The CM-fields with Class Number One which are Hilbert Class Fields of Quadratic Fields

By Stéphane LOUBOUTIN

Département de Mathématiques, U. F. R. Sciences, Université de Caen, France

(Communicated by Shokichi IYANAGA, M. J. A., Jan. 12, 1996)

It is known that there are only finitely many normal CM-fields with class number one (see [3]). Moreover, all the imaginary abelian number fields with call number one have been determined by K. Yamamura: There are 172 such fields. Hence, it is time to determine all the non-abelian normal CM-fields with class number one. The author and R. Okazaki in [7] found all the non-abelian normal octic CM-fields with class number one: There are 17 such fields, all of which are dihedral and narrow Hilbert class fields of real quadratic fields. Then, the author, R. Okazaki and M. Olivier in [4] found all the non-abelian normal CM-fields of degree 12 with class number one: There are 9 such fields, all of which are dehedral. We shall explain in this note how we determine in [6] all CM-fields $\boldsymbol{H}_s(\boldsymbol{k})$ with class number one (without fixing their degrees) which are narrow Hilbert class fields of quadratic fields $\boldsymbol{k}$: There are at least 95 such fields, and assuming a conjecture put forward in [5], there are exactly 95 such fields. All the proofs of the results stated here may be found in [6]. Note that 4 of them have degree 16,1 of them has degree 20 and 1 of them has degree 24, these six fields being non-abelian normal dihedral CM-fields.

We let $\boldsymbol{G}_{\boldsymbol{k}}$ be the genus field of $\boldsymbol{k}$, which is the maximal abelian number field that is unramified over $\boldsymbol{k}$ at all the finite places. In this paper, genus field will always stand for genus field of some quadratic field. The Hilbert class field (in larger sense) $\boldsymbol{H}_l(\boldsymbol{k})$ of a real quadratic field is totally real. Hence, it is not a CM-field. However, one can easily prove that the narrow Hilbert class field $\boldsymbol{H}_s(\boldsymbol{k})$ of a real quadratic field $\boldsymbol{k}$ is a CM-field if and only if the norm of the fundamental unit of $\boldsymbol{k}$ is equal to $+1$, which we will assume for the rest of this paper. In that case, $\boldsymbol{H}_l(\boldsymbol{k})$ is the maximal totally real subfield of $\boldsymbol{H}_s(\boldsymbol{k})$.

1. Let us first focus on Hilbert class fields of imaginary quadratic fields.

Theorem 1 (See [2, proof of Th. 6.1]). *Let $\boldsymbol{k}$ be an imaginary quadratic field. Let $\boldsymbol{H}_s(\boldsymbol{k})$ be the Hilbert class field of $\boldsymbol{k}$. Then, $\boldsymbol{H}_s(\boldsymbol{k})$ is Galois and its Galois group* $\mathrm{Gal}(\boldsymbol{H}_s(\boldsymbol{k})/\boldsymbol{Q})$ *is a generalized dihedral group which is a semi-direct product of* $\boldsymbol{A} = \mathrm{Gal}(\boldsymbol{H}_s(\boldsymbol{k})/\boldsymbol{k})$ *which is canonically isomorphic to the ideal class group of $\boldsymbol{k}$ with* $\{\mathrm{Id}, c\}$ *where the complex conjugation c acts on $\boldsymbol{A}$ via $cac^{-1} = a^{-1}$.*

Now, an imaginary normal number field is a CM-field if and only if the complex conjugation is in the center of its Galois group. Hence, the Hilbert class field $\boldsymbol{H}_s(\boldsymbol{k})$ of an imaginary quadratic field $\boldsymbol{k}$ is a CM-field if and only if the ideal class group of $\boldsymbol{k}$ has exponent ≤ 2, in which case $\boldsymbol{H}_s(\boldsymbol{k}) = \boldsymbol{G}_{\boldsymbol{k}}$. Hence, we have only to determine all imaginary genus fields $\boldsymbol{G}_{\boldsymbol{k}} = \boldsymbol{Q}(\sqrt{p_1^*}, \cdots, \sqrt{p_t^*})$ with class number one. Here, $\boldsymbol{k} = \boldsymbol{Q}(\sqrt{p_1^* p_2^* \cdots p_t^*})$ has discriminant $p_1^* p_2^* \cdots p_t^*$, where $p_1, p_2, \cdots, p_t$ are $t \geq 1$ distinct primes and

$$p_i^* = \begin{cases} p_i & \text{if } p_i \equiv 1 \pmod 4, \\ -p_i & \text{if } p_i \equiv 3 \pmod 4, \\ -4,\ -8 \text{ or } 8 & \text{if } p_i \equiv 2. \end{cases}$$

Note that $\boldsymbol{G}_{\boldsymbol{k}}$ has degree 2^t. In fact, it is easy to determine all imaginary genus fields with relative class number one, and then to compute the class numbers of their maximal real subfields. To this end, we prove that if $\boldsymbol{G}$ and $\boldsymbol{G}'$ are two imaginary genus fields such that $\boldsymbol{G} \subseteq \boldsymbol{G}'$ then the relative class number of $\boldsymbol{G}$ divides that of $\boldsymbol{G}'$, and if $\boldsymbol{G}_{\boldsymbol{k}}$ has odd relative class number, then $t \leq 3$. As all the imaginary quadratic fields with class number ≤ 2 are known, we get (see [6]):

Theorem 2. *There are exactly* 73 *imaginary genus fields $\boldsymbol{G}_{\boldsymbol{k}} = \boldsymbol{Q}(\sqrt{p_1^*}, \cdots, \sqrt{p_t^*})$ with relative class number one: those which appear in the follow-*

1991 *Mathematics Subject Classification*. Primary 11R29; Secondary 11 R37, 11R20.

ing Table I. *Note that* 30 *out of them are genus fields of imaginary quadratic fields* $\boldsymbol{k}$, *and* 43 *out of them are genus fields of real quadratic fields* $\boldsymbol{k}$. *Only* 4 *out of them do not have class number one, those which are the genus fields of the four following real quadratic fields* $\boldsymbol{k}: \boldsymbol{Q}(\sqrt{7\cdot 67})$, $\boldsymbol{Q}(\sqrt{2\cdot 163})$, $\boldsymbol{Q}(\sqrt{11\cdot 43})$ *in which cases* $\boldsymbol{G_k}$ *and* $\boldsymbol{k}$ *have class number* 3, *and* $\boldsymbol{Q}(\sqrt{19\cdot 43})$ *in which case* $\boldsymbol{G_k}$ *and* $\boldsymbol{k}$ *have class number* 5.

Corollary 3 (to Th. 1 and Th. 2). *There are exactly* 30 *CM-fields with class number one which are Hilbert class fields of imaginary quadratic fields. All these fields are abelian.*

2. Let us now focus on narrow Hilbert class fields of real quadratic fields $\boldsymbol{k}$, which are always CM-fields since we still assume that the fundamental unit of $\boldsymbol{k}$ has norm $+1$.

Theorem 4. *Let* $\boldsymbol{k}$ *be a real quadratic field. Let* $\boldsymbol{H}_s(\boldsymbol{k})$ *be the narrow Hilbert class field of* $\boldsymbol{k}$. *Then,* $\boldsymbol{H}_s(\boldsymbol{k})$ *is a normal CM-field and its Galois group* $\boldsymbol{G} = \mathrm{Gal}(\boldsymbol{H}_s(\boldsymbol{k})/\boldsymbol{Q})$ *is a generalized dihedral group which is a semi-direct product* $\boldsymbol{G} = \boldsymbol{A} \rtimes \{\mathrm{Id}, \sigma\}$ *of* $\boldsymbol{A} = \mathrm{Gal}(\boldsymbol{H}_s(\boldsymbol{k})/\boldsymbol{k})$ *which is canonically isomorphic to the narrow ideal class group of* $\boldsymbol{k}$ *with* $\{\mathrm{Id}, \sigma\}$ *which acts on* $\boldsymbol{A}$ *via* $\sigma a \sigma^{-1} = a^{-1}$. *Here* σ *is any element of* $\boldsymbol{G} = \mathrm{Gal}(\boldsymbol{H}_s(\boldsymbol{k})/\boldsymbol{Q})$ *whose restriction to* $\boldsymbol{k}$ *is non trivial, which implies that* σ *has order* 2 *in* $\boldsymbol{G}$.

Hence, the narrow Hilbert class field $\boldsymbol{H}_s(\boldsymbol{k})$ of a real quadratic field $\boldsymbol{k}$ is abelian if and only if the narrow ideal class group of $\boldsymbol{k}$ has exponent ≤ 2, in which case $\boldsymbol{H}_s(\boldsymbol{k}) = \boldsymbol{G_k}$.

Corollary 5 (to Th. 2 and Th. 4). *There are exactly* 39 *imaginary abelian number fields with class number one which are Hilbert class fields of real quadratic fields.*

Let $\boldsymbol{k}$ be any one of the four real quadratic fields whose genus fields have class numbers greater than one given in Theorem 2. According to explicit constructions of their Hibert class fields $\boldsymbol{H}_s(\boldsymbol{k})$, and to the computation of the class numbers of these $\boldsymbol{H}_s(\boldsymbol{k})$ by using the system for computational number theory Pari/GP (see [1]) we get:

Theorem 6. *Let* $\boldsymbol{k}$ *be a real quadratic field and* $\boldsymbol{M}$ *a CM-field such that* $\boldsymbol{k} \subseteq \boldsymbol{M} \subseteq \boldsymbol{H}_s(\boldsymbol{k})$. *If* $\boldsymbol{H}_s(\boldsymbol{k})$ *has class number one, then* $\boldsymbol{M}$ *has relative class number one and class number equal to the degree* $[\boldsymbol{H}_s(\boldsymbol{k}) : \boldsymbol{M}]$. *Hence, if* $\boldsymbol{G_k}$ *is imaginary, then it has relative class number one and it is given in Theorem* 2. *Hence, there are exactly* 4 *non-abelian CM-fields with class number one which are narrow Hilbert class fields of real quadratic fields* $\boldsymbol{k}$ *such that* $\boldsymbol{G_k}$ *is imaginary.*

Hence, we are reduced to the determination of those $\boldsymbol{H}_s(\boldsymbol{k})$ with class number one for which $\boldsymbol{G_k}$ is real. Note that the complex conjugation c which is in $\boldsymbol{A} = \mathrm{Gal}(\boldsymbol{H}_s(\boldsymbol{k})/\boldsymbol{k})$ is a square in $\boldsymbol{A}$ if and only if $\boldsymbol{G_k}$ is real. Indeed, since $\boldsymbol{G_k}/\boldsymbol{Q}$ is the maximal abelian sub-extension of $\boldsymbol{H}_s(\boldsymbol{k})/\boldsymbol{Q}$ unramified at the finite places, then $\mathrm{Gal}(\boldsymbol{H}_s(\boldsymbol{k})/\boldsymbol{G_k})$ is equal to the derived group $D(\boldsymbol{G}) = \boldsymbol{A}^2$ of $\boldsymbol{G}$, and $\boldsymbol{G_k}$ is real if and only if c is in $\mathrm{Gal}(\boldsymbol{H}_s(\boldsymbol{k})/\boldsymbol{G_k})$. The key step to the determination of all $\boldsymbol{H}_s(\boldsymbol{k})$ with class number one is the following result:

Theorem 7. *Let* $\boldsymbol{G_k}$ *be real. If* $\boldsymbol{H}_s(\boldsymbol{k})$ *has class number one, then the* 2*-Sylow subgroup of the narrow ideal class group of* $\boldsymbol{k}$ *is cyclic of order* ≥ 4. *Hence, the narrow Hilbert* 2*-class field* $\boldsymbol{H}_{s,2}(\boldsymbol{k})$ *of* $\boldsymbol{k}$ *is a dihedral CM-field with relative class number one. Finally, the narrow Hilbert* 2*-class field* $\boldsymbol{H}_{s,2}(\boldsymbol{k})$ *of a real quadratic field* $\boldsymbol{k}$ *has odd relative class number, if and only if* $\boldsymbol{k} = \boldsymbol{Q}(\sqrt{pq})$ *where* $2 \leq p < q$ *are two distinct primes not congruent to* 3 *modulo* 4 *and such that the Legendre's symbol* (p/q) *is equal to* $+1$. *In that situation the Hasse unit index of* $\boldsymbol{H}_{s,2}(\boldsymbol{k})$ *is equal to* 2 *and its relative class number is a square.*

Proof. We delineate the proof of this key step to our desired determination. First, $\boldsymbol{G_k}$ is real if and only if the complex conjugation is a square in $\boldsymbol{A} = \mathrm{Gal}(\boldsymbol{H}_s(\boldsymbol{k})/\boldsymbol{k})$. Hence, if $\boldsymbol{G_k}$ is real, then $\boldsymbol{A}$ has 4-rank greater than or equal to one. Second, assume that the 2-Sylow subgroup $\boldsymbol{A}_2$ of the narrow ideal class group of $\boldsymbol{k}$ is not cyclic. Then, there exists a subgroup $\boldsymbol{B}$ of $\boldsymbol{A}$ which does not contain the complex conjugation, which has even order and such that $\boldsymbol{A}/\boldsymbol{B}$ is cyclic of order $4n \geq 4$ ($\boldsymbol{B}$ is obtained as follows. Let $\sigma \in \boldsymbol{A}$ be a square root of c and let $\boldsymbol{C}$ be the cyclic subgroup of order 4 generated by σ. Let $\chi_{\boldsymbol{C}}$ be a character of order 4 defined on $\boldsymbol{C}$ and let χ denote any character of $\boldsymbol{G}$ whose restriction to $\boldsymbol{C}$ is equal to $\chi_{\boldsymbol{C}}$. Then take $\boldsymbol{B}$ equal to the kernel of χ). Third, let $\boldsymbol{H}$ be the subfield of $\boldsymbol{H}_s(\boldsymbol{k})$ such that $\mathrm{Gal}(\boldsymbol{H}_s(\boldsymbol{k})/\boldsymbol{H}) = \boldsymbol{B}$. Then $\boldsymbol{H}$ is a normal field containing $\boldsymbol{k}$ such that the complex conjugation is a non trivial element of $\mathrm{Gal}(\boldsymbol{H}/\boldsymbol{Q})$. Hence, it is easily seen that $\boldsymbol{H}$ is a dihedral

CM-field of degree $8n \geq 8$. According to Theorem 6, the relative class number of $\boldsymbol{H}$ is odd (in fact, it is equal to one). Now, we prove in [6] that any dihedral CM-field of degree $8n \geq 8$ with odd relative class number has Hasse unit index equal to 2, which implies that the canonical homomorphism from the ideal class group of the maximal totally real subfield $\boldsymbol{H}^+$ of $\boldsymbol{H}$ to the one of $\boldsymbol{H}$ is injective, and the class number of $\boldsymbol{H}^+$ is odd (see [8, Chapter 10]). Hence the class number of $\boldsymbol{H}$ is odd. However, according to Theorem 6, this field $\boldsymbol{H}$ has class number $[\boldsymbol{H}_s(\boldsymbol{k}) : \boldsymbol{H}] = |\boldsymbol{B}|$ which is even. A contradiction.

By using the results of [3], we can prove that if such a dihedral $\boldsymbol{H}_{s,2}(\boldsymbol{k})$ with odd relative class number has relative class number one, then its degree is less than or equal to 128. Moreover, S. Louboutin and R. Okazaki determined in [7] all octic dihedral CM-fields with relative class number one: there are 19 such number fields, and S. Louboutin found in [5] five dihedral CM-fields of degree 16 with relative class number one. Now, we have shown in [5] that it is reasonable to conjecture that there are only these 24 dihedral CM-fields of 2-power degrees with relative class number one. According to explicit constructions of the corresponding $\boldsymbol{H}_s(\boldsymbol{k})$, to the computation of their class numbers by using the system for computational number theory Pari/GP (see [1]) and to Theorem 6 we get:

Theorem 8. *There are at least* 26 *real quadratic fields* $\boldsymbol{k} = \boldsymbol{Q}(\sqrt{pq})$ *whose narrow Hilbert class fields* $\boldsymbol{H}_s(\boldsymbol{k})$ *are non abelian CM-fields with class number one: those which appear in the following* Table II *(where,* n_{pq} *denotes the degree* $[\boldsymbol{H}_s(\boldsymbol{k}) : \boldsymbol{Q}]$*). Assuming the conjecture put forward in* [5], *there are only these* 26 *non-abelian CM-fields with class number one which are narrow Hilbert class fields of real quadratic fields.*

Table I

$\boldsymbol{k}$ imaginary		$\boldsymbol{k}$ real		
$\{p_i^*\}$	$\{p_i^*\}$	$\{p_i^*\}$	$\{p_i^*\}$	$\{p_i^*\}$
{− 3}	{− 4, 13}	{− 3, − 4}	{− 7, − 19}	{− 43, − 67}
{− 4}	{− 4, 37}	{− 3, − 7}	{− 7, − 43}	{− 43, − 163}
{− 7}	{− 7, 5}	{− 3, − 8}	{− 7, − 67}	{− 67, − 163}
{− 8}	{− 7, 13}	{− 3, − 11}	{− 7, − 163}	
{− 11}	{− 7, 61}	{− 3, − 19}	{− 8, − 11}	{− 3, − 4, 5}
{− 19}	{− 8, 5}	{− 3, − 43}	{− 8, − 19}	{− 3, − 7, 5}
{− 43}	{− 8, 29}	{− 3, − 67}	{− 8, − 43}	{− 3, − 8, 5}
{− 67}	{− 11, 8}	{− 3, − 163}	{− 8, − 67}	{− 3, − 11, 8}
{− 163}	{− 11, 17}	{− 4, − 7}	{− 8, − 163}	{− 3, − 11, 17}
		{− 4, − 11}	{− 11, − 19}	{− 4, − 7, 5}
{− 3, 5}	{− 3, − 4, − 7}	{− 4, − 19}	{− 11, − 43}	{− 4, − 7, 13}
{− 3, 8}	{− 3, − 4, − 11}	{− 4, − 43}	{− 11, − 67}	{− 7, − 8, 5}
{− 3, 17}	{− 3, − 4, − 19}	{− 4, − 67}	{− 11, − 163}	
{− 3, 41}	{− 3, − 7, − 8}	{− 4, − 163}	{− 19, − 43}	
{− 3, 89}	{− 3, − 11, − 19}	{− 7, − 8}	{− 19, − 67}	
{− 4, 5}	{− 4, − 7, − 19}	{− 7, − 11}	{− 19, − 163}	

Table II

(p, q)	n_{pq}	(p, q)	n_{pq}	(p, q)	n_{pq}
(2,17)	8	(5,389)	8	(2,163)	12
(2,73)	8	(13,17)	8	(7,67)	12
(2,89)	8	(13,29)	8	(11,43)	12
(2,233)	8	(13,157)	8	(5,101)	16
(2,281)	8	(13,181)	8	(5,181)	16
(5,41)	8	(17,137)	8	(13,53)	16
(5,61)	8	(29,53)	8	(13,61)	16
(5,109)	8	(73,97)	8	(19,43)	20
(5,149)	8			(5,269)	24

References

[1] H. Cohen: A Course in Computational Algebraic Number Theory. Springer-Verlag, Grad. Texts Math., **138**, New York, Berlin (1993).

[2] D. Cox: Primes of the Form $x^2 + ny^2$. Wiley-Interscience Publication, John Wiley and sons Inc., New York (1989).

[3] J. Hoffstein: Some analytic bounds for zeta functions and class numbers. Inventiones Math., **55**, 37–47 (1979).

[4] S. Louboutin, R. Okazaki and M. Olivier: The class number one problem for some non-abelian normal CM-fields (preprint Univ. Caen (1995)) (submitted).

[5] S. Louboutin: Calcul des nombres de classes relatifs de certains corps de classes de Hilbert. C. R. Acad. Sci. Paris, **319**, Série I, 321–325 (1994).

[6] S. Louboutin: Corps quadratiques à corps de classes de Hilbert principaux et à multiplication complexe (to appear in Acta Arith.).

[7] S. Louboutin and R. Okazaki: Determination of all non-normal quartic CM-fields and of all non-abelian normal octic CM-fields with class number one. Acta Arith., **67**, 47–62 (1994).

[8] L. C. Washington: Introduction to Cyclotomic Fields. Springer-Verlag, Grad. Texts Math., **83**, New York, Berlin (1982).

[9] K. Yamamura: The determination of the imaginary abelian number fields with classnumber one. Math. Comp., **62**, 899–921 (1994).