A note on the $\mathbf{Z}_p \times \mathbf{Z}_q$-extension over $\mathbf{Q}$

By Kuniaki Horie

Department of Mathematics, Tokai University, 1117, Kitakaname, Hiratsuka, Kanagawa 259-1292

(Communicated by Shigefumi Mori, M. J. A., June 12, 2001)

Abstract: Let S be a non-empty set of prime numbers; $1 \leq |S| \leq \infty$. Let $\mathbf{Q}^S$ denote the abelian extension of the rational field $\mathbf{Q}$ whose Galois group over $\mathbf{Q}$ is topologically isomorphic to the direct product of the additive groups of l-adic integers for all $l \in S$. In this note, we shall give simple examples of S such that, for some $l \in S$, the Hilbert l-class field over $\mathbf{Q}^S$ is a nontrivial extension of $\mathbf{Q}^S$. Our results imply that, if S contains 2, 3, 31, and 73, then there exists an unramified cyclic extension of degree $2263 = 31 \cdot 73$ over $\mathbf{Q}^S$.

Key words: Hilbert class field; Iwasawa theory.

We shall suppose that all algebraic extensions over the rational field $\mathbf{Q}$ are contained in the complex field. For each prime number l, let $\mathbf{Z}_l$ denote the ring of l-adic integers. As in the above abstract, let S be a non-empty set of prime numbers and let $\mathbf{Q}^S$ denote the unique abelian extension over $\mathbf{Q}$ such that the Galois group $\mathrm{Gal}(\mathbf{Q}^S/\mathbf{Q})$ is topologically isomorphic to the additive group of the direct product $\prod_{l \in S} \mathbf{Z}_l$. Clearly, for any finite algebraic number field k in $\mathbf{Q}^S$, there exists a tower

$$k = \boldsymbol{k}_1 \subset \cdots \subset \boldsymbol{k}_n \subset \boldsymbol{k}_{n+1} \subset \cdots \subset \mathbf{Q}^S$$

of intermediate fields of $\mathbf{Q}^S/k$ with finite degrees such that

$$\bigcup_{n=1}^{\infty} \boldsymbol{k}_n = \mathbf{Q}^S$$

and that, for each positive integer n, some prime ideal of $\boldsymbol{k}_n$ is fully ramified in $\boldsymbol{k}_{n+1}$. We thus obtain:

Lemma 1. *Let k be a finite algebraic number field in $\mathbf{Q}^S$, and k' a finite unramified Galois extension over k. Then not only the composite $\mathbf{Q}^S k'$ is an unramified Galois extension over $\mathbf{Q}^S$ but the restriction map $\mathrm{Gal}(\mathbf{Q}^S k'/\mathbf{Q}^S) \to \mathrm{Gal}(k'/k)$ is an isomorphism.*

Now let p be any prime number in S: $p \in S$. For each algebraic number field K and for each prime number l, let $H_l(K)$ denote the Hilbert l-class field over K, namely, the maximal unramified abelian l-extension over K. Then, in particular,

$$H_p(\mathbf{Q}^S) = \bigcup_k H_p(k),$$

with k ranging over the finite algebraic number fields in $\mathbf{Q}^S$ (cf. [7]). Therefore, both [5] and [6] show us that

$$H_p(\mathbf{Q}^S) = \mathbf{Q}^S \quad \text{when } |S| = 1, \text{ i.e., } S = \{p\}.$$

We assume henceforth that S contains a prime number q other than p:

$$\{p, q\} \subseteq S, \quad q \neq p.$$

The $\mathbf{Z}_p \times \mathbf{Z}_q$-extension over $\mathbf{Q}$ is nothing but $\mathbf{Q}^S$ for the case $S = \{p, q\}$. Let L_q denote the unique subfield of $\mathbf{Q}^S$ of degree q. Then L_q is contained in $\mathbf{Q}(\cos(\pi/q^2))$, the maximal real subfield of the $2q^2$-th cyclotomic field. Let E_q denote the unit group of L_q, $R_{p,q}$ the p-adic regulator of L_q, and $\mathbf{Q}_p$ the field of p-adic numbers. We understand that $R_{p,q}$ is an element of a fixed algebraic closure Ω_p of $\mathbf{Q}_p$, considering L_q to be a subfield of Ω_p by means of a fixed embedding $L_q \to \Omega_p$. Furthermore, $R_{p,q} \neq 0$ as [1] implies. Let C_q denote the group of circular units of L_q: namely, in the case $q = 2$, let C_q be the subgroup of E_q generated by -1 and $1 + \sqrt{2}$; in the case $q > 2$, let C_q be the subgroup of E_q generated by -1 and by all conjugates, over $\mathbf{Q}$, of the norm of

$$\frac{\sin(r\pi/q^2)}{\sin(\pi/q^2)} = \frac{e^{r\pi i/q^2} - e^{-r\pi i/q^2}}{e^{\pi i/q^2} - e^{-\pi i/q^2}}$$

for the extension $\mathbf{Q}(\cos(\pi/q^2))/L_q$, where r is a primitive root modulo q^2 (obviously, C_q does not depend on the choice of r). Then, in Ω_p, the p-adic regulator for C_q is defined in the usual way. We de-

1991 Mathematics Subject Classification. Primary 11R20; Secondary 11R23.

note it by $R^*_{p,q}$. On the other hand, the group index of C_q in E_q equals the class number of L_q (cf. [3]). Hence

$$|R^*_{p,q}|_p[H_p(L_q):L_q] = |R_{p,q}|_p \neq 0,$$

where $|\cdot|_p$ denotes the normalized absolute value on Ω_p; $|p|_p = p^{-1}$. Put

$$a_q(p) = p^{1-q}|R^*_{p,q}|_p^{-1} = p^{1-q}[H_p(L_q):L_q]|R_{p,q}|_p^{-1}.$$

Note that the following three conditions are equivalent:

(i) p is completely decomposed in L_q,
(ii) $L_q \subset \mathbf{Q}_p$,
(iii) $p^{q-1} \equiv 1 \pmod{q^2}$ or $p^2 \equiv 1 \pmod{16}$ according as $q > 2$ or $q = 2$.

We easily see that, if one of the above conditions is satisfied, then $R_{p,q}$ belongs to $p^{q-1}\mathbf{Z}_p$ so that

$$a_q(p) = p^u$$

with some integer $u \geq 0$.

Let us first consider the case $q = 2$.

Lemma 2. *Assume that*

$$q = 2, \quad p^2 \equiv 1 \pmod{16}.$$

Then $H_p(\mathbf{Q}^S)$ contains an extension of degree $a_2(p)$ over $\mathbf{Q}^S$.

Proof. We have

$$\mathbf{Q}(\sqrt{2}) = L_q \subset \mathbf{Q}_p$$

by the assumption. As readily verified,

$$a_2(p) = p^{-1}|(1+\sqrt{2})^{p-1} - 1|_p^{-1}.$$

Let F be the unique intermediate field of $\mathbf{Q}^S/\mathbf{Q}(\sqrt{2})$ with degree $a_2(p)$ over $\mathbf{Q}(\sqrt{2})$. Proposition 1 of [2] then implies that $a_2(p)$ divides $[H_p(F):F]$ (cf. also [8, Theorem 1.1]). This fact, together with Lemma 1, proves the present lemma. □

Proposition 1. *If 2 and 31 belong to S, then $H_{31}(\mathbf{Q}^S)$ is a nontrivial extension of $\mathbf{Q}^S$.*

Proof. As $31^2 \equiv 1 \pmod{16}$, we let $p = 31$ in the assumption of Lemma 2. It is not difficult to see that

$$(1+\sqrt{2})^{30} - 1 \equiv 31^2 \cdot 2\sqrt{2} \pmod{31^3}$$

in the ring of algebraic integers in $\mathbf{Q}(\sqrt{2})$. Hence we have $a_2(31) = 31$ and the proposition is proved by Lemma 2. □

Remark. One knows from [4] that, in the case $q = 2$, there exists no example of $p \neq 31$ satisfying

$$p^2 \equiv 1 \pmod{16}, \quad p \mid a_2(p), \quad p < 20000.$$

We next consider the case $q > 2$.

Lemma 3. *Assume that*

$$p > 2, \quad q > 2, \quad p^{q-1} \equiv 1 \pmod{q^2}.$$

Then $H_p(\mathbf{Q}^S)$ contains an extension of degree $a_q(p)$ over $\mathbf{Q}^S$.

Proof. In fact, Theorem 1.1 of [8] combined with [1] implies that there exists an intermediate field k of $\mathbf{Q}^S/L_q$ with finite degree for which

$$a_q(p) \mid [H_p(k):k]. \qquad \square$$

Proposition 2. *If 3 and 73 belong to S, then $H_{73}(\mathbf{Q}^S)$ is a nontrivial extension of $\mathbf{Q}^S$.*

Proof. Since $73^2 \equiv 1 \pmod 9$, we let $(p,q) = (73,3)$ in the assumption of Lemma 3. Note that $L_3 = \mathbf{Q}(\cos(\pi/9))$, 2 is a primitive root modulo 9, and

$$\frac{\sin(2\pi/9)}{\sin(\pi/9)} = 2\cos\frac{\pi}{9}$$

is a zero of the polynomial $x^3 - 3x - 1$. Let ε_1, ε_2, ε_3 be the conjugates of $2\cos(\pi/9)$ over $\mathbf{Q}$ so that

$$(\varepsilon_1-\varepsilon_2)^2(\varepsilon_2-\varepsilon_3)^2(\varepsilon_3-\varepsilon_1)^2 = 81.$$

Solving the congruence $x^3 - 3x - 1 \equiv 0 \pmod{73^3}$ and rearranging $\varepsilon_1, \varepsilon_2, \varepsilon_3$ if necessary, we then obtain

$$\begin{aligned} \varepsilon_1 &\equiv 157183 \pmod{73^3}, \\ \varepsilon_2 &\equiv 257651 \pmod{73^3} \end{aligned}$$

in $\mathbf{Z}_{73}$. These yield

$$\begin{aligned} 144\log\varepsilon_1 &\equiv 2(\varepsilon_1^{72}-1) - (\varepsilon_1^{72}-1)^2 \\ &\equiv 4511\cdot 73 \pmod{73^3}, \\ 144\log\varepsilon_2 &\equiv 2(\varepsilon_2^{72}-1) - (\varepsilon_2^{72}-1)^2 \\ &\equiv 2106\cdot 73 \pmod{73^3}, \end{aligned}$$

where log denotes the 73-adic logarithmic function. On the other hand, ε_1 and ε_2 represent a basis of the free abelian group $C_3/\{\pm 1\}$, and

$$\sigma(\varepsilon_2) = \varepsilon_3 = \varepsilon_1^{-1}\varepsilon_2^{-1}$$

for the $\sigma \in \mathrm{Gal}(L_3/\mathbf{Q})$ with $\sigma(\varepsilon_1) = \varepsilon_2$. Therefore, in view of

$$4511(-4511-2106) - 2106^2 \equiv 31\cdot 73 \pmod{73^2},$$

we know that

$$|R^*_{73,3}|_{73} = 73^{-3}, \quad \text{i.e.,} \quad a_3(73) = 73.$$

Hence the proposition follows from Lemma 3. □

With the help of Kida's UBASIC and a personal computer, we have checked for the case $q = 3$ that there exists no example of $p \neq 73$ which satisfies

$$p^2 \equiv 1 \pmod 9), \quad p \mid a_3(p), \quad p < 10000.$$

It would be interesting to continue our discussion under the assumption $q \geq 5$, but here we only add the following

Remark. In the case $|S| < \infty$, $H_p(\mathbf{Q}^S)$ is a finite extension of $\mathbf{Q}^S$ if and only if Greenberg's conjecture for the $\mathbf{Z}_p$-extension over k is true for every finite algebraic number field k in $\mathbf{Q}^S$.

Acknowledgement. The author thanks his wife Mitsuko for her kind assistance in the process of computation.

References

[1] Brumer, A.: On the units of algebraic number fields. Mathematika, **14**, 121–124 (1967).

[2] Fukuda, T., and Komatsu, K.: On the λ invariants of $\mathbf{Z}_p$-extensions of real quadratic fields. J. Number Theory, **23**, 238–242 (1986).

[3] Hasse, H.: Über die Klassenzahl abelscher Zahlkörper. Academie, Berlin (1952); Springer, Berlin (1985).

[4] Hatada, K.: Mod 1 distribution of Fermat and Fibonacci quotients and values of zeta functions at $2-p$. Comment. Math. Univ. St. Pauli, **36**, 41–51 (1987).

[5] Fröhlich, A.: On the absolute class-group of abelian fields. J. London Math. Soc., **29**, 211–217 (1954).

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

[7] Iwasawa, K.: On Γ-extensions of algebraic number fields. Bull. Amer. Math. Soc., **65**, 183–226 (1959).

[8] Taya, H.: On p-adic zeta functions and $\mathbf{Z}_p$-extensions of certain totally real number fields. Tohoku Math. J., **51**, 21–33 (1999).