T. Komatsu and S. Nakano
Nagoya Math. J.
Vol. 164 (2001), 133–146

ON THE GALOIS MODULE STRUCTURE OF IDEAL CLASS GROUPS

TORU KOMATSU AND SHIN NAKANO

Abstract. Let K/k be a Galois extension of a number field of degree n and p a prime number which does not divide n. The study of the p-rank of the ideal class group of K by using those of intermediate fields of K/k has been made by Iwasawa, Masley et al., attaining the results obtained under respective constraining assumptions. In the present paper we shall show that we can remove these assumptions, and give more general results under a unified viewpoint. Finally, we shall add a remark on the class numbers of cyclic extensions of prime degree of $\mathbb{Q}$.

Introduction

Throughout this paper, p will denote a prime number and $\mathbb{F}_p$ the finite field with p elements. For an integer $n > 1$ prime to p, denote by $c(n,p)$ the order of p in the multiplicative group $(\mathbb{Z}/n\mathbb{Z})^\times$, and by $d(n,p)$ the minimum of $c(l,p)$ for all prime factors l of n. For a finite abelian group A, denote by r_pA its p-rank; $r_pA = \dim_{\mathbb{F}_p}(A/pA)$. We will use this notation r_p instead of $\dim_{\mathbb{F}_p}$ even for vector spaces over $\mathbb{F}_p$. Denote by $C(K)$ and $h(K)$ the ideal class group and the class number of an algebraic number field K.

Let k be an algebraic number field of finite degree and K a Galois extension of k of degree n prime to p. Iwasawa [5] deduced the inequality $r_pC(K) \geqq d(n,p)$ under the conditions $p \nmid h(k)$ and $p|h(K)$ from the following group theoretical proposition:

> *Let G be a group of order n prime to p and M an $\mathbb{F}_p[G]$-module such that the action of G on M is non-trivial. Then $r_pM \geq d(n,p)$.*

Suppose G and M are as above. Then G acts non-trivially on the quotient module M/M^G, where M^G is the submodule of M consisting of elements

Received May 26, 2000.
Revised September 22, 2000.
2000 Mathematics Subject Classification: 11R29.

left fixed by G. Therefore the conclusion of the above property can be replaced by $r_pM - r_pM^G \geq d(n,p)$. From this simple observation, we can improve a little the above result of Iwasawa on ideal class groups. It will be seen that M/M^G is isomorphic to the kernel of the norm map: $M \to M$, $x \mapsto \sum_{\sigma\in G} \sigma x$.

In this paper, we shall utilize the kernels of the maps of this kind to study the behavior of the p-rank of finite G-modules, and apply it to the rank of ideal class groups. After group theoretical discussions of same kind as above, we shall apply them to the estimation of the rank of ideal class groups, and extend the results of Masley[7], Cornell–Rosen[3] and others, as well as to the non-l-part of the ideal class group in $\mathbb{Z}_l$-extensions. Finally, we shall add a remark on the class numbers of cyclic fields of prime degrees of $\mathbb{Q}$ including a conjecture.

The authors would like to thank the referee for valuable suggestions.

§1. Group theoretical discussions

Let G be a finite group and M a finite G-module. Let $x \in M$. The stabilizer of x is denoted by G_x and the G-orbit of x by Gx, that is,

$$G_x = \{\sigma \in G \mid \sigma x = x\}, \quad Gx = \{\sigma x \in M \mid \sigma \in G\}.$$

It is familiar that $|Gx| = (G : G_x)$.

LEMMA 1. *Assume that $G_x = \{1\}$ for every $x(\neq 0) \in M$. Then we have $|M| \equiv 1 \pmod{|G|}$.*

Proof. Decompose M to the G-orbits: $M = \{0\} \cup Gx_1 \cup \cdots \cup Gx_t$. It follows from the assumption that $|Gx_i| = (G : G_{x_i}) = |G|$ $(1 \leq i \leq t)$. Hence we have $|M| = 1 + t|G| \equiv 1 \pmod{|G|}$. □

For a subgroup H of G, we define a subset M^H of M by

$$M^H = \{x \in M \mid \sigma x = x \text{ for all } \sigma \in H\}.$$

The norm map N_H for H is an endomorphism of M as an H-module defined by

$$N_H : M \to M, \quad x \mapsto \sum_{\sigma\in H} \sigma x.$$

https://doi.org/10.1017/S0027763000008072 Published online by Cambridge University Press

Put $H(\sigma) = \sigma H \sigma^{-1}$ for $\sigma \in G$. We easily see that

$$\sigma M^H = M^{H(\sigma)}, \quad \sigma N_H x = N_{H(\sigma)}(\sigma x)$$

for $\sigma \in G$ and $x \in M$. In particular, if H is a normal subgroup of G then M^H is a G-module and N_H is a G-homomorphism.

LEMMA 2. *Let H be a subgroup of G.*

(1) $\operatorname{Ker} N_H \subseteq \operatorname{Ker} N_G$.

(2) *If H is a normal subgroup acting on M trivially, then M becomes a G/H-module and* $\operatorname{Ker} N_{G/H} \subseteq \operatorname{Ker} N_G$.

Proof. Use the decomposition to the cosets of H in G. □

LEMMA 3. *If $(|G|, |M^G|) = 1$, then $N_G M = M^G$ and $M = M^G \oplus \operatorname{Ker} N_G$.*

Proof. The inclusion $N_G M \subseteq M^G$ is clear. We must make sure of the converse. Let $x \in M^G$. Then we have $N_G x = |G|x$. It follows from the assumption that there exists an $a \in \mathbb{Z}$ such that $a|G| \equiv 1 \pmod{|M^G|}$. Thus $x = a|G|x = aN_G x$ and we conclude $M^G \subseteq N_G M$. Furthermore, the same argument shows that $M^G \cap \operatorname{Ker} N_G = \{0\}$. Comparing the orders, we obtain $M = M^G \oplus \operatorname{Ker} N_G$. □

LEMMA 4. *If $|G|$ is prime and $(|G|, |\operatorname{Ker} N_G|) = 1$, then $|\operatorname{Ker} N_G| \equiv 1 \pmod{|G|}$.*

Proof. Let $x(\neq 0) \in \operatorname{Ker} N_G$. If $G_x = G$, then $0 = N_G x = |G|x$ which yields $x = 0$ by the assumption $(|G|, |\operatorname{Ker} N_G|) = 1$. This is a contradiction. Thus we have $G_x \subsetneq G$. Since the order of G is prime, we have $G_x = \{1\}$ which completes the proof by Lemma 1. □

In order to state our results on the p-rank of G-modules, we shall use the notation $c(n,p), d(n,p)$ defined in Introduction for an integer $n > 1$ prime to p, and one more notation $e(n,p)$ defined as the greatest common divisor of $c(l,p)$ for all prime factors l of n. The following relations hold among them:

https://doi.org/10.1017/S0027763000008072 Published online by Cambridge University Press

$$\begin{array}{ccc} & & c(l,p) \leq c(n,p) \\ & & \| \\ d(n,p) & \leq & d(l,p) \\ \vee| & & \| \\ e(n,p) & \leq & e(l,p) \end{array}$$

where l is a prime factor of n. For an abelian group A and a positive integer m, let $A[m]$ be the kernel of the multiplication-by-m map, i.e.,

$$A[m] = \{a \in A \mid ma = 0\}.$$

It is easy to see that $A[p]$ is an $\mathbb{F}_p$-vector space and its dimension is equal to $r_p A$ provided A is finite.

PROPOSITION 1. *Let G be a cyclic group of prime order $l \neq p$ and M a finite G-module. Then we have*

$$r_p \operatorname{Ker} N_G \equiv 0 \pmod{c(l,p)}.$$

Proof. One may easily check that $r_p \operatorname{Ker} N_G = r_p(M[p] \cap \operatorname{Ker} N_G)$. So we can assume M to be an $\mathbb{F}_p$-space. Then, by Lemma 4, we have $|\operatorname{Ker} N_G| = p^{r_p \operatorname{Ker} N_G} \equiv 1 \pmod{l}$ which implies the desired congruence from the definition of $c(l,p)$. ∎

Remark. We have $r_p M = r_p M^G + r_p \operatorname{Ker} N_G$ by Lemma 3. So the conclusion of the above proposition can be replaced by

$$r_p M - r_p M^G \equiv 0 \pmod{c(l,p)},$$

like in the following results (Propositions 2 and 3).

We next state two propositions which extend slightly the results of Iwasawa [5], Cornell–Rosen [3] or Cornell [2]. Though the heart of the proof may be found in their original arguments, we present here an approach via the direct use of the kernels of norm maps, which seems to us more easily comprehensible.

PROPOSITION 2. *Let G be a group of order n prime to p. Let M be a finite p-group and also a G-module on which the action of G is non-trivial. Then we have*

$$r_p \operatorname{Ker} N_G \geq d(n,p).$$

https://doi.org/10.1017/S0027763000008072 Published online by Cambridge University Press

Proof. Choose $\sigma \in G$ with minimal order such that the action of σ on M is non-trivial. Let l be a prime dividing the order of σ. Put $H = \langle\sigma\rangle/\langle\sigma^l\rangle$. Since σ^l acts on M trivially, M is an H-module and the action of H on M is non-trivial. (The use of such H is owing to Iwasawa [5].) One can use Proposition 1 to see $r_p \operatorname{Ker} N_H \equiv 0 \pmod{c(l,p)}$. If $\operatorname{Ker} N_H = \{0\}$ then the norm map N_H is injective and consequently $M = N_H M \subseteq M^H \subseteq M$. This means $M = M^H$ which contradicts the non-triviality of the action of H. Thus we conclude $\operatorname{Ker} N_H \neq \{0\}$. It follows from Lemma 2 that $\operatorname{Ker} N_H \subseteq \operatorname{Ker} N_{\langle\sigma\rangle} \subseteq \operatorname{Ker} N_G$. Hence

$$r_p \operatorname{Ker} N_G \geq r_p \operatorname{Ker} N_H \geq c(l,p) \geq d(n,p),$$

which completes the proof. ∎

PROPOSITION 3. *Let G be a solvable group of order n prime to p and M a finite G-module. Then there exists a non-negative integer x_l for each prime factor l of n such that*

$$r_p \operatorname{Ker} N_G = \sum_{l|n} x_l c(l,p);$$

therefore we have

$$r_p \operatorname{Ker} N_G \equiv 0 \pmod{e(n,p)}.$$

Proof. Since G is solvable, G has the composition series

$$G = G_0 \supset G_1 \supset \cdots \supset G_t = \{1\}$$

such that every factor group $H_i = G_{i-1}/G_i$ is cyclic of prime order. In view of the sequence

$$M^G = M^{G_0} \subseteq M^{G_1} \subseteq \cdots \subseteq M^{G_t} = M,$$

we write

$$r_p M - r_p M^G = \sum_{i=1}^{t} \left(r_p M^{G_i} - r_p M^{G_{i-1}} \right).$$

Note that M^{G_i} is an H_i-module and further $(M^{G_i})^{H_i} = M^{G_{i-1}}$. Therefore, by Lemma 3 and Proposition 1,

$$r_p M^{G_i} - r_p M^{G_{i-1}} = r_p \operatorname{Ker} \left(N_{H_i} : M^{G_i} \to M^{G_i} \right) \equiv 0 \pmod{c(l_i,p)},$$

https://doi.org/10.1017/S0027763000008072 Published online by Cambridge University Press

where $l_i = |H_i| = (G_{i-1} : G_i)$. Hence we can take non-negative integers y_i such that

$$r_p \operatorname{Ker} N_G = r_p M - r_p M^G = \sum_{i=1}^{t} y_i c(l_i, p).$$

This proves our assertion. □

One may notice that Proposition 3 includes Proposition 1. In the rest of this section, we will extend Proposition 1 in a different direction. Define a subset $\Gamma_G M$ of M by

$$\Gamma_G M = \bigcap_H \operatorname{Ker}(N_H : M \to M),$$

where H runs through all the subgroups of G such that $H \neq \{1\}$. Here, even if the running range of H is restricted to all the cyclic subgroups of prime order, we have the same set as in the right-hand side of the above formula. This is confirmed by the fact that if subgroups H_1, H_2 satisfy $H_1 \subseteq H_2$ then $\operatorname{Ker} N_{H_1} \subseteq \operatorname{Ker} N_{H_2}$ by Lemma 2. It must be also noted that $\Gamma_G M$ becomes a G-module, as shown by the relation $\sigma \operatorname{Ker} N_H = \operatorname{Ker} N_{H(\sigma)}$ for $\sigma \in G$.

LEMMA 5. *If* $(|G|, |\Gamma_G M|) = 1$, *then* $|\Gamma_G M| \equiv 1 \pmod{|G|}$.

Proof. Let x be a non-zero element of $\Gamma_G M$. From Lemma 1, it is enough to show that $G_x = \{1\}$. Suppose that there exists $\sigma(\neq 1) \in G_x$. Let s be the order of σ. It follows from $x \in \Gamma_G M \subseteq \operatorname{Ker} N_{\langle\sigma\rangle}$ that $sx = N_{\langle\sigma\rangle} x = 0$; thus we have $x = 0$ by the assumption. This is a contradiction. □

The next proposition is shown in the same way as Proposition 1 using this lemma.

PROPOSITION 4. *Let G be a group of order n prime to p and M a finite G-module. Then we have*

$$r_p \Gamma_G M \equiv 0 \pmod{c(n, p)}.$$

This is a natural generalization of Proposition 1, because $\Gamma_G M$ is nothing but $\operatorname{Ker} N_G$ in case G is cyclic of prime order.

https://doi.org/10.1017/S0027763000008072 Published online by Cambridge University Press

§2. Rank of ideal class groups

Throughout this section, k denotes a finite algebraic number field. We will apply the results of the previous section to the p-rank of the ideal class groups. We shall describe the behavior of p-rank for a Galois extension of k.

Let K/k be a Galois extension of degree n with the Galois group G. Note that both $C(K)$ and $C(K)[p]$ are G-modules. Furthermore, we can show that if p does not divide n then $C(k)[p]$ is naturally isomorphic to $C(K)[p]^G = C(K)^G[p]$. Thus, for the usual norm map $N_{K/k} : C(K) \to C(k)$, we have

$$r_p \operatorname{Ker} N_{K/k} = r_p C(K) - r_p C(K)^G = r_p C(K) - r_p C(k).$$

From this, we obtain Theorems 1, 2, 3 below as consequence of Propositions 1, 2 and 3, respectively. We add that Theorems 2 and 3 improve the results of [5], [3] or [2].

THEOREM 1. *Let K/k be a cyclic extension of prime degree $l \neq p$. Then we have*

$$r_p C(K) \equiv r_p C(k) \pmod{c(l,p)}.$$

THEOREM 2. *Let K/k be a Galois extension of degree n prime to p. Assume that $r_p C(K) \neq r_p C(k)$. Then we have*

$$r_p C(K) - r_p C(k) \geq d(n,p).$$

THEOREM 3. *Let K/k be a solvable extension of degree n prime to p. Then there exists a non-negative integer x_l for each prime factor l of n such that*

$$r_p C(K) - r_p C(k) = \sum_{l|n} x_l c(l,p);$$

therefore we have

$$r_p C(K) \equiv r_p C(k) \pmod{e(n,p)}.$$

Next, in order to restate Proposition 4, we define a subgroup $B(K/k)$ of $C(K)$, for a finite Galois extension K/k, by

$$B(K/k) = \bigcap_F \operatorname{Ker}(N_{K/F} : C(K) \to C(F)),$$

https://doi.org/10.1017/S0027763000008072 Published online by Cambridge University Press

where F runs through all the fields such that $k \subseteq F \subsetneq K$ and K/F is cyclic of prime degree. Though we may make F run through all the intermediate fields ($\neq K$), the right-hand side turns out to be the same group as above, as remarked after the definition of $\Gamma_G M$. Then Proposition 4 shows the following general result.

THEOREM 4. *Let K/k be a Galois extension of degree n prime to p. Then we have*

$$r_p B(K/k) \equiv 0 \pmod{c(n,p)}.$$

There are several corollaries of Theorem 4. We first present the result on a cyclic extension which generalizes Theorem 1 naturally.

COROLLARY 1. *Let K/k be a cyclic extension of prime degree $l \neq p$. Assume that there is a subfield k_0 of k such that K/k_0 is cyclic of degree l^d. Then we have*

$$r_p C(K) \equiv r_p C(k) \pmod{c(l^d,p)}.$$

Proof. Use the identity $B(K/k_0) = \operatorname{Ker} N_{K/k}$. □

This leads us to the result on the non-l-part of the ideal class groups in a $\mathbb{Z}_l$-extension.

COROLLARY 2. *Let l be a prime different from p. Let k_∞/k be a $\mathbb{Z}_l$-extension and k_n its n-th layer, that is, $[k_n : k] = l^n$. Then we have*

$$r_p C(k_n) \equiv r_p C(k_{n-1}) \pmod{c(l^n,p)},$$

for $n \geq 1$.

Remark. If k is abelian over $\mathbb{Q}$, then there is no interest in applying this result to the layers of sufficiently large degrees. In fact, Washington [9] has proved that, in such a case, the non-l-part of the class number $h(k_n)$ is bounded as $n \to \infty$ (see also [10, Ch. 16]).

Next we generalize the result of Masley [7] where the restricted case that K/k is abelian and moreover $r_p C(k) = 0$ is treated (cf. [3] and [10, Ch. 10]).

https://doi.org/10.1017/S0027763000008072 Published online by Cambridge University Press

COROLLARY 3. *Let K/k be a Galois extension of degree n prime to p. Assume that $r_pC(F) = r_pC(k)$ for every intermediate fields $k \subseteq F \subsetneq K$ such that K/F is cyclic of prime degree. Then we have*

$$r_pC(K) \equiv r_pC(k) \pmod{c(n,p)}.$$

Proof. We abbreviate $(\operatorname{Ker} N_{K/F})[p]$ to $D(F)$ for an intermediate field F of K/k. Then we have $r_pD(F) = r_p \operatorname{Ker} N_{K/F} = r_pC(K) - r_pC(F)$. If K/F is cyclic of prime degree, then $r_pD(F) = r_pD(k)$ by our assumption, and thus $D(F) = D(k)$. Hence we find $B(K/k)[p] = D(k)$. The desired congruence follows from this and Theorem 4. □

Remark. Let A be a finite abelian group and m a positive integer. We define p^m-rank of A by $r_{p^m}A = \dim_{\mathbb{F}_p}(p^{m-1}A/p^mA)$. Obviously, it is also given by $r_{p^m}A = r_p(A[p^m]/A[p^{m-1}])$. Considering $C(K)[p^m]/C(K)[p^{m-1}]$ instead of $C(K)[p]$, we may extend all the results of this section to those on the p^m-rank of ideal class groups. For example, Theorem 2 is generalized as

$$r_{p^m}C(K) - r_{p^m}C(k) \geq d(n,p), \quad \text{if } r_{p^m}C(K) \neq r_{p^m}C(k),$$

and the conclusion of Theorem 4 is rewritten in the form

$$r_{p^m}B(K/k) \equiv 0 \pmod{c(n,p)},$$

for a positive integer m. The other results are also to be modified in the same manner. Note that $c(n,p)$ is independent of m.

§3. A remark on cyclic extensions of prime degrees of $\mathbb{Q}$

The results mentioned in the previous section are of a nature to restrict the structure of the ideal class group $C(K)$ of a number field K by those of its subfields. We now consider the simplest case where K is a cyclic extension over $\mathbb{Q}$ of prime degree l. The set of the class numbers $h(K)$ of all such fields K is denoted by $H(l)$. We define a set $\mathcal{H}(l)$ of positive integers by

$$\mathcal{H}(l) = \{a \in \mathbb{N} \mid p^{v_p(a)} \equiv 1 \pmod{l} \text{ for all prime numbers } p \neq l\},$$

where $v_p(a)$ is the additive p-adic valuation of a, that is, the non-negative integer v satisfying $p^v | a$ and $p^{v+1} \nmid a$.

PROPOSITION 5. *For a prime l, we have $H(l) \subset \mathcal{H}(l)$.*

https://doi.org/10.1017/S0027763000008072 Published online by Cambridge University Press

Proof. Let $h \in H(l)$ and take an arbitrary cyclic extension K over $\mathbb{Q}$ of degree l with $h = h(K)$. Then for any power p^m of a prime $\neq l$, we find $r_{p^m}C(K) \equiv 0 \pmod{c(l,p)}$ by the "p^m-rank version" of Theorem 1. Thus

$$v_p(h) = \sum_{m=1}^{\infty} r_{p^m}C(K) \equiv 0 \pmod{c(l,p)},$$

which means $p^{v_p(h)} \equiv 1 \pmod{l}$. Hence $h \in \mathcal{H}(l)$. □

It seems to us that the converse inclusion is also true, and we would like to propose the following

CONJECTURE 1. $H(l) = \mathcal{H}(l)$.

Since $\mathcal{H}(2) = \mathbb{N}$, the conjecture for $l = 2$ says that there exists a quadratic field of which the class number is any given positive integer.

Put $H_x(l) = \{h \in H(l) \mid h \leq x\}$ and define $\mathcal{H}_x(l)$ similarly. We have carried out a computer search whether $H_x(l) = \mathcal{H}_x(l)$ or not for $l = 2, 3, 5$ and for several values of x. Using PARI/GP and KASH, we could confirm the following;

$$H_{5000}(2) = \mathcal{H}_{5000}(2), \quad H_{283}(3) = \mathcal{H}_{283}(3), \quad H_{81}(5) = \mathcal{H}_{81}(5).$$

We will illustrate them with some numerical results. First, we have made the complete list of the class numbers of quadratic fields $\mathbb{Q}(\sqrt{-m})$ with positive square-free integers m up to 10^7. Any positive integer $h \leq 5000$ appears in the list as a class number except $h = 4801$ and 4921. A little further search revealed $h(\mathbb{Q}(\sqrt{-10074671})) = 4801$ and $h(\mathbb{Q}(\sqrt{-10483871})) = 4921$. Next, to examine the case of the cyclic cubic fields, we have used the polynomial $F_m(X) = X^3 + mX^2 - (m+3)X + 1$ with $m \in \mathbb{Q}$ that parameterizes all the cyclic cubic extensions of $\mathbb{Q}$ (cf. [8]). The computer search showed that all integers $h \in \mathcal{H}_{350}(3) \setminus \{289, 337\}$ are covered with the class numbers of the cubic fields K_m defined by $F_m(X) = 0$ for irreducible fractions $m = s/r$ where $1 \leq r, s \leq 1000$. In Tables 1 and 2 we present K_m of class number h which has the least conductor $\mathfrak{f}$ in the running range of $m = s/r$. In quintic case, several types of parametric polynomials with cyclic Galois group of degree 5 appear in [1, Ch. 5], [4], [6] and others. We could use them to discover a cyclic quintic field of class number h for each $h \in \mathcal{H}(5)$ less than 200 with three exceptions. Table 3 shows irreducible polynomials $g(X)$ that define such fields and their conductors $\mathfrak{f}$.

https://doi.org/10.1017/S0027763000008072 Published online by Cambridge University Press

Table 1: Cyclic Cubic Fields

h	m	$\mathfrak{f}$	h	m	$\mathfrak{f}$
1	5/1	7	75	59/12	6901
3	3/2	63	76	163/1	27067
4	11/1	163	79	146/103	161911
7	16/1	313	81	73/8	7657
9	3/8	657	84	37/18	6283
12	31/16	679	91	205/1	42649
13	31/1	1063	93	116/1	13813
16	195/14	1777	97	77/122	168067
19	37/1	1489	100	136/1	18913
21	111/34	1261	103	139/6	22147
25	345/58	7753	108	126/1	16263
27	47/8	3913	109	89/10	11491
28	336/1	4219	111	114/1	13347
31	70/1	5119	112	142/1	20599
36	27/4	1197	117	156/1	8271
37	471/1	8269	121	239/1	57847
39	29/6	1687	124	284/1	81517
43	107/1	11779	127	121/1	15013
48	9/16	2817	129	407/351	17557
49	444/1	7351	133	200/1	40609
52	127/1	16519	139	322/1	104659
57	23/18	4687	144	127/153	21931
61	86/15	13291	147	31/34	14527
63	51/1	2763	148	277/1	77569
64	101/1	10513	151	283/157	435223
67	155/1	24499	156	149/1	22657
73	79/10	9511	157	28/167	265813

https://doi.org/10.1017/S0027763000008072 Published online by Cambridge University Press

Table 2: Cyclic Cubic Fields (continuation)

h	m	$\mathfrak{f}$	h	m	$\mathfrak{f}$
163	20/119	134989	256	427/237	991447
169	212/1	45589	259	364/1	133597
171	65/6	5719	268	472/1	224209
172	169/36	58477	271	869/582	5320951
175	254/1	65287	273	198/1	39807
181	446/139	558787	277	367/1	135799
183	196/1	39013	279	822/145	45277
189	119/8	17593	283	163/115	201829
192	311/121	48769	289	———	———
193	403/1	163627	291	58/299	122857
196	20/121	139429	292	359/1	129967
199	262/257	865087	300	171/1	29763
201	207/1	43479	301	70/99	113899
208	290/1	84979	304	406/1	166063
211	688/149	980689	307	295/337	1407391
217	259/1	67867	309	330/1	109899
219	211/1	45163	313	463/1	215767
223	206/1	43063	316	395/1	157219
225	233/1	54997	324	89/36	29197
228	59/6	4867	325	343/1	118687
229	304/1	93337	327	119/12	19741
237	44/215	63763	331	5/108	106621
241	136/167	337633	333	39/185	47313
243	81/94	15561	336	707/348	29467
244	332/1	111229	337	———	———
247	368/1	136537	343	266/1	71563
252	34/155	33313	349	131/12	23173

https://doi.org/10.1017/S0027763000008072 Published online by Cambridge University Press

Table 3: Cyclic Quintic Fields

h	$g(X)$	$\mathfrak{f}$
1	$X^5 + X^4 - 4X^3 - 3X^2 + 3X + 1$	11
5	$X^5 - 65X^4 - 6395X^3 + 7840X^2 - 1625X + 1$	275
11	$X^5 + 4X^4 - 70X^3 + 135X^2 + 54X + 1$	191
16	$X^5 + 16X^4 - 274X^3 + 817X^2 + 178X + 1$	941
25	$X^5 + 1640X^4 + 41950X^3 - 7043X^2 - 15122X + 1$	2651
31	$X^5 + X^4 - 4912X^3 - 32913X^2 + 4053123X + 17302471$	12281
41	$X^5 + X^4 - 4024X^3 - 73244X^2 + 1163776X + 5996224$	10061
55	$X^5 + 49X^4 + 452X^3 + 1125X^2 - 207X + 1$	1271
61	$X^5 + X^4 - 8560X^3 + 255100X^2 + 1951600X - 5058176$	21401
71	$X^5 + X^4 - 33388X^3 - 1459073X^2 + 31681585X + 1537601101$	83471
80	$X^5 + 25X^4 - 460X^3 + 1605X^2 + 285X + 1$	1775
81	$X^5 + 524X^4 - 558634X^3 + 87180396X^2 + 1430815089X - 443695552$	1671161
101	Not found.	———
121	$X^5 + X^4 - 5728X^3 + 7447X^2 + 7652455X - 3749609$	14321
125	$X^5 + X^4 - 5592X^3 + 32436X^2 + 5992704X - 2659392$	13981
131	Not found.	———
151	$X^5 + X^4 - 150036X^3 + 30802473X^2 - 2034901683X + 34977429477$	375091
155	$X^5 - 1755X^4 + 98729X^3 - 101785X^2 + 3278X + 1$	8651
176	$X^5 + X^4 - 5068X^3 + 158641X^2 - 847031X - 4729247$	12671
181	Not found.	———
191	$X^5 + X^4 - 8844X^3 - 72524X^2 + 5838896X - 42516736$	22111

https://doi.org/10.1017/S0027763000008072 Published online by Cambridge University Press

References

[1] H. Cohen, Advanced topics in computational number theory, Springer-Verlag, New York, 2000.
[2] G. Cornell, *Group theory and the class group*, Number theory and applications, NATO adv. Sci. Inst. Ser. C, **265** (1989), 347–352.
[3] G. Cornell and M. Rosen, *Group-theoretic constraints on the structure of the class group*, J. Number Theory, **13** (1981), 1–11.
[4] R. Dentzer,, *Polynomials with cyclic Galois group*, Comm. in Algebra, **23** (1995), 1593–1603.
[5] K. Iwasawa, *A note on ideal class groups*, Nagoya Math. J., **27** (1966), 239–247.
[6] E. Lehmer, *Connection between Gaussian period and cyclic units*, Math Comp., **50** (1988), 535–541.
[7] J. M. Masley, *Class numbers of real cyclic number fields with small conductor*, Compositio Math., **37** (1978), 297–319.
[8] J-P. Serre, Topics in Galois theory, Jones and Bartlett Publishers, Boston, 1992.
[9] L. C. Washington, *The non-p-part of the class number in a cyclotomic $\mathbb{Z}_p$-extension*, Invent. Math., **49** (1978), 87–97.
[10] L. C. Washington, Introduction to cyclotomic fields, 2nd edition, Springer-Verlag, New York, 1997.

Toru Komatsu
Department of Mathematics
Tokyo Metropolitan University
Hachioji, Tokyo 192-0397
Japan
trkomatu@comp.metro-u.ac.jp

Shin Nakano
Department of Mathematics
Gakushuin University
Toshima-ku, Tokyo 171-8588
Japan
shin@math.gakushuin.ac.jp