ON FORMAL GROUPS AND TATE COHOMOLOGY IN LOCAL FIELDS

NILS ELLERBROCK AND ANDREAS NICKEL

ABSTRACT. Let L/K be a Galois extension of local fields of characteristic 0 with Galois group G. If $\mathcal{F}$ is a formal group over the ring of integers in K, one can associate to $\mathcal{F}$ and each positive integer n a G-module F_L^n which as a set is the n-th power of the maximal ideal of the ring of integers in L. We give explicit necessary and sufficient conditions under which F_L^n is a cohomologically trivial G-module. This has applications to elliptic curves over local fields and to ray class groups of number fields.

1. INTRODUCTION

Let L/K be a Galois extension of local fields with Galois group G and residue characteristic p. We denote the ring of integers in K and L by $\mathcal{O}_K$ and $\mathcal{O}_L$, respectively. Let $\mathfrak{P}_L$ be the maximal ideal in $\mathcal{O}_L$ and let n be a positive integer. Then $\mathfrak{P}_L^n$ is an $\mathcal{O}_K[G]$-module in a natural way. Köck [Köc04] has shown that $\mathfrak{P}_L^n$ is a projective $\mathcal{O}_K[G]$-module if and only if L/K is at most weakly ramified and $n \equiv 1 \mod g_1$, where g_1 denotes the cardinality of the first ramification group (which is the unique p-Sylow subgroup of the inertia subgroup of G). As $\mathfrak{P}_L^n$ is torsionfree as an $\mathcal{O}_K$-module, it is $\mathcal{O}_K[G]$-projective if and only if it is a cohomologically trivial G-module.

Now suppose that the local fields L and K are of characteristic 0. Then for sufficiently large n, the p-adic logarithm induces $\mathbb{Z}_p[G]$-isomorphisms $U_L^n \simeq \mathfrak{P}_L^n$, where $U_L^n := 1 + \mathfrak{P}_L^n$ are the principal units of level n. It follows that the $\mathbb{Z}_p[G]$-module U_L^n is cohomologically trival under the same conditions on L/K and n, at least if n is sufficiently large. Now it is very natural to ask whether this is still true for small n and maybe as well for local fields of positive characteristic. However, it is well known (and reproved in §2.7) that U_L^1 is cohomologically trivial if and only if L/K is at most *tamely* ramified. Nevertheless, we give an affirmative answer to this question in §2 whenever $n > 1$. The proof is rather elementary and requires only some basic knowledge on Tate cohomology and local class field theory.

Now let $\mathcal{F}$ be a formal group over $\mathcal{O}_K$ with formal group law F, where we again assume that the characteristic of K is 0. Then for each positive integer n one can define a $\mathbb{Z}_p[G]$-module $F_L^n = \mathcal{F}(\mathfrak{P}_L^n)$ which as a set equals $\mathfrak{P}_L^n$, but where addition is defined via F. Let $\mathbb{G}_a$ and $\mathbb{G}_m$ be the additive and the multiplicative formal group, respectively. Then we have $\mathbb{G}_a(\mathfrak{P}_L^n) = \mathfrak{P}_L^n$ and $\mathbb{G}_m(\mathfrak{P}_L^n) \simeq U_L^n$. This leads to the question whether F_L^n is cohomologically trivial under the same conditions on L/K and n as above. We again give an affirmative answer whenever $n > 1$ in §3. Moreover, we show that F_L^1 is cohomologically trivial whenever L/K is tamely ramified. Here, we build on results of Hazewinkel [Haz74] on norm maps of formal groups.

Date: Version of 6th December 2016.

2010 *Mathematics Subject Classification.* 14L05, 20J06, 12B25, 11G07.

Key words and phrases. formal groups, principal units, Tate cohomology, local fields, elliptic curves, ray class groups.

Finally, we give two applications in §4. First, we consider elliptic curves E/K. Then E defines a formal group over the ring of integers in K such that we may apply our main result of §3. In particular, we deduce a generalization of the following classical result of Mazur [Maz72]: When E has good reduction and L/K is unramified, then the norm map $E(L) \to E(K)$ is surjective. In fact, our approach gives rise to similar results when E/K has additive or split multiplicative reduction. Second, we consider finite Galois CM-extensions L/K of number fields. Generalizing a result of the second author [Nic11] we show that the minus p-part of certain ray class groups is cohomologically trivial whenever L/K is weakly ramified above a fixed prime p. When L/K is tamely ramified, such a result was essential in the proof of the p-minus part of the equivariant Tamagawa number conjecture for certain Tate motives [Nic11, Nic16]. We therefore believe that our result might be useful in this direction as well.

Acknowledgements. The authors acknowledge financial support provided by the DFG within the Collaborative Research Center 701 'Spectral Structures and Topological Methods in Mathematics'.

Notation and conventions. All rings are assumed to have an identity element and all modules are assumed to be left modules unless otherwise stated.

2. Cohomology of principal units

2.1. **Tate cohomology.** Let G be a finite group and let M be a $\mathbb{Z}[G]$-module. We denote by M^G and M_G the maximal submodule and maximal quotient of M upon which the action of G is trivial, respectively. For an integer q we write $H^q(G, M)$ for the q-th Tate cohomology group of G with coefficients in M. We recall that for $q > 0$ Tate cohomology coincides with usual group cohomology and that for $q < -1$ we have $H^q(G, M) = H_{-q-1}(G, M)$, where the right hand side denotes group homology of G in degree $(-q-1)$. Moreover, we have $H^0(G, M) = M^G/N_G(M)$, where $N_G := \sum_{\sigma \in G} \sigma \in \mathbb{Z}[G]$ and $N_G(M)$ denotes the image of the map

$$\begin{array}{rcl} N_G = N_{G,M} : M & \longrightarrow & M \\ m & \mapsto & N_G \cdot m. \end{array}$$

Finally, we let $\Delta(G)$ be the kernel of the natural augmentation map $\mathbb{Z}[G] \to \mathbb{Z}$ which sends each $\sigma \in G$ to 1. Then we have an equality $H^{-1}(G, M) = \ker(N_{G,M})/\Delta(G)M$.

Definition 2.1. Let G be a finite group and let M be a $\mathbb{Z}[G]$-module. Then M is called *cohomologically trivial* if $H^q(U, M) = 0$ for all $q \in \mathbb{Z}$ and all subgroups U of G.

Remark 2.2. We note that $H^0(G, M)$ vanishes if and only if the norm map $N_{G,M} : M \to M^G$ is surjective.

We recall the following observation (see Köck [Köc04, Proof of Lemma 1.4]).

Lemma 2.3. *Let N be a normal subgroup of G and let M be a $\mathbb{Z}[G]$-module. Suppose that $H^i(G/N, M^N) = 0$ and $H^i(N, M) = 0$ for all $i \in \mathbb{Z}$. Then $H^i(G, M) = 0$ for all $i \in \mathbb{Z}$.*

Proof. This follows from the Hochschild–Serre spectral sequence

$$H^p(G/N, H^q(N, M)) \implies H^{p+q}(G, M).$$

□

Now suppose that G is cyclic. Then for any $i \in \mathbb{Z}$ one has isomorphisms $H^i(G,M) \simeq H^{i+2}(G,M)$ by [NSW08, Proposition 1.7.1], and we let

$$h(M) := \frac{|H^0(G,M)|}{|H^1(G,M)|} = \frac{|H^{2r}(G,M)|}{|H^{2r+1}(G,M)|}, \quad r \in \mathbb{Z}$$

be the *Herbrand quotient* of M (whenever the quotient on the right hand side is well defined). The Herbrand quotient is multiplicative on short exact sequences of $\mathbb{Z}[G]$-modules (see [NSW08, Proposition 1.7.5]).

2.2. **Principal units.** If L is a local field, we denote the ring of integers in L by $\mathcal{O}_L$. We note that $\mathcal{O}_L$ is a complete discrete valuation ring and we let v_L be the corresponding normalized valuation. We put $\mathfrak{P}_L := \{x \in \mathcal{O}_L \mid v_L(x) > 0\}$ which is the unique maximal ideal in $\mathcal{O}_L$. The residue field $\lambda := \mathcal{O}_L/\mathfrak{P}_L$ is a finite field of characteristic $p := \mathrm{char}(\lambda) > 0$. We let $U_L := \mathcal{O}_L^\times$ be the group of units in L.

Definition 2.4. For each $n \in \mathbb{N}$ we put $U_L^n := 1 + \mathfrak{P}_L^n$ and call U_L^n the *group of principal units of level* n.

Each U_L^n is a subgroup of U_L of finite index. More precisely, one has (non-canonical) isomorphisms

$$U_L/U_L^1 \simeq \lambda^\times \tag{2.1}$$

$$U_L^n/U_L^{n+1} \simeq \lambda \tag{2.2}$$

for all $n \in \mathbb{N}$.

2.3. **Ramification groups.** Let L/K be a finite Galois extension of local fields with Galois group G. We denote the residue field of K by κ and put $f := [\lambda : \kappa]$. Let I be the inertia subgroup of G and $e := |I|$ the ramification index. Then G/I naturally identifies with $\mathrm{Gal}(\lambda/\kappa)$ and we have $[L:K] = |G| = e \cdot f$.

Definition 2.5. Let $i \geq -1$. Then we call

$$G_i := \{\sigma \in G \mid v_L(\sigma(x) - x) \geq i + 1 \, \forall x \in \mathcal{O}_L\}$$

the *i-th ramification group* of the extension L/K. We let g_i be the cardinality of G_i.

We note that the ramification groups form a descending chain of normal subgroups of G with abelian quotients (and thus the extension is solvable). One has $G_{-1} = G$, $G_0 = I$ and G_1 is the (unique) p-Sylow subgroup of I. We recall that the extension L/K is said to be *unramified* if $G_0 = 1$, *tamely ramified* if $G_1 = 1$ and *weakly ramified* if $G_2 = 1$.

If H is a subgroup of G, we obviously have $H_i = G_i \cap H$. We define

$$\begin{aligned} \phi = \phi_G : [-1,\infty) &\longrightarrow [-1,\infty) \\ s &\mapsto \int_0^s [G_0 : G_t]^{-1} dt, \end{aligned}$$

where $[G_0 : G_t] := [G_t : G_0]^{-1}$ if $t < 0$. Then $G_i H/H = (G/H)_{\phi_H(i)}$ for every normal subgroup H of G. The map ϕ is piecewise linear and strictly increasing. We let $\psi := \phi^{-1}$ be its inverse. For any $s \geq -1$ we then have the two inequalities

$$\phi(s) \leq s, \quad s \leq \psi(s). \tag{2.3}$$

We also recall from [Ser79, Chapter IV, §3] that for $s \geq 0$ we have the formula

$$\phi(s) = \frac{1}{g_0}\left((\sum_{i=1}^{\lfloor s \rfloor} g_i) + (s - \lfloor s \rfloor) g_{\lceil s \rceil}\right). \tag{2.4}$$

Here, we write $\lfloor s \rfloor$ for the largest integer which is less or equal to s, and $\lceil s \rceil$ for the least integer which is greater or equal to s. Finally, we will frequently use the fact that $\psi(n)$ is an integer whenever $n \geq -1$ is an integer [Ser79, Chapter IV, §3, Proposition 13].

2.4. **Statement of the main result.** The main result of this section is the following theorem.

Theorem 2.6. *Let L/K be a finite Galois extension of local fields with Galois group G. Let $n > 1$ be an integer. Then the G-module U_L^n is cohomologically trivial if and only if L/K is at most weakly ramified and $n \equiv 1 \mod g_1$. Moreover, the G-module U_L^1 is cohomologically trivial if and only if L/K is at most tamely ramified.*

The remaining part of this section is devoted to the proof of Theorem 2.6.

2.5. **Galois invariants of principal units.** We first recall the following result on Galois invariants of ideals in L.

Lemma 2.7. *Let L/K be a finite Galois extension of local fields and let n be an integer. Then we have an equality*

$$(\mathfrak{P}_L^n)^G = \mathfrak{P}_K^{1+\lfloor \frac{n-1}{e} \rfloor}.$$

Proof. This is [Köc04, Lemma 1.4 (a)]. □

Corollary 2.8. *Let L/K be a finite Galois extension of local fields and let $n \geq 1$ be an integer. Then we have an equality*

$$(U_L^n)^G = U_K^{1+\lfloor \frac{n-1}{e} \rfloor}.$$

Proof. As $U_L^n = 1 + \mathfrak{P}_L^n$, this is immediate from Lemma 2.7. □

2.6. **Cohomology in totally ramified extensions.** In this section we calculate the Herbrand quotient of U_L when L/K is a totally ramified cyclic extension. We begin with the following easy lemma.

Lemma 2.9. *Let L/K be a totally ramified Galois extension of local fields. Then the map $H^0(G, L^\times) \to H^0(G, \mathbb{Z})$ induced by the valuation $v_L : L^\times \to \mathbb{Z}$ is trivial.*

Proof. We have $H^0(G, L^\times) = K^\times / N_G(L^\times)$ and, as L/K is totally ramified, we have $H^0(G, \mathbb{Z}) = \mathbb{Z}/e\mathbb{Z}$. However, $v_L(x)$ is divisible by e for every $x \in K^\times$. □

Remark 2.10. In fact, the map $H^i(G, L^\times) \to H^i(G, \mathbb{Z})$ induced by the valuation is trivial for every $i \in \mathbb{Z}$ (see [Ser79, Chapter XII, §1, Exercise 2]). However, we will not need this more general statement.

Corollary 2.11. *Let L/K be a totally ramified cyclic Galois extension of local fields. Let $d := [L : K]$ be its degree. Then we have isomorphisms*

$$H^i(G, U_L) \simeq \mathbb{Z}/d\mathbb{Z}$$

for every $i \in \mathbb{Z}$. In particular, we have $h(U_L) = 1$.

Proof. We first observe that $H^{-1}(G,\mathbb{Z}) \simeq H^1(G,\mathbb{Z}) = \mathrm{Hom}(G,\mathbb{Z}) = 0$. As $H^1(G,L^\times)$ vanishes by Hilbert's Theorem 90, Lemma 2.9 and the long exact sequence in (Tate) cohomology of the short exact sequence

$$0 \longrightarrow U_L \longrightarrow L^\times \xrightarrow{v_L} \mathbb{Z} \longrightarrow 0$$

induces isomorphisms

$$H^1(G,U_L) \simeq H^0(G,\mathbb{Z}) = \mathbb{Z}/d\mathbb{Z}$$

and

$$H^0(G,U_L) \simeq H^0(G,L^\times) \simeq H^{-2}(G,\mathbb{Z}) \simeq G \simeq \mathbb{Z}/d\mathbb{Z}$$

by local class field theory. As $H^i(G,U_L) \simeq H^{i+2}(G,U_L)$ for every $i \in \mathbb{Z}$, we are done. □

2.7. **Tamely ramified extensions.** In this subsection we record two probably well-known results on the cohomology of principal units in tamely ramified extensions. We give proofs for convenience.

Proposition 2.12. *Let L/K be a tamely ramified Galois extension of local fields. Then U_L^n is cohomologically trivial for every integer $n \geq 1$.*

Proof. As U_L^n is a pro-p-group for every $n \geq 1$, we may and do assume that G is a p-group. In particular, we may assume that L/K is unramified. However, in this case the isomorphisms (2.1) and (2.2) are G-equivariant. The cohomology of λ and $\lambda^\times$ vanishes. Thus the result follows from the cohomological triviality of U_L in unramified extensions [NSW08, Proposition 7.1.2]. □

Proposition 2.13. *The group of principal units U_L^1 is cohomologically trivial if and only if L/K is tamely ramified.*

Proof. If L/K is tamely ramified, then U_L^1 is cohomologically trivial by Proposition 2.12. Now suppose that L/K is wildly ramified. Then there exists a subgroup of the inertia group of order p. Replacing G by this subgroup we may assume that G has order p and that L/K is totally ramified. As the index of U_L^1 in U_L is finite of order prime to p by (2.1), we then have isomorphisms $H^i(G,U_L^1) \simeq H^i(G,U_L)$ for all $i \in \mathbb{Z}$. Now Corollary 2.11 implies that U_L^1 is not cohomologically trivial. □

2.8. **Weakly ramified extensions.** Our first task in this subsection is to prove an analogue of Proposition 2.12 for weakly ramified extensions.

Proposition 2.14. *Let L/K be a weakly ramified Galois extension of local fields. Let $n > 1$ be an integer such that $n \equiv 1 \mod g_1$. Then U_L^n is cohomologically trivial.*

Proof. Let H be a subgroup of G. Then L/L^H is also weakly ramified and $n \equiv 1 \mod |H_1|$. So we may and do assume that $H = G$. As G is solvable, Lemma 2.3 and Proposition 2.12 imply that we may further assume that G is cyclic of order p, and that L/K is totally ramified. Then for $s \geq 1$ we have

$$\phi(s) = \frac{1}{p}(p+s-1)$$

by equation (2.4). This gives the second equality in the computation

$$\begin{aligned} N_G(U_L^n) &= U_L^{\lceil \phi(n) \rceil} \\ &= U_L^{1+\lceil \frac{n-1}{p} \rceil} \\ &= U_L^{1+\lfloor \frac{n-1}{p} \rfloor} \\ &= (U_L^n)^G, \end{aligned}$$

whereas the first is [Ser79, Chapter V, §3, Corollary 4], the third holds as $n \equiv 1 \mod p$ by assumption, and the last equality is Corollary 2.8. It follows that $H^0(G, U_L^n)$ vanishes. As the Herbrand quotient of a finite module is trivial [Ser79, Chapter VIII, §4, Proposition 8], it follows from (2.1), (2.2) and Corollary 2.11 that

$$h(U_L^n) = h(U_L) = 1.$$

Thus U_L^n is cohomologically trivial as desired. □

We now prove the following converse of Proposition 2.14.

Proposition 2.15. *Let L/K be a finite Galois extension of local fields with Galois group G and let $n \geq 1$ be an integer. Suppose that U_L^n is cohomologically trivial as G-module. Then it holds:*

(i) *We have that $n \equiv 1 \mod g_1$.*
(ii) *The extension L/K is at most weakly ramified.*

Proof. By Proposition 2.13 we may assume that $n > 1$. If U_L^n is cohomologically trivial as a G-module, then in particular as a G_1-module. We may therefore assume that $G = G_1$ and also that G is non-trivial. Then there is an integer $k \geq 1$ such that $|G| = g_1 = p^k$. We put $m := \lfloor \phi(n-1) \rfloor$. Then by (2.4) we have

$$m = \lfloor \phi(n-1) \rfloor = \left\lfloor \frac{1}{p^k} \sum_{i=1}^{n-1} g_i \right\rfloor = 1 + \left\lfloor \frac{1}{p^k} \sum_{i=2}^{n-1} g_i \right\rfloor \geq 1 + \left\lfloor \frac{n-2}{p^k} \right\rfloor \geq \left\lfloor \frac{n-1}{p^k} \right\rfloor. \tag{2.5}$$

We now consider the following chain of inclusions:

$$N_G(U_L^n) \subseteq N_G(U_L^{\psi(m)+1}) \subseteq U_K^{m+1} \subseteq U_K^{1+\lfloor \frac{n-1}{p^k} \rfloor}. \tag{2.6}$$

Here, the first inclusion follows from $m \leq \phi(n-1)$ and thus $\psi(m)+1 \leq n$. The second inclusion is [Ser79, Chapter V, §6, Proposition 8] and the last is due to (2.5). However, as $H^0(G, U_L^n)$ vanishes, Corollary 2.8 implies that

$$U_K^{1+\lfloor \frac{n-1}{p^k} \rfloor} = (U_L^n)^G = N_G(U_L^n).$$

Thus all inclusions in (2.6) are in fact equalities and therefore $m = \lfloor \frac{n-1}{p^k} \rfloor$. It now follows from (2.5) that

$$1 + \left\lfloor \frac{n-2}{p^k} \right\rfloor = \left\lfloor \frac{n-1}{p^k} \right\rfloor$$

and thus (i) holds. Now choose $t \in \mathbb{Z}$ such that $G_t \neq 1$ and $G_{t+1} = 1$. Note that $t \geq 1$. If H is any subgroup of G, then one has $H_i = H \cap G_i$ for all $i \geq -1$. So we may further assume that $k = 1$ and thus we have

$$G = G_{-1} = G_0 = \cdots = G_t \simeq \mathbb{Z}/p\mathbb{Z}.$$

In this special situation we have

$$\phi(s) = \begin{cases} s & \text{if} \quad s \leq t, \\ t + \frac{s-t}{p} & \text{if} \quad s \geq t. \end{cases}$$

As $m = \lfloor \phi(n-1) \rfloor = \lfloor \frac{n-1}{p} \rfloor$, we have $n - 1 > t$ and thus

$$\left\lfloor \frac{n-1}{p} \right\rfloor = t + \left\lfloor \frac{n-1-t}{p} \right\rfloor.$$

This is only possible if $t = 1$ and therefore G_2 vanishes. □

Proof of Theorem 2.6. This now follows easily from Propositions 2.13, 2.14 and 2.15. □

3. Formal groups

The aim of this section is to generalize Theorem 2.6 to arbitrary formal groups over local fields of characteristic 0.

3.1. **Basic definitions and examples.**

Definition 3.1. Let R be a commutative ring. A (commutative) *formal group* $\mathcal{F}$ over R is given by a power series $F(X, Y) \in R[\![X, Y]\!]$ with the following properties:

(i) $F(X, Y) \equiv X + Y \mod (\deg 2)$.
(ii) $F(X, F(Y, Z)) = F(F(X, Y), Z)$.
(iii) $F(X, Y) = F(Y, X)$.

The power series F is called the *formal group law* of the formal group $\mathcal{F}$.

If R is a complete discrete valuation ring, then one can associate proper groups to a formal group over R.

Definition 3.2. Let R be a complete discrete valuation ring with maximal ideal $\mathfrak{m}$. Let $\mathcal{F}$ be a formal group over R with formal group law $F \in R[\![X, Y]\!]$. Then for every positive integer n one can associate to $\mathcal{F}$ the group $\mathcal{F}(\mathfrak{m}^n)$ which as a set equals $\mathfrak{m}^n$ with the new group law

$$x +_{\mathcal{F}} y = F(x, y), \quad x, y \in \mathcal{F}(\mathfrak{m}^n).$$

We will call $\mathcal{F}(\mathfrak{m}^n)$ the *associated group of level* n.

Examples 3.3. Let R be a commutative ring.

(i) The power series $F(X, Y) = X + Y$ obviously defines a formal group which is called the *additive formal group* and will be denoted by $\mathbb{G}_a$. If R is a complete discrete valuation ring with maximal ideal $\mathfrak{m}$, then one has $\mathbb{G}_a(\mathfrak{m}^n) = \mathfrak{m}^n$ as groups for every positive integer n.
(ii) The power series $F(X, Y) = X + Y + XY$ defines a formal group which is called the *multiplicative formal group* and will be denoted by $\mathbb{G}_m$. If $R = \mathcal{O}_L$ is the ring of integers in a local field L, then one has canonical isomorphisms $\mathbb{G}_m(\mathfrak{P}_L^n) \simeq U_L^n$ for every $n \in \mathbb{N}$.
(iii) Let L be a local field of characteristic 0 and let $\pi \in \mathfrak{P}_L$ be a uniformizer. Let q denote the cardinality of the residue field λ. Then for every power series $f \in \mathcal{O}_L[\![Z]\!]$ such that $f(Z) \equiv Z^q \mod \pi$ and $f(Z) \equiv \pi Z \mod Z^2$ there is a unique power series $F(X, Y) \in \mathcal{O}_L[\![X, Y]\!]$ such that $F(X, Y) \equiv X + Y \mod (\deg 2)$ and $f(F(X, Y)) = F(f(X), f(Y))$. This power series defines a formal group $\mathcal{F}_\pi$ over $\mathcal{O}_L$, the *Lubin–Tate formal group* associated to π. In fact, π determines

the formal group $\mathcal{F}_\pi$ up to isomorphism. We refer the reader to [LT65] for more details.

(iv) Let L be a local field of characteristic 0 and let E/L be an elliptic curve given by a minimal Weierstraß equation. Then E defines a formal group $\hat{E}$ over $\mathcal{O}_L$. The associated group of level n will be denoted by E_L^n. Then one has isomorphisms

$$E_L^n \simeq E_n(L) := \{(x,y) \in E(L) \mid v_L(x) \leq -2n\} \cup \{O\}\,.$$

Indeed by [Sil09, Chapter VII, Proposition 2.2] the map $E_1(L) \to E_L^1$, $(x,y) \mapsto -\frac{x}{y}$ is an isomorphism. As $2v_L(y) = 3v_L(x)$, we have $-\frac{x}{y} \in E_L^n$ if and only if $v_L(x) \leq -2n$ (see also [Sil09, Exercise 7.4]).

3.2. **Galois invariants.** For the rest of this section we let L/K be a finite Galois extension of local fields of characteristic 0. Recall the notation of §2. In particular, we have $G = \mathrm{Gal}(L/K)$ and e denotes the ramification index. If $\mathcal{F}$ is a formal group over $\mathcal{O}_K$ with formal group law $F \in \mathcal{O}_K[\![X,Y]\!]$, we put $F_L^n := \mathcal{F}(\mathfrak{P}_L^n)$ and $F_K^n := \mathcal{F}(\mathfrak{P}_K^n)$ for every positive integer n. As $\mathcal{F}$ is defined over $\mathcal{O}_K$, the Galois group G acts on the associated groups F_L^n.

Lemma 3.4. *Let $\mathcal{F}$ be a formal group over $\mathcal{O}_K$ and let $n > 0$ be an integer. Then we have an equality*

$$(F_L^n)^G = F_K^{1+\lfloor \frac{n-1}{e} \rfloor}.$$

Proof. This is immediate from Lemma 2.7. □

3.3. **The norm map.** Let $\mathcal{F}$ be a formal group over $\mathcal{O}_K$ and let $k > 0$ be an integer. If $x_1, \ldots, x_k$ belong to F_L^1, we let

$$\sum_{j\in J}^{\mathcal{F}} x_j := x_1 +_{\mathcal{F}} \cdots +_{\mathcal{F}} x_k,$$

where $J = \{1, \ldots, k\}$ and similarly for other index sets J.

Definition 3.5. Let $\mathcal{F}$ be a formal group over $\mathcal{O}_K$. We define a *norm map*

$$\begin{array}{rcl} N_G^{\mathcal{F}} : F_L^1 & \longrightarrow & F_K^1 \\ x & \mapsto & \displaystyle\sum_{\sigma\in G}^{\mathcal{F}} \sigma(x). \end{array}$$

We let $\mathrm{Tr}_{L/K} := N_G^{\mathbb{G}_a}$ and $N_{L/K} := N_G^{\mathbb{G}_m}$ be the usual trace and norm maps, respectively.

Lemma 3.6. *Let $\mathcal{F}$ be a formal group over $\mathcal{O}_K$ and let $x \in F_L^1$. Then there are $a_i \in \mathcal{O}_K$, $1 \leq i < \infty$, such that*

$$N_G^{\mathcal{F}}(x) \equiv \mathrm{Tr}_{L/K}(x) + \sum_{i=1}^{\infty} a_i (N_{L/K}(x))^i \mod \mathrm{Tr}_{L/K}(x^2\mathcal{O}_L).$$

Proof. This is [Haz74, Corollary 2.4.2]. □

3.4. **Norm maps in totally ramified extensions.** We first prove a generalization of [Ser79, Chapter V, §3, Proposition 4]. Let $t \in \mathbb{Z}$ be the last ramification jump, that is $G_t \neq 1$ and $G_{t+1} = 1$.

Proposition 3.7. *Let ℓ be a prime and suppose that L/K is totally ramified and cyclic of degree ℓ. Then for every $n \in \mathbb{N}$ we have inclusions*

(i) $N_G^{\mathcal{F}}(F_L^{\psi(n)}) \subseteq F_K^n$ *and*
(ii) $N_G^{\mathcal{F}}(F_L^{\psi(n)+1}) \subseteq F_K^{n+1}$.

Proof. We only prove (i), the proof of (ii) being similar. Let $x \in \mathfrak{P}_L^{\psi(n)}$. By Lemma 3.6 it suffices to show that $v_K(\mathrm{Tr}_{L/K}(x)) \geq n$ and $v_K(N_{L/K}(x)) \geq n$. As L/K is totally ramified, we indeed have

$$v_K(N_{L/K}(x)) = v_L(x) \geq \psi(n) \geq n,$$

where the last inequality is (2.3). For the trace one knows by [Ser79, Chapter V, §3, Lemma 4] that

$$v_K(\mathrm{Tr}_{L/K}(x)) \geq \left\lfloor \frac{(t+1)(\ell-1)+\psi(n)}{\ell} \right\rfloor. \tag{3.1}$$

If $n \leq t$ then $\psi(n) = n$ and so (3.1) implies that

$$v_K(\mathrm{Tr}_{L/K}(x)) \geq \left\lfloor \frac{(n+1)(\ell-1)+n}{\ell} \right\rfloor = \left\lfloor \frac{n\ell+\ell-1}{\ell} \right\rfloor = n.$$

If on the other hand $n \geq t$ we have $\psi(n) = t + \ell(n-t)$. Thus (3.1) simplifies to

$$v_K(\mathrm{Tr}_{L/K}(x)) \geq \left\lfloor \frac{n\ell+\ell-1}{\ell} \right\rfloor = n$$

as desired. □

Corollary 3.8. *Let ℓ be a prime and suppose that L/K is totally ramified and cyclic of degree ℓ. Then for every $n > t$ we have*

$$N_G^{\mathcal{F}}(F_L^{\psi(n)}) = F_K^n \quad \textit{and} \quad N_G^{\mathcal{F}}(F_L^{\psi(n)+1}) = F_K^{n+1}.$$

Proof. Proposition 3.7 implies that the norm map $N_G^{\mathcal{F}}$ induces maps

$$N_n^{\mathcal{F}} : F_L^{\psi(n)}/F_L^{\psi(n)+1} \longrightarrow F_K^n/F_K^{n+1}$$

for every $n \in \mathbb{N}$. Now let $m \geq n > t$ be integers. Then by [Sil09, Chapter IV, Proposition 3.2] we have a commutative diagram

$$\begin{array}{ccc} F_L^{\psi(m)}/F_L^{\psi(m)+1} & \xrightarrow{N_m^{\mathcal{F}}} & F_K^m/F_K^{m+1} \\ \downarrow \simeq & & \downarrow \simeq \\ U_L^{\psi(m)}/U_L^{\psi(m)+1} & \xrightarrow{N_m^{\mathbb{G}_m}} & U_K^m/U_K^{m+1} \end{array}$$

The maps $N_m^{\mathbb{G}_m}$ are surjective by [Ser79, Chapter V, §3, Corollary 2]. Thus the maps $N_m^{\mathcal{F}}$ are also surjective and likewise

$$F_L^{\psi(m)}/F_L^{\psi(m+1)} \twoheadrightarrow F_L^{\psi(m)}/F_L^{\psi(m)+1} \twoheadrightarrow F_K^m/F_K^{m+1}$$

for every $m \geq n > t$. Now [Ser79, Chapter V, §1, Lemma 2] implies that $N_G^{\mathcal{F}} : F_L^{\psi(n)} \to F_K^n$ is surjective. The second equality follows from the first and Proposition 3.7 via the chain of inclusions

$$F_K^{n+1} = N_G^{\mathcal{F}}(F_L^{\psi(n+1)}) \subseteq N_G^{\mathcal{F}}(F_L^{\psi(n)+1}) \subseteq F_K^{n+1}.$$

□

Corollary 3.9. *Let ℓ be a prime and suppose that L/K is totally ramified and cyclic of degree ℓ. Then for every $v > t$, $v \in \mathbb{R}$ we have*

$$N_G^{\mathcal{F}}(F_L^{\lceil \psi(v) \rceil}) = F_K^{\lceil v \rceil}.$$

Proof. The proof is completely analogous to [Ser79, Chapter V, §3, Corollary 4] using Proposition 3.7 and Corollary 3.8. □

Corollary 3.10. *Suppose that L/K is totally ramified. Then for every $n \in \mathbb{N}$ we have inclusions*

$$N_G^{\mathcal{F}}(F_L^{\psi(n)}) \subseteq F_K^n \quad \text{and} \quad N_G^{\mathcal{F}}(F_L^{\psi(n)+1}) \subseteq F_K^{n+1}.$$

Proof. As the Galois extension L/K is solvable, this follows from Proposition 3.7 by induction. □

3.5. **The cohomology of the associated groups.** We start with the following auxiliary result.

Lemma 3.11. *Suppose that L/K is cyclic of prime degree. Then $h(F_L^n) = 1$ for every $n \in \mathbb{N}$.*

Proof. As the index of F_L^{n+1} in F_L^n is finite, the Herbrand quotient $h(F_L^n)$ does not depend on n. So we may assume that n is sufficiently large such that the formal logarithms of $\mathcal{F}$ and $\mathbb{G}_m$ induce an isomorphism $F_L^n \simeq U_L^n$. If L/K is tamely ramified, we have $h(U_L^n) = 1$ by Theorem 2.6. If L/K is wildly ramified, then it is totally ramified and thus $h(U_L^n) = h(U_L) = 1$ by Corollary 2.11. □

Proposition 3.12. *Let L/K be tamely ramified. Then the associated groups F_L^n are cohomologically trivial for every $n \in \mathbb{N}$.*

Proof. If L/K is tamely ramified, then the ideals $\mathfrak{P}_L^n$ are cohomologically trivial by [Köc04, Theorem 1.1]. As we have isomorphisms $F_L^n/F_L^{n+1} \simeq \mathfrak{P}_L^n/\mathfrak{P}_L^{n+1}$ for every $n \in \mathbb{N}$, it suffices to show that F_L^1 is cohomologically trivial. By Lemma 2.3 we may suppose that L/K is cyclic of prime degree. The norm map $N_G^{\mathcal{F}} : F_L^1 \to F_K^1$ is surjective by [Haz74, Proposition 3.1] and thus $H^0(G, F_L^1)$ vanishes. Now the result follows from Lemma 3.11. □

Proposition 3.13. *Let L/K be weakly ramified and let $n > 1$ be an integer such that $n \equiv 1 \mod g_1$. Then F_L^n is cohomologically trivial.*

Proof. By Proposition 3.12 and Lemma 2.3 we may and do assume that L/K is cyclic of order p and totally ramified. We then have

$$(F_L^n)^G = F_K^{1+\lfloor \frac{n-1}{p} \rfloor} = F_K^{1+\lceil \frac{n-1}{p} \rceil} = N_G^{\mathcal{F}}(F_L^n).$$

Here, the first and last equality follow from Lemma 3.4 and Corollary 3.9, respectively. As $n \equiv 1 \mod p$, the remaining equality is also clear. We obtain $H^0(G, F_L^n) = 1$, and Lemma 3.11 again implies the result. □

We are now in a position to state and prove the main result of this section.

Theorem 3.14. *Let L/K be a finite Galois extension of local fields of characteristic 0 with Galois group G. Let $\mathcal{F}$ be a formal group over $\mathcal{O}_K$ with formal group law F and let $n > 1$ be an integer. Then F_L^n is a cohomologically trivial G-module if and only if L/K is weakly ramified and $n \equiv 1 \mod g_1$.*

Proof. Suppose that $n > 1$ is an integer such that F_L^n is cohomologically trivial. Then the same reasoning as in the proof of Proposition 2.15 using Lemma 3.4 and Corollary 3.10 shows that L/K is weakly ramified and $n \equiv 1 \mod g_1$. The converse also holds by Proposition 3.13. □

Remark 3.15. It is in general *not* true that F_L^1 is cohomologically trivial if and only if L/K is tamely ramified. In fact, even in the case $\mathcal{F} = \mathbb{G}_a$ Köck's result [Köc04, Theorem 1.1] shows that $\mathbb{G}_a(\mathfrak{P}_L) = \mathfrak{P}_L$ is cohomologically trivial if and only if L/K is weakly ramified. We now give a second example.

Example 3.16. We denote the absolute Galois group of $\mathbb{Q}_p$ by $G_{\mathbb{Q}_p}$ and let $\chi : G_{\mathbb{Q}_p} \to \mathbb{Z}_p^\times$ be an unramified character. Let $K/\mathbb{Q}_p$ be an unramified extension and put $\pi := p\chi(\varphi)$, where φ denotes the absolute Frobenius of $\mathbb{Q}_p$. We consider the Lubin–Tate formal group $\mathcal{F} = \mathcal{F}_\pi$ over $\mathcal{O}_K$. Now let L/K be a finite Galois extension with Galois group G and suppose that the absolute Frobenius φ_L of L does not belong to the kernel of χ. We put $\omega_L := v_{\mathbb{Q}_p}(1 - \chi(\varphi_L))$ and observe that $\omega_L \geq 0$. Then by [BC16, Lemma 4.1.1 and Theorem 4.2.3] there is a $\mathbb{Z}_p[G]$-module I and an exact sequence of $\mathbb{Z}_p[G]$-modules

$$0 \longrightarrow F_L^1 \longrightarrow I \longrightarrow I \longrightarrow \mathbb{Z}/p^{\omega_L}\mathbb{Z}(\chi) \longrightarrow 0.$$

The $\mathbb{Z}_p[G]$-module I is cohomologically trivial by [BC16, Lemma 4.1.2]. Now suppose that L/K is weakly and wildly ramified. Then $G_1 \neq 1$ and we have isomorphisms

$$H^i(G_1, F_L^1) \simeq H^{i-2}(G_1, \mathbb{Z}/p^{\omega_L}\mathbb{Z})$$

for every $i \in \mathbb{Z}$. It follows that F_L^1 is cohomologically trivial if and only if $\omega_L = 0$.

4. Applications

4.1. **Elliptic curves.** Let L/K be a finite Galois extension of local fields of characteristic 0 and let E/K be an elliptic curve given by a minimal Weierstraß equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with discriminant $\Delta \in \mathcal{O}_K$. We denote the reduction of E by $\overline{E}$ which is a not necessarily smooth curve over the residue field κ. We denote by $\overline{E}_{ns}(\lambda)$ the subset of $\overline{E}(\lambda)$ comprising all non-singular points. We let $E_0(L)$ be the set of L-rational points of E which have non-singular reduction. By [Sil09, Chapter VII, Proposition 2.1] one then has a short exact sequence

$$0 \longrightarrow E_1(L) \longrightarrow E_0(L) \longrightarrow \overline{E}_{ns}(\lambda) \longrightarrow 0. \tag{4.1}$$

Proposition 4.1. *Suppose that L/K is unramified and that E/K has good reduction. Then the set $E(L)$ of L-rational points is a cohomologically trivial G-module.*

Proof. We observe that we have $E_0(L) = E(L)$ and $\overline{E}_{ns}(\lambda) = \overline{E}(\lambda)$. Now E_L^1 is cohomologically trivial by Proposition 3.12, whereas $\overline{E}(\lambda)$ is cohomologically trivial by [Lan56, Proposition 3]. Moreover, we have $E_L^1 \simeq E_1(L)$ by [Sil09, Chapter VII, Proposition 2.2]. Now the result follows from sequence (4.1). □

Remark 4.2. If L/K is unramified and E has good reduction, then Proposition 4.1 in particular implies that the norm map $E(L) \to E(K)$ is surjective. This is a classical result of Mazur [Maz72, Corollary 4.4].

Proposition 4.3. *Suppose that L/K is unramified and that E/K has additive reduction. Then the set $E_0(L)$ is a cohomologically trivial G-module. If in addition the order of G is prime to 6, then also $E(L)$ is a cohomologically trivial G-module.*

Proof. We know that $E_L^1 \simeq E_1(L)$ is cohomologically trivial by Proposition 3.12. Likewise $\overline{E}_{ns}(\lambda) \simeq \lambda$ is cohomologically trivial, as L/K is unramified. It follows from sequence (4.1) that $E_0(L)$ is cohomologically trivial. As the index of $E_0(L)$ in $E(L)$ is at most 4 by the theorem of Kodaira and Néron [Sil09, Chapter VII, Theorem 6.1], the final claim is also clear. □

Proposition 4.4. *Suppose that L/K is unramified and that E/K has split multiplicative reduction. Then the set $E_0(L)$ is a cohomologically trivial G-module. If in addition the order of G is prime to $v_K(\Delta)$, then also $E(L)$ is a cohomologically trivial G-module.*

Proof. The first claim again follows from Proposition 3.12 and sequence (4.1) once we observe that $\overline{E}_{ns}(\lambda) \simeq \lambda^\times$ is cohomologically trivial. Likewise, the final claim again follows from the theorem of Kodaira and Néron [Sil09, Chapter VII, Theorem 6.1] which says that in this case $E(L)/E_0(L)$ is a cyclic group of order $v_L(\Delta) = v_K(\Delta)$. □

4.2. **Ray class groups.** In this section we let L/K be a finite Galois extension of number fields with Galois group G. If $\mathfrak{m}$ is an ideal of the ring of integers $\mathcal{O}_L$ in L, we write $\mathrm{cl}_L^{\mathfrak{m}}$ for the ray class group of L to the ray $\mathfrak{m}$. We say that the modulus $\mathfrak{m}$ is G-equivariant if $\sigma(\mathfrak{m}) = \mathfrak{m}$ for every $\sigma \in G$. In this case the ray class group $\mathrm{cl}_L^{\mathfrak{m}}$ is endowed with a natural G-action.

Now suppose that L/K is a CM-extension, so K is totally real, L is totally complex and complex conjugation induces a unique automorphism $j \in G$ which is indeed central in G. If M is a G-module, we denote by M^+ and M^- the submodules of M upon which j acts by $+1$ and -1, respectively. When $\mathfrak{m}$ is G-equivariant, we put $A_L^{\mathfrak{m}} := (\mathrm{cl}_L^{\mathfrak{m}})^-$.

Now let p be a prime. For every prime $\mathfrak{p}$ in K above p we choose a prime $\mathfrak{P}$ in L above $\mathfrak{p}$. We say that L/K is weakly ramified above p if the local extensions $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ are weakly ramified for all primes $\mathfrak{p}$ in K above p. We let $e_{\mathfrak{p}}$ be the ramification index of the extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$ which does not depend on the choice of the prime $\mathfrak{P}$. We write $e_{\mathfrak{p}} = p^{k_{\mathfrak{p}}} e'_{\mathfrak{p}}$, where $k_{\mathfrak{p}}$ and $e'_{\mathfrak{p}}$ are integers such that $e'_{\mathfrak{p}}$ is not divisible by p.

Theorem 4.5. *Let L/K be a Galois CM-extension of number fields with Galois group G. Let p be an odd prime and suppose that L/K is weakly ramified above p. Choose a G-equivariant modulus*

$$\mathfrak{m} = \prod_{\mathfrak{P}} \mathfrak{P}^{n_{\mathfrak{P}}}$$

such that:

(i) *if $\mathfrak{p}$ is a prime that ramifies in L/K, then $\mathfrak{P}$ divides $\mathfrak{m}$;*
(ii) *we have $n_{\mathfrak{P}} \equiv 1 \mod p^{k_{\mathfrak{p}}}$ and $n_{\mathfrak{P}} \neq 1$ for every prime $\mathfrak{P}$ above p;*
(iii) *if ζ is a root of unity in L such that $\zeta \equiv 1 \mod \mathfrak{m}$, then $\zeta = 1$.*

Then the $\mathbb{Z}_p[G]$-module $A_L^{\mathfrak{m}} \otimes_{\mathbb{Z}} \mathbb{Z}_p$ is cohomologically trivial.

Proof. Using Theorem 2.6 this may be proved along the lines of [Nic11, Theorem 1]. □

Remark 4.6. Condition (iii) on the modulus $\mathfrak{m}$ is satisfied when $\mathfrak{m}$ is divisble by at least two primes with different residue characteristic. In particular, whenever L/K is weakly ramified above p, there exists a modulus $\mathfrak{m}$ with the above properties.

Remark 4.7. When L/K is tamely ramified above p, a variant of this result has been established by the second author [Nic11, Theorem 1]. This was an essential step in the proof of (the minus part of) the equivariant Tamagawa number conjecture for certain tamely ramified CM-extensions [Nic16].

Remark 4.8. In characteristic 0 it is easy to prove Theorem 2.6 when we choose n sufficiently large. However, in order to generalize the aforementioned results on the equivariant Tamagawa number conjecture to weakly ramified extensions, one most likely has to apply Theorem 4.5 for infinitely many Galois extensions L_m/K_m, $m \in \mathbb{N}$, where L_m denotes the m-th layer in the cyclotomic $\mathbb{Z}_p$-extension of L. Moreover, one has to choose compatible moduli for each layer m and this is only possible when we take the full strength of Theorem 4.5 (and thus of Theorem 2.6) into account.

References

[BC16] Werner Bley and Alessandro Cobbe, *The equivariant local ϵ-constant conjecture for unramified twists of $\mathbb{Z}_p(1)$*, to appear in Acta Arith., 2016.

[Haz74] Michiel Hazewinkel, *On norm maps for one dimensional formal groups. I. The cyclotomic Γ-extension*, J. Algebra **32** (1974), 89–108. MR 0349692

[Köc04] Bernhard Köck, *Galois structure of Zariski cohomology for weakly ramified covers of curves*, Amer. J. Math. **126** (2004), no. 5, 1085–1107. MR 2089083

[Lan56] Serge Lang, *Algebraic groups over finite fields*, Amer. J. Math. **78** (1956), 555–563. MR 0086367

[LT65] Jonathan Lubin and John Tate, *Formal complex multiplication in local fields*, Ann. of Math. (2) **81** (1965), 380–387. MR 0172878

[Maz72] Barry Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266. MR 0444670

[Nic11] Andreas Nickel, *On the equivariant Tamagawa number conjecture in tame CM-extensions*, Math. Z. **268** (2011), no. 1-2, 1–35. MR 2805422

[Nic16] ———, *Integrality of Stickelberger elements and the equivariant Tamagawa number conjecture*, J. Reine Angew. Math. **719** (2016), 101–132. MR 3552493

[NSW08] Jürgen Neukirch, Alexander Schmidt, and Kay Wingberg, *Cohomology of number fields*, second ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008. MR 2392026

[Ser79] Jean-Pierre Serre, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York-Berlin, 1979, Translated from the French by Marvin Jay Greenberg. MR 554237

[Sil09] Joseph H. Silverman, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009. MR 2514094

Universität Bielefeld, Fakultät für Mathematik, Postfach 100131, Universitätsstr. 25, 33501 Bielefeld, Germany

E-mail address: nils.ellerbrock@uni-bielefeld.de

Universität Bielefeld, Fakultät für Mathematik, Postfach 100131, Universitätsstr. 25, 33501 Bielefeld, Germany

E-mail address: anickel3@math.uni-bielefeld.de

URL: http://www.math.uni-bielefeld.de/∼anickel3/english.html