CORRECTION TO 'ON THE RELATIVE GALOIS MODULE STRUCTURE OF RINGS OF INTEGERS IN TAME EXTENSIONS'

A. AGBOOLA AND L. R. MCCULLOH

Abstract. This note explains and corrects an error in our paper 'On the relative Galois module structure of tame extensions'. The main results of the paper remain unchanged.

The proof of [1, Theorem E] contains an error. The error occurs in the proof of [1, Theorem 15.5] where the existence of a cohomology class b satisfying certain local properties is claimed. Unfortunately the class b constructed there will in general be ramified at places in T (because Ω_F in general acts non-trivially on Γ), and so will not satisfy conditions (i) and (iii) of [1, Theorem 15.5]. This in turn invalidates Step III of the proof of [1, Theorem 16.4]. We are most grateful to Brandon Alberts, Ila Varma, Jiuya Wang, and Melanie Wood for pointing this out to us.

In what follows, we shall describe how the arguments of [1, Section 16] may be modified (completely avoiding Step III of the proof of [1, Theorem 16.4]) in order to prove [1, Theorem E]. This is accomplished by replacing the use of 'Property R' in [1, Definition 16.1] by a much weaker condition (see Definition 1.2 below) which nevertheless suffices for our purposes. We also explain why the proofs of [1, Theorem 16.4]) and [1, Theorem E] given in [1] do in fact hold for nilpotent groups G of odd order, and we describe a explicit examples which show that [1, Conjecture B] is false in general.

1. Corrections

We follow the notation of [1].

Let us first recall the definition of 'Property R (see [1, Definition 16.1]).

Definition 1.1. Let S be any finite (possibly empty) set of places of F. We shall say that $\mathrm{LC}(O_F G)_S$ *satisfies Property R* if the following holds. Suppose given any fully ramified $x \in \mathrm{LC}(O_F G)_S$. For each finite place v of F, suppose also given a homomorphism $\pi_{v,x} \in \mathrm{Hom}(\Omega_{F_v}, G)$ such that $[\pi_{v,x}] \in H^1_t(F_v, G)$ and $\lambda_v(x) = \Psi_v([\pi_{v,x}])$. (Note that in general, such a choice of $\pi_{v,x}$ is not unique.) Then there exists $\Pi \in \mathrm{Hom}(\Omega_F, G)$ with $[\Pi] \in H^1_t(F, G)$ such that

(a) $x = \Psi([\Pi])$;

Date: Version of April 18, 2021.

(b) $\Pi\mid_{I_v} = \pi_{v,x}\mid_{I_v}$ for each finite place v of F.

(Hence in particular, x is cohomological, and F_Π is a field, because Π is fully ramified (see the proof of [1, Theorem 13.6]). Also, Π is unramified at all places in S.) □

We shall require the following definition:

Definition 1.2. Let S be any finite (possibly empty) set of finite places of F, and let $\mathcal{F}/F$ be a finite extension. We shall say that $\mathrm{LC}(O_F G)_S$ *satisfies Property* $\mathrm{Sp}(\mathcal{F}/F)$ if the following holds. Suppose given any fully ramified $x \in \mathrm{LC}(O_F G)_S$. For each finite place v of F, suppose also given a homomorphism $\pi_{v,x} \in \mathrm{Hom}(\Omega_{F_v}, G)$ such that $[\pi_{v,x}] \in H^1_t(F_v, G)$ and $\lambda_v(x) = \Psi_v([\pi_{v,x}])$. (Such a choice of $\pi_{v,x}$ is not in general unique.) Then there exists $\Pi \in \mathrm{Hom}(\Omega_F, G)$ with $[\Pi] \in H^1_t(F, G)$ such that if we set

$$\begin{aligned} S_\Pi(x) &:= \{v : \Pi\mid_{I_v} \neq 0 \text{ and } \pi_{v,x}\mid_{I_v} = 0\} \\ &= \{v : \Pi_v \text{ is ramified and } \lambda_v(x) \text{ is unramified}\}, \end{aligned}$$

then:

(i) $\Pi\mid_{I_v} = \pi_{v,x}\mid_{I_v}$ for all $v \notin S_\Pi(x)$.

(ii) Each place $v \in S_\Pi(x)$ is totally split in $\mathcal{F}/F$.

(iii) Π is unramified at all places in S. (So, in particular, $S \cap S_\Pi(x) = \emptyset$.)

(Here again Π is fully ramified, and so F_Π is a field (see the proof of [1, Theorem 13.6]). However, it is not in general the case that $\Psi([\Pi]) = x$.) □

Remark 1.3. If $\mathrm{LC}(O_F G)_S$ satisfies Property R, then it satisfies Property $\mathrm{Sp}(\mathcal{F}/F)$ for any choice of $\mathcal{F}$, because in this case, in the definition of Property $\mathrm{Sp}(\mathcal{F}/F)$, we may always ensure that $S_\Pi(x) = \emptyset$. □

Remark 1.4. Suppose that $\mathcal{F}/F$ is a finite extension, and that $F_{|G|} \subseteq \mathcal{F}$, where $F_{|G|}$ denotes the ray class group of F modulo $|G| \cdot O_F$. Then if v is totally split in $\mathcal{F}/F$, it follows that $q_v \equiv 1 \pmod{|G|}$, and so $\Sigma_v(G) = G$ (see [1, Definition 7.2]). Similarly, if $H \leq G$, then we also have $\Sigma_v(H) = H$. □

Proposition 1.5. *If G is abelian, then $\mathrm{LC}(O_F G)$ satisfies Property $\mathrm{Sp}(\mathcal{F}/F)$ for any finite extension $\mathcal{F}/F$.*

Proof. It is shown in [1, Proposition 16.2] that $\mathrm{LC}(O_F G)$ satisfies Property R whenever G is abelian. The desired result now follows at once from Remark 1.3 above. □

Definition 1.6. (cf. [1, Definition 15.4]) Let l be a prime, and suppose that Γ is an elementary abelian l-group on which Ω_F acts trivially. Let $T := \{v_1, \ldots, v_r\}$ be any finite set of finite places of F containing all places above l, and write $\mathfrak{p}_i$ for the prime ideal of F corresponding to v_i. [1, Proposition 4.8] implies that we may choose an integer $N = N(T)$ such that for each v_i, we have

$$\mathrm{Hom}_{\Omega_{F_{v_i}}}(A_\Gamma, U_{\mathfrak{p}_i^N}(O_{F^c_{wv_i}})) \subseteq \mathrm{rag}[\mathrm{Hom}_{\Omega_{F_{v_i}}}(R_\Gamma, O^\times_{F^c_{v_i}})].$$

Set

$$\mathfrak{a} = \mathfrak{a}(T) = \prod_{i=1}^{r} \mathfrak{p}_i.$$

Let $F_{\mathfrak{a}^N}$ denote the ray class field of F modulo $\mathfrak{a}^N$.

[Note that the difference between the above definition and that of [1, Definition 15.4] is that here we are assuming that Ω_F acts trivially on Γ.] □

The following result is a corrected version of [1, Theorem 15.5]. The crucial additional hypothesis required is that Ω_F acts trivially on Γ.

Theorem 1.7. *Let l be a prime, and suppose that Γ is an elementary abelian l-group on which Ω_F acts trivially. Let $v \notin T$ be any finite place of F that splits completely in $F_{\mathfrak{a}^N}/F$, and suppose that s is any non-trivial element of Γ. Then there is an element $b = b(v; s) \in H^1(F, \Gamma)$ satisfying the following local conditions:*

(i) $\mathrm{loc}_{v_i}(b) = 0$ *for* $1 \leq i \leq r$*;*

(ii) $b\,|_{I_v} = \tilde{\varphi}_{v,s}$ *(see* [1, Remark 7.11]*);*

(iii) b is unramified away from v.

Proof. Let $\mathfrak{p}$ be the prime ideal of F corresponding to v. Our hypotheses on v imply that $\mathfrak{p}$ is principal, with $\mathfrak{p} \equiv 1 \pmod{\mathfrak{a}^N}$. As Γ is abelian, we have that $\mathcal{H}(F\Gamma) \simeq \mathrm{Hom}_{\Omega_F}(A_\Gamma, (F^c)^\times)$ (see [1, (4.6)]). Let ϖ be a generator of $\mathfrak{p}$, and define $\rho \in \mathrm{Hom}_{\Omega_F}(A_\Gamma, (F^c)^\times)$ by

$$\rho(\alpha) = \varpi^{\langle \alpha, s\rangle_\Gamma}.$$

(This homomorphism is Ω_F-equivariant because Ω_F acts trivially on Γ.) Then ρ is the reduced resolvend of a normal basis generator of an extension $F_{\pi(\rho)}/F$ corresponding to $[\pi(\rho)] \in H^1(F, \Gamma)$. Since $\mathfrak{p} \equiv 1 \pmod{\mathfrak{a}^N}$, for each place v_i in T, we have

$$\mathrm{loc}_{v_i}(\rho) \in \mathrm{Hom}_{\Omega_{F_{v_i}}}(A_\Gamma, U_{\mathfrak{p}_i^N}(O_{F^c_{v_i}})) \subseteq \mathrm{rag}[\mathrm{Hom}_{\Omega_{F_{v_i}}}(R_\Gamma, O^\times_{F^c_{v_i}})],$$

and so it follows that $\mathrm{loc}_{v_i}(\pi(\rho)) = 0$ (see [1, (4.7)]). In particular, $\pi(\rho)$ is unramified at all places in T.

For all places w of F not lying in $T \cup \{v\}$ we have that

$$\mathrm{loc}_w(\rho) \in \mathrm{Hom}_{\Omega_{F_w}}(A_\Gamma, O^\times_{F^c_w}),$$

and so $\pi(\rho)$ is unramified at w. This implies that $\pi(\rho)$ is unramified away from v, since we have already seen that $\pi(\rho)$ does not ramify at any place in T. It is also easy to see that

$$\pi(\rho)\mid_{I_v} = \tilde{\varphi}_{v,s}$$

(cf. the proof of [1, Proposition 10.5(a)]). Hence $b = \pi(\rho)$ satisfies the conditions (i), (ii) and (iii) of the theorem.

□

The following result replaces [1, Theorem 16.4]. We shall follow [1] very closely in order to help the reader make any desired comparisons.

Theorem 1.8. *Let $\mathcal{F}/F$ be a finite, abelian extension with $F_{|G|} \subseteq \mathcal{F}$.*

Suppose that there is an exact sequence

$$0 \to B \to G \to D \to 0,$$

where B is an abelian minimal normal subgroup of G with $l \cdot B = 0$ for an odd prime l. Let S be any finite set of finite places of F containing all places dividing $|G|$.

(a) Assume that the following conditions hold:
(i) The set $\mathrm{LC}(O_F D)_S$ satisfies Property $\mathrm{Sp}(\mathcal{F}/F)$.
(ii) The field F contains no non-trivial l-th roots of unity.
Then $\mathrm{LC}(O_F G)_S$ also satisfies Property $\mathrm{Sp}(\mathcal{F}/F)$.

(b) Suppose that in addition the following conditions also hold:
(iii) The group B is central in G.
(iv) Either G admits no non-trivial irreducible symplectic characters, or F has no real places.
(v) $(|G|, h_F) = 1$.
Then $\mathrm{LC}(O_F G)_S$ satisfies Property R.

Proof. We shall establish these results in several steps, one of which crucially involves Neukirch's Lifting Theorem (see [1, Theorem 15.1]).

Suppose that $x \in \mathrm{LC}(O_F G)_S$ is fully ramified. For each finite place v of F, choose $\pi_{v,x} \in \mathrm{Hom}(\Omega_{F_v}, G)$ such that $[\pi_{v,x}] \in H^1_t(F_v, G)$ with

$$\lambda_v(x) = \Psi_v([\pi_{v,x}]).$$

The choice of $\pi_{v,x}$ is not unique. However, if $a(\pi_{v,x})$ is any normal integral basis generator of $F_{\pi_{v,x}}/F_v$, with Stickelberger factorisation (see [1, Definition 7.12])

$$\mathbf{r}_G(a(\pi_{v,x})) = u(a(\pi_{v,x})) \cdot \mathbf{r}_G(a_{nr}(\pi_{v,x})) \cdot \mathbf{r}_G(\varphi(\pi_{v,x})), \tag{1.1}$$

then [1, Proposition 10.5(c)] implies that $\mathrm{Det}(\mathbf{r}_G(\varphi(\pi_{v,x})))$ is independent of the choice of $\pi_{v,x}$. Hence, if $\varphi(\pi_{v,x}) = \varphi_{v,s}$, say, then it follows from [1, Proposition 10.5(b)] that the subgroup $\langle s \rangle$ of G (up to conjugation) and the determinant $\mathrm{Det}(\mathbf{r}_G(\varphi_{v,s}))$ of the resolvend $\mathbf{r}_G(\varphi_{v,s})$ do not depend upon the choice of $\pi_{v,x}$.

We write $q : G \to D$ for the obvious quotient map, and we use the same symbol q for the induced maps

$$K_0(O_F G, F^c) \to K_0(O_F D, F^c), \quad H^1(F, G) \to H^1(F, D),$$
$$H^1(F_v, G) \to H^1(F_v, D).$$

Set

$$\overline{x} := q(x), \quad \pi_{v,\overline{x}} := q(\pi_{v,x}).$$

Then $\overline{x} \in \mathrm{LC}(O_F D)_S$ with

$$\lambda_v(\overline{x}) = \Psi_{D,v}(\pi_{v,\overline{x}})$$

for each finite place v of F, and $\overline{x}$ is fully ramified.

By hypothesis, $\mathrm{LC}(O_F D)_S$ satisfies Property $\mathrm{Sp}(\mathcal{F}/F)$, and so there exists $\rho \in \mathrm{Hom}(\Omega_F, D)$ unramified outside S with $[\rho] \in H^1_t(F, D)$, such that

(i) We have

$$\rho\mid_{I_v} = \pi_{v,\overline{x}}\mid_{I_v} \tag{1.2}$$

for each finite place $v \notin S_\rho(\overline{x})$.

(ii) Each place $v \in S_\rho(\overline{x})$ is totally split in $\mathcal{F}/F$.

Hence, for each v at which $\overline{x}$ is ramified, ρ is also ramified, and we have that

$$\mathrm{Det}(\mathbf{r}_D(\varphi(\rho_v))) = \mathrm{Det}(\mathbf{r}_D(\varphi(\pi_{v,\overline{x}}))),$$

using the notation established in (1.1) above concerning Stickelberger factorisations. As $\overline{x}$ is fully ramified, we see from the proof of [1, Theorem 13.6] that ρ is surjective, and so F_ρ is a field. We also see that, as $\overline{x} \in \mathrm{LC}(O_F D)_S$, the extension F_ρ/F is unramified at all places dividing $|G|$, and so in particular is unramified at all places lying above l. Hence, as $F \cap \mu_l = \{1\}$ by hypothesis, it follows that $F_\rho \cap \mu_l = \{1\}$ also.

For each finite place v of F, we are now going to use the fact that $x \in \mathrm{LC}(O_F G)_S$ to construct a lift $\tilde{\rho}_v \in \mathrm{Hom}(\Omega_{F_v}, G)$ of ρ_v such that $[\tilde{\rho}_v] \in H^1_t(F_v, G)$ with

$$\tilde{\rho}_v\mid_{I_v} = \pi_{v,x}\mid_{I_v} \tag{1.3}$$

for all places v at which x is ramified.

Write

$$\rho_v = \rho_{v,r} \cdot \rho_{v,nr},$$

with $[\rho_{v,nr}] \in H^1_{nr}(F_v, D)$ (see [1, (7.7)]). Since $\rho_{v,nr}$ is unramified, [1, Proposition 15.2] implies that $[\rho_{v,nr}]$ may be lifted to $[\tilde{\rho}_{v,nr}] \in H^1_{nr}(F_v, G)$. Let $a(\tilde{\rho}_{v,nr})$ be a normal integral basis generator of $F_{\tilde{\rho}_{v,nr}}/F_v$.

(A) Suppose first that $v \notin S_\rho(\overline{x})$. If $\varphi(\pi_{v,x}) = \varphi_{v,s}$, then $\varphi(\pi_{v,\overline{x}}) = \varphi_{v,\overline{s}}$, where $\overline{s} = q(s)$, and so we have

$$\varphi(\rho_v) = \varphi(\pi_{v,\overline{x}}) = \varphi_{v,\overline{s}}$$

(see (1.2)).

It follows that $\mathbf{r}_G(a(\tilde{\rho}_{v,nr})) \cdot \mathbf{r}_G(\varphi_{v,s})$ is the resolvend of a normal integral basis generator of a tame Galois G-extension $F_{\tilde{\rho}_v}/F_v$ such that $q([\tilde{\rho}_v]) = \rho_v$ (cf. [1, Corollary 7.8 and Theorem 7.9]). As $\varphi(\pi_{v,x}) = \varphi_{v,s}$, we see from the construction of $\tilde{\rho}$ that

$$\tilde{\rho}_v \mid_{I_v} = \pi_{v,x} \mid_{I_v} = \tilde{\varphi}_{v,s},$$

where $[\tilde{\varphi}_{v,s}] \in H^1_t(I_v, G)$ is defined in [1, Remark 7.11]. The map $\tilde{\rho}_v$ is our desired lift of ρ_v.

(B) Suppose now that $v \in S_\rho(\overline{x})$ with $\varphi(\rho_v) = \varphi_{v,\overline{s}}$, say. Then v is totally split in $\mathcal{F}/F$, and so $\Sigma_v(G) = G$ (see Remark 1.4). Hence, if we choose any $s \in G$ such that $q(s) = \overline{s}$, then, arguing just as in (A) above, we see that $\mathbf{r}_G(a(\tilde{\rho}_{v,nr})) \cdot \mathbf{r}_G(\varphi_{v,s})$ is the resolvend of a normal integral basis generator of a tame Galois G-extension $F_{\tilde{\rho}_v}/F_v$ such that $q([\tilde{\rho}_v]) = \rho_v$. We have that

$$\tilde{\rho}_v \mid_{I_v} = \tilde{\varphi}_{v,s}.$$

We are now ready to apply the results contained in [1, Section 15]. Consider the following diagram:

$$\begin{array}{ccccccccc} 0 & \longrightarrow & B & \longrightarrow & G & \xrightarrow{q} & D & \longrightarrow & 0 \\ & & & & & & \big\uparrow{\scriptstyle\rho} & & \\ & & & & & & \Omega_F & & \end{array}$$

The group D acts on B via inner automorphisms, and we view B as being an Ω_F-module via ρ. Then B is a simple Ω_F-module because B is a minimal normal subgroup of G and ρ is surjective. The field of definition $F(B)$ of B is contained in the field F_ρ, and so in particular $F(B)$ contains no non-trivial l-th roots of unity. We are going to construct an element $\Pi_2 \in \mathcal{H}om_D(\Omega_F, G)$ satisfying the following properties:

(i) $\Pi_2 \mid_{I_v} = \pi_{v,x} \mid_{I_v}$ for each finite place $v \notin S_{\Pi_2}(x)$;

(ii) Each place $v \in S_{\Pi_2}(x)$ is totally split in $\mathcal{F}/F$.

(iii) Π_2 is unramified at all places in S.

This will be accomplished in the following two steps:

I. We begin by observing that our construction above of a lift $\tilde{\rho}_v$ of ρ_v for each finite v shows that $J_f(\mathcal{H}om_D(\Omega_F, G))$ is non-empty. Let

$$\mathcal{S} := \{v : x \text{ is ramified at } v\} \cup S \cup S_\rho(\overline{x}).$$

[1, Theorem 15.1] implies that there exists $\Pi_1 \in \mathcal{H}om_D(\Omega_F, G)$ such that $\Pi_{1,v} = \tilde{\rho}_v$ for all $v \in \mathcal{S}$.

Note also that Π_1 may well be ramified outside $\mathcal{S}$.

II. Recall that $\mathcal{H}om_D(\Omega_F, G)$ (respectively $\mathcal{H}om_D(\Omega_{F_v}, G)$ for each finite v) is a principal homogeneous space over $H^1(F, B)$ (respectively $H^1(F_v, B)$). Let $\mathcal{S}_1$ denote the set of finite places $v \notin \mathcal{S}$ of F at which Π_1 is ramified. For each $v \in \mathcal{S}_1$, choose $y_v \in H^1(F_v, B)$ so that $y_v \cdot \Pi_{1,v} \in \mathcal{H}om_D(\Omega_{F_v}, G)$ is unramified.

[1, Theorem 15.3] implies that there exists an element $z \in H^1(F, B)$ such that

(z1) $z_v = y_v$ for all $v \in \mathcal{S}_1$;

(z2) $z_v = 1$ for all $v \in \mathcal{S}$;

(z3) If $v \notin \mathcal{S} \cup \mathcal{S}_1$, then z_v is cyclic, and if z_v is ramified, then v splits completely in the abelian extension $(F(B) \cdot \mathcal{F})/F$.

Set

$$\Pi_2 := z \cdot \Pi_1 \in \mathcal{H}om_D(\Omega_F, G).$$

Then it follows from the construction of Π that

$$\Pi_2|_{I_v} = \pi_{v,x}\,|_{I_v}$$

for each finite place v of F at which x is ramified, and that $S_{\Pi_2}(x)$ consists precisely of the places $v \notin \mathcal{S} \cup \mathcal{S}_1$ at which z is ramified. It follows from (z3) that each place $v \in S_{\Pi_2}(x)$ is totally split in $\mathcal{F}/F$.

We have thus shown that that $\mathrm{LC}(O_F G)_S$ satisfies Property $\mathrm{Sp}(\mathcal{F}/F)$, as asserted. This completes the proof of part (a).

We now turn to the proof of part (b). Suppose in addition that B is central in G. Then Ω_F acts trivially on B. Taking $\Gamma = B$ in Definition 1.6, we may also suppose that $F_{\mathfrak{a}^N} \subseteq \mathcal{F}$. In this case, after carrying out steps I and II above, we may use Theorem 1.7 to eliminate all ramification of Π_2 in $S_{\Pi_2}(x)$ by carrying out the following additional step.

III. We have shown in Step II above that each place $v \in S_{\Pi_2}(x)$ is totally split in $\mathcal{F} \supseteq F(\mathfrak{a}^N)$. Hence Theorem 1.7 implies that for each $v \in S_{\Pi_2}(x)$, we may choose $b(v) \in H^1(F, B)$ such that

(b1) $b(v)_w = 1$ for all $w \in \mathcal{S}$;
(b2) $b(v) \mid_{I_v} = z_v^{-1} \mid_{I_v}$;
(b3) $b(v)$ is unramified away from v.

Set

$$\Pi_3 := \left[\left(\prod_{v \in S_{\Pi_2(x)}} b(v) \right) \cdot z \right] \cdot \Pi_2.$$

Then it follows directly from the construction of Π_2 that we have

$$\Pi_3 \mid_{I_v} = \pi_{v,x} \mid_{I_v} \tag{1.4}$$

for all finite places v of F.

We claim that

$$x = \Psi(\Pi_3).$$

To show this, let $\tau = \Psi(\Pi_3)^{-1} \cdot x$. We see from (1.4) that

$$\lambda_v(\tau) \in \mathrm{Im}(\Psi_v^{nr})$$

for every finite place v of F. As either G admits no non-trivial irreducible symplectic characters or F has no real places, and as $(h_F, |G|) = 1$ by hypothesis, [1, Proposition 6.8(b)] implies that $\tau = 0$. Hence $x = \Psi(\Pi_3)$, as claimed.

This completes the proof that $\mathrm{LC}(O_F G)_S$ satisfies Property R. □

Remark 1.9. It follows from Proposition 1.5 that in Theorem 1.8, we may take D to be a finite abelian group of arbitrary order (subject of course to the obvious constraint that all other conditions of Theorem 1.8 are satisfied). This enables one to show that Property $\mathrm{Sp}(\mathcal{F}/F)$ (for $\mathcal{F}/F$ as in Theorem 1.8) holds for many non-abelian groups of even order (e.g. S_3). However, if for example G is a non-abelian 2-group (e.g. H_8), then because $\mu_2 \subseteq F$ for any number field F, we can no longer appeal to Neukirch's Lifting Theorem, and our proof of Theorem 1.8 fails. It appears very likely that new ideas are needed to establish Property $\mathrm{Sp}(\mathcal{F}/F)$ in such cases (cf. also the remarks contained in the final paragraph of [4, Introduction], where a similar difficulty is briefly discussed in the context of the inverse Galois problem for finite groups). □

Remark 1.10. Suppose that $F = \mathbf{Q}$ and $G = S_3$, and consider the exact sequence of groups

$$0 \to C_3 \to S_3 \to C_2 \to 0.$$

Theorem 1.8 implies that if S is any set of rational primes containing 2 and 3, and if $\mathcal{F}$ is any extension of $\mathbf{Q}$ such that $\mathbf{Q}(\zeta_6)^+ \subseteq \mathcal{F}$, then $\mathrm{LC}(\mathbf{Z}S_3)_S$ satisfies Property $\mathrm{Sp}(\mathcal{F}/F)$. We shall now show that $\mathrm{LC}(\mathbf{Z}S_3)$ does not satisfy Property R by constructing examples of fully ramified, locally cohomological classes in $K_0(\mathbf{Z}S_3, \mathbf{Q}^c)$ which are not cohomological. This also shows that [1, Conjecture B] is false in general.

To do this, we first observe that there is a unique S_3 field extension of $\mathbf{Q}$ ramified only at 23, and its ramification index at 23 is equal to 2 (per [3]). Write $[\pi_{23}] \in H^1_t(\mathbf{Q}, S_3)$ for the tame cohomology class corresponding to this extension.

Suppose that $p \equiv 1 \pmod 3$ is prime. Write $L(p)$ for the unique subfield of $\mathbf{Q}(\zeta_3)$ such that $L(p)/\mathbf{Q}$ is a C_3-extension; this extension is totally ramified at p, and is unramified at all other finite primes. Write $[\pi(p)] \in H^1_t(\mathbf{Q}, C_3)$ for the tame cohomology class corresponding to to the extension $L(p)/\mathbf{Q}$. Let $[\pi_p] \in H^1_t(\mathbf{Q}, S_3)$ denote the image of $[\pi(p)]$ under the natural map $H^1(\mathbf{Q}, C_3) \to H^1(\mathbf{Q}, S_3)$, so $\mathbf{Q}_{\pi_p} \simeq L(p) \oplus L(p)$. The ramification index of $\mathbf{Q}_{\pi_p}/\mathbf{Q}$ at p is plainly equal to 3.

The class $x_{p,23} := \Psi_{S_3}([\pi_{23}]) \cdot \Psi_{S_3}([\pi_p]) \in K_0(\mathbf{Z}S_3, \mathbf{Q}^c)$ is locally cohomological and fully ramified. Hence, if it were cohomological, it would correspond to an S_3 field extension of $\mathbf{Q}$ ramified at p and 23, and unramified at all other finite primes. However, if e.g. $p < 61$, then no such extension exists (again per [3]). $\square$

Theorem 1.8 implies the following result for finite groups G of odd order.

Theorem 1.11. *Let G be of odd order, and let S be any finite set of finite places of F containing all places dividing $|G|$. Suppose that F contains no non-trivial $|G|$-th roots of unity.*

(a) If $\mathcal{F}/F$ is any finite abelian extension with $F_{|G|} \subseteq \mathcal{F}$, then $\mathrm{LC}(O_F G)_S$ *satisfies Property* $\mathrm{Sp}(\mathcal{F}/F)$*.*

(b) If G is nilpotent and $(|G|, h_F) = 1$, then $\mathrm{LC}(O_F G)_S$ *satisfies Property R.*

Proof. We first note that Proposition 1.5 implies that the if G is abelian, then $\mathrm{LC}(O_F G)_S$ satisfies Property R, and so in particular satisfies Property $\mathrm{Sp}(\mathcal{F}/F)$ for *any* finite extension $\mathcal{F}/F$.

Suppose now that G is an arbitrary finite group of odd order. As $|G|$ is odd, a well known theorem of Feit and Thompson (see [2]) implies that G is soluble. Hence G has an abelian minimal normal subgroup B such that $l \cdot B = 0$ for some odd prime l (see e.g. [5, Theorem 5.24]), and there is an exact sequence

$$0 \to B \to G \to D \to 0$$

with D soluble. We may therefore suppose by induction that $\mathrm{LC}(O_F D)_S$ satisfies Property $\mathrm{Sp}(\mathcal{F}/F)$. Part (a) now follows from Theorem 1.8(a).

If in addition G is nilpotent, then the group B above may be taken to be central in G, and D is also nilpotent. As G is of odd order, neither G nor D admit any non-trivial irreducible symplectic characters. We may therefore suppose by induction that $\mathrm{LC}(O_F D)_S$ satisfies Property R. Part (b) now follows from Theorem 1.8(b). □

We can now prove the following result for nilpotent groups of odd order.

Theorem 1.12. *Let G be a finite nilpotent group of odd order. Assume that F contains no non-trivial $|G|$-th roots of unity, and that $(|G|, h_F) = 1$.*

Then $\mathcal{R}(O_F G)$ is a subgroup of $\mathrm{Cl}(O_F G)$. If $c \in \mathcal{R}(O_F G)$, then there exist infinitely many $[\pi] \in H^1_t(F, G)$ such that F_π is a field and $(O_\pi) = c$. The extensions F_π/F may be chosen to have ramification disjoint from any finite set of finite places S of F containing all places dividing $|G|$.

Proof. Let S be any finite set of finite places of F containing all places dividing $|G|$. We have shown in Theorem 1.11(b) that $\mathrm{LC}(O_F G)_S$ satisfies Property R. The result now follows from [1, Theorem 16.3]. □

In order to extend Theorem 1.12 to arbitrary finite groups of odd order, we shall require the following result.

Proposition 1.13. *Fix an ideal $\mathfrak{b}$ of O_F such that*

(i) $\mathfrak{b}$ is divisible by $|G|^n \cdot O_F$, where $n \geq 1$ is an integer large enough for the homomorphism $\Theta^t_{\mathfrak{b}}$ of [1, Proposition 11.6] *to be defined;*

(ii) $F(\zeta_{|G|}) \subseteq F_{\mathfrak{b}}$, where $F_{\mathfrak{b}}$ denotes the ray class field of F modulo $\mathfrak{b}$.

Let $s \in G$ with $s \neq e$, and suppose that v is a finite place of F which is totally split in $F_{\mathfrak{b}}/F$. (Note that Remark 1.4 implies that $\Sigma_v(G) = G$, and so $f_{v,s}$ is defined.) Then there exists $b(f_{v,s}) \in \mathrm{LC}(O_F G)$ with $\partial^0(b(f_{vs})) = 0$ such that

$$\lambda(b(f_{v,s})) = \alpha_{nr} \cdot K\Theta^t(f_{v,s}),$$

where $\alpha_{\mathrm{nr}} \in \prod_v \mathrm{Im}(\Psi_v^{\mathrm{nr}})$. (Hence, $b(f_{v,s})$ is ramified only at v.)

If G is abelian, then in fact $b(f_{v,s}) \in \mathrm{Im}(\Psi)$.

Proof. As v is totally split in $F_{\mathfrak{b}}/F$, the element $f_{v,s}$ maps to zero under the natural surjection $\mathbf{F}_S \to \mathrm{Cl}'^{+}_{\mathfrak{b}}(\Lambda(O_F G))$ (see [1, Proposition 11.5]). Hence it follows that there exist $\alpha_{nr} \in \prod_v \mathrm{Im}(\Psi_v^{\mathrm{nr}})$ and $\alpha_\infty \in \partial^1(K_1(F^c G))$ such that

$$\alpha_\infty \cdot \alpha^{\mathrm{nr}} \cdot K\Theta^t(f_{v,s}) = 1$$

i.e.

$$\alpha_\infty^{-1} = \alpha^{\mathrm{nr}} \cdot K\Theta^t(f_{v,s}). \tag{1.5}$$

We now see that the class $b(f_{v,s}) \in K_0(O_F G, F^c)$ represented by the idele

$$((1)_v, \alpha_\infty)) \in J(K_1(FG)) \times \mathrm{Det}(F^c G)$$

satisfies the required conditions. If in addition G is abelian, then $\mathrm{Im}(\Psi) = \mathrm{LC}(O_F G)$, and so in fact $b(f_{v,s}) \in \mathrm{Im}(\Psi)$, as asserted. □

The following result is a strengthening of [1, Theorem 16.3].

Theorem 1.14. *We retain the notation established in Proposition 1.13. Let $\mathcal{F}/F$ be a finite extension with $F_{\mathfrak{b}} \subseteq \mathcal{F}$, and let S be any finite set of finite places of F containing all places dividing $|G|$.*

Suppose that $\mathrm{LC}(O_F G)_S$ satisfies Property $\mathrm{Sp}(\mathcal{F}/F)$, and that $(|G^{\mathrm{ab}}|, h_F) = 1$. Assume also either that F has no real places or that G admits no irreducible, symplectic characters. Then $\mathcal{R}(O_F G)$ is a subgroup of $\mathrm{Cl}(O_F G)$. If $c \in \mathcal{R}(O_F G)$, then there exist infinitely many $[\pi] \in H^1_t(F, G)$ such that F_π is a field and $(O_\pi) = c$. The extensions F_π/F may be chosen to have ramification disjoint from S.

Proof. [1, Proposition 13.5] implies that

$$\partial^1(K_1(F^c G)) \cdot \mathrm{LC}(O_F G) = \partial^1(K_1(F^c G)) \cdot \mathrm{LC}(O_F G)_S.$$

Recall (see [1, Theorems 6.6 and 6.7]) that $\partial^1(K_1(F^c G)) \cdot \mathrm{LC}(O_F G)$ is a subgroup of $K_0(O_F G, F^c)$ because it is the kernel of the homomorphism

$$K_0(O_F G, F^c) \xrightarrow{\lambda} J(K_0(O_F G, F^c)) \to \frac{J(K_0(O_F G, F^c))}{\lambda[\partial^1(K_1(F^c G))] \cdot \mathrm{Im}\,\Psi^{\mathrm{id}}}.$$

Hence, to show that $\mathcal{R}(O_F G)$ is a subgroup of $\mathrm{Cl}(O_F G)$, it suffices to show that

$$\partial^0(\mathrm{Im}(\Psi)) = \partial^0(\mathrm{LC}(O_F G)_S).$$

Suppose therefore that $x \in \mathrm{LC}(O_F G)_S$. By multiplying x by sufficiently many elements of the form $b(f_{v,s_v})$, with $v \notin S$, v totally split in $\mathcal{F}/F$, and $\partial^0(b_{v,s}) = 0$, if necessary (see Proposition 1.13), we may suppose without loss of generality that x is fully ramified.

As $\mathrm{LC}(O_F G)_S$ satisfies Property $\mathrm{Sp}(\mathcal{F}/F)$, we may choose $\Pi \in \mathrm{Hom}(\Omega_F, G)$ with $[\Pi] \in H^1_t(F, G)$ such that:

(i) $\Pi \mid_{I_v} = \pi_{v,x} \mid_{I_v}$ for all finite places $v \notin S_\Pi(x)$.

(ii) Each place $v \in S_\Pi(x)$ of F is totally split in $\mathcal{F}/F$.

(iii) Π is unramified at all places in S.

We remark that F_Π is a field because Π is fully ramified.

For each $v \in S_\Pi(x)$, write

$$\Pi|_{I_v} = \tilde{\varphi}_{v,s_v}$$

(see [1, Remark 7.11]), and let $b(f_{v,s_v})$ denote the element defined in Proposition 1.13.

Next, we consider

$$y := x^{-1} \cdot \Psi([\Pi]) \cdot \prod_{v \in S_{\Pi(x)}} b(f_{v,s_v})^{-1}.$$

We see at once that $\lambda_v(y) \in \mathrm{Im}(\Psi_v^{\mathrm{nr}})$ for each finite place v of F. As $(|G^{\mathrm{ab}}|, h_F) = 1$ and either F has no real places or G admits no irreducible symplectic characters, [1, Proposition 6.8(c)] implies that $y = 0$. Since $\partial^0(b(f_{v,s_v})) = 0$ for each $v \in S_{\Pi(x)}$, it follows that

$$\partial^0(x) = \partial^0(\Psi([\Pi])).$$

This implies that $\partial^0(\mathrm{Im}(\Psi)) = \partial^0(\mathrm{LC}(O_F G)_S)$, and so $\mathcal{R}(O_F G)$ is a subgroup of $\mathrm{Cl}(O_F G)$, as claimed.

If $c \in \mathcal{R}(O_F G)$, then [1, Proposition 13.5] implies that there are infinitely many $x \in \mathrm{LC}(O_F G)_S$ such that x is fully ramified and $\partial^0(x) = c$. The remaining assertions of the Proposition follow at once via applying the immediately preceding argument to each such element x. $\square$

We can now prove [1, Theorem E].

Theorem 1.15. *Let G be of odd order and suppose that $(|G|, h_F) = 1$, where h_F denotes the class number of F. Suppose also that F contains no non-trivial $|G|$-th roots of unity. Then $\mathcal{R}(O_F G)$ is a subgroup of $\mathrm{Cl}(O_F G)$. If $c \in \mathcal{R}(O_F G)$, then there exist infinitely many $[\pi] \in H^1_t(F, G)$ such that F_π is a field and $(O_\pi) = c$. The extensions F_π/F may be chosen to have ramification disjoint from any finite set S of places of F.*

Proof. Let $\mathcal{F}/F$ be any abelian extension such that $F_{\mathfrak{b}} \subset \mathcal{F}$, where $\mathfrak{b}$ is any ideal of O_F satisfying the conditions listed in Proposition 1.13. As $|G|$ is odd, and F contains no $|G|$-th roots of unity, Theorem 1.11 implies that $\mathrm{LC}(O_F G)_S$ satisfies Property $\mathrm{Sp}(\mathcal{F}/F)$. The desired result is now an immediate consequence of Theorem 1.14. $\square$

References

[1] A. Agboola, L. McCulloh, *On the relative Galois module structure of rings of integers in tame extensions*, Algebra and Number Theory **12** (2018), 1824–1886.

[2] W. Feit, J. Thompson, *Solvability of groups of odd order*, Pacific J. Math **13** (1963), 775–1029.

[3] L-functions and modular forms database.

[4] J. Neukirch, *On solvable number fields*, Invent. Math. **33** (1979), 135–164.

[5] J. Rotman, *An introduction to the theory of groups (fourth edition)*, Springer, Berlin, 1995.

Department of Mathematics, University of California, Santa Barbara, CA 93106.

Email address: agboola@math.ucsb.edu

Department of Mathematics, University of Illinois, 1409 W. Green Street, Urbana, IL 61801.

Email address: mcculloh@math.uiuc.edu