Corrigendum to "Real abelian fields satisfying the Hilbert-Speiser condition for some small primes p"

Proc. Japan Acad. Ser. A Math. Sci. **92** (2016), no. 1, 19–22.

By Humio ICHIMURA

Faculty of Science, Ibaraki University, Bunkyo 2-1-1 Mito, Ibaraki 310-8512, Japan

(Communicated by Shigefumi MORI, M.J.A., June 12, 2019)

Abstract: We correct and change Proposition 1 and the proof of Proposition 2 of the previous paper [7].

Key words: Hilbert-Speiser number fields; real abelian fields.

We use the same notation as in the paper [7]. In particular, for a prime number p, a number field F satisfies the Hilbert-Speiser condition (H_p) when every tame cyclic extension K/F of degree p has a normal integral basis. In [7], we claimed the following two results.

Proposition 1. *Let $p \geq 7$ be a prime number with $p \equiv 3 \bmod 4$. Let F be a number field unramified at p, and let $N = F(\sqrt{-p})$. If F satisfies the Hilbert-Speiser condition (H_p), then the exponent of the class group Cl_N of N divides $h(\mathbf{Q}(\sqrt{-p}))$.*

Proposition 2. *Let $p \geq 7$ be a prime number with $h(\mathbf{Q}(\sqrt{-p})) = 1$. When $p = 7$ (resp. 11), a real abelian field F satisfies (H_p) if and only if $F = \mathbf{Q}(\sqrt{5})$ or $\mathbf{Q}(\sqrt{13})$ (resp. $F = \mathbf{Q}(\cos 2\pi/7)$). When $p = 19$, 43, 67 or 163, there is no real abelian field satisfying (H_p).*

In Proposition 2, we are excluding the case $F = \mathbf{Q}$ because the rationals $\mathbf{Q}$ satisfies (H_p) for all p.

In his email of 30th May 2018, Fabio Ferri kindly informed us that the formula $[A_\Delta : \mathcal{S}_\Delta] = h_k^-$ in [7, eq (2)] is incorrect and provided a counter-example. As he pointed out, the mistake was caused by our confusion of the ideal $\mathcal{S}_\Delta$ with the Stickelberger ideal associated to $\mathbf{Q}(\sqrt{-p})$ by Sinnott [12]. In [7], we proved Proposition 1 using the incorrect formula, and proved Proposition 2 using Proposition 1. We could not confirm whether or not the assertions of Proposition 1 and its corollary ([7, Corollary]) are true. However, we can save the situation by replacing Proposition 1 with the following weaker assertion on the minus class group Cl_N^- of $N = F(\sqrt{-p})$. Here, Cl_N^- is defined to be the kernel of the norm map $Cl_N \to Cl_F$.

Proposition 3. *Let $p \geq 7$ be a prime number with $p \equiv 3 \bmod 4$, and let F be a totally real number field satisfying the Hilbert-Speiser condition (H_p). Then the exponent of the minus class group Cl_N^- of the CM-field $N = F(\sqrt{-p})$ divides $h(\mathbf{Q}(\sqrt{-p}))$, and the exponent of Cl_F divides $(p-1)/2$.*

Proposition 2 is correct. In the following, we show Proposition 3, and change and correct the proof of Proposition 2 in [7] using Proposition 3. In the proof of Proposition 3, we partially repeat some of the arguments in [7] for the convenience of the reader.

Proof of Proposition 3. Let $G = (\mathbf{Z}/p\mathbf{Z})^\times$ be the multiplicative group, which we naturally identify with the Galois group $\mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$. We define elements θ_G and θ_2 of $\mathbf{Q}[G]$ by

$$\theta_G = \frac{1}{p}\sum_{a=1}^{p-1} a\sigma_a^{-1} \quad \text{and} \quad \theta_2 = (2-\sigma_2)\theta_G$$

where $\sigma_a = a \bmod p$ is the automorphism of $\mathbf{Q}(\zeta_p)$ sending ζ_p to ζ_p^a. The Stickelberger ideal $\mathcal{S}_G$ of the group ring $\mathbf{Z}[G]$ is defined by

$$\mathcal{S}_G = \mathbf{Z}[G] \cap \theta_G \mathbf{Z}[G].$$

We have $p\theta_G \in \mathcal{S}_G$ by the definition of $\mathcal{S}_G$, and $\theta_2 \in \mathcal{S}_G$ by [13, Lemma 6.9].

In this paragraph, let F denote an arbitrary number field. Let $\Gamma = \mathbf{Z}/p\mathbf{Z}$ be the additive group. Denote by $Cl(\mathcal{O}_F[\Gamma])$ the locally free class group associated to the group ring $\mathcal{O}_F[\Gamma]$, and by $Cl^0(\mathcal{O}_F[\Gamma])$ the kernel of the map $Cl(\mathcal{O}_F[\Gamma]) \to Cl_F$ induced by the augmentation $\mathcal{O}_F[\Gamma] \to \mathcal{O}_F$.

2010 Mathematics Subject Classification. Primary 11R33, 11R18.

doi: 10.3792/pjaa.95.80

Through the natural action of $G = (\mathbf{Z}/p\mathbf{Z})^{\times}$ on Γ, the groups $Cl(\mathcal{O}_F[\Gamma])$ and $Cl^0(\mathcal{O}_F[\Gamma])$ are regarded as modules over the group ring $\mathbf{Z}[G]$. By the main theorem of McCulloh [9], F satisfies (H_p) if and only if the condition

$$(1) \qquad Cl^0(\mathcal{O}_F[\Gamma])^{\mathcal{S}_G} = \{0\}$$

is satisfied.

Now, let p and F be as in Proposition 3. Let $N = F(\sqrt{-p})$ and let $K = F(\zeta_p)$. Note that N is contained in K since $p \equiv 3 \bmod 4$. As F satisfies (H_p) and $p \geq 7$, the extension $F/\mathbf{Q}$ is unramified at p by Greither and Johnston [4, Theorem 1.1]. Hence, the Galois group $\mathrm{Gal}(K/F)$ naturally identifies with $G = \mathrm{Gal}(\mathbf{Q}(\zeta_p)/\mathbf{Q})$ via restriction. Let Cl_{K,ϖ_p} be the ray class group of K defined modulo the ideal $\varpi_p\mathcal{O}_K$ with $\varpi_p = \zeta_p - 1$. The class groups Cl_{K,ϖ_p} and Cl_K are regarded as modules over $\mathbf{Z}[G]$ by the above identification. As $F/\mathbf{Q}$ is unramified at p, it follows that $Cl^0(\mathcal{O}_F[\Gamma]) \cong Cl_{K,\varpi_p}$ as $\mathbf{Z}[G]$-modules by Brinkhuis [1, Proposition 2.1]. Therefore, we see from (1) that the Stickelberger ideal $\mathcal{S}_G$ annihilates Cl_{K,ϖ_p} and Cl_K. It follows that $\mathcal{S}_G$ annihilates Cl_N (resp. Cl_F) since the norm map from Cl_K to Cl_N (resp. Cl_F) is surjective by [13, Theorem 10.1].

We denote by χ the quadratic character of $G = (\mathbf{Z}/p\mathbf{Z})^{\times}$, and we extend it to a ring homomorphism $\mathbf{Z}[G] \to \mathbf{Z}$ by linearlity. The restriction of the automorphism $\sigma_a \in G$ to $\mathbf{Q}(\sqrt{-p})$ and $N = F(\sqrt{-p})$ is the trivial map or the complex conjugation depending on whether $\chi(a) = 1$ or -1, respectively. Accordingly, σ_a acts on the minus class group Cl_N^- trivially or via (-1)-multiplication. This implies that $\alpha \in \mathbf{Z}[G]$ acts on Cl_N^- via $\chi(\alpha)$-multiplication. Here recall the following class number formula (see (6.2) of Fröhlich and Taylor [6, Chapter VIII]):

$$(2) \qquad h(\mathbf{Q}(\sqrt{-p})) = -\frac{1}{p}\sum_{a=1}^{p-1} a\chi(a).$$

We already know that the elements $-p\theta_G$ and $-\theta_2$ belong to $\mathcal{S}_G$ and hence they annihilate Cl_N^-. By (2), we observe that $\chi(-p\theta_G) = ph(\mathbf{Q}(\sqrt{-p}))$ and that

$$\chi(-\theta_2) = (2 - \chi(2))\chi(-\theta_G)$$

equals $h(\mathbf{Q}(\sqrt{-p}))$ or $3h(\mathbf{Q}(\sqrt{-p}))$ depending on whether $\chi(2) = 1$ or -1, respectively. Now we see that $h(\mathbf{Q}(\sqrt{-p}))$-multiplication annihilates Cl_N^- as $p \geq 7$.

Let χ_0 be the trivial character of $G = (\mathbf{Z}/p\mathbf{Z})^{\times}$, which extends to a ring homomorphism $\mathbf{Z}[G] \to \mathbf{Z}$ by linearlity. As $\sigma_a \in G$ acts on Cl_F trivially, the element $\theta_2 \in \mathcal{S}_G$ acts on Cl_F via multiplication by $\chi_0(\theta_2) = (p-1)/2$. We obtain the assertion for Cl_F because $\mathcal{S}_G$ annihilates Cl_F. □

Corrected proof of Proposition 2. Let $p \geq 7$ be an odd prime number with $h(\mathbf{Q}(\sqrt{-p})) = 1$. Let $F \neq \mathbf{Q}$ be a real abelian field satisfying (H_p), and let $d = [F : \mathbf{Q}]$ and $N = F(\sqrt{-p})$. Then $F/\mathbf{Q}$ is unramified at p by [4, Theorem 1.1], and $h_N^- = 1$ by Proposition 3. Imaginary abelian fields K with $h_K^- = 1$ are determined by Louboutin [8], Park and Kwon [10,11] and Chang and Kwon [2,3]. In our setting where $K = N = F(\sqrt{-p})$, we have the following three cases:

(I) $d = 3$,

(II) $d \geq 5$ and $N/\mathbf{Q}$ is a cyclic extension,

(III) $N/\mathbf{Q}$ is non-cyclic.

The fields F and $\mathbf{Q}(\sqrt{-p})$ are linearly disjoint over $\mathbf{Q}$ as $F/\mathbf{Q}$ is unramified at p. Therefore, d is odd for case (II), and conversely, the case where d is even is contained in (III). Case (I) is dealt with in [10], case (II) in [2], and case (III) in [3].

First, let us deal with case (I) under the notation in [10]. All imaginary sectic fields K with relative class number 1 are listed in [10, Table 3]. The fields K are parametrized with the conductors f of K, f^+ of K^+ and m of the imaginary quadratic subfield of K. In our case $K = N = F(\sqrt{-p})$, we have $m = p$ and $p \nmid f^+$ as $F/\mathbf{Q}$ is unramified at p. From the table, we find that $F/\mathbf{Q}$ is unramified at p and $h_N^- = 1$ when and only when (i) $p = 7$ and F is the cyclic cubic field of conductor 9 or 13 or (ii) $p = 11$ and F is the cyclic cubic field of conductor 7.

Next, let us deal with case (II) under the notation in [2]. All imaginary cyclic fields K such that $[K : \mathbf{Q}] \geq 10$, $[K : \mathbf{Q}]$ is not a 2-power and $h_K^- = 1$ are listed in [2, Table I]. Among them we need those ones with $[K : \mathbf{Q}]/2$ is odd, namely those ones in the upper half of the table. This is because d is odd for case (II). Such fields K are parametrized with the conductors f_K of K, f_{K^+} of K^+ and f_2 of the imaginary quadratic subfield of K. In our case $K = F(\sqrt{-p})$, we have $f_2 = p$ and $p \nmid f_{K^+}$. In the table, we find no such fields.

Finally, let us deal with case (III) under the notation in [3]. All imaginary non-cyclic fields K with relative class number 1 are listed in [3, Table I]. The table is arranged according to the type of the

Galois group $G = \mathrm{Gal}(K/\mathbf{Q})$. Let us look at those ones with type $G = (2^*, 2^*)$. These are imaginary $(2,2)$-extensions of $\mathbf{Q}$. They are parametrized with the conductors $f_1 = f_{k_1}$ and $f_2 = f_{k_2}$ of the imaginary quadratic subfields k_1 and k_2 of K. Then, in our case $K = N = F(\sqrt{-p})$, we have $f_1 = p$, $p|f_2$ and $p \nmid f_2/p$ (swapping f_1 and f_2 if necessary). From the table, we find $F/\mathbf{Q}$ is unramified at p and $h_N^- = 1$ when and only when (iii) $p = 7$ and $F = \mathbf{Q}(\sqrt{5})$, $\mathbf{Q}(\sqrt{13})$ or $\mathbf{Q}(\sqrt{61})$ or (iv) $p = 11$ and $F = \mathbf{Q}(\sqrt{2})$ or $\mathbf{Q}(\sqrt{17})$. Next let us look at those K with $G = (2^*, 2^*, 2^*)$. These are imaginary $(2,2,2)$-extension. They are parametrized by conductors of three imaginary quadratic subfields similary to the case $G = (2^*, 2^*)$. From the table, we find no desired pair (p, F). Now let us look at those K with $G \neq (2^*, 2^*)$, $(2^*, 2^*, 2^*)$. These K are parametrized with a set of generators of the group X_K of the associated Dirichlet characters. In our case $K = F(\sqrt{-p})$, X_K contains $\chi_p^{(p-1)/2}$ where χ_p is a Dirichlet character of conductor p and order $p-1$. For each K in the table, we checked that p is ramified in K^+ from the data on X_K. Therefore, we obtain no desired pair (p, F) from those K.

Therefore, we obtain 8 pairs (p, F) such that $F/\mathbf{Q}$ is unramified at p and $h_N^- = 1$, namely those listed in (i)–(iv) above. Fortunately, these 8 pairs coincide with the pairs which we dealt with in [7]. We have already shown in [7] that (H_p) is satisfied when $p = 7$ (resp. 11) and $F = \mathbf{Q}(\sqrt{5})$ or $\mathbf{Q}(\sqrt{13})$ (resp. $\mathbf{Q}(\cos 2\pi/7)$), and that (H_p) is not satisfied for the other 5 pairs. Thus the proof of Proposition 2 is corrected. □

Remark 1. Let p be as in Proposition 2, and let F be a real abelian field satisfying (H_p). Then, Proposition 1 asserts $h_N = 1$, while Proposition 3 asserts that $h_N^- = 1$. So what we have actually determined in [7] using Proposition 1 is all real abelian fields $F \neq \mathbf{Q}$ satisfying (H_p) and $h_N = 1$.

Remark 2. A correct proof of Proposition 2 is also given in F. Ferri and C. Greither [5, §6]. It is slightly different from ours. The subject of [5] is a "C_p-Leopoldt field", a number field satisfying a condition somewhat weaker than (H_p). They obtained several conditions for a field F to be C_p-Leopoldt using the main theorem of [9]. One of them asserts that if $h(\mathbf{Q}(\sqrt{-p})) = 1$, then a real abelian field F unramified at p is C_p-Leopoldt only when $h_N^- = 1$ with $N = F(\sqrt{-p})$. Again, they show that $h_N^- = 1$ is a necessary condition for (H_p) to hold. Using the above cited papers on relative class numbers, they observed that there is no $F \neq \mathbf{Q}$ unramified at p such that $h_N^- = 1$ but $h_N^+ > 1$. This gives an alternative proof of Proposition 2 (see Remark 1).

Acknowledgements. The author heartfully thanks Mr. Fabio Ferri for kindly informing him of the serious error contained in the previous paper [7]. The author is very grateful to the anonymous referee for several useful comments and for encouraging him to rewrite the first version of this corrigendum, thanks to which he was able to improve the presentation of the whole paper.

References

[1] J. Brinkhuis, Normal integral bases and complex conjugation, J. Reine Angew. Math. **375/376** (1987), 157–166.

[2] K.-Y. Chang and S.-H. Kwon, Class number problem for imaginary cyclic number fields, J. Number Theory **73** (1998), no. 2, 318–338.

[3] K.-Y. Chang and S.-H. Kwon, Class numbers of imaginary abelian number fields, Proc. Amer. Math. Soc. **128** (2000), no. 9, 2517–2528.

[4] C. Greither and H. Johnston, On totally real Hilbert-Speiser fields of type C_p, Acta Arith. **138** (2009), no. 4, 329–336.

[5] F. Ferri and C. Greither, Tame Galois module structure revisited, Ann. Mat. Pura Appl. (2019), doi: 10.1007/s10231-019-00852-x.

[6] A. Fröhlich and M. J. Taylor, *Algebraic number theory*, Cambridge Studies in Advanced Mathematics, 27, Cambridge University Press, Cambridge, 1993.

[7] H. Ichimura, Real abelian fields satisfying the Hilbert-Speiser condition for some small primes p, Proc. Japan Acad. Ser. A Math. Sci. **92** (2016), no. 1, 19–22.

[8] S. Louboutin, CM-fields with cyclic ideal class groups of 2-power orders, J. Number Theory **67** (1997), no. 1, 1–10.

[9] L. R. McCulloh, Galois module structure of elementary abelian extensions, J. Algebra **82** (1983), no. 1, 102–134.

[10] Y.-H. Park and S.-H. Kwon, Determination of all imaginary abelian sextic number fields with class number ≤ 11, Acta Arith. **82** (1997), no. 1, 27–43.

[11] Y.-H. Park and S.-H. Kwon, Determination of all non-quadratic imaginary cyclic number fields of 2-power degree with relative class number ≤ 20, Acta Arith. **83** (1998), no. 3, 211–223.

[12] W. Sinnott, On the Stickelberger ideal and the circular units of an abelian field, Invent. Math. **62** (1980/81), no. 2, 181–234.

[13] L. C. Washington, *Introduction to cyclotomic fields*, 2nd ed., Graduate Texts in Mathematics, 83, Springer-Verlag, New York, 1997.