J. Math. Soc. Japan
Vol. 39, No. 4, 1987

A note on l-parts of ray class groups

By Teruo TAKEUCHI

(Received Feb. 19, 1986)

1. Notation and the result.

Let l be an odd prime number and let k be an algebraic number field of finite degree. For an integer $i>0$, let ζ_i denote a primitive l^i-th root of unity and put $k_i=k(\zeta_i)$. For an ideal $\mathfrak{a}$ of k, let $k(\mathfrak{a})$ denote the group of elements of k prime to $\mathfrak{a}$ and let $k_{\mathfrak{a}}$ denote the ray number group of k modulo $\mathfrak{a}$, i.e., $k_{\mathfrak{a}}=\{x\in k(\mathfrak{a}) \mid x\equiv 1 \bmod \mathfrak{a}\}$. Further, let $I(\mathfrak{a})$ (resp. $P(\mathfrak{a})$) denote the group of ideals (resp. principal ideals) of k prime to $\mathfrak{a}$, and $P_{\mathfrak{a}}$ the ray ideal group of k modulo $\mathfrak{a}$, i.e., $P_{\mathfrak{a}}=\{(x) \mid x\in k_{\mathfrak{a}}\}$. Moreover let $P'_{\mathfrak{a}}$ (resp. $k'_{\mathfrak{a}}$) denote the group of elements of $P(\mathfrak{a})$ (resp. $k(\mathfrak{a})$) whose order modulo $P_{\mathfrak{a}}$ (resp. $k_{\mathfrak{a}}$) is prime to l. The purpose of this note is to prove the following.

THEOREM. *Assume $\zeta_1\notin k$ and $k_1\neq k_2$. Let*

$$1 \longrightarrow N \longrightarrow M \xrightarrow{g} I/P \longrightarrow 1$$

be an abelian extension of the ideal class group I/P of k by a finite abelian l-group N. Then there exist infinitely many ideals S of k which satisfy the following: there is an isomorphism $\Phi: I(S)/P'_S\to M$ such that Φ induces an isomorphism $\Phi: P(S)/P'_S\to N$ and the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & P(S)/P'_S & \longrightarrow & I(S)/P'_S & \longrightarrow & I/P & \longrightarrow & 1 \\ & & \downarrow \wr\!\!| & & \downarrow \wr\!\!| & & \| & & \\ 1 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & I/P & \longrightarrow & 1 \end{array}$$

commutes.

2. Proof of the theorem.

Let $(a_i)_{i=1,\dots,s}$ and $(b_j)_{j=1,\dots,r}$ be bases of M and N, respectively. Choose distinct prime ideals $\mathfrak{a}_1, \cdots, \mathfrak{a}_s$ prime to l which represent $g(a_1), \cdots, g(a_s)$, respectively (if $g(a_i)=1$, then choose an arbitrary principal prime ideal $\mathfrak{a}_i$). Put $A=$

This research was partially supported by Grant-in-Aid for Scientific Research (No. 61540022), Ministry of Education, Science and Culture.

$\langle \mathfrak{a}_1, \cdots, \mathfrak{a}_s \rangle$ (the ideal group generated by $\mathfrak{a}_1, \cdots, \mathfrak{a}_s$). Since A is free, we can define an epimorphism $f: A \to M$ by setting $f(\mathfrak{a}_i) = a_i$. Then f induces an epimorphism $f: A \cap P \to N$. Indeed, if $\mathfrak{b} = \prod_i \mathfrak{a}_i^{e_i} \in A \cap P$, then $g(f(\mathfrak{b})) = g(\prod_i a_i^{e_i}) = (\prod_i \mathfrak{a}_i^{e_i} \bmod P) = 1$, hence we see $f(\mathfrak{b}) \in N$. Conversely, if $b = \prod_i a_i^{e_i} \in N$, then $1 = g(b) = g(\prod_i a_i^{e_i}) = (\prod_i \mathfrak{a}_i^{e_i} \bmod P)$, and so $\prod_i \mathfrak{a}_i^{e_i} \in P$. Thus for $\mathfrak{b} = \prod_i \mathfrak{a}_i^{e_i} \in A \cap P$ we have $f(\mathfrak{b}) = b$. Therefore, since $\ker(f) \subset A \cap P$, we have a commutative diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & A\cap P/\ker(f) & \longrightarrow & A/\ker(f) & \longrightarrow & A/A\cap P & \longrightarrow & 1 \\ & & \downarrow \wr\!\!\!| & & \downarrow \wr\!\!\!| & & \downarrow \wr\!\!\!| & & \\ 1 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & I/P & \longrightarrow & 1, \end{array}$$

where $A/A \cap P \to I/P$ is the natural injection.

Let $F = \{x \in k \mid (x) \in A \cap P\}$, then F is finitely generated and F/E_k is free since $A \cap P$ is a finitely generated free abelian group, where E_k denotes the group of units of k. Hence there exists a direct decomposition $F = E_k \oplus D$ such that $D \cong \boldsymbol{Z}^m$ for some positive integer m. Let $\varphi: F \to A \cap P/\ker(f)$ be the epimorphism defined by $\varphi(x) = [(x) \bmod \ker(f)]$. Let $N_j = l^{n_j}$ be the order of b_j for $j = 1, \cdots, r$. Put $N_0 = \max N_j$. Since $f \circ \varphi: F \to N$ is an epimorphism and $E_k \subset \ker(f \circ \varphi)$, we can choose elements β_j $(j = 1, \cdots, r)$ of D with $f(\varphi(\beta_j)) = b_j$. Let $F_0 = \langle \beta_1, \cdots, \beta_r \rangle$, then $D \subset F_0 \cdot \ker(f \circ \varphi)$ since $f(\varphi(D)) = f(\varphi(F_0)) = N$. Moreover, since $\{f(\varphi(\beta_j))\}_{j=1,\dots,r}$ is a basis of N and $D/D^{N_0} \cong (\boldsymbol{Z}/N_0\boldsymbol{Z})^m$, we have a direct decomposition $D/D^{N_0} = (F_0 \cdot D^{N_0}/D^{N_0}) \oplus (F'' \cdot D^{N_0}/D^{N_0})$ with $F'' \subset \ker(f \circ \varphi)$. Put $F' = F'' \cdot E_k \cdot F^{N_0}$, $\bar{F}' = F'/F^{N_0}$, and $\langle \bar{\beta}_j \rangle = \langle \beta_j \rangle F^{N_0}/F^{N_0}$. Then $F/F^{N_0} = \langle \bar{\beta}_1 \rangle \oplus \langle \bar{\beta}_2 \rangle \oplus \cdots \oplus \langle \bar{\beta}_r \rangle \oplus \bar{F}'$ with $f \circ \varphi(F') = 1$. Furthermore, put $F_j = \langle \beta_1, \cdots, \beta_{j-1}, \beta_{j+1}, \cdots, \beta_r \rangle \cdot F'$ for $j = 1, \cdots, r$.

Now, by assumption, we can choose prime ideals $\mathfrak{p}_1, \cdots, \mathfrak{p}_r$ of k which satisfy the following conditions: For $j = 1, \cdots, r$, it holds that (i) $\mathfrak{p}_j$ is prime to l and $\mathfrak{a}_1, \cdots, \mathfrak{a}_s$; (ii) the decomposition field of a prime divisor of $\mathfrak{p}_j$ in $k_{n_j}(\sqrt[N_j]{F})/k$ is $k_{n_j}(\sqrt[N_j]{F_j})$; (iii) a prime divisor of $\mathfrak{p}_j$ in k_{n_j} inerts in k_{n_j+1}. To see this, we first note $k_1 \neq k_2$ implies $k_i \neq k_{i+1}$ for $i = 1, 2, \cdots$. Moreover we see that $l > 2$ implies $F^{N_j} = F \cap k_{n_j}^{\times N_j}$. Indeed, if $x = \gamma^{N_j} \in F$ for $\gamma \in k_{n_j}$, then by [1, Satz 1] there exists an element c of k such that $x = c^{N_j}$. On the other hand, since $x \in F$, we can write $(x) = (c)^{N_j} = \prod_i \mathfrak{a}_i^{e_i}$. Here we note that $\mathfrak{a}_i$ are distinct prime ideals of k, so that we have $N_j | e_i$ and $(c) = \prod_i \mathfrak{a}_i^{e_i/N_j} \in A$. Thus we obtain $c \in F$ and $x = c^{N_j} \in F^{N_j}$. Hence we have a natural isomorphism $F/F^{N_j} = F/(F \cap k_{n_j}^{\times N_j}) \cong F \cdot k_{n_j}^{\times N_j}/k_{n_j}^{\times N_j}$, and so $\mathrm{Gal}(k_{n_j}(\sqrt[N_j]{F})/k_{n_j})$ is isomorphic to the dual of F/F^{N_j}. Furthermore $k_{n_j}(\sqrt[N_j]{F})$ and k_{n_j+1} are linearly disjoint over k_{n_j}. In fact, if $k_{n_j+1} \subset k_{n_j}(\sqrt[N_j]{F})$, then we can choose an element x of F such that $k_{n_j+1} = k_{n_j}(\sqrt[l]{x})$. Since k_{n_j+1}/k is an abelian extension, it follows that $k(\sqrt[l]{x})/k$ is a cyclic extension of degree l; in particular, $k(\sqrt[l]{x})$ contains ζ_1. On the other hand,

$[k(\zeta_1):k]$ divides $l-1$, and hence from $[k(\sqrt[l]{x}):k]=l$ we see that $\zeta_1\in k$, which contradicts the assumption. This proves that $k_{n_j}(\sqrt[N_j]{F})$ and k_{n_j+1} are linearly disjoint over k_{n_j}. Therefore we can take elements σ and τ of $\mathrm{Gal}(k_{n_j+1}(\sqrt[N_j]{F})/k_{n_j})$ such that $\langle\sigma\rangle=\mathrm{Gal}(k_{n_j+1}(\sqrt[N_j]{F})/k_{n_j+1}(\sqrt[N_j]{F_j}))$ and $\langle\tau\rangle=\mathrm{Gal}(k_{n_j+1}(\sqrt[N_j]{F})/k_{n_j}(\sqrt[N_j]{F}))$. Put $\rho=\sigma\tau$ and let K be the fixed field of $\langle\rho\rangle$. Then $k_{n_j+1}(\sqrt[N_j]{F})/K$ is cyclic of degree N_j. Hence by the Čebotarev density theorem we can choose a prime ideal $\mathfrak{P}_j$ of $k_{n_j+1}(\sqrt[N_j]{F})$ prime to $\mathfrak{a}_1,\cdots,\mathfrak{a}_s$, and l such that the decomposition group of $\mathfrak{P}_j$ is $\langle\rho\rangle$. Put $\mathfrak{p}_j=\mathfrak{P}_j\cap k$. Then $\mathfrak{p}_j$ satisfies (i), (ii), and (iii).

Put $S=\mathfrak{p}_1\cdots\mathfrak{p}_r$. We prove this S satisfies the conditions of our theorem. First we see the following: (1) $\#(k(\mathfrak{p}_j)/k'_{\mathfrak{p}_j})=N_j$; (2) $F_j\subset k'_{\mathfrak{p}_j}$; (3) $F'\subset k'_S$, in particular, $E_k\subset k'_S$, i.e., $P(S)/P'_S\cong k(S)/k'_S$; (4) $F\cdot k'_{\mathfrak{p}_j}/k'_{\mathfrak{p}_j}=\langle\beta_j\rangle k'_{\mathfrak{p}_j}/k'_{\mathfrak{p}_j}$ is cyclic of order N_j; (5) $F\cdot k'_S/k'_S\cong\prod_j(F\cdot k'_{\mathfrak{p}_j}/k'_{\mathfrak{p}_j})$ (direct product). Indeed, from (ii) and (iii) we see that $\mathfrak{p}_j$ is completely decomposed in k_{n_j} but not in k_{n_j+1}, so that (1) holds by [**2**, Teil I, Satz 19, S. 39]. Let $\mathfrak{P}$ be a prime divisor of $\mathfrak{p}_j$ in k_{n_j}. Then, as is easily seen, $k_{n_j}(\mathfrak{P})/(k_{n_j})_{\mathfrak{P}}\cong k(\mathfrak{p}_j)/k_{\mathfrak{p}_j}$ and $k\cap(k_{n_j})_{\mathfrak{P}}=k_{\mathfrak{p}_j}$, since $\mathfrak{p}_j$ is completely decomposed in k_{n_j}. Therefore using (1) we have that, for $x\in k(\mathfrak{p}_j)$, x is N_j-th power residue modulo $\mathfrak{P}$ in k_{n_j} if and only if $x\in k'_{\mathfrak{p}_j}$. Hence, by Kummer Theory (e.g. see [**2**, Teil II, S. 45]) $x\in k'_{\mathfrak{p}_j}$ if and only if $\mathfrak{p}_j$ is completely decomposed in $k_{n_j}(\sqrt[N_j]{x})/k$, and so we have (2) and (3) from (ii). Furthermore (4) follows from (1) and (2), because we know by (ii) that β_j is not l-th power residue modulo $\mathfrak{p}_j$. Finally we check (5). Clearly the natural homomorphism: $F\cdot k'_S/k'_S\to\prod_j(F\cdot k'_{\mathfrak{p}_j}/k'_{\mathfrak{p}_j})$ is injective. Moreover, using the direct decomposition $F/F^{N_0}=\langle\bar{\beta}_1\rangle\oplus\cdots\oplus\langle\bar{\beta}_r\rangle\oplus\bar{F}'$ and (4), we see this is surjective, so that (5) holds.

Next we prove $\ker(f)=A\cap P'_S$. If $\prod_i\mathfrak{a}_i^{h_i}\in P'_S$, then $\prod_i\mathfrak{a}_i^{h_i}=(x)$ for $x\in F\cap k'_S$. Here we write $x=\prod_j\beta_j^{t_j}y$ with $y\in F'$. Since $f(\varphi(y))=1$, we see $f\circ\varphi(x)=\prod_j f\circ\varphi(\beta_j)^{t_j}$, i.e., $\prod_i a_i^{h_i}=\prod_j b_j^{t_j}$. On the other hand, x, $y\in k'_S$ implies $\prod_j\beta_j^{t_j}\in k'_S$, so that $N_j|t_j$ by (2), (4) and (5). Hence we obtain $\prod_i a_i^{h_i}=\prod_j b_j^{t_j}=1$, which shows $A\cap P'_S\subset\ker(f)$. In particular, $\#(A\cap P/A\cap P'_S)\geqq\#(A\cap P/\ker(f))=\#(N)$. On the other hand, using (1)$\sim$(5), we see $A\cap P/A\cap P'_S\cong F/F\cap k'_S\cong F\cdot k'_S/k'_S\cong\prod_j(F\cdot k'_{\mathfrak{p}_j}/k'_{\mathfrak{p}_j})\cong\prod_j(\langle\beta_j\rangle k'_{\mathfrak{p}_j}/k'_{\mathfrak{p}_j})\cong\prod_j(k(\mathfrak{p}_j)/k'_{\mathfrak{p}_j})\cong k(S)/k'_S\cong P(S)/P'_S$. In particular, $\#(A\cap P/A\cap P'_S)=\#(P(S)/P'_S)=\prod_j N_j=\#(N)$. Thus we have $\ker(f)=A\cap P'_S$.

Therefore we obtain a commutative diagram:

$$\begin{array}{ccccccccc}
1 & \longrightarrow & P(S)/P'_S & \longrightarrow & I(S)/P'_S & \longrightarrow & I/P & \longrightarrow & 1 \\
 & & \uparrow & & \uparrow & & \uparrow\wr\!\!\parallel & & \\
1 & \longrightarrow & A\cap P/A\cap P'_S & \longrightarrow & A/A\cap P'_S & \longrightarrow & A/A\cap P & \longrightarrow & 1 \\
 & & \downarrow\wr\!\!\parallel & & \downarrow\wr\!\!\parallel & & \downarrow\wr\!\!\parallel & & \\
1 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & I/P & \longrightarrow & 1\,.
\end{array}$$

Since $A\cap P/A\cap P_S' \cong P(S)/P_S'$, we see by the diagram that the natural injection: $A/A\cap P_S' \rightarrow I(S)/P_S'$ gives an isomorphism. Thus we obtain an isomorphism $\Phi: I(S)/P_S' \rightarrow M$, as required. This proves the theorem.

3. Remark.

The assumptions $\zeta_1 \notin k$ and $k_1 \neq k_2$ are necessary for the theorem. However we can prove similarly without these assumptions that for an arbitrarily given abelian extension M of the ideal class group I/P of k by a finite abelian l-group N there exist infinitely many tamely ramified abelian extensions K/k which satisfy the following: (1) K coincides with the genus field of K/k (i.e., the maximal abelian extension of k contained in the Hilbert class field of K); (2) there exists an isomorphism $\Phi: \mathrm{Gal}(K/k) \rightarrow M$ inducing an isomorphism $\mathrm{Gal}(K/\bar{k}) \rightarrow N$, which makes the diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathrm{Gal}(K/\bar{k}) & \longrightarrow & \mathrm{Gal}(K/k) & \longrightarrow & \mathrm{Gal}(\bar{k}/k) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 1 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & I/P & \longrightarrow & 1 \end{array}$$

commutative, where $\bar{k}$ denotes the Hilbert class field of k.

References

[1] H. Hasse, Zum Existenzsatz von Grunwald in der Klassenkörpertheorie, J. Reine. Angew. Math., 188 (1950), 40-64.

[2] H. Hasse, Bericht über neuere Untersuchengen und Problem aus der Theorie der algebraischen Zahlkörper, Physica-Verlag Würzburg-Wien, 1970.

Teruo TAKEUCHI
Department of Mathematics
Faculty of General Education
Niigata University
Niigata 950-21
Japan