A Remark on Boston's Question Concerning the Existence of Unramified p-Extensions. II

By Akito NOMURA

Department of Mathematics, Kanazawa University

(Communicated by Shokichi IYANAGA, M. J. A., Jan. 13, 1997)

§1. Introduction. Fontaine and Mazur have conjectured that there does not exist an everywhere unramified p-adic representation of the absolute Galois group of a number field with infinite image.

Conjecture 1 (Fontaine-Mazur). If K is a number field, and $\rho: \mathrm{Gal}(\bar{K}/K) \to \mathrm{GL}_n(\boldsymbol{Q}_p)$ an everywhere unramified representation, then the image of ρ is finite.

This conjecture has been studied in [1], [2] and [3].

Definition. A pro-p group G is called powerful if $G/\overline{G^p}$ (resp. $G/\overline{G^4}$) is abelian for p odd (resp. $p = 2$), where the line denotes topological closure.

Conjecture 1 is equivalent to the following (cf. [1]).

Conjecture 2 (Fontaine-Mazur-Boston). If K is a number field and M/K is an unramified pro-p extension of infinite degree, then the Galois group $\mathrm{Gal}(M/K)$ is not powerful.

In [1], Boston pointed out that this conjecture is closely related to the existence of unramified p-extensions of a certain type, and introduced the following question.

Question (Boston [1]). Let K be a number field, p an odd prime, and $K(p)$ its p-class field. Suppose that the class number of $K(p)$ is divisible by p. Then is there always an everywhere unramified extension M of degree p of $K(p)$ such that M is Galois over K and $exp(\mathrm{Gal}(M/K)) = exp(\mathrm{Gal}(K(p)/K))$? The "*exp*" stands for the exponent of the group.

In general, the answer to this question is in the negative. A counter example noted by Lemmermeyer can be found in Boston [2].

Concerning this question, Boston [1] noticed that the truth of the Fontaine-Mazur conjecture implies an affirmative answer, when K has an infinite p-class field tower. In the previous paper [5], we proved some sufficient conditions for the answer to Boston's question for K and p to be affirmative. In this article, we shall prove another sufficient condition for the answer to the question to be affirmative, and study the structure of $\mathrm{Gal}(K^{ur}(p)/K)$, where $K^{ur}(p)/K$ is the maximal unramified pro-p extension.

§2 Main theorem. Let k be an algebraic number field and p an odd prime. For a Galois extension L/k, we denote by $Ram(L/k)$ the set of primes of k which are ramified in L/k. For a finite set S of primes of k, let $B_k(S) = \{\alpha \in k^* \mid (\alpha) = \mathfrak{a}^p$ for some ideal $\mathfrak{a}$ of k, and $\alpha \in {k_{\mathfrak{q}}}^p$ for any $\mathfrak{q}$ of $S\}$.

Theorem. Assume that the Galois extension F/k satisfies the following conditions (1), (2), and (3).

(1) $\mathrm{Gal}(F/k)$ is isomorphic to $\boldsymbol{Z}/p\boldsymbol{Z} \times \boldsymbol{Z}/p\boldsymbol{Z}$.

(2) Any prime of k above p is unramified, and any prime contained in $Ram(F/k)$ is decomposed in F/k.

(3) $B_k(Ram(F/k)) = k^{*p}$.

If K/k is a p-extension such that $F \cap K = k$ and that $Ram(F/k) \subset Ram(K/k)$, then the answer to Boston's question for K and p is affirmative.

We need the lemma below.

Lemma ([4; Corollary of Theorem 4]). Let F/k be a Galois extension with the Galois group isomorphic to $\boldsymbol{Z}/p\boldsymbol{Z} \times \boldsymbol{Z}/p\boldsymbol{Z}$. Assume that $B_k(Ram(F/k)) = k^{*p}$. Then the following condisions (1) and (2) are equivalent.

(1) There exists a Galois extension $L/F/k$ such that $\mathrm{Gal}(L/k)$ is isomorphic to

$$H = \langle x, y \mid x^p = y^p = z^p = 1, \\ yx = xyz, xz = zx, yz = zy \rangle$$

and that L/F is unramified.

(2) Any prime of k which is ramified in F/k is decomposed in F/k.

Remark. H is a non-abelian p-group of order p^3, and the exponent of H is p. Therefore

H is not powerful.

Proof of theorem. By the preceding lemma, there exists a Galois extension $L/F/k$ such that $\mathrm{Gal}(L/k)$ is isomorphic to $H = \langle x, y \mid x^p = y^p = z^p = 1, yx = xyz, xz = zx, yz = zy \rangle$ and that L/F is unramified. By the assumption $F \cap K = k$ $Ram(F/k) \subset Ram(K/k)$, LK/K is unramified and $\mathrm{Gal}(LK/K)$ is isomorphic to H. Let $M = K(p)KL$. Then $M/K(p)/K$ is unramified and the degree $[M : K(p)]$ is equal to p. Since $\mathrm{Gal}(M/K)$ is isomorphic to a subgroup of the direct product $\mathrm{Gal}(K(p)/K) \times \mathrm{Gal}(LK/K)$, $exp(\mathrm{Gal}(M/K)) = exp(\mathrm{Gal}(K(p)/K))$. This completes the proof.

Remark. If k is the rational number field $\boldsymbol{Q}$, then the condition (3) of Theorem is always satisfied.

Example. Let k_1 (resp. k_2) be the subfield of $\boldsymbol{Q}(\zeta_7)$ (resp. $\boldsymbol{Q}(\zeta_{181})$) such that $[k_1 : \boldsymbol{Q}] = 3$ (resp. $[k_2 : \boldsymbol{Q}] = 3$). Since $7^{60} \equiv 1 (\mathrm{mod}\ 181)$, $181^2 \equiv 1 (\mathrm{mod}\ 7)$, $k = \boldsymbol{Q}$ $F = k_1 k_2$ $p = 3$ satisfies the assumption (1), (2), and (3).

Notation. For a number field K, $K^{(0)} = K$ and $K^{(n+1)}$ is the maximal unramified elementary abelian p-extension of $K^{(n)}$.

Corollary. Let K/k be a p-extension which satisfies the same assumption in Theorem. If M/K is unramified p-extension and M containes $K^{(2)}$, then the Galois group $\mathrm{Gal}(M/K)$ is not powerful.

Proof. The proof is by contradiction. Assume that $\mathrm{Gal}(M/K)$ is powerful. By the proof of Theorem, there exists an unramified Galois extension L_1/K such that the Galois group $\mathrm{Gal}(L_1/K)$ is isomorphic to $H = \langle x, y \mid x^p = y^p = z^p = 1, yx = xyz, xz = zx, yz = zy \rangle$. We claim that if G is powerful and N is an open normal subgroup, then G/N is also powerful. Since $M \supset K^{(2)} \supset L_1$, $\mathrm{Gal}(L_1/K) = \mathrm{Gal}(M/K) / \mathrm{Gal}(L_1/K)$ is powerful. This is a contradiction. We have completed the proof of Corollary.

References

[1] N. Boston: Some cases of the Fontaine-Mazur conjecture. J. Number Theory, **42**, 285–291 (1992).

[2] N. Boston: Some cases of the Fontaine-Mazur conjecture. II (preprint).

[3] F. Hajir: On the growth of p-class groups in p-class field towers. Calf. Inst. Tech. (preprint).

[4] A. Nomura: On the existence of unramified p-extensions. Osaka J. Math., **28**, 55–62 (1991).

[5] A. Nomura: A remark on Boston's question concerning the existence of unramified p-extensions. J. Number Theory, **58**, 66–70 (1996).