41. Orders in Quadratic Fields. III

By R. A. MOLLIN

Mathematical Department, The University of Calgary, Canada

(Communicated by Shokichi IYANAGA, M. J. A., June 7, 1994)

Abstract: We disprove a conjecture posed in [3] concerning a criterion for the class group of complex quadratic orders to be generated by given ideal classes. Secondly we prove a necessary and sufficient condition for the class group C_Δ (for $\Delta < 0$) to be generated by ambiguous ideals in terms of the factorization of the Rabinowitsch polynomial. This shows that the well-known Rabinowitsch result [5] linking $h_\Delta = 1$ to the primality of Frobenius-Rabinowitsch polynomial for $\Delta < 0$ is not just a curiosity but rather underlies a deeper phenomenon.

The results herein continue the work of [3]-[4] to which we refer the reader for background and notation. The conjecture in [3, p. 48] says that the converse of [3, Theorem 2.1, p. 46] holds. We now show that this is, in fact, false. First, we need a useful technical result.

Lemma 1. *Let Δ be a discriminant with conductor f such that $(f, F_{\Delta,1}(x)) = 1$ for all integers $x \geq 0$. If a prime p divides Δ_0 then p^2 does not divide $F_{\Delta,1}(x)$ for any non-negative integers x.*

Proof. Since

$$4F_{\Delta,1}(x) = (2x + \sigma - 1)^2 - \Delta,$$

then $F_{\Delta,1}(x) \equiv 0 (mod\ p^2)$ implies that p^2 divides Δ; whence, $p = 2$ and $\Delta \equiv 0 (mod\ 4)$. However, in this case, $F_{\Delta,1}(x) = x^2 - \Delta/4 = x^2 - f^2 D_0$ where $D_0 \equiv 2$ or $3\ (mod\ 4)$, a contradiction to $F_{\Delta,1}(x) \equiv 0 (mod\ 4)$.

The following example shows that the conjecture is false for $\Delta > 0$.

Example 1. Let $\Delta = \Delta_0 = 2^2 \cdot 5 \cdot 11 = 220$ where $D_0 = 55 \equiv 3 (mod\ 4)$, then $C_\Delta = \langle Q_2 \rangle$ where Q_2 is the unique ideal over 2, and $\lfloor M_\Delta \rfloor = 7$ ($\lfloor y \rfloor$ denotes the greatest integer less than or equal to y.) If the conjecture were true, then there would exist an integer $x \geqq 0$ and a $q \mid 2$ such that $| F_{\Delta,q}(x) | = 5r$ where r is not divisible by any unramified primes. By Lemma 1, $5r$ must be square-free; whence, $r \mid 22$. We further note that $F_{\Delta,1}(x) = x^2 - 55$ and $F_{\Delta,2}(x) = 2x^2 + 2x - 27$. To examine the possibilities we consider the following chart where we exhibit all $F_{\Delta,q}(x)$ such that $x \geq 0$, $q \mid 2,5 \mid F_{\Delta,q}(x)$ and $| F_{\Delta,q}(x) | \leq 110$.

x	0	10
$\lvert F_{\Delta,1}(x) \rvert$	$5 \cdot 11$	$5 \cdot 9$

x	2	7
$\lvert F_{\Delta,2}(x) \rvert$	$5 \cdot 3$	$5 \cdot 17$

We observe that only $| F_{\Delta,1}(x) | = 5 \cdot 11$ fits the criterion. However, the

conjecture further states that we must now be able to find an integer $y \geq 0$ and $q \mid 2$ such that $\mid F_{\Delta,q}(y) \mid = 11$ which is clearly impossible.

The following example shows that the conjecture is false for $\Delta < 0$.

Example 2. Let $\Delta = \Delta_0 = -3 \cdot 11 \cdot 19 = -627 \equiv 1 (mod\ 4)$ then $\lfloor M_\Delta \rfloor = 14$ and $C_\Delta = \langle Q_{11} \rangle \times \langle Q_{19} \rangle$ with $Q_3 \sim Q_{11}Q_{19}$ where Q_q (for $q = 3$, 11, or 19) is the unique ideal over q. If the conjecture were true then we could have an integer $x \geq 0$ and $q \mid 209$ such that $F_{\Delta,q}(x) = 3r$ where $r \mid 209$ (by Lemma 1). We now investigate this possibility in the following chart where we exhibit all $x \geq 0$ and $F_{\Delta,q}(x) = qx^2 + qx + (q^2 - \Delta)/4q$ with $q \mid 209$, $3 \mid F_{\Delta,q}(x)$ and $F_{\Delta,q}(x) \leq 627$.

x	1	4	7	10	13	16	19
$F_{\Delta,1}(x)$	$3 \cdot 53$	$3 \cdot 59$	$3 \cdot 71$	$3 \cdot 89$	$3 \cdot 113$	$3 \cdot 11 \cdot 13$	$3 \cdot 179$

x	1	4
$F_{\Delta,11}(x)$	$3 \cdot 13$	$3 \cdot 79$

x	1	4
$F_{\Delta,19}(x)$	$3 \cdot 17$	$3 \cdot 131$

x	1
$F_{\Delta,209}(x)$	$3 \cdot 157$

The chart yields no satisfaction of the necessary criterion, hence the conjecture fails.

Remark 1. The main result of Halter-Koch in [1] is false. This motivated our main result in [2] which not only corrected the error in [1] but also provided a sufficient condition for the class group to be generated by ambiguous ideals (hence of exponent $e_\Delta \leq 2$). Theorem 2.1 of [3] weakened the hypothesis of Theorem 3.1 of [2], generalized the result to arbitrary orders and achieved the same conclusion as that of Theorem 3.1 of [2]. The conjecture made in [3] said that the converse of Theorem 2.1 of [3] holds. Examples 1–2 above, show that this is false. However, these examples suggest the hypothesis of Theorem 2.1 of [3] might be weakened further in order to get a necessary and sufficient condition. For instance, in Example 1, $F_{\Delta,1}(10) = 5 \cdot 9$ and $F_{\Delta,1}(8) = 9$; and in Example 2, $F_{\Delta,19}(1) = 3 \cdot 17$ and $F_{\Delta,11}(0) = 17$. Thus, one might be lured into thinking that perhaps the hypothesis of Theorem 2.1 of [3] could be weakened by allowing r to be divisible by *unramified* primes. The following example shows that if we do so then Theorem 2.1 of [3] fails.

Example 3. Let $\Delta = -2^3 \cdot 13$ then $\lfloor M_\Delta \rfloor = 5$ and both 3 and 5 split. Since $F_{\Delta,1}(x) = x^2 + 26$ and $F_{\Delta,2}(x) = 2x^2 + 13$, then $F_{\Delta,2}(2) = 21$ and $F_{\Delta,2}(5) = 3 \cdot 21$, while $F_{\Delta,1}(5) = 51$ and $F_{\Delta,2}(11) = 5 \cdot 51$. However, $C_\Delta \neq \langle Q_2 \rangle$, in fact, $C_\Delta = \langle Q_2 \rangle \times \langle Q_3 \rangle$, with $h_\Delta = 6$.

The following example shows how (even for maximal orders) Theorem 2.1 of [3] is an improvement over Theorem 3.1 of [2] in that we may have C_Δ generated by ambiguous ideals with $\mid F_{\Delta,q}(x) \mid$ not being prime for all relevant non-inert primes less than M_Δ.

Example 4. Let $\Delta = -2^2 \cdot 3 \cdot 7$ then $\lfloor M_\Delta \rfloor = 5$ and $C_\Delta = \langle Q_2 \rangle \times \langle Q_3 \rangle$ with the split prime $Q_5 \sim Q_2 Q_3$. A look at $F_{\Delta,q}(x)$ for $q \mid 6$ shows that $F_{\Delta,q}(x) \neq 5$ for any q and any $x \geq 0$. However, $F_{\Delta,2}(3) = 5 \cdot 7$ and $F_{\Delta,3}(0) = 7$.

Despite the negative aspects of Examples 1-3, we now obtain necessary and sufficient conditions for the generation of C_Δ by ambiguous ideals when $\Delta < 0$ in terms of the factorization of the Rabinowitsch polynomial $F_{\Delta,1}(x)$. This result (Theorem 1 below) turns out to be a very palatable generalization of the well-known Rabinowitsch [5] result for complex quadratic fields and yields more recent results in the literature as consequences such as Sasaki [6].

The following generalizes [6, Lemma 2, p. 38].

Lemma 2. *If $\Delta < 0$ is a discriminant and $I = [a, b + \omega_\Delta]$ is a primitive, regular ideal of O_Δ with $N(b + \omega_\Delta)^2 < N(\omega_\Delta)^2$ then I is principal if and only if $a = 1$ or $a = N(b + \omega_\Delta)$.*

Proof. Clearly, if $a = 1$, then I is principal and if $a = N(b + \omega_\Delta)$ then $I = (b + \omega_\Delta)$ is principal. On the other hand, if $I = [a, b + \omega_\Delta] \sim 1$ and $ac = N(b + \omega_\Delta) < N(\omega_\Delta)^2$ then either $a < N(\omega_\Delta)$ or $c < N(\omega_\Delta)$. However, since $I \sim 1$ then there are integers x and y with $\alpha = ax + (b + \omega_\Delta)y$ and $N(\alpha) = a$. Thus, $a = (ax + by)^2 + (\omega_\Delta + \bar{\omega}_\Delta)xy + \omega_\Delta \bar{\omega}_\Delta y^2 > \omega_\Delta \bar{\omega}_\Delta = N(\omega_\Delta)$ if $y \neq 0$, since $N(\omega_\Delta) > 0$ when $\Delta < 0$. Thus, if $a < N(\omega_\Delta)$ then $a = 1$. If $c < N(\omega_\Delta)$ then since $(b + \omega_\Delta) = [ac, b + \omega_\Delta] = [a, b + \omega_\Delta]$ $[c, b + \omega_\Delta]$ we must have $[c, b + \omega_\Delta] \sim 1$. By the same argument as above, $c = 1$.

Corollary 1. *If $\Delta < 0$ and $I = [a, b + \omega_\Delta]$ is a primitive, regular ideal of O_Δ and $1 < a < N(\omega_\Delta)$, $N(b + \omega_\Delta) < N(\omega_\Delta)^2$ then I is not principal.*

We will also need the following useful fact.

Lemma 3. *If $\Delta < 0$ ($\Delta \neq -3, -4$) is a discriminant then $F_{\Delta,1}(x) < N(\omega_\Delta)^2$ if and only if $x \in I = \{0,1,2,\ldots,\lfloor |\Delta|/4 - 1 \rfloor\}$.*

Proof. We have that $F_{\Delta,1}(x) = ((\sigma x + \sigma - 1)^2 - D)/\sigma^2$. If $\sigma = 1$, then $\lfloor |\Delta|/4 - 1 \rfloor = -D - 1$; whence, $F_{\Delta,1}(x) \leq F_{\Delta,1}(-D - 1) = (D + 1)^2 - D = D^2 + D + 1 < D^2 = N(\omega_\Delta)^2$ unless $\Delta = -4$ which is excluded by hypothesis. If $\sigma = 2$, then $\lfloor |\Delta|/4 - 1 \rfloor = -(D + 7)/4$; whence, $F_{\Delta,1}(x) \leq F_{\Delta,1}(-(D + 7)/4) = ((1 - (D + 7)/2)^2 - D)/4 = (D^2 + 6D + 25)/16 < (D^2 - 2D + 1)/16 = N(\omega_\Delta)^2$, unless $\Delta = -3$ which is excluded by hypothesis. Hence, if $x \in I$ then $F_{\Delta,1}(x) < N(\omega_\Delta)^2$.

Suppose that $F_{\Delta,1}(x) < N(\omega_\Delta)^2$. If $\sigma = 1$ then $F_{\Delta,1}(|\Delta|/4) = F_{\Delta,1}(-D) = D^2 - D > D^2 = N(\omega_\Delta)^2$. Thus, $x \leq |\Delta|/4 - 1$. If $\sigma = 2$ then $F_{\Delta,1}(-(D + 3)/4) = N(\omega_\Delta)^2$. Since $-(D + 3)/4 = \lceil |\Delta|/4 - 1 \rceil$ where $\lceil x \rceil$ denotes the least integer greater than or equal to x, then $x \leq -(D + 7)/4 = \lfloor |\Delta|/4 - 1 \rfloor$.

Remark 2. It is worth observing that the proof of Lemma 3 actually shows that $x = \lfloor |\Delta|/4 - 1 \rfloor$ is the **largest** integer such that $F_{\Delta,1}(x)$ is less than $N(\omega_\Delta)^2$.

Definition 1. Let $F(\Delta)$ denote the maximum number of (not necessarily

distinct) primes which divide $F_{\Delta,1}(x)$ for any $x \in I$.

Although the following holds for arbitrary orders we prove it only for maximal orders so that we may present it in its most palatable, and as it turns out, most useful form.

Theorem 1. *Let $\Delta = \Delta_0 < 0$ ($\Delta \neq -3, 4$) be a discriminant divisible by exactly $N+1$ ($N \geq 0$) distinct primes then C_Δ is generated by ambiguous ideals if and only if $h_\Delta = 2^{F(\Delta)-1}$ and $F(\Delta) = N+1$.*

Proof. Since Gauss tells us that C_Δ is generated by ambiguous ideals if and only if $h_\Delta = 2^N$ then the 'if' part of the proof is clear. We now prove the 'only if' part.

First we establish that $2^{F(\Delta)-1} \geq h_\Delta$. If $N = 0$ then $h_\Delta = 1$ so this is clear (observing that $F(\Delta) \geq 1$ since $F(\Delta) = 0$ if and only if $\Delta = -3$ or -4). So assume that $N \geq 1$ and let $C_\Delta = \langle Q_1 \rangle \times \langle Q_2 \rangle \times \ldots \times \langle Q_N \rangle$ with $h_\Delta = 2^N$ where Q_i is the unique O_Δ-prime above the prime divisor q_i of Δ for $i = 1,2,\ldots,N$. By Gauss, Δ is divisible by exactly one more distinct prime q_{N+1} which we may assume without loss of generality (by Theorem 1.2 of [3]) is the largest such prime. Form the ideal $Q = \prod_{i=1}^{N} Q_i$ which has a representation $Q = [q, b + \omega_\Delta]$ where $0 \leq b < q = \prod_{i=1}^{N} q_i$. Moreover, $q < |\Delta|/4 - 1$ (since $\Delta = -3$ or -4 by hypothesis, and $\Delta \neq -7$ for which $N = 0$). Since Q is not principal (being the product of the generators of C_Δ) then q divides $N(b + \omega_\Delta) = F_{\Delta,1}(b) > q$. Hence, $F(\Delta) \geq N + 1$; i.e., $2^{F(\Delta)-1} \geq h_\Delta$. Now we show that $h_\Delta \geq F(\Delta) - 1$.

Let $F(\Delta) = n$ then there exists an $x \in I$ such that $r = \prod_{i=1}^{M} p_i^{e_i} = F_{\Delta,1}(x)$ where the p_i's are distinct primes for $1 \leq i \leq M$ and $\sum_{i=1}^{M} e_i = n$ ($M \geq 1$ since $F(\Delta) = 0$ if and only if $\Delta = -3$ or -4). Thus if $P = \prod_{i=1}^{M} P_i^{e_i} = [r, x + \omega_\Delta]$ where P_i is a fixed choice of ideal over p_i for $1 \leq i \leq M$ then P is a primitive principal ideal since $N(x + \omega_\Delta) = F_{\Delta,1}(x) = r$. Now, let $S' \subseteq S = \{1,2,\ldots,N\}$ be the subset of indices, i, such that e_i is odd. Hence, (since $e_\Delta \leq 2$) we have $1 \sim P \sim \prod_{i \in S'} P_i = [r', x + \omega_\Delta]$ where $r' = \prod_{i \in S'} p_i$. Therefore, by Lemmas 2-3, either $r' = 1$ (in which case e_i is even for all $i \in S$) or $r' = r$ (in which case $e_i = 1$ for all $i \in S$ and $n = M$). If the former occurs then $1 \sim P \sim P_1^2 = [p_1^2, x + \omega_\Delta]$. By Lemma 2, $p_1^2 = N(x + \omega_\Delta) = r$; i.e., $M = 1$ and $e_1 = 2 = n$. Thus $p_1 < N(\omega_\Delta)$ and $h_\Delta \geq 2 = 2^{F(\Delta)-1}$ by Corollary 1. Thus for the remainder of the proof, we may assume the latter above; i.e., that $n = F(\Delta) = M$ and $e_i = 1$ for $1 \leq i \leq M$.

Suppose that a_1 and a_2 are two positive relatively prime divisors of r. If $I_1 = [a_1, x + \omega_\Delta] \sim I_2 = [a_2, x + \omega_\Delta]$ then $J = I_1 I_2 = [a_1 a_2, x + \omega_\Delta] \sim I_2^2 \sim 1$ since $e_\Delta \leq 2$. Moreover, J is a principal, primitive ideal since $\gcd(a_1, a_2) = 1$. Therefore, by Lemma 2, $N(x + \omega_\Delta) = a_1 a_2$. Thus, the exact number of equivalences among ideals whose norms are relatively prime positive divisors of r is equal to the number of distinct factorizations of r into 2 positive factors (where order of the factors is **not** taken account). We claim that this number is 2^{n-1}. To see this, a simple induction argument will suffice. If $n = 1$ then there is the trivial factorization $r = p_1 \cdot 1$ ($p_1 = 1$ or $p_1 =$ prime) only; i.e., $2^{n-1} = 2^0 = 1$ such factorizations. Assume that $\prod_{i=1}^{n-1} p_i$ has 2^{n-2}

factorizations and we prove that $r = \prod_{i=1}^{n} p_i$ has 2^{n-1} factorizations. To the 2^{n-2} factorization of $\prod_{i=1}^{n-1} p_i$ we must add those now involving p_n and there are $\sum_{i=0}^{n-1} \binom{n-1}{i}$ of them (since for each $i = 0,1,\ldots,n-1$ we choose i of the p_i's to form a product with p_n). Moreover, $\sum_{i=0}^{n-1} \binom{n-1}{i} = 2^{n-2}$ (since this is just a special case of the binomial theorem $(a+b)^{n-1} = \sum_{i=0}^{n-1} \binom{n-1}{i} a^{n-1-i} b^i$ with $a = b = 1$). Hence there are a total of $2 \cdot 2^{n-2} = 2^{n-1}$ distinct factorizations of r, thereby securing the claim.

We have therefore shown that there are $\tau(r) - 2^{n-1} = 2^n - 2^{n-1} = 2^{n-1}$ pairwise inequivalent ideals; i.e., $h_\Delta \geq 2^{F(\Delta)-1}$.

Remark 3. The proof of Theorem 1 actually contains some hidden information which we isolate below. First we need another definition.

Definition 2. Let $G(\Delta)$ denote the maximum number of *distinct* primes which divide $F_{\Delta,1}(x)$ for any $x \in I$.

Corollary 2. *If $\Delta = \Delta_0 < 0$ ($\Delta \neq -3, -4$) C_Δ is generated by ambiguous ideals then $F(\Delta) = G(\Delta) = N + 1$.*

Proof. The proof of Theorem 1 shows that the result holds except possibly when $F(\Delta) = 2$. We now show that if $F(\Delta) = 2$ then $G(\Delta) = 2$. By Theorem 1, $h_\Delta = 2$. If $\Delta \equiv 0 \pmod 8$ then $F_{\Delta,1}(0) = -\Delta/4$ is even composite. If $\Delta \equiv 4 \pmod 8$ then $F_{\Delta,1}(1) = 1 - \Delta/4$ is even composite (since $\Delta < -4$ when $h_\Delta = 2$). If $\Delta \equiv 1 \pmod 8$ then $F_{\Delta,1}(0) = (1-\Delta)/4$ is even composite. If $\Delta \equiv 5 \pmod 8$ then $h_\Delta = 2$ implies $\Delta = -q_1 q_2$ where $q_1 \neq q_2 \pmod 4$. Thus $F_{\Delta,1}((q_1 - 1)/2) = q_1(q_1 + q_2)/4$ is composite.

Corollary 3. *$F(\Delta) \geq N + 1$ for any discriminant $\Delta = \Delta_0 < 0$ ($\Delta \neq -3, -4$).*

Proof. By Gauss, C_Δ always contains an elementary abelian 2-subgroup of order 2^N. The result now follows as in the second paragraph of the proof of Theorem 1.

Remark 4. In [6], Sasaki observed (in his Remark at the end of the paper) that there are fields for which $h_\Delta > F(\Delta)$ and cites $\Delta = -21$ as an example where $h_\Delta = 4$ and $F(\Delta) = 3$. However, Theorem 1 asserts that C_Δ is generated by ambiguous ideals if and only if $h_\Delta = 2^{F(\Delta)-1} = 2^{N-1}$. Thus $h_\Delta = F(\Delta)$ if and only if $h_\Delta = 1$ or 2 (when $e_\Delta \leq 2$). These fields are uniquely characterized by the following well-known results.

Corollary 4 (Rabinowitsch [5]). *If $\Delta = \Delta_0 < 0$ ($\Delta \neq -3, -4$) is a discriminant then $h_\Delta = 1$ if and only if $F(\Delta) = 1$.*

Proof. If $h_\Delta = 1$ then by Theorem 1, $F(\Delta) = 1$. If $F(\Delta) = 1$ and $p < \sqrt{-\Delta/3}$ is any non-inert prime, then we may form the ideal $P = [p, b + \omega_\Delta]$ where $0 \leq b < p < \sqrt{-\Delta/3} \leq -\Delta/4$ (since $\Delta \neq -3, -4$). Since $p \mid N(b + \omega_\Delta)$ then $F_{\Delta,1}(b) = N(b + \omega_\Delta) = p$ so $P \sim 1$. This secures the result by Theorem 1.2 of [3].

Corollary 5 (Sasaki [6]). *If $\Delta = \Delta_0 < 0$ is a discriminant then $h_\Delta = 2$ if and only if $F(\Delta) = 2$.*

Proof. If $h_\Delta = 2$ then $F(\Delta) = 2$ by Theorem 1. If $F(\Delta) = 2$ then let P and Q be any non-principal prime ideal. We may assume that $-\Delta \leq -12$ (since $h_\Delta = 1$ otherwise contradicting Corollary 3). Thus $I = [pq, b +$

$\omega_\Delta]$ with $0 \leq b < pq < -\Delta/3 \leq -\Delta/4 - 1$, thus $N(b + \omega_\Delta) = F_{\Delta,1}(b) = pq$ forcing $PQ \sim 1$. In particular, if $P = Q$ then $P^2 \sim 1$; i.e., $e_\Delta = 2$. Furthermore, if $h_\Delta \geq 4$ then let P and Q be distinct generators of C_Δ. Since $PQ \sim 1$ then $P \sim Q' \sim Q$ (since the conjugate Q' must be in the same class as Q when $e_\Delta = 2$), a contradiction.

Remark 5. We note that the condition $F(\Delta) = N + 1$ cannot be removed in Theorem 1 and still maintain a necessary and sufficient condition. Although we have clearly shown that when C_Δ is generated by ambiguous ideals then $h_\Delta = 2^{F(\Delta)-1}$, the converse fails without the condition that $F(\Delta) = N + 1$. For example, if $\Delta = -2^3 \cdot 23$ then $N = 1$, $F(\Delta) = 3$, $h_\Delta = 4 = 2^{F(\Delta)-1}$, but C_Δ is cyclic. We have also shown that if C_Δ is generated by ambiguous ideals then $F(\Delta) = N + 1$. However, if we remove the condition $h_\Delta = 2^{F(\Delta)-1}$ then the converse fails. For example, if $\Delta = -9867$ then $F(\Delta) = N + 1 = 4$ but $h_\Delta = 2^4 \neq 2^{F(\Delta)-1}$. Hence C_Δ has an element of order 4.

Acknowledgements. The author's research is supported by NSERC Canada grant # A8484. Also, thanks must go to the referee for so carefully looking at original manuscript which led to a complete rewriting of the results for a much sounder and more complete paper.

References

[1] F. Halter-Koch: Prime-producing quadratic polynomials and class numbers of quadratic orders. Computational Number Theory (eds. A. Petho, *et al.*). de Gruyter, Berlin, pp. 73–82 (1991).

[2] R. A. Mollin: Ambiguous Classes in Quadratic Fields. Math. Comp., **61**, 355–360 (1991).

[3] ——: Orders in quadratic fields. I. Proc. Japan Acad., **69**A, 45–48 (1993).

[4] R. A. Mollin and L.-C. Zhang: Orders in quadratic fields II. ibid., **69**A, 368–371 (1993).

[5] G. Rabinowitsch: Eindeutigkeit der Zerlegung in Primfaktoren in quadratischen Zahlkörpern. J. Reine angew. Math., **142**, 153–164 (1913).

[6] R. Sasaki: On a lower bound for the class number of an imaginary quadratic field. Proc. Japan Acad., **62**A, 37–39 (1986).