JOURNAL
de Théorie des Nombres
de BORDEAUX
anciennement Séminaire de Théorie des Nombres de Bordeaux

Yutaka KONOMI

On the p-rank of the ideal class group of a normal extension with simple Galois group

Tome 31, n° 3 (2019), p. 671-678.

<http://jtnb.centre-mersenne.org/item?id=JTNB_2019__31_3_671_0>

Journal de Théorie des Nombres de Bordeaux **31** (2019), 671–678

On the p-rank of the ideal class group of a normal extension with simple Galois group

par Yutaka KONOMI

Résumé. Soient p un nombre premier et L une extension normale finie d'un corps de nombres K dont le groupe de Galois est simple et non abélien. Le but de cet article est d'estimer la borne inférieure du quotient du p-rang du groupe de classes d'idéaux de L par le p-rang du groupe de p-classes ambiges de L par rapport à K.

Abstract. Let p be a prime and L a finite normal extension over a number field K whose Galois group is simple and non-abelian. The aim of this paper is to estimate a lower bound of the ratio of the p-rank of the ideal class group of L to the p-rank of the ambiguous p-class group of L with respect to K.

1. Introduction and the main result

Let p denote a prime number. For an algebraic number field K of finite degree, denote the p-part of the ideal class group of K by $\mathrm{Cl}_p(K)$ and put $h_p(K) = \#\,\mathrm{Cl}_p(K)$. When L/K is a finite Galois extension, we put

$$\mathrm{Amb}_p(L/K) = \{x \in \mathrm{Cl}_p(L) \mid \forall\, \sigma \in \mathrm{Gal}(L/K), x^\sigma = x\}$$

and

$$a_p(L/K) = \#\,\mathrm{Amb}_p(L/K).$$

These are called the ambiguous p-class group and the ambiguous p-class number of L with respect to K, respectively. It is known that

$$\mathrm{Amb}_p(L/K) \simeq \mathrm{Cl}_p(K)$$

if $p \nmid \#\,\mathrm{Gal}(L/K)$. For a finite additive group A, the finite field $\mathbb{F}_p$ with p-elements acts on A/pA. We call $\dim_{\mathbb{F}_p} A/pA$ the p-rank of A and denote it by $p\text{-rank}(A)$.

In the former paper, the author essentially showed the following theorem.

Theorem 1.1 ([2, Theorem 2])**.** *Assume $n \geq 5$ and $\mathrm{Gal}(L/K)$ is isomorphic to A_n, the alternating group of degree n. Let l_n be the maximal prime number satisfying $l_n \neq p$ and $l_n \leq \sqrt{n}$. If $h_p(L) > a_p(L/K)$, then we have*

$$p\text{-rank}\,(\mathrm{Cl}_p(L)/\,\mathrm{Amb}_p(L/K)) \geq l_n + 1.$$

Manuscrit reçu le 16 décembre 2018, révisé le 5 février 2019, accepté le 18 février 2019.
2010 *Mathematics Subject Classification.* 11R29, 20D06, 20D08.
Mots-clefs. Class group, simple group.

There is ample room for further improvement in Theorem 1.1. In response, the aim of this paper is to give explicit lower bounds of the p-rank of ambiguous ideal class groups on which the simple and non-abelian Galois group act.

We state the main results. Let $G = \mathrm{Gal}(L/K)$ be simple and non-abelian. Under these notations, we obtain as follows.

Theorem 1.2. *Let p denote a prime and set*

$$\lambda(p) = \max\{f_\ell(p) \mid \ell \text{ is a prime divisor of } \#G\}$$

where

$$f_\ell(p) = \begin{cases} \min\{i \in \mathbb{Z}_{>0} \mid p^i \equiv 1 \pmod{\ell}\}, & \text{if } p \neq \ell; \\ \dfrac{1 + \sqrt{1 + 8 \cdot \mathrm{ord}_p(\#G)}}{2}, & \text{if } p = \ell. \end{cases}$$

If $h_p(L) > a_p(L/K)$, we have

$$p\text{-rank}\,(\mathrm{Cl}_p(L)/\,\mathrm{Amb}_p(L/K)) \geq \lambda(p).$$

Theorem 1.3. *Fix ℓ a prime divisor of $\#G$. Let μ_ℓ be the maximal value of the dimensions of elementary abelian ℓ-subgroups of G over $\mathbb{F}_\ell$. For every prime p different from ℓ, if $h_p(L) > a_p(L/K)$, then we have*

$$p\text{-rank}\,(\mathrm{Cl}_p(L)/\,\mathrm{Amb}_p(L/K)) \geq \mu_\ell + 1.$$

Theorem 1.4. *Let ℓ be an odd prime divisor of $\#G$, ν_ℓ the ℓ-adic order of the maximal order of an abelian ℓ-subgroup of G. Assume $h_\ell(L) > a_\ell(L/K)$. Then we have*

$$\ell\text{-rank}\,(\mathrm{Cl}_\ell(L)/\,\mathrm{Amb}_\ell(L/K)) \geq 2\sqrt{\nu_\ell}$$

and

$$2\text{-rank}\,(\mathrm{Cl}_2(L)/\,\mathrm{Amb}_2(L/K)) \geq 2\sqrt{\mu_2}.$$

Remark 1.5 (see Section 3)**.** If one is able to factor $\#G$, it is easy to calculate $\lambda(p)$ for each p. In addition, we can also get μ_ℓ and ν_ℓ by using a computer. The value $\lambda(p)$ depends on p, while μ_ℓ does not. However, Theorem 1.2 yields much better numbers than Theorem 1.3 in some cases. When we write $l_{\max}$ for the maximal prime divisor of $\#G$, $\lambda(p)$ is less than or equal to $l_{\max}-1$. By Dirichlet's theorem on arithmetic progressions, there are infinitely many primes p such that $\lambda(p)$ is equal to not only $l_{\max} - 1$ but also 1.

Acknowledgments. The author would like to thank the referee for [2], who communicated to him the ideas of some proofs. He also thanks Yoshichika Iizuka who communicated the proof of Proposition 2.6. The author is grateful to Professor Shin Nakano for his unfailing encouragement. Last not least, the author would like to thank the referee of this paper for careful reading and many valuable suggestions which improved this paper.

2. Proofs of the main theorems

In this section, we give proofs of the main theorems. When G is a group and M a G-module, we put

$$M^G = \{x \in M \mid \forall\, g \in G, gx = x\}.$$

The following lemma is a key of the proofs of the main Theorems.

Lemma 2.1. *Let G be a finite non-abelian simple group, M a G-module whose order is a p-power. Assume $M \supsetneq M^G$ and set $r = p\text{-rank}(M/M^G)$. Then G embeds into $\mathrm{SL}_r(\mathbb{F}_p)$.*

Proof. We show $(M/M^G)^G$ is trivial. The short exact sequence

$$0 \longrightarrow M^G \longrightarrow M \longrightarrow M/M^G \longrightarrow 0$$

produces the exact cohomology sequence

$$0 \longrightarrow (M^G)^G = M^G \longrightarrow M^G \longrightarrow (M/M^G)^G \longrightarrow H^1(G, M^G).$$

We have $H^1(G, M^G) = \mathrm{Hom}(G, M^G)$ because G acts on trivially M^G. Since G is simple and non-abelian, $\mathrm{Ker}(\chi)$ is equal to G for any $\chi \in \mathrm{Hom}(G, M^G)$. Thus, $H^1(G, M^G)$ is trivial and we obtain $(M/M^G)^G = 0$ by this exact cohomology sequence.

We construct an injective group homomorphism $G \longrightarrow \mathrm{SL}_r(\mathbb{F}_p)$. Let $V = \{x \in M/M^G \mid px = 0\}$. Then, V has the following properties:

(i) The group ring $\mathbb{F}_p[G]$ acts on V,

(ii) Looking at the kernel and cokernel of the group homomorphism $M/M^G \to M/M^G, x \mapsto px$, we see that $\#V = \#(M/M^G)/p(M/M^G)$, that is, $\dim_{\mathbb{F}_p} V = r$,

(iii) $V \neq 0$ and $V^G = 0$.

From (i) and (ii), we get the natural group homomorphism

$$\rho : G \longrightarrow \mathrm{Aut}_{\mathbb{F}_p}(V) \simeq \mathrm{GL}_r(\mathbb{F}_p).$$

By the simplicity of G, $\mathrm{Ker}(\rho)$ is equal to 1_G or G. If $\mathrm{Ker}(\rho) = G$, then $V = V^G$. This is a contradiction to (iii). Thus, $\rho : G \longrightarrow \mathrm{GL}_r(\mathbb{F}_p)$ is injective.

Similarly, $\mathrm{Ker}(\det \circ \rho : G \longrightarrow \mathbb{F}_p^\times)$ is equal to 1_G or G. If $\mathrm{Ker}(\det \circ \rho) = 1_G$, then G is abelian. This is a contradiction and hence $\mathrm{Im}(\rho)$ is subset of $\mathrm{SL}_r(\mathbb{F}_p)$. □

We give two estimations of lower bounds of $r = p\text{-rank}(M/M^G)$ in order to prove Theorem 1.2.

Proposition 2.2. *Fix ℓ a prime divisor of $\#G$. Under the same notations and assumptions of Lemma 2.1, we have the following estimation of r:*

(1) *Let p denote a prime different from ℓ and f the order of p in $(\mathbb{Z}/\ell\mathbb{Z})^\times$. Then r is greater than or equal to f.*

(2) *If $p = \ell$, then r is greater than or equal to* $\frac{1+\sqrt{1+8\cdot \mathrm{ord}_p(\#G)}}{2}$.

Proof. Note that

$$\#\,\mathrm{SL}_r(\mathbb{F}_p) = p^{\frac{r(r-1)}{2}} \prod_{k=2}^{r} (p^k - 1)$$

and $\#G$ divides $\#\,\mathrm{SL}_r(\mathbb{F}_p)$ by Lemma 2.1.

(1) There exists i such that $1 \leq i \leq r$ and $p^i \equiv 1 \pmod{\ell}$ from the assumptions. Hence, we obtain $r \geq f$.
(2) This is because $\mathrm{ord}_p(\#G) \leq \mathrm{ord}_p(\#\,\mathrm{SL}_r(\mathbb{F}_p)) = \frac{r(r-1)}{2}$.

□

By applying Proposition 2.2 to $\mathrm{Cl}_p(L)/\,\mathrm{Amb}_p(L/K)$, on which a simple and non-abelian Galois group acts, we can prove Theorem 1.2.

We calculate another lower bound of r in order to prove Theorem 1.3.

Proposition 2.3. *Fix ℓ a prime divisor of $\#G$. Under the same notations and assumptions of Lemma 2.1, let $\mathcal{B}_\ell$ denote an elementary abelian ℓ-subgroup of G. Then r is greater than or equal to* $\dim_{\mathbb{F}_\ell} \mathcal{B}_\ell + 1$ *for every prime p different from ℓ.*

Proof. Let W_ℓ denote the group of ℓ-th roots of unity over $\mathbb{F}_p$. There exists q such that q is p-power and $W_\ell \subset \mathbb{F}_q$. If $A \in \mathcal{B}_\ell$, then the eigenvalues of A are elements in W_ℓ because $A^\ell = (\delta_{ij})_{1\leq i,j\leq r}$. Here, δ_{ij} is the Kronecker delta. We can regard $\mathcal{B}_\ell$ as an elementary abelian ℓ-subgroup of $\mathrm{SL}_r(\mathbb{F}_q)$ by Lemma 2.1 and noting that $\mathbb{F}_p \subset \mathbb{F}_q$. Then $\mathcal{B}_\ell$ has the following two properties:

(i) For all $X, Y \in \mathcal{B}_\ell$, $XY = YX$.
(ii) Since p is different from ℓ, there exist $\alpha_1, \ldots, \alpha_r \in W_\ell$ and $P \in \mathrm{SL}_r(\mathbb{F}_q)$ such that

$$P^{-1}AP = (\alpha_i \delta_{ij})_{1\leq i,j\leq r}.$$

Consequently, all elements of $\mathcal{B}_\ell$ can be diagonalized simultaneously. When we write $\mathrm{Diag}(W_\ell)$ by the group of diagonal matrices whose diagonal elements are included in W_ℓ, $\mathcal{B}_\ell$ is conjugate to a subgroup of $\mathrm{SL}_r(\mathbb{F}_p) \cap \mathrm{Diag}(W_\ell)$. Hence, $\dim_{\mathbb{F}_\ell} \mathcal{B}_\ell \leq r - 1$ holds. □

Applying Proposition 2.3 to $\mathrm{Cl}_p(L)/\,\mathrm{Amb}_p(L/K)$ with the simple and non-abelian Galois group action, we are able to show Theorem 1.3.

We mention a corollary of Theorem 1.3.

Corollary 2.4. *Suppose $p \neq 2$, $n \geq 5$ and* $\mathrm{Gal}(L/K) \simeq A_n$. *If $h_p(L) > a_p(L/K)$, then*

$$p\text{-rank}\,(\mathrm{Cl}_p(L)/\,\mathrm{Amb}_p(L/K)) \geq 2\left\lfloor \frac{n}{4} \right\rfloor + 1$$

holds. Here, $\lfloor \cdot \rfloor$ *means the floor function.*

Proof. Put $T_k = \{(1), (4k-3\ 4k-2)(4k-1\ 4k), (4k-3\ 4k-1)(4k-2\ 4k), (4k-3\ 4k)(4k-2\ 4k-1)\}$ for a positive integer k. Then $\bigoplus_{i=1}^{k} T_k$ is an elementary 2-subgroup of the alternating group A_{4k}. Hence, μ_2 is at least $2\lfloor \frac{n}{4} \rfloor$. The claim of this corollary follows from Theorem 1.3. □

Remark 2.5. The above corollary is pointed out by the referee for [2] in the form that

$$h_p(L)/a_p(L/K) \geq p^{2\lfloor \frac{n}{4} \rfloor + 1}$$

if $h_p(L) > a_p(L/K)$.

To show Theorem 1.4, we give further evaluation of r when p divides $\#G$.

Proposition 2.6. *Under the same notations and assumptions of Lemma 2.1, let* ℓ *denote a prime divisor of* $\#G$.

(1) *The value of* r *is greater than or equal to* $2\sqrt{\mu_\ell}$.
(2) *If* ℓ *is an odd,* r *is greater than or equal to* $2\sqrt{\nu_\ell}$.

Proof. (1). Due to Lemma 2.1, an elementary abelian ℓ-subgroup of G is embedded in an elementary abelian ℓ-subgroup of $\mathrm{SL}_r(\mathbb{F}_\ell)$. By the Theorem in [3] and the Sylow theorems, the maximal p-rank of an elementary abelian p-subgroup of $\mathrm{SL}_r(\mathbb{F}_p)$ is equal to $\lfloor \frac{r^2}{4} \rfloor$ for all primes p. Consequently, we have $\mu_\ell \leq \frac{r^2}{4}$.

(2). An abelian ℓ-subgroup of G is embedded in an abelian ℓ-subgroup of $\mathrm{SL}_r(\mathbb{F}_\ell)$ owing to Lemma 2.1. It is known that the unitriangular matrix group of degree r over $\mathbb{F}_p$ is a Sylow p-subgroup of $\mathrm{GL}_r(\mathbb{F}_p)$ for all primes p. By the Theorem in [1] and the Sylow theorems, the maximal order of an abelian p-subgroup of $\mathrm{SL}_r(\mathbb{F}_p)$ is equal to $p^{\lfloor \frac{r^2}{4} \rfloor}$ for all odd primes p. If ℓ is odd, then we have $\nu_\ell \leq \frac{r^2}{4}$. □

Applying Proposition 2.6 to $\mathrm{Cl}_\ell(L)/\mathrm{Amb}_\ell(L/K)$, we are able to obtain Theorem 1.4.

3. Examples and tables

In this section, we compute explicit values of $\lambda(p)$ and μ_ℓ for some concrete simple groups. To begin with, we confirm that Theorem 1.2 and Theorem 1.3 are better than Theorem 1.1 for A_n-extensions.

Example 3.1. With regard to the alternating group A_{100}, we get $l_{100} = 7$ and $\mu_2 = 50$ by Theorem 1.1 and Corollary 2.4, respectively. Certainly, Theorem 1.3 is better than Theorem 1.1. We have $\lambda(2) = 82$, $\lambda(3) = 88$,

$\lambda(5) = \lambda(7) = 96$, $\lambda(11) = 72$, $\lambda(101) = 82$ and $\lambda(p) \leq 96$ for any prime p. There are 1229 primes less than 10^4, and such primes p satisfy that

$$\lambda(p) \leq \mu_2 + 1 = 51$$

if and only if

$$p = 997, 1613, 4021, 4547, 9337, 9781.$$

Then, $\lambda(997) = \lambda(1613) = \lambda(4547) = \lambda(9781) = 46$ and $\lambda(4021) = \lambda(9337) = 48$ hold. In this case, Theorem 1.2 may be superior to Theorem 1.3.

The classification of finite simple groups is known, that is, every finite simple group is cyclic, or alternating, or in one of 16 families of groups of Lie type, or one of 26 sporadic groups. We pick two groups of Lie type, $A_2(29)$ and $C_3(2)$, in order to compare the three Theorems.

Example 3.2. We get

$$\#A_2(29) = \frac{29^3}{\gcd(3, 28)} \prod_{i=1}^{2} (29^{i+1} - 1) = 2^5 \cdot 3 \cdot 5 \cdot 7^2 \cdot 13 \cdot 29^3 \cdot 67$$

and $\mu_2 = \mu_7 = \mu_{29} = \nu_7 = \nu_{29} = 2$ by using Magma. We see that $\lambda(2) \geq 2\sqrt{\mu_2}$ and $\lambda(\ell) \geq 2\sqrt{\nu_\ell}$ for ℓ any odd prime divisor of $\#G$ by $\lambda(2) = \lambda(7) = \lambda(13) = 66$, $\lambda(3) = \lambda(5) = 22$, $\lambda(67) = 14$ and $\lambda(29) = 3$. Hence Theorem 1.2 is superior to Theorem 1.4. Only four primes $p = 252589$, 304849, 448631, 511211 satisfy that $\lambda(p) < 3$ in 78498 primes less than 10^6. In this case, Theorem 1.2 is much better than Theorem 1.3 for almost all primes p.

Example 3.3. We get

$$\#C_3(2) = 2^{3^2} \prod_{i=1}^{3} (2^{2i} - 1) = 2^9 \cdot 3^4 \cdot 5 \cdot 7,$$

$\mu_2 = 6$, and $\mu_3 = \nu_3 = 3$ by using Magma. If p is odd, then Theorem 1.3 is completely superior to Theorem 1.2 because $\lambda(p) \leq 6 < \mu_2 + 1 = 7$ for all odd primes p. If ℓ is even, Theorem 1.2 is as good as Theorem 1.4, as $\lambda(2) = \frac{1+\sqrt{73}}{2}$.

For the Lie type groups $D_4(2^2)$, $F_4(2^4)$, $E_6(3)$ and Fischer–Griess group F_1, we may not get μ_ℓ and ν_ℓ even by using a computer. However, we can

calculate $\lambda(p)$ because these orders are factored into

$$\begin{aligned}
\#D_4(2^2) &= 4^{12}(4^4-1)\prod_{i=1}^{3}(4^{2i}-1) = 2^{24}\cdot 3^5\cdot 5^4\cdot 7\cdot 13\cdot 17^2,\\
\#F_4(2^4) &= 16^{24}\prod_{i\in\{2,6,8,12\}}(16^i-1)\\
&= 2^{96}\cdot 3^6\cdot 5^4\cdot 7^2\cdot 13^2\cdot 17^4\cdot 97\cdot 241^2\cdot 257^2\cdot 673\cdot 65537,\\
\#E_6(3) &= 3^{36}\prod_{i\in\{2,5,6,8,9,12\}}(3^i-1) = 2^{17}\cdot 3^{36}\cdot 5^2\cdot 7^2\cdot 11^2\cdot 13^3\cdot 41\cdot 73\cdot 757,\\
\#F_1 &= 2^{46}\cdot 3^{20}\cdot 5^9\cdot 7^6\cdot 11^2\cdot 13^3\cdot 17\cdot 19\cdot 23\cdot 29\cdot 31\cdot 41\cdot 47\cdot 59\cdot 71.
\end{aligned}$$

For example, we get $(\lambda(2),\lambda(3))=(12,16),(48,65536),(756,12)$ and $(58,35)$ respectively with regard to these four groups.

Lastly, we list the results of calculations using Magma for some other finite simple groups.

TABLE 3.1. some Lie Type groups

Group	the order	$\lambda(2)$	$\lambda(3)$	μ_2	μ_3	ν_3
$A_1(2^3)$	$2^3\cdot 3^2\cdot 7$	3	6	3	1	2
$A_1(2^7)$	$2^7\cdot 3\cdot 43\cdot 127$	14	126	7	1	1
$A_2(3^3)$	$2^4\cdot 3^9\cdot 7\cdot 13^2\cdot 757$	756	9	2	6	6
$A_3(2^2)$	$2^{12}\cdot 3^4\cdot 5^2\cdot 7\cdot 17$	8	16	8	3	3
$A_4(3)$	$2^9\cdot 3^{10}\cdot 5\cdot 11^2\cdot 13$	12	5	4	6	6
$B_2(2^4)$	$2^{16}\cdot 3^2\cdot 5^2\cdot 17^2\cdot 257$	16	256	12	2	2
$C_3(2^2)$	$2^{18}\cdot 3^4\cdot 5^3\cdot 7\cdot 13\cdot 17$	12	16	12	3	3
$G_2(3)$	$2^6\cdot 3^6\cdot 7\cdot 13$	12	6	3	4	4
$G_2(2^2)$	$2^{12}\cdot 3^3\cdot 5^2\cdot 7\cdot 13$	12	6	6	2	2

TABLE 3.2. some sporadic groups

Group	the order	$\lambda(2)$	$\lambda(3)$	μ_2	μ_3	ν_3
M_{12}	$2^6\cdot 3^3\cdot 5\cdot 11$	10	6	3	2	2
J_2	$2^7\cdot 3^3\cdot 5^2\cdot 7$	$(1+\sqrt{57})/2$	6	4	2	2
Co_3	$2^{10}\cdot 3^7\cdot 5^3\cdot 7\cdot 11\cdot 23$	11	11	4	5	5
McL	$2^7\cdot 3^6\cdot 5^3\cdot 7\cdot 11$	10	6	4	4	4
He	$2^{10}\cdot 3^3\cdot 5^2\cdot 7^3\cdot 17$	8	16	6	2	2
Suz	$2^{13}\cdot 3^7\cdot 5^2\cdot 7\cdot 11\cdot 13$	12	6	6	5	5

References

[1] J. T. GOOZEFF, "Abelian p-subgroups of the general linear group", *J. Aust. Math. Soc.* **11** (1970), p. 257-259.

[2] Y. KONOMI, "On p-class group of an A_n-extension", *Proc. Japan Acad.* **84** (2008), no. 7, p. 87-88.

[3] G. N. THWAITES, "The Abelian p-subgroups of $\mathrm{GL}(n,p)$ of maximal rank", *Bull. Lond. Math. Soc.* **4** (1972), p. 313-320.

Yutaka KONOMI
Department of Mathematics
Meijo University
Tempaku-ku, Nagoya 468-8502, Japan
E-mail: konomi@meijo-u.ac.jp