10. On Class Numbers of Quadratic Extensions of Algebraic Number Fields

By Richard A. MOLLIN
Mathematics Department, University of Calgary,
Calgary, Alberta, Canada, T2N 1N4

(Communicated by Shokichi IYANAGA, M. J. A., Jan. 13, 1986)

In [14] Nagell showed that there are infinitely many imaginary quadratic extensions of the rational number field $\boldsymbol{Q}$, each of which has class number divisible by a given integer. Subsequently several authors have proved this result (see [1], [4], [5] and [17] as well as the most recent proof by Uehara [16]). In this paper we generalize this well-known result by explicit construction of infinitely many imaginary quadratic extensions of a given number field K (subject only to having a totally ramified rational prime) each with class number divisible by a given integer. The proof and construction given is simpler than that given in previous proofs cited above for the trivial case $K=\boldsymbol{Q}$, and applications are given. The next result is a sufficient condition for an arbitrary quadratic extension of $\boldsymbol{Q}$ to have an element of given order in its class group. Finally for a certain class of real quadratic extensions of $\boldsymbol{Q}$ we give a sufficient condition for its class number to be divisible by a given prime, and we provide applications.

Before presenting the first result some comments on notation and a lemma are required. For a given number field K, $h(K)$ denotes the class number of K, C_K denotes the class group of K, $\mathcal{O}_K$ denotes the ring of integers of K, (α) for $\alpha \in \mathcal{O}_K$ denotes the principal ideal generated by α, and $N(\cdot)$ denotes the norm from K to $\boldsymbol{Q}$.

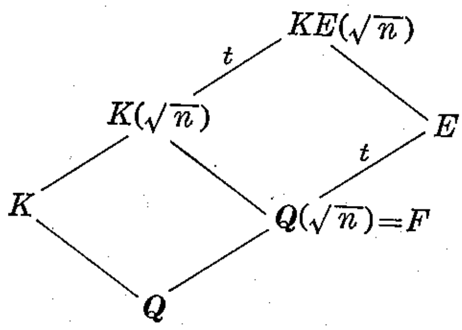
In the proof of Theorem 1 we will need the following result whose proof (mutatis mutandis) is the same as that of [1, Lemma 1, p. 321] of which the following lemma is a generalization.

Lemma 1. *Let ε be any positive real number and let p be any odd prime. Denote by N the number of square-free integers of the form p^g-x^2 where x is an even integer such that $0<x<\varepsilon p^{g/2}$. Then for g sufficiently large, $N\geq c_p\varepsilon p^{g/2}$ where c_p is a positive constant depending only on p.*

Theorem 1. *Let $t>1$ be any integer. If K is any algebraic number field in which there is a totally ramified rational odd prime p, then there are infinitely many imaginary quadratic extensions L of K such that $t \mid h(L)$. Moreover L may be chosen of the form $K(\sqrt{n})$ where n is any square-free rational integer of the form $n=r^2-m^t$ where p does not divide n and r is an even integer subject to $r^2\leq m^{t-1}(m-1)$.*

Proof. Let r be an arbitrarily chosen but fixed even integer. Let n

be an integer of the form $n=r^2-m^t$ where m is any odd integer with $r^2 \leq m^{t-1}(m-1)$ and p does not divide n. By [7, Corollary 2.6] $t \mid h(\boldsymbol{Q}(\sqrt{n}))$. Therefore there exists an abelian unramified extension E of $F=\boldsymbol{Q}(\sqrt{n})$ with $|E:F|=t$. By Abhyankar's Lemma (see [2] or [3]) $KE(\sqrt{n})$ is an unramified extension of $K(\sqrt{n})$. Moreover we claim that $K \cap E=F$. To see this we recall that p does not ramify in F since p fails to divide n. Since p is totally ramified in K and ramification degrees multiply in towers then any $\boldsymbol{Q}(\sqrt{n})$-prime above p is totally ramified in $K(\sqrt{n})$. This proves the claim. Hence from [6, Theorem 7, p. 263] it follows that $KE(\sqrt{n})$ is of degree t over $K(\sqrt{n})$. The following diagram describes the situation:



To conclude the proof of the theorem it remains to show that there are infinitely many square-free integers of the form $n=r^2-m^t$ where r is even, $r^2 \leq m^{t-1}(m-1)$ and p does not divide n.

Let $\varepsilon=[(p-1)/p]^{1/2}$ and let k be sufficiently large such that $g=kt$ satisfies the hypothesis of Lemma 1; that is, the number N of square-free integers of the form m^t-r^2, with $m=p^k$, and $0<r<\varepsilon m^{t/2}$ is greater than $c_p \varepsilon m^{t/2}$. Since ε is fixed and c_p is a positive constant depending only on p then k may be chosen such that N is as large as we want. Q.E.D.

The following application to biquadratic fields is immediate from Theorem 1.

Corollary 1. *Let $K=\boldsymbol{Q}(\sqrt{s})$ where s is any square-free integer, and let $F=\boldsymbol{Q}(\sqrt{n})$ where g.c.d. $(n, 2s)=1$, $n=r^2-m^t$ is square-free, $r^2 \leq m^{t-1}(m-1)$ and r even, then $t \mid h(KF)$. (In fact $t \mid h(F)$.)*

The following is an application to imaginary quadratic extensions of pure fields of prime degree (see Mollin [11, pp. 421–423]).

Corollary 2. *Let $K=\boldsymbol{Q}(\sqrt[p]{p})$ where p is an odd prime, and let n be a square-free integer of the form $n=r^2-m^t$ relatively prime to p and with r even, and $r^2 \leq m^{t-1}(m-1)$; then $t \mid h(K(\sqrt{n}))$.*

The reader may compare the above with Mollin [8, pp. 166–168] where conditions for the divisibility of the class numbers of imaginary quadratic extensions of cyclotomic fields by a power of 2 are given.

We now turn to establishing a sufficient condition for any quadratic field to have an element of order $t>1$ in its class group for a given integer t.

Theorem 2. *Let $K=\boldsymbol{Q}(\sqrt{n})$, where $n=a^2-4b^t$ is a square-free integer where $b>1$ and $t>1$ are integers. If $\pm b^c$ is not the norm of any element of $\mathcal{O}_K$ for all c properly dividing t then t divides the exponent of C_K.*

Proof. Let $b=p_1^{a_1}\cdots p_r^{a_r}$ where the p_i's are distinct rational primes and the a_i's are positive integers. Clearly each p_i splits in K, so $p_i\mathcal{O}_K=\mathcal{P}_iQ_i$ where $\mathcal{P}_i$ and Q_i are $\mathcal{O}_K$-primes for $i=1, 2, \cdots, r$. Let $\alpha=(a+\sqrt{n})/2$ and $\bar{\alpha}=(a-\sqrt{n})/2$, then $(b)^t=(\alpha\bar{\alpha})=\prod_{i=1}^r(\mathcal{P}_iQ_i)^{a_it}$. Since $\alpha+\bar{\alpha}=a$, $(\alpha-\bar{\alpha})^2=n$ and g.c.d. $(a, b)=1$ (whence g.c.d. $(a, n)=1$), then $\mathcal{P}_i$ divides both α and $\bar{\alpha}$ only if 1 is in $\mathcal{P}_i$. Therefore, for an appropriate choice of $\mathcal{R}_i=\mathcal{P}_i$ or Q_i we must have that $(\alpha)=(\prod_{i=1}^r\mathcal{R}_i^{a_i})^t=\mathcal{A}^t$, say. If $\mathcal{A}^c$ is principal for any c properly dividing t then $N(\mathcal{A}^c)=\pm b^c$ violates the hypothesis. Hence $\mathcal{A}$ is an element of order t in C_K; i.e., t divides the exponent of C_K. Q.E.D.

Maintaining the notation of Theorem 2 we have:

Corollary 3 (Mollin [7, Corollary 2.4]). *If $n=a^2-4b^t<0$ and $a^2\leq 4b^{t-1}(b-1)$ then t divides $h(K)$.*

Note that if t divides the exponent of C_K then there is a non-principal ideal $\mathcal{J}$ such that $\mathcal{J}^t=(\alpha)$ for some $\alpha\in\mathcal{O}_K$, but $\mathcal{J}^c$ is not principal for any c properly dividing t. Therefore if $\alpha=(a+s\sqrt{m})/2$ then $a^2-s^2m=4b^t$ where $N(\mathcal{J})=b$; i.e., $K=\boldsymbol{Q}(\sqrt{n})=\boldsymbol{Q}(\sqrt{m})$ for $n=s^2m$. Is the converse of Theorem 2 valid?; i.e., is it true that if t divides the exponent of C_K then $\pm b^c$ is not the norm of any $\beta\in\mathcal{O}_K$ for all c properly dividing t? Note that if such a β exists then $N(\mathcal{J}^c)=N(\beta)$. However this does not necessarily imply that $\mathcal{J}^c$ is principal. Is there some restriction on K such that the condition "$\pm b^c$ is not a norm of an integer in $\mathcal{O}_K$" becomes necessary and sufficient for t to divide the exponent of C_K? Compare the above with Uehara [16, Theorem 2, p. 257].

We now turn to the real quadratic field case.

Proposition 1. *Let $K=\boldsymbol{Q}(\sqrt{n})$ where n is a square-free integer of the form $n=a^2+t^p\not\equiv 1 \pmod 4$ where $a>0$ and $t>1$ are integers and p is a prime. Suppose furthermore that $n=(st)^2+r>7$ where the following conditions are satisfied:*

(i) *$s>1$, t not a square and g.c.d. $(t, r)=1$.*

(ii) *r divides $4s$ with $-2s<r\leq 2s$;*

then p divides $h(K)$.

Proof. By Mollin [9, Theorem 1.2] $x^2-ny^2=\pm t$ is not solvable in integers (x, y), and so by Mollin [10, Theorem 3], p divides $h(K)$. Q.E.D.

The following table provides examples as an application of Proposition 1.

Table I

r	t	s	a	p	n	$h(n)$
1	3	1	1	2	10	2
1	5	1	1	2	26	2
1	9	1	1	2	82	4
1	11	1	1	2	122	2
1	13	1	1	2	170	4
−2	3	5	14	3	223	3
1	15	1	1	2	226	8
−2	3	7	14	5	439	5
4	9	3	4	3	733	3

All class numbers are taken from B. Oriat's "Groupes des Classes des Corps Quadratiques Réels $Q(\sqrt{d})$, $d<10,000$", Faculté des Sciences de Besançon.

Finally we note that Proposition 1 has relevance to the representation of integers as sums of powerful numbers, (see [12] and [13]), a difficult problem in elementary number theory.

Acknowledgement. The author welcomes the opportunity to thank the referee for pointing out the applicability of [1, Lemma 1, p. 321] in the proof of Theorem 1.

References

[1] N. C. Ankeny and S. Chowla: On the divisibility of the class number of quadratic fields. Pacific J. Math., **5**, 321–324 (1955).

[2] G. Cornell: Abhyankar's Lemma and the Class Group. Number Theory Carbondale, Springer Lecture Notes, **751**, 82–88.

[3] ——: On the construction of relative genus fields. Trans. Amer. Math. Soc., **271** (2), 501–511 (1982).

[4] P. Hampert: Sur les nombres de classes de certain corps quadratiques. Comment. Math. Helv., **12**, 233–245 (1939/40).

[5] S. N. Kuroda: On the class number of imaginary quadratic number fields. Proc. Japan Acad., **40**, 365–367 (1964).

[6] D. A. Marcus: Number Fields. Springer-Verlag, New York (1977).

[7] R. A. Mollin: Diophantine equations and class numbers (to appear in J. Number Theory).

[8] ——: On the cyclotomic polynomial. J. Number Theory, **17** (2), 165–175 (1983).

[9] ——: On the insolubility of a class of diophantine equations and the nontriviality of the class numbers of related real quadratic fields of Richaud-Degert type (to appear).

[10] ——: Lower bounds for class numbers of real quadratic fields (to appear in Proc. Amer. Math. Soc.).

[11] ——: Class numbers and a generalized Fermat theorem. J. Number Theory, **16** (3), 420–429 (1983).

[12] R. A. Mollin and P. G. Walsh: On Powerful Numbers (to appear).

[13] ——: On Nonsquare powerful numbers (to appear in The Fibonacci Quarterly).

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

[15] W. Narkiewicz: Number Theory. World Scientific Publishers, Singapore (1983).

[16] T. Uehara: On class numbers of imaginary quadratic and quartic fields. Archiv. der Math., **41** (3), 256–260 (1983).

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