COLLOQUIUM MATHEMATICUM

VOL. 122 2011 NO. 1

SOME QUARTIC NUMBER FIELDS CONTAINING AN IMAGINARY QUADRATIC SUBFIELD

BY

STÉPHANE R. LOUBOUTIN (Marseille)

Abstract. Let ε be a quartic algebraic unit. We give necessary and sufficient conditions for (i) the quartic number field $K = \mathbb{Q}(\varepsilon)$ to contain an imaginary quadratic subfield, and (ii) for the ring of algebraic integers of K to be equal to $\mathbb{Z}[\varepsilon]$. We also prove that the class number of such K's goes to infinity effectively with the discriminant of K.

1. Introduction. People have studied parametrized families of number fields $K = \mathbb{Q}(\varepsilon)$ defined by $\mathbb{Q}$-irreducible monic polynomials $\Pi_\varepsilon(X) = X^n + a_{n-1}X^{n-1} + \cdots + a_1X \pm 1 \in \mathbb{Z}[X]$, for which algebraic units are known beforehand. From these units, they try to build a system of r independent algebraic units in K, where r is the rank of the unit group of the ring of algebraic integers of K. Then they try to find necessary and sufficient conditions for the rings of algebraic integers of these K's to be also known beforehand. In that way, they end up with families of number fields with known rings of algebraic integers and known regulators for which some information on their class numbers can be deduced.

The simplest situation is for $r = 1$, when K is either a real quadratic number field, or a non-totally real cubic number field, or a totally imaginary quartic number field. In [Lou06] we solved these questions for non-totally real cubic number fields, building on [Nag]. Here, we solve these questions for quartic number fields containing an imaginary quadratic subfield.

Throughout this paper, ε is a totally imaginary quartic algebraic unit. Let $\Pi_\varepsilon(X) = X^4 - aX^3 + bX^2 - cX + 1 \in \mathbb{Z}[X]$ be its $\mathbb{Q}$-irreducible monic minimal polynomial, of positive discriminant $d_\varepsilon > 0$. Let $K = \mathbb{Q}(\varepsilon)$ be the totally imaginary quartic number field generated by ε. Let d_K be the absolute value of its discriminant. By changing ε into $-\varepsilon$, $1/\varepsilon$ or $-1/\varepsilon$, we may assume that $|c| \le a$. By choosing another complex root of $\Pi_\varepsilon(X)$, we may also assume that $|\varepsilon| \ge 1$. We will prove the following result (used in [PL, proof of Th. 3]), which in our situation is more explicit than [PL, Th. 4]:

2010 *Mathematics Subject Classification*: Primary 11R16; Secondary 11R27, 11R29.
Key words and phrases: quartic number field, class number, fundamental unit.

DOI: 10.4064/cm122-1-13

THEOREM 1. *Let ε, with $|\varepsilon| \geq 1$, be a totally imaginary quartic unit whose minimal polynomial is of the form $\Pi_\varepsilon(X) = X^4 - aX^3 + bX^2 - cX + 1 \in \mathbb{Z}[X]$, with $|c| \leq a$. Then* (i) *the totally imaginary quartic number field $K = \mathbb{Q}(\varepsilon)$ contains an imaginary quadratic subfield and at the same time* (ii) *$\mathbb{Z}[\varepsilon]$ is the ring of algebraic integers of K if and only if we are in one of the following mutually exclusive seven cases:*

1. *$\Pi_\varepsilon(X) = X^4 - aX^3 + bX^2 - aX + 1$ with $b \geq 3$ and $1 \leq a \leq \sqrt{4b-11}$,* (i) *$b \equiv 0 \pmod 2$ implies $b \equiv 2a \pmod 4$,* (ii) *$b \equiv 1 \pmod 2$ implies $b \not\equiv a+1 \pmod 4$, and* (iii) *the odd parts of $b+2-2a$, $b+2+2a$ and $D_\varepsilon = 4b - 8 - a^2 > 0$ are square-free. In that case, $d_K = d_\varepsilon = ((b+2)^2 - 4a^2)D_\varepsilon^2$, $L = \mathbb{Q}(\sqrt{-D_\varepsilon})$ is the only quadratic subfield of K, $d_L = D_\varepsilon$, K is not normal, and $|\varepsilon|^2 \leq \sqrt{d_\varepsilon/9} + 6$.*
2. *$\Pi_\varepsilon(X) = X^4 - aX^3 + bX^2 + aX + 1$ with $b \geq -1$ and $1 \leq a \leq \sqrt{4b+5}$,* (i) *$b \not\equiv 0 \pmod 4$,* (ii) *$b \equiv 1 \pmod 2$ implies $b \not\equiv a+1 \pmod 4$,* (iii) *$(b-2)^2 + 4a^2 \equiv 0 \pmod{p^2}$ with $p \geq 3$ implies $b \equiv 2 \pmod p$, $a \equiv 0 \pmod p$ but $(b-2)^2 + 4a^2 \not\equiv 0 \pmod{p^3}$, and* (iv) *the odd part of $D_\varepsilon = 4b + 8 - a^2 > 0$ is square-free. In that case, $d_K = d_\varepsilon = ((b-2)^2 + 4a^2)D_\varepsilon^2$, $L = \mathbb{Q}(\sqrt{-D_\varepsilon})$ is the only quadratic subfield of K, $d_L = D_\varepsilon$, K is not normal, and $|\varepsilon|^2 \leq \sqrt{d_\varepsilon/9} + 6$.*
3. *$\Pi_\varepsilon(X) = X^4 - 2aX^3 + a^2X^2 + 1$ with $a \geq 1$, and the odd part of $a^4 + 16$ is square-free. In that case, $d_K = d_\varepsilon = 16(a^4+16)$, $L = \mathbb{Q}(\sqrt{-1})$ is the only quadratic subfield of K, $d_L = 4$, K is not normal, and $|\varepsilon|^2 \leq \sqrt{d_\varepsilon/16}$.*
4. *$\Pi_\varepsilon(X) = X^4 - 2aX^3 + (a^2-1)X^2 + aX + 1$ with $a \geq 1$, $a^4 + 4a^2 + 16 = 2^m 3^n N$ where $\gcd(6, N) = 1$ and N is square-free. In that case, $d_K = d_\varepsilon = 9(a^4 + 4a^2 + 16)$, $L = \mathbb{Q}(\sqrt{-3})$ is the only quadratic subfield of K, $d_L = 3$, K is not normal, and $|\varepsilon|^2 \leq \sqrt{d_\varepsilon/9} - 1$.*
5. *$\Pi_\varepsilon(X) = X^4 - 2aX^3 + (a^2+1)X^2 - aX + 1$ with $a \geq 3$, $a^4 - 4a^2 + 16 = 2^m 3^n N$ where $\gcd(6, N) = 1$ and N is square-free. In that case, $d_K = d_\varepsilon = 9(a^4 - 4a^2 + 16)$, $L = \mathbb{Q}(\sqrt{-3})$ is the only quadratic subfield of K, $d_L = 3$, K is not normal, and $|\varepsilon|^2 \leq \sqrt{d_\varepsilon/9} + 1$.*
6. *$\Pi_\varepsilon(X) = X^4 + bX^2 + 1$ with $b \geq 3$,* (i) *$b \equiv 0 \pmod 4$ or $b \equiv 3 \pmod 4$, and* (ii) *the odd parts of $b-2$ and $b+2$ are square-free. In that case, $K = \mathbb{Q}(\sqrt{-(b-2)}, \sqrt{-(b+2)})$ is abelian, $d_K = d_\varepsilon = 16(b^2-4)^2$ and $|\varepsilon|^2 = (b + \sqrt{b^2-4})/2 \leq \sqrt[4]{d_\varepsilon/16} + 1$.*
7. *$\Pi_\varepsilon(X) = X^4 + 1$, in which case $d_K = d_\varepsilon = 256$ and $K = \mathbb{Q}(\zeta_8)$; $\Pi_\varepsilon(X) = X^4 - X^2 + 1$ or $\Pi_\varepsilon(X) = X^4 - 4X^3 + 5X^2 - 2X + 1$, in which cases $d_K = d_\varepsilon = 144$ and $K = \mathbb{Q}(\zeta_{12})$; $\Pi_\varepsilon(X) = X^4 - 3X^3 + 2X^2 + 1$ or $\Pi_\varepsilon(X) = X^4 - 5X^3 + 8X^2 - 4X + 1$, in which cases $\mathbb{Z}[\varepsilon] = \mathbb{Z}[\eta]$ with $\Pi_\eta(X) = X^4 - 2X^3 + 2X^2 - X + 1$, $d_K = d_\varepsilon = 117$ and K is not normal.*

2. Containing an imaginary quadratic subfield. Our first step is to characterize in Theorem 2 when K contains an imaginary quadratic subfield. It will follow that we must be in one of the seven cases of Theorem 1. It will then remain to obtain in Section 3 necessary and sufficient conditions for the ring of algebraic integers of $\mathbb{Q}(\varepsilon)$ to be equal to $\mathbb{Z}[\varepsilon]$.

THEOREM 2. *Let ε be a quartic algebraic unit with $|\varepsilon| \geq 1$. The quartic number field $K = \mathbb{Q}(\varepsilon)$ contains an imaginary quadratic subfield if and only if we are in one of the following (not mutually exclusive) five cases:*

1. *$\Pi_\varepsilon(X) = X^4 - aX^3 + bX^2 - aX + 1$ with $b \geq 3$ and $|a| \leq \sqrt{4b-11}$. In that case, $d_\varepsilon = D_\varepsilon^2 f_\varepsilon$, where $D_\varepsilon = 4b - 8 - a^2 > 0$ and $f_\varepsilon = (b+2)^2 - 4a^2 > 0$,*

$$(2\varepsilon^3 - 2a\varepsilon^2 + (2b-2)\varepsilon - a)^2 = -D_\varepsilon, \tag{1}$$

$L = \mathbb{Q}(\sqrt{-D_\varepsilon}) \subseteq K$, and

$$|\varepsilon|^2 = \Big(b - 2 + \sqrt{f_\varepsilon} + \sqrt{2b^2 - 4a^2 - 8 + 2(b-2)\sqrt{f_\varepsilon}}\Big)/4 \leq \sqrt{d_\varepsilon/9} + 6. \tag{2}$$

2. *$\Pi_\varepsilon(X) = X^4 - aX^3 + bX^2 + aX + 1$ with $b \geq -1$ and $|a| \leq \sqrt{4b+5}$. In that case, $d_\varepsilon = D_\varepsilon^2 f_\varepsilon$, where $D_\varepsilon = 4b + 8 - a^2 > 0$ and $f_\varepsilon = (b-2)^2 + 4a^2 > 0$,*

$$(2\varepsilon^3 - 2a\varepsilon^2 + (2b+2)\varepsilon + a)^2 = -D_\varepsilon, \tag{3}$$

$L = \mathbb{Q}(\sqrt{-D_\varepsilon}) \subseteq K$, and

$$|\varepsilon|^2 = \Big(b + 2 + \sqrt{f_\varepsilon} + \sqrt{2b^2 + 4a^2 - 8 + 2(b+2)\sqrt{f_\varepsilon}}\Big)/4 \leq \sqrt{d_\varepsilon/9} + 6. \tag{4}$$

3. *$\Pi_\varepsilon(X) = X^4 - aX^3 + bX^2 - cX + 1$ with $a = 2A$ and $c = 2C$ even, and $b = (a^2 + c^2)/4 = A^2 + C^2$. In that case, $d_\varepsilon = D_\varepsilon^2 f_\varepsilon$ where $D_\varepsilon = 4(AC - 1)$ and $f_\varepsilon = (A^2 + C^2)^2 - 16(AC - 1) > 0$,*

$$\big(C\varepsilon^3 - (2AC-1)\varepsilon^2 + ((A^2+C^2)C - A)\varepsilon - C^2\big)/(AC-1) \tag{5}$$

is a complex primitive fourth root of unity, $L = \mathbb{Q}(\sqrt{-1}) \subseteq K$,

$$|\varepsilon|^2 = \Big(b + \sqrt{f_\varepsilon} + \sqrt{2b^2 - 4ac + 2b\sqrt{f_\varepsilon}}\Big)/4, \tag{6}$$

and ζ given in (5) is in $\mathbb{Z}[\varepsilon]$ if and only if $\Pi_\varepsilon(X) = X^4 - 4X^3 + 5X^2 - 2X + 1$ or $\Pi_\varepsilon(X) = X^4 - aX^3 + (a^2/4)X^2 + 1$, $a \geq 2$ even.

4. *$\Pi_\varepsilon(X) = X^4 - aX^3 + (B-1)X^2 - cX + 1$ with $B = (a^2 + ac + c^2)/3$ and $c \equiv a \pmod 3$. In that case, $d_\varepsilon = D_\varepsilon^2 f_\varepsilon$, where $D_\varepsilon = 3(AC - 1)$ and $f_\varepsilon = (B+4)^2 - 4(A+C)^2 > 0$, where $A = (2a + c)/3$ and $C = (a + 2c)/3$,*

$$\big(C\varepsilon^3 - (aC-1)\varepsilon^2 + (BC - A)\varepsilon - C^2\big)/(AC-1) \tag{7}$$

is a complex primitive third root of unity, $L = \mathbb{Q}(\sqrt{-3}) \subseteq K$,

(8) $$|\varepsilon|^2=\Big(B+\sqrt{f_\varepsilon}+\sqrt{2B^2-4B-4ac+2B\sqrt{f_\varepsilon}}\Big)/4,$$

and ζ given in (7) *is in $\mathbb{Z}[\varepsilon]$ if and only if $\Pi_\varepsilon(X)=X^4-3X^3+2X^2+1$ or $\Pi_\varepsilon(X)=X^4-aX^3+(a^2/4-1)X^2+(a/2)X+1$, $a\geq 0$ even.*

5. *$\Pi_\varepsilon(X)=X^4-aX^3+(B+1)X^2+cX+1$ with $B=(a^2+ac+c^2)/3$ and $c\equiv a \pmod 3$. In that case, $d_\varepsilon=D_\varepsilon^2 f_\varepsilon$, where $D_\varepsilon=3(AC+1)$ and $f_\varepsilon=(B-4)^2+4(A+C)^2>0$, where $A=(2a+c)/3$ and $C=(a+2c)/3$,*

(9) $$\big(-C\varepsilon^3+(aC+1)\varepsilon^2-(BC+A)\varepsilon-C^2\big)/(AC+1)$$

is a complex primitive third root of unity, $L=\mathbb{Q}(\sqrt{-3})\subseteq K$ and

(10) $$|\varepsilon|^2=\Big(B+\sqrt{f_\varepsilon}+\sqrt{2B^2+4B+4ac+2B\sqrt{f_\varepsilon}}\Big)/4,$$

and ζ given in (9) *is in $\mathbb{Z}[\varepsilon]$ if and only if $\Pi_\varepsilon(X)=X^4-5X^3+8X^2-4X+1$ or $\Pi_\varepsilon(X)=X^4-aX^3+(a^2/4+1)X^2-(a/2)X+1$, $a\geq 2$ even.*

Proof. Let L be an imaginary quadratic subfield of K. Then ε is quadratic over L, and $\varepsilon^2-\alpha\varepsilon+\beta=0$ for some algebraic integers $\alpha=(a+\sqrt{-D})/2$ and β of L, for some $D\geq 0$ such that $L=\mathbb{Q}(\sqrt{-D})$ if $D>0$. Hence,

$$\Pi_\varepsilon(X)=X^4-(\alpha+\bar\alpha)X^3+(|\alpha|^2+\beta+\bar\beta)X^2-(\alpha\bar\beta+\bar\alpha\beta)X+|\beta|^2.$$

Therefore, $|\beta|^2=1$, β is a complex root of unity in L and

$$\Pi_\varepsilon(X)=X^4-aX^3+((a^2+D)/4+2\Re(\beta))X^2-2\Re(\alpha\bar\beta)X+1.$$

There are eight cases to look at (with $\zeta_n=\exp(2\pi i/n)$):

β	$\Pi_\varepsilon(X)$
± 1	$X^4-aX^3+((a^2+D)/4\pm 2)X^2\mp aX+1$
$\pm\zeta_4$	$X^4-aX^3+\frac{a^2+D}{4}X^2\mp\sqrt{D}X+1$
$\pm\zeta_3$	$X^4-aX^3+((a^2+D)/4\mp 1)X^2\pm\frac{a-\sqrt{3D}}{2}X+1$
$\pm\zeta_3^2$	$X^4-aX^3+((a^2+D)/4\mp 1)X^2\pm\frac{a+\sqrt{3D}}{2}X+1$

The desired results follow. For example, if we are in the case $\beta=\zeta_3$ of this table, then $c=-(a-\sqrt{3D})/2$, hence $D=(a+2c)^2/3$ and $b=(a^2+D)/4-1$ $=(a^2+ac+c^2)/3-1$. Moreover,

$$\alpha=(a+\sqrt{-D})/2=(3a+\sqrt{-3}\sqrt{3D})/6=(3a+(2\zeta_3+1)(a+2c))/6$$
$$=((2a+c)+(a+2c)\zeta_3)/3,$$

$\beta=\zeta_3$, and $\varepsilon^2-\alpha\varepsilon+\beta=0$ yield $\zeta_3=(3\varepsilon^2-(2a+c)\varepsilon)/((a+2c)\varepsilon-3)$ and the formula given in (7).

Let us now explain how we obtained the formulae for $|\varepsilon|^2$. Assume that ε is a complex root of unity. Either (i) $\Pi_\varepsilon(X)=X^4+1$, we are in cases 2 (with $a=b=0$) and 3 (with $a=c=0$) and (4) and (6) are valid, or (ii)

$\Pi_\varepsilon(X) = X^4 - X^2 + 1$, we are in cases 2 (with $a = 0$ and $b = -1$) and 4 (with $a = c = 0$) and (4) and (8) are valid. Assume that ε is not a complex root of unity. Then $|\varepsilon| > 1$ ([Was, Lemma 1.6]). Let $x_1 = \varepsilon$, $x_2 = \bar{\varepsilon}$, $x_3 = \varepsilon'$ and $x_4 = \bar{\varepsilon}'$ be roots of $\Pi_\varepsilon(X) = X^4 - \sigma_1 X^3 + \sigma_2 X^2 - \sigma_3 X + \sigma_4$. The $x_i x_j$, $1 \le i < j \le 4$, are roots of

$$X^6 - \sigma_2 X^5 + (\sigma_1\sigma_3 - \sigma_4)X^4 - (\sigma_1^2\sigma_4 - 2\sigma_2\sigma_4 + \sigma_3^2)X^3 + (\sigma_1\sigma_3\sigma_4 - \sigma_4^2)X^2 - \sigma_2\sigma_4^2 X + \sigma_4^3.$$

Hence, $|\varepsilon|^2 > 1$ and $1/|\varepsilon|^2 < 1$ are real roots of

$$X^6 - bX^5 + (ac-1)X^4 - (a^2 - 2b + c^2)X^3 + (ac-1)X^2 - bX + 1.$$

The absolute values of the other complex roots $\varepsilon\varepsilon'$, $\varepsilon\bar{\varepsilon}'$, $\bar{\varepsilon}\varepsilon' = 1/\varepsilon\bar{\varepsilon}'$ and $\bar{\varepsilon}\bar{\varepsilon}' = 1/\varepsilon\varepsilon'$ are equal to 1. Therefore, $\rho = |\varepsilon|^2 + 1/|\varepsilon|^2 > 2$, $2\Re(\varepsilon\varepsilon') \in [-2, 2]$ and $2\Re(\varepsilon\bar{\varepsilon}') \in [-2, 2]$ are roots of $R_\varepsilon(X) = X^3 - bX^2 + (ac-4)X - (a^2 - 4b + c^2)$, with

$\Pi_\varepsilon(X)$	$R_\varepsilon(X)$
Case 1	$(X-2)(X^2 - BX + a^2 - 2b)$ where $B = b - 2$
Case 2	$(X+2)(X^2 - BX - a^2 + 2b)$ where $B = b + 2$
Case 3	$X(X^2 - BX + ac - 4)$ where $B = (a^2 + c^2)/4$
Case 4	$(X+1)(X^2 - BX + B + ac - 4)$ where $B = (a^2 + ac + c^2)/3$
Case 5	$(X-1)(X^2 - BX - B - ac - 4)$ where $B = (a^2 + ac + c^2)/3$

In these five cases, $2 < |\varepsilon|^2 + 1/|\varepsilon|^2 = \rho = (B + \sqrt{f_\varepsilon})/2$ is a root of a quadratic polynomial $X^2 - BX + C \in \mathbb{Z}[X]$ of positive discriminant $f_\varepsilon = B^2 - 4C$, and $|\varepsilon|^2 > 1$ yields

$$|\varepsilon|^2 = (\rho + \sqrt{\rho^2 - 4})/2 = \Big(B + \sqrt{f_\varepsilon} + \sqrt{2B^2 - 4C - 16 + 2B\sqrt{f_\varepsilon}}\Big)/4.$$

Finally, let us determine when ζ given in (5), (7) and (9) is in $\mathbb{Z}[\varepsilon]$.

Assume that ζ given in (5) is in $\mathbb{Z}[\varepsilon]$. Then $|C| \le A$ and $AC - 1 \ne 0$ (for otherwise $A = C = 1$ and $\Pi_\varepsilon(X) = X^4 - 2X^3 + 2X^2 - 2X + 1$ is $\mathbb{Q}$-reducible) and $AC - 1$ divides $2AC - 1$, hence divides 1. Therefore, either $AC = 2$, which on using $|C| \le A$ yields $A = 2$, $C = 1$, $\Pi_\varepsilon(X) = X^4 - 4X^3 + 5X^2 - 2X + 1$ and $\zeta = \varepsilon^3 - 3\varepsilon^2 + 3\varepsilon - 1 \in \mathbb{Z}[\varepsilon]$, or $AC = 0$, which on using $|C| \le A$ yields $C = 0$, $\Pi_\varepsilon(X) = X^4 - aX^3 + (a^2/4)X^2 + 1$ and $\zeta = -\varepsilon^2 + (a/2)\varepsilon \in \mathbb{Z}[\varepsilon]$.

Assume that ζ given in (7) is in $\mathbb{Z}[\varepsilon]$. Then $|C| \le A$ and $AC - 1 \ne 0$ (for otherwise $A = C = 1$, hence $a = c = 1$ and $\Pi_\varepsilon(X) = X^4 - X^3 - X + 1$ is $\mathbb{Q}$-reducible) and $AC - 1$ divides C. Therefore, either $C = 0$, $\Pi_\varepsilon(X) = X^4 - aX^3 + (a^2/4 - 1)X^2 + (a/2)X + 1$ and $\zeta = -\varepsilon^2 + (a/2)\varepsilon \in \mathbb{Z}[\varepsilon]$, or $C \ne 0$, which on using $1 \le |C| \le A$ yields $A = 2$ and $C = 1$, i.e. $a = 3$ and $c = 0$, $\Pi_\varepsilon(X) = X^4 - 3X^3 + 2X^2 + 1$ and $\zeta = \varepsilon^3 - 2\varepsilon^2 + \varepsilon - 1 \in \mathbb{Z}[\varepsilon]$.

Finally, the proof for ζ given by (9) is similar to the previous one. ∎

3. Proof of Theorem 1. By Theorem 2, we must be in one of the seven cases of Theorem 1 (for example, we are in cases 1 and 2 of Theorem 2 if and only if $a = 0$, which is dealt with in case 6 of Theorem 1). Moreover, either (i) K is not normal and contains only one imaginary quadratic subfield, or (ii) K is abelian and contains two distinct imaginary quadratic subfields. By using Theorem 2, we check that this latter possibility never occurs in cases 1–5 of Theorem 1.

3.1. Dedekind's criterion. Let ε be a complex root of a $\mathbb{Q}$-irreducible monic quartic polynomial $\Pi_\varepsilon(X) = X^4 - aX^3 + bX^2 - cX + 1 \in \mathbb{Z}[X]$ of discriminant d_ε. Let A_K and d_K be the ring of algebraic integers and the discriminant of the quartic number field $K = \mathbb{Q}(\varepsilon)$. Then $d_\varepsilon = (A_K : \mathbb{Z}[\varepsilon])^2 d_K$. If $p \geq 2$ is a prime, $\mathbb{Z}[\varepsilon]$ is called *p-maximal* if p does not divide the index $(A_K : \mathbb{Z}[\varepsilon])$. Therefore, A_K is equal to $\mathbb{Z}[\varepsilon]$ if and only if $\mathbb{Z}[\varepsilon]$ is p-maximal for any prime $p \geq 2$ such that p^2 divides d_ε.

LEMMA 3 (Dedekind's criterion, see [Coh, Theorem 6.1.4], [ABZ, Lemma 3.1]). *Let $p \geq 2$, where p^2 divides d_ε. Then $\mathbb{Z}[\varepsilon]$ is p-maximal if and only if*

(i) *$\Pi_\varepsilon(\alpha) \not\equiv 0 \pmod{p^2}$ for any $\alpha \in \mathbb{Z}$ such that $\Pi_\varepsilon(\alpha) \equiv \Pi'_\varepsilon(\alpha) \equiv 0 \pmod{p}$, which for $p = 2$ is equivalent to: $b \equiv a + c \equiv 0 \pmod 2$ implies $b \equiv a + c \pmod 4$,*

(ii) *if $\bar{\Pi}_\varepsilon(X) = \bar{Q}(X)^2$ in $\mathbb{F}_p[X]$, where $Q(X) = X^2 - AX + B \in \mathbb{Z}[X]$ is irreducible in $\mathbb{F}_p[X]$, then $\bar{Q}(X)$ does not divide $\bar{f}(X)$ in $\mathbb{F}_p[X]$, where $f(X) = (\Pi_\varepsilon(X) - Q(X)^2)/p \in \mathbb{Z}[X]$, which for $p = 2$ is equivalent to: $a \equiv b - 1 \equiv c \equiv 0 \pmod 2$ implies $a \not\equiv b - 1 \pmod 4$ or $c \not\equiv b - 1 \pmod 4$.*

Proof. We have $\Pi_\varepsilon(\alpha) \equiv \Pi'_\varepsilon(\alpha) \equiv 0 \pmod 2$ if and only if $\alpha \equiv 1 \pmod 2$ and $b \equiv a + c \equiv 0 \pmod 2$. In that case, $\Pi_\varepsilon(\alpha) \equiv \Pi_\varepsilon(1) \equiv 2 - (a + c) + b \pmod 4$, which proves the result for $p = 2$ in (i). Since X^2+X+1 is the only irreducible quadratic polynomial in $\mathbb{F}_2[X]$, since $\Pi_\varepsilon(X) \equiv (X^2 + X + 1)^2 \pmod 2$ if and only if $a \equiv b - 1 \equiv c \equiv 0 \pmod 2$, and since $X^2 + X + 1$ divides

$$f(X) = (\Pi_\varepsilon(X) - (X^2 + X + 1)^2)/2 = X\left(-\frac{a+2}{2}X^2 + \frac{b-3}{2}X - \frac{c+2}{2}\right)$$

in $\mathbb{F}_2[X]$ if and only if $(a+2)/2 \equiv (b-3)/2 \equiv (c+2)/2 \pmod 2$, we obtain the result for $p = 2$ in (ii). ∎

LEMMA 4. *Set $\Pi_\varepsilon(X) = X^4 - aX^3 + bX^2 - cX + 1 \in \mathbb{Z}[X]$. Let $p \geq 3$ be a prime. There exists $Q(X) = X^2 - AX + B \in \mathbb{Z}[X]$ irreducible in $\mathbb{F}_p[X]$ with $\bar{\Pi}_\varepsilon(X) = \bar{Q}(X)^2$ in $\mathbb{F}_p[X]$ such that $\bar{Q}(X)$ divides $\bar{f}(X)$ in $\mathbb{F}_p[X]$, where $f(X) = (\Pi_\varepsilon(X) - Q(X)^2)/p \in \mathbb{Z}[X]$, if and only if for $s = -1$ or for $s = +1$ we have* (i) *$c + sa \equiv 4b + 8s - a^2 \equiv 0 \pmod{p^2}$ and* (ii) *$a^2 + 16s$ is not a square mod p.*

If (a) $\Pi_\varepsilon(X) = X^4 - aX^3 + bX^2 - aX + 1$ *and the odd part of* $4b - 8 - a^2$ *is square-free, or if* (b) $\Pi_\varepsilon(X) = X^4 - aX^3 + bX^2 + aX + 1$, *the odd part of* $4b + 8 - a^2$ *is square-free and* p^4 *does not divide* $(b-2)^2 + 4a^2$, *then this does not happen.*

Proof. $\bar{\Pi}_\varepsilon(X) = \bar{Q}(X)^2$ in $\mathbb{F}_p[X]$ if and only if for $s = -1$ or for $s = +1$ we have $B \equiv -s \pmod p$, $2A \equiv a \pmod p$ and $b + 2s - A^2 \equiv c + 2sA \equiv 0 \pmod p$. It follows that $4b + 8s - a^2 \equiv c + sa \equiv 0 \pmod p$, and $Q(X) = X^2 - \frac{p+1}{2}aX - s$ is irreducible in $\mathbb{F}_p[X]$ if and only if $a^2 + 16s$ is not a square mod p. Then

$$f(X) = X\left(aX^2 + \frac{4b + 8s - (p+1)^2a^2}{4p}X - \frac{c + (p+1)sa}{p}\right)$$

and $\bar{Q}(X)$ divides $\bar{f}(X)$ in $\mathbb{F}_p[X]$ if and only if

$$\frac{4b + 8s - (p+1)^2a^2}{4p} \equiv -\frac{p+1}{2}a^2 \pmod p$$

and

$$\frac{c + (p+1)sa}{p} \equiv sa \pmod p,$$

i.e. if and only if $4b + 8s - a^2 \equiv c + sa \equiv 0 \pmod{p^2}$.

For the last assertion, in case (a) we must choose $s = +1$ in (i) (the odd part of $4b - 8 - a^2$ being square-free), and we would have $c + a = 2a \equiv 0 \pmod{p^2}$, hence $a \equiv 0 \pmod p$, and $a^2 + 16s = a^2 + 16 \equiv 16 \pmod p$ would be a square mod p, a contradiction. In case (b), we must choose $s = -1$ in (i) (the odd part of $4b + 8 - a^2$ being square-free), and we would have $c - a = -2a \equiv 0 \pmod{p^2}$, hence $a \equiv 0 \pmod{p^2}$, and $4b - 8 - a^2 \equiv 0 \pmod{p^2}$ would imply $b \equiv 2 \pmod{p^2}$ and p^4 would divide $(b-2)^2 + 4a^2$, a contradiction. ∎

3.2. Proof of Theorem 1. It remains to prove the necessary and sufficient conditions for $\mathbb{Z}[\varepsilon]$ to be the ring of algebraic integers of $\mathbb{Q}(\varepsilon)$.

1. The first case. By Lemma 3, conditions (i) and (ii) combined are equivalent to $\mathbb{Z}[\varepsilon]$ being 2-maximal. Now, assume that the odd part of $b + 2 - 2a$ (respectively, of $b + 2 + 2a$) is not square-free. There exists a prime $p \geq 3$ whose square divides it and we have $\Pi_\varepsilon(1) = b + 2 - 2a \equiv 0 \pmod{p^2}$ and $\Pi'_\varepsilon(1) = 2(b+2-2a) \equiv 0 \pmod p$ (respectively, $\Pi_\varepsilon(-1) = b+2+2a \equiv 0 \pmod{p^2}$ and $\Pi'_\varepsilon(-1) = -2(b + 2 + 2a) \equiv 0 \pmod p$). Hence, $\mathbb{Z}[\varepsilon]$ is not p-maximal, by Lemma 3, and $A_K \neq \mathbb{Z}[\varepsilon]$. If the odd part of D_ε is not square-free, then $A_K \neq \mathbb{Z}[\varepsilon]$, by (1).

Conversely, assume that the odd parts of $b + 2 - 2a$, $b + 2 + 2a$ and $D_\varepsilon = 4b - 8 - a^2$ are square-free, and let us prove that $\mathbb{Z}[\varepsilon]$ is p-maximal for any prime $p \geq 3$ whose square divides $d_\varepsilon = (b + 2 - 2a)(b + 2 + 2a)D_\varepsilon^2$. By

Lemmas 3 and 4, it suffices to prove that $\Pi_\varepsilon(\alpha) \not\equiv 0 \pmod{p^2}$ for any $\alpha \in \mathbb{Z}$ which is a double root of $\Pi_\varepsilon(X)$ modulo p (i.e., such that $\Pi_\varepsilon(\alpha) \equiv \Pi'_\varepsilon(\alpha) \equiv 0 \pmod{p}$).

First, if p divides $b+2-2a$ or $b+2+2a$, then $\Pi_\varepsilon(X) \equiv (X-1)^2(X^2-(a-2)X+1) \pmod{p}$ or $\Pi_\varepsilon(X) \equiv (X+1)^2(X^2-(a+2)X+1) \pmod{p}$. Hence, $\alpha \equiv \pm 1 \pmod{p}$ and $\Pi_\varepsilon(\alpha) \equiv \Pi_\varepsilon(\pm 1) = b+2 \mp 2a \not\equiv 0 \pmod{p^2}$.

Second, if p divides $D_\varepsilon = 4b-8-a^2$, then $\Pi_\varepsilon(X) \equiv (X^2 - \frac{a}{2}X + 1)^2 \pmod{p}$. Hence, $\alpha^2 - \frac{a}{2}\alpha + 1 \equiv 0 \pmod{p}$, $\alpha \not\equiv 0 \pmod{p}$, $\frac{a}{2}\alpha - 1 \equiv \alpha^2 \not\equiv 0 \pmod{p}$, and

$$\Pi_\varepsilon(X) = \left(X^2 - \frac{a}{2}X + 1\right)^2 + \frac{D_\varepsilon}{4}\left(X^2 - \frac{a}{2}X + 1\right) + \frac{D_\varepsilon}{4}\left(\frac{a}{2}X - 1\right)$$

yields $\Pi_\varepsilon(\alpha) \equiv \frac{D_\varepsilon}{4}\left(\frac{a}{2}\alpha - 1\right) \not\equiv 0 \pmod{p^2}$.

2. The second case. By Lemma 3, conditions (i) and (ii) together are equivalent to $\mathbb{Z}[\varepsilon]$ being 2-maximal. Now, assume that (iii) is not satisfied, i.e. that $(b-2)^2 + 4a^2 \equiv 0 \pmod{p^2}$ for some prime $p \geq 3$ and that either $b \not\equiv 2 \pmod{p}$, $a \not\equiv 0 \pmod{p}$ or $(b-2)^2 + 4a^2 \equiv 0 \pmod{p^3}$. If $p \equiv 3 \pmod 4$, then $b \equiv 2 \pmod{p^2}$, $a \equiv 0 \pmod{p^2}$, $\Pi_\varepsilon(X) \equiv Q(X)^2 \pmod{p^2}$, where $Q(X) = X^2+1$ is irreducible in $\mathbb{F}_p[X]$. Hence, $\mathbb{Z}[\varepsilon]$ is not p-maximal, by Lemma 3(ii), and $A_K \neq \mathbb{Z}[\varepsilon]$. If $p \equiv 1 \pmod 4$, then there exists $\zeta \in \mathbb{Z}$ such that $\zeta^2 \equiv -1 \pmod{p^3}$. If $b \not\equiv 2 \pmod{p}$ or $a \not\equiv 2 \pmod{p}$, then p cannot divide both $b-2-2a\zeta$ and $b-2+2a\zeta$. Since $(b-2-2a\zeta)(b-2+2a\zeta) \equiv (b-2)^2 + 4a^2 \equiv 0 \pmod{p^2}$, we may assume that $b-2-2a\zeta \equiv 0 \pmod{p^2}$. If neither $b \not\equiv 2 \pmod{p}$ nor $a \not\equiv 2 \pmod{p}$, then $(b-2-2a\zeta)(b-2+2a\zeta) \equiv (b-2)^2 + 4a^2 \equiv 0 \pmod{p^3}$ and we may assume that $b-2-2a\zeta \equiv 0 \pmod{p^2}$. In both cases, we obtain $\Pi_\varepsilon(\zeta) = -(b-2-2a\zeta) \equiv 0 \pmod{p^2}$, $\Pi'_\varepsilon(\zeta) = 2\zeta(b-2-2a\zeta) \equiv 0 \pmod{p}$, and $\mathbb{Z}[\varepsilon]$ is not p-maximal, by Lemma 3, and $A_K \neq \mathbb{Z}[\varepsilon]$. If (iv) is not satisfied, i.e. if the odd part of D_ε is not square-free, then $A_K \neq \mathbb{Z}[\varepsilon]$, by (1).

Conversely, assume that (iii) and (iv) are satisfied, and let us prove that $\mathbb{Z}[\varepsilon]$ is p-maximal for any prime $p \geq 3$ whose square divides $d_\varepsilon = ((b-2)^2+4a^2)D_\varepsilon^2$. By Lemmas 3 and 4, it suffices to prove that $\Pi_\varepsilon(\alpha) \not\equiv 0 \pmod{p^2}$ for any $\alpha \in \mathbb{Z}$ which is a double root of $\Pi_\varepsilon(X) \bmod p$.

First, assume that p divides $D_\varepsilon = 4b+8-a^2$, whose odd part is square-free, by assumption. Then $\Pi_\varepsilon(X) \equiv (X^2 - \frac{a}{2}X - 1)^2 \pmod{p}$. Hence, $\alpha^2 - \frac{a}{2}\alpha - 1 \equiv 0 \pmod{p}$, $\alpha \not\equiv 0 \pmod{p}$, $\frac{a}{2}\alpha + 1 \equiv \alpha^2 \not\equiv 0 \pmod{p}$, and

$$\Pi_\varepsilon(X) = \left(X^2 - \frac{a}{2}X - 1\right)^2 + \frac{D_\varepsilon}{4}\left(X^2 - \frac{a}{2}X - 1\right) + \frac{D_\varepsilon}{4}\left(\frac{a}{2}X + 1\right)$$

yields $\Pi_\varepsilon(\alpha) \equiv \frac{D_\varepsilon}{4}(\frac{a}{2}\alpha + 1) \not\equiv 0 \pmod{p^2}$.

Second, assume that p does not divide $D_\varepsilon = 4b+8-a^2$. Then p^2 divides $(b-2)^2+4a^2$, hence $b \equiv 2 \pmod p$ and $a \equiv 0 \pmod p$, by assumption, and $\Pi_\varepsilon(X) \equiv (X^2+1)^2 \pmod p$. If $p \equiv 3 \pmod 4$, then $\Pi_\varepsilon(X)$ has no double root modulo p. If $p \equiv 1 \pmod 4$ and $\zeta \in \mathbb{Z}$ is such that $\zeta^2 \equiv -1 \pmod{p^3}$, then $\alpha \equiv \pm\zeta \pmod p$ and $\Pi_\varepsilon(\alpha) \equiv \Pi_\varepsilon(\pm\zeta) = -(b-2\mp 2a\zeta) \not\equiv 0 \pmod{p^2}$ for otherwise we would have $(b-2)^2+4a^2 \equiv 0 \pmod{p^3}$.

3. The third case. If the odd part of $d_\varepsilon = 16(a^4+16)$ is not square-free, then there exists a prime $p \geq 3$ whose square divides d_ε and we have $\Pi_\varepsilon(a/2) = d_\varepsilon/256 \equiv 0 \pmod{p^2}$ and $0 = \Pi'_\varepsilon(a/2) \equiv 0 \pmod p$. Hence, $\mathbb{Z}[\varepsilon]$ is not p-maximal, by Lemma 3, and $A_K \neq \mathbb{Z}[\varepsilon]$. Conversely, if the odd part of d_ε is square-free, then $p=2$ is the only prime whose square divides d_ε and $\mathbb{Z}[\varepsilon]$ is 2-maximal, by Lemma 3. Hence, $A_K = \mathbb{Z}[\varepsilon]$.

4. The fourth case. If the square of a prime $p > 3$ divides $d_\varepsilon = 9(a^4 \pm 4a^2+16)$, we have $\Pi_\varepsilon(a/2) = d_\varepsilon/144 \equiv 0 \pmod{p^2}$ and $0 = \Pi'_\varepsilon(a/2) \equiv 0 \pmod p$. Hence, $\mathbb{Z}[\varepsilon]$ is not p-maximal, by Lemma 3, and $A_K \neq \mathbb{Z}[\varepsilon]$. Conversely, if $d_\varepsilon = 2^m 3^n d'_\varepsilon$ with $\gcd(6, d'_\varepsilon) = 1$ and d'_ε square-free, then $p=2$ and $p=3$ are the only primes whose squares can divide d_ε. Since $\mathbb{Z}[\varepsilon]$ is 2-maximal, by Lemma 3, and 3-maximal, we have $A_K = \mathbb{Z}[\varepsilon]$. Indeed:

LEMMA 5. *If* $\Pi_\varepsilon(X) = X^4 - 2aX^3 + (a^2-s)X^2 + saX + 1 \in \mathbb{Z}[X]$, $s \in \{\pm 1\}$, *then* $\mathbb{Z}[\varepsilon]$ *is* 3*-maximal.*

Proof. By Lemma 4, we cannot be in the situation of Lemma 3(ii) (for $4b-8-a^2 = 4(a^2-s)-8-a^2 \not\equiv 0 \pmod{3^2}$ and $4b+8-a^2 = 4(a^2-s)+8-a^2 \not\equiv 0 \pmod{3^2}$). Now, since $\Pi_\varepsilon(X) \equiv (X^2 - aX + s)^2 \pmod 3$, it follows that if $\alpha \in \mathbb{Z}$ is a double root of $\Pi_\varepsilon(X)$ modulo 3, then $\alpha \not\equiv 0 \pmod 3$, $\alpha \not\equiv a \pmod 3$ and $\Pi_\varepsilon(\alpha) \equiv \Pi_\varepsilon(\alpha) - (\alpha^2 - a\alpha + s)^2 \equiv -3s\alpha(\alpha - a) \not\equiv 0 \pmod{3^2}$. ∎

5. The fifth case. The proof is similar to the previous one.

6 & 7. The sixth and seventh cases. The proof is easy.

4. Conclusion. Let $K = \mathbb{Q}(\varepsilon)$ be a quartic number field containing an imaginary quadratic subfield L, where ε with $|\varepsilon| \geq 1$ is a totally imaginary quartic unit. As in Theorem 1, assume that K contains an imaginary quadratic subfield L and that $\mathbb{Z}[\varepsilon]$ is the ring of algebraic integers of K. By [Lou05, Corollary 11], if K is not normal, we have an explicit lower bound

$$h_K \mathrm{Reg}_K \gg \sqrt{d_K/d_L}/\log^2(d_K/d_L) \gg d_K^{3/8}/\log^2 d_K,$$

in cases 1 and 2 of Theorem 1 (for $d_K \gg d_L^4$ and $d_K/d_L \gg d_K^{3/4}$ in these two cases), and we have the better lower bound

$$h_K \mathrm{Reg}_K \gg \sqrt{d_K}/\log d_K$$

if $d_L = 3$ or 4, i.e. in cases 3, 4 and 5 of Theorem 1. From our explicit upper bounds on $|\varepsilon|^2$ (Theorem 1), we obtain $\mathrm{Reg}_K \leq 2\log|\varepsilon| \ll \log d_K$. Hence, h_K goes effectively to infinity as d_K goes to infinity. As in [Lou06], we could determine all these K's of class number one by using the method explained in [Lou95] (by noticing that ε is a fundamental unit of the order $\mathbb{Z}[\varepsilon]$, except in six cases, by [Lou08, Theorem 10], and by using [BP] for the special case that K is abelian, i.e. in case 6 of Theorem 1). However, while we were completing this paper, we learnt about [PL] in which the determination of all the totally imaginary quartic number fields $K = \mathbb{Q}(\varepsilon)$ with class number one is completed, provided that (i) ε is a totally imaginary quartic algebraic unit and (ii) the ring of algebraic integers of K is equal to $\mathbb{Z}[\varepsilon]$. In fact, they proved that in this situation, h_K goes effectively to infinity as d_K goes to infinity (see [PL, Theorem 3]).

REFERENCES

[ABZ] A. Ash, J. Brakenhoff and T. Zarrabi, *Equality of polynomial and field discriminants*, Experiment. Math. 16 (2007), 367–374.

[BP] E. Brown and C. J. Parry, *The imaginary bicyclic biquadratic fields with class-number 1*, J. Reine Angew. Math. 266 (1974), 118–120.

[Coh] H. Cohen, *A Course in Computational Algebraic Number Theory*, 4th printing, Grad. Texts in Math. 138, Springer, 2000.

[Lou95] S. Louboutin, *Calcul du nombre de classes des corps de nombres*, Pacific J. Math. 171 (1995), 455–467.

[Lou05] —, *The Brauer–Siegel theorem*, J. London Math. Soc. (2) 72 (2005), 40–52.

[Lou06] —, *The class-number one problem for some real cubic number fields with negative discriminants*, J. Number Theory 121 (2006), 30–39.

[Lou08] —, *The fundamental unit of some quadratic, cubic or quartic orders*, J. Ramanujan Math. Soc. 23 (2008), 191–210.

[Nag] T. Nagell, *Zur Theorie der kubischen Irrationalitäten*, Acta Math. 55 (1930), 33–65.

[PL] S.-M. Park and G.-N. Lee, *The class number one problem for some totally complex quartic number fields*, J. Number Theory 129 (2009), 1338–1349.

[Was] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, 1997.

Stéphane R. Louboutin
Institut de Mathématiques de Luminy, UMR 6206
163, avenue de Luminy, Case 907
13288 Marseille Cedex 9, France
E-mail: loubouti@iml.univ-mrs.fr

Received 8 September 2009;
revised 1 December 2010 (5269)