EXPLICIT KUMMER GENERATORS FOR CYCLOTOMIC EXTENSIONS

FRITZ HÖRMANN, ANTONELLA PERUCCA, PIETRO SGOBBA, SEBASTIANO TRONTO

ABSTRACT. If p is a prime number congruent to 1 modulo 3, then we explicitly describe an element of the cyclotomic field $\mathbb{Q}(\zeta_3)$ whose third root generates the cubic subextension of $\mathbb{Q}(\zeta_{3p})/\mathbb{Q}(\zeta_3)$. Similarly, if p is a prime number congruent to 1 modulo 4, then we explicitly describe an element of the cyclotomic field $\mathbb{Q}(\zeta_4)$ whose fourth root generates the quartic cyclic subextension of $\mathbb{Q}(\zeta_{4p})/\mathbb{Q}(\zeta_4)$. For further number fields we express generators of Kummer extensions inside cyclotomic fields in terms of Gauss sums.

1. INTRODUCTION

Consider the cyclotomic extensions of the form $\mathbb{Q}(\zeta_{3p})/\mathbb{Q}(\zeta_3)$, where p is a prime number congruent to 1 modulo 3. Since the base field contains the third roots of unity, the subextension of $\mathbb{Q}(\zeta_{3p})/\mathbb{Q}(\zeta_3)$ is a Kummer extension, generated by the third root of some element of $\mathbb{Q}(\zeta_3)$. Similarly, the cyclotomic extensions $\mathbb{Q}(\zeta_{4p})/\mathbb{Q}(\zeta_4)$, where p is a prime number congruent to 1 modulo 4, have a quartic cyclic subextension which is a Kummer extension, generated by the fourth root of some element of $\mathbb{Q}(\zeta_4)$. We describe generators of those Kummer extensions:

Theorem 1. *Let p be a prime number such that $p \equiv 1 \pmod 3$.*

(1) There exists $\pi \in \mathbb{Q}(\zeta_3)$ such that $\pi \cdot \overline{\pi} = p$ and $\pi \equiv 1 \pmod 3$. Up to complex conjugation, π is uniquely determined by these conditions.
(2) The element $\pi \cdot p$ (equivalently, $\overline{\pi} \cdot p$) is such that any of its third roots generates the cubic subextension of $\mathbb{Q}(\zeta_{3p})/\mathbb{Q}(\zeta_3)$.

Theorem 2. *Let p be a prime number such that $p \equiv 1 \pmod 4$.*

(1) There exists $\pi \in \mathbb{Q}(\zeta_4)$ such that $\pi \cdot \overline{\pi} = p$ and $\pi \cdot \overline{\pi}^3 \equiv 1 \pmod 4$. The element π is uniquely determined up to sign and up to complex conjugation.
(2) The element $\gamma_p := \pi \cdot \overline{\pi}^3$ is such that any of its fourth roots generates the quartic subextension of $\mathbb{Q}(\zeta_{4p})/\mathbb{Q}(\zeta_4)$.

We also have:

Theorem 3. *Let p be a prime number such that $p \equiv 1 \pmod 4$. The quadratic extension of $\mathbb{Q}(\sqrt{p})$ inside $\mathbb{Q}(\zeta_p)$ is generated by the square roots of $\omega_p := u\sqrt{p}$, where u is a fundamental unit of $\mathbb{Q}(\sqrt{p})$ such that for any embedding $\sigma : \mathbb{Q}(\sqrt{p}) \to \mathbb{R}$ the sign of $\sigma(u\sqrt{p})$ is positive if and only if $p \equiv 1 \pmod 8$. Moreover, we have*

$$\mathbb{Q}(\sqrt{\omega_p}) = \mathbb{Q}(\zeta_p) \cap \mathbb{Q}\big(\zeta_4, \sqrt[4]{\gamma_p}\big) \quad \text{and} \quad \mathbb{Q}\big(\zeta_4, \sqrt{\omega_p}\big) = \mathbb{Q}\big(\zeta_4, \sqrt[4]{\gamma_p}\big)\,,$$

2010 *Mathematics Subject Classification.* Primary: 11R11; Secondary: 11R18, 11R21, 11Y40.
Key words and phrases. Kummer theory, Kummer extension, number field, cyclotomic field.

where γ_p is as in Theorem 2.

Example 4. The cyclotomic field $\mathbb{Q}(\zeta_5)$ is a quartic cyclic extension of $\mathbb{Q}$, which is generated by ζ_5. By considering the sine and cosine of $\frac{2\pi}{5}$ we get the expression

$$\zeta_5 = \frac{\sqrt{5}-1}{4} + \sqrt{-\frac{5+\sqrt{5}}{8}}$$

so we know that $\mathbb{Q}(\zeta_5)$ over $\mathbb{Q}(\sqrt{5})$ is the quadratic extension generated by the square root of $-\frac{5+\sqrt{5}}{8}$. Up to a square this element is $-\frac{\sqrt{5}+1}{2} \cdot \sqrt{5}$ and we may easily check with [6] that the first factor is a fundamental unit.

In the last section we consider further number fields and present generators for Kummer extensions inside cyclotomic fields by making use of Gauss sums. Notice that the results in this note may be in part well-known to the experts however they are useful for applications and hence we have provided a comprehensive reference. We thank the referee for suggesting a short proof of Lemma 5.

Notation. For an integer $n \geqslant 1$ we denote by ζ_n a primitive n-th root of unity, and by μ_n the multiplicative group generated by ζ_n. Recall that a prime number $p \equiv 1 \pmod{n}$ decomposes fully (i.e. it splits completely) in $\mathbb{Q}(\zeta_n)$. If K is a number field, then after choosing an embedding of K in $\mathbb{C}$ we write $\overline{x}$ for the complex conjugate of an element $x \in K$. Given a prime $\mathfrak{p}$ of K, we denote by $K_\mathfrak{p}$ the completion of K at $\mathfrak{p}$ with respect to the $\mathfrak{p}$-adic valuation of K. If L is a local field of characteristic 0, we denote by v_L its valuation and by $\mathcal{O}_L$ its valuation ring. Finally, if we write a congruence modulo an algebraic integer in K, then we mean the congruence modulo the integral ideal generated by that element in the ring of integers.

2. The cubic subextension of $\mathbb{Q}(\zeta_{3p})/\mathbb{Q}(\zeta_3)$

Let $\mathcal{O}$ be the ring of integers of $\mathbb{Q}(\zeta_3)$, and recall that $\mathcal{O}^\times = \mu_6$. We will write $\xi := 1 - \zeta_3$.

Lemma 5. *The quotient map $\mathcal{O} \to \mathcal{O}/3\mathcal{O}$ induces an group isomorphism $\mu_6 \to (\mathcal{O}/3\mathcal{O})^\times$.*

Proof. Since $\mathcal{O} = \mathbb{Z}[\zeta_3]$, the quotient map is clearly injective on $\mu_6 = \{\pm 1, \pm\zeta_3, \pm(1+\zeta_3)\}$. We conclude because the class of 0 and the classes of $\pm\xi$ are not units, as $(1-\zeta_3)^2 = -3\zeta_3$. □

Proof of Theorem 1 (1). Since $p \equiv 1 \pmod{3}$, there is $\pi \in \mathcal{O}$ and a root of unity $\zeta \in \mu_6$ such that $\zeta \cdot \pi \cdot \overline{\pi} = p$. We deduce from Lemma 5 and from the assumption on p that π is invertible modulo 3. Again by Lemma 5 there exists a unique $u \in \mu_6$ such that $u\pi \equiv 1 \pmod{3}$. Replacing π by $u\pi$, we then get

$$\pi \equiv \overline{\pi} \equiv \pi\overline{\pi} \equiv 1 \equiv p \pmod{3}.$$

Since 1 is the only root of unity in μ_6 which is congruent to 1 modulo 3, we deduce that $\pi \cdot \overline{\pi} = p$. As for the unicity, we could replace π by $\overline{\pi}$, but to mantain the property $\pi \equiv 1 \pmod{3}$ we cannot multiply π by a root of unity in $\mathcal{O}$ distinct from 1, see Lemma 5. □

Lemma 6. *Let K' be the unique unramified extension of $\mathbb{Q}_3(\zeta_3)$ of degree 3. If $\alpha \in K'$ is a unit such that $v_{K'}(1-\alpha) \geqslant 4$, then α is a third power.*

Proof. For $n \geqslant 1$, set

$$U^{(n)} := \{x \in \mathcal{O}_{K'} \mid x \equiv 1 \pmod{\xi^n}\}$$

and denote by $\overline{U^{(n)}}$ the image of $U^{(n)}$ in $(K')^\times/(K')^{\times 3}$. We have to show that $\overline{U^{(4)}}$ is trivial. We know that $\overline{U^{(5)}}$ is trivial by applying Hensel's Lemma to the polynomial $x^3 - a$ with value $x_0 = 1$ and $a \in U^{(5)}$, noticing that $v_{K'}(3) = 2$ and hence $v_{K'}(1-a) > 2v_{K'}(3)$. Consider the map raising to the third power from $U^{(2)}/U^{(3)}$ onto $U^{(4)}/U^{(5)}$ (both quotients are isomorphic to $\mathbb{F}_3$). An element $1 + a\xi^2 \pmod{\xi^3}$ is mapped to $1 + au\xi^4 \pmod{\xi^5}$, where u is the unit such that $3 = u\xi^2$. Thus the map is the multiplication by u, which is surjective. We have found that any element of $U^{(4)}$ is an element of $U^{(5)}$ up to third powers, and hence $\overline{U^{(4)}} = \overline{U^{(5)}}$ is trivial. □

Proposition 7. *If $\alpha \in \mathcal{O}$ is such that $\alpha \equiv 1 \pmod{\xi^3}$, then the Kummer extension generated by $\sqrt[3]{\alpha}$ is unramified over $\mathbb{Q}(\zeta_3)$ at (ξ). Among the elements $u\alpha$ with $u \in \mu_6$, only α and $-\alpha$ have this ramification property.*

Proof. Let $K = \mathbb{Q}(\zeta_3)$ and $K_{(\xi)} = \mathbb{Q}_3(\zeta_3)$. It suffices to see that α acquires a third root over the unique unramified cubic extension of local fields $K'/K_{(\xi)}$. We will consider elements in K' as power series in ξ but with coefficients in a fixed residue system of $\mathbb{F}_{27}$ in the unique unramified extension of $\mathbb{Q}_3$ of degree 3.

Noticing that $\zeta_3^2 = -1 - \zeta_3$ and hence $\xi^2 = -3\zeta_3$, and considering that $-\zeta_3 \equiv -1 \pmod{\xi}$, we can write

$$(1 + x\xi)^3 \equiv 1 + (-x + x^3)\xi^3 \pmod{\xi^4}.$$

We have $\alpha \equiv 1 + y\xi^3 \pmod{\xi^4}$ with $y \in \mathbb{F}_3$. The equation $-x + x^3 = y$ with $y \in \mathbb{F}_3$ is solvable in $\mathbb{F}_{27}$. We deduce that $(1 + x\xi)^3 \equiv \alpha \pmod{\xi^4}$ for some $x \in \mathbb{F}_{27}$ (notice that we can work with the residues in $\mathbb{F}_{27}$ because two representatives for x differ by an element of (ξ)). The ratio $\alpha/(1 + x'\xi)^3$, where x' is a lift of x, thus lies in

$$U^{(4)}_{K'} := \{z \in \mathcal{O}_{K'} \mid z \equiv 1 \pmod{\xi^4}\}.$$

Thus α has a third root in K' up to multiplication by some element of $U^{(4)}_{K'}$, but all those elements are third powers in K' by Lemma 6.

As for the second assertion, notice that $K(\sqrt[3]{\alpha}) = K(\sqrt[3]{-\alpha})$ and that if $K(\sqrt[3]{\alpha})$ and $K(\sqrt[3]{u\alpha})$ are both unramified at ξ, then $K(\sqrt[3]{u})$ is unramified at ξ, which implies that $u = \pm 1$. □

Proof of Theorem 1 (2). By Kummer theory there is some $\beta_p \in \mathbb{Q}(\zeta_3)$ such that $\sqrt[3]{\beta_p}$ generates the cubic extension inside $\mathbb{Q}(\zeta_{3p})$, which is unramified at ξ because $(3) = (\xi^2)$. Since this extension is invariant by complex conjugation, we are allowed to replace β_p by its complex conjugate. Up to multiplying β_p by a cube we may suppose that each prime ideal appearing in the factorization of the fractional ideal (β_p) has exponent either 1 or 2. Such prime ideals ramify in $\mathbb{Q}(\zeta_{3p})$ by [3, Lemma C.1.7 and its proof]. Since only the ideals over p ramify in the extension $\mathbb{Q}(\zeta_{3p})/\mathbb{Q}(\zeta_3)$, we deduce that

$$\beta_p = u \cdot \pi^x \cdot \overline{\pi}^y \tag{1}$$

where $u \in \mu_6$ is a unit and where $x, y \in \{0, 1, 2\}$. The exponents x and y cannot be both 0 by [3, Lemma C.1.7 and its proof] because p is totally ramified in $\mathbb{Q}(\zeta_p)/\mathbb{Q}$.

Since the extension $\mathbb{Q}(\zeta_{3p})$ is abelian over $\mathbb{Q}$ and invariant under complex conjugation, the fields $\mathbb{Q}(\zeta_3, \sqrt[3]{\beta_p})$ and $\mathbb{Q}(\zeta_3, \sqrt[3]{\overline{\beta_p}})$ must be equal. By Kummer theory we then have, up to cubes, either $\beta_p = \overline{\beta_p}$ or $\beta_p^2 = \overline{\beta_p}$. Thus in (1) it cannot be that exactly one among x and y is 0.

We can also exclude the cases $x = y = 1$ and $x = y = 2$ because then $\beta_p = u \cdot p$ or $\beta_p = u \cdot p^2$, which would imply that $\sqrt[3]{p}$ is contained in a cyclotomic extension of $\mathbb{Q}$. So we have found that $\{x, y\} = \{1, 2\}$, and, up to working with the complex conjugate of β_p instead, we have

$$\beta_p = u \cdot \pi^2 \cdot \overline{\pi} = u \cdot \pi p$$

for some $u \in \mu_6$.

We claim that $\pi p \equiv 1 \pmod{\xi^3}$. Since π and p are congruent to 1 modulo 3, we can write

$$\pi \equiv 1 + 3a \pmod{\xi^3}$$

$$p \equiv 1 + 3b \pmod{\xi^3}$$

with some $a, b \in \mathbb{F}_3 = \mathcal{O}/(\xi) = \{0, 1, 2\}$. Notice that ξ^3 and $\overline{\xi}^{\,3}$ generate the same ideal because $\overline{\xi} = 1 - \zeta_3^2$ gives $\overline{\xi}/\xi = 1 + \zeta_3 \in \mu_6$. The equation $\pi\overline{\pi} = p$ then gives

$$(1 + 3a)^2 \equiv 1 + 3b \pmod{\xi^3}$$

and therefore (since $9 \in (\xi^3)$) we have $3b \equiv 6a \pmod{\xi^3}$. Hence

$$\pi \cdot p \equiv (1 + 3a)(1 + 6a) \equiv 1 \pmod{\xi^3}$$

and the claim is proven. We conclude the proof by applying Proposition 7 to the element $\pi \cdot p$ and noticing that we may replace β_p by its opposite. □

3. The quartic subextension of $\mathbb{Q}(\zeta_{4p})/\mathbb{Q}(\zeta_4)$

Let p be a prime number such that $p \equiv 1 \pmod 4$. Let $\mathcal{O}$ be the ring of integers of $\mathbb{Q}(\zeta_4)$, and recall that $\mathcal{O}^\times = \mu_4$. Let $\xi := 1 - \zeta_4$.

Lemma 8. *Let K'' be the unique unramified extension of $\mathbb{Q}_2(\zeta_4)$ of degree 4. If $\alpha \in K''$ is a unit such that $v_{K''}(1 - \alpha) \geqslant 7$, then α is a fourth power.*

Proof. For $n \geqslant 1$, set

$$U^{(n)} := \{x \in \mathcal{O}_{K''} \mid x \equiv 1 \pmod{\xi^n}\}$$

and denote by $\overline{U^{(n)}}$ the image of $U^{(n)}$ in $(K'')^\times/(K'')^{\times 4}$. We have to show that $\overline{U^{(7)}}$ is trivial. We know that $\overline{U^{(9)}}$ is trivial by applying Hensel's Lemma to the polynomial $x^4 - a$ with value $x_0 = 1$ and $a \in U^{(8)}$, noticing that $v_{K''}(4) = 4$ and hence $v_{K''}(1 - a) > 2v_{K''}(4)$. Consider the two maps raising to the fourth power from $U^{(3)}/U^{(4)}$ onto $U^{(7)}/U^{(8)}$ and from $U^{(4)}/U^{(5)}$ onto $U^{(8)}/U^{(9)}$ (the four quotients are isomorphic to $\mathbb{F}_{16}$). They map an element $1 + a\xi^3 \pmod{\xi^4}$ to $1 + a\xi^7 \pmod{\xi^8}$, and an element $1 + a\xi^4 \pmod{\xi^5}$ to $1 + a\xi^8 \pmod{\xi^9}$, respectively, where $a \in \mathbb{F}_{16}$. Thus the two maps are surjective. We have found that any element of $U^{(8)}$ is an element of $U^{(9)}$ up to fourth powers, and hence $\overline{U^{(8)}} = \overline{U^{(9)}}$ is trivial.

We have also found that any element of $U^{(7)}$ is an element of $U^{(8)}$ up to fourth powers, and hence $\overline{U^{(7)}} = \overline{U^{(8)}}$ is trivial. □

Proposition 9. *If $\alpha \in \mathcal{O}$ is such that for some $y \in \{0,1\}$ we have*

$$\alpha \equiv 1 + (y + y\xi)\xi^4 \pmod{\xi^6},$$

then $\mathbb{Q}(\zeta_4, \sqrt[4]{\alpha})/\mathbb{Q}(\zeta_4)$ is unramified at (ξ). Moreover, among the elements $u\alpha$, with $u \in \mu_4$, only α has this ramification property.

Notice that when $y = 0$, then α is already a square (by reasoning as in Lemma 8).

Proof. Let $K = \mathbb{Q}(\zeta_4)$ and $K_{(\xi)} = \mathbb{Q}_2(\zeta_4)$. Let $K'' \supset K' \supset K_{(\xi)}$, where K'' is the unique unramified extension of degree 4 of $K_{(\xi)}$ and K' is the unique subextension of degree 2.

For the second assertion consider that if $K(\sqrt[4]{\alpha})$ and $K(\sqrt[4]{\zeta_4^n \alpha})$ are both unramified at (ξ), then the same holds for $K(\sqrt[4]{\zeta_4^n})$ and hence $\zeta_4^n = 1$.

For the first assertion it suffices to see that α acquires a fourth root in K''. We will work with a fixed representative system of the residue field taken in the unique unramified extension of $\mathbb{Q}_2$, so that the difference of any two lifts lies in $(2) = (\xi^2)$. Notice that $2 = \xi^2 - \xi^3$ hence $\pm 3 \equiv 1 \pmod{\xi^2}$, so we have:

$$\begin{aligned}(1+x\xi)^4 &= 1 + 4x\xi + 6x^2\xi^2 + 4x^3\xi^3 + x^4\xi^4 \\ &\equiv 1 + x\xi^5 + 3(\xi^2 - \xi^3)x^2\xi^2 + x^4\xi^4 \qquad \pmod{\xi^6} \\ &\equiv 1 + x\xi^5 + x^2\xi^4 + x^2\xi^5 + x^4\xi^4 \qquad \pmod{\xi^6}\end{aligned}$$

but $x^2 + x = y$ with $y \in \{0,1\}$ is solvable in $\mathbb{F}_4$ and hence also $x^4 + x^2 = (x^2 + x)^2 = y$. We then have $\alpha \equiv (1 + x\xi)^4 \pmod{\xi^6}$ with $x \in \mathcal{O}_{K'}/(\xi) \simeq \mathbb{F}_4$. So $\alpha/(1+x\xi)^4$ lies in

$$U^{(6)}_{K'} := \{x \in \mathcal{O}_{K'} \mid x \equiv 1 \pmod{\xi^6}\}.$$

This means that α has a fourth root in K' up to multiplication by an element of $U^{(6)}_{K'}$, which is of the form $1 + w\xi^6 \pmod{\xi^7}$, for some $w \in K'$. We can write

$$(1 + z\xi^2)^4 \equiv 1 + (z + z^2)\xi^6 \pmod{\xi^7},$$

but $z + z^2 = w$ with $w \in \mathbb{F}_4$ is solvable in $\mathbb{F}_{16}$, hence α has a fourth root in K'' up to an element of

$$U^{(7)}_{K''} := \{x \in \mathcal{O}_{K''} \mid x \equiv 1 \pmod{\xi^7}\}.$$

We can conclude because $U^{(7)}_{K''}$ consists of fourth powers by Lemma 8. □

Lemma 10. *Let $\pi \in \mathbb{Q}(\zeta_4)$ be such that $\pi \cdot \overline{\pi} = p$ holds. The element π can be chosen, by multiplying it with a root of unity, in such a way that*

$$\pi \cdot \overline{\pi}^3 \equiv 1 + (x + x\xi)\xi^4 \pmod{\xi^6}$$

holds for some $x \in \{0,1\}$. In particular, we have $\pi \cdot \overline{\pi}^3 \equiv 1 \pmod{4}$. The element π is then unique up to sign and up to complex conjugation.

Proof. We have $(\mathcal{O}/(\xi^3))^\times = \{\pm 1, \pm\zeta_4\}$ (the non-invertible elements are $0, 1-\zeta_4, \zeta_4-1, \zeta_4+1$) and $\mathcal{O}/(\xi) = \{0,1\} \simeq \mathbb{F}_2$. Up to multiplying π by a root of unity, we may thus suppose that $\pi \equiv 1 \pmod{\xi^3}$. Write

$$\pi \equiv 1 + (\lambda_0 + \lambda_1\xi)\xi^3 \pmod{\xi^5}$$

where $\lambda_0, \lambda_1 \in \{0,1\}$. Since $\overline{\xi} = \xi - \xi^2$ and hence $\overline{\xi} \equiv \xi + \xi^2 \pmod{\xi^4}$, we have

$$\overline{\pi} \equiv 1 + (\lambda_0 + (\lambda_1 + \lambda_0)\xi)\xi^3 \pmod{\xi^5}$$

$$\overline{\pi}\pi \equiv 1 + \lambda_0\xi^4 \pmod{\xi^5}.$$

The prime number p is either congruent to 1 or to $1-4$ modulo 8, which gives

$$p \equiv 1 \pmod{\xi^6} \quad \text{or} \quad p \equiv 1 + \xi^4 \pmod{\xi^6}$$

We also have

$$\overline{\pi}\pi = p \equiv 1 + \lambda_0\xi^4 \pmod{\xi^6}$$

and furthermore

$$\pi^2 \equiv 1 + \lambda_0\xi^5 \pmod{\xi^6}$$

thus

$$\overline{\pi}\pi^3 \equiv 1 + (\lambda_0 + \lambda_0\xi)\xi^4 \pmod{\xi^6}$$

as required. □

Proposition 11. *Let (π) be a prime of $\mathbb{Q}(\zeta_4)$ above p. Then there is exactly one element $\zeta \in \mu_4$ such that any of the fourth roots of*

$$\zeta \cdot \pi \cdot \overline{\pi}^3$$

generates the cyclic quartic subextension of $\mathbb{Q}(\zeta_{4p})$ over $\mathbb{Q}(\zeta_4)$. The element ζ is such that $\zeta \cdot \pi \cdot \overline{\pi}^3$ is congruent to 1 modulo 4.

Proof. Write $p\mathcal{O} = (\pi) \cdot (\overline{\pi})$. Let $\gamma_p \in \mathbb{Q}(\zeta_4)^\times$ be such that $\sqrt[4]{\gamma_p}$ generates the cyclic quartic subextension of $\mathbb{Q}(\zeta_{4p})$ over $\mathbb{Q}(\zeta_4)$. Up to multiplying this element by a fourth power in $\mathbb{Q}(\zeta_4)$, we may suppose that each prime ideal appearing in the factorization of the fractional ideal (γ_p) has exponent 1, 2 or 3. Such ideals must ramify in $\mathbb{Q}(\zeta_{4p})$ by [3, Lemma C.1.7 and its proof]. Since only the ideals over p ramify in the extension $\mathbb{Q}(\zeta_{4p})/\mathbb{Q}(\zeta_4)$, we deduce that

$$(\gamma_p) = (\pi)^x \cdot (\overline{\pi})^y$$

with $x, y \in \{0,1,2,3\}$. We cannot have $x = y = 0$ because the Kummer extension needs to be ramified at p, as p is totally ramified in $\mathbb{Q}(\zeta_p)$. We cannot have $x = y = 1$ or $x = y = 3$ because otherwise $\sqrt[4]{p}$ or $\sqrt[4]{p^3}$ would be contained in a cyclotomic extension of $\mathbb{Q}$. Since the quadratic subextension of $\mathbb{Q}(\zeta_{4p})/\mathbb{Q}(\zeta_4)$ is $\mathbb{Q}(\zeta_4, \sqrt{p})$, we must have that γ_p equals p times a square in $\mathbb{Q}(\zeta_4)$, so that $\{x, y\} = \{1, 3\}$. Thus we have

$$(\gamma_p) = (\pi) \cdot (\overline{\pi})^3 \qquad \text{or} \qquad (\gamma_p) = (\pi)^3 \cdot (\overline{\pi}).$$

Notice that γ_p and its third power generate the same Kummer extension. Thus, up to replacing γ_p with its third power, we may suppose that $(\gamma_p) = (\pi) \cdot (\overline{\pi})^3$ and hence that

$$\gamma_p = \zeta \cdot \pi \cdot \overline{\pi}^3$$

for some root of unity $\zeta \in \mu_4$. By Lemma 10 and Proposition 9 there is exactly one choice of ζ such that the field generated by $\sqrt[4]{\gamma_p}$ is unramified at 2 (as it is the case for the considered subextension of $\mathbb{Q}(\zeta_{4p})/\mathbb{Q}(\zeta_4)$), and this is exactly the choice that makes $\zeta \cdot \pi \cdot \overline{\pi}^3$ congruent to 1 modulo 4. □

Proof of Theorem 2. The result is a consequence of Lemma 10 and Proposition 11. □

Proof of Theorem 3. Let $\omega_p \in \mathbb{Q}(\sqrt{p})$ be such that $\sqrt{\omega_p}$ generates the quadratic extension of $\mathbb{Q}(\sqrt{p})$ inside $\mathbb{Q}(\zeta_p)$. Since p is the only prime number ramifying in $\mathbb{Q}(\zeta_p)$ and it is totally ramified, by [3, Lemma C.1.7 and its proof] the prime $(\sqrt{p})$ above p is the only prime ideal appearing in the factorization of the fractional ideal (ω_p) with odd valuation. So we can write $(\omega_p) = (\sqrt{p})I^2$ for some ideal I, and hence I^2 is principal. Since the class number of $\mathbb{Q}(\sqrt{p})$ is odd (see for example [5, Example 2.9]), I is principal. By working up to squares of elements in K, we may then suppose that $(\omega_p) = (\sqrt{p})$. So we can write $\omega_p = u\sqrt{p}$ where u is a unit. Since $\sqrt[4]{p}$ is not contained in a cyclotomic extension, the element u cannot be a root of unity. Up to squares of a fundamental unit, we may then suppose that u is a fundamental unit.

Considering the tower of quadratic extensions in $\mathbb{Q}(\zeta_p)$ we deduce that only the largest field is not fixed by complex conjugation, since this automorphism generates a subgroup of order 2. The quadratic extension of $\mathbb{Q}(\sqrt{p})$ is then totally imaginary if and only if it is that largest field, which means that $p \not\equiv 1 \pmod 8$. We have a totally imaginary field by adding $\sqrt{\omega_p} = \sqrt{u\sqrt{p}}$ if and only if the sign of $\sigma(u\sqrt{p})$ is negative for any embedding $\sigma : \mathbb{Q}(\sqrt{p}) \to \mathbb{R}$. □

4. Generators for Kummer extensions in terms of Gauss sums

Let q and p be prime numbers such that $p \equiv 1 \bmod q^n$ holds for some $n \geqslant 1$. We call $K = \mathbb{Q}(\zeta_{q^n})$ and $L = \mathbb{Q}(\zeta_{q^n p})$, and denote by K' the cyclic subextension of L/K of degree q^n. We call $\mathcal{O}_K$ the ring of integers of K: notice that, if $\wp \subset \mathcal{O}_K$ is a prime ideal over p, then we have a canonical isomorphism $\mathcal{O}_K/\wp \cong \mathbb{Z}/p\mathbb{Z}$.

Theorem 12. *We keep the above notation.*

(1) The prime ideals $\wp$ of $\mathcal{O}_K$ lying over p are in bijection with the surjective homomorphisms $\chi : (\mathbb{Z}/p\mathbb{Z})^* \to \mu_{q^n}$ obtained by defining $\chi(\zeta_{q^n} \bmod \wp) = (\zeta_{q^n})^{\frac{p-1}{q^n}}$.

(2) For each χ as above the element

$$g(\chi) := \sum_{a \in (\mathbb{Z}/p\mathbb{Z})^*} \chi(a)(\zeta_p)^a$$

generates K' and we have $G(\chi) := g(\chi)^{q^n} \in K$ thus $K' = K(\sqrt[q^n]{G(\chi)})$.

(3) If $\wp$ corresponds to χ, then we have the prime factorization

$$(G(\chi)) = \prod_{\substack{1 \leqslant x < q^n \\ (x,q)=1}} \sigma_x^{-1}(\wp)^x ,$$

where σ_x denotes the image of x under the isomorphism $(\mathbb{Z}/q^n\mathbb{Z})^* \cong \mathrm{Gal}(K/\mathbb{Q})$.

Proof. See [4, Chapter 14] or [7, Section 6]. For a nice proof of (3) see also [2, p. 605]. □

Let $q = 2$, $n \geqslant 2$ (thus $p \equiv 1 \bmod 4$), and consider the field diagram

$$\begin{tikzcd}
L' = \mathbb{Q}(\zeta_{2^{n-1}p}) \arrow[r, dash, "2"] \arrow[d, dash] & L = \mathbb{Q}(\zeta_{2^n p}) \arrow[d, dash] \\
K_2' \arrow[r, dash, "2"] \arrow[d, dash, "2^{n-1}"] & K_2 \arrow[d, dash, "2^{n-1}"] \\
K_1' = K'(\sqrt{p}) \arrow[r, dash, "2"] \arrow[d, dash, "2"] & K_1 = K(\sqrt{p}) \arrow[d, dash, "2"] \\
K' = \mathbb{Q}(\zeta_{2^{n-1}}) \arrow[r, dash] & K = \mathbb{Q}(\zeta_{2^n})
\end{tikzcd}$$

By Theorem 12 we have

$$K_2 = K(\sqrt[2^n]{G(\chi)}) = K_1\Big(\sqrt[2^{n-1}]{\sqrt{G(\chi)}}\Big)$$

and obviously $\sqrt{G(\chi)} \in K_1$. Let $\sigma \in \mathrm{Gal}(L/\mathbb{Q}) \cong (\mathbb{Z}/2^n\mathbb{Z})^* \times (\mathbb{Z}/p\mathbb{Z})^*$ be the canonical lift of the nontrivial automorphism of K/K', which corresponds to $(1 + 2^{n-1}, 1)$, and define

$$\xi := \big(g(\chi) + \sigma(g(\chi))\big)^{2^{n-1}}.$$

Note that ξ is easily computable by [6] in the basis

$$1, \zeta_{2^{n-1}}, \dots, \zeta_{2^{n-1}}^{\varphi(2^{n-1})-1}, \sqrt{p}, \zeta_{2^{n-1}}\sqrt{p}, \dots, \zeta_{2^{n-1}}^{\varphi(2^{n-1})-1}\sqrt{p}$$

of $K_1'/\mathbb{Q}$ by evaluating the Gauss sum.

Proposition 13. *With the above notation, we have $\xi \in K_1'$ and $K_2' = K_1'(\sqrt[2^{n-1}]{\xi})$.*

Proof. If $\tau \in \mathrm{Gal}(L/K_1) \subset (\mathbb{Z}/p\mathbb{Z})^*$, then $\tau(g(\chi)) = \chi(\tau)g(\chi)$ and since σ is the identity on $\mu_{2^{n-1}}$ then we also have $\tau\sigma(g(\chi)) = \chi(\tau)\sigma(g(\chi))$. Thus ξ is fixed by $\mathrm{Gal}(L/K_1)$ and it is in K_1' because it is fixed by σ. Since $\mathrm{Gal}(L/K_1) \cong \mathrm{Gal}(L'/K_1')$, we have shown that

$$\tau\big(g(\chi) + \sigma(g(\chi))\big) = \chi'(\tau)\big(g(\chi) + \sigma(g(\chi))\big)$$

where $\chi' : \mathrm{Gal}(L'/K_1') \to \mu_{2^{n-1}}$ is the restriction of χ and hence it is a surjective character with kernel $\mathrm{Gal}(L'/K_2')$. Furthermore $g(\chi) + \sigma(g(\chi)) \neq 0$ (by inspection of the formula for $g(\chi)$) and hence it generates K_2'. □

REFERENCES

[1] FESENKO, I.B. - VOSTOKOV, S.V.: *Local fields and their extensions*, volume 121 of Translations of Mathematical Monographs. American Mathematical Society, Providence, RI, second edition, 2002. ISBN 0-8218-3259-X. doi: 10.1090/mmono/121. `https://doi.org/10.1090/mmono/121`. With a foreword by I. R. Shafarevich.

[2] FRÖHLICH, A.: *Stickelberger without Gauss sums*, in Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), pages 589–607, 1977.

[3] HINDRY, M. - SILVERMAN, J. H.: *Diophantine geometry - An introduction*, Graduate Texts in Mathematics, **201**, Springer-Verlag, New York, 2000.

[4] IRELAND, K. - ROSEN, M. : *A classical introduction to modern number theory*, volume 84 of Graduate Texts in Mathematics. Springer-Verlag, New York, second edition, 1990. ISBN 0-387-97329- X. doi: 10.1007/978-1-4757-2103-4. URL https://doi.org/10.1007/978-1-4757-2103-4.

[5] MASLEY, J. M.: *Class numbers of real cyclic number fields with small conductor*, Compositio Math. **37** (1978), no. 3, 297–319.

[6] THE SAGE DEVELOPERS, *SageMath, the Sage Mathematics Software System (Version 9.2)*, https://www.sagemath.org, 2021.

[7] WASHINGTON, L. C.: *Introduction to cyclotomic fields*, volume 83 of Graduate Texts in Mathematics. Springer-Verlag, New York, 1982. ISBN 0-387-90622-3. doi: 10.1007/978-1-4684-0133-2. URL https://doi.org/10.1007/978-1-4684-0133-2.

MATHEMATISCHES INSTITUT, ALBERT-LUDWIGS-UNIVERSITÄT FREIBURG, ERNST-ZERMELO-STRASSE 1, D-79104 FREIBURG, GERMANY

Email address: fritz.hoermann@math.uni-freiburg.de

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF LUXEMBOURG, 6 AV. DE LA FONTE, 4364 ESCH-SUR-ALZETTE, LUXEMBOURG

Email address: antonella.perucca@uni.lu, pietro.sgobba@uni.lu, sebastiano.tronto@uni.lu