A note on quadratic fields in which a fixed prime number splits completely. II

By Humio ICHIMURA

Department of Mathematics, Yokohama City University,
22-2 Seto, Kanazawa-ku, Yokohama, Kanagawa 236-0027
(Communicated by Shokichi IYANAGA, M.J.A., Oct. 12, 1999)

1. Introduction. Let p be a fixed prime number and let $M(p)^+$ (resp. $M(p)^-$) be the set of all real (resp. imaginary) quadratic fields in which p splits. For a quadratic field K in which p splits, denote by n_K the order of the ideal class of a prime ideal of K over p. Here, an ideal class is the one in the usual sense. We are concerned with the images of the maps

$$\begin{aligned} \delta_p^+ &: M(p)^+ \longrightarrow \boldsymbol{N}, \quad K \to n_K \\ \delta_p^- &: M(p)^- \longrightarrow \boldsymbol{N}, \quad K \to n_K. \end{aligned}$$

In the previous paper [2, Theorem 2], we proved that the image $\operatorname{Im}\delta_p^-$ of δ_p^- equals $\boldsymbol{N}$ for any p. For the real quadratic case, we remarked in [2, Remark 3] that $\operatorname{Im}\delta_p^+$ contains 1 and 2 for any p. The purpose of the present note is to prove the following:

Theorem. *The image of the map δ_p^+ contains 2^n for all $n \geq 0$ and any prime number p.*

Notation. We denote by $\boldsymbol{N}$ and $\boldsymbol{Q}$ the set of natural numbers and the field of rationals, respectively. The ideal class group Cl_K of a quadratic field K is the one in the usual sense. Namely, Cl_K is the quotient of the group of fractional ideals by the subgroup of *all* principal ideals.

2. Lemma. We fix a prime number p and a natural number n. Take natural numbers r and X such that

(1) $(r, 2p) = 1$ and $r \notin (\boldsymbol{Q}^\times)^2$,
(2) $(X, 2p) = 1$ and $X \notin (\boldsymbol{Q}^\times)^2$.

We assume that r and X satisfy the following conditions.

(3) $rX \notin (\boldsymbol{Q}^\times)^2$ and $rX + 4p^{2^n} \notin (\boldsymbol{Q}^\times)^2$.
(4) There exist natural numbers Y, Z such that

$$r(Y^2 - X^2Z^2) = 4(XZ^2p^{2^n} \pm 1).$$

By the conditions (1), (2) and (3), $rX(rX + 4p^{2^n})$ is not a square in $\boldsymbol{Q}^\times$, and hence

$$K = \boldsymbol{Q}(\sqrt{rX(rX + 4p^{2^n})})$$

is a real quadratic field in which p splits. Let $\mathcal{P}$ be a prime ideal of K over p. For an ideal $\mathcal{A}$ of K, we denote by $[\mathcal{A}]$ the ideal class represented by $\mathcal{A}$. The following lemma is a consequence of the well known fact (cf. eg. Hecke [1, Section 45]) on 2–ranks of the ideal class groups of quadratic fields.

Lemma. *Under the above setting, the order of $[\mathcal{P}]$ is 2^{n+1}. Namely, $\delta_p^+(K) = 2^{n+1}$.*

To prove this, we need the following claims.

Claim 1. $K(\sqrt{r}) \neq K(\sqrt{rX + 4p^{2^n}})$.

Claim 2. *Let ϵ be the fundamental unit of K with $\epsilon > 1$. Then, $N(\epsilon) = 1$ and $K(\sqrt{\epsilon}) = K(\sqrt{r})$. Here, N denotes the norm map.*

Proof of Claim 1. This follows easily from (1), (2) and (3). □

Proof of Claim 2. From (4), we see that

$$\delta = \frac{Y\sqrt{r} + Z\sqrt{X(rX + 4p^{2^n})}}{2}$$

is a unit of $K(\sqrt{r})$ and that $\delta \notin K^\times$. Therefore, $\eta = \delta^2$ is a totally positive unit of K and $\eta \notin (K^\times)^2$. From this, we obtain the assertion. □

Proof of Lemma. Put $x = rX + 4p^{2^n}$ for brevity. We have

$$K = \boldsymbol{Q}(\sqrt{x(x - 4p^{2^n})}).$$

Write $x = f^2d$ with d square free, and $d = \ell_1 \cdots \ell_s$ where ℓ_i $(1 \leq i \leq s)$ are prime numbers different from each other. By (1) and (2), d and $x - 4p^{2^n}$ are relatively prime. Hence, ℓ_i is ramified in K : $(\ell_i) = \mathcal{L}_i^2$.

We put

$$\alpha = \frac{x + \sqrt{x(x - 4p^{2^n})}}{2}.$$

We have $N(\alpha) = xp^{2^n}$ and $Tr(\alpha) = x$ where Tr is the trace map. Hence, $(\alpha, \alpha') \supseteq (x)$. From these, we obtain

$$(\alpha) = f\mathcal{L}_1 \cdots \mathcal{L}_s\mathcal{P}^{2^n},$$

Partially supported by Grant-in-Aid for Scientific Research (C), (No. 11640041), the Ministry of Education, Science, Sports and Culture of Japan.

where $\mathcal{P}$ is a prime ideal of K over p. Therefore, it suffices to show that $[\mathcal{L}_1 \cdots \mathcal{L}_s] \neq 1$ since $(\mathcal{L}_1 \cdots \mathcal{L}_s)^2 = (d)$.

Assume, to the contrary, that $[\mathcal{L}_1 \cdots \mathcal{L}_s] = 1$. Then, we have

$$(A + B\sqrt{d(x - 4p^{2^n})}) = \mathcal{L}_1 \cdots \mathcal{L}_s$$

for some $A, B \in \boldsymbol{Q}$. We easily see that $AB \neq 0$. Writing $A = A'd$, we obtain

$$(A'\sqrt{d} + B\sqrt{x - 4p^{2^n}}) = (1)$$

in $K(\sqrt{d})$. Therefore,

$$\delta' = A'\sqrt{d} + B\sqrt{x - 4p^{2^n}}$$

is a unit of $K(\sqrt{d})$, and $\delta' \notin K^\times$ (as $AB \neq 0$). Hence, $\eta' = \delta'^2$ is a totally positive unit of K and $\eta' \notin (K^\times)^2$. From this, we see that $K(\sqrt{d}) = K(\sqrt{\epsilon})$. Therefore, by Claim 2, we obtain

$$K(\sqrt{r}) = K(\sqrt{d}) = K(\sqrt{rX + 4p^{2^n}}).$$

However, this is impossible by Claim 1. $\square$

3. Proof of Theorem. It suffices to give a real quadratic field $K \in M(p)^+$ such that $\delta_p^+(K) = 2^m$ for each integer $m \geq 2$ by [2, Remark 3]. For $n \geq 1$, we define an integer a_n as follows and put $K_n = \boldsymbol{Q}(\sqrt{a_n})$.

$$a_n = \begin{cases} 3(3p^{2^n}+1)(25p^{2^n}+3) & \text{when } p \geq 5 \\ 7(7p^{2^n}+1)(81p^{2^n}+7) & \text{when } p = 3 \\ 3(12p^{2^n}+1)(64p^{2^n}+3) & \\ \qquad\qquad \text{when } p = 2 \text{ and } n \text{ is odd} & \\ 3(48p^{2^n}-1)(196p^{2^n}-3) & \\ \qquad\qquad \text{when } p = 2 \text{ and } n \text{ is even.} & \end{cases}$$

Clearly, p splits in K_n. The above real quadratic field is obtained by setting

$$(r, X, Y, Z) = \begin{cases} ((3p^{2^n}+1)/4, 3, 5, 1) & \text{when } p \geq 5 \\ ((7p^{2^n}+1)/8, 7, 9, 1) & \text{when } p = 3 \\ ((12p^{2^n}+1)/7, 3, 8, 2) & \\ \qquad\qquad \text{when } p = 2 \text{ and } n \text{ is odd} & \\ ((48p^{2^n}-1)/13, 3, 14, 4) & \\ \qquad\qquad \text{when } p = 2 \text{ and } n \text{ is even} & \end{cases}$$

in the notation of Section 2. When $(p, n) \neq (3, 1)$, the above quadruple satisfies the conditions (1),..., (4) in Section 2, and hence $\delta_p^+(K_n) = 2^{n+1}$ by the Lemma. When $(p, n) = (3, 1)$, it is easy to see that $\delta_3^+(K_1) = 2^2$. Therefore, we obtain the Theorem. $\square$

Remark. For an integer x relatively prime to $2p$ and a natural number N, we put

$$K = \boldsymbol{Q}(\sqrt{x^2 \pm 4p^N}) \quad \text{and} \quad \beta = \frac{x + \sqrt{x^2 \pm 4p^N}}{2}.$$

We see that p splits in K and that $(\beta) = \mathcal{P}^N$ where $\mathcal{P}$ is a prime ideal of K over p. It is plausible that $\delta_p^+(K) = N$ for infinitely many x. Namely, we can hope that $\mathrm{Im}\ \delta_p^+ = \boldsymbol{N}$ and that the inverse image $(\delta_p^+)^{-1}(N)$ of N is an infinite set for each N. Quadratic fields of the form $\boldsymbol{Q}(\sqrt{a^2 \pm 4b^N})$ were used by Nagell [3], Yamamoto [4] and several others to construct quadratic fields whose class numbers are divisible by a given integer N.

References

[1] E. Hecke: Lectures on the Theory of Algebraic Numbers. Springer, New York, pp. 1–239 (1981).

[2] H. Ichimura: A note on quadratic fields in which a fixed prime number splits completely. Nagoya Math. J., **99**, 63–71 (1985).

[3] T. Nagell: Über die Klassenzahl imaginär–quadratischer Zahlkörper. Abh. Math. Sem. Univ. Hamburg, **1**, 140–150 (1922).

[4] Y. Yamamoto: On unramified Galois extensions of quadratic number fields. Osaka J. Math., **7**, 57–76 (1970).