Notes on the structure of the ideal class groups of abelian number fields

By Miho Aoki

Department of Mathematics, Tokyo Institute of Technology
2-12-1 Oh-okayama, Meguro-ku, Tokyo 152-8551
(Communicated by Shigefumi Mori, M. J. A., May 12, 2005)

Abstract: In this paper, we give explicit formulae of certain higher annihilators of the ideal class groups defined by V. Kolyvagin and K. Rubin, which come from Euler systems of Stickelberger elements and cyclotomic units. Further, using these explicit formulae, we reformulate Kolyvagin-Rubin's structure theorem of the ideal class groups of abelian number fields.

Key words: Ideal class groups; Euler systems.

1. Introduction. Let K be an abelian number field, and for a fixed odd rational prime p, we denote by A_K the Sylow p-subgroup of the ideal class group of K. In this paper, we will give explicit formulae of certain higher annihilators of A_K which were introduced by V. Kolyvagin and K. Rubin. These higher annihilators are given by Euler systems of cyclotomic units and Stickelberger elements (or Gauss sums), and they annihilate the ideal class groups except finitely many primes. By using these explicit formulae, we will reformulate Kolyvagin-Rubin's structure theorem of A_K in the case $p \nmid [K:\mathbf{Q}]$. The contents of this paper are as follows. In Section 2, we recall the definition of higher annihilators given by V. Kolyvagin and K. Rubin. In Section 3, we give a Key proposition (Proposition 7) and calculate higher annihilators (Theorem 9, 13). In Section 4, we study the structure of A_K in the case $p \nmid [K:\mathbf{Q}]$. We reformulate Kolyvagin-Rubin's structure theorem of A_K using the results of Section 3 (Theorem 14, 15).

2. Higher annihilators. In this section, we recall higher annihilators. For details, see [1, 3, 4]. Let K be an abelian number field and set $G = \mathrm{Gal}(K/\mathbf{Q})$. We fix an odd rational prime p and write $G \simeq \Delta \times G_p$ with $p \nmid |\Delta|$ and p-group G_p. For a character χ of Δ, we say an odd character (resp. even character) if $\chi(-1) = -1$ (resp. $\chi(-1) = 1$). By embedding $\overline{\mathbf{Q}}$ (the algebraic closure of $\mathbf{Q}$) to $\overline{\mathbf{Q}}_p$, we think of χ as a $\overline{\mathbf{Q}}_p$-valued character. We define the idempotent $e_\chi \in \mathbf{Z}_p[\Delta]$ by $e_\chi = \frac{1}{|\Delta|}\sum_{\sigma\in\Delta}\mathrm{Tr}(\chi^{-1}(\sigma))\sigma$, where $\mathrm{Tr} : \mathbf{Q}_p(\chi(\sigma) \mid \sigma \in \Delta) \to \mathbf{Q}_p$ is the trace map. Let $\mathcal{O}_\chi$ denote the extension ring of $\mathbf{Z}_p$ generated by the values of χ. For any $\mathbf{Z}_p[\Delta]$-module Y, we define the χ-part Y_χ of Y by $Y_\chi = e_\chi Y$. If two characters χ_1 and χ_2 of Δ satisfy $\chi_1 = {\chi_2}^\sigma$ for some $\sigma \in \mathrm{Gal}(\overline{\mathbf{Q}}_p/\mathbf{Q}_p)$, we say χ_1 is conjugate to χ_2 over $\mathbf{Q}_p$. The number of characters that conjugate to χ is $\mathrm{rank}_{\mathbf{Z}_p}\mathcal{O}_\chi$. The $\mathbf{Z}_p[\Delta]$-module Y is decomposed as $Y \simeq \bigoplus_{\chi:\mathrm{rep.}} Y_\chi$, where χ runs over all representatives of $\mathbf{Q}_p$-conjugacy classes of characters of Δ. Let A_K be the Sylow p-subgroup of the ideal class group of K, then A_K is a $\mathbf{Z}_p[\Delta]$-module and decomposed as $A_K \simeq \bigoplus_{\chi:\mathrm{rep.}} A_{K,\chi}$. We define the higher annihilators of $A_{K,\chi}$ for each character χ of Δ. The construction of these annihilators are different according to odd characters or even characters. For odd characters χ, we use the Euler system of Stickeberger elements, and for even characters χ, we use the Euler system of cyclotomic elements. Let N be the conductor of K, then K is a subfield of the cyclotomic field $L = \mathbf{Q}(\mu_N)$. We write $N = p^t N_0$ with $t \geq 0$ and $p \nmid N_0$. Let M be a power of p such that $M > p^t$. For any integer $i \geq 0$, let $\mathsf{S}_i = \{n \in \mathbf{Z} > 0 \mid \text{squarefree}, n = \ell_1 \cdots \ell_i \text{ (product of primes)}, \ell_j \equiv 1 \pmod{MN_0}\}$, and set $\mathsf{S} = \bigcup_{i\geq 0}\mathsf{S}_i$. For every integer $n \in \mathsf{S}$ and every prime $\ell \in \mathsf{S}_1$, set $G_N = \mathrm{Gal}(L/\mathbf{Q})$, $G_N^+ = \mathrm{Gal}(L^+/\mathbf{Q})$, $G = \mathrm{Gal}(K/\mathbf{Q})$, $G^+ = \mathrm{Gal}(K^+/\mathbf{Q})$, $G_n = \mathrm{Gal}(L(\mu_n)/L) \simeq \mathrm{Gal}(K(\mu_n)/K) \simeq \mathrm{Gal}(\mathbf{Q}(\mu_n)/\mathbf{Q})$, $N_n = \sum_{\tau\in G_n}\tau$, $D_\ell = \sum_{i=0}^{\ell-2} i{\rho_\ell}^i$, $D_n = \prod_{\ell\mid n} D_\ell$, where L^+ (resp. K^+) is the maximal real subfield of L (resp. K), and ρ_ℓ is a fixed generator of $G_\ell\,(\simeq (\mathbf{Z}/\ell)^\times)$. Fix $n \in \mathsf{S}$. By the canonical

2000 Mathematics Subject Classification. Primary 11R23; Secondary 11R18, 11R29.

isomorphism $\mathrm{Gal}(L(\mu_n)/\mathbf{Q}) \simeq (\mathbf{Z}/nN)^\times$ we write $\tau_a \in \mathrm{Gal}(L(\mu_n)/\mathbf{Q})$ corresponding to $a \in (\mathbf{Z}/nN)^\times$ ($\zeta^{\tau_a} = \zeta^a$ for every $\zeta \in \mu_{nN}$). Further define $\sigma_a \in G_N$ and $\tau_{n,a} \in G_n$ by $\tau_a \mapsto (\sigma_a, \tau_{n,a})$ under the isomorphism $\mathrm{Gal}(L(\mu_n)/\mathbf{Q}) \simeq G_N \times G_n$.

2.1. Higher annihilators of the minus part. In this subsection, we define the higher annihilator of $A_{K,\chi}$ for an odd character χ. We assume $\chi \neq \omega$ (Teichmüller character). We know Stickelberger element as a good annihilator of $A_{K,\chi}$. For each $n \in \mathsf{S}$, we choose an integer $b_n > 0$ such that $(b_n, nNp) = 1$ and $b_n \equiv 1 \pmod{n}$.

Definition 1 (Stickelberger element)**.** For any $n \in \mathsf{S}$, we define Stickelberger element $\theta_n \in \mathbf{Z}_p[\mathrm{Gal}(L(\mu_n)/\mathbf{Q})]$ by

$$\theta_n = (\sigma_{b_n} - b_n) \sum_{\substack{a=1 \\ (a,nN)=1}}^{nN} \frac{a}{nN} {\tau_a}^{-1}.$$

Stickelberger's theorem says that $e_\chi \mathrm{Res}_{L/K}(\theta_1)$ annihilates $A_{K,\chi}$, namely ${A_{K,\chi}}^{e_\chi \mathrm{Res}_{L/K}(\theta_1)} = 0$, where $\mathrm{Res}_{L/K} : \mathbf{Z}_p[G_N] \to \mathbf{Z}_p[G]$ is the natural restriction ([6, Theorem 6.10]). We define an element $\delta(n) \in (\mathbf{Z}/M)[G_N]$ for each $n \in \mathsf{S}$, which is the natural image of θ_1 for $n = 1$.

Lemma 2 (4, Lemma 2.1)**.** *For any $n \in \mathsf{S}$, we have*

$$D_n\theta_n \in (\mathbf{Z}/M)[\mathrm{Gal}(L(\mu_n)/\mathbf{Q})]^{G_n} = N_n(\mathbf{Z}/M)[G_N].$$

By this lemma, we define the higher annihilator $\delta(n) \in (\mathbf{Z}/M)[G_N]$ to be the element satisfying $D_n\theta_n = N_n\delta(n)$. For any $n \in \mathsf{S}$, let $B_K(n)$ be the $\mathbf{Z}_p[\Delta]$-submodule of A_K which is generated by the classes of prime ideals of K dividing n. V. Kolyvagin showed that $e_\chi \mathrm{Res}_{L/K}\,\delta(n)$ annihilates $A_{K,\chi}/B_K(n)_\chi$.

Proposition 3 (V. Kolyvagin [1, Theorem 5], K. Rubin [4, Proposition 2.3])**.** *Let $n \in \mathsf{S}$. If M is a power of p satisfying $M \geq |A_{K,\chi}|$, then we have* $(A_{K,\chi}/B_K(n)_\chi)^{e_\chi \mathrm{Res}_{L/K}(\delta(n))} = 0$.

2.2. Higher annihilators of the plus part. In this subsection, we define the higher annihilators of $A_{K,\chi}$ for an even character χ. In this case, we can consider χ as a character of $G^+ = \mathrm{Gal}(K^+/\mathbf{Q})$, and we have an isomorphism $A_{K,\chi} \simeq A_{K^+,\chi}$. Hence we study $A_{K^+,\chi}$ instead of $A_{K,\chi}$. First, we define the cyclotomic unit.

Definition 4 (cyclotomic unit)**.** For any $n \in \mathsf{S}$, we define the cyclotomic unit $\xi_{L^+,n}$ by

$$\xi_{L^+,n} = \Bigl(\zeta_N \prod_{\ell | n} \zeta_\ell - 1\Bigr)\Bigl({\zeta_N}^{-1} \prod_{\ell | n} \zeta_\ell - 1\Bigr) \in L^+(\mu_n)^\times.$$

Lemma 5 (3, Appendix, Lemma 2.2)**.** *For any $n \in \mathsf{S}$, there is a unique $\kappa_{L^+,n} \in {L^+}^\times/({L^+}^\times)^M$ such that $\kappa_{L^+,n} \equiv {\xi_{L^+,n}}^{D_n} \pmod{(L^+(\mu_n)^\times)^M}$.*

Next, we define certain map whose image is in $(\mathbf{Z}/M)[G_N^+]$, and we construct higher annihilators by the image of $\kappa_{L^+,n}$. Let $\ell \in \mathsf{S}_1$ and fix a prime ideal $\mathcal{L}$ of L^+ above ℓ, and denote the unique prime ideal of $L^+(\mu_\ell)$ above $\mathcal{L}$ by $\widetilde{\mathcal{L}}$. We choose an element $\pi_{\mathcal{L}}$ of the ring of integers $\mathcal{O}_{L^+(\mu_\ell)}$ of $L^+(\mu_\ell)$ such that the principal ideal generated by $\pi_{\mathcal{L}}$ satisfies $(\pi_{\mathcal{L}}) = \widetilde{\mathcal{L}}\mathfrak{a}$, where $\mathfrak{a}$ is an ideal of $L^+(\mu_\ell)$ which is prime to ℓ. For a fixed generator ρ_ℓ of G_ℓ, we can see that ${\pi_{\mathcal{L}}}^{\rho_\ell - 1} \bmod \widetilde{\mathcal{L}}$ is a generator of $(\mathcal{O}_{L^+(\mu_\ell)}/\widetilde{\mathcal{L}})^\times \simeq (\mathbf{Z}/\ell)^\times$ and ${\pi_{\mathcal{L}}}^{\rho_\ell - 1} \equiv 1 \pmod{\widetilde{\mathcal{L}^\tau}}$ for every $\tau (\neq 1) \in G_N^+$. Hence ${\pi_{\mathcal{L}}}^{\rho_\ell - 1} \bmod \prod_{\tau \in G_N^+} \widetilde{\mathcal{L}^\tau}$ is a generator of $X_{L^+,\ell} = (\mathcal{O}_{L^+(\mu_\ell)}/\prod_{\tau \in G_N^+} \widetilde{\mathcal{L}^\tau})^\times$ as a G_N^+-module. Further, we can easily show that the following map is an isomorphism of $(\mathbf{Z}/M)[G_N^+]$-modules.

$$\begin{array}{cccc} \psi_{\pi_{\mathcal{L}}} : & X_{L^+,\ell}/{X_{L^+,\ell}}^M & \simeq & (\mathbf{Z}/M)[G_N^+] \\ & \Bigl({\pi_{\mathcal{L}}}^{\rho_\ell - 1} \bmod \prod_{\tau \in G_N^+} \widetilde{\mathcal{L}^\tau}\Bigr)^x & \mapsto & x\,. \end{array}$$

Remark. Let I_{L^+} denote the ideal group of L^+. For $x \in {L^+}^\times$, let $[x] \in I_{L^+}/MI_{L^+}$ be the projection of the principal ideal (x) and $[x]_\ell \in I_{L^+,\ell}/MI_{L^+,\ell}$ be its ℓ-part (product of prime ideals dividing ℓ). The map $\psi_{\pi_{\mathcal{L}}}$ satisfies the following commutative diagram.

$$\begin{array}{ccccc} & x & \mapsto & [N_{L^+(\mu_\ell)/L^+}(x)]_\ell & \\ x & L^+(\mu_\ell)^\times & \rightarrow & I_{L^+,\ell}/MI_{L^+,\ell} & \mathcal{L} \\ \downarrow & \downarrow & & \downarrow & \downarrow \\ x^{\rho_\ell - 1} & X_{L^+,\ell}/{X_{L^+,\ell}}^M & \underset{\psi_{\pi_{\mathcal{L}}}}{\rightarrow} & (\mathbf{Z}/M)[G_N^+] & 1 \end{array}$$

Proposition 6 (V. Kolyvagin [1, Theorem 5], K. Rubin [3, Appendix, Lemma 2.2])**.** *Let $n \in \mathsf{S}$. Assume that M is a power of p satisfying $M \geq |A_{K^+,\chi}|$. For each class $c \in A_{K^+,\chi}$, we choose a prime ideal λ as the representative of c which divides a rational prime $\ell \in \mathsf{S}_1$ satisfying $\ell \equiv 1$ $\pmod{MnN_0}$ (We can choose such λ by the Chebotarev density theorem). Then for any prime ideal $\mathcal{L}$ of L^+ above λ, we have $c^{e_\chi \mathrm{Res}_{L^+/K^+} \psi_{\pi_{\mathcal{L}}}(\kappa_{L^+,n})} = 0$ in $A_{K^+,\chi}/B_{K^+}(n)_\chi$.*

Remarks. (1) Note that the higher annihilator $\psi_{\pi_{\mathcal{L}}}(\kappa_{L^+,n})$ of the plus part are different for each class $c \in A_{K^+,\chi}$. (2) For $n = 1$, this proposition is essentially the result of F. Thaine [5].

3. Explicit formulae of higher annihilators. In this section, we will give explicit formulae of the higher annihilators $\delta(n)$ and $\psi_{\pi_{\mathcal{L}}}(\kappa_{L^+,n})$ in Section 2. First, we show the following Key proposition. For any prime $\ell \in \mathsf{S}_1$, let g_ℓ be the generator of $(\mathbf{Z}/\ell)^\times$ corresponding to a fixed generator $\rho_\ell \in G_\ell$ by the canonical isomorphism $G_\ell \simeq (\mathbf{Z}/\ell)^\times$.

Proposition 7. *For any*

$$Y_n = \sum_{\substack{a=1,\\(a,nN)=1}}^{nN} y_a {\tau_a}^{-1} \in (\mathbf{Z}/M)[\mathrm{Gal}(L(\mu_n)/\mathbf{Q})],$$

$y_a \in \mathbf{Z}/M$ satisfying

$$D_n Y_n \in (\mathbf{Z}/M)[\mathrm{Gal}(L(\mu_n)/\mathbf{Q})]^{G_n} = N_n(\mathbf{Z}/M)[G_N],$$

if we write $D_n Y_n = N_n Z_n$ with $Z_n \in (\mathbf{Z}/M)[G_N]$, then we have

$$Z_n = \sum_{\substack{a=1\\(a,nN)=1}}^{nN} y_a \Bigl(\prod_{\substack{\ell | n\\ \text{prime}}} \nu_\ell(a)\Bigr) {\sigma_a}^{-1} \in (\mathbf{Z}/M)[G_N],$$

where $\nu_\ell : (\mathbf{Z}/\ell)^\times \to \mathbf{Z}/(\ell-1)$ denotes the logarithm map given by ${g_\ell}^{\nu_\ell(a)} \equiv a \pmod{\ell}$.

Proof. This proposition is a consequence of the following lemma by putting $n' = n$. □

Lemma 8. *For any divisor n' of n,*

$$D_n Y_n \equiv D_{n/n'} N_{n'} \times \sum_{\substack{a=1\\(a,nN)=1}}^{nN} y_a \Bigl(\prod_{\substack{\ell | n'\\ \text{prime}}} \nu_\ell(a)\Bigr) {\sigma_a}^{-1} {\tau_{n/n',a}}^{-1} \pmod{M}.$$

Proof. We use the induction with respect to the number of primes dividing n'. For $n' = 1$, it is trivial. Let q be a rational prime such that $q \nmid n'$ and $q | n$, then we have $n'q | n$. We will prove the assertion for $n'q$. Let ρ_q be the fixed generator of G_q corresponding to a generator g_q of $(\mathbf{Z}/q)^\times$, we have $\tau_{q,a} = {\rho_q}^{\nu_q(a)}$. From the decomposition $G_{n/n'} \simeq G_{n/(n'q)} \times G_q$, we can write ${\tau_{n/n',a}}^{-1} = {\tau_{n/(n'q),a}}^{-1} {\tau_{q,a}}^{-1} = {\tau_{n/(n'q),a}}^{-1} {\rho_q}^{\nu_q(a^{-1})}$. Further we have

$$D_{n/n'} = D_{n/(n'q)} D_q \quad \text{and} \quad D_q = \sum_{d=1}^{q-1} \nu_q(d) {\rho_q}^{\nu_q(d)}.$$

By the assumption of the induction, we obtain

$$\begin{aligned} &D_n Y_n \\ &\equiv D_{n/n'} N_{n'} \sum_{\substack{a=1\\(a,nN)=1}}^{nN} y_a \Bigl(\prod_{\substack{\ell | n'\\ \text{prime}}} \nu_\ell(a)\Bigr) {\sigma_a}^{-1} {\tau_{n/n',a}}^{-1} \\ &\equiv D_{n/(n'q)} N_{n'} \sum_{d=1}^{q-1} \sum_{\substack{a=1\\(a,nN)=1}}^{nN} \\ &\qquad y_a \Bigl(\prod_{\substack{\ell | n'\\ \text{prime}}} \nu_\ell(a)\Bigr) {\sigma_a}^{-1} {\tau_{n/(n'q),a}}^{-1} {\rho_q}^{\nu_q(da^{-1})} \nu_q(d) \\ &\qquad \pmod{M}. \end{aligned}$$

By replacing d with ad, we can write

$$D_n Y_n \equiv \sum_{d=1}^{q-1} K_d {\rho_q}^{\nu_q(d)} \pmod{M},$$

where

$$\begin{aligned} K_d &= D_{n/(n'q)} N_{n'} \\ &\quad \times \sum_a y_a \Bigl(\prod_{\substack{\ell | n'\\ \text{prime}}} \nu_\ell(a)\Bigr) {\sigma_a}^{-1} {\tau_{n/(n'q),a}}^{-1} \nu_q(ad) \\ &\quad \in (\mathbf{Z}/M)[\mathrm{Gal}(L(\mu_{n/q})/\mathbf{Q})]. \end{aligned}$$

Since $D_n Y_n \in (\mathbf{Z}/M)[\mathrm{Gal}(L(\mu_n)/\mathbf{Q})]^{G_q}$, we have $K_d = K_1$ for every d with $1 \le d \le q-1$. Therefore, we get

$$\begin{aligned} D_n Y_n &\equiv K_1 N_q \equiv D_{n/(n'q)} N_{n'q} \\ &\quad \sum_{\substack{a=1\\(a,nN)=1}}^{nN} y_a \Bigl(\prod_{\substack{\ell | n'q\\ \text{prime}}} \nu_\ell(a)\Bigr) {\sigma_a}^{-1} {\tau_{n/(n'q),a}}^{-1} \\ &\quad \pmod{M}. \end{aligned}$$

□

Next, we calculate higher annihilators by using Proposition 7. First, we consider the annihilator $\delta(n)$ of the minus part. For $n \in \mathsf{S}$, let $\theta_n \in \mathbf{Z}_p[\mathrm{Gal}(L(\mu_n)/\mathbf{Q})]$ be the Stickelberger element defined in Subsection 2.1. By Lemma 2, we apply Proposition 7 to θ_n and get the explicit formula of $\delta(n)$.

Theorem 9. *For any $n \in \mathsf{S}$, we have*

$$\delta(n) = (\sigma_{b_n} - b_n) \sum_{\substack{a=1\\(a,nN)=1}}^{nN} \frac{a}{nN} \Bigl(\prod_{\substack{\ell | n\\ \text{prime}}} \nu_\ell(a)\Bigr) {\sigma_a}^{-1} \in (\mathbf{Z}/M)[G_N].$$

Proof. We apply Proposition 7 to

$$\theta_n = (\sigma_{b_n} - b_n) \sum_{\substack{a=1\\(a,nN)=1}}^{nN} \frac{a}{nN}{\tau_a}^{-1} = \sum_{\substack{a=1\\(a,nN)=1}}^{nN} y_a{\tau_a}^{-1}$$

with

$$y_a = \left\{\frac{b_n a}{nN}\right\} - b_n\left\{\frac{a}{nN}\right\} \in \mathbf{Z},$$

where $\{x\}$ denotes the fractional part of x for any $x \in \mathbf{Q}$. Then we have

$$\begin{aligned}
\delta(n) &= \sum_{\substack{a=1\\(a,nN)=1}}^{nN} y_a\Bigg(\prod_{\substack{\ell|n\\\text{prime}}} \nu_\ell(a)\Bigg){\sigma_a}^{-1}\\
&= \sum_{\substack{a=1,\\(a,nN)=1}}^{nN} \left\{\frac{b_n a}{nN}\right\}\Bigg(\prod_{\substack{\ell|n\\\text{prime}}} \nu_\ell(a)\Bigg){\sigma_a}^{-1}\\
&\quad - b_n \sum_{\substack{a=1\\(a,nN)=1}}^{nN} \frac{a}{nN}\Bigg(\prod_{\substack{\ell|n\\\text{prime}}} \nu_\ell(a)\Bigg){\sigma_a}^{-1}\\
&= \sum_{\substack{a=1,\\(a,nN)=1}}^{nN} \frac{a}{nN}\Bigg(\prod_{\substack{\ell|n\\\text{prime}}} \nu_\ell(a{b_n}^{-1})\Bigg){\sigma_{a{b_n}^{-1}}}^{-1}\\
&\quad - b_n \sum_{\substack{a=1,\\(a,nN)=1}}^{nN} \frac{a}{nN}\Bigg(\prod_{\substack{\ell|n\\\text{prime}}} \nu_\ell(a)\Bigg){\sigma_a}^{-1}\\
&= (\sigma_{b_n} - b_n) \sum_{\substack{a=1,\\(a,nN)=1}}^{nN} \frac{a}{nN}\Bigg(\prod_{\substack{\ell|n\\\text{prime}}} \nu_\ell(a)\Bigg){\sigma_a}^{-1}
\end{aligned}$$

because of $a{b_n}^{-1} \equiv a \pmod{\ell}$ for any ℓ with $\ell|n$ by the definition of b_n (cf. Subsection 2.1). □

Next, we consider the annihilator $\psi_{\pi_\mathcal{L}}(\kappa_{L^+,n})$ of the plus part. We begin with giving a new definition of the map $\psi_{\pi_\mathcal{L}}$. Let $F/\mathbf{Q}$ be a finite Galois extension, and λ be a prime ideal of F which is completely decomposed in $F/\mathbf{Q}$. We denote the rational prime below λ by ℓ and denote the unique prime ideal of $F(\mu_\ell)$ above λ by $\widetilde{\lambda}$. Define the logarithm map ν_λ : $\{x \in F^\times \mid \mathrm{ord}_\lambda(x) = 0\} \to \mathbf{Z}/(\ell-1)$ by $g_\ell{}^{\nu_\lambda(x)} \equiv x \pmod{\lambda}$, where $g_\ell \in (\mathbf{Z}/\ell)^\times$ is a fixed generator. Let $\mathcal{O}_F$ denote the ring of integers of F. Set

$$X_{F,\ell} = \Bigg(\mathcal{O}_F \Big/ \prod_{\tau\in\mathrm{Gal}(F/\mathbf{Q})} \lambda^\tau\Bigg)^\times$$
$$\Bigg(\simeq \big(\mathcal{O}_{F(\mu_\ell)} \Big/ \prod_{\tau\in\mathrm{Gal}(F/\mathbf{Q})} \widetilde{\lambda^\tau}\big)^\times\Bigg).$$

We define the $\mathrm{Gal}(F/\mathbf{Q})$-isomorphism

$$\varphi_\lambda : X_{F,\ell} \simeq (\mathbf{Z}/(\ell-1))[\mathrm{Gal}(F/\mathbf{Q})]$$

by $\varphi_\lambda(x) = \sum_{\tau\in\mathrm{Gal}(F/\mathbf{Q})} \nu_{\lambda^\tau}(\widetilde{x})\tau \pmod{(\ell-1)}$, where $\widetilde{x}$ is a lifting of $x \in X_{F,\ell}$ to $F^\times$. If $\ell \equiv 1 \pmod{M}$, then we also denote the isomorphism $X_{F,\ell}/{X_{F,\ell}}^M \simeq (\mathbf{Z}/M)[\mathrm{Gal}(F/\mathbf{Q})]$ by φ_λ. We can show the following lemma by a direct calculation.

Lemma 10. *Let F and λ be as before. For any subfield F' of F, we have*
(i) $\mathrm{Res}_{F/F'}(\varphi_\lambda(x)) = \varphi_{N_{F/F'}(\lambda)}(x^{N_{F/F'}})$ *for any* $x \in X_{F,\ell}$,
(ii) $\varphi_\lambda(y) = N_{F/F'}(\varphi_{N_{F/F'}(\lambda)}(y))$ *for any* $y \in X_{F',\ell}$,
where $\mathrm{Res}_{F/F'} : (\mathbf{Z}/(\ell-1))[\mathrm{Gal}(F/\mathbf{Q})] \to (\mathbf{Z}/(\ell-1))[\mathrm{Gal}(F'/\mathbf{Q})]$ *is the natural restriction map, and* $N_{F/F'} = \sum_{\tau\in\mathrm{Gal}(F/F')} \tau$.

Lemma 11. *Let $\mathcal{L}$ be a prime ideal of L^+ lying above a rational prime $\ell \in \mathsf{S}_1$. The map $\varphi_\mathcal{L}$ coincides with the map $\psi_{\pi_\mathcal{L}}$ defined in Subsection 2.2 : $\varphi_\mathcal{L} = \psi_{\pi_\mathcal{L}}$. Especially, the map $\psi_{\pi_\mathcal{L}}$ is independent of the choice of an element $\pi_\mathcal{L} \in \mathcal{O}_{L^+(\mu_\ell)}$.*

Proof. It is enough to show $\varphi_\mathcal{L}({\pi_\mathcal{L}}^{\rho_\ell - 1} \bmod \prod_{\tau\in G_N^+} \widetilde{\mathcal{L}^\tau}) = 1$. By the definition of $\pi_\mathcal{L}$ (cf. Subsection 2.2), we can write $\pi_\mathcal{L} = (1-\zeta_\ell)y$ where $y \in L^+(\mu_\ell)$ is prime to $\widetilde{\mathcal{L}}$. Since $(1-\zeta_\ell)^{\rho_\ell - 1} \equiv g_\ell \pmod{\widetilde{\mathcal{L}}}$ and $y^{\rho_\ell - 1} \equiv 1 \pmod{\widetilde{\mathcal{L}}}$, we get ${\pi_\mathcal{L}}^{\rho_\ell - 1} \equiv g_\ell \pmod{\widetilde{\mathcal{L}}}$. The assertion follows this. □

By the above lemma, we consider $\varphi_\mathcal{L}(\kappa_{L^+,n})$ instead of $\psi_{\pi_\mathcal{L}}(\kappa_{L^+,n})$. Let $\mathcal{L}$ be a prime ideal of L^+ lying above a rational prime $\ell \equiv 1 \pmod{MnN_0}$. Fix prime ideals $\mathcal{L}'$ of L and $\widehat{\mathcal{L}}$ of $L(\mu_n)$ lying above $\mathcal{L}$ such that $\widehat{\mathcal{L}} \supset \mathcal{L}'$. We apply Proposition 7 to $\varphi_{\widehat{\mathcal{L}}}(\xi_{L^+,n}) \in (\mathbf{Z}/M)[\mathrm{Gal}(L(\mu_n)/\mathbf{Q})]$, where $\xi_{L^+,n} \in L^+(\mu_n)^\times$ is the cyclotomic unit defined in Subsection 2.2. By the canonical isomorphism $\mathrm{Gal}(L^+(\mu_n)/\mathbf{Q}) \simeq ((\mathbf{Z}/N)^\times/\{\pm1\}) \times (\mathbf{Z}/n)^\times \simeq (\mathbf{Z}/Nn)^\times/\{\langle -1,1\rangle\}$, we write $\overline{\tau_a} \in \mathrm{Gal}(L^+(\mu_n)/\mathbf{Q})$ corresponding to $a \in (\mathbf{Z}/Nn)^\times/\{\langle -1,1\rangle\}$, and define $\overline{\sigma_a} \in G_N^+ = \mathrm{Gal}(L^+/\mathbf{Q})$ by $\overline{\tau_a} \mapsto (\overline{\sigma_a}, \tau_{n,a})$ under the isomorphsm $\mathrm{Gal}(L^+(\mu_n)/\mathbf{Q}) \simeq G_N^+ \times G_n$. Further, we define $\beta_n \in (\mathbf{Z}/Nn)^\times$ by $\beta_n \mapsto (-1,1)$ under the isomorphism $(\mathbf{Z}/Nn)^\times \simeq (\mathbf{Z}/N)^\times \times (\mathbf{Z}/n)^\times$.

Definition 12. For any $a \in (\mathbf{Z}/Nn)^\times/\{\langle -1,1\rangle\}$, we define $T_{n,\ell,a} \in (\mathbf{Z}/\ell)^\times$ by

$$T_{n,\ell,a} = \big(g_\ell{}^{\frac{\ell-1}{Nn}a} - 1\big)\big(g_\ell{}^{\frac{\ell-1}{Nn}\beta_n a} - 1\big),$$

where $g_\ell \in (\mathbf{Z}/\ell)^\times$ is a fixed generator.

Theorem 13. *For any $n \in \mathsf{S}$ and prime ideal $\mathcal{L}$ of L^+ lying above a rational prime $\ell \equiv 1$*

(mod MnN_0), *we have*

$$\varphi_{\mathcal{L}}(\kappa_{L^+,n}) = \sum_{a\in(\mathbf{Z}/Nn)^\times/\{\langle -1,1\rangle\}} \nu_\ell(T_{n,\ell,a})\Big(\prod_{\substack{q|n \\ \text{prime}}} \nu_q(a)\Big)\overline{\sigma_a}^{-1} \in (\mathbf{Z}/M)[G_N^+].$$

Proof. Since

$$\xi_{L^+,n}{}^{D_n} \in [L^+(\mu_n)^\times/(L^+(\mu_n)^\times)^M]^{G_n}$$

(cf. [3, Appendix, Lemma 2.1]) and $\varphi_{\widehat{\mathcal{L}}}$ is a $\mathrm{Gal}(L(\mu_n)/\mathbf{Q})$-homomorphism, we have

$$D_n\varphi_{\widehat{\mathcal{L}}}(\xi_{L^+,n}) = \varphi_{\widehat{\mathcal{L}}}(\xi_{L^+,n}{}^{D_n}) \in (\mathbf{Z}/M)[\mathrm{Gal}(L(\mu_n)/\mathbf{Q})]^{G_n}.$$

Hence we can apply Proposition 7 to $\varphi_{\widehat{\mathcal{L}}}(\xi_{L^+,n})$. Then we have

$$\varphi_{\widehat{\mathcal{L}}}(\xi_{L^+,n}{}^{D_n}) = N_n \sum_{a\in(\mathbf{Z}/Nn)^\times} \nu_{\widehat{\mathcal{L}}^{\tau_a^{-1}}}(\xi_{L^+,n})\Big(\prod_{\substack{q|n \\ \text{prime}}} \nu_q(a)\Big)\sigma_a{}^{-1}.$$

By the injection $\mu_{Nn} \hookrightarrow (\mathcal{O}_{L(\mu_n)}/\widehat{\mathcal{Q}})^\times$ (cf. [6, Lemma 2.12]), we have the isomorphism of abelian groups:

$$(\mathcal{O}_{L(\mu_n)}/\widehat{\mathcal{L}})^\times \simeq (\mathbf{Z}/\ell)^\times\Big(\zeta_N\prod_{q|n}\zeta_q \mapsto g_\ell{}^{\frac{\ell-1}{Nn}}\Big).$$

Using this isomorphism, for any $a \in (\mathbf{Z}/Nn)^\times$ we get

$$\xi_{L^+,n}{}^{\tau_a} = \Big(\Big(\zeta_N\prod_{q|n}\zeta_q\Big)^a - 1\Big)\Big(\Big(\zeta_N{}^{-1}\prod_{q|n}\zeta_q\Big)^a - 1\Big) \equiv T_{n,\ell,a} \pmod{\widehat{\mathcal{L}}}.$$

Hence we have

$$\nu_{\widehat{\mathcal{L}}^{\tau_a^{-1}}}(\xi_{L^+,n}) = \nu_{\widehat{\mathcal{L}}}(\xi_{L^+,n}{}^{\tau_a}) = \nu_\ell(T_{n,\ell,a}).$$

We conclude

$$\varphi_{\widehat{\mathcal{L}}}(\xi_{L^+,n}{}^{D_n}) = N_n \sum_{a\in(\mathbf{Z}/Nn)^\times} \nu_\ell(T_{n,\ell,a})\Big(\prod_{\substack{q|n \\ \text{prime}}} \nu_q(a)\Big)\sigma_a{}^{-1}.$$

We consider the following diagram which is commutative by Lemma 10 (ii).

$$\begin{array}{llcl} \varphi_{\mathcal{L}'}: & X_{L,\ell}/X_{L,\ell}{}^M & \simeq & (\mathbf{Z}/M)[G_N] \\ & \downarrow & & \downarrow N_n \\ \varphi_{\widehat{\mathcal{L}}}: & (X_{L(\mu_n),\ell}/X_{L(\mu_n),\ell}{}^M)^{G_n} & \simeq & (\mathbf{Z}/M)[\mathrm{Gal}(L(\mu_n)/\mathbf{Q})]^{G_n} \\ & & & \| \\ & & & N_n(\mathbf{Z}/M)[G_N] \end{array}$$

From this diagram and $\kappa_{L^+,n} \equiv \xi_{L^+,n}{}^{D_n} \bmod (L^+(\mu_n)^\times)^M$ (Lemma 5), we get

$$\varphi_{\mathcal{L}'}(\kappa_{L^+,n}) = \sum_{a\in(\mathbf{Z}/Nn)^\times} \nu_\ell(T_{n,\ell,a})\Big(\prod_{\substack{q|n \\ \text{prime}}} \nu_q(a)\Big)\sigma_a{}^{-1}.$$

By Lemma 10 (i), we have

$$\begin{aligned} &\varphi_{\mathcal{L}}(\kappa_{L^+,n}{}^{N_{L/L^+}}) \\ &= \sum_{a\in(\mathbf{Z}/Nn)^\times} \nu_\ell(T_{n,\ell,a}))\Big(\prod_{\substack{q|n \\ \text{prime}}} \nu_q(a)\Big)\overline{\sigma_a}^{-1} \\ &= 2\sum_{a\in(\mathbf{Z}/Nn)^\times/\{\langle -1,1\rangle\}} \nu_\ell(T_{n,\ell,a}))\Big(\prod_{\substack{q|n \\ \text{prime}}} \nu_q(a)\Big)\overline{\sigma_a}^{-1}. \end{aligned}$$

Since $\kappa_{L^+,n}{}^{N_{L/L^+}} = \kappa_{L^+,n}{}^2$ and $p \neq 2$, we have

$$\varphi_{\mathcal{L}}(\kappa_{L^+,n}) = \sum_{a\in(\mathbf{Z}/Nn)^\times/\{\langle -1,1\rangle\}} \nu_\ell(T_{n,\ell,a})\Big(\prod_{\substack{q|n \\ \text{prime}}} \nu_q(a)\Big)\overline{\sigma_a}^{-1}.$$

□

4. The ideal class groups of abelian number fields whose degrees are prime to p. In this section, we reformulate the Kolyvagin-Rubin's structure theorem of A_K in the case $p \nmid [K:\mathbf{Q}]$, using the results of Section 3. Let $\chi : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \to \overline{\mathbf{Q}_p}^\times$ be a character of finite and prime-to-p order with conductor N, and K be the abelian number field corresponding to χ. If χ is the Teichmüller character ω or the trivial character $\mathbf{1}$, then we have $A_{K,\chi} = 0$. Hence we assume $\chi \neq \omega, \mathbf{1}$. For an odd character χ, we see that $B_{1,\chi^{-1}}$ (the generalized Bernoulli number) annihilates $A_{K,\chi}$. On the other hand, for an even character χ, F. Thaine [5] constructed annihilators of $A_{K,\chi}$ from cyclotomic units. Let E denote the group of units in K, and set $E_\chi = (E \otimes_{\mathbf{Z}} \mathbf{Z}_p)_\chi$. By the Dirichlet unit theorem, we have $E_\chi \simeq \mathcal{O}_\chi$. We define the χ-part $\mathcal{C}_\chi$ of the group of cyclotomic units to be the $\mathcal{O}_\chi$-module generated by $\xi_{K,1}{}^{e_\chi} = \{(\zeta_N - 1)(\zeta_N{}^{-1} - 1)\}^{N_{L^+/K}e_\chi} \in E_\chi$, where $N_{L^+/K}$ is the norm map. Let η be the power of p such that $E_\chi/\mathcal{C}_\chi \simeq \mathcal{O}_\chi/\eta\mathcal{O}_\chi$. We know from Thaine's result that η annihilates $A_{K,\chi}$. V. Kolyvagin [1] extended Thaine's method and showed $|\mathcal{O}_\chi/B_{1,\chi^{-1}}\mathcal{O}_\chi|$ (resp. $|E_\chi/\mathcal{C}_\chi|) = |A_{K,\chi}|$) (they were also known as consequences of the Iwasawa main conjecture [2]). Further, Kolyvagin's method determines the structure of $A_{K,\chi}$ by using higher annihilators of $A_{K,\chi}/B_K(n)_\chi$ defined in Section 2.

4.1. The minus part of the ideal class groups. For an odd character $\chi\,(\neq \omega)$, we use the Euler system of Gauss sums to determine the structure of $A_{K,\chi}$. For each $n \in \mathsf{S}$, choose the integer $b_n \in \mathsf{S}$ in Subsection 2.1 so that $\chi(b_n) - b_n \in \mathcal{O}_\chi{}^\times$. For any $n \in \mathsf{S}$, we define $\delta(n) \in (\mathbf{Z}/M)[G_N]$ as in Subsection 2.1, and let $d(n)$ be the largest power of p which divides $e_\chi \operatorname{Res}_{L/K}(\delta(n)) \in (\mathbf{Z}/M)[G]e_\chi \simeq \mathcal{O}_\chi/M$, where $\operatorname{Res}_{L/K} : (\mathbf{Z}/M)[G_N] \to (\mathbf{Z}/M)[G]$ is the natural restriction. Note that $d(1)$ is the largest power of p which divides $B_{1,\chi^{-1}}$. V. Kolyvagin showed that $e_\chi \operatorname{Res}_{L/K}(\delta(n))$ annihilates $A_{K,\chi}/B_K(n)_\chi$ (Proposition 3), and showed that the structure of $A_{K,\chi}$ is determined by $d(n)$'s (cf. V. Kolyvagin [1, Theorem 7] K. Rubin [4, Theorem 4.4]). From this and Theorem 9, we get the following theorem.

Theorem 14. *Let $\chi\,(\neq \omega)$ be an odd character whose order is finite and prime-to-p, K be the abelian number field corresponding to χ, and M be a power of p satisfying $M \geq |A_{K,\chi}|^2$. Write*

$$A_{K,\chi} \simeq \bigoplus_{i=1}^{m} \mathcal{O}_\chi/p^{e_i},\ e_1 \geq \cdots \geq e_m,$$

as $\mathcal{O}_\chi$-modules. Then we have

$$\begin{aligned} &e_{i+1} + \cdots + e_m \\ &= \min\Bigg\{\operatorname{ord}_p\Bigg(\sum_{\substack{a=1\\(a,nN)=1}}^{nN} \frac{a}{nN}\Bigg(\prod_{\substack{\ell | n\\ \text{prime}}} \nu_\ell(a)\Bigg)\chi^{-1}(a) \\ &\qquad \in \mathcal{O}_\chi/M\Bigg) \;\Bigg|\; n \in \mathsf{S}_i\Bigg\}, \end{aligned}$$

for any i with $0 \leq i \leq m-1$.

4.2. The plus part of the ideal class groups. For an even character $\chi\,(\neq \mathbf{1})$, we use the Euler system of cyclotomic units to determine the structure of $A_{K,\chi}$. In this case, we have $K = K^+$. We write $N = p^t N_0$ with $t = 0$ or 1 and $p \nmid N_0$. Let $n \in \mathsf{S}$ and $\mathcal{L}$ be a prime ideal of L^+ lying above a rational prime $\ell \equiv 1 \pmod{MnN_0}$. V. Kolyvagin [1, Theorem 5] showed that $e_\chi \operatorname{Res}_{L^+/K}(\psi_{\pi_\mathcal{L}}(\kappa_{L^+,n}))$ annihilates the class of $N_{L^+/K}(\mathcal{L})$ in $A_{K,\chi}/B_K(n)_\chi$ (Proposition 6) and that the structure of $A_{K,\chi}$ is determined by $\operatorname{ord}_p(e_\chi \operatorname{Res}_{L^+/K}(\psi_{\pi_\mathcal{L}}(\kappa_{L^+,n})))$'s (cf. V. Kolyvagin [1, Theorem 7]). From this and Lemma 11, Theorem 13, we get the following theorem.

Theorem 15. *Let $\chi\,(\neq \mathbf{1})$ be an even character whose order is finite and prime-to-p, K be the abelian number field corresponding to χ, and M be a power of p satisfying $M \geq |A_{K,\chi}|^2$. Write*

$$A_{K,\chi} \simeq \bigoplus_{i=1}^{m} \mathcal{O}_\chi/p^{e_i},\ e_1 \geq \cdots \geq e_m,$$

as $\mathcal{O}_\chi$-modules. Then we have

$$\begin{aligned} &e_{i+1} + \cdots + e_m \\ &= \min\Bigg\{\operatorname{ord}_p\Bigg(\sum_{a \in (\mathbf{Z}/Nn)^\times/\{\langle -1,1\rangle\}} \nu_\ell(T_{n,\ell,a}) \\ &\qquad \times \Bigg(\prod_{\substack{q|n\\ \text{prime}}} \nu_q(a)\Bigg)\chi^{-1}(a) \in \mathcal{O}_\chi/M\Bigg) \;\Bigg|\; n \in \mathsf{S}_i, \\ &\qquad \textit{rational primes } \ell \textit{ with } \ell \equiv 1 \pmod{MnN_0}\Bigg\}, \end{aligned}$$

for any i with $0 \leq i \leq m-1$.

Acknowledgments. I am very grateful to Prof. M. Kurihara and Prof. T. Fukuda for valuable advice.

References

[1] V. A. Kolyvagin, Euler systems, in *The Grothendieck Festschrift,* Vol. II, Progr. Math., 87, Birkhäuser Boston, Boston, 1990, pp. 435–483.

[2] B. Mazur and A. Wiles, Class fields of abelian extensions of **Q**, Invent. Math. **76** (1984), no. 2, 179–330.

[3] S. Lang, *Cyclotomic fields* I *and* II, Combined 2nd ed., Springer, New York, 1990, pp. 397–419.

[4] K. Rubin, Kolyvagin's system of Gauss sums, in *Arithmetic algebraic geometry* (*Texel, 1989*), 309–324 Progr. Math., 89, Birkhäuser Boston, Boston, 1991.

[5] F. Thaine, On the ideal class groups of real abelian number fields, Ann. of Math. (2) **128** (1988), no. 1, 1–18.

[6] L. C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Springer, New York, 1997.