CLASS NUMBERS OF PURE FIELDS

R. A. MOLLIN

ABSTRACT. Necessary and sufficient conditions are given for the class number \( h_{K_i} \) of a pure field \( K = Q(m^{1/p^i}) \) (for \( i = 1, 2 \)) to be divisible by \( p^r \) for a given positive integer \( r \) and prime \( p \). Moreover the divisibility of \( h_{K_i} \) by \( p \) is linked with the \( p \)-rank of the class group of the \( K(\zeta) \) and prime divisors of \( m \), where \( \zeta \) is a primitive \( p \)th root of unity.

Finally we prove in an easy fashion that for a given odd prime \( p \) and any natural number \( t \) there exist infinitely many non-Galois algebraic number fields (in fact pure fields) of degree \( p^t \) (\( i = 1, 2 \)) over \( Q \) whose class numbers are all divisible by \( p^t \).

1. Introduction. Pure cubic, quartic, quintic, and sextic fields have been extensively studied by many authors (for example see [3–4] and [8–12]). Parry and Walter [11] studied the Galois closure \( L = Q(\zeta, \sqrt[p]{m}) \) of pure fields \( K_1 = Q(\sqrt[p]{m}) \) of prime degree and classified those \( m \) for which the class number \( h_L \) of \( L \) is relatively prime to \( p \). However necessary and sufficient conditions (for arbitrary \( p \)) such that \( h_K \) is divisible by \( p \) have failed to make their way into the literature. Our first result is to give such conditions for regular primes. We use this result as a tool for linking the divisibility of \( h_K \) by \( p \) with the rank of the Sylow \( p \)-subgroup of the class group of \( L \) and also with certain primes dividing \( m \). Moreover for the pure fields \( K_2 = Q(\sqrt[p]{m^2}) \) of prime squared degree we obtain necessary conditions and sufficient conditions for \( h_{K_2} \) to be divisible by \( p \), and use this result as a tool to provide applications similar to that of \( K_1 \) described above.

Finally when \( m \) is divisible by \( t \) primes congruent to 1 modulo \( p \) we give an explicit description of an unramified extension of \( K_i \) (\( i = 1 \) or 2) of degree \( p^t \) (therefore of infinitely many such \( K_i \)).

2. Pure fields. Throughout the remainder of the discussion the following notation will be in force.

\[ Z = \text{the ring of rational integers.} \]
\[ Q = \text{the field of rational numbers.} \]
\[ p = \text{an odd rational prime.} \]
\[ m > 1, \text{a } p \text{-power free rational integer.} \]
\[ \zeta = \text{a primitive } p \text{th root of unity.} \]
\[ k = Q(\zeta) = \text{the } p \text{th cyclotomic field.} \]
\[ K_i = Q(m^{1/p^i}), \text{a pure field of degree } p^i, \text{where } i = 1 \text{ or } 2. \]
\[ L_i = K_i k, \text{where } i = 1 \text{ or } 2. \]
\[ G(F_1/F_2) = \text{the Galois group of a normal extension } F_1/F_2 \text{ of number fields.} \]
$U(F) = \text{the group of units of the ring of integers of a number field } F.$
$h_F = \text{the class number of a field } F.$
$C_F = \text{the ideal class group of a number field } F.$
$G(p) = \text{the Sylow } p\text{-subgroup of a group } G.$
$r(F,p) = \text{the rank of } C_F(p).$
$|y|_p = \text{the } p\text{-primary part of } y \in \mathbb{Z}.$
$a_1(p) = 1 + (p-3)/4.$
$a_2(p) = (p-1)^3/4.$
$b_1(p) = (p^2 - 5)/4.$
$b_2(p) = (p-1)^3/4 - (p-3)/2.$
$Q_1 = |U(L_1) : U(k)\prod_1 U(K_1)_i| \text{ with the product ranging over the conjugates (}K_1)_i \text{ of } K_1 \text{ over } Q.$
$Q_2 = |U(L_2) : U(L_1)\prod_1 U(K_2)_i| \text{ with the product ranging over the conjugates (}K_2)_i \text{ of } K_2 \text{ over } K_1.$

Finally we assume throughout that $p$ is regular, i.e. that $p$ does not divide $h_k$.

Now, we begin with a result which includes necessary conditions and sufficient conditions (but unfortunately not necessary and sufficient) for $h_K|_p = p^r$ for a given positive integer $r$. This result was motivated by the quintic ($p = 5, r = 1$) case given by Parry [8] of which part (i) of the following may be considered to be a generalization, and part (ii) provides a generalization of the cubic case ($p = 3, r = 1$) provided by Walter [12], which motivated this second result.

**Theorem 2.1.** Let $r$ be a positive integer.

(i) If $p^a_1(p)+(r-1)(p-1)$ divides $h_{K_1}$, then $p^r$ divides $h_{K_1}$. Conversely if $p^r$ divides $h_{K_1}$ and $p(p-2)(p-3)/2$ divides $Q_1$, then $p^a_1(p)+(r-1)(p-1)$ divides $h_{L_1}$. Furthermore, if $p$ divides $h_{K_1}$, then $p$ divides $h_{L_1}$.

(ii) Assume that $p$ does not divide $h_{L_1}$. Then $p^a_2(p)+(r-1)(p-1)$ divides $h_{L_2}$ implies that $p^r$ divides $h_{K_2}$. If $p > 3$, $p^r$ divides $h_{K_2}$, and $p(p-4)(p+1)/2$ divides $Q_2$, then $p^a_2(p)+(r-1)(p-1)$ divides $h_{L_2}$. Finally, if $p$ divides $h_{K_2}$, then $p$ divides $h_{L_2}$.

**Proof.** (i) We first note the following formulas obtained from Walter [12]:

(2.2) $h_{L_1}p^{b_1(p)} = Q_1h_kh_{K_1}^{-1}$, and

(2.3) $Q_1$ divides $p^{(p-1)(p-2)/2}$.

Now we assume that $p^a_1(p)+(r-1)(p-1)$ divides $h_{K_1}$. Hence from (2.2) we have that $|h_kp|^{-p}p^a_1(p)+b_1(p)+(r-1)(p-1)$ divides $Q_1$. But

$$a_1(p) + b_1(p) = 1 + (p-1)(p-2)/2.$$ 

Thus we get that $p^r$ divides $h_{K_1}$ from (2.3).

Conversely from (2.2) we have that $p^{((p-2)(p-3)/2)+r(p-1)-b_1(p)}$ divides $h_{L_1}$. But $(p-2)(p-3)/2 = a_1(p) + b_1(p) - (p-1)$. Hence $p^a_1(p)+(r-1)(p-1)$ divides $h_{L_1}$.

The last statement of part (i) follows from Iwasawa [6], since there is a $K_1$-prime above $p$ which is totally ramified in $L_1$.

(ii) From Walter [12] we have

(2.4) $p^a_2(p)h_{L_2}^2h_{K_2}^{-1} = Q_2h_{L_1}h_{K_2}^{-1}$, and

(2.5) $Q_2$ divides $p^{(p-1)(p-2)/2}$.

We first assume that $p^a_2(p)+(r-1)(p-1)$ divides $h_{L_2}$. Then from (2.4) we have that $|h_{K_2}|P^a_2(p)+b_2(p)+(r-1)(p-1)$ divides $Q_2$. But $a_2(p)+b_2(p) = 1+p(p-1)(p-2)/2$. Thus (2.5) yields that $p^r$ divides $h_{K_2}$.
Conversely if $p^r$ divides $h_{K_1}$, then from (2.4) we have that $h'_{L_2}$ is divisible by $p((p-4)(p+1)/2) + r(p-1) - b_2(p)$. But $(p-4)(p+1)/2 = a_2(p) + b_2(p) - (p-1)$. Hence $p^{a_2(p) + r(p-1)}$ divides $h_{L_2}$.

Finally the last statement of the theorem is immediate from Iwasawa [6]. Q.E.D.

We note that the above conditions are the "best possible", in the sense of being minimal. This fact is illustrated by the simplest case where $r = 1$ and $p = 3$, wherein we have $a_1(p) + (r - 1)(p - 1) = 1$. We have from Theorem 2.1 that if 3 does not divide $h_{K_1}$, then 3 does not divide $h_{K_1}$. Conversely if 3 does not divide $h_{K_1}$, then, since $Q_1 = 3$, we have that 3 does not divide $h_{L_1}$ from (2.2), i.e. for $p = 3$ we have $p|h_{K_1}$ if and only if $p|h_{L_1}$. Moreover the necessary and sufficient conditions for $p$ to divide $h_{L_1}$ were given by Parry and Walter [11]. Finally, in this connection we note that it is not enough to know $p$-divisibility conditions for $h_{L_1}$ in order to settle the question for $h_{K_1}$. We see this already for $p = 5$. Since $5^3|Q_1$ (see Parry [8]), then $5|h_{K_1}$ if and only if $5^2|h_{L_1}$ from Theorem 2.1.

The following result links the rank of $C_{L_i}(p)$ to the divisibility of $h_{K_i}$ by $p$.

**Theorem 2.2.** Suppose that $p^r$ divides $Q_i$, where $c = (p-2)(p-3)/2$ if $i = 1$ and $c = (p-4)(p+1)/2$ if $i = 2$. Then if $r(L_i,p) < p - 1$ and either $p > 7$ or $i = 2$ then $p$ does not divide $h_{K_i}$. If $i = 1$, $3 < p < 7$ and $r(L_1,p) = 1$, then $p$ does not divide $h_{K_i}$.

**Proof.** By Theorem 2.1, if $p$ divides $h_{K_1}$, then $p^{a_2(p)}$ divides $h_{L_1}$. Now if $C_{L_1}(p)$ has an element of order $p^2$, then by Cornell and Rosen [2, Theorem 5, p. 7] we have that $r(L_1,p) \geq p - 1$. Thus $C_{L_1}(p)$ must be elementary abelian which implies that $r(L_1,p) = a_1(p)$. Hence $p - 1 \geq a_1(p)$ if $p > 7$ or $p = 2$, a contradiction. If $3 < p < 7$ and $i = 1$, then $1 \geq a_1(p)$, again a contradiction. Q.E.D.

We isolate the following special case which motivated the above.

**Corollary 2.1 (Parry [8]).** If $p = 5$ and $5|h_{K_1}$, then $C_{L_1}(p)$ is not cyclic.

The final result actually gives an explicit description of an unramified extension $F$ of $K_i$ of degree $p^t$ whenever $m$ is divisible by $t$ primes $q \equiv 1 \pmod p$. The following is a generalization of the cubic case by Honda [3] which motivated our result. It is also a generalization of the quintic case by Parry [8]. In what follows $\zeta_q$ denotes a primitive $q$th root of unity.

**Proposition 2.1.** Suppose that $m$ is divisible by $t \geq 1$ primes $q \equiv 1 \pmod p$. Let $F^{(q)}$ be the subfield of $Q(\zeta_q)$ such that $|F^{(q)} : Q| = p$, and let $M$ be the compositum of the $t F^{(q)}$'s. Then $MK_i$ is unramified over $K_i$, i.e. $p^t$ divides $h_{K_i}$.

**Proof.** It is a straightforward application of Abhyankar's lemma (e.g. see [1, Theorem 3, p. 504] that $MK_i$ is unramified over $K_i$. Q.E.D.

Note that in the above result we did not require that $p$ be regular. Therefore we have the following proposition as an immediate consequence.

**Proposition 2.2.** Let $p$ be an odd prime. Then given any natural number $t$ there exist infinitely many non-Galois algebraic number fields of degree $p^t$ ($i = 1$ or 2) over $Q$, whose class numbers are all divisible by $p^t$.

Note that the above is a generalization of the main result of Ishida [5, Theorem 1, p. 65]. Moreover our proof is much easier than that given in [5].
REFERENCES

10. _, *Pure quartic number fields whose class numbers are even*, J. Reine Angew. Math. 264 (1975), 102–112.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALGARY, CALGARY, ALBERTA, T2N 1N4, CANADA