A criterion for a certain type of imaginary quadratic fields to have 3-ranks of the ideal class groups greater than one

By Yasuhiro KISHI

Department of Mathematics, Tokyo Metropolitan University, 1-1, Minami-Ohsawa, Hachioji, Tokyo 192-0397

(Communicated by Shokichi IYANAGA, M. J. A., June 23, 1998)

§1 Statement of the result. In our previous paper [3], a characterization of the quadratic fields whose class numbers are divisible by 3 is given. In this paper, we study a certain type of imaginary quadratic fields, and give a criterion for them to have the 3-ranks of the ideal class groups greater than one.

Our main result is:

Theorem 1. *Let $D < 0$ be a square free integer which satisfies $D \equiv 1 \pmod 3$. Assume that a fundamental unit ε of the real quadratic field $\boldsymbol{Q}(\sqrt{-3D})$ satisfies the condition:*

$$(1.1)\quad Tr_{\boldsymbol{Q}(\sqrt{-3D})/\boldsymbol{Q}}\varepsilon \equiv \pm 2 \pmod 9,\quad \not\equiv \pm 2 \pmod{81}.$$

Then the 3-rank of the ideal class group of $\boldsymbol{Q}(\sqrt{D})$ is greater than 1 if and only if there exists a pair of relatively prime integers u and w with the following three properties:

(i) $4w^3 - 27Du^2$ is a square;

(1.2) (ii) $g(Z) = Z^3 - DwZ - D^2u$ is irreducible over $\boldsymbol{Q}$;

(iii) $3 \mid u$ and $w \equiv 1 \pmod 3$.

There exist infinitely many real quadratic fields which have fundamental units satisfying the condition (1.1) with $Tr_{\boldsymbol{Q}(\sqrt{-3D})/\boldsymbol{Q}}\varepsilon \equiv -2 \pmod 9$. To see this, we need

Proposition 1 (Katayama [2]). *For every prime $p \neq 5$, $\varepsilon = (p + 2 + \sqrt{p(p+4)})/2$ is a fundamental unit of $k = \boldsymbol{Q}(\sqrt{p(p+4)})$.*

Take a prime p so that we have $p \equiv 23 \pmod{81}$, and put $p = 81p' + 23$. Then we have

$$Tr_{k/\boldsymbol{Q}}\varepsilon = p + 2 = 81p' + 25 \equiv -2 \pmod 9,\quad \not\equiv \pm 2 \pmod{81}.$$

Let D be a square free part of $-3p(p+4)$. Since

$$-3p(p+4) = -81(81p' + 23)(3p' + 1),$$

we have

$$D \equiv -(81p' + 23)(3p' + 1) \equiv 1 \pmod 3.$$

Hence there exist infinitely many D to which our criterion of Theorem 1 is applicable.

Let us quote two propositions which we need for the proof of Theorem 1. For a prime number p and an integer m, we denote the greatest exponent μ of p such that $p^\mu \mid m$ by $V_p(m)$.

Proposition 2 (Llorente and Nart [5]). *Suppose that the cubic polynomial*

$$f(X) = X^3 - aX - b,\quad a, b \in \boldsymbol{Z},$$

is irreducible over $\boldsymbol{Q}$, and that either $V_p(a) < 2$ or $V_p(b) < 3$ holds for every prime p. Let $\Delta = 4a^3 - 27b^2$ be the discriminant of $f(X)$, and θ be a root of $f(X) = 0$.

(i) *If $a \equiv 3 \pmod 9$, $b^2 \equiv a + 1 \pmod{27}$, $V_3(\Delta) = 6$ and $\Delta/3^6 \equiv 1 \pmod 3$, then 3 remains prime in $\boldsymbol{Q}(\theta)$.*

(ii) *If $3 \nmid a$, then 3 splits into three prime ideals in $\boldsymbol{Q}(\theta)$ if and only if $a \equiv 1 \pmod 3$ and $3 \mid b$.*

Proposition 3 (Imaoka [1], Komatsu [4]). *Let D be a square free integer. Every unramified cyclic cubic extension of $\boldsymbol{Q}(\sqrt{D})$ is given by a cubic equation of the form*

$$f(X) = X^3 - DwX - D^2u,\quad u, w \in \boldsymbol{Z},\quad (u, w) = 1$$

where $4w^3 - 27Du^2$ is a square in $\boldsymbol{Z}$ and $(3, w) = 1$.

Remark. Proposition 3 is a result of Imaoka and Komatsu; they independently improved a portion of results of [3].

§2 Proof of Theorem 1. First we show two lemmas.

Lemma 1. *Let D be a square free integer and $k = \boldsymbol{Q}(\sqrt{D})$. Let $\alpha = (a + b\sqrt{D})/2\ (a, b \in \boldsymbol{Z})$ be an integer in k whose norm is a cube in $\boldsymbol{Z}$; $N_{k/\boldsymbol{Q}}\alpha = m^3\ (m \in \boldsymbol{Z})$. Then the polynomial $f(X) = X^3 - 3mX - a$ is reducible over $\boldsymbol{Q}$ if and only if α is a cube in k.*

Proof. Assume that α is not a cube in k. By Cardano's formula, the roots of $f(X) = 0$ are of the form $\xi + \xi'$ where ξ and ξ' are cube root of $(a + b\sqrt{D})/2$ and $(a - b\sqrt{D})/2$, respectively, with $\xi \cdot \xi' = m$. Now express

$$\xi = c + d\sqrt{D},$$
$$\xi' = c - d\sqrt{D}$$

with $c, d \in \boldsymbol{C}$, $d = \sqrt{c^2 - m}/\sqrt{D}$. Then $2c$ is a root of $f(X) = 0$. Since

$$\frac{a + b\sqrt{D}}{2} = \xi^3 = c^3 + 3cd^2D + (3c^2d + d^3D)\sqrt{D},$$

$$\frac{a - b\sqrt{D}}{2} = \xi'^3 = c^3 + 3cd^2D - (3c^2d + d^3D)\sqrt{D},$$

we have

$$\text{(2.1)} \qquad \frac{a}{2} = c^3 + 3cd^2,$$

$$\text{(2.2)} \qquad \frac{b}{2} = 3c^2d + d^3D = (3c^2 + d^2D)d.$$

Suppose that $2c$ is rational; then we see d^2 is also rational by (2.1). Hence d is also rational by (2.2). This contradicts the assumption that α is not a cube in k. Therefore $f(X)$ is irreducible over $\boldsymbol{Q}$.

Conversely, assume that α is a cube in k, and take $\beta = c + d\sqrt{D}$ $(c, d \in \boldsymbol{Q})$ in k so that we have $\alpha = \beta^3$. Then we have $m = c^2 - d^2D$ and $a = 2(c^3 + 3cd^2D)$ because $\alpha = \beta^3 = c^3 + 3cd^2D + (3c^2d + d^3D)\sqrt{D}$. Therefore

$$f(X) = X^3 - 3(c^2 - d^2D)X - 2(c^3 + 3cd^2D)$$
$$= (X - 2c)(X^2 + 2cX + c^2 + 3d^2D),$$

that is, $f(X)$ is reducible over $\boldsymbol{Q}$. □

Lemma 2. *Let $D < 0$ be a square free integer which is not divisible by* 3, *and put*

$$f(X) = X^3 - 3X - s$$

where s is the trace of a fundamental unit $\varepsilon = (s + t\sqrt{-3D})/2$ of $\boldsymbol{Q}(\sqrt{-3D})$. If $s \equiv \pm 2 \pmod 9$, then the roots of $f(X) = 0$ generate an unramified cyclic cubic extension K of $\boldsymbol{Q}(\sqrt{D})$. Furthermore if $D \equiv 1 \pmod 3$ and $s \not\equiv \pm 2 \pmod{81}$, then the prime 3 *splits into two prime ideals in K.*

Proof. We apply Main Theorem of [3] to the case $u = s^2$, $w = 3$. Then we have $g(Z) = Z^3 - 3s^2Z - s^4$. Note that $g(sX) = s^3X^3 - 3s^3X - s^4 = s^3f(X)$, and the discriminants of $g(Z)$ and $f(Z)$ have the same square free part D. Now we see

$$\text{(2.3)} \qquad uw = 3s^2 \equiv 3 \pmod 9.$$

Suppose that $s \equiv \pm 2 \pmod 9$. Since $N_{\boldsymbol{Q}(\sqrt{-3D})/\boldsymbol{Q}}\varepsilon = (s^2 + 3t^2D)/4 = 1$, we have $3t^2D = 4 - s^2 \equiv 0 \pmod 9$, and hence $3 \mid t$. Therefore $s^2 \equiv 4 \pmod{27}$. Then we have

$$\text{(2.4)} \qquad u = s^2 \equiv 4 = w + 1 \pmod{27}.$$

By Lemma 1, $f(X)$ is irreducible over $\boldsymbol{Q}$. Hence by the Main Theorem of [3], (2.3) and (2.4) imply that K is an unramified cyclic cubic extension of $\boldsymbol{Q}(\sqrt{D})$.

Suppose $D \equiv 1 \pmod 3$ and $s \not\equiv \pm 2 \pmod{81}$. It follows immediately from the former condition that 3 splits in $\boldsymbol{Q}(\sqrt{D})$. Since $s \not\equiv \pm 2 \pmod{81}$, we see $3^2 \nmid t$. Hence 3 remains prime in $\boldsymbol{Q}(\theta)$ because of Proposition 2 (i). Therefore 3 splits into two prime ideals in K. □

If $D \equiv 1 \pmod 3$ and (1.1) holds, then there exists an unramified cyclic cubic extension K_1 of $\boldsymbol{Q}(\sqrt{D})$ and 3 splits into two prime ideals in K_1 by Lemma 2.

Suppose that the 3-rank is greater than 1. Then there exists another unramified cyclic cubic extension K_2 of $\boldsymbol{Q}(\sqrt{D})$. Put $K := K_1 \cdot K_2$. Then K is normal over $\boldsymbol{Q}$ of degree 18 and the Galois group of $K/\boldsymbol{Q}(\sqrt{D})$ is bicyclic bicubic. Now we consider of prime decomposition of 3 in K. Let T and Z denote the inertial group and the decomposition group, respectively, of an ideal $\mathfrak{P} \mid 3$ in K. Put $G := Gal(K/\boldsymbol{Q})$. Let f and g denote order of the quotient group Z/T and G/Z, respectively. Then $f \cdot g = 18$ because 3 is not ramified in K. Since 3 splits in $\boldsymbol{Q}(\sqrt{D})$ and does not split completely in K_1, we have $f = 3$ or 9. Since the quotient group Z/T must be cyclic, we see $f = 3$ and $g = 6$. Hence 3 splits into six prime ideals in K. There is, therefore, an unramified cyclic cubic extension $K' \subset K$ of $\boldsymbol{Q}(\sqrt{D})$ in which 3 splits into six prime ideals, and then 3 splits into three prime ideals in a cubic subfield of K'. By Proposition 3, there is a pair (u, w) for $K'/\boldsymbol{Q}(\sqrt{D})$ with the conditions (i) and (ii) of (1.2). It follows from (ii) of Proposition 2 that the pair (u, w) must satisfy (iii) of (1.2).

Conversely, suppose that there exist relatively prime integers u and w satisfying the condition (1.2). Then by (ii) of Proposition 2 there is an unramified cyclic cubic extension K'' of $\boldsymbol{Q}(\sqrt{D})$ in which the prime 3 splits into six prime ideals. Since K'' is different from K_1, the 3-rank of the ideal class group $\boldsymbol{Q}(\sqrt{D})$ is greater than 1. Theorem 1 is completely proved.

Remark. Let α be an integer in a quadratic field k whose norm is a cube in $\boldsymbol{Z}$; $N_{k/\boldsymbol{Q}}\alpha = m^3 (m \in \boldsymbol{Z})$. Put

$$f_\alpha(X) = X^3 - 3mX - Tr_{k/\boldsymbol{Q}}\alpha.$$

In Lemma 2, we showed that α is a cube in k if and only if $f_\alpha(X)$ is reducible over $\boldsymbol{Q}$. Suppose that α is not a cube in k. For an integer β in k, we define

$$f_{\alpha\beta^3}(X) = X^3 - 3mnX - Tr_{k/\boldsymbol{Q}}(\alpha\beta^3),$$

where $N_{k/\boldsymbol{Q}}\beta = n$. By modifying Lemma II.4 in [4], we can verify that the minimal splitting field of $f_{\alpha\beta^3}(X)$ coincides with the minimal splitting field of $f_\alpha(X)$. We see furthermore that $f_\alpha(X)$ and $f_{\alpha^2}(X)$ give the same splitting field. Indeed, if we put $\alpha=(a+b\sqrt{D})/2$, then we have

$$f_\alpha(X)=X^3-3mX-a,$$

$$f_{\alpha^2}(X)=X^3-3m^2X-\frac{a^2+b^2D}{2},$$

and by a simple calculation

$$f_{\alpha^2}(X+m)=-\frac{X^3}{a}f_\alpha\left(\frac{a}{X}\right).$$

§ 3 Table. There are 175 square free negative integers D with $D\equiv 1 \pmod 3$ greater than -10^6 for which the imaginary quadratic field $\boldsymbol{Q}(\sqrt{D})$ has the 3-rank greater than 1. (All of the 3-ranks are equal to 2.) The real quadratic field $\boldsymbol{Q}(\sqrt{-3D})$ has a fundamental unit satisfying the condition (1.1) in 115 cases out of the 175 cases. We list D of all 175 cases and u, w in these 115 cases.

Table

D	u	w	D	u	w
−974	—	—	−30161	8·3	97
−3299	4·3	61	−30341	30·3	529
−5069	8·3	73	−31214	22·3	103
−5306	2·3	67	−31271	2·3	31
−5417	8·3	385	−31430	2·3	991
−6221	10·3	61	−32522	—	—
−6914	14·3	211	−32561	—	—
−8522	4·3	553	−33065	6·3	769
−9497	—	—	−33437	—	—
−11651	—	—	−34742	24·3	25
−12131	1·3	4	−35813	—	—
−13829	2·3	193	−36713	36·3	925
−14033	—	—	−37649	2·3	193
−16049	22·3	553	−38738	26·3	547
−16238	—	—	−39113	—	—
−16301	4·3	469	−39626	—	—
−17282	2·3	187	−40934	—	—
−17399	1·3	73	−41015	—	—
−17561	—	—	−41063	—	—
−17723	—	—	−41186	34·3	763
−18362	30·3	451	−41354	2·3	763
−18458	6·3	427	−42158	8·3	313
−19187	—	—	−42866	—	—
−19286	8·3	241	−43121	8·3	841
−19427	4·3	853	−43190	8·3	1969
−19679	—	—	−43307	1·3	70
−19919	1·3	103	−43763	4·3	85
−20129	—	—	−43847	2·3	307
−21449	16·3	97	−44318	26·3	367
−22481	6·3	13	−45131	—	—
−23165	4·3	61	−45557	4·3	205
−26234	8·3	289	−45887	15·3	169
−26789	—	—	−48770	8·3	1129
−27635	10·3	91	−50855	3·3	529
−27773	6·3	157	−51995	4·3	301
−28031	—	—	−52541	—	—
* −29399	—	—	−53843	17·3	256
−29957	—	—	−54071	—	—

D	u	w	D	u	w
−54251	2·3	271	−76070	36·3	121
−54695	—	—	−76667	13·3	82
−54707	11·3	790	−77594	2·3	619
−55247	—	—	−77705	10·3	3121
−55271	1·3	7	−77897	—	—
−55598	—	—	−78362	—	—
−56510	84·3	1369	−78482	36·3	25
−56666	—	—	−79163	3·3	100
−56981	—	—	−79418	—	—
−57185	18·3	2869	−79865	2·3	829
−59105	2·3	1429	−81002	—	—
−59198	—	—	−81137	—	—
−59609	—	—	−82493	6·3	337
−59690	58·3	451	−83081	38·3	517
−60290	80·3	1561	−83381	4·3	157
−60974	6·3	391	−83522	—	—
−62201	—	—	−83585	66·3	181
−64067	—	—	−83723	19·3	100
−64478	26·3	607	−85199	19·3	271
−64571	21·3	484	−86597	64·3	841
−64814	6·3	487	−87401	12·3	157
−65051	3·3	466	−87503	5·3	211
−65657	—	—	−88001	8·3	433
−65813	2·3	493	−88223	13·3	991
−66377	2·3	265	−88310	38·3	271
−66494	2·3	1039	−88970	12·3	361
−67010	12·3	241	−90461	—	—
−67142	20·3	889	−90545	16·3	121
−67157	—	—	−90686	42·3	631
−67385	—	—	−91190	48·3	841
−68006	2·3	223	−91241	6·3	577
−68021	2·3	577	−91643	1·3	112
−68321	—	—	−92657	8·3	457
−68351	1·3	703	−92798	18·3	1135
−69758	8·3	985	−93629	—	—
−70226	—	—	−93989	6·3	4537
−71411	1·3	94	−94022	—	—
−71423	1·3	169	−94673	—	—
−71585	2·3	529	−95558	—	—
−71621	18·3	817	−95585	12·3	589
−71849	—	—	−96254	—	—
−72494	10·3	439	−96551	2·3	211
−72815	1·3	61	−96827	2·3	379
−73007	1·3	265	−97502	24·3	385
−73694	6·3	1663	−97583	—	—
−74117	—	—	−97649	—	—
−74615	—	—	−97799	1·3	841
−74957	8·3	817	−98390	22·3	1159

D	u	w	D	u	w
-98678	—	—	-99707	—	—
-98795	$1\cdot 3$	376			

In this table, there is only one case, $D = -29399$, for which the quadratic field $\boldsymbol{Q}(\sqrt{-3D})$ is of the type of Proposition 1. The largest D of the type of Proposition 1 which satisfies not only the assumptions of Theorem 1 but also the condition (1.2) is $D = -699863$. (Then we have $u = 27\cdot 3$, $w = 955$.) There are about 41.7% of 115 cases of D for which we have $Tr_{Q(\sqrt{-3D})/Q}\varepsilon \equiv +2 \pmod 9$.

References

[1] M. Imaoka: Generating Polynomials and Ramification Conditions of Cubic Fields. Tokyo Metropolitan University, Master thesis (1997/98) (in Japanese).

[2] S. Katayama: On Fundamental Units of Real Quadratic Fields with Norm +1. Proc. Japan Acad., **68A**, 18–20 (1992).

[3] Y. Kishi and K. Miyake: Characterization of the Quadratic Fields whose Class Numbers are Divisible by Three. Tokyo Metro. Univ. Math. Preprint Series, no. 7 (1997).

[4] T. Komatsu: The Relation between Elliptic Curves and Quadratic Fields whose Class Numbers are Divisible by 3, and its Application to Real Quadratic Fields. Tokyo Metropolitan University, Master thesis (1997/98) (in Japanese).

[5] P. Llorente and E. Nart: Effective Determination of the Decomposition of the Rational Prime in a Cubic Field. Proc. American Math. Soc., **87**, 579–585 (1983).