o_n/2 = t_F(r)$. Moreover, $v_2(d) = e - 1$, and the odd-primary part of ζ_{2d} lies in F ; hence $\zeta_{2d} = u\zeta_{2^e}$ for some $u \in F^\times$. Theorem 2.1(2) therefore shows that its trace coefficient lies in F if and only if $\zeta_{2^e}(\zeta_{t_F(r)} - \zeta_{t_F(r)}^{-1}) \in F$.

Finally, suppose that $e > 0$ and $\circ_F(\zeta_{2^e}) > 2$. Then $\circ_F(\zeta_{2^e}) = 2^{e-1}$, $t_F(n) = 2o_n$. Since $\zeta_{d/2} \in F^\times$, Theorem 2.1(3) and (4) give respectively $\zeta_{t_F(n)} + \zeta_{t_F(n)}^{-1} \in F$ and $\zeta_{t_F(n)} - \zeta_{t_F(n)}^{-1} \in F$. The latter occurs precisely when e has property $\mathcal{C}_2$, hence, by Lemma 3.3, precisely when $e = c_2(F)$. This proves the forward implication.

Conversely, assume that $\zeta_n \notin F$ and that one of the stated conditions holds. Removing from ζ_n all primary components already contained in F does not change the field it generates, since multiplication or division by an element of $F^\times$ does not change the field generated over F .

In case (1), we obtain $F(\zeta_n) = F(\zeta_{t_F(n)})$. Since $\zeta_{t_F(n)} + \zeta_{t_F(n)}^{-1} \in F$, the element $\zeta_{t_F(n)}$ satisfies $x^2 - (\zeta_{t_F(n)} + \zeta_{t_F(n)}^{-1})x + 1 \in F[x]$. Thus $[F(\zeta_{t_F(n)}) : F] \leq 2$, and $\zeta_{t_F(n)} \notin F$ gives equality. In case (2), let $\delta := \zeta_{2^e}$, $\xi := \delta\zeta_{t_F(r)}$. Removing the components that lie in F , we obtain $F(\zeta_n) = F(\xi)$. Since $\circ_F(\delta) = 2$, we have $\delta^2 \in F$. By hypothesis, $a := \delta(\zeta_{t_F(r)} - \zeta_{t_F(r)}^{-1}) \in F$, and ξ satisfies $\xi^2 - a\xi - \delta^2 = 0$. Hence $[F(\xi) : F] \leq 2$, and since $\xi \notin F$, the degree is exactly 2.

In case (3), we again have $F(\zeta_n) = F(\zeta_{t_F(n)})$. If F has property $\mathcal{C}_2$ and $e = c_2(F)$, then $\zeta_{t_F(n)} - \zeta_{t_F(n)}^{-1} \in F$, so $\zeta_{t_F(n)}$ satisfies $x^2 - (\zeta_{t_F(n)} - \zeta_{t_F(n)}^{-1})x - 1 \in F[x]$. Otherwise, $\zeta_{t_F(n)} + \zeta_{t_F(n)}^{-1} \in F$, so $\zeta_{t_F(n)}$ satisfies $x^2 - (\zeta_{t_F(n)} + \zeta_{t_F(n)}^{-1})x + 1 \in F[x]$. In either case $[F(\zeta_{t_F(n)}) : F] = 2$. The three alternatives are mutually exclusive by their conditions on the 2-primary component. $\square$

3.6 The upper primary invariant $\nu_{p^\infty, F}$

This invariant records the last p -power level that can contribute to a quadratic cyclotomic extension. It is a corrected reformulation of the corresponding upper invariant in [9], with the exceptional 2-primary level separated explicitly.

Definition 3.4. For $p \in \mathbb{P}_F$, define

$$\nu_{p^\infty, F}^+ := \sup \left\{ k \in \mathbb{N} : \zeta_{t_F(p^k)} + \zeta_{t_F(p^k)}^{-1} \in F \right\} \in \mathbb{N}_0 \cup \{\infty\},$$

with $\sup \emptyset = 0$. Put

$$\nu_{p^\infty, F} := \begin{cases} \nu_{2^\infty, F}^+ + 1, & p = 2 \text{ and } F \text{ has property } \mathcal{C}_2, \\ \nu_{p^\infty, F}^+, & \text{otherwise.} \end{cases}$$

Lemma 3.1 shows that the set defining $\nu_{p^\infty, F}^+$ is an initial interval of exponents, so the supremum is a genuine endpoint (possibly ∞). If F has property $\mathcal{C}_2$, then in fact $\nu_{2^\infty, F}^+ = c_2(F) - 1$. Indeed, Lemma 3.3 gives the plus-trace condition at every lower level; it cannot hold at $c_2(F)$, since together with the defining minus-trace condition it would imply $\zeta_{2^{c_2(F)}} \in F$; and Lemma 3.1 then excludes the plus-trace condition at every higher level. Thus the expression $\nu_{2^\infty, F}^+ + 1$ in Definition 3.4 is finite whenever it occurs and equals $c_2(F)$.

The next result shows that, for each prime p , the exponents giving quadratic p -primary cyclotomic extensions form a single interval between the lower and upper invariants.

Theorem 3.2. Let $p \in \mathbb{P}_F$.

- (1) One always has $\ell_{p^\infty, F} \leq \nu_{p^\infty, F}$.
- (2) If $\ell_{p^\infty, F} < \infty$, then $[F(\zeta_{p^e}) : F] = 2$ if and only if $\ell_{p^\infty, F} < e \leq \nu_{p^\infty, F}$. If $\ell_{p^\infty, F} = \infty$, no p -power root generates a nontrivial cyclotomic extension.
- (3) For $p = 2$, the endpoint is described more explicitly as follows:
 - (a) if $\ell_{2^\infty, F} = \infty$, then $\nu_{2^\infty, F} = \infty$ and there are no quadratic 2-primary extensions;
 - (b) if $2 \leq \ell_{2^\infty, F} < \infty$, then $\nu_{2^\infty, F} = \ell_{2^\infty, F} + 1$;
 - (c) if $\ell_{2^\infty, F} = 1$, then $\nu_{2^\infty, F} = \sup\{k \geq 2 : F(\zeta_{2^k}) = F(\zeta_4)\}$, which may be finite or infinite.

Proof. For every $k \leq \ell_{p^\infty, F}$, $\zeta_{p^k} \in F$, so $t_F(p^k) = 1$ and the plus-trace condition in Definition 3.4 is automatic. This proves (1).

Assume $\ell := \ell_{p^\infty, F} < \infty$, and let $e > \ell$ be such that $[F(\zeta_{p^e}) : F] = 2$.

If $p \neq 2$, or if $p = 2$ and $e \neq c_2(F)$, Theorem 3.1 gives $\zeta_{t_F(p^e)} + \zeta_{t_F(p^e)}^{-1} \in F$. Hence, by the definition of $\nu_{p^\infty, F}^+$, $e \leq \nu_{p^\infty, F}^+ \leq \nu_{p^\infty, F}$. The only remaining case is $p = 2$ and $e = c_2(F)$. In that case, Lemma 3.3 gives $\nu_{2^\infty, F}^+ = c_2(F) - 1$, and therefore, by definition, $\nu_{2^\infty, F} = \nu_{2^\infty, F}^+ + 1 = c_2(F) = e$. Thus in all cases $e \leq \nu_{p^\infty, F}$.

Conversely, let $\ell < e \leq \nu_{p^\infty, F}$. If $e \leq \nu_{p^\infty, F}^+$, then by the definition of $\nu_{p^\infty, F}^+$ and Lemma 3.1, $\zeta_{t_F(p^e)} + \zeta_{t_F(p^e)}^{-1} \in F$. Since $e > \ell$, we have $\zeta_{p^e} \notin F$, and Theorem 3.1 yields $[F(\zeta_{p^e}) : F] = 2$. The only remaining possibility is that $\nu_{p^\infty, F} > \nu_{p^\infty, F}^+$. By Definition 3.4, this occurs only when $p = 2$ and F has property $\mathcal{C}_2$. In that case $e = \nu_{2^\infty, F}^+ + 1 = c_2(F)$, and the fact that the extension is quadratic follows from Lemma 3.3. This proves (2).

For 3(a), the assertion follows from Remark 3.

Suppose next that $2 \leq \ell_{2^\infty, F} < \infty$. Since $\zeta_{2^{\ell_{2^\infty, F}}} \in F$ but $\zeta_{2^{\ell_{2^\infty, F}+1}} \notin F$, the latter is a root of $x^2 - \zeta_{2^{\ell_{2^\infty, F}}}$, so $F(\zeta_{2^{\ell_{2^\infty, F}+1}})/F$ is quadratic and its order over F is 2. Because $\ell_{2^\infty, F} + 1 > 2$, no higher 2-power can generate a quadratic extension: if $j > \ell_{2^\infty, F} + 1$ and $F(\zeta_{2^j})/F$ were quadratic, then it would contain the quadratic subfield $F(\zeta_{2^{\ell_{2^\infty, F}+1}})$ and hence would equal it, contradicting Lemma 2.2 (1). It follows that no exponent greater than $\ell_{2^\infty, F} + 1$ gives a quadratic 2-primary extension. Consequently, $\nu_{2^\infty, F} = \ell_{2^\infty, F} + 1$, proving (3)(b).

Finally, suppose that $\ell_{2^\infty, F} = 1$. Then $\zeta_4 \notin F$, while $\zeta_4^2 = -1 \in F$, so $[F(\zeta_4) : F] = 2$. For every $k \geq 2$, $\zeta_4 = \zeta_{2^k}^{2^{k-2}}$, and hence $F(\zeta_4) \subseteq F(\zeta_{2^k})$. Therefore, if $F(\zeta_{2^k})/F$ is quadratic, then the above inclusion between two nontrivial quadratic extensions must be an equality. Conversely, this equality clearly implies that $F(\zeta_{2^k})/F$ is quadratic. By 2, since $\ell_{2^\infty, F} = 1$, the quadratic 2-power levels are precisely those with $2 \leq k \leq \nu_{2^\infty, F}$. Consequently,

$$\nu_{2^\infty, F} = \sup\{k \geq 2 : F(\zeta_{2^k}) = F(\zeta_4)\}.$$

This supremum may be finite or infinite. For $F = \mathbb{Q}$, it equals 2, since $[\mathbb{Q}(\zeta_8) : \mathbb{Q}] = 4$. □

3.7 Global compatibility and classification

We now pass from primary information to arbitrary roots of unity. Define

$$\mathcal{M}_2(F) := \{\zeta \in \mu_\infty \setminus F : [F(\zeta) : F] = 2\} \quad \text{and} \quad \mathcal{E}_2(F) := \{F(\zeta) : \zeta \in \mathcal{M}_2(F)\}.$$

Thus $\mathcal{M}_2(F)$ is the set of quadratic cyclotomic generators and $\mathcal{E}_2(F)$ is the set of quadratic cyclotomic fields inside the fixed algebraic closure.

Call a prime $p \in \mathbb{P}_F$ *active* if some p -power root of unity generates a quadratic extension, equivalently if $\ell_{p^\infty, F} < \nu_{p^\infty, F}$. Let $\mathcal{P}_2(F)$ denote the set of active primes.

Proposition 3.1. *Let p be active. If e and f are such that $[F(\zeta_{p^e}) : F] = [F(\zeta_{p^f}) : F] = 2$, then $F(\zeta_{p^e}) = F(\zeta_{p^f})$. We denote this common quadratic field by E_p .*

Proof. If p is odd and $F(\zeta_{p^e})/F$ is quadratic, Lemma 2.1 gives $F(\zeta_{p^t}) = F(\zeta_{p^e})$ for every lower nontrivial level t . If two exponents $e < f$ are both quadratic, applying the lemma to f gives $F(\zeta_{p^e}) = F(\zeta_{p^f})$.

For $p = 2$, if $\ell_{2^\infty, F} \geq 2$, Theorem 3.2 shows that there is only one quadratic exponent. If $\ell_{2^\infty, F} = 1$, every quadratic $F(\zeta_{2^e})$ contains the nontrivial quadratic field $F(\zeta_4)$, hence equals it. This proves uniqueness in all cases. $\square$

Define an equivalence relation on $\mathcal{P}_2(F)$ by

$$p \sim_F q \iff E_p = E_q.$$

Let

$$\mathcal{M}_F := \mathcal{P}_2(F) / \sim_F$$

be the set of compatibility classes. For $M \in \mathcal{M}_F$, write E_M for the common field E_p with $p \in M$. We note that E_M is well defined, since if $p, q \in M$, then $p \sim_F q$, and hence $E_p = E_q$.

For an extended exponent $a \in \mathbb{N}_0 \cup \{\infty\}$, use the convention $\mu_{p^a} = \mu_{p^\infty}$ when $a = \infty$. Define

$$\mu_M := \left(\bigvee_{p \in M} \mu_{p^{\nu_{p^\infty, F}}} \right) \vee \left(\bigvee_{p \in \mathbb{P}_F \setminus M} \mu_{p^{\ell_{p^\infty, F}}} \right).$$

Conceptually, μ_M allows precisely the nontrivial primary components that generate the single quadratic field E_M ; all primary components outside M are required to lie already in F .

Theorem 3.3. *For each $M \in \mathcal{M}_F$, every $\zeta \in \mu_M \setminus \mu_\infty(F)$ generates the field E_M . Conversely, every $\zeta \in \mathcal{M}_2(F)$ belongs to exactly one such set. Hence*

$$\mathcal{M}_2(F) = \coprod_{M \in \mathcal{M}_F} (\mu_M \setminus \mu_\infty(F)),$$

and $M \mapsto E_M$ is a bijection from $\mathcal{M}_F$ onto $\mathcal{E}_2(F)$.

Proof. Let $M \in \mathcal{M}_F$ and let $\zeta \in \mu_M \setminus \mu_\infty(F)$. Decompose ζ into its primary components. By the definition of μ_M , every component corresponding to a prime outside M lies in F . For $p \in M$, a primary component either lies in F or, by Theorem 3.2, generates $E_p = E_M$. Hence every primary component of ζ belongs to E_M , so $\zeta \in E_M$. Since $\zeta \notin F$, we obtain $F(\zeta) = E_M$.

Conversely, let $\zeta_n \in \mathcal{M}_2(F)$ and put $E = F(\zeta_n)$. Define

$$S_{F,n} := \{p \mid n : \zeta_{p^{v_p(n)}} \notin F\}.$$

This set is nonempty since $\zeta_n \notin F$. For every $p \in S_{F,n}$, $F \subsetneq F(\zeta_{p^{v_p(n)}}) \subseteq E$. Since $[E : F] = 2$, we have $F(\zeta_{p^{v_p(n)}}) = E$. Thus p is active and $E_p = E$. Hence all primes in $S_{F,n}$ belong to the same compatibility class M .

For $p \in S_{F,n}$, Theorem 3.2 gives $v_p(n) \leq \nu_{p^\infty, F}$. For $p \notin S_{F,n}$, the corresponding primary component lies in F , so $v_p(n) \leq \ell_{p^\infty, F}$ whenever $\ell_{p^\infty, F} < \infty$. Therefore $\zeta_n \in \mu_M \setminus \mu_\infty(F)$. The class M is unique: any class M' for which $\zeta_n \in \mu_{M'} \setminus \mu_\infty(F)$ must contain every prime in the nonempty set $S_{F,n}$.

It follows that

$$\mathcal{M}_2(F) = \coprod_{M \in \mathcal{M}_F} (\mu_M \setminus \mu_\infty(F)).$$

Finally, the correspondence $M \mapsto E_M$ is injective by the definition of the compatibility classes, and it is surjective because every field in $\mathcal{E}_2(F)$ is generated by some element of $\mathcal{M}_2(F)$. $\square$

4 Finite fields

The preceding classification becomes especially transparent over a finite field.

Example 1. Let $F = \mathbb{F}_q$, where $q = r^m$ and r is prime. For every n prime to r ,

$$[\mathbb{F}_q(\zeta_n) : \mathbb{F}_q] = \text{ord}_n(q),$$

the multiplicative order of q modulo n . Hence

$$[\mathbb{F}_q(\zeta_n) : \mathbb{F}_q] = 2 \iff n \mid (q^2 - 1) \text{ and } n \nmid (q - 1).$$

It follows that, for every $p \neq r$,

$$\ell_{p^\infty, \mathbb{F}_q} = v_p(q - 1), \quad \nu_{p^\infty, \mathbb{F}_q} = v_p(q^2 - 1).$$

All active primes have the same primary quadratic field, namely $\mathbb{F}_{q^2}$. Thus there is a single compatibility class and

$$\mathcal{E}_2(F) = \{\mathbb{F}_{q^2}\}, \quad \mathcal{M}_2(F) = \mu_{q^2-1} \setminus \mu_{q-1}.$$

Acknowledgements

The authors thank the referee for a careful report that led to substantial corrections and a reorganization of the manuscript.

References

- [1] Acosta de Orozco, M., & Vélez, W. Y. (1982). The lattice of subfields of a radical extension. *Journal of Number Theory*, 15(3), 388–405.
- [2] Cele, M., & Marques, S. (2022). The geometry of the moduli space of non-cyclic biquadratic field extensions. *Quaestiones Mathematicae*, 45(10), 1501–1527.
- [3] Conrad, K. *Cyclotomic extensions*. Expository notes. Available online at: <https://kconrad.math.uconn.edu/blurbs/galoistheory/cyclotomic.pdf>.
- [4] DeMeyer, F., & Ingraham, E. (1971). *Separable Algebras over Commutative Rings*. Lecture Notes in Mathematics, Vol. 181. Springer-Verlag, Berlin–Heidelberg.
- [5] Gay, D., & Vélez, W. Y. (1981). The torsion group of a radical extension. *Pacific Journal of Mathematics*, 92(2), 317–327.
- [6] Kitamura, K. (1973). On the free quadratic extensions of a commutative ring. *Osaka Journal of Mathematics*, 10(1), 15–20.
- [7] Marques, S., & Mrema, E. (2024). *When is a 2-power cyclotomic extension cyclic?* Preprint. Available online at: <https://arxiv.org/abs/2308.08865>.
- [8] Micali, A., & Revoy, P. (1979). *Modules quadratiques*. *Mémoires de la Société Mathématique de France*, 63, 5–144.
- [9] Mrema, E. (2024). *Study of Cyclotomic Extension of Degree Power of 2 and Classification of Radical Extensions up to Isomorphism*. PhD thesis, Stellenbosch University. Available online at: <https://scholar.sun.ac.za/handle/10019.1/130317>.
- [10] Norris, M., & Vélez, W. (1980). Structure theorems for radical extensions of fields. *Acta Arithmetica*, 38(2), 111–115.
- [11] Poonen, B. (2008). The moduli space of commutative algebras of finite rank. *Journal of the European Mathematical Society*, 10(3), 817–836.
- [12] Schinzel, A. (1975). On linear dependence of roots. *Acta Arithmetica*, 28(2), 161–176.
- [13] Szeto, G., & Wong, Y.-F. (1981). On free quadratic extensions of rings. *Monatshefte für Mathematik*, 92(4), 323–328.
- [14] Vélez, W. Y. (1985). Several results on radical extensions. *Archiv der Mathematik*, 45(4), 342–349.
- [15] Voight, J. (2016). Discriminants and the monoid of quadratic rings. *Pacific Journal of Mathematics*, 283(2), 483–510.
- [16] Waterhouse, W. C. (1993). The degrees of the cyclotomic extension fields. *Linear Algebra and its Applications*, 195, 181–189.