On p-class group of an A_n-extension

By Yutaka KONOMI

Department of Mathematics, Gakushuin University, 1-5-1, Mejiro, Toshima-ku, Tokyo 171-8588, Japan

(Communicated by Shigefumi MORI, M.J.A., June 10, 2008)

Abstract: Let p be a prime and L an A_n-extension over a number field K. The aim of this paper is to estimate the ratio of the p-class number of L to the ambiguous p-class number of L with respect to K.

Key words: Ideal class group; ambiguous class group; A_n-extension.

Let p denote a fixed prime number throughout this paper. For an algebraic number field of finite degree K, denote the p-Sylow subgroup of the ideal class group of K by $\mathrm{Cl}_K\{p\}$. Put $h_K\{p\} = \sharp\mathrm{Cl}_K\{p\}$. Consider a finite Galois extension L/K. We put

$$\mathrm{Amb}_{L/K} := \{x \in \mathrm{Cl}_L\{p\} \mid \forall\sigma \in \mathrm{Gal}(L/K) : x^\sigma = x\}$$

and

$$a_{L/K} := \sharp\mathrm{Amb}_{L/K}.$$

They are called the ambiguous p-class group and the ambiguous p-class number of L with respect to K, respectively.

In [1], Ohta obtained the following

Theorem 1 (Ohta [1], see Theorem 5). *Assume p is odd and $\mathrm{Gal}(L/K)$ is isomorphic to S_n, the symmetric group of degree n for some $n \geq 5$. Let M denote the unique intermediate field of L/K so that $[M : K] = 2$. If $h_L\{p\} > a_{L/M}$ then $h_L\{p\}/a_{L/K}$ is divisible by p^3.*

The main result of this paper is the following theorem, which is similar to the above. We consider an A_n-extension instead of S_n.

Theorem 2. *Let L be a finite Galois extension over K an algebraic number field of finite degree. Assume $n \geq 5$ and $\mathrm{Gal}(L/K)$ is isomorphic to A_n, the alternating group of degree n. Let l be the maximal prime number satisfying $l \neq p$ and $l \leq \sqrt{n}$. If $h_L\{p\} > a_{L/K}$ then $h_L\{p\}/a_{L/K}$ is divisible by p^{l+1}.*

Note that this Theorem implies Theorem 1 since $l \geq 2$ and $a_{L/M} \geq a_{L/K}$.

Using this Theorem, we have the following corollary.

Corollary 3. *Suppose $5 \leq n < p$. Let L be a Galois extension of K such that $\mathrm{Gal}(L/K) \simeq A_n$. Let l be the maximal prime number satisfying $l \leq \sqrt{n}$.*

(1) *If $h_L\{p\} > h_K\{p\}$, then $h_L\{p\}$ is divisible by $p^{l+1}h_K\{p\}$.*

(2) *If $h_L\{p\} > h_K\{p\}$, then*

$$\sharp\mathrm{Ker}(N_{L/K} : \mathrm{Cl}_L\{p\} \to \mathrm{Cl}_K\{p\})$$

is divisible by p^{l+1}.

Proof. (1) Since $\mathrm{Gal}(L/K) \simeq A_n$, we can apply Theorem 2 to L/K. Granting Proposition 4 below, we have the conclusion.

(2) The norm map $N_{L/K} : \mathrm{Cl}_L\{p\} \to \mathrm{Cl}_K\{p\}$ is surjective since $n < p$. We obtain the following relation

$$\sharp\mathrm{Ker}(N_{L/K} : \mathrm{Cl}_L\{p\} \to \mathrm{Cl}_K\{p\}) = h_L\{p\}/h_K\{p\}.$$

It follows from (1) that $\sharp\mathrm{Ker}(N_{L/K} : \mathrm{Cl}_L\{p\} \to \mathrm{Cl}_K\{p\})$ is divisible by p^{l+1}. □

In the above proof, we used the following fact.

Proposition 4 (Cornel & Rosen [2], Lemma 3). *Let L be a Galois extension over K and M an intermediate field of L/K. If $[L : M]$ is not divisible by p, then $\mathrm{Cl}_M\{p\} \simeq \mathrm{Amb}_{L/M}$.*

We devote the rest of this paper to the proof of Theorem 2. We need the following fact.

Theorem 5 (Ohta [1], Theorem 2). *Assume l is a prime and $p \neq l$. Let L be a Galois extension over K whose Galois group is the abelian group of type (l, l). Let $M_0, M_1, \cdots M_l$ be the $l + 1$ distinct intermediate fields of L/K with $[M_i : K] = l$. If $h_L\{p\} > 1$ then $\mathrm{Cl}_L\{p\}/\mathrm{Amb}_{L/K}$ is decomposed into the direct sum as following*

$$\mathrm{Cl}_L\{p\}/\mathrm{Amb}_{L/K} \simeq \bigoplus_{i=0}^{l} \mathrm{Amb}_{L/M_i}/\mathrm{Amb}_{L/K}.$$

2000 Mathematics Subject Classification. Primary 11R29, 11R32; Secondary 11R21.

For distinct elements of $a_1, a_2, \cdots, a_t$ in $\{1, 2, \cdots, n\}$, we denote by $(a_1\ a_2 \cdots a_t)$ the cyclic permutation in S_n which sends a_i to a_{i+1} for $1 \leq i \leq t-1$ and a_t to a_1, as usual.

Lemma 6. *Let l be a prime with $l \leq \sqrt{n}$. Consider the elements in A_n,*

$$\sigma := (1\ 2 \cdots l)(l+1\ l+2 \cdots 2l) \cdots (l^2-l+1\ l^2-l+2 \cdots l^2)$$

and

$$\tau := (1\ l+1\ 2l+1 \cdots l^2-l+1)(2\ l+2 \cdots l^2-l+2) \cdots (l\ 2l\ \cdots l^2).$$

Then, $l+1$ elements $\sigma, \sigma\tau, \sigma^2\tau, \cdots, \sigma^{l-1}\tau, \tau$ are conjugate each other in A_n. And so, $\langle\sigma, \tau\rangle \simeq \mathbf{Z}/l\mathbf{Z} \oplus \mathbf{Z}/l\mathbf{Z}$.

Proof. It is easy to see $\langle\sigma, \tau\rangle \simeq \mathbf{Z}/l\mathbf{Z} \oplus \mathbf{Z}/l\mathbf{Z}$. If $l = 2$, then we have $\sigma = (1\ 4\ 2)\tau(1\ 2\ 4) = (1\ 3\ 2)\sigma\tau(1\ 2\ 3)$. We consider the case $l \neq 2$. Fix $i \in \{1, \cdots, l\}$ and put $\varphi := \sigma^i\tau$. Then,

$$\varphi = (1\ \varphi(1)\ \varphi^2(1) \cdots \varphi^{l-1}(1))(2\ \varphi(2) \cdots \varphi^{l-1}(2)) \cdots (l\ \varphi(l) \cdots \varphi^{l-1}(l)).$$

Therefore, $\sigma, \sigma\tau, \sigma^2\tau, \cdots, \sigma^{l-1}\tau, \tau$ are conjugate each other in S_n because they consist of the same number of disjoint cycles of the same length. We show σ and $\sigma^i\tau$ are conjugate in A_n. There exists $\rho \in S_n$ such that $\sigma^i\tau = \rho\sigma\rho^{-1}$. If $\rho \in S_n \setminus A_n$, put

$$\xi := (1\ \varphi(1))(2\ \varphi(2)) \cdots (l\ \varphi(l)).$$

We have $\rho\xi \in A_n$ and $\sigma^i\tau = (\rho\xi)\sigma(\rho\xi)^{-1}$ because $\sigma\xi = \xi\sigma$. Therefore, $\sigma, \sigma\tau, \sigma^2\tau, \cdots, \sigma^{l-1}, \tau$ are conjugate each other in A_n. □

Now we give a proof of Theorem 2. Let σ and τ be the permutations appeared in Lemma 6. We regard them the elements in $\mathrm{Gal}(L/K)$. Let F be the fixed field of $\langle\sigma, \tau\rangle$ in L. Let $M_0, \cdots, M_l$ be the fixed fields of the subgroups $\langle\sigma\rangle, \langle\sigma^1\tau\rangle, \cdots, \langle\sigma^{l-1}\tau\rangle, \langle\tau\rangle$ of $\langle\sigma, \tau\rangle$ in L, respectively. Then L/F is a Galois extension whose Galois group is the abelian group of type (l, l). Applying Theorem 5 to L/F, we obtain the following decomposition:

$$\bigoplus_{i=0}^{l} \mathrm{Amb}_{L/M_i}/\mathrm{Amb}_{L/F} \simeq \mathrm{Cl}_L\{p\}/\mathrm{Amb}_{L/F},$$

which yields

$$\prod_{i=0}^{l} \frac{a_{L/M_i}}{a_{L/F}} = \frac{h_L\{p\}}{a_{L/F}}.$$

As $M_0, \cdots, M_l$ are conjugate over K by Lemma 6, we have $a_{L/M_0} = \cdots = a_{L/M_l}$. Hence

$$\left(\frac{a_{L/M_0}}{a_{L/F}}\right)^{l+1} = \frac{h_L\{p\}}{a_{L/F}}.$$

Since $h_L\{p\}/a_{L/K}$ is divisible by $h_L\{p\}/a_{L/F}$, it suffices to show that $h_L\{p\} > a_{L/F}$ under the assumption $h_L\{p\} > a_{L/K}$, to complete the proof. Now assume that $h_L\{p\} = a_{L/F}$. Then we have $\mathrm{Amb}_{L/F} = \mathrm{Cl}_L\{p\}$. Moreover, $\mathrm{Amb}_{L/F'} = \mathrm{Cl}_L\{p\}$ for any conjugate field F' of F over K. We note that the intersection of all conjugates of F over K coincides with K, because it is Galois over K and $\mathrm{Gal}(L/K) \simeq A_n$ that is simple for $n \geq 5$.

Therefore we obtain

$$\mathrm{Amb}_{L/K} = \bigcap \mathrm{Amb}_{L/F'} = \mathrm{Cl}_L\{p\},$$

where F' runs over all conjugates of F/K. This completes the proof.

Acknowledgments. The author is most grateful to Prof. Shin Nakano and Prof. Yoshitaka Hachimori who gave him continuous encouragement and valuable advice. He would like to thank Prof. Kazuo Matsuno for kindly giving me valuable advice and information. He thanks Mr. Yoshichika Iizuka for various discussions on Number Theory and calculations of groups. He is grateful to the referee for some valuable suggestion.

References

[1] K. Ohta, On the p-group of a Galois number field and its subfields, J. Math. Soc. Japan **30** (1978), no. 4, 763–770.

[2] G. Cornell and M. Rosen, Group-theoretic constrains on the structure of the class groups, J. Number Theory **13** (1981), no. 1, 1–11.