22. *Pre-special Unit Groups and Ideal Classes of* $\boldsymbol{Q}(\zeta_p)^+$

By Fumika KURIHARA
Department of Mathematics, Tokyo Institute of Technology

(Communicated by Shokichi IYANAGA, M. J. A., April 13, 1992)

Let m be a positive integer and $\boldsymbol{Q}(\zeta_m)^+$ the maximal real subfield of the field of m-th roots of unity. Let E_m be the global unit group of $\boldsymbol{Q}(\zeta_m)^+$ and let $\mathcal{C}_m$ be Karl Rubin's special unit group of $\boldsymbol{Q}(\zeta_m)^+$ (see [4]). Then Rubin's main results in [4] implies the following:

Theorem (cf. Th 1.3 and Th 2.2 of [4]). *If* $\alpha: E_m \to \boldsymbol{Z}[\mathrm{Gal}(\boldsymbol{Q}(\zeta_m)^+/\boldsymbol{Q})]$ *is any* $\mathrm{Gal}(\boldsymbol{Q}(\zeta_m)^+/\boldsymbol{Q})$*-module map, then* $4\alpha(\mathcal{C}_m)$ *annihilates the ideal class group of* $\boldsymbol{Q}(\zeta_m)^+$.

When m is an odd prime p, our result (Th 3) gives a condition for $\alpha(\mathcal{C}_m)$ to be a "minimal" element that annihilates the ideal class group of $\boldsymbol{Q}(\zeta_p)^+$.

Let p be a fixed prime number and let $\mathcal{S}_p=\{l$; odd prime number such that $l\equiv\pm 1 \pmod p\}$, $\mathcal{S}_p^+=\{l\in\mathcal{S}_p;\ l\equiv 1 \pmod p\}$. For any prime number l in $\mathcal{S}_p$, we denote by $\boldsymbol{Q}(\zeta_p,\zeta_l)^{++}$ the composite field of $\boldsymbol{Q}(\zeta_p)^+$ and $\boldsymbol{Q}(\zeta_l)^+$. We fix any prime ideal $\mathfrak{l}$ of $\boldsymbol{Q}(\zeta_p)^+$ above l and we write $\tilde{\mathfrak{l}}$ for the prime ideal of $\boldsymbol{Q}(\zeta_p,\zeta_l)^{++}$ above $\mathfrak{l}$. Also we fix any generator σ of $G=\mathrm{Gal}(\boldsymbol{Q}(\zeta_p,\zeta_l)^{++}/\boldsymbol{Q}(\zeta_l)^+)$. Let E_p, $E_{p,l}$ be the group of global units of $\boldsymbol{Q}(\zeta_p)^+$, $\boldsymbol{Q}(\zeta_p,\zeta_l)^{++}$ respectively. We define $\mathcal{E}_p(l)=\{\eta\in E_{p,l};\ N_{\boldsymbol{Q}(\zeta_p,\zeta_l)^{++}/\boldsymbol{Q}(\zeta_p)^+}(\eta)=1\}$, $\mathcal{C}_p(l)=\{\varepsilon\in E_p;\ \exists\eta\in\mathcal{E}_p(l)$ such that $\varepsilon^2\equiv\eta \pmod{\prod_{j=0}^{(p-3)/2}\tilde{\mathfrak{l}}^{\sigma^j}}\}$. We call $\mathcal{C}_p(l)$ the *pre-l-special* unit group of $\boldsymbol{Q}(\zeta_p)^+$, and we define the special unit group of $\boldsymbol{Q}(\zeta_p)^+$ by $\mathcal{C}_p=\{\varepsilon\in E_p;\ \varepsilon\in\mathcal{C}_p(l)$ for all but finitely many l in $\mathcal{S}_p\}$ (see [4]).

We fix any sufficiently large integer M, and we put $\mathcal{S}_p^{(M)}=\{l\in\mathcal{S}_p^+;\ l\equiv 1 \pmod{p^M}\}$. Let g_p be a primitive root modulo p such that $\sigma(\zeta_p)=\zeta_p^{g_p}$, and for $i=0,\cdots,(p-3)/2$, let $\varepsilon_i=2/(p-1)\sum_{j=0}^{(p-3)/2}\omega^{-2i}(g_p^j)\sigma^j$ be the idempotents in $\boldsymbol{Z}/p^M\boldsymbol{Z}[G]$, where ω is the Teichmüller character. Then $E_p/E_p^{p^M}=\bigoplus_{i=1}^{(p-3)/2}\varepsilon_i(E_p/E_p^{p^M})$. For each $i=1,\cdots,(p-3)/2$, we take any basis η_i of $\varepsilon_i(E_p/E_p^{p^M})$ and let $\alpha: E_p/E_p^{p^M}\to\boldsymbol{Z}/p^M\boldsymbol{Z}[G]$ be a G-module map such that $\alpha(\eta_i)=\varepsilon_i$. We sometimes use the following condition for l.

Condition-L. *Let l be a prime number in $\mathcal{S}_p^{(M)}$. There is a G-module map*

$$\varphi: (\boldsymbol{Z}[\zeta_p]^+/l\boldsymbol{Z}[\zeta_p]^+)^\times\otimes\boldsymbol{Z}/p^M\boldsymbol{Z}\to\boldsymbol{Z}/p^M\boldsymbol{Z}[G]$$

such that the following diagram is commutative:

$$\begin{array}{ccc} E_p/E_p^{p^M} & \xrightarrow{\ \alpha\ } & \boldsymbol{Z}/p^M\boldsymbol{Z}[G] \\ \downarrow{\scriptstyle\psi} & \nearrow{\scriptstyle\varphi} & \\ (\boldsymbol{Z}[\zeta_p]^+/l\boldsymbol{Z}[\zeta_p]^+)\otimes\boldsymbol{Z}/p^M\boldsymbol{Z} & & \end{array}$$

Here, $\boldsymbol{Z}[\zeta_p]^+$ is the integer ring of $\boldsymbol{Q}(\zeta_p)^+$ and ψ is the reduction map.

Now for any prime number l in $\mathcal{S}_p^+$, let I_l, P_l be the fractional ideal group and the principal ideal group of $\boldsymbol{Q}(\zeta_p, \zeta_l)^{++}$ respectively. We denote by $I_p^{(l)}$ the lift of the fractional ideal group of $\boldsymbol{Q}(\zeta_p)^+$ into $\boldsymbol{Q}(\zeta_p, \zeta_l)^{++}$. Let $\mathfrak{C}_p$ be the ideal class group of $\boldsymbol{Q}(\zeta_p)^+$, and we define the l-ideal class group $\mathfrak{C}_p^{(l)}$ of $\boldsymbol{Q}(\zeta_p, \zeta_l)^{++}$ to be $\mathfrak{C}_p^{(l)}=I_l/P_l I_p^{(l)}$. We denoto by $(\mathfrak{l})$, $(\tilde{\mathfrak{l}})_l$ the ideal class, the l-ideal class of $\mathfrak{l}$, $\tilde{\mathfrak{l}}$ respectively. Let $\mathfrak{C}_p^{(l)\prime}$ be the subgroup of $\mathfrak{C}_p^{(l)}$ generated by $\{(\tilde{\mathfrak{l}}^{\sigma^j})\}_{0\le j\le (p-3)/2}$. We put $A_p=\mathfrak{C}_p/p^M\mathfrak{C}_p$, $A_p^{(l)}=\mathfrak{C}_p^{(l)\prime}/p^M\mathfrak{C}_p^{(l)\prime}$, then $A_p=\bigoplus_{i=1}^{(p-3)/2}\varepsilon_i A_p$, $A_p^{(l)}=\bigoplus_{i=1}^{(p-3)/2}\varepsilon_i A_p^{(l)}$. We denote by $[\mathfrak{l}]$, $[\tilde{\mathfrak{l}}]_l$ the projection of $(\mathfrak{l})$, $(\tilde{\mathfrak{l}})_l$ into A_p, $A_p^{(l)}$.

Let v_p be the p-adic valuation normalized by $v_p(p)=1$. For any subgroup H of E_p, we write $(E_p/H)_p=(E_p/H)_{p,M}$ for $(E_p/E_p^{p^M})/(H/H\cap E_p^{p^M})$.

Our main theorem states the following.

Theorem 1. *For each $i=1,\cdots,(p-3)/2$;*

(i) *If $l\in\mathcal{S}_p^+$, then*
$v_p(|\varepsilon_i(E_p/C_p(l))_p|)\le v_p(\mathrm{ord}\,\varepsilon_i[\tilde{\mathfrak{l}}]_l)$.

(ii) *If $l\in\mathcal{S}_p^{(M)}$ then*
$v_p(\mathrm{ord}\,\varepsilon_i[\mathfrak{l}])\le v_p(\mathrm{ord}\,\varepsilon_i[\tilde{\mathfrak{l}}]_l)$.

(iii) *If $l\in\mathcal{S}_p^{(M)}$ and l satisfies the Condition-L then*
$v_p(|\varepsilon_i(E_p/C_p(l))_p|)=v_p(\mathrm{ord}\,\varepsilon_i[\tilde{\mathfrak{l}}]_l)$.

From Th 1 (iii), we obtain a relation between the p-part of the index of the pre-l-special unit group and the order of the ideal class of $\tilde{\mathfrak{l}}$.

Next, using Th 1, we shall discuss some relation between $(E_p/C_p)_p$ and A_p. Let $m_0=m_0^{(i)}=\min\{m\,;\,0\le m\in\boldsymbol{Z},\ p^m\varepsilon_i A_p=0\}$. Then from Rubin's Theorem above and the definition of α, we have $m_0\le v_p(|\varepsilon_i(E_p/C_p)_p|)$. Now, let $\mathcal{S}_p^{(M,\alpha)}=\{l\in\mathcal{S}_p^{(M)}\,;\,l$ satisfies the Condition-L$\}$ and let $C_p^{(M,\alpha)}=\{\varepsilon\in E_p\,;\,\varepsilon\in C_p(l)$ for all but finitely many l in $\mathcal{S}_p^{(M,\alpha)}\}$, then clearly $C_p\subset C_p^{(M,\alpha)}$. It is not known whether $m_0=v_p(|\varepsilon_i(E_p/C_p^{(M,\alpha)})_p|)$, but we have the following.

Proposition 2. *The inequality $m_0\le v_p(|\varepsilon_i(E_p/C_p^{(M,\alpha)})_p|)$ holds. Particularly, if $\varepsilon_i A_p$ is cyclic then $m_0=v_p(|\varepsilon_i(E_p/C_p^{(M,\alpha)})_p|)$.*

And we give the following condition for $m_0=v_p(|\varepsilon_i(E_p/C_p^{(M,\alpha)})_p|)$.

Theorem 3. *The equality $m_0=v_p(|\varepsilon_i(E_p/C_p^{(M,\alpha)})_p|)$ holds if and only if there exists a prime number l satisfying*

(i) $l\in\mathcal{S}_p^{(M,\alpha)}$

(ii) $\varepsilon_i(C_p^{(M,\alpha)}/C_p^{(M,\alpha)}\cap E_p^{p^M})=\varepsilon_i(C_p(l)/C_p(l)\cap E_p^{p^M})$

(iii) $v_p(\mathrm{ord}\,\varepsilon_i[\mathfrak{l}])=v_p(\mathrm{ord}\,\varepsilon_i[\tilde{\mathfrak{l}}]_l)$.

It is not known whether or not there exists an l satisfying (i)–(iii) of Th 3 in general. But we obtain the following.

Proposition 4. *For each $i=1,\cdots,(p-3)/2$, there are infinitely many rational primes l satisfying:*

(i) $l\in\mathcal{S}_p^{(M,\alpha)}$

(ii) $\varepsilon_i(C_p^{(M,\alpha)}/C_p^{(M,\alpha)}\cap E_p^{p^M})=\varepsilon_i(C_p(l)/C_p(l)\cap E_p^{p^M})$.

It is not known whether or not $p\nmid[C_p^{(M,\alpha)}:C_p]$. If $v_p(|\varepsilon_i(C_p^{(M,\alpha)}/C_p)_p|)=0$ then from Th 3 we have $m_0=v_p(|\varepsilon_i(E_p/C_p)_p|)$ if and only if there exists a prime number l satisfying (i)–(iii) of Th 3.

References

[1] Kummer, E.: Über eine besondere Art, aus complexen Einheiten gebildeter Ausdrücke. J. Reine Angew. Math., **50**, 212–232 (1855).
[2] Lang, S.: Cyclotomic Fields. Graduate Texts in Mathematics, Springer-Verlag, New York (1989).
[3] Mazur, B. and Wiles, A.: Class fields of abelian extensions of $\boldsymbol{Q}$. Invent. Math., **76**, 179–330 (1984).
[4] Rubin, K.: Global units and ideal class groups. ibid., **89**, 511–526 (1987).
[5] Thaine, F.: On the ideal class groups of real abelian number fields. Ann. of Math., **128**, 1–18 (1988).
[6] Washington, L. C.: Introduction to Cyclotomic Fields. Graduate Texts in Mathematics, Springer-Verlag, New York (1982).