Suppose for example that $N\varrho = \pm 4$. Since $2 = \pi\bar{\pi}$ where $\pi = 3+\theta$, unique factorization implies that up to a unit factor, ϱ must equal π^2, $\pi\bar{\pi}$ or $\bar{\pi}^2$. Since $\varrho > 0$ this unit factor is w^n for some $n \in \boldsymbol{Z}$. Now $w = 27+10\theta$ so that $w^2 \equiv 1 \pmod 4$. Hence, $\varrho \equiv \pi^2,\ \pi\bar{\pi},\ \bar{\pi}^2,\ w\pi^2,\ w\pi\bar{\pi}$, or $w\bar{\pi}^2 \pmod 4$. Multiplying these out we find that none of them is compatible with the hypothesis $\varrho \equiv 2+3\theta \pmod 4$.

The rest of the cases in this proposition are settled by similar calculations. ∎

References

[1] H. Chatland and H. Davenport, *Euclid's algorithm in real quadratic fields*, Canadian J. Math. 2 (1950), pp. 289–296.

[2] H. Davenport, *Indefinite binary quadratic forms, and Euclid's algorithm in real quadratic fields*, Proc. London. Math. Soc. (2) 53 (1951), pp. 65–82.

[3] M. Eichler, *Allgemeine Kongruenzklasseneinteilungen der Ideale einfacher Algebren über algebraischen Zahlkörper und ihre L-Reihen*, J. Reine Angew. Math. 179 (1938), pp. 227–251. See especially pp. 240–241.

[4] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, fourth edition, Oxford Univ. Press, 1960. See especially § 14.8 and § 14.9.

[5] C. G. Lekkerkerker, *Geometry of Numbers*, Walters-Noordhoff and North-Holland, 1969. See especially § 47.5 and § 48.3.

[6] H. W. Lenstra, Jr., *Euclidean number fields* 2, Math. Intelligencer 2 (1980), pp. 73–77.

[7] R. K. Markanda and V. S. Albis-Gonzales, *Euclidean algorithm in principal arithmetic algebras*, Tamkang J. Math. (to appear).

DEPARTMENT OF MATHEMATICS
THE OHIO STATE UNIVERSITY
COLUMBUS, OHIO 43210

DEPARTAMENTO DE MATEMATICAS
UNIVERSIDAD DE OS ANDES
MERIDA, VENEZUELA

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF IOWA
IOWA CITY, IOWA 52242

DEPARTMENT OF MATHEMATICS
VIRGINIA POLYTECHNIC INSTITUTE AND STATE UNIVERSITY
BLACKSBURG, VIRGINIA 24061

Received on 20. 12. 1984
and in revised form on 11. 4. 1985 (1481)

ACTA ARITHMETICA
XLVII (1986)

On the l-rank of ideal class groups of certain number fields

by

KIYOAKI IIMURA (Tokyo)

Introduction. Throughout this paper we shall fix an odd prime number l. Let $\boldsymbol{Z}$ and $\boldsymbol{Z}_l$ denote the ring of rational integers and of l-adic integers respectively. Let K be a nonabelian Galois extension of the rational numbers $\boldsymbol{Q}$ satisfying the following conditions.

(a) The degree $(K:\boldsymbol{Q})$ is nl with $n \mid l-1$, $n \neq 1$.

(b) The Galois group G of K over $\boldsymbol{Q}$ is generated by two elements σ and τ with the relations

$$\sigma^l = 1, \quad \tau^n = 1, \quad \tau\sigma\tau^{-1} = \sigma^r,$$

where r is a rational integer of order n in the multiplicative group $(\boldsymbol{Z}/l\boldsymbol{Z})^{\times}$.

Let T (resp. S) be the subgroup of G generated by τ (resp. σ), and let L (resp. k) be the fixed field of T (resp. S). Then $k/\boldsymbol{Q}$ is a cyclic extension of degree n, whose Galois group is generated by the restriction of τ to k. Also $L/\boldsymbol{Q}$ is a non-Galois extension of degree l, with Galois closure K. An important example of this situation is $L = \boldsymbol{Q}(\sqrt[l]{m})$, $k = \boldsymbol{Q}(\zeta)$, and $K = L \cdot k$, where ζ is a primitive lth root of unity and m is an lth power-free rational integer; such a field is called a *pure field of degree* l.

Let $H(L)$ denote the l-class group of L, i.e., the Sylow l-subgroup of the ideal class group of L. The *l-rank of* $H(L)$ is defined to be the number of invariants of $H(L)$ divisible by l, which we call *rank* $H(L)$. The main purpose of the paper is to establish lower bounds for rank $H(L)$ (see Theorem 2.3 in § 2) by making use of the genus number formula found by Jaulent ([11], Theorem 3). In particular in the pure field case $L = \boldsymbol{Q}(\sqrt[l]{m})$, $l \neq 3$, one of our lower bounds in the corollary to Theorem 2.3 is equal to the number of distinct prime factors $\equiv \pm 1 \pmod l$ of m; this is an extension of one of the results in [1] which was a consequence of rational genus theory. Also we shall illustrate this Theorem 2.3 with some examples in Section 4, one of which says that if $p = (c_0^l + c_1^l)/(c_0 + c_1)$ with $l \geqslant 5$ and c_0,

$c_1 \in \boldsymbol{Z}$, is a prime and if $(c_0+c_1)^{(p-1)/l} \equiv 1 \pmod p$, then the l-class group of the pure field $\boldsymbol{Q}(\sqrt[l]{p})$ is not cyclic, i.e., rank $H(\boldsymbol{Q}(\sqrt[l]{p})) \geqslant 2$.

We conclude this introduction with some remarks about notations. In general we use multiplicative notations for groups and modules. Also the action of a group or a ring on a module is expressed by exponentiation, and $(x^\sigma)^\tau = x^{\sigma\tau}$.

1. Preliminaries. We use the notation of the introduction. For a finite extension $F/\boldsymbol{Q}$, let $H(F)$ denote the l-class group of F. If A is a finite abelian group, rank A is defined to be the number of invariants divisible by l. Also $\boldsymbol{Z}_l[A]$ is the group ring of A over $\boldsymbol{Z}_l$. We denote by X the group of l-adic characters of T, i.e., homomorphisms of T into the group $\boldsymbol{Z}_l^\times$ of units in $\boldsymbol{Z}_l$. Note that $\boldsymbol{Z}_l^\times$ contains the nth roots of unity since $n \mid l-1$. For a character χ in X, let e_χ be the idempotent of $\boldsymbol{Z}_l[T]$ attached to χ; i.e.,

$$e_\chi = n^{-1} \sum_{\varrho \in T} \chi(\varrho^{-1})\,\varrho.$$

Then the e_χ are mutually orthogonal. For a $\boldsymbol{Z}_l[T]$-module M, let $M^{(\chi)} = M^{e_\chi} = \{m^{e_\chi};\ m \in M\}$; then $M^{(\chi)} = \{m \in M;\ m^\tau = m^{\chi(\tau)}\}$ and $M = \prod_{\chi \in X} M^{(\chi)}$ (direct product). By θ we shall denote the element of X such that $\varrho\sigma\varrho^{-1} = \sigma^{\theta(\varrho)}$ for all ϱ in T; then θ is of order n, so generates X. Furthermore let $\Delta = 1-\sigma$, $\delta = \sum_{i=0}^{l-1} \sigma^i$, and $\eta = l^{-1}(\Delta^{l-1}-\delta)$; η is known to be a unit of $\boldsymbol{Z}_l[S]$ (cf. [3], proof of Proposition 4.1 and [10], Lemma II.6).

For each integer $i \geqslant 0$, we define

$$I_i = H(K)^{\Delta^i} H(K)^l / H(K)^{\Delta^{i+1}} H(K)^l.$$

Then each I_i is a $\boldsymbol{Z}_l[G]$-module and $I_i^l = 1$. Also $I_i = 1$ for all $i \geqslant l$ since $\Delta^l \in l\boldsymbol{Z}_l[S]$. As the degree $(K:L) = n$ is prime to l by our assumption (a), the inclusion map: $H(L) \to H(K)$ is injective, so $H(L)$ may be considered to be a subgroup of $H(K)$, and then $H(L) = H(K)^{(\chi_0)}$, where χ_0 is the trivial character in X.

LEMMA 1.1. rank $H(L) = \sum_{i=0}^{l-2} \operatorname{rank} I_i^{(\chi_0)}$.

Proof. Since η is invertible in $\boldsymbol{Z}_l[S]$ and $H(L)^\delta = 1$, then $H(L)^l = H(K)^{\Delta^{l-1}(\chi_0)}$, which implies the assertion of the lemma.

LEMMA 1.2. *rank* $I_0^{(\chi_0)} = s$, *where* s *is the number of rational primes ramified fully in* L *and decomposed completely in* k.

Proof. This is immediate from [11], Theorem 3.

Let U be the kernel of the Δ-map from I_0 onto I_1. It is easily seen that $e_\theta \Delta \equiv \Delta e_{\chi_0} \pmod{\Delta^2 \boldsymbol{Z}_l[G]}$ (cf. e.g. [10], Proposition II.5 (ii)); so that the Δ-map gives rise to an exact sequence

$$1 \to U^{(\theta)} \to I_0^{(\theta)} \xrightarrow{\Delta} I_1^{(\chi_0)} \to 1,$$

and therefore

$$\operatorname{rank} I_1^{(\chi_0)} = \operatorname{rank} I_0^{(\theta)} - \operatorname{rank} U^{(\theta)}. \tag{1.1}$$

The norm map, N, from K to k induces a homomorphism of the group of ideals of K to the group of ideals of k and so of $H(K)$ to $H(k)$ and we shall denote these homomorphisms by N also. Let $\bar{H}(K)$ be the kernel of N: $H(K) \to H(k)$, and let $J = \bar{H}(K)/H(K)^\Delta$; then $\bar{H}(K)$ and J are $\boldsymbol{Z}_l[T]$-modules, and $J^l = 1$ since $l \in \delta\boldsymbol{Z}_l[S] + \Delta^{l-1}\boldsymbol{Z}_l[S]$. If K/k is unramified, then $J = 1$ (cf. e.g. [6]). In the case that K/k is ramified, the genus number formula obtained by Jaulent ([11], Theorem 3) provides rank $J^{(\theta)}$. To describe it we introduce some notations. Let s_0 denote the number of rational primes which are ramified fully in L and whose decomposition groups in $k/\boldsymbol{Q}$ are of order $\leqslant 2$. We define

$$a = \begin{cases} 1, & \text{if } K/k \text{ is ramified and } l = 3, \\ 0, & \text{otherwise}. \end{cases}$$

Let $E(k)$ be the tensor product, over $\boldsymbol{Z}$, of $\boldsymbol{Z}_l$ and of the group of units in k, and let $E = E(k)/(E(k) \cap NK)$; $E(k)$ and so E are $\boldsymbol{Z}_l[G]$-modules. Then by the genus number formula,

$$\operatorname{rank} J^{(\theta)} = s_0 - a - \operatorname{rank} E^{(\theta)}. \tag{1.2}$$

Let $H'(k) = NH(K)$ and $\bar{H}(k) = \{h \in H(k);\ h^l = 1\}$; they both, as well as $H(k)$, may be regarded as $\boldsymbol{Z}_l[T]$-modules by restricting T to k. Class field theory says that $H'(k)^{(\chi)} = H(k)^{(\chi)}$ for any character $\chi \neq \theta^{-1}$, and that $H(k)^{(\theta^{-1})}/H'(k)^{(\theta^{-1})}$ is trivial or cyclic of order l according as K/k is ramified or not; hence unless K/k is unramified and $l = 3$, then $H'(k)^{(\theta)} = H(k)^{(\theta)}$. But in the case that K/k is unramified and $l = 3$, it is known that rank $H(L) = \operatorname{rank} H(k) - 1$ (cf. [2] and [4]); so that from now on until the end of the last section we shall leave out this case.

Now we let ι: $H(k) \to H(K)$ be the inclusion map; it is easily seen that $H(K)^\Delta H(K)^l = H(K)^\Delta \iota H'(k)$. But since $H'(k)^{(\theta)} = H(k)^{(\theta)}$, then

$$(H(K)^\Delta H(K)^l)^{(\theta)} = H(K)^{\Delta(\theta)} \iota H(k)^{(\theta)}.$$

Furthermore we define the canonical homomorphisms:

$$\varphi\colon\ H(K) \to H(K)/H(K)^\Delta H(K)^l = I_0,$$

$$\psi\colon\ \bar{H}(K) \to \bar{H}(K)/H(K)^\Delta = J,$$

$$\xi\colon\ H(k) \to H(k)/H(k)^l.$$

In particular if K/k is unramified, ψ is the trivial map since then $J = 1$.

LEMMA 1.3. *We have*

$$\operatorname{rank} I_0^{(\theta)} = \operatorname{rank} H(k)^{(\theta)} + \operatorname{rank} J^{(\theta)} - \operatorname{rank} \psi\big(\iota \bar{H}(k)^{(\theta)}\big).$$

Proof. Let $B = H(K)/H(K)^{\Delta}$; then $\operatorname{rank} I_0^{(\theta)} = \operatorname{rank} (B^{(\theta)}/B^{(\theta)l})$. The norm map N gives rise to exact sequences:

$$\begin{tikzcd}
1 \arrow[r] & J^{(\theta)} \arrow[r] & B^{(\theta)} \arrow[r, "N"] & H(k)^{(\theta)} \arrow[r] & 1 \\
1 \arrow[r] & D \arrow[r] \arrow[u, phantom, "\cup"] & B^{(\theta)l} \arrow[r, "N"] \arrow[u, phantom, "\cup"] & H(k)^{(\theta)l} \arrow[r] \arrow[u, phantom, "\cup"] & 1,
\end{tikzcd}$$

where $D = \psi\big((H(K)^l H(K)^{\Delta})^{(\theta)} \cap \bar{H}(K)\big)$. As

$$\big(H(K)^l H(K)^{\Delta}\big)^{(\theta)} = \big(H(K)^{\Delta}\big)^{(\theta)} \iota H(k)^{(\theta)} \quad \text{and} \quad H(K)^{\Delta} \subset \bar{H}(K),$$

the kernel D is the same as $\psi\big(\iota H(k)^{(\theta)} \cap \bar{H}(K)\big)$. But by definition, $\iota H(k)^{(\theta)} \cap \bar{H}(K) = \iota \bar{H}(k)^{(\theta)}$, so $D = \psi\big(\iota \bar{H}(k)^{(\theta)}\big)$. The above exact sequences now give the required result.

We conclude this section with the following

LEMMA 1.4. *Let H be a $Z_l[T]$-submodule of $H(K)$. Then*

$$\operatorname{rank} \varphi(H^{(\theta)})$$
$$= \operatorname{rank} \xi(NH^{(\theta)}) + \operatorname{rank} \psi\big(H^{(\theta)} \iota H(k)^{(\theta)} \cap \bar{H}(K)\big) - \operatorname{rank} \psi\big(\iota \bar{H}(k)^{(\theta)}\big).$$

Proof. Since $\big(H(K)^{\Delta} H(K)^l\big)^{(\theta)} = \big(H(K)^{\Delta}\big)^{(\theta)} \iota H(k)^{(\theta)}$, the module $\varphi(H^{(\theta)})$ is isomorphic to $\tilde{\psi}\big(H^{(\theta)} \iota H(k)^{(\theta)}\big)/\tilde{\psi}\big(\iota H(k)^{(\theta)}\big)$ where $\tilde{\psi}$ denotes the canonical homomorphism of $H(K)$ onto $H(K)/H(K)^{\Delta}$. The norm map N induces the following exact sequences:

$$\begin{tikzcd}
1 \arrow[r] & \psi\big(H^{(\theta)} \iota H(k)^{(\theta)} \cap \bar{H}(K)\big) \arrow[r] & \tilde{\psi}\big(H^{(\theta)} \iota H(k)^{(\theta)}\big) \arrow[r, "N"] & N H^{(\theta)} H(k)^{(\theta)l} \arrow[r] & 1, \\
1 \arrow[r] & \psi\big(\iota H(k)^{(\theta)} \cap \bar{H}(K)\big) \arrow[r] \arrow[u, phantom, "\cup"] \arrow[d, equal] & \tilde{\psi}\big(\iota H(k)^{(\theta)}\big) \arrow[r, "N"] \arrow[u, phantom, "\cup"] & H(k)^{(\theta)l} \arrow[r] \arrow[u, phantom, "\cup"] & 1. \\
& \psi\big(\iota \bar{H}(k)^{(\theta)}\big) & & &
\end{tikzcd}$$

Since $N H^{(\theta)} H(k)^{(\theta)l}/H(k)^{(\theta)l}$ is isomorphic to $\xi(NH^{(\theta)})$, the lemma follows at once from these sequences.

2. Lower bounds. We use the foregoing notations. Let H_1 (resp. $\dot{H}_1$) denote the set of elements h in $H(K)$ with $h^{\Delta} = 1$ (resp. $h^{\Delta} \in H(K)^{\delta}$); they are $Z_l[G]$-modules. Since $\dot{H}_1^{\Delta^2} = 1$ and $e_\theta \Delta \equiv \Delta e_{\chi_0} (\operatorname{mod} \Delta^2 Z_l[G])$, it follows that $\dot{H}_1^{(\theta)} = H_1^{(\theta)}$. For an ideal $\mathfrak{a}$ of K, we denote by $c(\mathfrak{a})$ the ideal class of K containing $\mathfrak{a}$. Let H_1' be the subgroup of $H(K)$ generated by the classes $c(\mathfrak{a})$ with $\mathfrak{a}^{\sigma} = \mathfrak{a}$; H_1' is also a $Z_l[G]$-module. Then, by [14], Theorem 1.8, $H_1^{(\theta)} = H_1'^{(\theta)}$, and therefore $\dot{H}_1^{(\theta)} = H_1'^{(\theta)}$.

LEMMA 2.1. *Let as before U be the kernel of the Δ-map:*

$$I_0 = H(K)/H(K)^{\Delta} H(K)^l \to I_1 = H(K)^{\Delta} H(K)^l/H(K)^{\Delta^2} H(K)^l.$$

Then $U^{(\theta)} = \varphi(H_1'^{(\theta)})$.

Proof. Let $\hat{H}_1$ be the set of elements h in $H(K)$ with $h^{\Delta} \in H(K)^l$; then $U = \varphi(\hat{H}_1)$, and so we want to show that $\varphi(\hat{H}_1) = \varphi(\dot{H}_1)$. First assume $h \in \hat{H}_1$; then $(hc^{-\eta^{-1}\Delta^{l-2}})^{\Delta} = c^{-\eta^{-1}\delta}$ for some $c \in H(K)$ since $l = \eta^{-1}\Delta^{l-1} - \eta^{-1}\delta$. Putting $h_1 = hc^{-\eta^{-1}\Delta^{l-2}}$ and $h_2 = c^{-\eta^{-1}}$, we have $h_1^{\Delta} = h_2^{\delta}$ and $h = h_1 h_2^{-\Delta^{l-2}}$; so that $h_1 \in \dot{H}_1$ and $\varphi(h) = \varphi(h_1)$. Conversely assume $h_1 \in \dot{H}_1$; then $h_1^{\Delta} = h_2^{\delta}$ for some $h_2 \in H(K)$, and it is easy to see that $h^{\Delta} \in H(K)^l$ where $h = h_1 h_2^{-\Delta^{l-2}}$; therefore $h_1 \in \hat{H}_1$ and $\varphi(h_1) = \varphi(h)$. This completes the proof.

Now let s be the number defined in Lemma 1.2, let $p_1, \ldots, p_s$ be the rational primes ramified fully in L and decomposed completely in k, let $\mathfrak{p}_i$ be a prime ideal of k above p_i, and let $\mathfrak{P}_i$ be the unique prime ideal of K above $\mathfrak{p}_i$. Put $e = e_\theta$. Let g denote the order of the factor group $C(k)/H(k)$, $C(k)$ being the full ideal class group of k. Let Γ denote the subgroup of $H(k)$, generated by the classes $c(\mathfrak{P}_i^g)^e$, $1 \leqslant i \leqslant s$. Then Γ is a $Z_l[T]$-module, and it is easily seen that

$$H_1'^{(\theta)} = \Gamma \iota H(k)^{(\theta)}.$$

Since $\big(H(K)^{\Delta} H(K)^l\big)^{(\theta)} = \big(H(K)^{\Delta}\big)^{(\theta)} \iota H(k)^{(\theta)}$, it follows from Lemma 2.1 that

$$U^{(\theta)} = \varphi(\Gamma).$$

So it is clear that

$$\operatorname{rank} U^{(\theta)} = \operatorname{rank} \varphi(\Gamma) \leqslant s. \tag{2.1}$$

PROPOSITION 2.2. *With the foregoing notations, we have*

$$\begin{aligned}
\operatorname{rank} I_1^{(\chi_0)} &= s_0 - a - \operatorname{rank} E^{(\theta)} + \operatorname{rank} H(k)^{(\theta)} \\
&\quad - \operatorname{rank} \psi\big(\Gamma \iota H(k)^{(\theta)} \cap \bar{H}(K)\big) - \operatorname{rank} \xi(N\Gamma) \\
&\geqslant s_0 - s - a - \operatorname{rank} E^{(\theta)} + \operatorname{rank} H(k)^{(\theta)} - \operatorname{rank} \psi\big(\iota \bar{H}(k)^{(\theta)}\big).
\end{aligned}$$

Proof. By equation (1.1),

$$\operatorname{rank} I_1^{(\chi_0)} = \operatorname{rank} I_0^{(\theta)} - \operatorname{rank} U^{(\theta)}.$$

By Lemma 1.3 and equation (1.2),

$$\operatorname{rank} I_0^{(\theta)} = \operatorname{rank} H(k)^{(\theta)} + s_0 - a - \operatorname{rank} E^{(\theta)} - \operatorname{rank} \psi\big(\iota \bar{H}(k)^{(\theta)}\big). \tag{2.2}$$

Since $\operatorname{rank} U^{(\theta)} \leqslant s$ by equation (2.1), then $\operatorname{rank} I_1^{(\chi_0)} \geqslant \operatorname{rank} I_0^{(\theta)} - s$. So the desired inequality in the proposition follows at once. Also by equation (2.1), $\operatorname{rank} U^{(\theta)} = \operatorname{rank} \varphi(\Gamma)$. But if we apply Lemma 1.4 to the $\boldsymbol{Z}_l[T]$-module Γ, then

$$\operatorname{rank} \varphi(\Gamma) = \operatorname{rank} \psi\big(\Gamma\iota H(k)^{(\theta)} \cap \bar{H}(K)\big) - \operatorname{rank} \psi\big(\iota\bar{H}(k)^{(\theta)}\big) + \operatorname{rank} \xi(N\Gamma),$$

which together with equation (2.2) provides the desired equality in the proposition.

Combining Lemmas 1.1, 1.2 and 2.2 yields the following

THEOREM 2.3. *We have*

$$\begin{aligned}\operatorname{rank} H(L) &\geqslant s + s_0 - a - \operatorname{rank} E^{(\theta)} + \operatorname{rank} H(k)^{(\theta)} \\ &\qquad - \operatorname{rank} \psi\big(\Gamma\iota H(k)^{(\theta)} \cap \bar{H}(K)\big) - \operatorname{rank} \xi(N\Gamma) \\ &\geqslant s_0 - a - \operatorname{rank} E^{(\theta)} + \operatorname{rank} H(k)^{(\theta)} - \operatorname{rank} \psi\big(\iota\bar{H}(k)^{(\theta)}\big).\end{aligned}$$

Of special interest is the pure field case, $L = \boldsymbol{Q}(\sqrt[l]{m})$ where m is an lth power-free rational integer. In this case the number s (resp. s_0) is precisely the number of prime factors $\equiv 1 \pmod{l}$ (resp. $\pm 1 \pmod{l}$) of m. Also $E(k)^{(\theta)} = 1$ or $\langle \zeta_3 \rangle$ according as $l \neq 3$ or $l = 3$, where ζ_3 is a primitive cube root of unity (cf. [14], § 1); in the cubic case it is known that $\operatorname{rank} E^{(\theta)} = 0$ or 1 according to whether or not every prime factor $\neq 3$ of m is congruent to $\pm 1 \pmod 9$ (cf. [7]). Furthermore the extension K/k in which k is the lth cyclotomic field and $K = k(\sqrt[l]{m})$, is of course ramified. Therefore Theorem 2.3 then provides

COROLLARY. *Let $L = \boldsymbol{Q}(\sqrt[l]{m})$ be a pure field of degree l where m is an l-th power-free rational integer. Then*

$$\begin{aligned}\operatorname{rank} H(L) &\geqslant s + s_0 + \operatorname{rank} H(k)^{(\theta)} - \operatorname{rank} \psi\big(\Gamma\iota H(k)^{(\theta)} \cap \bar{H}(K)\big) - \operatorname{rank} \xi(N\Gamma) \\ &\geqslant s_0 + \operatorname{rank} H(k)^{(\theta)} - \operatorname{rank} \psi\big(\iota\bar{H}(k)^{(\theta)}\big) \\ &\geqslant s_0 \quad \text{if} \quad l \geqslant 5; \\ \operatorname{rank} H(L) &= s + s_0 - 1 - a' - \operatorname{rank} \psi(\Gamma) \quad \text{if} \quad l = 3.\end{aligned}$$

Here s (resp. s_0) is the number of primes $\equiv 1 \pmod{l}$ (resp. $\pm 1 \pmod{l}$) dividing m, and $a' = 0$ or 1 according to whether or not every prime factor $\neq 3$ of m is congruent to $\pm 1 \pmod 9$.

Remark. The rank formula in the cubic case $l = 3$ in the corollary has been already obtained, independently of each other, by Gerth [2], Gras [4], and Kobayashi [12]. The corollary applies to the pure quintic case $l = 5$ to show that if at least one prime $\equiv -1 \pmod 5$ divides m, then the class number of the pure quintic field $L = \boldsymbol{Q}(\sqrt[5]{m})$ is a multiple of 5; but this follows also from Theorems 1, 2 and 3 in [11], and gives an answer to one of the question raised in [8].

3. Computation of the ranks of $\psi\big(\Gamma\iota H(k)^{(\theta)} \cap \bar{H}(K)\big)$ and $\psi\big(\iota\bar{H}(k)^{(\theta)}\big)$. In this section we interpret the ranks in terms of the ranks of certain matrices whose elements are in the finite field $\boldsymbol{F}_l$ of l elements. We put $V = \Gamma\iota H(k)^{(\theta)} \cap \bar{H}(K)$ and $W = \iota\bar{H}(k)^{(\theta)}$. By virtue of [6], Theorem 1, rank $\psi(V)$ and rank $\psi(W)$ appearing in our lower bounds can be expressed as follows. Let $\mathfrak{q}_1, \ldots, \mathfrak{q}_t$ be the prime ideals of k ramified fully in K, let $(\ ,K/k)_{\mathfrak{q}}$ be the norm residue symbol at a prime $\mathfrak{q}$ of k in the cyclic extension K/k (as to its definition and properties see [5], Part II, § 6), and let $\lambda_{\mathfrak{q}}: k^\times = k\setminus\{0\} \to S = G(K/k)$ be the homomorphism defined by $\lambda_{\mathfrak{q}}(\gamma) = (\gamma, K/k)_{\mathfrak{q}}$, $\gamma \in k^\times$. Let $\alpha_1, \ldots, \alpha_v$ (resp. $\beta_1, \ldots, \beta_w$) be elements of $k^\times$ such that the classes $c(N^{-1}(\alpha_i))$'s (resp. $c(N^{-1}(\beta_i))$'s) generate V (resp. W), where N^{-1} denotes the inverse for N and (γ) denotes the principal ideal of k generated by $\gamma \in k^\times$. Let $\{\varepsilon_1, \ldots, \varepsilon_u\}$ be a set of generators for $E(k)^{(\theta)}$.

For these α's (resp. β's; ε's), we denote by M'_V (resp. M'_W; M) the $v \times t$ (resp. $w \times t$; $u \times t$) matrix with i, j component $\lambda_{\mathfrak{q}_j}(\alpha_i)$ (resp. $\lambda_{\mathfrak{q}_j}(\beta_i)$; $\lambda_{\mathfrak{q}_j}(\varepsilon_i)$), and let

$$M_V = \begin{pmatrix} M'_V \\ M \end{pmatrix}, \qquad M_W = \begin{pmatrix} M'_W \\ M \end{pmatrix}.$$

Then it follows easily from [6], Theorem 1, that

$$\operatorname{rank} \psi(V) = \operatorname{rank} M_V - \operatorname{rank} M,$$
$$\operatorname{rank} \psi(W) = \operatorname{rank} M_W - \operatorname{rank} M,$$

where M_V, M_W and M all may be viewed in the obvious manner as matrices over the field $\boldsymbol{F}_l$. Their ranks, of course, are independent of the choice of the α's, β's and ε's.

Now we let $\bar{e}$ be an element of $\boldsymbol{Z}[T]$ such that $\bar{e} \equiv e \pmod{l\boldsymbol{Z}_l[T]}$, and let $\bar{\theta}$: $T \to \boldsymbol{Z}$ be the map given by $\bar{\theta}(\varrho) \equiv \theta(\varrho) \pmod{l\boldsymbol{Z}_l}$ for all $\varrho \in T$. Then for all $\gamma \in k^\times$ and for all $\varrho \in T$, we have

$$\gamma^{\bar{e}\varrho} \equiv \gamma^{\bar{e}\bar{\theta}(\varrho)} \pmod{k^{\times l}}.$$

As is easily seen, the $\alpha^{\bar{e}}$'s (resp. $\beta^{\bar{e}}$'s; $\varepsilon^{\bar{e}}$'s) may be taken for the α's (resp. β's; γ's); we may write α_i (resp. β_i; ε_i) instead of $\alpha_i^{\bar{e}}$ (resp. $\beta_i^{\bar{e}}$; $\varepsilon_i^{\bar{e}}$), and then each one of them, say γ, satisfies $\gamma^\varrho \equiv \gamma^{\bar{\theta}(\varrho)} \pmod{k^{\times l}}$ for all $\varrho \in T$. From this and the basic properties of the norm residue symbol it follows that for all $\varrho \in T$ and for all prime $\mathfrak{q}$, $\lambda_{\mathfrak{q}^\varrho}(\gamma) = \lambda_{\mathfrak{q}}(\gamma)^{\bar{\theta}(\varrho^{-2})}$; in particular this implies that if the decomposition group of $\mathfrak{q}$ in $G(k/\boldsymbol{Q})$ has an order other than 1 or 2, then $\lambda_{\mathfrak{q}}(\gamma) = 1$. Let p_i, $\mathfrak{p}_i$, $1 \leqslant i \leqslant s$, be as defined in Section 2, let $p_{s+1}, \ldots, p_{s_0}$ be the rational primes which are ramified fully in L and whose decomposition groups in $G(k/\boldsymbol{Q})$ are of order 2, and let $\mathfrak{p}_i$, $s+1 \leqslant i \leqslant s_0$, be a prime ideal of k above p_i. Let $\tilde{M}'_V$ (resp. $\tilde{M}'_W$; $\tilde{M}$) denote the $v \times s_0$ (resp. $w \times s_0$; $u \times s_0$)

matrix with i, j component $\lambda_{\mathfrak{p}_j}(\alpha_i)$ (resp. $\lambda_{\mathfrak{p}_j}(\beta_i)$; $\lambda_{\mathfrak{p}_j}(\varepsilon_i)$), and let $\tilde{M}_V = \begin{pmatrix} \tilde{M}'_V \\ \tilde{M} \end{pmatrix}$, $M_W = \begin{pmatrix} \tilde{M}'_W \\ \tilde{M} \end{pmatrix}$. Then it follows from the above that

$$\operatorname{rank} \psi(V) = \operatorname{rank} \tilde{M}_V - \operatorname{rank} \tilde{M},$$
$$\operatorname{rank} \psi(W) = \operatorname{rank} \tilde{M}_W - \operatorname{rank} \tilde{M}.$$

So our next task is to consider each $\lambda_{\mathfrak{p}_j}$, $1 \leqslant j \leqslant s_0$. Call $\mathfrak{p}$ one of these primes $\mathfrak{p}_j$'s, let p be the rational prime below $\mathfrak{p}$, and let $k_\mathfrak{p}$ (resp. $\boldsymbol{Q}_p$) denote the completion of k (resp. $\boldsymbol{Q}$) at $\mathfrak{p}$ (resp. p). Then the compositum $K \cdot k_\mathfrak{p}$ is a cyclic extension of $k_\mathfrak{p}$ of degree l. Let $J_\mathfrak{p}$ denote the subgroup of $k_\mathfrak{p}^\times = k_\mathfrak{p} \setminus \{0\}$ corresponding to the cyclic extension $K \cdot k_\mathfrak{p}/k_\mathfrak{p}$ in the sense of local field theory. After identifying the Galois group $G(K/k)$ that is isomorphic to the Galois group $G(K \cdot k_\mathfrak{p}/k_\mathfrak{p})$ with the factor group $k_\mathfrak{p}^\times/J_\mathfrak{p}$ in the natural manner, we may regard $\lambda_\mathfrak{p}$ in question as a homomorphism of $k^\times$ to $k_\mathfrak{p}^\times/J_\mathfrak{p}$. So we are now interested only in the group $J_\mathfrak{p}$. To examine it we use some facts which may be found in [13]. Let $\mathfrak{f}$ be the conductor of the cyclic extension K/k; then $\mathfrak{f}^\tau = \mathfrak{f}$. We distinguish the following five cases.

Case 1. $p \neq l$ and $p \in \{p_1, \ldots, p_s\}$; in this case $k_\mathfrak{p} = \boldsymbol{Q}_p$ and $p \equiv 1 \pmod{l}$. Also $\mathfrak{p} \| \mathfrak{f}$.

Case 2. $p = l \in \{p_1, \ldots, p_s\}$. Write $\mathfrak{p} = \mathfrak{l}$; then $k_\mathfrak{l} = \boldsymbol{Q}_l$ and $\mathfrak{l}^2 \| \mathfrak{f}$.

Case 3. $p \neq l$ and $p \in \{p_{s+1}, \ldots, p_{s_0}\}$, in which case $k_\mathfrak{p}/\boldsymbol{Q}_p$ is a quadratic unramified extension and $p \equiv -1 \pmod{l}$. Also $\mathfrak{p} \| \mathfrak{f}$.

Case 4. $p = l \in \{p_{s+1}, \ldots, p_{s_0}\}$ and $k_\mathfrak{l}/\boldsymbol{Q}_l$ is a quadratic unramified extension. In this case $\mathfrak{l}^2 \| \mathfrak{f}$.

Case 5. $p = l \in \{p_{s+1}, \ldots, p_{s_0}\}$ and $k_\mathfrak{l}/\boldsymbol{Q}_l$ is a quadratic ramified extension. If $l \geqslant 5$, then $\mathfrak{l}^2 \| \mathfrak{f}$. If $l = 3$, then either $\mathfrak{l}^2 \| \mathfrak{f}$ or $\mathfrak{l}^4 \| \mathfrak{f}$; but in this case the Hasse's product formula for the norm residue symbol enables us to delete the column of the matrices $\tilde{M}$, $\tilde{M}_V$ and $\tilde{M}_W$ that involves the prime $\mathfrak{l}$, and so we may leave out this cubic case.

Now we let, for each integer $i \geqslant 1$,

$$U_\mathfrak{p}^{(i)} = \{\alpha \in k_\mathfrak{p}^\times;\ \alpha \equiv 1 \pmod{\mathfrak{p}^i}\},$$

let $U_\mathfrak{p} = \{\alpha \in k_\mathfrak{p}^\times;\ (\alpha, \mathfrak{p}) = 1\}$ be the $\mathfrak{p}$-units, and let ζ_m be a primitive mth root of unity contained in $k_\mathfrak{p}^\times$.

Case 3. In this case it is seen that

$$J_\mathfrak{p} = \langle p \rangle \times \langle \zeta_{p^2-1} \rangle^l \times U_\mathfrak{p}^{(1)} \text{ (direct product)}.$$

In fact $\mathfrak{p} \| \mathfrak{f}$ means that $U_\mathfrak{p}^{(1)} \subset J_\mathfrak{p}$. Since the extension $L \cdot \boldsymbol{Q}_p/\boldsymbol{Q}_p$ is nonabelian of degree l, local class field theory shows that $\boldsymbol{Q}_p^\times \subset J_\mathfrak{p}$. Also this extension is tamely ramified, so we have $L \cdot \boldsymbol{Q}_p = \boldsymbol{Q}_p(\sqrt[l]{pd})$ for some $d \in \boldsymbol{Q}_p^\times$, which implies that $pd \in J_\mathfrak{p}$. As the index of the group $\langle p \rangle \times \langle \zeta_{p^2-1} \rangle^l \times U_\mathfrak{p}^{(1)}$ in $k_\mathfrak{p}^\times$ is exactly l, it must coincide with $J_\mathfrak{p}$.

Case 4. An argument similar to the above shows that

$$J_\mathfrak{l} = \langle l \rangle \times \langle \zeta_{l^2-1} \rangle \times (U_\mathfrak{l}^{(1)} \cap \boldsymbol{Q}_l^\times)\, U_\mathfrak{l}^{(2)}.$$

Case 5. In this case there is an element π of $k^\times$ such that $\pi^2 \in l\boldsymbol{Z}_l^\times$ and $k_\mathfrak{l} = \boldsymbol{Q}_l(\pi)$. Then we have

$$J_\mathfrak{l} = \langle \pi \rangle \times \langle \zeta_{l-1} \rangle \times U_\mathfrak{l}^{(2)}.$$

Case 1. It is seen that $J_\mathfrak{p}$ is written in the form

$$J_\mathfrak{p} = \langle p\mu_\mathfrak{p} \rangle \times \langle \zeta_{p-1} \rangle^l \times U_\mathfrak{p}^{(1)},$$

where $\mu_\mathfrak{p} \in \boldsymbol{Z}$, $\mu_\mathfrak{p} \neq 0$. We note that there are exactly l subgroups of $k_\mathfrak{p}^\times$ of such form; they are $\langle p\mu_i \rangle \times \langle \zeta_{p-1} \rangle^l \times U_\mathfrak{p}^{(1)}$ where $\{\mu_1, \ldots, \mu_l\}$ is a set of coset representatives of $(\boldsymbol{Z}/p\boldsymbol{Z})^{\times l}$ in $(\boldsymbol{Z}/p\boldsymbol{Z})^\times$. However one has always

$$J_\mathfrak{p} \cap U_\mathfrak{p} = \langle \zeta_{p-1} \rangle^l \times U_\mathfrak{p}^{(1)}.$$

Let $I(\mathfrak{f})$ be the group of ideals of k prime to $\mathfrak{f}$, and let J denote the congruence subgroup of $I(\mathfrak{f})$ corresponding to the cyclic extension K/k in the sense of global class field theory. We shall show that the complete determination of the number $\mu_\mathfrak{p}$ may be done when the congruence group J is given. Let $\mathfrak{f}' = \mathfrak{f}/\mathfrak{p}$, and let $I(\mathfrak{f}')$ be the group of ideals of k prime to $\mathfrak{f}'$. As $\mathfrak{p} \| \mathfrak{f}$, $\mathfrak{f}'$ is prime to $\mathfrak{p}$, and so $I(\mathfrak{f}) \subsetneqq I(\mathfrak{f}')$. Let $P(\mathfrak{f}) = \{(\alpha);\ \alpha \in k^\times,\ \alpha \equiv 1 \pmod{\mathfrak{f}}\}$, and $P(\mathfrak{f}') = \{(\alpha);\ \alpha \in k^\times,\ \alpha \equiv 1 \pmod{\mathfrak{f}'}\}$. Since the conductor of J is $\mathfrak{f}$, then $I(\mathfrak{f}) \cap P(\mathfrak{f}') \not\subset J$, and so $J\big(I(\mathfrak{f}) \cap P(\mathfrak{f}')\big) \supsetneqq J$. This implies that $I(\mathfrak{f}) = J\big(I(\mathfrak{f}) \cap P(\mathfrak{f}')\big)$ since J is of index l in $I(\mathfrak{f})$. Also the canonical homomorphism of $I(\mathfrak{f})/P(\mathfrak{f})$ to $I(\mathfrak{f}')/P(\mathfrak{f}')$ is surjective. Hence it follows that

$$I(\mathfrak{f}') = I(\mathfrak{f})\, P(\mathfrak{f}') = J\big(I(\mathfrak{f}) \cap P(\mathfrak{f}')\big) P(\mathfrak{f}') = JP(\mathfrak{f}'),$$

and therefore there is an element $\omega_\mathfrak{p}$ of $k^\times$ such that $(\omega_\mathfrak{p})\mathfrak{p} \in J$. Now we let u_i, $1 \leqslant i \leqslant p-1$, be elements of $k^\times$ such that $u_i \equiv 1 \pmod{\mathfrak{f}'}$ and $u_i \equiv pi \pmod{\mathfrak{p}^2}$. For each i, put $\mathfrak{c}_i = (u_i)\mathfrak{p}^{-1}$; then $\mathfrak{c}_i \in I(\mathfrak{f})$. By the definition of the norm residue symbol in [5], Part II, § 6, we have

$$(u_i, K/k)_\mathfrak{p} = \left(\frac{K/k}{\mathfrak{c}_i}\right)$$

where $\left(\frac{K/k}{\quad}\right)$ denotes the Artin symbol of K/k. From this it follows that $u_i \in J_\mathfrak{p} \Leftrightarrow \mathfrak{c}_i \in J$. But it is clear that $\mathfrak{c}_i \in J \Leftrightarrow (\omega_\mathfrak{p} u_i) \in J$. Also we have $u_i \in J_\mathfrak{p} \Leftrightarrow pi \in J_\mathfrak{p}$ since $u_i \equiv pi \pmod{\mathfrak{p}^2}$ and since $U_\mathfrak{p}^{(2)} \subset J_\mathfrak{p}$. Thus we conclude that pi satisfying $(\omega_\mathfrak{p} u_i) \in J$ belongs to $J_\mathfrak{p}$, and accordingly we may set $u_\mathfrak{p} = pi$. As was shown in [13], the congruence group J can be defined by a linear functional on the F_l-space $(\mathfrak{O}/\mathfrak{f})^\times/(\mathfrak{O}/\mathfrak{f})^{\times l}$ where $\mathfrak{O}$ is the ring of integers in k and $(\mathfrak{O}/\mathfrak{f})^\times$ is the group of units in the factor ring $\mathfrak{O}/\mathfrak{f}$. Hence in Case 1 the linear functional attached to the congruence group J enables one to determine completely the group $J_\mathfrak{p}$.

Case 2. In this case $J_\mathfrak{l}$ is written in the form

$$J_\mathfrak{l} = \langle l(1+\mu_\mathfrak{l} l)\rangle \times \langle \zeta_{l-1}\rangle \times U_\mathfrak{l}^{(2)}$$

where $\mu_\mathfrak{l} \in Z$, $1 \leqslant \mu_\mathfrak{l} \leqslant l$. There are l subgroups of $k_\mathfrak{l}^\times$ of such form. As in Case 1, if we let $\omega_\mathfrak{l}$ be an element of $k^\times$ such that $(\omega_\mathfrak{l})\mathfrak{l} \in J$ (such $\omega_\mathfrak{l}$ does exist) and if we let v_i, $1 \leqslant i \leqslant l$, be elements of $k^\times$ such that $v_i \equiv 1 \pmod{\mathfrak{f}/\mathfrak{l}^2}$ and $v_i \equiv l(1+il) \pmod{\mathfrak{l}^3}$, then it is seen that $l(1+il)$ satisfying $(\omega_\mathfrak{l} v_i) \in J$ belongs to $J_\mathfrak{l}$, and accordingly we may set $l(1+\mu_\mathfrak{l} l) = l(1+il)$. So again the linear functional attached to the congruence group J enables one to determine completely the group $J_\mathfrak{l}$. Of course, it would not be hard to express the above numbers $\mu_\mathfrak{p}$ and $\mu_\mathfrak{l}$ by means of the coefficients of the linear functional, but we shall not explain it here.

Now we mention how to find the numbers α's and β's defined above. For an ideal $\mathfrak{a}$ of k, let $c'(\mathfrak{a})$ denote the ideal class of k containing $\mathfrak{a}$. Let $\mathfrak{b}_1, \ldots, \mathfrak{b}_{r'}$ be ideals of k whose classes $c'(\mathfrak{b})$'s generate the group $\bar{H}(k)^{(\theta)} = \{h \in H(k)^{(\theta)};\ h^l = 1\}$. For each i, write $\mathfrak{b}_i^l = (\bar{\beta}_i)$ with $\bar{\beta}_i \in k^\times$. In view of the definition of the β's, we may choose $\bar{\beta}^{e_\theta}$'s as the β's. As is well known, the ideals $\mathfrak{b}$'s and hence $\bar{\beta}$'s may be chosen to be prime to the ideal $\mathfrak{f}$; then the $\bar{\beta}^{e_\theta}$'s also are prime to $\mathfrak{f}$ since $\mathfrak{f}^\tau = \mathfrak{f}$. The restriction of the homomorphism $\lambda_\mathfrak{p}$: $k^\times \to k_\mathfrak{p}^\times/J_\mathfrak{p}$ to the group $k^\times \cap U_\mathfrak{p}$ induces the homomorphism of $k^\times \cap U_\mathfrak{p}$ to $U_\mathfrak{p}/(J_\mathfrak{p} \cap U_\mathfrak{p})$. Our result about $J_\mathfrak{p}$ described above shows that the group $J_\mathfrak{p} \cap U_\mathfrak{p}$ depends only on a pair $(k, \mathfrak{f})$ (though $J_\mathfrak{p}$ itself does not always). So by choosing these β's prime to $\mathfrak{f}$, we conclude that rank $\psi(W)$ depends only on the pair $(k, \mathfrak{f})$; namely if we denote by K_i, $i = 1, 2$, metacyclic extensions of Q with the same maximal abelian subfield k and with the same conductor $\mathfrak{f}$ over k, then with respect to these fields K_1 and K_2 both rank $\psi(W)$'s are the same, and therefore so are both of the second lower bounds in Theorem 2.3 that involve these ranks.

To find the numbers α's associated with the group $V = \Gamma\iota H(k)^{(\theta)} \cap \bar{H}(K)$, we must recall the definition of the group Γ described in Section 2, where Γ was defined to be $\langle c(\mathfrak{p}_i^g)^e;\ 1 \leqslant i \leqslant s\rangle$, so that $N\Gamma = \langle c'(\mathfrak{p}_i^g)^e;\ 1 \leqslant i \leqslant s\rangle$. Also $N\iota H(k)^{(\theta)} = H(k)^{(\theta)l}$. Therefore we have

$$N(\Gamma\iota H(k)^{(\theta)}) = \langle c'(\mathfrak{p}_i^{ge});\ 1 \leqslant i \leqslant s\rangle H(k)^{(\theta)l}.$$

Let $\mathfrak{a}_1, \ldots, \mathfrak{a}_r$ be ideals of k such that $\langle c'(\mathfrak{a}_1), \ldots, c'(\mathfrak{a}_r)\rangle = H(k)^{(\theta)}$, and let P_k denote the group of principal ideals in k. If we let $(\alpha'_1), \ldots, (\alpha'_u)$ be generators for the factor group

$$(\langle \mathfrak{p}_i^{ge},\ \mathfrak{a}_j^l;\ 1 \leqslant i \leqslant s,\ 1 \leqslant j \leqslant r\rangle \cap P_k)\,P_k^l/P_k^l,$$

it follows from the above that these numbers $\alpha'_1, \ldots, \alpha'_u$ may be chosen as the α's in question.

We conclude this section with a remark about the congruence subgroup $J_\mathfrak{p}$. A defining polynomial of L over Q, if known, enables one to determine immediately $J_\mathfrak{p}$ in our Cases 1 and 2 (cf. [9]).

4. Examples. As our first example, we let k/Q be a quadratic extension with class number 1. Let p_1, p_2 be distinct rational primes $\equiv 1 \pmod{l}$ which are completely decomposed in k, let $\mathfrak{f} = p_1 p_2$, and assume that every units of k are lth power residues mod $\mathfrak{f}$. Let $\mathfrak{O}$ be the ring of integers in k, and let $Y = (\mathfrak{O}/\mathfrak{f})^\times/(\mathfrak{O}/\mathfrak{f})^{\times l}$, which may be viewed as a F_l-space. Then Y is a $F_l[\tau]$-module where τ is the generator for the Galois group $G(k/Q)$, and $Y \cong F_l^4$. As before we let $I(\mathfrak{f})$ denote the group of ideals of k prime to $\mathfrak{f}$, let $P(\mathfrak{f}) = \{(\gamma);\ \gamma \in k^\times,\ \gamma \equiv 1 \pmod{\mathfrak{f}}\}$, and let $C = I(\mathfrak{f})/P(\mathfrak{f})$. Then it follows from our assumption on the units of k that Y is $F_l[\tau]$-isomorphic onto C/C^l through a map v defined by $v(\gamma) = (\gamma)$ for every $\gamma \in \mathfrak{O}$. Let $Y^+ = \{y \in Y;\ y^\tau = y\}$ and $Y^- = \{y \in Y;\ y^\tau = y^{-1}\}$; then $Y^+ \cong F_l^2$ and $Y^- \cong F_l^2$. For $i = 1, 2$, we denote by r_i a generator for the group $(Z/p_i Z)^\times$. Take $x_1 \in k^\times$ such that $x_1 \equiv r_1 \pmod{p_1}$ and $x_1 \equiv 1 \pmod{p_2}$; take $x_2 \in k^\times$ such that $x_2 \equiv 1 \pmod{p_1}$ and $x_2 \equiv r_2 \pmod{p_2}$. Then $\{(x_1 \bmod \mathfrak{f}), (x_2 \bmod \mathfrak{f})\}$ is a F_l-basis for Y^+. Furthermore take $x_3 \in k^\times$ such that $x_3 \equiv r_1 \pmod{\mathfrak{p}_1}$, $x_3 \equiv r_1^{-1} \pmod{\mathfrak{p}_1^\tau}$ and $x_3 \equiv 1 \pmod{p_2}$, and take $x_4 \in k^\times$ such that $x_4 \equiv 1 \pmod{p_1}$, $x_4 \equiv r_2 \pmod{\mathfrak{p}_2}$ and $x_4 \equiv r_2^{-1} \pmod{\mathfrak{p}_2^\tau}$, where for $i = 1, 2$, $\mathfrak{p}_i$ is a prime ideal of k above p_i. Then $\{(x_3 \bmod \mathfrak{f}), (x_4 \bmod \mathfrak{f})\}$ is a F_l-basis for Y^-. Let $\mathscr{J}$ be the set of congruence subgroups J of $I(\mathfrak{f})$ with the following properties: J contains $P(\mathfrak{f})$, is of index l in $I(\mathfrak{f})$, and has a conductor $\mathfrak{f}$, and the abelian extension K_J of k that corresponds to J is dihedral of degree $2l$ over Q. For $1 \leqslant j \leqslant l-1$, let Y_j be the subgroup of Y generated by Y^+ and by $(x_3 x_4^j \bmod \mathfrak{f})$. Then it is easily seen that $\mathscr{J} = \{v(Y_j);\ 1 \leqslant j \leqslant l-1\}$, and so there are precisely $(l-1)$ dihedral extensions of Q with the given conductor $\mathfrak{f}$ over k. Now fixing j, put $J = v(Y_j)$ and $x = x_3 x_4^j$. For $i = 1, 2$, write $\mathfrak{p}_i = (\pi_i)$ with $\pi_i \in \mathfrak{O}$; then $\pi_i^{1+\tau} = p_i a_i$ with $a_i \in \{\pm 1\}$. Clearly we can pick for $i = 1, 2$, $\alpha_i = \pi_i^{1-\tau}$, α_i being as defined in Section 3. Also our assumption that every units of k are lth power residues mod $\mathfrak{f}$ implies that $\tilde{M} = 0$, hence $\tilde{M}_V = (\lambda_{\mathfrak{p}_j}(\pi_i^{1-\tau}))$, $1 \leqslant i, j \leqslant 2$. However, from the Hasse's product formula for the norm residue symbol we have for $i = 1, 2$: $\lambda_{\mathfrak{p}_1}(\pi_i^{1-\tau}) \cdot \lambda_{\mathfrak{p}_2}(\pi_i^{1-\tau}) = 1$. So

$$\operatorname{rank} \psi(V) = \operatorname{rank}(\lambda_{\mathfrak{p}_1}(\pi_1^{1-\tau}),\ \lambda_{\mathfrak{p}_1}(\pi_2^{1-\tau})).$$

We now want to determine the group $J_{\mathfrak{p}_1}$. Put $\mathfrak{f}' = \mathfrak{f}/\mathfrak{p}_1$. Since $I(\mathfrak{f}') = JP(\mathfrak{f}')$ in which $I(\mathfrak{f}')$ is the group of ideals of k prime to $\mathfrak{f}'$ and $P(\mathfrak{f}') = \{(\gamma);\ \gamma \in k^\times,\ \gamma \equiv 1 \pmod{\mathfrak{f}'}\}$, then

$$\pi_1 \equiv x_1^{e_1} x_2^{e_2} x^{e_3} z^l \pmod{\mathfrak{f}'} \quad \text{with} \quad e_i \in F_l,\ (z) \in I(\mathfrak{f}).$$

Putting $x_0 = x_1^{e_1} x_2^{e_2} x^{e_3} z^l$ and $u_0 = \pi_1 x_0^{-1}$, we have that $u_0 \equiv 1 \pmod{\mathfrak{f}'}$, $(u_0) \in \mathfrak{p}_1 J$, and $x_0 \equiv r_1^{e_1+e_3} z^l \pmod{\mathfrak{p}_1}$. Take $b \in Z$ such that $\pi_1 \equiv p_1 b$

(mod $\mathfrak{p}_1^2$); then $u_0 \equiv p_1 b r_1^{-e_1-e_3} z^{-l}$ (mod $\mathfrak{p}_1^2$). On the other hand it follows from $\pi_1^{1+\tau} = p_1 a_1$ that $b \equiv a_1 r_1^{-e_1+e_3} z^{-l\tau}$ (mod $\mathfrak{p}_1$). Hence

$$u_0 \equiv p_1 r_1^{-2e_1} z^{-l(1+\tau)} a_1 \pmod{\mathfrak{p}_1^2},$$

so that $p_1 r_1^{-2e_1} \in J_{\mathfrak{p}_1}$, which implies that

$$J_{\mathfrak{p}_1} = \langle p_1 r_1^{-2e_1} \rangle \times \langle \zeta_{p_1-1} \rangle^l \times U_{\mathfrak{p}_1}^{(1)}.$$

Considering the map $\lambda_{\mathfrak{p}_1}$ to be a homomorphism of $k^\times$ to the factor group $k_{\mathfrak{p}_1}^\times / J_{\mathfrak{p}_1}$, we have from the above that

$$\lambda_{\mathfrak{p}_1}(\pi_1^{1-\tau}) = (r_1^{2e_3} \bmod J_{\mathfrak{p}_1}).$$

In view of the definition of e_3, it is clear that its vanishing is independent of the choice of J in $\mathscr{J}$, and therefore so is rank $(\lambda_{\mathfrak{p}_1}(\pi_1^{1-\tau}))$. But this follows also from the fact that $\lambda_{\mathfrak{p}_1}(\pi_1^{1-\tau}) = \lambda_{\mathfrak{p}_2}(\pi_1^{1-\tau})^{-1}$, which was a consequence of the Hasse's product formula. Thus rank $\psi(V)$ and hence the first lower bound in Theorem 2.3 that involves this rank are independent of the choice of J in $\mathscr{J}$. (Note that rank $\psi(V) = \operatorname{rank}(\lambda_{\mathfrak{p}_1}(\pi_2^{1-\tau}), \lambda_{\mathfrak{p}_2}(\pi_1^{1-\tau}))$ by means of the product formula.)

For our next example we let $L = \boldsymbol{Q}(\sqrt[l]{p})$ where $p = (c_0^l + c_1^l)/(c_0 + c_1)$ is a prime, $l \geqslant 5$, and $c_0, c_1 \in \boldsymbol{Z}$. Let ζ be a primitive lth root of unity, $k = \boldsymbol{Q}(\zeta)$, and $P(X) = c_0 + c_1 X$. Then p is a norm of $P(\zeta)$, and so $p \equiv 1$ (mod l). Also $\mathfrak{p} = (P(\zeta))$ is a prime ideal of k above p. Let r be a generator for the group $(\boldsymbol{Z}/l\boldsymbol{Z})^\times$, and τ be a generator for the Galois group $G(k/\boldsymbol{Q})$ defined by $\zeta^\tau = \zeta^r$. As before we denote by e the idempotent of $\boldsymbol{Z}_l[G(k/\boldsymbol{Q})]$ attached to the character θ; in this case θ is defined by $\theta(\tau^{-1}) \equiv r$ (mod l). So putting $g(X) = \sum_{i=0}^{l-2} r_i X^i$ where for $0 \leqslant i \leqslant l-2$, $r_i \in \boldsymbol{Z}$ are chosen such that $1 \leqslant r_i \leqslant l-1$ and $r_i \equiv r^i$ (mod l), we have $e \equiv -g(\tau)$ (mod l). Put $n(X) = \sum_{i=0}^{l-2} X^i$ and $f(X) = g(X) - n(X)$. For elements γ_1, γ_2 of $k^\times$ both prime to $\mathfrak{p}$, $\gamma_1 \underset{(l)}{\equiv} \gamma_2$ (mod $\mathfrak{p}$) means that $\gamma_1 \gamma_2^{-1}$ is an lth power residue mod $\mathfrak{p}$. Then it follows from the properties of the norm residue symbol that

$$(P(\zeta)^e, k(\sqrt[l]{p})/k)_{\mathfrak{p}} = 1 \Leftrightarrow P(\zeta)^{f(\tau)} \underset{(l)}{\equiv} 1 \pmod{\mathfrak{p}}.$$

As will be seen below, the latter condition is equivalent to saying that $c_0 + c_1 \underset{(l)}{\equiv} 1$ (mod $\mathfrak{p}$), or, what amounts to the same, $(c_0 + c_1)^{(p-1)/l} \equiv 1$ (mod p). Put

$$Q(X) = \prod_{i=1}^{l-2} (c_0 + c_1 X^{r_i})^{r_{i-1}};$$

then $Q(\zeta) = P(\zeta)^{f(\tau)}$. Furthermore put

$$c = \prod_{i=1}^{l-2} c_1^{(r_i-1)^2} \quad \text{and} \quad R(X) = cQ(X);$$

since $\zeta \equiv -c_0/c_1$ (mod $\mathfrak{p}$), then $R(\zeta) \equiv R(-c_0/c_1)$ (mod $\mathfrak{p}$). Let $A' = \{r_i - 1;\ 1 \leqslant i \leqslant l-2\} = \{1, 2, \ldots, l-2\}$, $A = \{2, 3, \ldots, (l-1)/2\}$, and $\bar{A} = \{(j_1, j_2) \in A \times A';\ j_1 + j_2 = l\}$. In the following the product $\prod$ and summation $\sum$ are both taken over all $j_1 \in A$, the product $\prod'$ over all $(j_1, j_2) \in \bar{A}$, and the summation $\sum'$ over all $j \in A'$. Putting $d = -c_0$, we have

$$R(-c_0/c_1) = d(d-c_1) \prod{}' d^l (d^{j_1} - c_1^{j_1})^{j_1} (d^{j_2} - c_1^{j_2})^{j_2}.$$

But, for each $(j_1, j_2) \in \bar{A}$,

$$d^{j_1 j_2} (d^{j_1} - c_1^{j_1})^{j_1} \equiv (d^l - c_1^{j_1} d^{j_2})^{j_1} \equiv (c_1^l - c_1^{j_1} d^{j_2})^{j_1} \equiv c_1^{j_1^2} (c_1^{j_2} - d^{j_2})^{j_1} \pmod{\mathfrak{p}}.$$

So we have

$$R(-c_0/c_1) \prod{}' d^{j_1 j_2} \equiv d(d-c_1) \prod{}' d^l \prod{}' \{(-1)^{j_1} c_1^{j_1^2} (d^{j_2} - c_1^{j_2})^l\} \pmod{\mathfrak{p}}.$$

Therefore

$$cQ(\zeta) \prod{}' d^{j_1 j_2} \underset{(l)}{\equiv} d(d-c_1) \prod c_1^{j_1^2} \pmod{\mathfrak{p}}.$$

Since $l \geqslant 5$, then $1 + \sum j_1^2 \equiv 0$ (mod l), which implies that

$$\prod{}' d^{j_1 j_2} \equiv \prod d^{lj_1 - j_1^2} \underset{(l)}{\equiv} d \pmod{\mathfrak{p}}.$$

Also

$$\sum{}' j^2 \equiv (1 + \sum j_1^2) + \sum (l - j_1)^2 \equiv \sum j_1^2 \pmod{l},$$

so that

$$c \underset{(l)}{\equiv} \prod c_1^{j_1^2} \pmod{\mathfrak{p}}.$$

Thus we conclude from the above that

$$Q(\zeta) \underset{(l)}{\equiv} d - c_1 \underset{(l)}{\equiv} c_0 + c_1 \pmod{\mathfrak{p}},$$

which was to be shown.

Now we assume that $(c_0 + c_1)^{(p-1)/l} \equiv 1$ (mod p). Let Γ be as defined in Section 2, and let $\mathfrak{P}$ be the unique prime ideal of $K = k(\sqrt[l]{p})$ above $\mathfrak{p} = (P(\zeta))$; then Γ is generated by $c(\mathfrak{P})^e$, and so $N\Gamma = 1$, which implies that $V = \Gamma \cdot {}_l\bar{H}(k)^{(\theta)} = \Gamma W$. Then $(P(\zeta)^e, K/k)_{\mathfrak{p}} = 1$ implies that rank $\psi(V)$

$= \operatorname{rank} \psi(W)$. Therefore the first lower bound for rank $H(Q(\sqrt[l]{p}))$ in the corollary to Theorem 2.3 becomes $2 + \operatorname{rank} H(k)^{(\theta)} - \operatorname{rank} \psi(W)$; in particular this says that the l-class group $H(Q(\sqrt[l]{p}))$ is not cyclic.

References

[1] A. Fröhlich, *The genus group and genus field in finite number fields*, (I) Mathematika 6 (1959), pp. 40–46; (II) ibid., pp. 142–146.

[2] F. Gerth III, *Ranks of 3-class groups of non-Galois cubic fields*, Acta Arith. 30 (1977), pp. 302–322.

[3] G. Gras, *Sur les l-classes d'idéaux dans les extensions cycliques relatives de degré premier l*, Ann. Inst. Fourier 23,3 (1973), pp. 1–48.

[4] — *Sur le 3-rang des corps cubiques non galoisiens*, Séminaire de Théorie des Nombres, Besançon, 1974–75.

[5] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Physica-Verlag, Würzburg-Wien 1970.

[6] F. Halter-Koch, *Ein Satz über die Geschlechter relativ-zyklischen Zahlkörper von Primezahlgrad und seine Anwendung auf biquadratische-bizyklische Körper*, J. Number Theory 4 (1972), pp. 144–156.

[7] T. Honda, *Pure cubic fields whose class numbers are multiples of* 3, ibid. 3 (1971), pp. 7–12.

[8] K. Iimura, *A criterion for the class number of a pure quintic field to be divisible by* 5, J. Reine Angew. Math. 292 (1977), pp. 201–210.

[9] M. Ishida, *An algorithm for constructing the genus field of an algebraic number field of odd prime degree*, J. Fac. Sci. Univ. Tokyo, Sec. IA, 24 (1977), pp. 61–75.

[10] J. F. Jaulent, *Structures galoisiennes dans les extensions métabéliennes*, Thèse, 3ème cycle, Besançon, 1979.

[11] — *Unités et classes dans les extensions métabéliennes de degré nl^s sur un corps de nombres algébriques*, Ann. Inst. Fourier 31,1 (1981), pp. 39–62.

[12] S. Kobayashi, *Complete determination of the 3-rank in pure cubic fields*, J. Math. Soc. Japan 29 (1977), pp. 373–384.

[13] J. Porusch, *Die Arithmetik in Zahlkörpern, deren zugehörige Galoissche Körpern spezielle metabelsche Gruppen besitzen, auf klassenkörpertheoretischer Grundlage*, Math. Zeit. 37 (1933), pp. 134–160.

[14] C. Walter, *The ambiguous class group and the group of certain non-normal extensions*, Mathematika 26 (1979), pp. 113–124.

THE METROPOLITAN COLLEGE OF TECHNOLOGY
6-6 ASAHIGAOKA, HINO, TOKYO 191, JAPAN

Received on 31. 1. 1985
and in revised form on 15. 5. 1985 (1490)

ACTA ARITHMETICA
XLVII (1986)

LeVeque's superelliptic equation over function fields

by

R. C. Mason (Cambridge) and B. Brindza (Debrecen)

1. Introduction. In a letter to Mordell written in 1925, later published, Siegel [9] proved that the hyperelliptic equation $y^2 = g(x)$ has only finitely many solutions in integers x and y: g denotes a polynomial with integer coefficients, possessing at least three simple zeros. Siegel's later investigations revealed his celebrated theorem [10] concerning the solutions of any polynomial equation $F(x, y) = 0$: he proved that there are only finitely many integer solutions, unless the curve associated with F has genus zero and no more than two infinite valuations. Siegel's proof was ineffective: he employed both the Mordell–Weil theorem and his own theorem on the approximation of algebraic numbers by rationals, which was a development of the pioneering work of Thue. In 1964 LeVeque [3] generalized Siegel's result on the hyperelliptic equation to prove that the superelliptic equation $y^m = f(x)$ has only finitely many solutions in any ring of algebraic integers, unless of course it falls into the exceptional cases predicted by Siegel's general theorem. The conditions on f and m equivalent to the exceptional cases are given below ($\dagger$). LeVeque's result was ineffective. In 1968 Baker proved the first general effective result on Diophantine equations by employing his celebrated lower bound for linear forms in logarithms: he effectively solved first the Thue equation, and then the hyperelliptic and certain superelliptic equations [1]. Baker's bounds were improved by Sprindžuk [11], [12]. LeVeque's theorem of 1964 was recently made completely effective by Brindza [2].

This paper is devoted to establishing a bound on the solutions of LeVeque's equation in the analogous case of function fields. Let k denote an algebraically closed field of characteristic zero, and $k(z)$ the rational function field over k. Let us consider the set of solutions X, Y in the ring of polynomials $k[z]$ of the hyperelliptic equation $Y^2 = G(X)$, where G is a polynomial with coefficients in $k[z]$ and possessing at least three simple zeros. It is plainly possible for this equation to have infinitely many solutions, for example if the coefficients of G actually lie in k. However, it is