ACTA ARITHMETICA
125.4 (2006)

Abelian p-class field towers over the cyclotomic $\mathbb{Z}_p$-extensions of imaginary quadratic fields

by

Keiji Okano (Tokyo)

1. Introduction. Let p be a prime number and F a finite algebraic number field. Denote the cyclotomic $\mathbb{Z}_p$-extension of F by F_∞. Iwasawa theory is centered on the study of various abelian pro-p-extensions over F_∞, especially the maximal unramified abelian pro-p-extension $L(F_\infty)$ of F_∞, to find the properties of the p-primary parts of the ideal class groups of subfields of F_∞. We will apply this theory to the study of the maximal unramified pro-p-extensions (called p-class field towers) of algebraic number fields. One of the classical problems in the theory of class field towers was the question whether the Galois groups of p-class field towers are always finite. Following Golod and Shafarevich's negative answer to this, many mathematicians showed examples of algebraic number fields with infinite class field towers. Another problem is what properties characterize the Galois groups of p-class field towers. Although this problem has been widely investigated, only a few results are known.

We consider the problem of *classifying the algebraic number fields which have abelian p-class field towers* (i.e., p-class field towers with abelian Galois groups). Note that abelian p-class field towers of finite algebraic number fields are finite extensions by class field theory. In this paper we classify the imaginary quadratic fields whose cyclotomic $\mathbb{Z}_p$-extensions have abelian p-class field towers in the case where p is odd. Some methods we use here are the same as those of Mizusawa and Ozaki [7] who treat the case where $p = 2$ (see §2). The main theorem is the following:

Theorem 1.1. *Let p be an odd prime number, k an imaginary quadratic field, and $A(k)$ the p-primary part of the ideal class group of k. Denote by $\widetilde{L}(k_\infty)$ the maximal unramified pro-p-extension of the cyclotomic $\mathbb{Z}_p$-extension k_∞ of k, and by λ_k the Iwasawa λ-invariant of k_∞/k. Then*

2000 *Mathematics Subject Classification*: Primary 11R23; Secondary 11R11, 11R37.

$\mathrm{Gal}(\widetilde{L}(k_\infty)/k_\infty)$ *is abelian if and only if one of the following two conditions holds*:

(i) $\lambda_k \le 1$,
(ii) $\lambda_k = 2$ *and* $A(k) = D(k)$,

where $D(k)$ *is the subgroup of* $A(k)$ *generated by the classes of powers of primes lying above* p.

REMARK. Note that $\mathrm{Gal}(\widetilde{L}(k_\infty)/k_\infty)$ is abelian if and only if all subfields of k_∞ have abelian p-class field towers, and that if $\mathrm{Gal}(\widetilde{L}(k_\infty)/k_\infty)$ is abelian, then $\mathrm{Gal}(\widetilde{L}(k_\infty)/k_\infty) \simeq \mathbb{Z}_p^{\oplus \lambda_k}$. Also condition (ii) implies that p splits in $k/\mathbb{Q}$. Moreover we see later that the structure of $\mathrm{Gal}(\widetilde{L}(k_\infty)/k_\infty)$ over the formal power series ring $\mathbb{Z}_p[[T]]$ is different in the cases where $A(k) = D(k) = 0$ and where $A(k) = D(k) \neq 0$ in (ii).

From now on, p is an odd prime number and we use the following notation for any algebraic number field F:

- $A(F)$: the p-primary part of the ideal class group of F,
- $\widetilde{L}(F)$: the maximal unramified pro-p-extension of F,
- $L(F)$: the maximal unramified abelian pro-p-extension of F,
- $\widetilde{G}(F) := \mathrm{Gal}(\widetilde{L}(F)/F)$,
- $X(F) := \mathrm{Gal}(L(F)/F) = \widetilde{G}(F)^{\mathrm{ab}}$,
- F_∞: the cyclotomic $\mathbb{Z}_p$-extension of F,
- F_n: the unique subfield of F_∞ with degree p^n over F,
- $\lambda_F := \dim_{\mathbb{Q}_p} X(F_\infty) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p$: the Iwasawa λ-invariant of F_∞/F.

2. Central p-class field theory. In this section we introduce the central p-class field theory, by means of which Mizusawa and Ozaki proved their result [7]. In the present paper we also follow their approach.

For any pro-p-group and its subgroups H_1, H_2, we use the notation $[H_1, H_2]$ for the closed normal subgroup generated by the elements of the form $[h_1, h_2] := h_1 h_2 h_1^{-1} h_2^{-1}$ $(h_i \in H_i)$. Let K be a finite p-extension of a finite algebraic number field k with Galois group $G := \mathrm{Gal}(K/k)$.

DEFINITION 2.1. We define the *genus p-class field* $\mathcal{G}(K/k)$ associated with K/k to be the compositum of K and the maximal abelian subextension of k in $L(K)$. The field $\mathcal{G}(K/k)$ coincides with the maximal abelian subextension of k in $L(K)$ if K/k itself is abelian. We also define the *central p-class field* $\mathcal{C}(K/k)$ associated with K/k to be the subfield of $L(K)$ fixed by $[\mathrm{Gal}(L(K)/k), \mathrm{Gal}(L(K)/K)]$.

By [3, Theorem 3.11, (3.24), Proposition 3.6], we have the exact sequence

$$(1)\quad 0 \to \frac{E(k)\cap N_{K/k}J_K}{E(k)\cap N_{K/k}K^\times} \to \mathcal{K}(K/k) \to \mathrm{Gal}(\mathcal{C}(K/k)/\mathcal{G}(K/k)) \to 0,$$

where $E(k)$ is the unit group of k, J_K is the idèle group of K, $N_{K/k}$ is the norm map and

$$\mathcal{K}(K/k) := \mathrm{Coker}(\widehat{H}^{-1}(G, J_K) \to \widehat{H}^{-1}(G, J_K/K^\times))$$

induced by the canonical map $J_K \to J_K/K^\times$. For each prime $\mathfrak{p}$ of k, we fix a prime of K lying above $\mathfrak{p}$ and denote by $Z_\mathfrak{p}$ its decomposition group in G. Then by Tate's duality theorem, we have the canonical isomorphisms

$$\widehat{H}^{-1}(G, J_K) \simeq \prod_\mathfrak{p} H_2(Z_\mathfrak{p}, \mathbb{Z}_p), \qquad \widehat{H}^{-1}(G, J_K/K^\times) \simeq H_2(G, \mathbb{Z}_p),$$

where the product in the first isomorphism is taken over all ramified primes of k. Therefore

$$(2)\qquad \mathcal{K}(K/k) \simeq \mathrm{Coker}\Big(\prod_\mathfrak{p} H_2(Z_\mathfrak{p}, \mathbb{Z}_p) \to H_2(G, \mathbb{Z}_p)\Big).$$

If K/k is an infinite pro-p-extension, by taking the projective limit with respect to the finite subextensions in K/k, we have an exact sequence similar to (1). Now, we apply the exact sequence (1) to an imaginary quadratic field k and the maximal unramified abelian p-extension $K = L(k_n)$ of k_n $(0 \le n \le \infty)$:

LEMMA 2.2. *Let $0 \le n \le \infty$ and let k be an imaginary quadratic field. Suppose that $\sqrt{-3} \notin k$ if $p = 3$. Then $\widetilde{G}(k_n)$ is abelian if and only if $\mathcal{K}(L(k_n)/k) = 0$.*

Proof. Note that $\mathcal{G}(L(k_n)/k) = L(k_n)$. In fact, the maximal abelian subfield F in $L(L(k_n))/k$ is contained in the maximal abelian subfield $L(k_n)$ in $L(L(k_n))/k_n$. By the assumption that $k \notin \sqrt{-3}$ if $p = 3$, we find that $\mathcal{K}(L(k_n)/k) = 0$ if and only if $\mathrm{Gal}(\mathcal{C}(L(k_n)/k)/L(k_n)) = 0$. The latter condition is equivalent to $L(L(k_n)) = L(k_n)$ and also equivalent to $\widetilde{L}(k_n) = L(k_n)$ by [3, Lemma 3.9]. ∎

By the above lemma, *the judgment whether $\widetilde{L}(k_n)/k_n$ is abelian or not is reduced to the computation of $\mathcal{K}(L(k_n)/k)$*. Next, we consider the commutative diagram of the minimal presentations

$$\begin{array}{ccccccccc} 1 & \longrightarrow & R & \longrightarrow & F & \longrightarrow & G_n & \longrightarrow & 1 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 1 & \longrightarrow & R_\mathfrak{p} & \longrightarrow & F_\mathfrak{p} & \longrightarrow & Z_{\mathfrak{p},n} & \longrightarrow & 1 \end{array}$$

of $G = G_n := \mathrm{Gal}(L(k_n)/k)$ and the decomposition groups $Z_{\mathfrak{p},n} \subset G_n$ by means of the free pro-p-groups F, $F_\mathfrak{p}$. Since the Hochschild–Serre spectral se-

quence yields isomorphisms $H_2(G_n,\mathbb{Z}_p)\simeq R\cap[F,F]/[R,F]$, $H_2(Z_{\mathfrak{p},n},\mathbb{Z}_p)\simeq R_\mathfrak{p}\cap[F_\mathfrak{p},F_\mathfrak{p}]/[R_\mathfrak{p},F_\mathfrak{p}]$, we see that $\mathcal{K}(L(k_n)/k)=0$ if and only if

$$\Phi:\ \prod_{\mathfrak{p}}\frac{R_\mathfrak{p}\cap[F_\mathfrak{p},F_\mathfrak{p}]}{(R_\mathfrak{p}\cap[F_\mathfrak{p},F_\mathfrak{p}])^p[R_\mathfrak{p},F_\mathfrak{p}]}\to\frac{R\cap[F,F]}{(R\cap[F,F])^p[R,F]}$$

is surjective by (2).

3. Preliminaries for the proof of Theorem 1.1. From now on throughout this paper, we suppose that k is an imaginary quadratic field and n is any non-negative integer. We put $X:=X(k_\infty)$, $X_n:=X(k_n)$ and $G_n:=\mathrm{Gal}(L(k_n)/k)$ for convenience. In this section we introduce the notation from Iwasawa theory and look for a necessary condition for $\widetilde{L}(k_\infty)/k_\infty$ to be abelian.

Put $\Gamma:=\mathrm{Gal}(k_\infty/k)$ and identify Γ with $\mathrm{Gal}(\mathbb{Q}_\infty/\mathbb{Q})$. Then $\Gamma_n:=\Gamma/\Gamma^{p^n}$ acts on X_n by inner automorphisms via the canonical isomorphism $X_n\simeq A(k_n)$ which is obtained by class field theory. Then $\varprojlim\mathbb{Z}_p[\Gamma_n]$ acts on the Galois group X, and hence the formal power series ring $\Lambda:=\mathbb{Z}_p[[T]]$ acts on X via the non-canonical isomorphism $\Lambda\simeq\varprojlim\mathbb{Z}_p[\Gamma_n]$ which is obtained by sending a fixed topological generator of Γ to $1+T$. It is well known that X is a finitely generated Λ-torsion Λ-module. Moreover, since k is an imaginary quadratic field and p is odd, there is an injective homomorphism $X\hookrightarrow\bigoplus_{i=1}^s\Lambda/(P_i)^{m_i}$ with finite cokernel, where the principal ideals (P_i) in Λ are prime ideals of height 1 and the structure of the right hand side is uniquely determined by p and k (for example, see [9, §13.3, 13.4]). Also by [2] we may take each P_i to be an irreducible distinguished polynomial. The polynomial $P(T):=\prod_{i=1}^s P_i^{m_i}$ is called the *characteristic polynomial* of X. Clearly $\deg P(T)=\lambda_k$. By considering X as the subgroup of $\mathrm{Gal}(L(k_\infty)/k)$, the Galois group X_n is described as

$$X_n\simeq X/\nu_n(T)Y,\qquad Y:=\mathrm{Gal}(L(k_\infty)/L(k)k_\infty),$$

where

$$\nu_n(T):=\frac{\omega_n(T)}{T},\qquad \omega_n(T):=(T+1)^{p^n}-1.$$

Remark. The above homomorphism $X\hookrightarrow\bigoplus_{i=1}^s\Lambda/(P_i)^{m_i}$ is not an isomorphism in general. But as we see later, we must determine precisely the Λ-module structure of X to compute $\widetilde{G}(k_\infty)$. It is one of the keys to the proof of our theorem.

We now look for a necessary condition for $\widetilde{L}(k_\infty)/k_\infty$ to be abelian. Denote the unit group of k_n by $E(k_n)$ and set

$$\mathcal{H}_n:=E(k_n)/E(k_n)\cap N_{L(k_n)/k_n}L(k_n)^\times,\qquad \mathcal{H}:=\varprojlim\mathcal{H}_n,$$

where the projective limit is taken with respect to the norm maps. Note that $\mathcal{H}_n$ is a p-group.

LEMMA 3.1. *Suppose that* $\sqrt{-3} \notin k$ *if* $p = 3$. *Then the module* $\mathcal{H}$ *is cyclic over* Λ.

Proof. First we prove that $E(k_n) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is cyclic over $\mathbb{Z}_p[\Gamma_n]$. Denote the unit group of $\mathbb{Q}_n$ by $E(\mathbb{Q}_n)$. Then by [9, Theorem 4.12], we obtain

$$E(k_n) \otimes_{\mathbb{Z}} \mathbb{Z}_p = E(\mathbb{Q}_n) \otimes_{\mathbb{Z}} \mathbb{Z}_p.$$

Therefore it is sufficient to prove that $E(\mathbb{Q}_n) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is cyclic over $\mathbb{Z}_p[\Gamma_n]$. Fix a primitive p^{n+1}th root of unity $\zeta_{p^{n+1}}$ and a primitive root g mod p^{n+1}. Consider the extension $\mathbb{Q}(\zeta_{p^{n+1}})^+/\mathbb{Q}$ and put $\Delta^+ := \mathrm{Gal}(\mathbb{Q}(\zeta_{p^{n+1}})^+/\mathbb{Q}_n)$, where $\mathbb{Q}(\zeta_{p^{n+1}})^+$ is the maximal real subfield of $\mathbb{Q}(\zeta_{p^{n+1}})$. Let $C^+_{p^{n+1}}$ be the group of cyclotomic units of $\mathbb{Q}(\zeta_{p^{n+1}})^+$, i.e. the group generated by -1 and the units ξ_a, where

$$\xi_a := \zeta_{p^{n+1}}^{(1-a)/2} \frac{1-\zeta_{p^{n+1}}^a}{1-\zeta_{p^{n+1}}}$$

and a satisfies $1 < a < \frac{1}{2}p^{n+1}$, $(a,p) = 1$. Then ξ_g generates $C^+_{p^{n+1}}/\{\pm 1\}$ as a module over $\mathbb{Z}[\Delta^+ \times \Gamma_n]$ by [9, Proposition 8.11], and therefore it also generates $C^+_{p^{n+1}} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ as a module over $\mathbb{Z}_p[\Delta^+ \times \Gamma_n]$. Taking the norm with respect to Δ^+, we find that $N_{\Delta^+}(C^+_{p^{n+1}} \otimes_{\mathbb{Z}} \mathbb{Z}_p)$ is generated by $N_{\Delta^+}\xi_g$ as a $\mathbb{Z}_p[\Gamma_n]$-module. On the other hand, by the computation in [9, §8.2], the index of the subgroup in $E(\mathbb{Q}_n)$ generated by $\{-1, N_{\Delta^+}(C^+_{p^{n+1}})\}$ equals the class number of $\mathbb{Q}_n$. Since the class number of $\mathbb{Q}_n$ is prime to p, we obtain

$$E(\mathbb{Q}_n) \otimes_{\mathbb{Z}} \mathbb{Z}_p = N_{\Delta^+}(C^+_{p^{n+1}} \otimes_{\mathbb{Z}} \mathbb{Z}_p).$$

This implies that $E(\mathbb{Q}_n) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is cyclic over $\mathbb{Z}_p[\Gamma_n]$, so that $E(k_n) \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is cyclic over $\mathbb{Z}_p[\Gamma_n]$. Combining these with the surjection $E(k_n) \otimes_{\mathbb{Z}} \mathbb{Z}_p \twoheadrightarrow \mathcal{H}_n$, we see that $\mathcal{H}_n$ is also cyclic over $\mathbb{Z}_p[\Gamma_n]$. Hence $\mathcal{H}$ is cyclic over Λ. ∎

Applying (1) in §2 to the unramified extension $L(k_n)/k_n$, we have the exact sequence

$$0 \to \mathcal{H}_n \to H_2(X_n, \mathbb{Z}_p) \to X_n^{(2)} \to 0,$$

where $X_n^{(2)}$ is the Galois group of $\mathcal{C}(L(k_n)/k_n)/L(k_n)$, since $\widehat{H}^{-1}(X_n, J_{L(k_n)}) = 0$ and $E(k_n) \subset N_{L(k_n)/k_n} J_{L(k_n)}$ by class field theory. Taking the projective limit, we also obtain the exact sequence

$$0 \to \mathcal{H} \to H_2(X, \mathbb{Z}_p) \to X^{(2)} \to 0, \qquad X^{(2)} := \varprojlim X_n^{(2)}.$$

PROPOSITION 3.2. *Suppose that* $\widetilde{G}(k_\infty)$ *is abelian* (*so that* $\widetilde{G}(k_\infty) = X$). *Then one of the following statements holds*:

(i) $\lambda_k \leq 1$, *in other words*, $\widetilde{G}(k_\infty)$ *is trivial or isomorphic to* $\mathbb{Z}_p$,

(ii) $2 \leq \lambda_k \leq 3$ *and* X *is cyclic as a* Λ*-module*,
(iii) $\lambda_k = 2$ *and* X *is generated by two elements as a* Λ*-module.*

Proof. If $p = 3$ and $k = \mathbb{Q}(\sqrt{-3})$, then the claim is trivial because $\widetilde{G}(k_\infty) = 0$. So we may discard this case. Suppose that $\widetilde{G}(k_\infty)$ is abelian. Then $X^{(2)} = 0$ and $X \wedge_{\mathbb{Z}_p} X \simeq H_2(X, \mathbb{Z}_p) \simeq \mathcal{H}$. Hence, by Lemma 3.1, there is a surjection $\Lambda \twoheadrightarrow X \wedge_{\mathbb{Z}_p} X$ which induces a surjection $\mathbb{F}_p[[T]] \twoheadrightarrow (X/pX) \wedge_{\mathbb{F}_p} (X/pX)$. We consider X/pX. Note that $X \simeq \mathbb{Z}_p^{\oplus \lambda_k}$ as $\mathbb{Z}_p$-modules since k is an imaginary quadratic field and p is odd. We can choose the representation

$$X/pX \simeq \bigoplus_{i=1}^{l} \mathbb{F}_p[[T]]/(T^{s_i}).$$

(If $X = 0$ we define $l = 1$, $s_1 = 0$.) Then $\lambda_k = \sum s_i$ and, as $\mathbb{F}_p[[T]]$-modules,

$$(X/pX) \wedge_{\mathbb{F}_p} (X/pX) \simeq \bigoplus_{i=1}^{l} (\mathbb{F}_p[[T]]/(T^{s_i}) \wedge_{\mathbb{F}_p} \mathbb{F}_p[[T]]/(T^{s_i})) \oplus \bigoplus_{i<j} (\mathbb{F}_p[[T]]/(T^{s_i}) \otimes_{\mathbb{F}_p} \mathbb{F}_p[[T]]/(T^{s_j})).$$

Therefore l must be 1 or 2. If the latter holds, we can easily check that X/pX must satisfy $X/pX \simeq \mathbb{F}_p[[T]]/(T) \oplus \mathbb{F}_p[[T]]/(T)$. Therefore $(X/pX) \wedge_{\mathbb{F}_p} (X/pX) \simeq \mathbb{F}_p$. This implies that statement (iii) holds by Nakayama's lemma. Assume that the former holds: $X/p \simeq \mathbb{F}_p[[T]]/(T^{\lambda_k})$. Then we obtain

$$\mathbb{F}_p[[T]]/(T^{\lambda_k}) \wedge_{\mathbb{F}_p} \mathbb{F}_p[[T]]/(T^{\lambda_k}) \simeq \mathbb{F}_p[[T]]/(T^{\lambda_k(\lambda_k-1)/2}). \tag{3}$$

Now we assume that $\lambda_k \geq 4$. Then, by the surjection $\mathbb{F}_p[[T]]/(T^{\lambda_k}) \twoheadrightarrow \mathbb{F}_p[[T]]/(T^4)$, the isomorphism (3) holds for $\lambda_k = 4$ and the kernel of multiplication by T on its left hand side must be isomorphic to $\mathbb{F}_p$. But this is a contradiction. In fact, if we write the fixed topological generator of Γ with respect to $1 + T \in \Lambda$ as γ and pick

$$1 \wedge \gamma,\ \gamma \wedge \gamma^2,\ \gamma^2 \wedge \gamma^3,\ \gamma^3 \wedge 1,\ 1 \wedge \gamma^2,\ \gamma \wedge \gamma^3$$

as an $\mathbb{F}_p$-basis of $\mathbb{F}_p[[T]]/(T^4) \wedge_{\mathbb{F}_p} \mathbb{F}_p[[T]]/(T^4)$, then the matrix of multiplication by T is

$$\begin{pmatrix} -1 & 1 & & & & \\ & -1 & 1 & & & \\ & & 5 & -1 & & -4 \\ -1 & 6 & & -1 & & -4 \\ & -4 & 4 & & 1 & -1 \end{pmatrix} \quad \text{(blank entries are zero)}$$

since $\gamma^4 \equiv 4\gamma^3 - 6\gamma^2 + 4\gamma - 1 \bmod T^4 = (\gamma - 1)^4$. The rank of the matrix

is $4 = 6 - 2$, so that the kernel of multiplication by T has dimension 2. This is a contradiction. Consequently, $\lambda_k \leq 3$ if $X/p \simeq \mathbb{F}_p[[T]]/(T^{\lambda_k})$. This implies that statement (i) or (ii) holds again by Nakayama's lemma. The isomorphism (3) holds if $\lambda_k \leq 3$ indeed. ∎

The same argument works on $X_0 \simeq A(k)$:

LEMMA 3.3. *If $\widetilde{G}(k)$ is abelian, then $A(k) = 0$ or $A(k)$ is cyclic.*

Proof. If $p = 3$ and $k = \mathbb{Q}(\sqrt{-3})$, the claim is trivial. So we may discard this case. Then $\mathcal{H}_0 = 0$ and $X_0^{(2)} = 0$. Therefore $H_2(X_0, \mathbb{Z}_p) = 0$. This implies that X_0 is trivial or cyclic. ∎

In the rest of this section we show Theorem 1.1 in the case where p is *non-splitting* in k. Recall $G_n := \mathrm{Gal}(L(k_n)/k)$.

LEMMA 3.4. *Suppose that p is non-splitting in $k/\mathbb{Q}$. Then $H_2(G_n, \mathbb{Z}_p) = 0$ if and only if $X_n = 0$ or X_n is cyclic.*

Proof. From the splitting exact sequence of pro-p-groups

$$1 \to X_n \to G_n \to \Gamma_n \to 1,$$

and also by [1] we obtain

$$H_2(G_n, \mathbb{Z}_p) \simeq H_2(\Gamma_n, \mathbb{Z}_p) \oplus H_1(\Gamma_n, X_n) \oplus H_2(X_n, \mathbb{Z}_p)_{\Gamma_n}. \tag{4}$$

We can easily check $H_2(\Gamma_n, \mathbb{Z}_p) = 0$ and $H_1(\Gamma_n, X_n) = 0$, since

$$\#H_1(\Gamma_n, X_n) = \#\widehat{H}^0(\Gamma_n, A(k_n)) = \#A(k_n)^{\Gamma_n}/\#A(k) = 1$$

by the genus formula (note that the lifting map $A(k) \to A(k_n)$ is injective by [9, Proposition 13.26]). On the other hand, by Nakayama's lemma,

$$\begin{aligned} H_2(X_n, \mathbb{Z}_p)_{\Gamma_n} = 0 &\Leftrightarrow (X_n \wedge X_n)/(p, T)(X_n \wedge X_n) = 0 \\ &\Leftrightarrow X_n \wedge X_n = 0 \\ &\Leftrightarrow X_n = 0 \text{ or } X_n \text{ is cyclic.} \end{aligned}$$

This completes the proof. ∎

PROPOSITION 3.5. *Let k be an imaginary quadratic field, and p an odd prime number. Suppose that p is non-splitting in $k/\mathbb{Q}$. Then $\widetilde{G}(k_\infty)$ is abelian if and only if $\lambda_k \leq 1$. More precisely, for any $0 \leq n < \infty$, $\widetilde{G}(k_n)$ is abelian if and only if $A(k_n) = 0$ or $A(k_n)$ is cyclic.*

Proof. Suppose that $\widetilde{G}(k_n)$ is abelian and let $Z_{\mathfrak{p},n} \subset G_n$ be the decomposition group of a prime of $L(k_n)$ lying above p. Then by Lemma 3.3, $A(k) = 0$ or $A(k)$ is cyclic. By Iwasawa's theorem [4], if $A(k) = 0$ then $X = 0$, since there is exactly one prime which ramifies, and it is totally ramified in k_∞/k. Hence we may assume that $A(k)$ is cyclic, in particular

$k \neq \mathbb{Q}(\sqrt{-3})$. Then again, since there is exactly one prime which ramifies, and it is totally ramified in k_∞/k, we have

$$X \simeq \Lambda/(P(T)) \quad \text{and} \quad X_n \simeq \Lambda/(P(T), \omega_n(T)).$$

This implies that the subgroup $D(k_n)$ of $A(k_n)$ generated by the class of a power of a prime lying above p is also trivial. In fact this follows from the injection $\varprojlim D(k_n) \hookrightarrow X^\Gamma = 0$. Therefore all primes lying above p split completely in $L(k_n)/k_n$. So the decomposition group $Z_{\mathfrak{p},n}$ coincides with the inertia group which is isomorphic to the cyclic group Γ_n. Hence $H_2(Z_{\mathfrak{p},n}, \mathbb{Z}_p) = 0$. Combining these with the considerations in §2, we obtain

$$H_2(G_n, \mathbb{Z}_p) = \mathcal{K}(L(k_n)/k) = 0.$$

The above lemma gives us the necessity part of the condition in the statement. On the other hand, the sufficiency part of the condition is trivial. ∎

4. Necessary condition in the splitting case. From now on, we study the case where p splits in k as $(p) = \mathfrak{pq}$. Note that the characteristic polynomial $P(T)$ of X is divided by T. In this section we continue to look for a necessary condition for $\widetilde{G}(k_\infty)$ to be abelian.

For any non-negative integer n, denote by $D(k_n)$ the subgroup of $A(k_n)$ generated by the classes of powers of primes lying above p in k_n. Note that $D(k_n)$ is a cyclic group, since the number of primes lying above p in k_n is exactly two and $\#A(\mathbb{Q}_n) = 1$.

LEMMA 4.1. *Suppose that p splits in k. Then*:

(i) $A(k_n)^{\Gamma_n} = i_n(A(k))D(k_n)$,
(ii) $D_\infty := \varprojlim D(k_n) \simeq X^\Gamma$,

where $i_n : A(k) \to A(k_n)$ is the (injective) lifting map for each n.

Proof. Let $I(k_n)$ (resp. $P(k_n)$) be the group of fractional ideals (resp. principal ideals) in k_n. Then the exact sequences of Γ_n-modules $0 \to E(k_n) \to k_n^\times \to P(k_n) \to 0$ and $0 \to P(k_n) \to I(k_n) \to I(k_n)/P(k_n) \to 0$ induce the exact sequence

$$I(k_n)^{\Gamma_n} \to (I(k_n)/P(k_n))^{\Gamma_n} \to H^2(\Gamma_n, E(k_n)) \to H^2(\Gamma_n, k_n^\times).$$

Hence

$$(I(k_n)/P(k_n))^{\Gamma_n}/(I(k_n)^{\Gamma_n}P(k_n)/P(k_n)) \simeq E(k) \cap N_{k_n/k}k_n^\times/N_{k_n/k}E(k_n),$$

which has the order prime to p. Therefore

$$\begin{aligned} A(k_n)^{\Gamma_n} &= (I(k_n)/P(k_n) \otimes \mathbb{Z}_p)^{\Gamma_n} = (I(k_n)/P(k_n))^{\Gamma_n} \otimes \mathbb{Z}_p \\ &= I(k_n)^{\Gamma_n}P(k_n)/P(k_n) \otimes \mathbb{Z}_p = I(k_n)^{\Gamma_n}P(k_n)/P(k_n) \cap A(k_n) \\ &= i_n(A(k))D(k_n). \end{aligned}$$

This implies that (i) holds. Taking the projective limit with respect to the norm maps of the exact sequence

$$0 \to D(k_n) \to A(k_n)^{\Gamma_n} \to i_n(A(k))/i_n(A(k)) \cap D(k_n) \to 0,$$

we obtain (ii) since we can check $\varprojlim A(k_n)^{\Gamma_n} \simeq X^{\Gamma}$ and $\varprojlim(i_n(A(k))) = 0$. ∎

Let $M(k)$ be the maximal abelian pro-p-extension which is unramified outside p, and $\mathfrak{X}(k)$ its Galois group: $\mathfrak{X}(k) := \mathrm{Gal}(M(k)/k)$. Then, since p splits in k, we see that $M(k) \subset L(k_\infty)$, $\mathrm{Gal}(M(k)/k_\infty) \simeq X/TX$ and the sequence

$$0 \to X/TX \to \mathfrak{X}(k) \to \Gamma \to 0 \tag{5}$$

is exact and splitting (for example, see [8, Proposition 1]). On the other hand, by class field theory, we have the exact sequence

$$0 \to \mathbb{Z}_p^{\oplus 2} \to \mathfrak{X}(k) \to A(k) \to 0 \tag{6}$$

and $\mathrm{rank}_{\mathbb{Z}_p} \mathfrak{X}(k) = [k : \mathbb{Q}]/2 + 1 = 2$.

Lemma 4.2. *Suppose that p splits in k. If $\lambda_k = 2$, then $P(T) \neq T^2$, i.e. $P(T) = T(T - \alpha)$ for some $0 \neq \alpha \in p\mathbb{Z}_p$.*

Proof. Assume that $P(T) = T^2$. Then X must be pseudo-isomorphic to $\Lambda/(T^2)$, in other words, there is an injection $X \hookrightarrow \Lambda/(T^2)$ with finite cokernel (see §3). In fact, if X is pseudo-isomorphic to $\Lambda/(T) \oplus \Lambda/(T)$, then $\mathrm{rank}_{\mathbb{Z}_p}(X/TX) = 2$, which contradicts (5) and $\mathrm{rank}_{\mathbb{Z}_p} \mathfrak{X}(k) = 2$. By [5] we can take the representation $X \simeq (T, p^m)/(T^2) \hookrightarrow \Lambda/(T^2)$ for some $m \geq 0$. Therefore we have $(X^{\Gamma} + TX)/TX \simeq (T)/(p^m T, T^2) \simeq \mathbb{Z}/p^m\mathbb{Z}$. By Lemma 4.1(ii), the quotient module $X/(X^{\Gamma} + TX)$ of X/TX corresponds to the Galois group of the maximal subextension $M'(k)$ of $M(k)/k_\infty$ which totally decomposes at all primes lying above p. Hence the above isomorphism implies that each prime lying above p has the decomposition group of finite order at $M(k)/k_\infty$. This contradicts [6, Lemma 3.1]. ∎

Proposition 4.3. *Suppose that p splits in k. If $\widetilde{G}(k_\infty)$ is abelian, then $A(k) = D(k)$.*

Proof. Denote by $L'(k)$ the fixed subfield of $L(k)$ under the Galois group corresponding to $D(k)$. Assume that $A(k) \neq D(k)$. Then $L'(k) \neq k$. We know $L'(k)$ is the maximal subextension of $L(k)/k$ which totally decomposes at all primes lying above p, so that p splits completely in the Galois extension $L'(k)/\mathbb{Q}$. This implies that the maximal abelian pro-p-extension $M(L'(k))$ of $L'(k)$ which is unramified outside p is contained in $L(L'(k)_\infty)$, which coincides with $L(k_\infty)$ by assumption. Since $L'(k)$ is a totally imaginary field

and also since Leopoldt's conjecture holds for $L'(k)$, we obtain

$$3 \geq \lambda_k \geq \operatorname{rank}_{\mathbb{Z}_p} \operatorname{Gal}(M(L'(k))/L'(k)_\infty) = [L'(k) : \mathbb{Q}]/2 + 1 - 1 \geq p.$$

Therefore we must have $p = 3$, $\lambda_k = 3$, $[A(k) : D(k)] = [L'(k) : k] = 3$. But in this case, $M(L'(k)) = L(L'(k)_\infty)$. Hence for the Galois groups, we obtain

$$X(L'(k)_\infty) = X(L'(k)_\infty)/TX(L'(k)_\infty),$$

and $X(L'(k)_\infty) = 0$ by Nakayama's lemma. This is a contradiction. Therefore $A(k) = D(k)$. ∎

The following proposition holds without the assumption that $\widetilde{G}(k_\infty)$ is abelian:

PROPOSITION 4.4. *Suppose that p splits in k and $A(k) = D(k)$. If $\lambda_k \leq 1$, then $\lambda_k = 1$. On the other hand, the following hold*:

(i) *If $\lambda_k \geq 2$ and $A(k) = 0$, then X is cyclic over Λ.*
(ii) *If $\lambda_k \geq 2$ and $A(k) = D(k) \neq 0$, then X is generated by two elements as a Λ-module.*

Proof. Note that X is generated by at most two elements as a Λ-module by (5) and (6). If $\lambda_k \leq 1$, it is clear that $\lambda_k = 1$ since p splits in k. Assume that $\lambda_k \geq 2$ and $A(k) = 0$. Then we have $X/TX \simeq \mathbb{Z}_p$ by (5) and (6). Therefore we obtain (i) by Nakayama's lemma. Next, assume that $A(k) = D(k) \neq 0$ and $X \simeq \Lambda/(P(T))$. Then

$$X/TX \simeq \Lambda/(T), \quad X/(X^\Gamma + TX) \simeq \Lambda/\left(\tfrac{P(T)}{T}, T\right) \neq 0 \quad (\text{since } \lambda_k \geq 2).$$

The second isomorphism implies that $M'(k) \neq k_\infty$, where $M'(k)$ is defined in the proof of Lemma 4.2. The set of all closed subgroups of $\mathbb{Z}_p \simeq X/TX$ is totally ordered by inclusion, so that $M'(k) \subset L(k)_\infty$ or $L(k)_\infty \subset M'(k)$ since both $L(k)_\infty$ and $M'(k)$ are contained in $M(k)$. Both cases contradict the fact that p does not split in $L(k)_\infty/k_\infty$, which follows from $A(k) = D(k)$. Therefore we obtain (ii). ∎

The above two propositions and Proposition 3.2 give a necessary condition for $\widetilde{G}(k_\infty)$ to be abelian: Suppose $\widetilde{G}(k_\infty)$ is abelian and $\lambda_k \geq 2$. Then $A(k) = D(k)$. If $A(k) = 0$, then X is cyclic over Λ and $2 \leq \lambda_k \leq 3$. If $A(k) = D(k) \neq 0$, then X is generated by two elements as a Λ-module and $\lambda_k = 2$. Moreover, X is then described as $X \simeq (T, p^m)/(P(T))$, $P(T) = T(T - \alpha)$, $0 < m \leq \operatorname{ord}_p(\alpha)$, by [5], where $\operatorname{ord}_p(\alpha)$ is the p-adic order of α.

In the rest of this paper, we will seek a sufficient condition. But before we start, we set the notation and assumptions, and compute the decomposition groups. Now, we still assume that k is an imaginary quadratic field such that an odd prime number p splits, but we remove the assumption that $\widetilde{G}(k_\infty)$ is abelian. The following cases will be considered:

Case I:

- $2 \le \lambda_k \le 3$, $A(k) = 0$,
- $X \simeq \Lambda/(P(T))$.

Case II:

- $\lambda_k = 2$, $A(k) = D(k) \neq 0$,
- $X \simeq (T, p^m)/(P(T))$, $P(T) = T(T-\alpha)$, $0 < m \le \mathrm{ord}_p(\alpha)$.

If $\lambda_k = 1$, then it is trivial that $\widetilde{G}(k_\infty)$ is abelian, so that it is sufficient to consider only the above two cases to obtain a sufficient condition. In each case we denote the decomposition group in G_∞ of a prime lying above $\mathfrak{p}$ (resp. $\mathfrak{q}$) by $Z_{\mathfrak{p},\infty}$ (resp. $Z_{\mathfrak{q},\infty}$), where $(p) = \mathfrak{pq}$ in k.

We define the notation $\widetilde{\varepsilon}$, $\widetilde{\gamma}$ as follows. If the conditions of Case I hold, we denote by $\widetilde{\varepsilon}$ a generator of X over Λ and by $\widetilde{\gamma} \in G_\infty$ a generator of the inertia group $I_{\mathfrak{p},\infty} \subset Z_{\mathfrak{p},\infty}$. On the other hand, if the conditions of Case II hold, then we can put $X = (T, p^m)/(P(T))\cdot\widetilde{\varepsilon}$, in other words, X is generated by $T\widetilde{\varepsilon}$, $p^m\widetilde{\varepsilon}$ over Λ. And as in Case I, denote by $\widetilde{\gamma} \in G_\infty$ a generator of the inertia group of a prime above $\mathfrak{p}$. Note that, in each case, $X^\Gamma \simeq \big(\frac{P(T)}{T}\big)/(P(T)) \simeq D_\infty$, so that a generator of X^Γ has the form $(\mathrm{unit})\frac{P(T)}{T}\widetilde{\varepsilon}$.

From now on, regarding X as a subset of G_∞, we write the operation of X multiplicatively instead of additively.

Lemma 4.5. *Let $\widetilde{\varepsilon}^{d(T)}$ be a generator of X^Γ. Then the decomposition groups $Z_{\mathfrak{p},\infty}$, $Z_{\mathfrak{q},\infty}$ are abelian and described as*

$$Z_{\mathfrak{p},\infty} = \langle\widetilde{\gamma}\rangle \times \langle\widetilde{\varepsilon}^{d(T)}\rangle,$$
$$Z_{\mathfrak{q},\infty} = \langle\widetilde{\gamma}\widetilde{\varepsilon}^{A(T)}\rangle \times \langle\widetilde{\varepsilon}^{d(T)}\rangle \quad (\textit{for some } A(T) \in \Lambda),$$

where $\langle x, y, \ldots\rangle$ stands for the pro-p-group generated by $x, y, \ldots$.

Proof. First, note that $Z_{\mathfrak{p},\infty} \cap X \lhd Z_{\mathfrak{p},\infty}$. In fact, this follows from $X \lhd G_\infty$. Since $Z_{\mathfrak{p},\infty} \cap X = X^\Gamma \simeq D_\infty$ and $Z_{\mathfrak{p},\infty}/Z_{\mathfrak{p},\infty} \cap X \simeq \Gamma = \langle\widetilde{\gamma}|_{k_\infty}\rangle$, we obtain the splitting exact sequence

$$1 \to X^\Gamma \to Z_{\mathfrak{p},\infty} \to \Gamma \to 1.$$

Hence $Z_{\mathfrak{p},\infty}$ is generated by $\widetilde{\gamma}$ and $\widetilde{\varepsilon}^{d(T)}$ as a pro-p-group. Since $I_{\mathfrak{p},\infty} \lhd Z_{\mathfrak{p},\infty}$ and $[G_\infty, G_\infty] \subset X$, we find

$$[\widetilde{\gamma}, \widetilde{\varepsilon}^{d(T)}] \in I_{\mathfrak{p},\infty} \cap [G_\infty, G_\infty] = 1.$$

Therefore $Z_{\mathfrak{p},\infty} = \langle\widetilde{\gamma}\rangle \times \langle\widetilde{\varepsilon}^{d(T)}\rangle$. Next, we choose a generator $\widetilde{\delta}$ of the inertia group of a prime lying above $\mathfrak{q}$ such that $\widetilde{\delta} \equiv \widetilde{\gamma} \bmod X$. Then there is some $A(T) \in \Lambda$ such that $\widetilde{\delta} = \widetilde{\gamma}\,\widetilde{\varepsilon}^{A(T)}$ by $G_\infty = I_{\mathfrak{p},\infty}X$. Following the same argument as above, we have $Z_{\mathfrak{q},\infty} = \langle\widetilde{\gamma}\widetilde{\varepsilon}^{A(T)}\rangle \times \langle\widetilde{\varepsilon}^{d(T)}\rangle$. ∎

5. Case I. We suppose that the conditions of Case I hold. We start with the computation of $A(T)$.

LEMMA 5.1. *By changing the generator $\widetilde{\varepsilon}$ if necessary, we have $A(T)=1$, $d(T) = P(T)/T$.*

Proof. (We use the method in the proof of Iwasawa's class number formula.) Recall $Y = \mathrm{Gal}(L(k_\infty)/L(k)k_\infty)$. Then $0 = A(k) = X/Y$, so that $Y = X \simeq \Lambda/(P(T))$. On the other hand, by [9, Lemma 13.15], we know that Y is generated by $\widetilde{\varepsilon}^{A(T)}$ and the module TX. Therefore $\Lambda = (A(T), T)$. This implies $A(T) \in \Lambda^\times$. We may assume that $A(T) = 1$ by changing $\widetilde{\varepsilon}^{A(T)}$ to $\widetilde{\varepsilon}$. Moreover, since the generator $\widetilde{\varepsilon}^{d(T)}$ of $X^\Gamma \simeq \big(\frac{P(T)}{T}\big)/(P(T))$ is determined up to multiplication by a unit, we may assume that $\widetilde{\varepsilon}^{d(T)} = \widetilde{\varepsilon}^{P(T)/T}$. ∎

In the following we determine whether $\widetilde{G}(k_n)$ is abelian or not for any fixed non-negative integer n, which is more refined and less complicated than whether $\widetilde{G}(k_\infty)$ is. Denote the projections of $\widetilde{\gamma}$, $\widetilde{\varepsilon}$ to G_n by $\widetilde{\gamma}_n$, $\widetilde{\varepsilon}_n$. Since $X_n \simeq X/\nu_n Y \simeq \Lambda/(P(T), \nu_n(T))$, we get $(X_n)_{\Gamma_n} \simeq \Lambda/(T, p^n) \simeq \mathbb{Z}/p^n\mathbb{Z}$. Hence

$$\begin{aligned} G_n^{\mathrm{ab}} &= \langle \widetilde{\gamma}_n \bmod [G_n, G_n]\rangle \times \langle \widetilde{\varepsilon}_n \bmod [G_n, G_n]\rangle \\ &\simeq \mathbb{Z}/p^n\mathbb{Z} \times \mathbb{Z}/p^n\mathbb{Z}. \end{aligned}$$

Thus, in particular, G_n is generated by two elements for $n \geq 1$.

LEMMA 5.2. *If $n \geq 1$, then $\dim_{\mathbb{F}_p} H_2(G_n, \mathbb{Z}_p)/pH_2(G_n, \mathbb{Z}_p) = 2$.*

Proof. By [1], we obtain the same isomorphism as (4). We see $H_1(\Gamma_n, X_n) \simeq \mathbb{Z}/p^n\mathbb{Z}$, since $A(k_n)^{\Gamma_n}/i_n(A(k)) = D(k_n) \simeq \mathbb{Z}/p^n\mathbb{Z}$ by Lemma 4.1(i) and the genus formula. Moreover, $H_2(X_n, \mathbb{Z}_p)_{\Gamma_n}/pH_2(X_n, \mathbb{Z}_p)_{\Gamma_n} = 0$ if and only if $X_n = 0$ or X_n is cyclic by Nakayama's lemma. But X_n is not cyclic for $n \geq 1$. In fact, by the isomorphism $X_1 \simeq \Lambda/(P(T), \nu_1(T))$, we have $X_1/pX_1 \simeq \Lambda/(T^{\lambda_k}, p) \simeq (\mathbb{Z}/p\mathbb{Z})^{\oplus\lambda_k} \neq \mathbb{Z}/p\mathbb{Z}$. On the other hand, the surjective map

$$\mathbb{F}_p \simeq (X/pX \wedge X/pX)_\Gamma \twoheadrightarrow (X_n/pX_n \wedge X_n/pX_n)_{\Gamma_n}$$

yields $\dim_{\mathbb{F}_p} H_2(X_n, \mathbb{Z}_p)_{\Gamma_n}/pH_2(X_n, \mathbb{Z}_p)_{\Gamma_n} \leq 1$. This completes the proof. ∎

Next, we give a minimal presentation of G_n by a free pro-p-group. Let $F := \langle \gamma, \varepsilon\rangle$ be a free pro-p-group of rank 2 and

$$R := \langle \gamma^{p^n}, \varepsilon^{\nu_n(\gamma-1)}, \varepsilon^{P(\gamma-1)}, [\varepsilon, \varepsilon^\gamma]\rangle_F,$$

where $\langle x, y, \ldots\rangle_F$ stands for the closed normal subgroup generated by $x, y, \ldots$ and their conjugates, and the action by polynomials is defined by the product of inner products such as

$$x^{a_n\gamma^n + \cdots + a_1\gamma + a_0} := x^{a_n\gamma^n} \cdots x^{a_1\gamma} x^{a_0} \qquad (a_i \in \mathbb{Z}_p).$$

LEMMA 5.3. *For arbitrary $z_1, z_2 \in \mathbb{Z}_p$, $i, j \in \mathbb{Z}$,*

(i) $[\varepsilon^{z_1\gamma^i}, \varepsilon^{z_2\gamma^j}]$ *is congruent to some power of* $[\varepsilon, \varepsilon^\gamma]$ *mod* $[R, F]$.

(ii) $[\varepsilon^{z_1\gamma^i}, \varepsilon^{z_2\gamma^j}] \equiv [\varepsilon, \varepsilon^\gamma]^{z_1 z_2 (j-i)} \bmod (R \cap [F,F])^p[R,F]$. *In particular, the left hand side is in* R.

Proof. We prove only (ii) because (i) is proven in the same way. The key point is $\lambda := \lambda_k \le 3$. Throughout the proof we treat things modulo $(R \cap [F,F])^p[R,F]$. First, we prove the case where $z_1 = z_2 = 1$, that is to say, we prove

$$R \ni [\varepsilon^{\gamma^i}, \varepsilon^{\gamma^j}] \equiv [\varepsilon, \varepsilon^\gamma]^{j-i}. \tag{7}$$

We may assume $i < j$. Moreover, we only have to prove

$$R \ni [\varepsilon^{\gamma^{-k}}, \varepsilon] \equiv [\varepsilon, \varepsilon^\gamma]^k \quad (k \ge 1). \tag{8}$$

If $k = \pm 1, 0$, then (8) is clear. Suppose that (8) holds for $1 \le i \le k$. Put $P(\gamma - 1) = \gamma^\lambda + p_{\lambda-1}\gamma^{\lambda-1} + \cdots + p_0$. Then since $\varepsilon^{P(\gamma-1)} \in R$, we have

$$\begin{aligned}
1 &\equiv [\varepsilon^{\gamma^{-k+(\lambda-1)}}, (\varepsilon^{-P(\gamma-1)})^{-1}] = [\varepsilon^{\gamma^{-k+(\lambda-1)}}, \varepsilon^{p_0}\varepsilon^{p_1\gamma}\cdots\varepsilon^{\gamma^\lambda}] \\
&\equiv [\varepsilon^{\gamma^{-k+(\lambda-1)}}, \varepsilon^{p_0}][\varepsilon^{\gamma^{-k+(\lambda-1)}}, \varepsilon^{p_1\gamma}\cdots\varepsilon^{\gamma^\lambda}] \\
&\equiv [\varepsilon^{\gamma^{-k+(\lambda-1)}}, \varepsilon]^{p_0}[\varepsilon^{\gamma^{-k+(\lambda-2)}}, \varepsilon^{p_1}\cdots\varepsilon^{\gamma^{\lambda-1}}]^\gamma \\
&\equiv [\varepsilon, \varepsilon^\gamma]^{p_0(k-(\lambda-1))}[\varepsilon^{\gamma^{-k+(\lambda-2)}}, \varepsilon^{p_1}\cdots\varepsilon^{\gamma^{\lambda-1}}] \\
&\equiv [\varepsilon, \varepsilon^\gamma]^{p_0(k-(\lambda-1))}[\varepsilon^{\gamma^{-k+(\lambda-2)}}, \varepsilon^{p_1}][\varepsilon^{\gamma^{-k+(\lambda-2)}}, \varepsilon^{p_2\gamma}\cdots\varepsilon^{\gamma^{\lambda-1}}] \\
&\equiv [\varepsilon, \varepsilon^\gamma]^{p_0(k-(\lambda-1))}[\varepsilon^{\gamma^{-k+(\lambda-2)}}, \varepsilon]^{p_1}[\varepsilon^{\gamma^{-k+(\lambda-3)}}, \varepsilon^{p_2}\cdots\varepsilon^{\gamma^{\lambda-2}}]^\gamma \\
&\equiv [\varepsilon, \varepsilon^\gamma]^{p_0(k-(\lambda-1))}[\varepsilon, \varepsilon^\gamma]^{p_1(k-(\lambda-2))}[\varepsilon^{\gamma^{-k+(\lambda-3)}}, \varepsilon^{p_2}\cdots\varepsilon^{\gamma^{\lambda-2}}] \\
&\cdots \\
&\equiv [\varepsilon, \varepsilon^\gamma]^{p_0(k-(\lambda-1))}[\varepsilon, \varepsilon^\gamma]^{p_1(k-(\lambda-2))}\cdots[\varepsilon, \varepsilon^\gamma]^{p_{\lambda-1}k}[\varepsilon^{\gamma^{-(k+1)}}, \varepsilon].
\end{aligned}$$

Therefore we obtain $[\varepsilon^{\gamma^{-(k+1)}}, \varepsilon] \in R$ and

$$[\varepsilon^{\gamma^{-(k+1)}}, \varepsilon] \equiv [\varepsilon, \varepsilon^\gamma]^{-p_0(k-(\lambda-1))-\cdots-p_{\lambda-1}k}.$$

If $\lambda = 2$, then $P(T) = (T+1)^2 + p_1(T+1) + p_0$. Consequently, $p_0 \equiv 1$, $p_1 \equiv -2 \pmod p$ and

$$[\varepsilon^{\gamma^{-(k+1)}}, \varepsilon] \equiv [\varepsilon, \varepsilon^\gamma]^{-(k-1)+2k} \equiv [\varepsilon, \varepsilon^\gamma]^{k+1}.$$

If $\lambda = 3$, then $P(T) = (T+1)^3 + p_2(T+1)^2 + p_1(T+1) + p_0$. Consequently, $p_0 \equiv -1$, $p_1 \equiv 3$, $p_2 \equiv -3 \pmod p$ and

$$[\varepsilon^{\gamma^{-(k+1)}}, \varepsilon] \equiv [\varepsilon, \varepsilon^\gamma]^{(k-2)-3(k-1)+3k} \equiv [\varepsilon, \varepsilon^\gamma]^{k+1}.$$

Therefore (8) holds for all $k \ge 1$. Finally, we prove the general case. Since any p-adic integer can be approximated by a positive integer, we may assume

that $1 \leq z_1, z_2 \in \mathbb{Z}$ (taking the limit later if necessary). Then by (7),

$$[\varepsilon^{z_1\gamma^i}, \varepsilon^{z_2\gamma^j}] \equiv [\varepsilon^{\gamma^i}, \varepsilon^{z_2\gamma^j}]^{z_1} \equiv [\varepsilon^{\gamma^i}, \varepsilon^{\gamma^j}]^{z_1 z_2} \equiv [\varepsilon, \varepsilon^{\gamma}]^{z_1 z_2 (j-i)}.$$

The desired result follows from this. ∎

Proposition 5.4. *The sequence of pro-p-groups*

$$1 \to R \to F \xrightarrow{\phi} G_n \to 1$$

is exact, where the map $\phi : F \to G_n$ *is given by* $\gamma \mapsto \widetilde{\gamma}_n$, $\varepsilon \mapsto \widetilde{\varepsilon}_n$. *In particular, this sequence is a minimal presentation of* G_n *for* $n \geq 1$.

Proof. It is clear that $R \subset \mathrm{Ker}(\phi)$ and ϕ is surjective, so that we have a surjective map $F/R \twoheadrightarrow G_n$ which induces surjective maps

$$F/[F,F]R = (F/R)^{\mathrm{ab}} \twoheadrightarrow G_n^{\mathrm{ab}}, \qquad [F,F]R/R = [F/R, F/R] \twoheadrightarrow [G_n, G_n].$$

We prove that they are isomorphisms. We know that $[F,F]$ is generated by $[\gamma, \varepsilon] = \varepsilon^{\gamma-1}$ and its conjugates. By Lemma 5.3 we find that $\varepsilon \in F$ acts on $[F,F]R/R$ trivially. In fact, this follows from the fact that, for $(\varepsilon^{\gamma-1})^{\gamma^k} \in [F,F]$,

$$\varepsilon(\varepsilon^{\gamma-1})^{\gamma^k}\varepsilon^{-1} = \varepsilon\varepsilon^{\gamma^{k+1}}\varepsilon^{-\gamma^k}\varepsilon^{-1} \equiv (\varepsilon^{\gamma-1})^{\gamma^k} \bmod R.$$

Therefore, using Lemma 5.3 again,

$$\begin{aligned}[F,F]R/R &= \langle (\varepsilon^{\gamma-1})^{F(\gamma-1)} \mid F(T) \in \Lambda \rangle R/R \\ &= \langle \varepsilon^{F(\gamma-1)} \mid F(T) \in (T, \nu_n(T))/(P(T), \nu_n(T)) \rangle R/R,\end{aligned}$$

since $\varepsilon^{\nu_n(\gamma-1)}, \varepsilon^{P(\gamma-1)} \in R$. Then we have the induced surjective map

$$[G_n, G_n] \simeq (T, \nu_n(T))/(P(T), \nu_n(T)) \twoheadrightarrow [F,F]R/R$$

and hence $[F,F]R/R \simeq [G_n, G_n]$. Finally, since $F/[F,F]R$ is generated by $\gamma \bmod [F,F]R$ and $\varepsilon \bmod [F,F]R$ which are annihilated by p^n, we have $\#(F/[F,F]R) \leq \#G_n^{\mathrm{ab}}$. Therefore $F/[F,F]R \simeq G_n^{\mathrm{ab}}$. ∎

Consider the subgroups $F_{\mathfrak{p}} := \langle \gamma, \varepsilon^{d(\gamma-1)} \rangle$, $F_{\mathfrak{q}} := \langle \gamma\varepsilon, \varepsilon^{d(\gamma-1)} \rangle$ of F. Put

$$\begin{aligned}R_{\mathfrak{p}} &:= \langle \gamma^{p^n}, (\varepsilon^{d(\gamma-1)})^{e_n}, [\gamma, \varepsilon^{d(\gamma-1)}] \rangle_{F_{\mathfrak{p}}}, \\ R_{\mathfrak{q}} &:= \langle (\gamma\varepsilon)^{p^n}, (\varepsilon^{d(\gamma-1)})^{e_n}, [\gamma\varepsilon, \varepsilon^{d(\gamma-1)}] \rangle_{F_{\mathfrak{q}}},\end{aligned}$$

where $e_n := \#(Z_{\mathfrak{p},n}/I_{\mathfrak{p},n})$. Then for $n \geq 1$ we have the minimal presentations

$$\begin{aligned}1 \to R_{\mathfrak{p}} \to F_{\mathfrak{p}} \to Z_{\mathfrak{p},n} \to 1, \\ 1 \to R_{\mathfrak{q}} \to F_{\mathfrak{q}} \to Z_{\mathfrak{q},n} \to 1\end{aligned}$$

of the decomposition groups $Z_{\mathfrak{p},n}$, $Z_{\mathfrak{q},n} \subset G_n$ by means of the free pro-p-groups $F_{\mathfrak{p}}$, $F_{\mathfrak{q}}$.

LEMMA 5.5.

(i) $R \cap [F,F]/[R,F] = \langle \varepsilon^{P(\gamma-1)}, [\varepsilon, \varepsilon^{\gamma}] \rangle [R,F]/[R,F]$,

(ii) $R_{\mathfrak{p}} \cap [F_{\mathfrak{p}}, F_{\mathfrak{p}}]/[R_{\mathfrak{p}}, F_{\mathfrak{p}}] = \langle [\gamma, \varepsilon^{d(\gamma-1)}] \rangle [R_{\mathfrak{p}}, F_{\mathfrak{p}}]/[R_{\mathfrak{p}}, F_{\mathfrak{p}}]$,

(iii) $R_{\mathfrak{q}} \cap [F_{\mathfrak{q}}, F_{\mathfrak{q}}]/[R_{\mathfrak{q}}, F_{\mathfrak{q}}] = \langle [\gamma\varepsilon, \varepsilon^{d(\gamma-1)}] \rangle [R_{\mathfrak{q}}, F_{\mathfrak{q}}]/[R_{\mathfrak{q}}, F_{\mathfrak{q}}]$.

Proof. (i) For any $x \in R \cap [F,F]/[R,F] \subset R$ there exist some $z_1, \ldots, z_4 \in \mathbb{Z}_p$ such that

$$x \equiv (\gamma^{p^n})^{z_1} \cdot (\varepsilon^{\nu_n(\gamma-1)})^{z_2} \cdot (\varepsilon^{P(\gamma-1)})^{z_3} \cdot [\varepsilon, \varepsilon^{\gamma}]^{z_4} \bmod [R,F].$$

Hence, since T divides $P(T)$,

$$(\gamma^{p^n})^{z_1} \cdot (\varepsilon^{\nu_n(\gamma-1)})^{z_2} \in R \cap [F,F] \subset [F,F].$$

This implies $\gamma^{p^n z_1} \varepsilon^{p^n z_2} \equiv 1 \bmod [F,F]$. Since γ and ε are linearly independent in $[F,F]$, we obtain $z_1 = z_2 = 0$. This implies $R \cap [F,F]/[R,F] \subset \langle \varepsilon^{P(\gamma-1)}, [\varepsilon, \varepsilon^{\gamma}] \rangle [R,F]/[R,F]$. The reverse inclusion is trivial. The other assertions are shown in the same way. ∎

REMARK. By Lemma 5.2, $\varepsilon^{P(\gamma-1)}$ and $[\varepsilon, \varepsilon^{\gamma}]$ are linearly independent modulo $(R \cap [F,F])^p [R,F]$ if $n \geq 1$, while $[\varepsilon, \varepsilon^{\gamma}] \in [R,F]$ if $n = 0$.

Now we are ready to determine whether $\widetilde{G}(k_n)$ is abelian or not.

PROPOSITION 5.6. *In Case I, the following equivalences hold*:

$$\lambda_k = 2 \;\Leftrightarrow\; \widetilde{G}(k_\infty) \text{ is abelian},$$

$$\lambda_k = 3 \;\Leftrightarrow\; \widetilde{G}(k_\infty) \text{ is not abelian}.$$

More precisely, $\widetilde{G}(k_n)$ is abelian if and only if $\lambda = 2$ or $n = 0$.

Proof. If $n = 0$ it is trivial that $\widetilde{G}(k)$ is abelian. Suppose that $n \geq 1$. First, note the above remark. By the above lemma, it is sufficient to determine whether the images of $[\gamma, \varepsilon^{d(\gamma-1)}]$ and $[\gamma\varepsilon, \varepsilon^{d(\gamma-1)}]$ under the map Φ of §2 generate $R \cap [F,F]/(R \cap [F,F])^p [R,F]$ which is generated by $\varepsilon^{P(\gamma-1)}$ and $[\varepsilon, \varepsilon^{\gamma}]$. Throughout the proof the notation $\equiv$ is used for $\equiv \bmod (R \cap [F,F])^p [R,F]$. Since

$$[\gamma, \varepsilon^{d(\gamma-1)}] \equiv \varepsilon^{P(\gamma-1)} [\varepsilon, \varepsilon^{\gamma}]^g, \quad [\varepsilon, \varepsilon^{d(\gamma-1)}] \equiv [\varepsilon, \varepsilon^{\gamma}]^h \quad (\text{note } d(T) = P(T)/T)$$

for some $g, h \in \mathbb{Z}_p$, we can check that Φ is surjective if and only if $h \in \mathbb{Z}_p^{\times}$. If $\lambda_k = 2$, we can put $P(T)/T = (T+1) + q_0$ and see $q_0 \equiv -1 \pmod p$. Therefore

$$[\varepsilon, \varepsilon^{d(\gamma-1)}] = [\varepsilon, \varepsilon^{\gamma+q_0}] = [\varepsilon, \varepsilon^{\gamma}],$$

which implies $h = 1$. So if $\lambda_k = 2$ then $\widetilde{G}(k_n)$ is abelian. On the other hand, if $\lambda_k = 3$, put $P(T)/T = (T+1)^2 + q_1(T+1) + q_0$. Then $q_0 \equiv 1, q_1 \equiv -2 \pmod p$. Therefore

$$[\varepsilon, \varepsilon^{d(\gamma-1)}] = [\varepsilon, \varepsilon^{\gamma^2} \varepsilon^{q_1\gamma} \varepsilon^{q_0}] \equiv [\varepsilon, \varepsilon^{\gamma^2}][\varepsilon, \varepsilon^{q_1\gamma}] \equiv 1,$$

which implies $h \in p\mathbb{Z}_p$. Hence if $\lambda_k = 3$ and $n \geq 1$, then $\widetilde{G}(k_n)$ is not abelian. This completes the proof. ∎

6. Case II. We suppose that the conditions of Case II hold. We start from the computation of $A(T)$ in the same way as in §5.

LEMMA 6.1. *By changing $\widetilde{\varepsilon}$ if necessary,*

$$A(T) = p^m + a_1(T-\alpha), \quad d(T) = P(T)/T = T - \alpha,$$

for some $a_1 \in \mathbb{Z}_p$.

Proof. The polynomial $A(T)$ is determined up to $P(T)$. So dividing by $P(T)$, we may assume $A(T) = a_0 + a_1(T-\alpha)$. Put $Y' := \mathrm{Gal}(L(k_\infty)/L'(k)k_\infty)$. Then $0 = A(k)/D(k) = X/Y'$, so that $Y' = X$. On the other hand, in the same way as in [9, Lemma 13.15], we see that Y' is generated by $\widetilde{\varepsilon}^{A(T)}$, $\widetilde{\varepsilon}^{P(T)/T}$ and the module TX. Therefore, since $m \leq \mathrm{ord}_p(\alpha)$, we find

$$(T, p^m) = (A(T), T-\alpha, T^2, p^m T) = (a_0, T-\alpha, \alpha p^m).$$

Now we prove $\mathrm{ord}_p(a_0) = m$. Assume that $\mathrm{ord}_p(a_0) > \mathrm{ord}_p(\alpha p^m)$. Then from $p^m \in (T-\alpha, \alpha p^m)$, we can put $p^m = (T-\alpha)f(T) + \alpha p^m g(T)$ for some $f(T), g(T) \in \Lambda$. Then we obtain $f(0) \in p^m\mathbb{Z}_p$, which contradicts $\alpha \in p\mathbb{Z}_p$. Therefore $\mathrm{ord}_p(a_0) \leq \mathrm{ord}_p(\alpha p^m)$ and $(T, p^m) = (a_0, T-\alpha)$. Assume that $\mathrm{ord}_p(a_0) > \mathrm{ord}_p(\alpha)$. Then from $p^m \in (a_0, T-\alpha)$, we can put $p^m = a_0 f'(T) + (T-\alpha)g'(T)$ for some $f'(T), g'(T) \in \Lambda$. Then we also obtain $g'(0) \in p^m\mathbb{Z}_p$, which yields a contradiction. Therefore $\mathrm{ord}_p(a_0) \leq \mathrm{ord}_p(\alpha)$. Consequently, we have $(T, p^m) = (a_0, T)$, $a_0 = up^m$ (for some $u \in \mathbb{Z}_p^\times$). Therefore if we change $\widetilde{\varepsilon}^u$ to $\widetilde{\varepsilon}$ and $u^{-1}a_1$ to a_1, the polynomial $A(T)$ is described as

$$A(T) = p^m + a_1(T-\alpha).$$

Finally, since we may change the generator $\widetilde{\varepsilon}^{d(T)}$ of X^Γ by multiplying it by a unit, we can assume that $\widetilde{\varepsilon}^{d(T)} = \widetilde{\varepsilon}^{P(T)/T}$. ∎

In the following, we show that $\widetilde{G}(k_\infty)$ is abelian. Since $G_\infty = X \rtimes \Gamma$, as in §5, we can easily check

$$\dim_{\mathbb{F}_p} H_2(G_\infty, \mathbb{Z}_p)/p \dim_{\mathbb{F}_p} H_2(G_\infty, \mathbb{Z}_p) = 2.$$

We give a minimal presentation of G_∞ by a free pro-p-group. Let $F := \langle \gamma, x, y \rangle$ be the subgroup of a free pro-p-group $\langle \gamma, \varepsilon \rangle$ of rank 2, where $x := \varepsilon^{p^m}$, $y := \varepsilon^{\gamma-1}$. Also let

$$R := \langle x^{\gamma-1} y^{-p^m}, (yx^\beta)^{\gamma-1}, [x,y] \rangle_F,$$

where $\beta := -\alpha/p^m \in \mathbb{Z}_p$.

LEMMA 6.2. *For arbitrary* $z_1, z_2 \in \mathbb{Z}_p$, $i, j \in \mathbb{Z}$,

$$[x^{z_1\gamma^i}, x^{z_2\gamma^j}] \equiv 1,$$
$$[y^{z_1\gamma^i}, y^{z_2\gamma^j}] \equiv 1,$$
$$[x^{z_1\gamma^i}, y^{z_2\gamma^j}] \equiv [x,y]^{z_1z_2} \bmod (R \cap [F,F])^p[R,F].$$

In particular, all the left hand sides are in R.

Proof. Throughout the proof $\equiv$ stands for $\equiv \bmod (R \cap [F,F])^p[R,F]$. The lemma follows from the following four congruences, which hold for arbitrary $z_1, z_2 \in \mathbb{Z}_p$, $j \geq 0$:

$$[x^{z_1}, x^{z_2\gamma^j}] \equiv 1, \quad [x^{z_1}, y^{z_2\gamma^j}] \equiv [x,y]^{z_1z_2},$$
$$[y^{z_1}, y^{z_2\gamma^j}] \equiv 1, \quad [y^{z_1}, x^{z_2\gamma^j}] \equiv [x,y]^{-z_1z_2}.$$

We only show the congruences in the first column because the other two are proved in the same way. We may assume that $0 \leq z_1, z_2 \in \mathbb{Z}$ because any p-adic integer can be approximated by positive integers. If $j = 0$, it is trivial that $[x^{z_1}, x^{z_2}] = 1$. And $[x^{z_1}, y^{z_2}] \equiv [x,y]^{z_1z_2}$ follows from the fact that $[x^{z_1}, y^{z_2}]$ can be decomposed as the product of z_1z_2 conjugates of $[x,y]$. Suppose that the congruences in the first column hold for $0 \leq i \leq j$. Then since

$$[x, y^{p^m\gamma^j}x^{\gamma^j}] \equiv [x, y^{p^m\gamma^j}][x, x^{\gamma^j}] \equiv [x,y]^{p^m} \equiv 1 \in R,$$

we obtain $[x, x^{\gamma^{j+1}}] = [x, (x^{\gamma-1}y^{-p^m})^{\gamma^j}y^{p^m\gamma^j}x^{\gamma^j}] \equiv 1$. Hence

$$[x^{z_1}, x^{z_2\gamma^{j+1}}] \equiv [x, x^{\gamma^{j+1}}]^{z_1z_2} \equiv 1.$$

Using this result, we have

$$[x, y^{\gamma^j}x^{\beta\gamma^j}x^{-\beta\gamma^{j+1}}] \equiv [x, y^{\gamma^j}][x, x^{\beta\gamma^j}][x, x^{-\beta\gamma^{j+1}}] \equiv [x,y] \in R.$$

Therefore $[x, y^{\gamma^{j+1}}] = [x, ((yx^\beta)^{\gamma-1})^{\gamma^j}y^{\gamma^j}x^{\beta\gamma^j}x^{-\beta\gamma^{j+1}}] \equiv [x,y]$. Hence

$$[x^{z_1}, y^{z_2\gamma^{j+1}}] \equiv [x, y^{\gamma^{j+1}}]^{z_1z_2} \equiv [x,y].$$

This completes the proof of the congruences in the first column. ∎

PROPOSITION 6.3. *The sequence of pro-p-groups*

$$1 \to R \to F \xrightarrow{\phi} G_\infty \to 1$$

is exact, where the map $\phi : F \to G_\infty$ *is given by* $\gamma \mapsto \widetilde{\gamma}$, $x \mapsto \widetilde{\varepsilon}^{p^m}$, $y \mapsto \widetilde{\varepsilon}^T$.

Proof. It is clear that $R \subset \mathrm{Ker}(\phi)$ and ϕ is surjective, so that we have the surjective map $F/R \twoheadrightarrow G_\infty$, which yields the exact commutative diagram

$$\begin{array}{ccccccccc}
1 & \longrightarrow & K/R & \longrightarrow & F/R & \longrightarrow & F/K & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \phi'} & & \downarrow{\scriptstyle \phi} & & \downarrow & & \\
1 & \longrightarrow & X & \longrightarrow & G_\infty & \longrightarrow & \Gamma & \longrightarrow & 1
\end{array}$$

where $K := \langle x, y, R\rangle_F$. The quotient F/K is a cyclic group generated by γ. In fact, we can easily check $x\gamma x^{-1} \equiv \gamma$, $y\gamma y^{-1} \equiv \gamma \bmod K$. Therefore the surjective map $F/K \to \Gamma$ is an isomorphism. The map $\phi' : K/R \to X$ is clearly surjective, so that the problem is reduced to showing that ϕ' is an isomorphism. We see from Lemma 6.2 that K/R is an abelian group generated over $\mathbb{Z}_p$ by

$$x,\ x^{\gamma},\ x^{\gamma^2},\ \ldots,\ y,\ y^{\gamma},\ y^{\gamma^2},\ \ldots$$

since $[x, y] \in R$. But since $x^{\gamma} \equiv y^{p^m}x$, $y^{\gamma} \equiv yx^{\beta}x^{-\beta\gamma} \equiv y^{1+\alpha} \bmod R$, we see that K/R is generated by the two elements x, y. Hence $\operatorname{rank}_{\mathbb{Z}_p}(K/R) \le 2 = \operatorname{rank}_{\mathbb{Z}_p} X$. It follows that ϕ' is an isomorphism. ∎

Consider the subgroups $F_{\mathfrak{p}} := \langle \gamma, yx^{\beta}\rangle$, $F_{\mathfrak{q}} := \langle \gamma x(yx^{\beta})^{a_1}, yx^{\beta}\rangle$ of F and put

$$R_{\mathfrak{p}} := \langle [\gamma, yx^{\beta}]\rangle_{F_{\mathfrak{p}}}, \qquad R_{\mathfrak{q}} := \langle [\gamma x(yx^{\beta})^{a_1}, yx^{\beta}]\rangle_{F_{\mathfrak{q}}}.$$

Then we have the minimal presentations

$$1 \to R_{\mathfrak{p}} \to F_{\mathfrak{p}} \to Z_{\mathfrak{p},\infty} \to 1,$$
$$1 \to R_{\mathfrak{q}} \to F_{\mathfrak{q}} \to Z_{\mathfrak{q},\infty} \to 1$$

of $Z_{\mathfrak{p},\infty}$, $Z_{\mathfrak{q},\infty}$ by means of the free pro-p-groups $F_{\mathfrak{p}}$, $F_{\mathfrak{q}}$.

Lemma 6.4.

(i) $R \cap [F, F]/[R, F] = \langle (yx^{\beta})^{\gamma-1}, [x, y]\rangle [R, F]/[R, F]$,
(ii) $R_{\mathfrak{p}} \cap [F_{\mathfrak{p}}, F_{\mathfrak{p}}]/[R_{\mathfrak{p}}, F_{\mathfrak{p}}] = \langle [\gamma, yx^{\beta}]\rangle [R_{\mathfrak{p}}, F_{\mathfrak{p}}]/[R_{\mathfrak{p}}, F_{\mathfrak{p}}]$,
(iii) $R_{\mathfrak{q}} \cap [F_{\mathfrak{q}}, F_{\mathfrak{q}}]/[R_{\mathfrak{q}}, F_{\mathfrak{q}}] = \langle [\gamma x(yx^{\beta})^{a_1}, yx^{\beta}]\rangle [R_{\mathfrak{q}}, F_{\mathfrak{q}}]/[R_{\mathfrak{q}}, F_{\mathfrak{q}}]$.

Proof. The same as in Lemma 5.5. ∎

Now we are ready to show that $\widetilde{G}(k_\infty)$ is abelian.

Proposition 6.5. *In Case II, $\widetilde{G}(k_\infty)$ is abelian. Therefore $\widetilde{G}(k_n)$ is abelian for any $n \ge 0$.*

Proof. Throughout the proof, $\equiv$ stands for $\equiv \bmod (R \cap [F, F])^p[R, F]$. By the above lemma, as in §5, it is sufficient to show that the images of $[\gamma, yx^{\beta}]$ and $[\gamma x(yx^{\beta})^{a_1}, yx^{\beta}]$ under the map Φ of §2 generate $R \cap [F, F]/(R \cap [F, F])^p[R, F]$ which is generated by $(yx^{\beta})^{\gamma-1}$ and $[x, y]$. Since

$$[\gamma, yx^{\beta}] = (yx^{\beta})^{\gamma-1}, \qquad [\gamma x(yx^{\beta})^{a_1}, yx^{\beta}] \equiv [x, yx^{\beta}][\gamma, yx^{\beta}],$$

we see that Φ is always surjective. In fact, by Lemma 6.2, we have $[x, yx^{\beta}] \equiv [x, y]$. This implies that $[\gamma, yx^{\beta}]$ and $[\gamma x(yx^{\beta})^{a_1}, yx^{\beta}]$ generate $R \cap [F, F]/(R \cap [F, F])^p[R, F]$. This completes the proof. ∎

Examples. We give examples of the case where $p = 3$ splits in the imaginary quadratic field k with $\lambda_k = 2$. Let $k := \mathbb{Q}(\sqrt{-14})$. Then $\lambda_k = 2$ and $A(k) = D(k) = 0$ (Case I). Therefore k_∞ has abelian 3-class field tower

and its Galois group is cyclic over Λ. Let $k := \mathbb{Q}(\sqrt{-107})$. Then $\lambda_k = 2$ and $A(k) = D(k) \neq 0$ (Case II). Therefore k_∞ has abelian 3-class field tower and its Galois group is generated by two elements as a Λ-module. On the other hand, if $k = \mathbb{Q}(\sqrt{-461})$ (resp. $k = \mathbb{Q}(\sqrt{-974})$), then $\lambda_k = 2$ and $X(k_\infty)$ is cyclic (resp. generated by two elements) over Λ. Since $A(k) \neq D(k)$, we conclude that k_∞ has non-abelian 3-class field tower.

Acknowledgements. The author would like to express his gratitude to Dr. Yasushi Mizusawa for a number of helpful suggestions.

References

[1] L. Evens, *The Schur multiplier of a semi-direct product*, Illinois J. Math. 16 (1972), 166–181.

[2] B. Ferrero and L. C. Washington, *The Iwasawa invariant μ_p vanishes for abelian number fields*, Ann. of Math. (2) 109 (1979), 377–395.

[3] A. Fröhlich, *Central Extensions, Galois Groups, and Ideal Class Groups of Number Fields*, Contemp. Math. 24, Amer. Math. Soc., Providence, RI, 1983.

[4] K. Iwasawa, *A note on class numbers of algebraic number fields*, Abh. Math. Sem. Univ. Hamburg 20 (1956), 257–258.

[5] M. Koike, *On the isomorphism classes of Iwasawa modules associated to imaginary quadratic fields with $\lambda = 2$*, J. Math. Sci. Univ. Tokyo 6 (1999), 371–396.

[6] J. Minardi, *Iwasawa modules for $\mathbb{Z}_p^d$-extensions of algebraic number fields*, thesis, Harvard Univ., 1986.

[7] Y. Mizusawa and M. Ozaki, *Abelian 2-class field towers over the cyclotomic $\mathbb{Z}_2$-extensions of imaginary quadratic fields*, preprint.

[8] M. Ozaki, *The class group of $\mathbb{Z}_p$-extensions over totally real number fields*, Tohoku Math. J. (2) 49 (1997), 431–435.

[9] L. C. Washington, *Introduction to Cyclotomic Fields*, 2nd ed., Grad. Texts in Math. 83, Springer, New York, 1997.

Department of Mathematical Sciences
School of Science and Engineering
Waseda University
Okubo, Shinjuku-ku
Tokyo 169-8555, Japan
E-mail: okano@suou.waseda.jp

Received on 3.4.2006 (5175)