H. Yokoi
Nagoya Math. J.
Vol. 102 (1986), 91–100

IMAGINARY BICYCLIC BIQUADRATIC FIELDS WITH THE REAL QUADRATIC SUBFIELD OF CLASS-NUMBER ONE

HIDEO YOKOI

It has been proved by A. Baker [1] and H. M. Stark [7] that there exist exactly 9 imaginary quadratic fields of class-number one. On the other hand, G.F. Gauss has conjectured that there exist infinitely many real quadratic fields of class-number one, and the conjecture is now still unsolved.

In connection with this Gauss' conjecture, we shall consider, in this paper, a real quadratic field $\boldsymbol{Q}(\sqrt{p})$ (prime $p \equiv 1 \; mod \; 4$) as a subfield of the imaginary bicyclic biquadratic field $K = \boldsymbol{Q}(\sqrt{p}, \sqrt{-q})$, which is a composite field of $\boldsymbol{Q}(\sqrt{p})$ with an imaginary quadratic field $\boldsymbol{Q}(\sqrt{-q})$ of class number one, and give various conditions for the class-number of $\boldsymbol{Q}(\sqrt{p})$ to be equal to one by using invariants of the relatively cyclic unramified extension K/F over imaginary quadratic field $F = \boldsymbol{Q}(\sqrt{-pq})$.

After notation in Section 1, we shall summarize in Section 2 well-known properties of a relatively cyclic extension and an unramified extension respectively, which we shall use in this paper. In Section 3 we shall consider the ideal class group of a cyclic unramified extension over a finite algebraic number field. Finally, we shall investigate in Section 4 the imaginary bicyclic biquadratic field $K = \boldsymbol{Q}(\sqrt{-q}, \sqrt{p})$, and give some conditions for the class-number of real quadratic subfield $\boldsymbol{Q}(\sqrt{p})$ to be equal to 1.

§1. Notation

Generally, for an arbitrary finite abelian group B and its subgroup B', the order of B and the index of B' in B are denoted by $|B|$ and $[B : B']$ respectively.

For an arbitrary number field k, the following notation is used

Received October 30, 1984.

https://doi.org/10.1017/S0027763000000441 Published online by Cambridge University Press

throughout this paper:

E_k: the group of units of k

C_k: the group of ideal classes of k

$h_k = |C_k|$: the class-number of k

$\tilde{k}$: the absolute or Hilbert class field of k.

For a finite Galois extension K/F of a finite algebraic number field F and the Galois group $G = Gal(K/F)$, we shall denote by $H^r(G, B)$ the r-dimensional Galois cohomology group of G acting on an abelian group B, and by $Q(B)$ the Herbrand quotient of B, i.e. $Q(B) = |H^0(G, B)|/|H^1(G, B)|$.

Furthermore, we shall use the following notation:

$\Pi e(\mathfrak{p})$: the product of ramification exponents of all finite prime divisors $\mathfrak{p}$ of F with respect to K/F

$\Pi e(\mathfrak{p}_\infty)$: the product of ramification exponents of all infinite prime divisors $\mathfrak{p}_\infty$ of F with respect to K/F

$\tilde{\Pi} e(\mathfrak{p}) = \Pi e(\mathfrak{p}) \cdot \Pi e(\mathfrak{p}_\infty)$: the product of ramification exponents of all finite and infinite prime divisors of F with respect to K/F

(ε): the group of units of F

(η): the group of those units of F which are norms of number of K

A: the group of ambiguous classes of C_K with respect to K/F

$a = |A|$: the ambiguous class number of K/F

A_0: the group of classes of C_K represented by *ambiguous* ideals with respect to K/F

$a_0 = |A_0|$

A_F: the group of classes of C_K represented by ideals of F

$a_F = |A_F|$

C_F^0: the group of those classes of C_F whose ideals become principal in K

$h_0 = |C_F^0|$

$N_{K/F}$: the norm mapping with respect to K/F, and simultaneously the homomorphism from C_K to C_F induced by the norm mapping

$j = j_{K/F}$: the homomorphism from C_F to C_K induced by extension of ideals

$N = j \circ N_{K/F}$: the endomorphism of C_K defined as composed mapping of $N_{K/F}$ and j.

§ 2. Preliminary results

In this section, we shall summarize several almost well-known

https://doi.org/10.1017/S0027763000000441 Published online by Cambridge University Press

results on a cyclic or an unramified extension, which we shall use in this paper.

LEMMA 1.[1] *Let K/F be a finite Galois extension of a finite algebraic number field F, then*

(1) $a_0 = h_F \cdot \frac{\Pi e(\mathfrak{p})}{|H^1(G, E_K)|}$

(2) $H^1(G, E_K) \cong (A_0)/(\alpha)$ *and* $|H^1(G, E_K)| \equiv 0 \pmod{h_0}$,

where (A_0) *is the group of ambiguous principal ideals of K with respect to K/F and* (α) *is the group of principal ideals of F.*

LEMMA 2.[2] *Let K/F be a finite cyclic extension of a finite algebraic number field F, then*

(3) $Q(C_K) = 1\,, \qquad Q(E_K) = \frac{\Pi e(\mathfrak{p}_\infty)}{[K:F]}$

(4) $a = h_F \cdot \frac{\tilde{\Pi} e(\mathfrak{p})}{[K:F][\varepsilon:\eta]} = |NC_K|\cdot|H^0(G, C_K)|$

(5) $\frac{a}{a_0} = [\eta : N_{K/F}(E_K)]\,, \qquad \frac{a_0}{a_F} = \frac{h_0 \cdot \Pi e(\mathfrak{p})}{|H^1(G, E_K)|}$

(6) $\tilde{\Pi} e(\mathfrak{p}) \equiv 0 \qquad (mod\ [\varepsilon : \eta])$

LEMMA 3.[3] *Let K/F be a finite Galois unramified extension of a finite algebraic number field F, then*

(7) $H^1(G, E_K) \cong C_F^0$

(8) $H^2(G, E_K) \cong A/A_F$

(9) $a = h_F \cdot \frac{|H^2(G, E_K)|}{|H^1(G, E_K)|}\,.$

§ 3. Cyclic unramified extension

Let F be a finite algebraic number field, and K be a finite cyclic unramified (in all finite and infinite prime divisors) extension field. For such extension K/F, we shall consider, in this section, the structure of the ideal class group C_K of K as Galois module.

PROPOSITION 1. *Let K/F be a finite cyclic unramified extension of a finite algebraic number field F, then*

1) For proofs, see Iwasawa [3], Yokoi [10].
2) For proofs, see Takagi [8, pp. 192–195], Yokoi [10].
3) For proofs, see Iwasawa [3].

(i) $a = \dfrac{h_F}{[K: F]}$, i.e. $\tilde{F} = K^*$,

where K^* *is the genus field with respect to* K/F.

(ii) $h_0 = |H^1(G, E_K)| = [K: F]\cdot[\eta: N_{K/F}(E_K)]$

(iii) $|H^0(G, C_K)| = |C_F^0 \cap N_{K/F}(C_K)|$

(iv) $|H^0(G, C_K)| \equiv 0 \ (mod\, |H^0(G, E_K)|)$,

and $|H^0(G, C_K)| = |H^0(G, E_K)|$ *if and only if* $NC_K = A_F$

(v) *any ambiguous class ideal of* K/F *becomes principal in* $\tilde{F}$.

Proof.

(i), (ii) See Yokoi [10]

(iii) See Kisilevsky [4]

(iv) By Lemma 2, (5), $[A: A_0]$ is equal to $[\eta: N_{K/F}(E_K)]$.

On the other hand, since $[\varepsilon: \eta] = 1$ by Lemma 2, (6), it holds $|H^0(G, E_K)| = [\eta: N_{K/F}(E_K)]$, and so $[A: A_0] = |H^0(G, E_K)|$. Hence it is clear from $[A_0: A_F] = 1$ that

$$|H^0(G, C_K)| = [A: A_0]\cdot[A_0: A_F]\cdot[A_F: NC_K]$$
$$= |H^0(G, E_K)|\cdot[A_F: NC_K],$$

which implies easily assertion (iv).

(v) See Terada [9], and cf (i).

PROPOSITION 2. *In the extension* K/F, *any two conditions of the following* (i) ~ (iii) *are equivalent to each other*:

(i) $h_K = a$, i.e. $C_K = A$

(ii) $\tilde{K} = K^*$, i.e. $C_K^{1-\sigma} = 1$,

where σ *is a generator of the cyclic Galois group* $G = \mathrm{Gal}\,(K/F)$.

(iii) $Ker\,(N_{K/F}) = 1$, i.e. $N_{K/F}: C_K \to C_F$ *is monomorphic.*

Proof. Since $[C_F: N_{K/F}(C_K)] = [K: F]$ and $a = h_F/[K: F]$ hold by class field theory and Proposition 1, (i) respectively, we get the following:

$$\mathrm{Ker}\,(N_{K/F}) = 1 \Longleftrightarrow |N_{K/F}(C_K)| = h_K$$
$$\Longleftrightarrow h_K = h_F/[K; F] \Longleftrightarrow h_K = a\,.$$

On the other hand, it follows from $C_K/A \cong C_K^{1-\sigma}$ that

$$h_K = a \Longleftrightarrow C_K = A \Longleftrightarrow C_K^{1-\sigma} = 1 \Longleftrightarrow \tilde{K} = K^*.$$

PROPOSITION 3. *In the extension* K/F, *any two conditions of the following* (i) ~ (iv) *are equivalent to each other*:

https://doi.org/10.1017/S0027763000000441 Published online by Cambridge University Press

(i) $a=a_0$, i.e. $A=A_0$
(ii) $[\eta: N_{K/F}(E_K)]=1$
(iii) $H^0(G, E_K)=1$
(iv) $|H^1(G, E_K)|=h_0=[K: F]$

Proof. (i) $\Longleftrightarrow$ (ii) It is evident by Lemma 2, (5) that (i) is equivalent to (ii).

(ii) $\Longleftrightarrow$ (iii) Since K/F is a cyclic unramified extension, we get $[\varepsilon: \eta]=1$ immediately by Lemma 2, (6), and so

$$|H^0(G, E_K)|=[\varepsilon: \eta]\cdot[\eta: N_{K/F}(E_K)]=[\eta: N_{K/F}(E_K)].$$

Hence

$$|H^0(G, E_K)|=1 \quad \text{if and only if} \quad [\eta: N_{K/F}(E_K)]=1.$$

(ii) $\Longleftrightarrow$ (iv) It is clear by Proposition 1, (ii) that (ii) is equivalent to (iv).

PROPOSITION 4. *In the extension K/F, any two conditions of the following* (i) ~ (iii) *are equivalent to each other*:
(i) $C_F=C_F^0\times N_{K/F}(C_K)$
(ii) $Ker(N)=Ker(N_{K/F})$
(iii) $H^0(G, C_K)=1$

Proof. (i) $\Longrightarrow$ (ii) Since $N=j\circ N_{K/F}$, it holds $Ker(N_{K/F})\subset Ker(N)$ in general. If $C_F=C_F^0\times N_{K/F}(C_K)$, then $C_F\cap N_{K/F}(C_K)=1$ holds, and hence for any C in $Ker(N)$ we get $N_{K/F}(C)\in C_F^0\cap N_{K/F}(C_K)$, and so $C\in Ker(N_{K/F})$. Therefore we get $Ker(N)\subset Ker(N_{K/F})$.

(ii) $\Longrightarrow$ (iii) If $Ker(N_{K/F})=Ker(N)$, then for any C' in $C_F^0\cap N_{K/F}(C_K)$, it holds

$$\phi\neq N_{K/F}^{-1}(C')\in N_{K/F}^{-1}(C_F^0)=Ker(N)=Ker(N_{K/F}), \text{ and so } C'=1.$$

Hence we get $C_F^0\cap N_{K/F}(C_K)=1$, from which follows $H^0(G, C_K)=1$ by Proposition 1, (iii).

(iii) $\Longrightarrow$ (i) If $H^0(G, C_K)=1$, then $C_F^0\cap N_{K/F}(C_K)=1$ holds by Proposition 1, (iii). On the other hand, by class field theory $|N_{K/F}(C_K)|=h_F/[K: F]$ holds, and also by Proposition 1, (ii),

$$|C_F^0|=h_0\equiv 0 \qquad (mod\,[K: F])$$

holds. Hence we get $C_F=C_F^0\times N_{K/F}(C_K)$.

https://doi.org/10.1017/S0027763000000441 Published online by Cambridge University Press

COROLLARY. *In the extension K/F, if any one of* 3 *conditions in Proposition* 4 *is satisfied, then each of* 4 *conditions in Proposition* 3 *is also satisfied.*

Proof. This assertion is an immediate consequence of Proposition 1, (iv), Proposition 3 and Proposition 4.

§ 4. Imaginary bicyclic biquadratic field

Let p be a prime congruent to 1 *mod* 4, and q be 1, 2 or a prime congruent to -1 *mod* 4. Put $k_1 = \boldsymbol{Q}(\sqrt{-q})$, $k_2 = \boldsymbol{Q}(\sqrt{p})$, $F = \boldsymbol{Q}(\sqrt{-pq})$ and $K = \boldsymbol{Q}(\sqrt{-q}, \sqrt{p})$. Then, applying the results of Section 3, we shall consider, in this section, the structure of the ideal class group $\boldsymbol{C}_K$ of K as Galois module with respect to K/F, and under the assumption that the class-number h_1 of k_1 is equal to 1, we shall give some kinds of conditions for the class-number h_2 of k_2 to be equal to 1.

THEOREM 1. *Let p be a prime congruent to* 1 *mod* 4, *and q be* 1, 2 *or a prime congruent to* -1 *mod* 4. *Put $F=\boldsymbol{Q}(\sqrt{-pq})$ and $K=\boldsymbol{Q}(\sqrt{-q}, \sqrt{p})$. Then, K/F is a cyclic unramified extension of degree* 2, *and moreover the following* (i) ~ (v) *hold*:

(i) $K^* = \tilde{F}$

(ii) $h_K = h_F \cdot \dfrac{h_1 \cdot h_2}{2}$

(iii) $H^0(G, E_K) = 1$

(iv) $a = a_0$, i.e. $A = A_0$

(v) $h_0 = 2$

Here, h_1 and h_2 are the class-number of quadratic number fields $k_1 = \boldsymbol{Q}(\sqrt{-q})$ and $k_2 = \boldsymbol{Q}(\sqrt{p})$ respectively.

Proof. In the imaginary bicyclic biquadratic field $K = \boldsymbol{Q}(\sqrt{-q}, \sqrt{p})$, the ramified finite primes are only p and q (or 2[4)]), and their ramification exponents with respect to $K/\boldsymbol{Q}$ are equal to theirs with respect to K/F respectively (all of them are equal to 2). Hence K/F is unramified.

(i) $\tilde{F} = K^*$ follows immediately from Proposition 1.

(ii) Since $p \equiv 1$ (*mod* 4), the fundamental unit ε_p of k_2 has norm -1. Hence, we know first

$$h_K = \frac{h_1 \cdot h_2 \cdot h_F}{2} \qquad \text{(see, for example, Brown and Parry [2]).}$$

4) In the special case of $q = 1$, there is choosen 2 instead of q.

https://doi.org/10.1017/S0027763000000441 Published online by Cambridge University Press

(iii) Since $N_{K/F}(\varepsilon_p) = N_{k_2}(\varepsilon_p) = -1$, we get

$$(\varepsilon) = \pm 1 = N_{K/F}(E_K).$$

Hence

$$H^0(G, E_K) \cong (\varepsilon)/N_{K/F}(E_K) = 1.$$

(iv), (v) Both $a = a_0$ and $h_0 = 2$ are immediate consequences of Proposition 3 and the above assertion (iii).

COROLLARY. *Let K/F be as in Theorem 1, then*

(i) $a = a_0 = h_F/2$

(ii) $H^1(G, E_K)$ *is a cyclic group of order 2.*

Proof. These two assertions are immediate consequences of Theorem 1 and Proposition 1.

THEOREM 2. *If the class-number h_1 of $\boldsymbol{Q}(\sqrt{-q})$ is equal to 1, then any two conditions of the following* (i) ~ (v) *are equivalent to each other*:

(i) *the class-number h_2 of $\boldsymbol{Q}(\sqrt{p})$ is equal to 1*

(ii) $h_K = a$, *i.e.* $C_K = A$

(iii) $\tilde{K} = K^*$, *i.e.* $C_K^{1-\sigma} = 1$

(iv) $N_{K/F}\colon C_K \to C_F$ *is monomorphic, i.e.* $Ker(N_{K/F}) = 1$

(v) $j\colon C_F \to C_K$ *is epimorphic, i.e.* $j(C_F) = C_K$.

Proof. (i) $\Longleftrightarrow$ (ii) By Theorem 1, it follows from the assumption that

$$h_2 = 1 \quad \text{if and only if} \quad h_K = h_F/2.$$

On the other hand, since $a = h_F/2$ by Proposition 1, (i), we have that

$$h_2 = 1 \quad \text{if and only if} \quad h_K = a.$$

(ii) $\Longleftrightarrow$ (iii) Since $C_K/A \cong C_K^{1-\sigma}$ and $[C_K; C_K^{1-\sigma}] = [K^*\colon K]$, it is clear that

$$C_K = A \Longleftrightarrow C_K^{1-\sigma} = 1 \Longleftrightarrow \tilde{K} = K^*.$$

(ii) $\Longleftrightarrow$ (iv) Since C_K is finite,

$$Ker(N_{K/F}) = 1 \quad \text{if and only if} \quad |N_{K/F}(C_K)| = h_K.$$

On the other hand, since $[C_F\colon N_{K/F}(C_K)] = 2$ by class field theory,

$$|N_{K/F}(C_K)| = h_K \quad \text{if and only if} \quad h_K = h_F/2,$$

which is equivalent to $h_K = a$.

(ii) $\Longleftrightarrow$ (v) Since $C_F/C_F^0 \cong j(C_F)$ and $|C_F^0| = 2$ by Theorem 1, we get

$$|j(C_F)| = [C_F: C_F^0] = h_F/2 .$$

Hence, for $C_K \supset j(C_F)$ we have

$$C_K = j(C_F) \Longleftrightarrow h_K = h_F/2 \Longleftrightarrow h_K = a .$$

Consequently, j is epimorphic if and only if $h_K = a$.

PROPOSITION 5. *If the class-number h_1 of $Q(\sqrt{-q})$ is equal to* 1, *then it is necessary for the class-number h_2 of $Q(\sqrt{p})$ to be equal to* 1 *that the following conditions* (i) ~ (iii) *are satisfied*:

(i) $H^0(G, C_K) = 1$ *or cyclic group* of *order* 2

(ii) 2 *rank s of the ideal class group C_K of K is equal to* 0 *or* 1

(iii) *all ideals of K become principal in $\tilde{F}$.*

Proof. (i) By Theorem 1, (v), it follows from $C_F^0 \supset C_F^0 \cap N_{K/F}(C_K)$ that

$$|C_F^0 \cap N_{K/F}(C_K)| = 1 \text{ or } 2 ,$$

and hence we know by Proposition 1, (iii)

$$|H^0(G, C_K)| = 1 \text{ or } 2 .$$

(ii) By Theorem 2 it holds $C_K = A$, which implies

$$NC_K = NA = A^2 = C_K^2 .$$

Thus we get

$$|H^0(G, C_K)| = [A: NC_K] = [C_K: C_K^2] = 2^s ,$$

and hence the assertion (ii) implies $s = 0$ or 1.

(iii) The assertion (iv) follows immediately from $C_K = A$ by Proposition 1, (v).

PROPOSITION 6. *Under the assumption $h_1 = 1$, if we assume moreover $h_2 = 1$, then any two conditions of the following* (i) ~ (iv) *are equivalent to each other*:

(i) $\left(\dfrac{q}{p}\right) = -1$,

where (—) *is the Legendre-Jacobi-Kronecker symbol.*

(ii) $h_F \not\equiv 0$ (*mod* 4), i.e. $2 \| h_F$

(iii) 2 *rank s of C_K is equal to* 0, *i.e.* $(h_K, 2) = 1$

https://doi.org/10.1017/S0027763000000441 Published online by Cambridge University Press

(iv) $H^n(G, C_K) = 1$ *for any integer n.*

Proof. (i) $\Longleftrightarrow$ (ii) It is an immediate consequence of Rédei and Reichardt's theorem that

$$h_F \not\equiv 0 \ (mod\ 4) \quad \text{if and only if} \quad \left(\frac{p}{q}\right) = -1$$

(see Rédei and Reichardt [6]) .

(ii) $\Longleftrightarrow$ (iii) Since assumption $h_1 = h_2 = 1$ implies $h_K = h_F/2$ by Theorem 1, (ii), it is clear that

$$(h_K, 2) = 1 \quad \text{if and only if} \quad h_F \not\equiv 0 \ (mod\ 4) .$$

(iii) $\Longleftrightarrow$ (iv) By Theorem 2, assumption $h_1 = h_2 = 1$ implies $C_K = A$. On the other hand,

$$(h_K, 2) = 1 \quad \text{if and only if} \quad C_K^2 = C_K .$$

Hence, if $(h_K, 2) = 1$, then we get

$$NC_K = NA = A^2 = C_K^2 = C_K = A ,$$

which shows $H^0(G, C_K) \cong A/NC_K = 1$, and by Lemma 2, (3) $H^n(G, C_K) = 1$ holds for any integer n. Conversely, if $H^n(G, C_K) = 1$ holds for any integer n, then in particular $H^0(G, C_K) = 1$ implies $A = NC_K$. Hence we get

$$C_K^2 = A^2 = NA = NC_K = A = C_K ,$$

which shows $(h_K, 2) = 1$.

PROPOSITION 7. *Under the assumption $h_1 = 1$, if the endomorphism N of C_K is epimorphic or monomorphic, the following conditions* (i) ~ (iii) *are satisfied*:

(i) $h_2 = 1$

(ii) $H^n(G, C_K) = 1$ *for any integer n*

(iii) 2 *rank s of C_K is equal to* 0,
i.e. $(h_K, 2) = 1$

Proof. Since C_K is a finite abelian group, the following conditions (1°) ~ (3°) for the endomorphism N of C_K are equivalent to each other:

1°) N is epimorphic

2°) N is monomorphic

3°) N is automorphic.

In this case, it follows from $C_K = NC_K$ that $C_K = A = NC_K$ holds, which implies $2^s = [C_K : C_K^2] = 1$ because $C_K^2 = A^2 = NA = NC_K = C_K$. Thus we know $s = 0$, which is assertion (iii).

Moreover, by Theorem 2, $C_K = A$ implies $h_2 = 1$, which is assertion (i).

On the other hand, $A = NC_K$ implies $H^0(G, C_K) \cong A/NC_K = 1$, and hence by Lemma 2, (3) we get $H^n(G, C_K) = 1$ for any integer n. Thus, we can complete the proof of Proposition 7.

Finally, we give some examples.

p	q	h_1	h_2	h_F	a	h_K
5	1	1	1	2	1	1
17	2	1	1	4	2	2
13	2	1	1	6	3	3
41	1	1	1	8	4	4
53	3	1	1	10	5	5
229	3	1	3	26	13	39

References

[1] A. Baker, Linear forms in the logarithms of algebraic numbers, Mathematika, **13** (1966), 204–216.

[2] E. Brown and C. J. Parry, The imaginary bicyclic biquadratic fields with class-number 1, J. Reine Angew. Math., **260** (1973), 118–120.

[3] K. Iwasawa, A note on the group of units of an algebraic number field, J. Math. Pures Appl., **35** (1956), 189–192.

[4] H. Kisilevsky, Some results related to Hilbert's Theorem 94, J. Number Theory, **2** (1970), 199–206.

[5] S. Kuroda, Über den Dirichletschen Körper, J. Fac. Sci. Imp. Univ. Tokyo, Sec. I, **4** (1943), 383–406.

[6] L. Rédei and H. Reichardt, Die Anzahl der durch 4 teilbaren Invarianten der Klassengruppe beliebigen quadratischen Zahlkörpers, J. Reine Angew. Math., **170** (1933), 69–74.

[7] H. M. Stark, A complete determination of the complex quadratic fields of class-number one, Michigan Math. J., **14** (1967), 1–27.

[8] T. Takagi, Algebraic number Theory (Japanese), Iwanami, Tokyo (1948).

[9] F. Terada, A principal ideal theorem in the genus fields, Tôhoku Math. J., **23-4** (1971), 697–718.

[10] H. Yokoi, On the class number of a relatively cyclic number field, Nagoya Math. J., **29** (1967), 31–44.

Department of Mathematics
College of General Education
Nagoya University
Chikusa-ku, Nagoya 464
Japan