Non-norm-Euclidean fields in basic $\boldsymbol{Z}_l$-extensions

By Kuniaki HORIE*) and Mitsuko HORIE**)

(Communicated by Masaki KASHIWARA, M.J.A., Dec. 14, 2015)

Abstract: We shall deal with infinite towers of cyclic fields of genus number 1 in which a prime number $l \geq 5$ is totally ramified. Our main result states that, if m is a positive divisor of $l-1$ less than $(l-1)/2$, then for any positive integer n, the cyclic field of degree ml^n with conductor l^{n+1} is not norm-Euclidean. In particular, it follows that, for any positive integer n, the (real) cyclic field of degree l^n with conductor l^{n+1} is not norm-Euclidean and that the (imaginary) cyclic field of degree 14 with conductor 49, whose class number is known to equal 1, is not norm-Euclidean.

Key words: Norm-Euclidean field; cyclic field; class number; genus number; basic $\boldsymbol{Z}_l$-extension.

1. Introduction. Given any finite extension F of the rational field $\boldsymbol{Q}$ in the complex field $\boldsymbol{C}$, we denote by N_F the norm map from F to $\boldsymbol{Q}$. The field F will be called norm-Euclidean if, for every pair (α, β) of algebraic integers in F with $\beta \neq 0$, there exists an algebraic integer γ in F such that $|N_F(\alpha - \gamma\beta)| < |N_F(\beta)|$. As is well known, when F is norm-Euclidean, the class number of F equals 1. We call F a cyclic field if F is a cyclic extension over $\boldsymbol{Q}$.

Among interesting results of McGown [Mc], Theorem 4.1 of the paper implies that, for any prime number $l \geq 5$, the cyclic field of degree l with conductor l^2 is not norm-Euclidean. The proof of the theorem, which is partly based on McGown's variant [Mc, Lemma 4.2] of Heilbronn's criterion (cf. [H]), enables us to extend the above assertion to the following.

Proposition 1. *Let l be a prime number not less than 5, and m a positive divisor of $l-1$ less than $(l-1)/2$. Then, for any positive integer n, the cyclic field of degree ml^n with conductor l^{n+1} is not norm-Euclidean.*

This result particularly implies that, if l is a prime number not less than 5, then for any positive integer n, the cyclic field of degree l^n with conductor l^{n+1} is not norm-Euclidean. On the other hand, the real cyclic field of degree 2^n with conductor 2^{n+2} for each $n \in \{1, 2, 3\}$ and the cyclic field of degree 3 with conductor 9 are known to be norm-Euclidean (cf. Cerri [C], Cohn and Deutsch [CD], Davenport [D]). Furthermore, certain real cyclic fields whose conductors are prime-powers, including all non-norm-Euclidean cyclic fields given by Proposition 1 for $m = 1$, are expected to have class number 1; indeed, there exist various known results that let us hold such expectations (cf. Bauer [B], Buhler, Pomerance and Robertson [BPR], [HH], van der Linden [Li], Masley [Ma], Miller [Mi], etc.). Proposition 1 seems remarkable in view of the facts mentioned above.

Throughout the rest of the present paper, we fix a prime number $l \geq 5$ and a positive divisor m of $l-1$. Let k be the cyclic field of degree m with conductor dividing l. We denote by $\boldsymbol{Z}_l$ the ring of l-adic integers, and by $\boldsymbol{B}_\infty$ the unique abelian extension of $\boldsymbol{Q}$ in $\boldsymbol{C}$ whose Galois group over $\boldsymbol{Q}$ is topologically isomorphic to the additive group of $\boldsymbol{Z}_l$. For each positive integer n, let $\boldsymbol{B}_n$ denote the subfield of $\boldsymbol{B}_\infty$ of degree l^n. It then follows that not only is l totally ramified in the compositum $k\boldsymbol{B}_n$ (in $\boldsymbol{C}$) but $k\boldsymbol{B}_n$ is the cyclic field of degree ml^n with conductor l^{n+1}. Naturally k and $k\boldsymbol{B}_n$ for all positive integers n form an increasing sequence of the intermediate fields between k and $k\boldsymbol{B}_\infty$ other than $k\boldsymbol{B}_\infty$. For each finite extension E of $\boldsymbol{Q}$ in $\boldsymbol{C}$, the compositum $E\boldsymbol{B}_\infty$ is called the basic $\boldsymbol{Z}_l$-extension over E, the extension $E\boldsymbol{B}_\infty/E$ being an abelian extension with Galois group topologically isomorphic to the additive group of $\boldsymbol{Z}_l$. Thus Proposition 1 can be restated as follows: *If $m < (l-1)/2$, then $k\boldsymbol{B}_n$ is not norm-Euclidean for any positive integer n, namely, no finite extension of k other than k in*

2010 Mathematics Subject Classification. Primary 11A05; Secondary 11R20, 11R29.

*) 3-9-2-302 Sengoku, Bunkyo-ku, Tokyo 112-0011, Japan.
**) Department of Mathematics, Ochanomizu University, 2-1-1 Otsuka, Bunkyo-ku, Tokyo 112-8610, Japan.

doi: 10.3792/pjaa.92.23

the basic $\boldsymbol{Z}_l$-extension over k is norm-Euclidean.

2. Preliminaries and proof. For the cyclic field $\boldsymbol{B}_1$ of degree l with conductor l^2, let $\mathcal{N}$ denote the set of the absolute norms of all non-zero integral ideals of $\boldsymbol{B}_1$. To prove Proposition 1, we first give a modification of [Mc, Lemma 4.2]:

Lemma 1. *Let m' be a positive divisor of $l-1$, and k' a cyclic field of degree m' in which l is totally ramified in the case $m'>1$. Assume that there exists a positive integer $a<l$ satisfying $a \notin \mathcal{N}$, $l-a \notin \mathcal{N}$, and $a \equiv g^{m'} \pmod{l}$ with some integer g. Then $k'\boldsymbol{B}_n$ is not norm-Euclidean for any positive integer n.*

Proof. Let n be any positive integer, and let $F' = k'\boldsymbol{B}_n$. For a contradiction, we suppose that F' is norm-Euclidean, whence the class number of F' is equal to 1. The condition on k' implies that l is totally ramified in F'. Let $\mathfrak{l}$ be the prime ideal of F' dividing l, and λ an algebraic integer in F' generating the principal ideal $\mathfrak{l}$. Since F' is norm-Euclidean, there exists an algebraic integer γ in F' which satisfies $|N_{F'}(g-\gamma\lambda)| < |N_{F'}(\lambda)| = l$. We put $\alpha = g - \gamma\lambda$, so that we have $\alpha \equiv g \pmod{\mathfrak{l}}$. Hence $N_{F'}(\alpha) \equiv g^{m'l^n} \pmod{\mathfrak{l}}$, i.e., $N_{F'}(\alpha) \equiv g^{m'l^n} \equiv g^{m'} \pmod{l}$. Consequently, $N_{F'}(\alpha) \equiv a \pmod{l}$. Since $|N_{F'}(\alpha)| < l$ and $0<a<l$, it follows that $N_{F'}(\alpha) = a$ or $N_{F'}(\alpha) = a - l$. We thus deduce that a or $l-a$ coincides with the absolute norm of the norm for $F'/\boldsymbol{B}_1$ of the principal ideal of F' generated by α. This contradicts the assumption of the lemma. □

Lemma 2. *Every integer b in $\mathcal{N}$ less than l fulfills $b^{l-1} \equiv 1 \pmod{l^2}$.*

Proof. If a prime divisor v of an integer a in $\mathcal{N}$ is not decomposed in $\boldsymbol{B}_1$, then v^l or l divides a according to whether v remains prime or is ramified in $\boldsymbol{B}_1$, so that one has $a \geq l$. Further, for any prime number $v' \neq l$, the order of v' modulo l^2 is equal to the order of the decomposition group of v' with respect to the cyclotomic extension $\boldsymbol{Q}(e^{2\pi i/l^2})/\boldsymbol{Q}$. Hence, for every integer b in $\mathcal{N}$ with $1<b<l$, every prime divisor w of b is decomposed in $\boldsymbol{B}_1$ and therefore satisfies $w^{l-1} \equiv 1 \pmod{l^2}$. In addition, it is obvious that $1 \in \mathcal{N}$ and $1^{l-1} \equiv 1 \pmod{l^2}$. □

For each integer a relatively prime to l, let $r(a)$ denote the order of a modulo l. Let R be the set of positive integers $a<l$ satisfying $a \equiv g^m \pmod{l}$ for some integer g. We easily find that a positive integer $a<l$ belongs to R if and only if $r(a)$ divides the integer $(l-1)/m$.

Lemma 3. *If $m<(l-1)/2$, then $\{a, l-a\} \cap \mathcal{N} = \emptyset$ with some element a of R.*

Proof. Assume that $m<(l-1)/2$, i.e., $2<(l-1)/m$. Then there exists a prime number v such that v^* divides $(l-1)/m$, where v^* denotes 4 or v according as $v=2$ or $v>2$. Simultaneously we can choose a positive integer $a'<l$ with $r(a') = v^*$. Since a' belongs to R, the conclusion of the lemma holds if $a' \notin \mathcal{N}$ and $l-a' \notin \mathcal{N}$. We now consider the case where an element b of $\{a', l-a'\} \cap \mathcal{N}$ exists. Note that $\{r(a'), r(l-a')\} = \{v^*, 2v\}$. We take the maximal integer $j>0$ with $b^j<l$. Let a and c be respectively the remainder and the quotient of the division of b^{j+1} by l. Obviously, $b^{j+1} = a + lc$, $0<a<l$ and $c>0$. As $b^{j+1} < l^{1+1/j}$, we have $c<l^{1/j}$. Furthermore, since $l \geq 5$, it is clear that $l^{1/j} < l-2$ if $j \geq 2$. In the case $j=1$, the relation $b^{j+1} = a + l(l-1)$ implies that $l-a = (l+b)(l-b) \geq l+b$, which is impossible. We thus obtain $1 \leq c \leq l-2$. On the other hand, as Lemma 2 yields $b^{l-1} \equiv 1 \pmod{l^2}$, we see that $(a+lc)^{l-1} \equiv (b^{l-1})^{j+1} \equiv 1 \pmod{l^2}$, so that $a^l \equiv (a+lc)^l \equiv a + lc \pmod{l^2}$; it then follows that $(l-a)^l \equiv -a^l \equiv -a - lc \pmod{l^2}$. Hence $a^l \not\equiv a \pmod{l^2}$ and $(l-a)^l \not\equiv l-a \pmod{l^2}$. Therefore, by Lemma 2, we have $\{a, l-a\} \cap \mathcal{N} = \emptyset$. As 1 belongs to $\mathcal{N}$, this implies that $a \notin \{1, l-1\}$, i.e., $r(a) \notin \{1,2\}$. However, $r(a)$ divides $r(b)$, an element of $\{v^*, 2v\}$. Thus $r(a)$ equals v^* or $2v$, i.e., $\{r(a), r(l-a)\} = \{v^*, 2v\}$. Hence, replacing a by $l-a$ if necessary, we may regard a as an element of R. □

We add that the converse of Lemma 3 is also true. In fact, if $(l-1)/m \leq 2$, then $R \subseteq \{1, l-1\}$ or, equivalently, $\{a, l-a\} \cap \mathcal{N} \ni 1$ for every element a of R.

Proof of Proposition 1. Under the assumption of the proposition, Lemma 3 shows that there exists a positive integer $a<l$ satisfying $a \notin \mathcal{N}$, $l-a \notin \mathcal{N}$, and $a \equiv g^m \pmod{l}$ for some integer g. Since l is totally ramified in k in the case $m>1$, we can take m and k respectively as m' and k' of Lemma 1. Therefore Lemma 1 completes the proof. □

3. Associated results. Let $\theta = \cos(2\pi/49) \times \cos(11\pi/49)\cos(36\pi/49)$. Since $\boldsymbol{B}_1 = \boldsymbol{Q}(\theta)$ if $l=7$, we see from Proposition 1 that $\boldsymbol{Q}(\theta, \sqrt{-7})$, the cyclic field of degree 14 with conductor 49, is not norm-Euclidean. Meanwhile, in [Y], Yamamura determined all imaginary finite abelian extensions over $\boldsymbol{Q}$ in $\boldsymbol{C}$ with class number 1. The theorem of [Y], together with the last table of [Y], tells us that $\boldsymbol{Q}(\theta, \sqrt{-7})$ is the unique imaginary cyclic field of class number 1 to which Proposition 1 is applicable.

Next let $\mathfrak{F}$ be a finite abelian extension over $\boldsymbol{Q}$ in $\boldsymbol{C}$. Let $\mathfrak{F}^*$ denote the maximal abelian extension over $\boldsymbol{Q}$, in the Hilbert class field over $\mathfrak{F}$ (in $\boldsymbol{C}$), that contains $\mathfrak{F}$. Then $\mathfrak{F}^*$ coincides with the genus field (Geschlechterkörper) of $\mathfrak{F}$ in the sense of Leopoldt [Le] or the maximal real subfield of this genus field of $\mathfrak{F}$ according to whether $\mathfrak{F}$ is imaginary or real. The genus number of $\mathfrak{F}$ is defined as the degree of $\mathfrak{F}^*/\mathfrak{F}$ (cf. Furuta [F]), so that the genus number of $\mathfrak{F}$ divides the class number of $\mathfrak{F}$. Hence $\mathfrak{F}$ is not norm-Euclidean if the genus number of $\mathfrak{F}$ exceeds 1. On the other hand, $\mathfrak{F}$ is a cyclic field of genus number 1 if the conductor of $\mathfrak{F}$ is a power of $l \geq 5$.

From now on, let us deal with cyclic fields of genus number 1 in which l is totally ramified and further a prime number other than l is ramified. We denote by t the highest power of 2 dividing $l-1$. Naturally $t \geq 2$ since $l \geq 5$. We denote by U the union of $\{4, 8\}$ and the set of prime numbers not equal to l but congruent to 3 modulo 4. Let $\mathfrak{K}$ be a cyclic field, not contained in the cyclotomic field $\boldsymbol{Q}(e^{2\pi i/l})$, such that l is totally and tamely ramified in $\mathfrak{K}$. Then, essentially by the genus theory of [Le], the following three conditions turn out to be equivalent (cf. also [F], Iyanaga and Tamagawa [IT]):

(1) the genus number of $\mathfrak{K}$ is equal to 1,
(2) $\mathfrak{K}$ is the compositum of a cyclic field in $\boldsymbol{Q}(e^{2\pi i/l})$ of odd degree and a real cyclic field of degree t whose conductor is the product of l and an element of U,
(3) for every positive integer n, the genus number of the cyclic field $\mathfrak{K}\boldsymbol{B}_n$ is equal to 1.

Under the condition (2), the ramification index for $\mathfrak{K}/\boldsymbol{Q}$ of the prime number other than l dividing the conductor of $\mathfrak{K}$ coincides with 2, whence $\mathfrak{K}$ is a real quadratic extension over a subfield of $\boldsymbol{Q}(\cos(2\pi/l))$.

Proposition 2. *Assume that* $(l-1)/(2m)$ *is an odd integer greater than* 1. *Let* q *be any element of* U, *and let* K *be the compositum of the maximal subfield of* k *with odd degree and the real cyclic field of degree* t *with conductor* lq. *Then* $K\boldsymbol{B}_n$ *is not norm-Euclidean for any positive integer* n.

Proof. We first note that, by the hypothesis and the fact stated just above the proposition, the real cyclic field K is a quadratic extension over k. As $(l-1)/m > 2$, Lemma 3 shows that there exists an element b of R with $\{b, l-b\} \cap \mathcal{N} = \emptyset$. When the divisor $r(b)$ of $(l-1)/m$ is even, we have $r(l-b) = r(b)/2$ since $(l-1)/(2m)$ is an odd integer. Hence $r(b)$ or $r(l-b)$ divides $(l-1)/(2m)$, namely, b or $l-b$ is congruent to g^{2m} modulo l for some integer g. Furthermore, l is totally and tamely ramified in K. The proposition thus holds by Lemma 1 for the case where $m' = 2m$ and $k' = K$. $\square$

In the above, $K = k(\sqrt{lq})$ if m is odd. This fact leads us to state an immediate consequence of Proposition 2, as follows:

Proposition 3. *Take any prime number* $p \neq l$ *with* $p \not\equiv 1 \pmod 4$. *Suppose that* $l \equiv 3 \pmod 4$, m *is odd, and* $l \geq 6m+1$. *Then neither* $k\boldsymbol{B}_n(\sqrt{l})$ *nor* $k\boldsymbol{B}_n(\sqrt{lp})$ *is norm-Euclidean for any positive integer* n.

We now take a positive integer n. In the case where $l \equiv 1 \pmod 4$ and $l \geq 13$, Proposition 1 for $m = 2$ asserts that $\boldsymbol{B}_n(\sqrt{l})$ is not norm-Euclidean. In the case where $l \equiv 3 \pmod 4$ and $l \geq 7$, Proposition 3 for $m = 1$ implies that $\boldsymbol{B}_n(\sqrt{l})$ is not norm-Euclidean. The following simple result is therefore obtained.

Proposition 4. *Whenever* $l \geq 7$, $\boldsymbol{B}_n(\sqrt{l})$ *is not norm-Euclidean for any positive integer* n.

Acknowledgment. The authors express their sincere gratitude to the referee who made many detailed and helpful comments for the paper.

References

[B] H. Bauer, Numerische Bestimmung von Klassenzahlen reeller zyklischer Zahlkörper, J. Number Theory **1** (1969), 161–162.

[BPR] J. Buhler, C. Pomerance and L. Robertson, Heuristics for class numbers of prime-power real cyclotomic fields, in *High primes and misdemeanours: lectures in honour of the 60th birthday of Hugh Cowie Williams*, Fields Inst. Commun., 41, Amer. Math. Soc., Providence, RI, 2004, pp. 149–157.

[C] J.-P. Cerri, De l'euclidianité de $\mathbf{Q}(\sqrt{2+\sqrt{2+\sqrt{2}}})$ et $\mathbf{Q}(\sqrt{2+\sqrt{2}})$ pour la norme, J. Théor. Nombres Bordeaux **12** (2000), no. 1, 103–126.

[CD] H. Cohn and J. Deutsch, Use of a computer scan to prove $\mathbf{Q}(\sqrt{2+\sqrt{2}})$ and $\mathbf{Q}(\sqrt{3+\sqrt{2}})$ are Euclidean, Math. Comp. **46** (1986), no. 173, 295–299.

[D] H. Davenport, On the product of three nonhomogeneous linear forms, Math. Proc. Cambridge Philos. Soc. **43** (1947), 137–152.

[F] Y. Furuta, The genus field and genus number in algebraic number fields, Nagoya Math. J. **29** (1967), 281–285.

[H] H. Heilbronn, On Euclid's algorithm in cyclic fields, Canadian J. Math. **3** (1951), 257–268.

[HH] K. Horie and M. Horie, The l-class group of the $\boldsymbol{Z}_p$-extension over the rational field, J. Math. Soc. Japan **64** (2012), no. 4, 1071–1089.

[IT] S. Iyanaga and T. Tamagawa, Sur la théorie du corps de classes sur le corps des nombres rationnels, J. Math. Soc. Japan **3** (1951), 220–227.

[Le] H. W. Leopoldt, Zur Geschlechtertheorie in abelschen Zahlkörpern, Math. Nachr. **9** (1953), 351–362.

[Li] F. J. van der Linden, Class number computations of real abelian number fields, Math. Comp. **39** (1982), no. 160, 693–707.

[Ma] J. M. Masley, Class numbers of real cyclic number fields with small conductor, Compositio Math. **37** (1978), no. 3, 297–319.

[Mc] K. J. McGown, Norm-Euclidean cyclic fields of prime degree, Int. J. Number Theory **8** (2012), no. 1, 227–254.

[Mi] J. C. Miller, Class numbers in cyclotomic $\mathbf{Z}_p$-extensions, J. Number Theory **150** (2015), 47–73.

[Y] K. Yamamura, The determination of the imaginary abelian number fields with class number one, Math. Comp. **62** (1994), no. 206, 899–921.