THE CLASS NUMBER OF PURE FIELDS OF PRIME DEGREE

CHARLES J. PARRY AND COLIN D. WALTER†

Here we give necessary and sufficient conditions for a prime l to divide the class number of the Galois closure of a pure field of degree l over the rationals. The work extends that of Honda in [**4**] and that of the first author in [**8**].

§1. *Notation.*

l an odd rational prime.

$t = (l-1)/2$.

$m > 1$ an l-power free rational integer .

$\sqrt[l]{x}$ the real l-th root of x if x is real, otherwise any l-th root of x.

ζ a primitive l-th root of unity.

$\mathbb{Z}$, $\mathbb{Q}$ the ring of rational integers and field of rational numbers.

$L = \mathbb{Q}(\zeta)$, L^+ the l-th cyclotomic field and its maximal real subfield.

$J = \mathbb{Q}(\sqrt{(-1)^t l}\,)$ the quadratic subfield of L.

$k = \mathbb{Q}(\sqrt[l]{m}\,)$ a pure field of degree l.

$K = \mathbb{Q}(\zeta, \sqrt[l]{m}\,)$ the Galois closure of $k/\mathbb{Q}$.

H, h_l, h^+, h^*, h the class numbers of K, L, L^+, J, and k respectively.

E, E^+ the unit groups of L and L^+.

$G(\Omega_1/\Omega_2)$ the Galois group of a normal extension Ω_1/Ω_2 of fields.

§2. *Extensions by roots of units.* In order to make use of Hasse's formula for the number of ambiguous classes of K/L it is necessary to consider the maximum abelian extension of L which is unramified outside l and whose Galois group has exponent l, namely

$$L^* = L(\sqrt[l]{l}\,, \sqrt[l]{e} \mid e \in E).$$

For a primitive root a modulo l set

$$e_n = \prod_{r=0}^{t-1} (\zeta^{a^r} + \zeta^{-a^r})^{a^{rn-r}} \qquad \textit{for odd } \; n \not\equiv 1 \bmod (l-1),$$

$$e_0 = \zeta \qquad \textit{and} \qquad e_1 = l,$$

and for such values of n define

$$L_n = L(\sqrt[l]{e_n}\,).$$

Then L_n is independent of the choice of a and depends only on l and the residue of n modulo $l-1$. The index of the group $\langle e_n \mid n \text{ odd}, \not\equiv 1 \bmod (l-1)\rangle$ in the group

† Work supported by a Rouse Ball studentship at Trinity College, Cambridge.

$\langle\, \zeta^{a^r} + \zeta^{-a^r} \mid 1 \le r \le t-1 \,\rangle$ of cyclotomic units is finite and prime to l because the determinant of the matrix $(a^{2sr})_{1\le r,s\le t-1}$ which relates the two given bases is non-zero modulo l. But the cyclotomic units have index in E^+ equal to the class number h^+ of L^+ ([**2**] §5.2 Theorem 2). Hence, if h^+ is also prime to l, then the $t-1$ fields L_n for odd $n \not\equiv 1 \bmod (l-1)$ generate $L(\sqrt[l]{e^+} \mid e^+ \in E^+)$. Kummer's lemma ([**2**] §3.1 Lemma 4) shows that

$$\sqrt[l]{\zeta} \;\notin\; L(\sqrt[l]{e^+} \mid e^+ \in E^+)$$

and

$$L(\sqrt[l]{e} \mid e \in E) \;=\; L(\sqrt[l]{\zeta}\,,\, \sqrt[l]{e^+} \mid e^+ \in E^+).$$

Also $\sqrt[l]{l} \notin L(\sqrt[l]{e} \mid e \in E)$, because otherwise $le = \alpha^l$ for some $e \in E$, $\alpha \in L$, and this is plainly absurd when the norm for $L/\mathbb{Q}$ is applied. Thus the L_n are independent over L and generate L^* if $l \nmid h^+$. As this fact is basic to our investigation, *for this section and the next we make the supposition that* l *does not divide* h^+. It is true in all known cases and in particular when l is a regular prime, *i.e.* when $l \nmid h_l$.

Define $\mu, \lambda_n \in G(L^*/\mathbb{Q})$ by

$$\mu : \zeta \mapsto \zeta^a,\ \sqrt[l]{e_n} \mapsto \sqrt[l]{e_n}^{\,\mu},$$

and

$$\lambda_n : \zeta \mapsto \zeta,\ \sqrt[l]{e_n} \mapsto \zeta\sqrt[l]{e_n}\,,\ \sqrt[l]{e_m} \mapsto \sqrt[l]{e_m} \ \textit{ for } \ m \neq n.$$

These automorphisms generate $G(L^*/\mathbb{Q})$. It is easy to verify that $\sqrt[l]{e_n}^{\,a^{n-1}\mu-1} \in L$, from which it follows that $L_n/\mathbb{Q}$ is normal and $\lambda_n\mu = \mu\lambda_n^{a^n}$. If $N = L(\sqrt[l]{e}\,) \neq L$ for $e = \prod e_n^{r(n)}$ and $N/\mathbb{Q}$ is normal then for some $b \not\equiv 0 \bmod l$ we have

$$e^b \;\sim\; e^{\mu-1} \;=\; \prod e_n^{\mu-1 r(n)} \;\sim\; \prod e_n^{a^{n-1} r(n)},$$

where $\sim$ means equality up to an l-th power in L. Hence $br(n) \equiv a^{n-1}r(n) \bmod l$ for all n, and $r(n) \equiv 0 \bmod l$ for all but one n. Thus $N = L_n$ for some n.

THEOREM 1. *Suppose* $l \nmid h^+$. *Then the only subfields of* L^* *with degree* l *over* L *and normal over* $\mathbb{Q}$ *are the* $t+1$ *fields* L_n. *They are independent over* L *and generate* L^*. *Moreover,*

$$G(L_n/\mathbb{Q}) \;\cong\; \langle \lambda_n, \mu \mid \lambda_n^{\,l} = \mu^{l-1} = 1,\ \lambda_n\mu \;=\; \mu\lambda_n^{a^n} \rangle.$$

With some simple calculations the condition for λ_n and μ^i to commute yields:

LEMMA 2. *Each element of* $G(L_n/\mathbb{Q})$ *has order dividing* $l(n, l-1)$ *or* $l-1$ *and there are elements of both orders.*

§3. *Ambiguous classes.* We shall follow the notation of Hasse ([**3**], **I***a*, §**13**) for the cyclic extension K/L with generating automorphism λ. An ideal class C of K is called ambiguous over L if $C^\lambda = C$. Let $\eta^* = N_{K/L}(K) \cap E$ and define q^* by $[\eta^* : E^l] = l^{q^*}$. Lastly suppose d is the number of primes of L which ramify in K.

LEMMA 3. *The number* A *of ambiguous classes in* K/L *is given by*

$$A = h_l\, l^{q^*+d-t-1} .$$

Moreover $A|H$, *and* $l|A \Leftrightarrow l|H$.

Proof. The formula for A is given by Hasse (*loc. cit.*). The other assertions are proved by Moriya in [**7**]. The ambiguous classes form a subgroup of the ideal class group of K and so A divides H. For the remaining implication, decompose the ideal class group of K into orbits under λ.

Now let $\mathfrak{p}$ be a prime ideal in L lying over a rational prime $p \neq l$ which divides m, and recall the assumption that $l \nmid h^+$ for this section.

LEMMA 4. *The Hilbert norm residue symbol*

$$\left(\frac{e_n, m}{\mathfrak{p}}\right)_L$$

is 1, *if, and only if, the Artin symbol* $[\mathfrak{p}, L_n/L]$ *is trivial. Further,* $[\mathfrak{p}, L_n/L] = 1$ *when* $p^n \not\equiv 1 \bmod l$, *and* $[\mathfrak{p}, L_0/L] = 1$, *if, and only if,* $p^{l-1} \equiv 1 \bmod l^2$.

Proof. The notation and elementary properties for residue symbols are described by Hasse in [**3**], part **II**. If $p^r \parallel m$ then $\mathfrak{p}^r \parallel m$ in L and so

$$\left(\frac{e_n, m}{\mathfrak{p}}\right) = \left(\frac{m, e_n}{\mathfrak{p}}\right)^{-1} = \left(\frac{L_n / L}{\mathfrak{p}}\right)^{-r}$$

where the final term is the Artin symbol considered as a root of unity.

Let f be the least positive integer such that $p^f \equiv 1 \bmod l$ and assume $p^n \not\equiv 1 \bmod l$. Then $\mathfrak{p}$ has degree f over $\mathbb{Q}$ from which $[\mathfrak{p}, L/\mathbb{Q}]$ has order f. If $\mathfrak{P}$ is a prime divisor of $\mathfrak{p}$ in L_n with degree f' over L then $f' = 1$ or l and $[\mathfrak{P}, L_n/\mathbb{Q}]$ has order ff' in $G(L_n/\mathbb{Q})$. As f divides $l-1$ but not n, Lemma 2 ensures that $f' = 1$. Hence $1 = [\mathfrak{P}, L_n/\mathbb{Q}]^f = [\mathfrak{P}, L_n/L]$ as required.

Finally suppose $n = 0$. Then with f as above $[\mathfrak{p}, L_0/L] = 1 \Leftrightarrow \mathfrak{p}$ splits completely in $L_0 \Leftrightarrow p^f \equiv 1 \bmod l^2 \Leftrightarrow p^{l-1} \equiv 1 \bmod l^2$.

THEOREM 5. *Suppose* $l \nmid h^+$. *If* N *denotes the number of odd* n *with* $1 < n < l$ *such that* $p^n \not\equiv 1 \bmod l$ *for all* $p|m$, *then*

$$q^* \geq N + \delta,$$

where $\delta = 0$ *or* 1 *according as* m *has a prime divisor* $p \neq l$ *with* $p^{l-1} \not\equiv 1 \bmod l^2$, *or not*.

Proof. The unit e_n is a norm in K/L, if, and only if ,

$$\left(\frac{e_n, m}{\mathfrak{p}}\right) = 1$$

for all primes $\mathfrak{p}$ containing (m). Since (l) has only one prime divisor in L, the product formula for the norm residue symbol permits this prime to be ignored. Lemma 4 ensures that there are at least N values of n such that

$$\left(\frac{e_n, m}{\mathfrak{p}}\right) = 1$$

for all $\mathfrak{p}$. Thus at least N of the units e_n are norms and ζ is a norm exactly when $\delta = 1$. Since the units e_n and ζ generate a subgroup of index prime to l in E it follows that $q^* \geq N + \delta$.

If $f \mid n$ then the primes p which have order f modulo l divide into two classes according as $[\mathfrak{p}, L_n/L] = 1$ or not. Lemma 2 and the Tchebotarev Density Theorem prove the existence of infinitely many primes in either class relative to each L_n. The remainder of this section considers the problem for L_t. Let $t > 1$ be odd and suppose the (imaginary) quadratic subfield $J = \mathbb{Q}(\sqrt{(-l)})$ of L has class number h^*. It is well-known [**1**, p. 300] that $h^* < l$ and consequently $l \nmid h^*$.

LEMMA 6. *L_t is a class field over J with conductor* (l).

Proof. Let I^l be the group of fractional ideals of J which are prime to l and let $P_l^{(n)}$ be the subgroup generated by elements $\alpha \equiv 1 \bmod (\sqrt{(-l)})^n$ of J. Since the only units of J are ± 1 it follows from [**6**, p. 111] that the ray class group $I^l/P_l^{(n)}$ has order $h^* l^{n-1} t$. At least one member of the corresponding tower of class fields $L^{(n)}$ contains L because $(\sqrt{-l})$ is the only prime ramified in L/J. Hence $L \subset L^{(1)}$ as $[L : J]$ is prime to $[L^{(n)} : L^{(1)}]$ and $L^{(n)}/J$ is abelian. Again from degree considerations and $l \nmid h^*$ there can only be one abelian extension N/J of conductor (l) and degree l over L. As the complex conjugate of N also has the same properties, $N/\mathbb{Q}$ must be normal. Being unramified outside $\sqrt{(-l)}$, N is a subfield of L^*, and Theorem 1 shows that $N = L_0$ or L_t. Thus it suffices to prove that the conductor of L_0/J is not (l). Suppose the contrary and choose $\alpha \in J$ with $\alpha \equiv 1 \bmod (l)$ but $\alpha \not\equiv 1 \bmod (\sqrt{(-l)})^3$. Then $1 = [(\alpha), L_0/J] = [N_{J/\mathbb{Q}}(\alpha), L_0/\mathbb{Q}]$. Hence

$$N_{J/\mathbb{Q}}\, \alpha \;=\; 1 \bmod l^2$$

as $L_0/\mathbb{Q}$ has conductor (l^2). This contradiction establishes the lemma.

LEMMA 7. $[\mathfrak{p}, L_t/L] \neq 1$ *precisely for those primes p which satisfy*

$$p^{h^*} = (x^2 + ly^2)/4$$

for some integers x, y with $y \not\equiv 0 \bmod l$.

Proof. After Lemma 6 let $\mathbf{H}$ be the subgroup of I^l corresponding to L_t. Then $[\mathbf{H} : P_l^{(2)}] = h^*$ is prime to l. Also let $\mathfrak{p}^*$ be a prime divisor of p in J and suppose $\mathfrak{p}^{*h^*} = (x + y\sqrt{(-l)})/2$. By means of the Artin map, $[\mathfrak{p}, L_t/L] \neq 1$, if, and only if, l divides the order of $[\mathfrak{p}^*, L_t/J]$. This holds, if, and only if, l divides the order of $\mathfrak{p}^*$ in $I^l/\mathbf{H}$, which holds, if, and only if, l divides the order of $\mathfrak{p}^{*h^*}$ in $I^l/P_l^{(2)}$. This holds, if, and only if, l divides the order of $(x + y\sqrt{(-l)})/2 \bmod l$, which holds, if, and only if, $y \not\equiv 0 \bmod 1$.

§4. *The class numbers of K and k.*

THEOREM 8. *The class number of $K = \mathbb{Q}(\sqrt[l]{m}, \zeta)$ is prime to l, if, and only if, l is a regular prime and m may be taken as one of the following*:

$$l,\;\; p_1,\;\; lp_2^{\,a},\;\; p_3 p_4^{\,a}$$

where:

$$1 \le a \le l-1\ ;$$

p_1, p_2, p_3, p_4, *and* l *are distinct primes* ;

p_1 and p_3 *have order* l–1 *or non-trivial odd order* $(l-1)/2$ *modulo* l, *and* p_2 *and* p_4 *have order* l–1 ;

$p_1^{l-1} \equiv 1 \bmod l^2$ *if* p_1 *has odd order*, $p_2^{l-1} \not\equiv 1 \bmod l^2$, $p_3^{l-1} \not\equiv 1 \bmod l^2$, *and* $(p_3p_4^{a})^{l-1} \equiv 1 \bmod l^2$;

and, if $p = p_1$ *or* $p = p_3$ *has odd order, then the representation* $p^{h^*} = (x^2 + ly^2)/4$ *has* $y \not\equiv 0 \bmod l$ *for the class number* h^* *of* $\mathbb{Q}(\sqrt{(-l)})$.

Remark. The earlier supposition that $l \nmid h^+$ is no longer required here.

Proof. If $l \nmid H$ Lemma 3 shows that l must be a regular prime and

$$q^* + d - t - 1 = 0\ .$$

Let $\{p_i\}$ be the set of primes $\neq l$ which divide m, and let f_i be the order of p_i modulo l. The number of odd $n \not\equiv 1$ satisfying $p_i^n \not\equiv 1 \bmod l$ is t–1 when f_i is even, $t - 1 - tf_i^{-1}$ when f_i is odd, but $\neq 1$, and 0, when $f_i = 1$. Set $\delta = 1$ or 0 according as ζ is a norm in K/L, or not; and $\delta' = 1$ or 0 according as $(1-\zeta)$ is ramified in K/L, or not. It follows from Theorem 5 that

$$q^* + d - t - 1 \ \ge\ \Big(t - 1 - \sum_{f_i\text{odd}} tf_i^{-1} + \delta\Big) + \Big(\delta' + \sum_{i} 2tf_i^{-1}\Big) - t - 1$$

$$= \ \delta + \delta' - 2 \ +\ \sum_{f_i\text{even}} 2tf_i^{-1} \ +\ \sum_{f_i\text{odd}} tf_i^{-1} \qquad (*)$$

Thus m contains at most two factors p_i. When there are two, they have order $2t$ or odd order t modulo l if distinct from l and so $\delta + \delta' = 0$. Lemma 4 shows $\delta = 1$ exactly when $p_i^{l-1} \equiv 1 \bmod l^2$ for all i and Theorems 3 and 4 of [**9**] show $\delta' = 0$ exactly when $m^{l-1} \equiv 1 \bmod l^2$. This yields the conditions modulo l^2 and the exclusion of three primes including l dividing m. When $\{p_i\}$ includes just one prime then certainly $\delta + \delta' = 1$. Thus the prime must have order $2t$ or odd order t and for $l|m$ the condition modulo l^2 is immediate. If only l divides m then $\delta + \delta' = 2$.

The precise conditions have now been found to ensure that the right side of (*) is zero. It remains to discover the further conditions required for equality. Strict inequality holds, if, and only if, the estimate for q^* is not exact. This happens, if some prime has order 1 modulo l, or if two primes have the same odd order. Except for p_2 this settles the order of each p_i. With these restrictions inequality occurs just when $t \neq 1$, there is a prime of odd order, and $q^* = t - 1 + \delta$. This yields the requirement that e_t is not a norm, if some p_i has odd order $t \neq 1$. The condition for this is given in Lemma 7.

Suppose therefore that m has a prime divisor $p \neq l$ with odd order. Then

$$\left(\frac{e_t, m}{\mathfrak{p}}\right) \neq 1$$

where $\mathfrak{p}$ is a prime divisor of (p) in L because e_t is not a norm. If no other prime $\neq l$ divides m and ζ is not a norm, then

$$\left(\frac{\zeta, m}{\mathfrak{p}}\right) \neq 1 .$$

A suitable choice of b gives

$$\left(\frac{\zeta e_t^{\,b}, m}{\mathfrak{p}}\right) = \left(\frac{\zeta, m}{\mathfrak{p}}\right)\left(\frac{e_t, m}{\mathfrak{p}}\right)^b = 1$$

and makes ζe_t^b a norm. Thus $q^* = t - 1$ and equality holds in (*), if, and only if, $\delta = 1$. The congruence modulo l^2 for p_1 is now obtained and p_2 cannot have odd order as $\delta = 0$ in that case. If $p' \neq l$ also divides m then the conditions modulo l^2 show that

$$\left(\frac{\zeta, m}{\mathfrak{p}'}\right) \neq 1$$

and the order $2t$ of p' modulo l gives

$$\left(\frac{e_t, m}{\mathfrak{p}'}\right) = 1 .$$

Thus

$$\left(\frac{\zeta e_t^{\,b}, m}{\mathfrak{p}'}\right) \neq 1$$

for all b and ζe_t^b cannot be a norm. So $q^* = t - 2 + \delta$ and (*) is an equality. This completes the proof.

COROLLARY 9. *Let m have one of the forms described in Theorem* 8. *If $l \nmid h^+$ then l does not divide the class number of* $\mathbb{Q}(\sqrt[l]{m})$.

Proof. By [**5**] h divides H because K/k contains a totally ramified prime above l.

References

1. R. Ayoub. *An introduction to the analytic theory of numbers* (Amer. Math. Soc., Providence, R.I., 1963).

2. Z. I. Borevich and I. R. Shafarevich. *Number theory* (Academic Press, New York, 1966).

3. H. Hasse. *Bericht über Neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper* (Physcia-Verlag, Würzburg/Wien, 1970).

4. T. Honda. "Pure cubic fields whose class numbers are multiples of three", *J. of Number Theory*, 3 (1971), 7–12.

5. K. Iwasawa. “A note on class numbers of algebraic number fields”, *Abh. Math. Sem. Univ. Hamburg*, 20 (1956), 257–258.

6. G. J. Janusz. *Algebraic number fields* (Academic Press, New York, 1973).

7. M. Moriya. “Über die Klassenzahl eines relativ-zyklischen Zahlkörpers vom Primzahlgrad”, *Proc. Imper. Acad. Japan*, 6 (1930), 245–247.

8. C. Parry. “Class number relations in pure quintic fields”, *Symposia Mathematica*, 15 (1975), 475–485.

9. R. Van der Waall. “On the conductor of the non-abelian simple character of the galois group of a special field extension”, *Symposia Mathematica*, 15 (1975), 389–395.

Department of Mathematics,
VPI & SU,
Blacksburg, Virginia, U.S.A.

Department of Mathematics,
University College, Dublin

12A50: *ALGEBRAIC NUMBER THEORY, FIELD THEORY*; *Algebraic number theory*: *global fields*; *Class number.*

Received on the 21*st of June*, 1976.

Printed by C. F. Hodgson & Son, Ltd., 50 Holloway Road, London N7 8JL