ANNALES

DE

L'INSTITUT FOURIER

Cyril DEMARCHE,
Giancarlo LUCCHINI ARTECHE & Danny NEFTIN

The Grunwald problem and approximation properties for homogeneous spaces

THE GRUNWALD PROBLEM AND APPROXIMATION PROPERTIES FOR HOMOGENEOUS SPACES

by Cyril DEMARCHE,
Giancarlo LUCCHINI ARTECHE & Danny NEFTIN (*)

———

Abstract. — Given a group G and a number field K, the Grunwald problem asks whether given field extensions of completions of K at finitely many places can be approximated by a single field extension of K with Galois group G. This can be viewed as the case of constant groups G in the more general problem of determining for which K-groups G the variety SL_n/G has weak approximation. We show that away from an explicit set of bad places both problems have an affirmative answer for iterated semidirect products with abelian kernel. Furthermore, we give counterexamples to both assertions at bad places. These turn out to be the first examples of transcendental Brauer–Manin obstructions to weak approximation for homogeneous spaces.

Résumé. — Pour un groupe G et un corps de nombres K, le problème de Grunwald est le suivant : étant données des extensions des complétés de K en un ensemble fini de places, peut-on les approcher de façon simultanée par une seule extension de K de groupe de Galois G ? Cela peut être interprété comme un cas particulier de la question plus générale de déterminer pour quels K-groupes G la variété SL_n/G vérifie l'approximation faible. Nous démontrons qu'en dehors d'un ensemble explicite de mauvaises places, ces deux problèmes ont une réponse positive pour les groupes obtenus par des produits semi-directs itérés à noyau abélien. En outre, nous donnons des contre-exemples aux deux affirmations dans l'ensemble des mauvaises places. Ceux-ci sont par ailleurs les premiers exemples d'obstructions de Brauer–Manin transcendantes à l'approximation faible pour les espaces homogènes.

———

1. Introduction

The Grunwald–Wang theorem has fundamental applications to the structure theory of finite dimensional semisimple algebras, cf. [12, Ch. 18], and provides an answer for abelian groups G to the more general Grunwald problem. The latter is an inverse Galois problem of increasing interest due to its recently studied connections with the regular inverse Galois problem and with weak approximation, cf. [3, 6].

Fix a number field K, let K_v denote the completion of K at a place v, and $\mathrm{Gal}(K)$ denote its absolute Galois group. Let G be a finite group, and S a finite set of places of K. The Grunwald problem then asks whether every prescribed local Galois extensions $L^{(v)}/K_v$, $v \in S$, with embeddings $\mathrm{Gal}(L^{(v)}/K_v) \hookrightarrow G$ can be approximated by a global extension L/K with Galois group G. More precisely:

GRUNWALD PROBLEM. — *Is the restriction map*

$$\mathrm{Hom}(\mathrm{Gal}(K), G) \to \prod_{v \in S} \mathrm{Hom}(\mathrm{Gal}(K_v), G)/ \sim$$

surjective?

Here $\phi_1 \sim \phi_2$ if $\phi_1 = g\phi_2 g^{-1}$ for some $g \in G$. Note that the quotient by $\sim$ is necessary since the decomposition group of a place v of K is defined up to conjugation.

Families of groups G and number fields K for which (G, K, S) has an affirmative answer to the Grunwald problem for every S include: (1) abelian groups of odd order over every number field, by the Grunwald–Wang theorem [5, 16]; (2) solvable groups of order prime to the number of roots of unity in K, by Neukirch's theorem [10]; and (3) groups with a generic extension over K, by Saltman's theorem [13].

Recent results by Dèbes-Ghazi on the inverse Galois problem [3] and by Harari on weak approximation for homogeneous spaces [6], suggest that for every finite group G there exists a finite set $T := T(G, K)$ of "bad places" of K such that the Grunwald problem has an affirmative answer for (G, K, S) for every set S that is disjoint from T. In fact, the existence of such a set T is implied by a conjecture of Colliot-Thélène on the Brauer–Manin obstruction for rationally connected varieties. The connection is done by considering the following more general version of the Grunwald problem for finite K-groups G.

APPROXIMATION PROPERTY. — *A K-group G has* (weak) *approxima-tion in a set S of places of K if the natural restriction map*

$$\mathrm{H}^1(K, G) \to \prod_{v \in S} \mathrm{H}^1(K_v, G),$$

is surjective. We shall say G has approximation away from T, *if G has approximation in S for every finite set S of places of K that is disjoint from T.*

The approximation property for every finite $S \subset \Omega_K$ is equivalent to weak approximation for certain homogeneous spaces (hence its name), see Section 2.5. Moreover, for constant groups G, it is equivalent to a positive answer to the Grunwald problem for (G, K, S), see Section 2.3.

The existence of a finite set T of "bad places" away from which the approximation property holds is expected to hold for arbitrary finite K-groups, and is strongly related with arithmetic properties of homogeneous spaces. Moreover, the existence of such a set T for K-groups has been proved over arbitrary number fields K for: (1) abelian K-groups G by Wang, cf. [16]; (2) iterated semidirect products $G = A_1 \rtimes (A_2 \rtimes \cdots \rtimes A_r)$ of abelian K-groups by Harari, cf. [6]; and (3) solvable K-groups G of order prime to the number of roots of unity in an extension of K splitting G by the second author (here $T = \emptyset$, cf. [8]).

Ever since Wang's work on the subject, triples (G, K, S) having a neg-ative answer to the Grunwald problem (and thus not having the approxi-mation property) are known to exist. However, it is unclear what the set $T = T(G, K)$ should be. In fact, there is no explicit description of a set T even for basic groups such as semidirect products of two abelian p-groups.

This paper gives both affirmative and negative answers to the Grun-wald problem and the approximation property, suggesting that the set $T = T(G, K)$ can always be taken to be the union of the places of K which divide the order of G and those which ramify in the minimal extension splitting G.

1.1. Main results

We give a precise description of the set T of "bad places" for iterated semidirect products of abelian groups, complementing Harari's result [6, Thm. 1].

THEOREM 1.1. — *Let K be a number field and G be a finite K-group which is an iterated semidirect product $G = A_1 \rtimes (A_2 \rtimes \cdots \rtimes A_r)$ of abelian*

K-groups. Let L/K be an extension splitting G, and T the set of places that either divide the order of G, or ramify in L. Then G has approximation away from T.

If G is constant, $L = K$ and hence the only condition on places $v \in S$ is to be prime to the order of G. The Grunwald problem has then an affirmative answer for such (G, K, S). The family of iterated semidirect products of abelian groups contains the dihedral groups, the Heisenberg groups of order p^3, and the p-Sylow subgroups of the symmetric groups, cf. [17], of $\mathrm{GL}_n(\mathbb{F}_q)$, and of other classical groups over $\mathbb{F}_q$ when q is prime to p, cf. [7].

In an opposite scenario, when S consists of the primes of K dividing the order of G and G is constant, we give the following examples in which the approximation property doesn't hold. Recall that a *bicyclic group* is either cyclic or a direct product of two cyclic groups.

THEOREM 1.2. — *Let K be a number field and G a finite abelian p-group that is not bicyclic. Assume that G is a Galois group over some completion of K (which a fortiori divides p) and let S be the finite set of places of K lying above p. Then there exists an abelian G-module A (of order a power of p) such that if we consider $E := A \rtimes G$ as a constant K-group and K contains sufficiently many roots of unity, the map*

$$\mathrm{H}^1(K, E) \to \prod_{v \in S} \mathrm{H}^1(K_v, E),$$

is not surjective.

In contrast to Wang's counterexamples, here the set S consists of the primes of K dividing any given rational prime p, as requested in [3, Section 1.6] by Dèbes-Ghazi. Examples of constant p-groups that do not admit the approximation property at the places dividing a given prime p were also given over $K = \mathbb{Q}(\mu_p)$ by the first author in [4, §6, Prop. 2], where an algebraic Brauer–Manin obstruction to the approximation property is given. However, in contrast with [6, §5], [4] and [9, §5.2], which study algebraic Brauer–Manin obstructions, Theorem 1.2 provides examples in which the approximation property doesn't hold and the algebraic Brauer–Manin obstruction vanishes, giving *the first examples* of a transcendental Brauer–Manin obstruction to weak approximation on homogeneous spaces, see Example 5.4.

1.2. Tame problems

The above results suggest that the answer to the Grunwald problem is affirmative away from a particular set of bad primes:

TAME APPROXIMATION PROBLEM. — *Does the approximation property hold for every finite K-group G and every finite set S of places of K that are prime to its order and are unramified in an extension splitting G?*

Here we do not consider the extension $\mathbb{C}/\mathbb{R}$ to be ramified, hence the question about *real approximation* (i.e. having the approximation property for the set S of archimedean places), asked years ago by Borovoi, is included in this last one.

Negative answers to these questions are unknown, and a complete affirmative answer is currently out of reach, as it implies a solution to the inverse Galois problem (see [6, §4]). In view of Theorem 1.1 and its proof, it seems reasonable to conjecture that the answer is affirmative for all solvable groups.

Acknowledgements

2. Preliminaries

2.1. Global and local Galois groups

All throughout this text, K denotes a number field, Ω_K is the set of places of K and, for $v \in \Omega_K$, K_v denotes the completion of K in v. For any Galois extension L/K we denote by $\mathrm{Gal}(L/K)$ the corresponding Galois group, and by $\mathrm{Gal}(K)$ the absolute Galois group. Throughout the text, we fix an embedding of $\mathrm{Gal}(K_v)$ in $\mathrm{Gal}(K)$ and identify it with its image for each $v \in \Omega_K$.

For a finite place $v \in \Omega_K$, let K_v^{tr} be the maximal tamely ramified extension of K_v, let $\Gamma_v := \mathrm{Gal}(K_v^{\mathrm{tr}}/K_v)$ be the tame Galois group and $W_v := \mathrm{Gal}(K_v^{\mathrm{tr}})$ the wild ramification group. Recall that the tame inertia group $T_v := \mathrm{Gal}(K_v^{\mathrm{tr}}/K_v^{\mathrm{un}})$ is a procyclic normal subgroup of Γ_v of order prime

to v; Let τ_v be a generator of T_v. The quotient $\Gamma_v/T_v \cong \mathrm{Gal}(K_v^{\mathrm{un}}/K_v) \cong \hat{\mathbb{Z}}$ is generated by a lift $\overline{\sigma}_v$ of the Frobenius automorphism.

We let $\sigma_v \in \Gamma_v$ be a preimage of $\overline{\sigma}_v$. Note that σ_v is defined up to conjugation and that its action by conjugation on T_v is equivalent to its action on roots of unity, that is, $\sigma_v \tau_v \sigma_v^{-1} = \tau_v^{q_v}$ where q_v is the cardinality of the residue field of K_v, see [11, §7.5].

For archimedean v, let σ_v be the generator of $\mathrm{Gal}(K_v)$ and put $\tau_v = 1$, so that $\Gamma_v := \mathrm{Gal}(K_v)$ and $T_v = \langle \tau_v \rangle = \{1\}$.

2.2. K-groups

A finite K-group G is a finite group scheme over K. Since K is of characteristic 0, there is an equivalence of categories between finite group schemes over K and finite $\mathrm{Gal}(K)$-groups. Identifying the two, we shall write G for the set of its geometric points. An extension L/K is said to *split* G if $G \times_K L$ is a constant L-group, i.e. if the Galois group $\mathrm{Gal}(L) \subset \mathrm{Gal}(K)$ acts trivially on G. We also need the following notion of "bad places" for such G:

DEFINITION 2.1. — *Let K be a number field, G be a finite K-group and L/K the minimal extension splitting G. We define the set of "bad places" $\mathrm{Bad}_G \subset \Omega_K$ as the union of the set of places dividing the order of G and the places ramified in L/K.*

Note that the minimal extension splitting G always exists. Indeed, the action of $\mathrm{Gal}(K)$ on G is a (continuous) morphism $\mathrm{Gal}(K) \to \mathrm{Aut}(G)$ and the minimal extension splitting G is given by the kernel of this morphism.

2.3. Cohomology

Recall [14, I, §5] that for a field K and a K-group G, the set $\mathrm{H}^1(K, G)$ is defined as the quotient of the set of 1-cocycles (also called *crossed homomorphisms*)

$$Z^1(K, G) := \{a : \mathrm{Gal}(K) \to G \text{ continuous} \mid a_{\sigma\tau} = a_\sigma{}^\sigma a_\tau, \ \forall \sigma, \tau \in \mathrm{Gal}(K)\},$$

by the equivalence

$$a \sim b \Leftrightarrow \exists g \in G \text{ such that } a_\sigma = g b_\sigma{}^\sigma g^{-1}, \ \forall \sigma \in \mathrm{Gal}(K).$$

Hence for a *constant* K-group G, the set $\mathrm{H}^1(K, G)$ is the set of continuous group homomorphisms $\mathrm{Gal}(K) \to G$ modulo conjugation in G. In particular, the Grunwald problem for (G, K, S) is equivalent to the approximation property for G constant. If L/K is an extension splitting G, then $\mathrm{Gal}(L/K)$ acts on G and one may similarly define the set $\mathrm{H}^1(L/K, G)$, which embeds into $H^1(K, G)$ by inflation.

A class $\alpha \in \mathrm{H}^1(K, G)$ is denoted by $[a]$ if it corresponds to the class of the cocycle a. For $\alpha \in \mathrm{H}^1(K, G)$, we denote by α_v its image under the restriction map $\mathrm{Res}_v : \mathrm{H}^1(K, G) \to \mathrm{H}^1(K_v, G)$.

2.4. Twisting

We recall briefly the basic properties of twisting. For further details see [14, §I.5]. Let Γ be a profinite group and G be a discrete Γ-group. Assume that G and Γ act both on the left on some object X in a compatible way, that is, $^\sigma(g \cdot x) = {}^\sigma g \cdot {}^\sigma x$ for $\sigma \in \Gamma$, $g \in G$, $x \in X$. Given a cocycle $a \in Z^1(\Gamma, G)$, define a new action of Γ on X by *twisting* the first action as follows:

$$^{\sigma*}x := a_\sigma \cdot {}^\sigma x.$$

Such a twisted object, denoted by $_aX$, still has an action of G. However, the latter is not necessarily compatible with the action of Γ. To fix this, one twists also the action of Γ on G. To do so it suffices to view G as acting on itself by conjugation, and repeat the same construction, so that

$$^{\sigma*}g := a_\sigma {}^\sigma g a_\sigma^{-1}.$$

This twist of G, denoted by $_aG$, is a Γ-group which acts on $_aX$ compatibly with the Γ-action.

This construction takes principal homogeneous spaces under G to principal homogeneous spaces under $_aG$. More precisely, one has [14, I.5.3, Prop. 35bis]:

PROPOSITION 2.2. — *Let $a \in Z^1(\Gamma, G)$ and let $G' = {}_aG$. The map*

$$t_a : Z^1(\Gamma, G') \to Z^1(\Gamma, G) : a' \mapsto (\sigma \mapsto a'_\sigma a_\sigma),$$

is a bijection which moreover induces a bijection

$$\tau_a : \mathrm{H}^1(\Gamma, G') \to \mathrm{H}^1(\Gamma, G),$$

sending the trivial element of $\mathrm{H}^1(\Gamma, G')$ to the class of a in $\mathrm{H}^1(\Gamma, G)$.

An exact sequence of Γ-groups such as $1 \to H \to E \to G \to 1$ gives rise to an exact sequence of pointed sets, cf. [14, I.5.5, Prop. 38]:

$$(2.1) \qquad \mathrm{H}^1(\Gamma, H) \to \mathrm{H}^1(\Gamma, E) \to \mathrm{H}^1(\Gamma, G),$$

which means that the elements in $\mathrm{H}^1(\Gamma, E)$ falling onto the trivial element of $\mathrm{H}^1(\Gamma, G)$ are precisely those coming from $\mathrm{H}^1(\Gamma, H)$.

Let $e \in Z^1(\Gamma, E)$ and let g be its image in $Z^1(\Gamma, G)$. To study the fiber of the class $[e] \in \mathrm{H}^1(\Gamma, E)$, that is, the fiber above $[g] \in \mathrm{H}^1(\Gamma, G)$, one uses twisting. Since E acts on E, on G and on H by conjugation, one may twist all three groups by e, getting an exact sequence

$$1 \to {}_eH \to {}_eE \to {}_eG \to 1$$

and the following commutative diagram of pointed sets with exact sequences:

$$
\begin{array}{ccccc}
\mathrm{H}^1(\Gamma, H) & \longrightarrow & \mathrm{H}^1(\Gamma, E) & \longrightarrow & \mathrm{H}^1(\Gamma, G) \\
& & \downarrow {\scriptstyle \tau_e^{-1}} & & \downarrow {\scriptstyle \tau_g^{-1}} \\
\mathrm{H}^1(\Gamma, {}_eH) & \longrightarrow & \mathrm{H}^1(\Gamma, {}_eE) & \longrightarrow & \mathrm{H}^1(\Gamma, {}_gG).
\end{array}
$$

Note that the twisted form of G is denoted by ${}_gG$ instead of ${}_eG$, since E acts on G via its own image in G. Since the lower row is exact and since the τ's are bijections sending $[g]$ and $[e]$ to the trivial elements, we now know that the fiber over $[g]$ is in bijection with the image of the set $\mathrm{H}^1(\Gamma, {}_eH)$ in $\mathrm{H}^1(\Gamma, {}_eE)$. Note also that in general there is no vertical arrow at the level of H (as Proposition 2.2 applies only to twists by a group acting on itself by conjugation).

Two elements in $\mathrm{H}^1(\Gamma, H)$ are mapped under (2.1) to the same element of $\mathrm{H}^1(\Gamma, E)$ if and only if they lie in the same orbit of $\mathrm{H}^0(\Gamma, G)$, [14, I.5.5, Prop. 39]. Here an element $g \in \mathrm{H}^0(\Gamma, G) = G^\Gamma$ acts on $\mathrm{H}^1(\Gamma, H)$ by sending a class $[a] \in \mathrm{H}^1(\Gamma, H)$ to the class of the cocycle

$$(2.2) \qquad (g \cdot a)_\sigma = e a_\sigma {}^\sigma e^{-1}$$

where $e \in E$ is a preimage of g.

2.5. Homogeneous spaces

Let us now recall the notion of weak approximation for K-varieties. Let X then be a (smooth, geometrically integral) K-variety such that $X(K) \neq \emptyset$.

DEFINITION 2.3. — *Let $S \subset \Omega_K$ be a finite set of places of K. We say that X has* approximation in S *if $X(K)$ is dense in the product $\prod_S X(K_v)$.*

We say that X has weak approximation away from $T \subset \Omega_K$ *if X has approximation in S for all finite $S \subset \Omega_K \smallsetminus T$. Equivalently, one can demand $X(K)$ to be dense in the product $\prod_{\Omega_K \smallsetminus T} X(K_v)$. The set T is usually refered to as the set of "bad places".*

We say that X has weak approximation *if one can take $T = \emptyset$.*

Let us briefly recall the Brauer–Manin obstruction to weak approximation, cf. [15, §5.1] for details. For X a (smooth, geometrically integral) K-variety, consider its unramified Brauer group $\mathrm{Br}_{\mathrm{un}}X$, as well as the subgroup of its "algebraic" elements $\mathrm{Br}_{\mathrm{un,al}}X := \ker[\mathrm{Br}_{\mathrm{un}}X \to \mathrm{Br}_{\mathrm{un}}(X \times_K \bar{K})]$. Denote, for $v \in \Omega_K$, $\mathrm{inv}_v : \mathrm{Br}\, K_v \to \mathbb{Q}/\mathbb{Z}$ the Hasse invariant map. Finally, denote by $X(K_\Omega)$ the product $\prod_{\Omega_K} X(K_v)$ in which $X(K)$ embeds diagonally. Then one can define the set $X(K_\Omega)^{\mathrm{Br}_{\mathrm{un}}}$ (resp. $X(K_\Omega)^{\mathrm{Br}_{\mathrm{un,al}}}$) as the subset of all families of points $(P_v)_{v \in \Omega_K} \in X(K_\Omega)$ such that

$$\sum_{v \in \Omega_K} \mathrm{inv}_v(\alpha(P_v)) = 0, \text{ for all } \alpha \in \mathrm{Br}_{\mathrm{un}}X \text{ (resp. } \alpha \in \mathrm{Br}_{\mathrm{un,al}}X),$$

where $\alpha(P_v) \in \mathrm{Br}\, K_v$ denotes the evaluation of α at the point P_v and the sum, which a priori is infinite, is actually finite for elements $\alpha \in \mathrm{Br}_{\mathrm{un}}X$. The following inclusions then hold:

$$\overline{X(K)} \subseteq X(K_\Omega)^{\mathrm{Br}_{\mathrm{un}}} \subseteq X(K_\Omega)^{\mathrm{Br}_{\mathrm{un,al}}} \subseteq X(K_\Omega).$$

If $X(K_\Omega)^{\mathrm{Br}_{\mathrm{un}}} \neq X(K_\Omega)$ (resp. $X(K_\Omega)^{\mathrm{Br}_{\mathrm{un,al}}} \neq X(K_\Omega)$) one says that there is a Brauer–Manin obstruction (resp. an algebraic Brauer–Manin obstruction) to weak approximation. A Brauer–Manin obstruction that is not algebraic is called transcendental.

A conjecture by Colliot-Thélène [1, Introduction] says that the Brauer–Manin obstruction to weak approximation should be the only obstruction for rationally connected varieties, that is, $\overline{X(K)} = X(K_\Omega)^{\mathrm{Br}_{\mathrm{un}}}$. Now, given a finite K-group G, one can always embed it into SL_n for some n and consider the homogeneous space $X = \mathrm{SL}_n/G$, which is unirational (since SL_n is itself a rational variety) and hence rationally connected. In [6, Thm. 1], Harari proved that if G is an iterated semidirect product of abelian groups, then we do have $\overline{X(K)} = X(K_\Omega)^{\mathrm{Br}_{\mathrm{un}}}$. The fact that this theorem implies the approximation property away from a finite set T of places as we claimed in §1 follows from the finiteness of $\mathrm{Br}_{\mathrm{un}}X/\mathrm{Br}\, K$, cf. [2, Prop. 5.1(iii)], and from [6, §1.2] or [8, §1]:

PROPOSITION 2.4. — *Let G a be K-group embedded into SL_n and put $X := \mathrm{SL}_n/G$. Let $S \subset \Omega_K$ be a finite set of places of K. Then X has approximation in S if and only if the natural map*

$$\mathrm{H}^1(K, G) \to \prod_{v \in S} \mathrm{H}^1(K_v, G),$$

is surjective.

Note that this result proves in particular that approximation properties for varieties such as $X = \mathrm{SL}_n/G$ depend only on G, i.e. they are independent of the embedding of G and even on the dimension of X since there is no condition on n, justifying the definition of the approximation property in §1.

The tame approximation problem is thus equivalent to determining whether G (or $X = \mathrm{SL}_n/G$) has weak approximation away from $T = \mathrm{Bad}_G$. Note that a positive answer to this question does not necessarily imply a positive answer to Colliot-Thélène's conjecture for $X = \mathrm{SL}_n/G$. Conversely, if the conjecture were true, we would only get the existence of a finite set T_{Br} of bad places. However, not enough is known on the unramified Brauer group of X in order to show that $T_{\mathrm{Br}} = \mathrm{Bad}_G$.

2.6. Poitou–Tate

We next recall the obstruction to weak approximation for finite abelian K-groups. Let A be a finite abelian K-group and let $\hat{A} = \mathrm{Hom}(A, \mathbb{G}_{\mathrm{m}})$ be its Cartier dual, which is also a finite abelian K-group.

Let K_v^{un} denote the maximal unramified extension and K_v^{tr} its maximal tamely ramified extension. Recall [14, II, §6] that for every finite place v such that $\mathrm{Gal}(K_v^{\mathrm{un}})$ acts trivially on A, the unramified cohomology $\mathrm{H}^1_{\mathrm{un}}(K_v, A)$ is defined as the image of the group $\mathrm{H}^1(K_v^{\mathrm{un}}/K_v, A)$ under inflation to $\mathrm{H}^1(K_v, A)$. One can consider then the restricted product $\prod_{\Omega_K} \mathrm{H}^1(K_v, A)$ with respect to these subgroups. It is well known that the product of the restriction maps Res_v sends $\mathrm{H}^1(K, A)$ into $\prod_{\Omega_K} \mathrm{H}^1(K_v, A)$. A classical result by Poitou and Tate [14, II.6.3] gives a perfect pairing

$$(2.3) \qquad \prod_{\Omega_K} \mathrm{H}^1(K_v, A) \times \prod_{\Omega_K} \mathrm{H}^1(K_v, \hat{A}) \to \mathbb{Q}/\mathbb{Z},$$

defined via local pairings and such that the image of $\mathrm{H}^1(K, A)$ is the orthogonal complement of the image of $\mathrm{H}^1(K, \hat{A})$ for this pairing. A classic consequence of these is the following well-known proposition [11, Lem. 9.2.2].

For a subset S of Ω_K, let $\text{III}^1_S(K, G) := \{\alpha \in \mathrm{H}^1(K, G) \,|\, \alpha_v = 1, \,\forall\, v \notin S\}$, and let $\text{III}^1(K, G) := \text{III}^1_\emptyset(K, G)$.

PROPOSITION 2.5. — *Let A be a finite abelian K-group and $S \subset \Omega_K$ be a finite set of places. Then there is a pairing*

$$\prod_{v \in S} \mathrm{H}^1(K_v, A) \times \text{III}^1_S(K, \hat{A}) \to \mathbb{Q}/\mathbb{Z},$$

such that its right kernel is $\text{III}^1(K, \hat{A})$ and its left kernel is the image of the restriction map

$$\mathrm{H}^1(K, A) \to \prod_{v \in S} \mathrm{H}^1(K_v, A)$$

In particular, A has approximation in S if and only if $\text{III}^1_S(K, \hat{A}) = \text{III}^1(K, \hat{A})$.

We shall use the following property of $\text{III}^1_S(K, \cdot)$ to descend to finite extensions:

LEMMA 2.6. — *Let A be a finite abelian K-group. Let L/K be a Galois extension splitting A. Then for any finite $S \subset \Omega_K$, $\text{III}^1_S(K, A)$ is contained in the image of $\mathrm{H}^1(L/K, A)$ by the inflation map.*

Proof. — Since $\mathrm{Gal}(L)$ acts trivially on A, we have the following commutative diagram with exact rows:

$$1 \longrightarrow \mathrm{H}^1(L/K, A) \xrightarrow{\ \text{inf}\ } \mathrm{H}^1(K, A) \xrightarrow{\ \text{Res}\ } \mathrm{H}^1(L, A)$$

$$\prod_{v \in \Omega_K} \mathrm{H}^1(K_v, A) \xrightarrow{\ \text{Res}\ } \prod_{w \in \Omega_L} \mathrm{H}^1(L_w, A).$$

Since L splits A, the H^1's on the right hand side of the diagram are actually groups of homomorphisms. Restricting a class $\alpha \in \text{III}^1_S(K, A)$ to $\mathrm{H}^1(L, A)$, we get a homomorphism $\mathrm{Gal}(L) \to A$ that is trivial everywhere locally except for the finitely many $w \in \Omega_L$ that lie above $S \subset \Omega_K$. By Chebotarev's density theorem it is the trivial morphism. Thus by exactness, α comes from $\mathrm{H}^1(L/K, A)$. $\qquad\square$

3. Reocurrence

The main idea in proving Theorem 1.1 is to show that, given a finite K-group G of order n and a finite place $v \notin \mathrm{Bad}_G$, there are infinitely

many other places w such that $\mathrm{H}^1(K_v, G) \cong \mathrm{H}^1(K_w, G)$. In the particular case of a constant group, this infinite set of places will only depend on v and n. Hence, for a place v prime to n, a group G of order n will appear as a Galois group over K_v if and only if it appears over K_w.

Let us start by proving that, for finite places not in Bad_G, the set $\mathrm{H}^1(K_v, G)$ depends only on the tamely ramified part $\Gamma_v = \mathrm{Gal}(K_v^{\mathrm{tr}}/K_v)$. Recall that Γ_v is generated by a lift σ_v of the Frobenius and a generator of the inertia group τ_v, as in §2.1. For every place v, we fix a choice of σ_v and τ_v and keep it all throughout the text.

LEMMA 3.1. — *Let G be a finite K-group of order n and let $v \in \Omega_K$ be a place outside Bad_G. Denote by T_v^n the subgroup of Γ_v generated by τ_v^n. Then there is an isomorphism $\mathrm{H}^1(K_v, G) \cong \mathrm{H}^1(\Gamma_v/T_v^n, G)$ given by inflation.*

Proof. — The statement is trivial for archimedean v, so we may assume that v is finite. Since the wild ramification subgroup $W_v \leqslant \mathrm{Gal}(K_v)$ acts trivially on G, the inflation-restriction sequence gives:

$$1 \to \mathrm{H}^1(\Gamma_v, G) \xrightarrow{\mathrm{inf}} \mathrm{H}^1(K_v, G) \xrightarrow{\mathrm{Res}} \mathrm{H}^1(W_v, G),$$

and $\mathrm{H}^1(W_v, G)$ is the set of morphisms $W_v \to G$ up to conjugation. Since W_v is a pro-p group with p not dividing n, there are no such nontrivial morphisms and hence $\mathrm{H}^1(K_v, G) \cong \mathrm{H}^1(\Gamma_v, G)$.

Consider now a class $\alpha \in \mathrm{H}^1(\Gamma_v, G)$. Since v is unramified in the minimal extension splitting G, T_v also acts trivially on G and hence α restricts to a morphism (up to conjugation) from T_v to G. It is then evident that this morphism is trivial over T_v^n. The same inflation-restriction argument then gives

$$\mathrm{H}^1(K_v, G) \cong \mathrm{H}^1(\Gamma_v/T_v^n, G). \qquad \square$$

The following reocurrence result generalizes the statement given in the beginning of the section.

PROPOSITION 3.2. — *Let G be a finite K-group of order n, L/K a Galois extension splitting G and let $v \in \Omega_K$ be either an archimedean place or a finite place which is unramified in L and does not divide n (in particular, $v \notin \mathrm{Bad}_G$). Then there exist infinitely many finite places $w \notin \mathrm{Bad}_G$ for which:*

(1) *the decomposition groups of v and w in $\mathrm{Gal}(L/K)$ are conjugate;*
(2) *there is an epimorphism $\phi : \Gamma_w/T_w^n \twoheadrightarrow \Gamma_v/T_v^n$ given by $\phi(\sigma_w) = \sigma_v, \phi(\tau_w) = \tau_v$, which is moreover an isomorphism if v is finite.*

The epimorphism ϕ induces a monomorphism $\phi^* : \mathrm{H}^1(K_v, G) \hookrightarrow \mathrm{H}^1(K_w, G)$, which is moreover an isomorphism if v is finite.

Proof. — By Chebotarev's density theorem applied to the Galois extension $L(\mu_n)/K$ (which is unramified in v) there are infinitely many places $w \notin \mathrm{Bad}_G$ for which the image of the decomposition group in $\mathrm{Gal}(L(\mu_n)/K)$ is generated by the image of σ_w and is conjugate to the image of σ_v. In particular, we get that these groups are conjugate in $\mathrm{Gal}(L/K)$.

If v is finite, the images of σ_v and σ_w coincide in the quotient $\mathrm{Gal}(K(\mu_n)/K)$ and hence their residue degrees q_v, q_w, respectively, are congruent mod n. Moreover, recall that the group Γ_v/T_v^n has the following presentation:

$$\langle \sigma_v, \tau_v \,|\, \sigma_v \tau_v \sigma_v^{-1} = \tau_v^{q_v}, \tau_v^n = 1 \rangle.$$

Since $q_w \equiv q_v \mod n$, we get an isomorphism $\phi : \Gamma_w/T_w^n \to \Gamma_v/T_v^n$ by setting $\phi(\sigma_w) = \sigma_v$ and $\phi(\tau_w) = \tau_v$. If v is archimedean, the same definition gives an epimorphism $\phi : \Gamma_w/T_w^n \to \mathrm{Gal}(K_v)$ since $\sigma_v^2 = \tau_v = 1$.

Let $\rho \in \mathrm{Gal}(K)$ be an element for which σ_w coincides with $\rho \sigma_v \rho^{-1}$ in $\mathrm{Gal}(L/K)$. Denote by $_\rho G$ the K_v-group where $\sigma \in \mathrm{Gal}(K_v)$ acts on G by $g \mapsto {}^{\rho \sigma \rho^{-1}} g$ and note that this action coincides with that of $\mathrm{Gal}(K_w)$ on G. Consider the maps

$$\mathrm{H}^1(\Gamma_v/T_v^n, G) \xrightarrow{\rho_*} \mathrm{H}^1(\Gamma_v/T_v^n, {}_\rho G) \xrightarrow{\phi^*} \mathrm{H}^1(\Gamma_w/T_w^n, G),$$

where ρ_* is a canonical isomorphism defined at the level of cocycles by the identity on Γ_v/T_v^n and by sending $g \in G$ to $^\rho g$. We abusively denote by ϕ^* the whole composition. Then evidently ϕ^* is an isomorphism if v is finite and injective as an inflation morphism if v is archimedean. Recall finally that by Lemma 3.1, we have $\mathrm{H}^1(K_v, G) \cong \mathrm{H}^1(\Gamma_v/T_v^n, G)$ for finite v and $\Gamma_v/T_v^n = \mathrm{Gal}(K_v)$ for archimedean v, hence the result. $\square$

We finally give a particular application necessary for the proof of Theorem 1.1:

LEMMA 3.3. — *Let G, L/K, v, w, ϕ and ϕ^* be as given by Proposition 3.2. Let $\alpha \in \mathrm{H}^1(K_v, G)$ and assume that there exists a class $\beta = [b] \in \mathrm{H}^1(K, G)$ such that $\beta_v = \alpha$, $\beta_w = \phi^* \alpha$ and such that the group morphism $\mathrm{Gal}(L) \to G$ obtained by restriction of b to $\mathrm{Gal}(L)$ is surjective. Denote by L' the extension defined by the kernel of this morphism. Then the decomposition groups of v and w in $\mathrm{Gal}(L'/K)$ are conjugate.*

We first note that L'/K is indeed Galois:

LEMMA 3.4. — *Let G be a K-group and L/K be a Galois extension splitting G. Let $b \in Z^1(K, G)$ and L'/L be the field fixed by the kernel of the restriction of b to $\mathrm{Gal}(L)$. Then L' is Galois over K.*

Proof. — Let $\tau \in \mathrm{Gal}(L')$ and $\sigma \in \mathrm{Gal}(K)$. Then

$$b_{\sigma\tau\sigma^{-1}} = b_\sigma{}^\sigma b_\tau{}^{\sigma\tau\sigma^{-1}} b_\sigma^{-1}.$$

Since L/K is Galois and $\tau \in \mathrm{Gal}(L') \subseteq \mathrm{Gal}(L)$, we get $\sigma\tau\sigma^{-1} \in \mathrm{Gal}(L)$, hence it acts trivially on b_σ. As $b_\tau = 1$ by definition of L', we get $b_{\sigma\tau\sigma^{-1}} = 1$, which proves that $\sigma\tau\sigma^{-1} \in \mathrm{Gal}(L')$ and thus L'/K is Galois.   □

Proof of Lemma 3.3. — We first show that the decomposition groups of v and w in $\mathrm{Gal}(L'/K)$ are quotients of Γ_v/T_v^n and Γ_w/T_w^n. Indeed, this holds for archimedean v since $\mathrm{Gal}(K_v) = \Gamma_v/T_v^n$. For finite v and w, L'/K is tamely ramified since L/K is unramified and L'/L is of degree n and hence prime to v and w. Since the restriction of b to T_v and T_w is a morphism, it must be trivial on T_v^n and T_w^n, i.e. $T_v^n, T_w^n \subset \mathrm{Gal}(L')$, proving the claim.

Denote then (abusively) by $\sigma_v, \sigma_w, \tau_v, \tau_w$, the images in $\mathrm{Gal}(L'/K)$ of these elements. Recall that by the proof of Proposition 3.2, there exists an element $\rho \in \mathrm{Gal}(K)$ such that σ_w coincides with $\rho\sigma_v\rho^{-1}$ in $\mathrm{Gal}(L/K)$. Also note that $\rho\tau_v\rho^{-1} = \tau_w = 1$ in $\mathrm{Gal}(L/K)$. We claim that we may choose ρ so that $b_\rho = 1$. Note that $b_{\chi\rho} = b_\chi b_\rho$ for $\chi \in \mathrm{Gal}(L)$. Since b is surjective when restricted to $\mathrm{Gal}(L)$, there exists $\chi \in \mathrm{Gal}(L)$ such that $b_\chi = b_\rho^{-1}$ so that $b_{\chi\rho} = 1$. Since $\chi \in \mathrm{Gal}(L)$, we have that σ_w coincides with $(\chi\rho)\sigma_v(\chi\rho)^{-1}$ in $\mathrm{Gal}(L/K)$, proving the claim.

The isomorphism ϕ^* between $\mathrm{H}^1(K_v, G)$ and $\mathrm{H}^1(K_w, G)$ is given at the level of cocycles by the morphisms $\rho_* : G \to G$ and $\phi : \Gamma_w/T_w^n \to \Gamma_v/T_v^n$, which satisfy $\rho_*(g) = {}^\rho g$, $\phi(\sigma_w) = \sigma_v$, and $\phi(\tau_w) = \tau_v$. In particular, if $\alpha = [a]$ for $a \in Z^1(\Gamma_v/T_v^n, G)$, then $\phi^*\alpha = [a']$ with $a'_{\sigma_w} = {}^\rho a_{\sigma_v}$ and $a'_{\tau_w} = {}^\rho a_{\tau_v}$.

Now, since $\beta_v = \alpha$ and $\beta_w = \phi^*\alpha$, we know that there exist $g, g' \in G$ such that

$$^\rho(gb_{\sigma_v}{}^{\sigma_v}g^{-1}) = {}^\rho a_{\sigma_v} = a'_{\sigma_w} = g'b_{\sigma_w}{}^{\sigma_w}g'^{-1},$$
$$^\rho(gb_{\tau_v}g^{-1}) = {}^\rho a_{\tau_v} = a'_{\tau_w} = g'b_{\tau_w}g'^{-1}.$$

Since b restricted to $\mathrm{Gal}(L'/L)$ is an isomorphism by hypothesis, there are unique $\chi, \chi' \in \mathrm{Gal}(L'/L)$ such that $b_\chi = g$, $b_{\chi'} = g'$, so that

(3.1)
$$^\rho b_\chi{}^\rho b_{\sigma_v}{}^{\rho\sigma_v}b_\chi^{-1} = b_{\chi'}b_{\sigma_w}{}^{\sigma_w}b_{\chi'}^{-1},$$
$$^\rho b_\chi{}^\rho b_{\tau_v}{}^\rho b_\chi^{-1} = b_{\chi'}b_{\tau_w}b_{\chi'}^{-1}.$$

Note now that since $b_\rho = 1$, we have $b_{\rho\eta\rho^{-1}} = {}^\rho b_\eta$ for every $\eta \in \mathrm{Gal}(L'/L)$, so in particular for $\eta = \chi, \tau_v$, and χ^{-1}. Noting that

$$\rho\,\mathrm{Gal}(L'/L)\rho^{-1} \subseteq \mathrm{Gal}(L'/L),$$

since L/K is Galois, that the restriction of b to $\mathrm{Gal}(L'/L)$ is a homomorphism, and putting $\rho_0 := \chi'^{-1}\rho\chi \in \mathrm{Gal}(L'/K)$, (3.1) gives $b_{\rho_0\tau_v\rho_0^{-1}} = b_{\tau_w}$ and hence $\rho_0\tau_v\rho_0^{-1} = \tau_w$ in $\mathrm{Gal}(L'/L) \subset \mathrm{Gal}(L'/K)$.

Finally, we claim that $\rho_0\sigma_v\rho_0^{-1} = \sigma_w$ in $\mathrm{Gal}(L'/K)$. Since $\chi, \chi' \in \mathrm{Gal}(L)$, we already know that σ_w and $\rho_0\sigma_v\rho_0^{-1}$ coincide on $\mathrm{Gal}(L/K)$ and hence act equally on G. Thus, on the one hand, (3.1) gives

$$b_{\rho_0}\,{}^\rho b_{\sigma_v}\,{}^{\sigma_w}b_{\rho_0}^{-1} = b_{\sigma_w}.$$

On the other hand, we have $\rho_0\sigma_v\rho_0^{-1} = \psi\sigma_w$ for some $\psi \in \mathrm{Gal}(L'/L)$. Applying b to this equality another direct computation gives

$$b_{\rho_0}\,{}^\rho b_{\sigma_v}\,{}^{\sigma_w}b_{\rho_0}^{-1} = b_\psi b_{\sigma_w}.$$

From the two last equalities we get that $b_\psi = 1$. Since b is an isomorphism over $\mathrm{Gal}(L'/L)$, we get $\psi = 1$, proving the claim. Thus conjugation by ρ_0 sends the decomposition group of v in L'/K to that of w. □

4. Weak approximation away from Bad_G

We now restate and prove Theorem 1.1 in the language of approximation properties. Recall that, given a K-group G, Bad_G denotes the set of bad places associated to it, cf. Definition 2.1.

THEOREM 4.1. — *Let K be a number field and G be a finite K-group with weak approximation away from Bad_G. Then every semidirect product $E = A \rtimes G$ with A an abelian K-group has weak approximation away from Bad_E.*

Remark 4.2. — Note that this result does imply Theorem 1.1. Indeed, one can prove it by induction starting with the fact that the trivial group has weak approximation.

Proof of Theorem 4.1. — Consider a finite set of places $S \subset \Omega_K$ not meeting Bad_E and local classes $\beta_v \in \mathrm{H}^1(K_v, E)$ for $v \in S$. We will find a global class $\beta \in \mathrm{H}^1(K, E)$ mapping to the β_v's in three steps:

Step 1. — Constructing a class $\beta' \in \mathrm{H}^1(K, E)$ with prescribed images in $\mathrm{H}^1(K_v, G)$ for v in $S \cup S'$ for a suitable S'.

We have the following commutative diagram of pointed sets with exact rows:

(4.1)

$$
\begin{array}{ccccc}
H^1(K, A) & \longrightarrow & H^1(K, E) & \longrightarrow & H^1(K, G) \\
\downarrow & & \downarrow & & \downarrow \\
\displaystyle\prod_{v \in \Omega_K} H^1(K_v, A) & \longrightarrow & \displaystyle\prod_{v \in \Omega_K} H^1(K_v, E) & \longrightarrow & \displaystyle\prod_{v \in \Omega_K} H^1(K_v, G),
\end{array}
$$

where the arrows going left are set-theoretical sections induced by a fixed section $G \to E$.

The β_v's give us images $\gamma_v \in H^1(K_v, G)$ for $v \in S$. Let $n = |E|$ and L a Galois extension splitting E. Then, by Proposition 3.2 applied to the extension $L(\mu_n)/K$ (which splits G), we know that for every $v \in S$ there exist places $v' \notin S \cup \mathrm{Bad}_E$ for which there are inclusions

$$
\phi_v^* : H^1(K_v, G) \hookrightarrow H^1(K_{v'}, G).
$$

Choose one such v' for each $v \in S$ and denote by S' the set of these places. We may assume that all the v' are different since we have an infinite choice at each time. Define then $\gamma_{v'} := \phi_v^*(\gamma_v) \in H^1(K_{v'}, G)$.

Since we've chosen these new places away from $\mathrm{Bad}_E \supset \mathrm{Bad}_G$, we know by hypothesis that there exists a global class $\gamma \in H^1(K, G)$ mapping onto γ_v for every $v \in S \cup S'$. Moreover, we may assume that the restriction of a cocycle $c \in Z^1(K, G)$, representing γ, to $\mathrm{Gal}(L(\mu_n))$ is surjective: Indeed by Chebotarev's density theorem, there are infinitely many places $w \notin S \cup S' \cup \mathrm{Bad}_E$ totally split in $L(\mu_n)$, so in particular such that G is constant over K_w; then, for each element $g \in G$ we may choose one such w and an unramified class $\gamma_w \in H^1(K_w, G)$ represented by a morphism sending σ_w to g, so that all w's are distinct; then finally, adding these local conditions to $S \cup S'$ forces c to be surjective when restricted to $\mathrm{Gal}(L(\mu_n))$.

Let β' be the image of γ in $H^1(K, E)$ via the section of diagram (4.1). Viewing G as a subgroup of E, the class β' is represented by the same cocycle c.

Step 2: Twisting. —   We twist by c to look for a class in $H^1(K, E)$ satisfying the necessary prescribed local conditions in S.

Let us now twist diagram (4.1) by the cocycle c representing β'. This gives us the following new diagram with exact rows

(4.2)

$$
\begin{array}{ccccc}
\mathrm{H}^1(K, {}_cA) & \longrightarrow & \mathrm{H}^1(K, {}_cE) & \longrightarrow & \mathrm{H}^1(K, {}_cG) \\
\downarrow & & \downarrow & & \downarrow \\
\prod_{v\in\Omega_K} \mathrm{H}^1(K_v, {}_cA) & \longrightarrow & \prod_{v\in\Omega_K} \mathrm{H}^1(K_v, {}_cE) & \longrightarrow & \prod_{v\in\Omega_K} \mathrm{H}^1(K_v, {}_cG).
\end{array}
$$

For every cohomology class ξ in a set of diagram (4.1), we denote by ${}_c\xi$ its twisted image in the corresponding set of diagram (4.2).

Since the images of β_v and β' coincide on $\mathrm{H}^1(K_v, G)$ for $v \in S$ by construction and ${}_c\beta'$ is trivial by the very definition of twisting, we know by exactness that ${}_c\beta_v \in \mathrm{H}^1(K_v, {}_cE)$ comes from an element $\alpha_v \in \mathrm{H}^1(K_v, {}_cA)$.

It suffices then to find a global class $\alpha \in \mathrm{H}^1(K, {}_cA)$ mapping onto α_v for $v \in S$ to conclude. Indeed, the image of α in $\mathrm{H}^1(K, {}_cE)$ would then map onto the ${}_c\beta_v$'s for $v \in S$ and hence its preimage in $\mathrm{H}^1(K, E)$ by the twisting morphism would map onto the β_v's as desired. Thus, in order to conclude, it will suffice by Proposition 2.5 to prove that $\Sha^1_S(K, {}_c\hat{A}) = \Sha^1(K, {}_c\hat{A})$.

Step 3: Proof of $\Sha^1_S(K, {}_c\hat{A}) = \Sha^1(K, {}_c\hat{A})$. — Consider a class α in $\Sha^1_S(K, {}_c\hat{A})$, i.e. a class in $\mathrm{H}^1(K, {}_c\hat{A})$ such that its image $\alpha_v \in \mathrm{H}^1(K_v, {}_c\hat{A})$ is trivial for every $v \notin S$, so in particular for $v' \in S'$. We must show that $\alpha_v = 0$ for $v \in S$ too.

Fix then $v \in S$ and its corresponding $v' \in S'$. Lemma 3.3 applies in this context to the local classes γ_v and $\gamma_{v'} = \phi_v^*(\gamma_v)$, the global class γ and the extension $L(\mu_n)/K$. By the lemma the decomposition groups of v and v' in $\mathrm{Gal}(L'/K)$ are conjugate, where L' is the extension of $L(\mu_n)$ given by the kernel of c restricted to $\mathrm{Gal}(L(\mu_n))$. Note moreover that L' splits ${}_c\hat{A}$. Indeed, since $|A|$ divides n we have ${}_c\hat{A} = \mathrm{Hom}({}_cA, \mu_n)$ and since L' contains μ_n, then this amounts to L' splitting ${}_cA$. The latter holds since the action of $\sigma \in \mathrm{Gal}(K)$ on $a \in {}_cA$ is given by $c_\sigma \, {}^\sigma a \, c_\sigma^{-1}$, where ${}^\sigma a$ denotes the action of σ on a as an element of A. Since c is trivial over $\mathrm{Gal}(L')$ and L' clearly splits A, we get then our claim. In particular, by Lemma 2.6, we know that the whole group $\Sha^1_S(K, {}_c\hat{A})$ comes by inflation from $\mathrm{H}^1(L'/K, {}_c\hat{A})$.

Our element $\alpha \in \Sha^1_S(K, {}_c\hat{A})$ comes then from $\mathrm{H}^1(L'/K, {}_c\hat{A})$ and hence α_v comes from $\mathrm{H}^1(L'^{(v)}/K_v, {}_c\hat{A})$, where $L'^{(v)}$ denotes the (unique) extension of K_v induced by L'/K. The same goes for v'. Since the decomposition

groups of v and v' are conjugate in $\mathrm{Gal}(L'/K)$, there is a canonical isomorphism

$$\mathrm{H}^1(L'^{(v)}/K_v, {}_c\hat{A}) \xrightarrow{\sim} \mathrm{H}^1(L'^{(v')}/K_{v'}, {}_c\hat{A}),$$

which is compatible with the restrictions from $\mathrm{H}^1(L'/K, {}_c\hat{A})$. But α is in $\mathrm{III}^1_S(K, {}_c\hat{A})$ and $v' \notin S$, so that $\alpha_{v'} = 0$ and hence $\alpha_v = 0$ too. Since the same argument works for every $v \in S$, we deduce that $\alpha \in \mathrm{III}^1(K, {}_c\hat{A})$, proving the claim. $\qquad\square$

5. Counterexamples to weak approximation

In this section we show that Theorem 4.1 is sharp in the sense that one cannot expect to get approximation (or to solve the Grunwald problem) on the set of bad places.

Recall that a group is bicyclic if and only if it is cyclic or a direct product of two cyclic groups. For a finite group G and a finite G-module A, we let

$$\mathrm{III}^1_{\mathrm{bic}}(G, A) := \ker\left[\mathrm{H}^1(G, A) \to \prod_{H \in \mathrm{bic}(G)} \mathrm{H}^1(H, A)\right],$$

where $\mathrm{bic}(G)$ denotes the set of bicyclic subgroups of G.

THEOREM 5.1. — *Let G be a finite abelian group, K a number field, and S a finite set of places of K. Let A be a finite G-module and $E = A \rtimes G$ a constant K-group. Assume:*

  (1) *K contains the $\exp(A)$-th roots of unity;*
  (2) *there exists $v_0 \in S$ such that G is a Galois group over K_{v_0};*
  (3) *S contains all the places of K dividing the order of G;*
  (4) *$\mathrm{III}^1_{\mathrm{bic}}(G, \hat{A}) \neq 0$ (in particular G is not bicyclic).*

Then the map $\mathrm{H}^1(K, E) \to \prod_{v \in S} \mathrm{H}^1(K_v, E)$ is nonsurjective.

Remark 5.2. — Note that, given the structure of local Galois groups recalled in Section 2.1, Condition (4) implies that the place v_0 in Condition (2) must divide the order of G.

COROLLARY 5.3. — *Assume in addition that K contains the $\exp(E)$-th roots of unity, then there is a transcendental Brauer–Manin obstruction to weak approximation on $X := \mathrm{SL}_n/E$.*

Proof. — Indeed, Theorem 5.1 and Proposition 2.4 tell us that X does not have approximation in S and hence it doesn't have weak approximation. Now, by [6, Thm. 1] the Brauer–Manin obstruction to weak approximation for such a variety is the only obstruction, whereas the formula

given in [9, Prop. 5.9] tells us that the algebraic part of $\mathrm{Br}_{\mathrm{un}}X$ is trivial, hence the lack of weak approximation for X cannot be explained by algebraic obstructions. The Brauer–Manin obstruction must then come from transcendental elements of $\mathrm{Br}_{\mathrm{un}}X$. $\qquad\square$

Example 5.4. — Let p be a prime number and let $G := (\mathbb{Z}/p\mathbb{Z})^3$. Let $A := \hat{I}$, where I is the augmentation ideal of $(\mathbb{Z}/p^3\mathbb{Z})[G]$. There is a natural action of G on A and $E := A \rtimes G$ is a group of order p^{3p^3}. Define K to be $\mathbb{Q}(\zeta_{p^4})$ and S to be the unique place of K dividing p. By Lemma 5.5 here below, we have $\mathrm{III}^1_{\mathrm{bic}}(G, \hat{A}) \neq 0$ and it is easy to see that all the other assumptions of Corollary 5.3 are satisfied, hence the group E provides the first explicit example of a transcendental Brauer–Manin obstruction to weak approximation on a homogeneous space.

LEMMA 5.5. — *Let G be a finite group of order n which is not bicyclic, let R be the group ring $(\mathbb{Z}/n\mathbb{Z})[G]$ and $I \lhd R$ the augmentation ideal. Then $\mathrm{III}^1_{\mathrm{bic}}(G, I)$ is nontrivial.*

Proof. — For a G-module A, denote by $\hat{\mathrm{H}}^0(G, A)$ the Tate cohomology group $A^G/N_G(A)$ where $N_G(A) := \{\sum_{\sigma \in G} {}^\sigma a \,|\, a \in A\}$. Put $B := R/I \cong \mathbb{Z}/n\mathbb{Z}$. Since R is an induced H-module for any subgroup $H \leqslant G$, we have $\hat{\mathrm{H}}^0(H, B) \cong \mathrm{H}^1(H, I)$ and hence $\mathrm{III}^1_{\mathrm{bic}}(G, I)$ is isomorphic to

$$\mathrm{III}^0_{\mathrm{bic}}(G, B) = \ker\left[\hat{\mathrm{H}}^0(G, B) \to \prod_{H \in \mathrm{bic}(G)} \hat{\mathrm{H}}^0(H, B)\right].$$

Since $\hat{\mathrm{H}}^0(H, B) \cong \mathbb{Z}/|H|\mathbb{Z}$ for every $H \leqslant G$, and since $G \notin \mathrm{bic}(G)$, we have:

$$\mathrm{III}^0_{\mathrm{bic}}(G, B) \cong \ker\left[\mathbb{Z}/n\mathbb{Z} \to \prod_{H \in \mathrm{bic}(G)} \mathbb{Z}/|H|\mathbb{Z}\right] \neq 0.$$

$\qquad\square$

Proof of Theorem 5.1. — We divide the proof into five steps.

Step 1: Setup. — We construct local classes in $\mathrm{H}^1(K_v, G)$, the fibers of which will contain elements that cannot be approximated by a global element in $\mathrm{H}^1(K, E)$.

By Condition (2), there exists an epimorphism $c_{v_0} : \mathrm{Gal}(K_{v_0}) \to G$. Since G is abelian and constant, $\mathrm{Hom}(\mathrm{Gal}(K), G) = Z^1(K, G) = \mathrm{H}^1(K, G)$ and their equivalents for the K_v's. One can then look at c_{v_0} as an element of $\mathrm{H}^1(K_{v_0}, G)$. We will omit these identifications from now on and abusively

use the same letters for cocycles and cohomology classes for G. For v in $S \smallsetminus \{v_0\}$, let $c_v := 0 \in \mathrm{H}^1(K_v, G)$.

Fix a section $s : G \to E$ of the following exact sequence

$$(5.1) \qquad 1 \longrightarrow A \longrightarrow E \overset{\overset{s}{\frown}}{\underset{\pi}{\longrightarrow}} G \longrightarrow 1.$$

Consider $s(c_v) \in Z^1(K_v, E)$, which we still denote abusively by c_v by looking at G as a subgroup of E via s, and let $\beta_v := [c_v] \in \mathrm{H}^1(K_v, E)$. If $(\beta_v)_{v \in S}$ is not contained in the image of the restriction map

$$\mathrm{H}^1(K, E) \to \prod_S \mathrm{H}^1(K_v, E),$$

then we are done. So we can assume that there exists $\beta \in \mathrm{H}^1(K, E)$ lifting the β_v's for all $v \in S$. Up to replacing β by $s(\pi(\beta))$, one can assume that $\beta = s(c)$ for some $c \in \mathrm{H}^1(K, G)$ lifting the c_v's for $v \in S$. Making once again an abuse of notation, we'll write $\beta = [c]$, viewing c as an element of $Z^1(K, E)$.

Step 2: Twisting. — To study the fibers over $c_v, v \in S$, we twist the exact sequence (5.1) by the cocycle c. We get the following twisted exact sequence:

$$1 \longrightarrow {}_cA \longrightarrow {}_cE \overset{\frown}{\longrightarrow} {}_cG \longrightarrow 1,$$

where we immediately remark that ${}_cG = G$ since G is abelian. Moreover, since c takes values in G, the section s is still well defined on these twisted forms.

By definition of twisting, the action of $\mathrm{Gal}(K)$ on ${}_cA$ is given by composition of the morphism $c : \mathrm{Gal}(K) \to G$ with the morphism $G \to \mathrm{Aut}(A)$ defining the action of G on A.

Step 3: Defining unattainable classes in $\mathrm{H}^1(K_v, E)$. — By Condition (1) of Theorem 5.1, we know that $\hat{A} = \mathrm{Hom}(A, \mathbb{Q}/\mathbb{Z})$ and the same goes for its twisted version ${}_c\hat{A}$. Since both G and $\mathrm{Gal}(K)$ act trivially on $\mathbb{Q}/\mathbb{Z}$, the action of $\mathrm{Gal}(K)$ on ${}_c\hat{A}$ corresponds via c with the action of G on $\hat{A}$, so that we get a pullback morphism $c^* : \mathrm{H}^1(G, \hat{A}) \to \mathrm{H}^1(K, {}_c\hat{A})$.

Note that since G is abelian, Condition (3) of Theorem 5.1 and the structure of local Galois groups imply that the image of $c : \mathrm{Gal}(K) \to G$ restricted to $\mathrm{Gal}(K_v)$ is a bicyclic subgroup, for all cocycles $c \in Z^1(K, G)$ and all places $v \notin S$. Therefore, for any $c \in Z^1(K, G)$, the morphism c^* restricts to a morphism

$$c^* : \mathrm{III}^1_{\mathrm{bic}}(G, \hat{A}) \to \mathrm{III}^1_S(K, {}_c\hat{A}).$$

Condition (4) tells us now that there exists $\gamma \neq 0 \in \text{III}^1_{\text{bic}}(G, \hat{A})$. Since c lifts c_{v_0}, and the latter was chosen to be surjective, c must also be surjective. Hence the above map c^* is an inflation map and is therefore injective, so that $c^*(\gamma) \neq 0 \in \text{III}^1_S(K, {}_cA)$.

In addition since c_{v_0} is surjective, one has by inflation that $c^*(\gamma)_{v_0} \neq 0$ in $\text{H}^1(K_{v_0}, {}_cA)$, hence $c^*(\gamma) \notin \text{III}^1(K, {}_cA)$. By Proposition 2.5, there exists therefore $(\alpha_v)_{v \in S} \in \prod_S \text{H}^1(K_v, {}_cA)$ which is not in the image of $\text{H}^1(K, {}_cA)$. Note also that $c^*(\gamma)_v = 0$ for all $v \in S \setminus \{v_0\}$ since $c_v = 0$ for these places, hence we can assume that $\alpha_v = 0$ for all $v \neq v_0$.

Consider now the image in $\prod_S \text{H}^1(K_v, {}_cE)$ of $(\alpha_v)_{v \in S}$. The twisting bijection $\text{H}^1(\cdot, {}_cE) \to \text{H}^1(\cdot, E)$ tells us that this element is the twist $({}_c\beta'_v)_{v \in S}$ of an element $(\beta'_v)_{v \in S} \in \prod_S \text{H}^1(K_v, E)$. We claim that $(\beta'_v)_{v \in S}$ is not in the image of $\text{H}^1(K, E)$.

Step 4: Compatibility between twists and obstructions. — To prove the latter claim, we first show a certain compatibility relation between the maps c^* and c'^* for every two classes c and c' in $Z^1(K, G) = \text{H}^1(K, G)$ such that $c_v = c'_v$ in $\text{H}^1(K_v, G)$ for all $v \in S$. Namely, we claim that there are canonical isomorphisms $i_v : \text{H}^1(K_v, {}_cA) \xrightarrow{\sim} \text{H}^1(K_v, {}_{c'}A)$ for $v \in S$ such that the following diagram
(5.2)

$$
\begin{array}{ccc}
& \text{III}^1_S(K, {}_c\hat{A}) \times \prod_S \text{H}^1(K_v, {}_cA) & \xrightarrow{\langle,\rangle_c} & \mathbb{Q}/\mathbb{Z} \\
c^* \nearrow & \downarrow \prod i_v & & \| \\
\text{III}^1_{\text{bic}}(G, \hat{A}) & & & \\
c'^* \searrow & \text{III}^1_S(K, {}_{c'}\hat{A}) \times \prod_S \text{H}^1(K_v, {}_{c'}A) & \xrightarrow{\langle,\rangle_{c'}} & \mathbb{Q}/\mathbb{Z},
\end{array}
$$

is commutative in the following sense: for all $\gamma \in \text{III}^1_{\text{bic}}(G, \hat{A})$ and all $(\alpha_v)_{v \in S}$ in $\prod_S \text{H}^1(K_v, {}_cA)$, one has

$$
\langle c^* \gamma, (\alpha_v) \rangle_c = \langle c'^* \gamma, (i_v(\alpha_v)) \rangle_{c'} \in \mathbb{Q}/\mathbb{Z}.
$$

The left-hand side arrows in the diagram were defined in Step 3, while the right-hand side arrows are given by Proposition 2.5. Now, for $v \in S$, since $c_v = c'_v$ as cocycles, there exists a natural isomorphism of $\text{Gal}(K_v)$-modules ${}_cA \to {}_{c'}A$ (given by the identity map) that induces a group isomorphism

$$
i_v : \text{H}^1(K_v, {}_cA) \to \text{H}^1(K_v, {}_{c'}A).
$$

Similarly, one can consider the dual isomorphism $_{c'}\hat{A} \to {}_c\hat{A}$ which induces a corresponding isomorphism $\hat{i}_v : \mathrm{H}^1(K_v, {}_{c'}\hat{A}) \to \mathrm{H}^1(K_v, {}_c\hat{A})$ such that

$$
\begin{array}{ccc}
 & & \mathrm{H}^1(K_v, {}_c\hat{A}) \\
 & \nearrow^{c_v^*} & \uparrow^{\hat{i}_v} \\
\mathrm{III}_{\mathrm{bic}}^1(G, \hat{A}) & & \\
 & \searrow_{c_v'^*} & \\
 & & \mathrm{H}^1(K_v, {}_{c'}\hat{A}),
\end{array}
$$

is commutative. Hence the claim reduces to the commutativity of the following diagram

$$
\begin{array}{ccc}
\mathrm{H}^1(K_v, {}_c\hat{A}) \times \mathrm{H}^1(K_v, {}_cA) & \xrightarrow{\langle\,,\,\rangle_c} & \mathbb{Q}/\mathbb{Z} \\
\hat{i}_v \uparrow \qquad\qquad \downarrow i_v & & \| \\
\mathrm{H}^1(K_v, {}_{c'}\hat{A}) \times \mathrm{H}^1(K_v, {}_{c'}A) & \xrightarrow{\langle\,,\,\rangle_{c'}} & \mathbb{Q}/\mathbb{Z},
\end{array}
$$

which is just the functoriality of cup-product (or of local duality), proving the claim.

Step 5: Proving that the local classes are globally unattainable. — Assume on the contrary that there exists $\beta' = [b'] \in \mathrm{H}^1(K, E)$ lifting the β_v''s for all $v \in S$. Define $c' := \pi(\beta') \in Z^1(K, G) = \mathrm{H}^1(K, G)$ and consider the class $\beta'' := s(\pi(\beta')) = [c'] \in \mathrm{H}^1(K, E)$ (we are once again doing an abuse of notation with c').

Let us now twist the exact sequence (5.1) by the cocycle c', so that we get the following twisted exact sequence:

$$
(5.3) \qquad\qquad 1 \longrightarrow {}_{c'}A \longrightarrow {}_{c'}E \xrightarrow{\quad} {}_{c'}G \longrightarrow 1.
$$

where we remark once again that $_{c'}G = G$ and that the section s is still well defined on these twisted forms.

Since β' and $\beta'' = [c']$ have the same image in $\mathrm{H}^1(K, G)$, we know that $_{c'}\beta'$ must come from an element $\alpha' \in \mathrm{H}^1(K, {}_{c'}A)$ and that its image $(\alpha_v')_{v \in S} \in \prod_S \mathrm{H}^1(K, {}_{c'}A)$ maps to $(_{c'}\beta'_v)_{v \in S} \in \prod_S \mathrm{H}^1(K, {}_{c'}E)$. In particular, since $(\alpha_v')_{v \in S}$ comes from a global element, we know by Proposition 2.5 that

$$
(5.4) \qquad\qquad (\alpha_v')_{v \in S} \text{ is orthogonal to } \mathrm{III}_S^1(K, {}_{c'}\hat{A}).
$$

Consider now Diagram (5.2) and the element $(\alpha_v)_{v \in S} \in \prod_S \mathrm{H}^1(K_v, {}_cA)$ from Step 3. By construction, this element is not orthogonal to $c^*(\gamma)$ and hence its image $(i_v(\alpha_v))_{v \in S} \in \prod_S \mathrm{H}^1(K, {}_{c'}A)$ is not orthogonal to $c'^*(\gamma)$.

The two elements $(i_v(\alpha_v))_{v \in S}$ and $(\alpha'_v)_{v \in S}$ have the same image in $\prod_{v \in S} \mathrm{H}^1(K_v, {}_{c'}E)$ by construction (recall that $c_v = c'_v$ for $v \in S$ and hence ${}_c\beta'_v = {}_{c'}\beta'_v$). Thus, $(i_v(\alpha_v))_{v \in S}$ and $(\alpha'_v)_{v \in S}$ differ by an action (as described in (2.2), §2.4) of an element of the group

$$\mathrm{Coker}\left(\prod_{v \in S} \mathrm{H}^0(K_v, {}_{b'}E) \to \prod_{v \in S} \mathrm{H}^0(K_v, {}_{c'}G)\right).$$

We denote by $(g_v)_{v \in S} \in \prod_S \mathrm{H}^0(K_v, {}_{c'}G)$ a lift of this element.

Now, for all $v \in S \setminus \{v_0\}$, we have by construction $\beta'_v = 1 \in \mathrm{H}^1(K_v, E)$ and hence b' (and a fortiori c') is trivial over $\mathrm{Gal}(K_v)$ since E is constant. The map $\mathrm{H}^0(K_v, {}_{b'}E) \to \mathrm{H}^0(K_v, {}_{c'}G)$ corresponds then to $E \to G$, which is surjective. Therefore, $i_v(\alpha_v) = \alpha'_v$ and $\mathrm{H}^0(K_v, {}_{c'}G)$ acts trivially on $i_v(\alpha_v)$ for these v. Finally, the map $\mathrm{H}^0(K, {}_{c'}G) \to \mathrm{H}^0(K_{v_0}, {}_{c'}G)$ is clearly surjective (recall that ${}_{c'}G = G$ and hence both groups are equal to G and the map is the identity), hence g_{v_0} lifts to an element $g \in \mathrm{H}^0(K, G)$. We conclude then that $g \cdot (i_v(\alpha_v))_{v \in S} = (\alpha'_v)_{v \in S}$.

Note that the natural paring ${}_{c'}A \times {}_{c'}\hat{A} \to \mathbb{G}_m$ is invariant under the morphism $(g, \hat{g}^{-1}) : {}_{c'}A \times {}_{c'}\hat{A} \to {}_{c'}A \times {}_{c'}\hat{A}$ given by $(a, f) \to (g \cdot a, \hat{g}^{-1} \cdot f)$, where $\hat{g} : {}_{c'}\hat{A} \to {}_{c'}\hat{A}$ is the dual map to $g : {}_{c'}A \to {}_{c'}A$ defined by the conjugation action of G on ${}_{c'}A$. By functoriality of cup products [11, Prop. 1.4.2], the cup product $\mathrm{H}^1(K_v, {}_{c'}A) \times \mathrm{H}^1(K_v, {}_{c'}\hat{A}) \to \mathbb{Q}/\mathbb{Z}$ is also invariant under the morphism induced by $(g, \hat{g}^{-1})$. Since $(i_v(\alpha_v))_{v \in S}$ is not orthogonal to $c'^*(\gamma)$, it follows that $g \cdot (i_v(\alpha_v))_{v \in S}$ is not orthogonal to $\hat{g}^{-1}(c'^*(\gamma))$. But as $c'^*(\gamma)$ is in $\mathrm{III}^1_S(K, {}_{c'}\hat{A})$ so is $\hat{g}^{-1}(c'^*(\gamma))$, hence we finally get that

$$g \cdot (i_v(\alpha_v))_{v \in S} = (\alpha'_v)_{v \in S} \text{ is not orthogonal to } \mathrm{III}^1_S(K, {}_{c'}\hat{A}),$$

contradicting (5.4). $\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\qquad\square$

BIBLIOGRAPHY

[1] J.-L. COLLIOT-THÉLÈNE, "Points rationnels sur les fibrations", in *Higher dimensional varieties and rational points (Budapest, 2001)*, Bolyai Soc. Math. Stud., vol. 12, Springer, 2003, p. 171-221.

[2] ———, "Groupe de Brauer non ramifié d'espaces homogènes de tores", *J. Théor. Nombres Bordx.* **26** (2014), no. 1, p. 69-83.

[3] P. DÈBES & N. GHAZI, "Galois covers and the Hilbert-Grunwald property", *Ann. Inst. Fourier* **62** (2012), no. 3, p. 989-1013.

[4] C. DEMARCHE, "Groupe de Brauer non ramifié d'espaces homogènes à stabilisateurs finis", *Math. Ann.* **346** (2010), no. 4, p. 949-968.

[5] W. GRUNWALD, "Ein allgemeines Existenztheorem für algebraische Zahlkörper", *J. Reine Angew. Math.* **169** (1933), p. 103-107.

[6] D. HARARI, "Quelques propriétés d'approximation reliées à la cohomologie galoisienne d'un groupe algébrique fini", *Bull. Soc. Math. France* **135** (2007), no. 4, p. 549-564.

[7] L. KALOUJNINE, "La structure des *p*-groupes de Sylow des groupes symétriques finis", *Ann. Sci. Éc. Norm. Supér.* **65** (1948), p. 239-276.

[8] G. LUCCHINI ARTECHE, "Approximation faible et principe de Hasse pour des espaces homogènes à stabilisateur fini résoluble", *Math. Ann.* **360** (2014), no. 3-4, p. 1021-1039.

[9] ———, "Groupe de Brauer non ramifié des espaces homogènes à stabilisateur fini", *J. Algebra* **411** (2014), p. 129-181.

[10] J. NEUKIRCH, "On solvable number fields", *Invent. Math.* **53** (1979), no. 2, p. 135-164.

[11] J. NEUKIRCH, A. SCHMIDT & K. WINGBERG, *Cohomology of number fields*, second ed., Grundlehren der Mathematischen Wissenschaften, vol. 323, Springer, 2008, xvi+825 pages.

[12] R. S. PIERCE, *Associative algebras*, Graduate Texts in Mathematics, vol. 88, Springer, 1982, Studies in the History of Modern Science, 9, xii+436 pages.

[13] D. J. SALTMAN, "Generic Galois extensions and problems in field theory", *Adv. Math.* **43** (1982), no. 3, p. 250-283.

[14] J.-P. SERRE, *Galois cohomology*, english ed., Springer Monographs in Mathematics, Springer, 2002, Translated from the French by Patrick Ion and revised by the author, x+210 pages.

[15] A. SKOROBOGATOV, *Torsors and rational points*, Cambridge Tracts in Mathematics, vol. 144, Cambridge University Press, 2001, viii+187 pages.

[16] S. WANG, "On Grunwald's theorem", *Ann. Math.* **51** (1950), p. 471-484.

[17] A. J. WEIR, "Sylow *p*-subgroups of the classical groups over finite fields with characteristic prime to *p*", *Proc. Amer. Math. Soc.* **6** (1955), p. 529-533.

Cyril DEMARCHE
Sorbonne Universités, UPMC Univ Paris 06
Institut de Mathématiques de Jussieu-Paris Rive
Gauche
UMR 7586, CNRS
Univ Paris Diderot, Sorbonne Paris Cité
F-75005, Paris (France)
Current address:
Département de Mathématiques et Applications
École Normale Supérieure
45 rue d'Ulm, 75230 Paris Cedex 05 (France)
cyril.demarche@imj-prg.fr

Giancarlo LUCCHINI ARTECHE
École polytechnique
Centre de Mathématiques Laurent Schwartz
UMR CNRS 7640
91128 Palaiseau Cedex (France)
giancarlo.lucchini-arteche@polytechnique.edu

Danny NEFTIN
Technion - Israel Institute of Technology
Mathematics Department
Haifa, 3200 (Israel)
dneftin@tx.technion.ac.il