On the local-global principle for tori over arithmetic curves

Jean-Louis Colliot-Thélène
(CNRS et Université Paris-Sud $\subset$ Paris-Saclay)

Petersburg Motives
Ivan Panin's 60th birthday
Euler Institute
Sankt-Petersburg
2-6 September 2019

After joint works with

D. Harbater
J. Hartmann
D. Krashen
R. Parimala
V. Suresh

Theorem (L. Euler) : Demonstratio theorematis Fermatiani omnem numerum sive integrum sive fractum esse summam quatuor pauciorumve quadratorum.

Novi commentarii academiae scientiarum Petropolitanae **5** (1754/55), 13–58.

k a global field, $k_v, v \in \Omega$, the set of all completions
For X a homogeneous space of a connected linear algebraic group G over k, does the local-global principle hold, namely, do we have

$$\prod_{v \in \Omega} X(k_v) \neq \emptyset \Longrightarrow X(k) \neq \emptyset$$

Particular interest in the case of principal homogeneous spaces under a group G, they are classified by the cohomology set $H^1(k, G)$
One then asks whether the set

$$Ш(k, G) := \mathrm{Ker}[H^1(k, G) \to \prod_v H^1(k_v, G)]$$

is reduced to one point.

Answer : No in general, yes under specific conditions

Counterexamples of the following type

• Norm equations

$$Norm_{K/k}(\xi) = c$$

with $c \in k^*$ (principal homogeneous space of the torus $Norm_{K/k}(\xi) = 1$)
for K/k Galois with group $(\mathbb{Z}/p)^2$

• Principal homogeneous spaces of some semisimple linear algebraic groups (neither simply connected nor adjoint)

$k = \mathbb{Q}$, $c \in \mathbb{Q}^*$, $D/\mathbb{Q}$ the Hamilton quaternions
Euler's theorem :

Local-global principle for

$$c = x^2 + y^2 + z^2 + t^2$$

principal homogeneous spaces under the group $SL(1, D)$, which is $\mathbb{Q}$-rational (Diophantos) and semisimple simply connected.

Local-global principle for homogeneous quadrics

$$cw^2 = x^2 + y^2 + z^2 + t^2$$

More generally, positive answer for :

• Quadrics (Hasse), more generally projective homogeneous varieties (Harder).

• Norm equations $c = Norm_{K/k}(\xi)$ for K/k cyclic (principal homogeneous space of the torus $1 = Norm_{K/k}(\xi)$.

Principal homogeneous spaces of :

• simply connected semisimple groups (very long history, basic for all results on other semisimple gorups)

• adjoint (semisimple) groups

• absolutely almost simple semisimple groups

• k-rational groups (function field $k(G)$ purely transcendental) (Sansuc)

The following theorem covers these various cases.

Theorem (Sansuc, Borovoi). *Let k be a number field and X a homogeneous space of a connected linear algebraic group. Assume that the stabilizers are connected. Let X_c be a smooth compactification of X. The Galois module $\mathrm{Pic}(\overline{X}_c)$ is a lattice. If $H^1(k, \mathrm{Pic}(\overline{X}_c)) = 0$, then the local-global principle holds for rational points of X.*

[Note : For X as above, $\mathrm{Br}(X_c)/Im(\mathrm{Br}(k)) = H^1(k, \mathrm{Pic}(\overline{X}_c))$.]

The proof uses Galois cohomology and class field theory to reduce to the basic case of principal homogeneous spaces of semisimple simply connected groups, where the proof is, as of to-day, case by case.

Let k be a number field. If k_v is a nonarchimedean completion, then any quadratic form over k_v in at least 5 variables has a nontrivial zero. As a consequence of the Hasse principle, over a number field any totally indefinite quadratic form in at least 5 variables has a nontrivial zero.

A field F is called C_i if any homogeneous form of degree d in $n > d^i$ variables has a non trivial zero. Serge Lang studied the behaviour of the C_i-property under extensions of the ground field (adding one variable, going over to a finite extension, completing for a discrete valuation).

Suppose K is a p-adic field and $F = K(C)$ is the function field of a curve. Associated to integral proper models of F there are completions F_w of F with respect to a family of obvious discrete valuations w of rank one of two types (trivial on K or not). Their residue fields are of two types : a p-adic field, or the function field of a curve over a finite field (the latter by Lang's theorems). Over the completions K_w, any quadratic form in 9 variables has a nontrivial zero. Can one conclude that any quadratic form in 9 variables over F has a nontrivial zero ?
Given a field L, one writes $u(L)$ for the maximum rank of an anisotropic quadratic form over L. The question is thus :

$$\text{Is} \quad u(F) = 8?$$

This question was solved affirmatively by Parimala and Suresh (for $p \neq 2$) (1998, 2010). They used arithmetical results of Kato and Saito on higher class field theory, along with Merkurjev's theorem on K_2. A very different proof (also for $p = 2$) was later given by D. Leep, who built in an essential manner on a result of Heath-Brown and on ideas going back to Lang.

A very different proof of a more general result was given by Harbater, Hartmann and Krashen (2009). They replaced the p-adic field by the field of fractions K of an arbitrary complete discrete valuation ring R.
The function field over a curve over such a field K is called a semi-global field.

Theorem (HHK 2009) *Let K be a complete dvr with residue field k of char. different from 2. Suppose :*
1) Any quadratic form of rang $> n$ over a finite extension of k has a nontrivial zero.
2) Any quadratic form over the function field of a curve over k of rank $> 2n$ has a nontrivial zero.
Then any quadratic form of rang $> 4n$ over the function field of a curve over K has a nontrivial zero.

A special case is : $u(F) = 8$ for the function field of a curve over a nondyadic p-adic field. Then k is a finite field, and one takes $n = 2$.

The HHK method : The patching set-up

R a complete dvr, k its residue field, assumed perfect, K its fraction field, $t \in R$ a uniformizing parameter.
$\mathcal{X}/R$ a regular, proper, integral curve over R.
$F = K(\mathcal{X})$, referred to as a semi-global field
Y/k the special fibre
$Y^{red} = \cup_{i \in I} Y_i$ with each Y_i/k smooth. One assumes normal crossings.
$\mathcal{P}$ a finite set of closed points of Y containing all the singular points of Y and at least one point of each component Y_i.

For each connected component U of $Y^{red} \setminus \mathcal{P}$, one denotes $R_U \subset F$ the ring of functions regular on U, then $\hat{R}_U$ its t-completion, and F_U the field of fractions of $\hat{R}_U$. There is a surjective map $\hat{R}_U \to k[U]$.
For $P \in Y \subset \mathcal{X}$ one lets F_P denote the quotient of the complete local ring $\hat{R}_P = O_{\mathcal{X},P}$.
For a closed point $P \in X$ in the closure of U, one considers the local ring of $\hat{R}_P = O_{\mathcal{X},P}$ at the codimension 1 point defined by U, completes it, and calls $F_{U,P}$ the field of fractions of that DVR.
One calls such a pair (U, P) a branch. There are inclusions $F_U \subset F_{U,P}$ and $F_P \subset F_{U,P}$. The field $F_{U,P}$ is in a sense built out of the fields F_U and F_P.
The original field $F = K(\mathcal{X})$ is the inverse limit of the entire system $\{F_U, F_P, F_{U,P}\}$.

Simplest case $\mathcal{X} = \mathbb{P}^1_{k[[t]]}$.
$F = k((t))(x)$
$U = \mathrm{Spec}\,(k[x^{-1}]) = \mathbb{A}^1_k \subset \mathbb{P}^1_k$
$P = \mathbb{P}^1_k \setminus \mathbb{A}^1_k$

$F_P = k((t, x))$
$F_U = k(x)((t))$
$F_{U,P} = k((x))((t))$.

Let G/F be a linear algebraic group, $\mathcal{X}/R$ and $\mathcal{P}$ as above, let $Ш_{\mathcal{P}}(F, G)$ be the kernel of the finite product of maps :

$$H^1(F, G) \to \prod_P H^1(F_P, G) \times \prod_U H^1(F_U, G).$$

Theorem (HHK 2015). *There is a bijection of pointed sets between* $Ш_{\mathcal{P}}(F, G)$ *and the double coset*

$$\prod_P G(F_P) \Big\backslash \prod_{U,P} G(F_{U,P}) \Big/ \prod_U G(F_U)$$

Theorem (HHK 2009) *If G is a connected reductive group and its underlying F-variety is F-**rational**, then this double quotient is reduced to one point.*

One thus gets local-global statements with respect to the finite set of overfields $\{F_U, F_P\}$.

The case of number fields would suggest investigating other local-global statements, namely with respect to completions of a field $F = K(\mathcal{X})$ at all discrete valuation rings of F. Let us write $Ш_{dvr}(F, G)$ for the corresponding kernel.

The relation between $Ш_{dvr}(F, G)$ and the various $Ш_{\mathcal{P}}(F, G)$ for varying $\mathcal{P}$ is not simple.

One has :

$$Ш_{\mathcal{P}}(F, G) \subset Ш_{dvr}(F, G)$$

If moreover G/F comes from a reductive group over a given regular model $\mathcal{X}$ ("G/F has good reduction over $\mathcal{X}$"), one also knows

$$\bigcup_{\mathcal{P}} Ш_{\mathcal{P}}(F, G) = Ш_{dvr}(F, G)$$

and to compute the latter set it is enough to look at the kernel $Ш_{dvr,\mathcal{X}}(F, G)$ associated to just the local rings at codimension one points of any given model $\mathcal{X}$.

In some cases it has been possible to deduce local-global principles with respect to discrete valuation rings from the patching result of HHK.

Theorem (CT, Parimala, Suresh 2012). Let $F = K(C)$ be the function field of a curve over the field of fractions of a complete discrete valuation ring of residue characteristic not 2. If a nondegenerate quadratic form of rank at least 3 over F is isotropic over all completions of F with respect to discrete valuations, then it is isotropic over F.

Note : this is wrong for quadratic forms of rank 2.

In the classical case of a number field k, the basic theorem is $Ш(k, G) = 1$ for G a semisimple simply connected group over k. And the triviality of $Ш(k, G)$ for G k-rational is ultimately a consequence of that fact.
In CPS12, for $F = K(C)$ the function field of a curve over the field of fractions of a complete dvr R with residue field k a finite field (i.e. K p-adic), we asked whether the various sets $Ш(F, G)$ are trivial if G/F is simply connected, and we proved it under certain hypotheses (using properties of the Rost invariant and arithmetic results of K. Kato).
One may ask the same question without the restriction on the residue field k.

To start with, it turned out to be difficult to produce even some *connected* linear algebraic group G with one of these $Ш(F, G)$ nontrivial.

In CPS16, we found the first examples, with $Ш_{\mathcal{P}}(F, G) \neq 0$ and $Ш_{dvr}(F, G) \neq 0$ for G a torus over the function field F of an elliptic curve over $K = \mathbb{C}((t))$. The elliptic curve has bad reduction, there is a loop in the special fibre of a regular model $\mathcal{X}/R$. The method did not use HHK. It used the Brauer group of the generic fibre of $\mathcal{X}/R$ and the Bloch-Ogus complex on the 2-dimensional regular model $\mathcal{X}/R$.

One can also produce a toric counterexample over the function field of $\mathbb{P}^1_{\mathbb{C}((t))}$.

In these examples, the torus has bad reduction over the regular model.

Question 1 : Are there counterexamples to the local-global principle over the field of functions F of a regular proper relative curve $\mathcal{X}/R$ (with R complete dvr) for a principal homogeneous space (over F) of *an $\mathcal{X}$-torus, in particular of an R-torus*?
Question 2 : What about the situation for principal homogeneous spaces of simply connected groups ?
It has now turned out that under a good reduction hypothesis on the group G over the model $\mathcal{X}$, using the HHK approach it is possible to produce precise estimates for the *size* of $Ш_{\mathcal{P}}(X, G)$ leading to

- new cases where the local-global principle holds
- new, simpler counterexamples to the local-global principle for homogeneous spaces of tori
- counterexamples for homogeneous spaces of simply connected groups, thus producing the first examples of this kind over a semi-global field.

Tori

Reminders (Voskresenskiĭ, Endo-Miyata, CT-Sansuc in the 70s).

Given a torus T over a field k, there exists a "nearly canonical" exact sequence of k-tori

$$1 \to S \to Q \to T \to 1$$

with Q a quasitrivial torus and S a flasque torus. By definition this is a torus S whose cocharacter group is H^1-trivial as a Galois lattice over k.

One way to get such a resolution is to take a smooth compactification X of T over k and to consider the dual of the exact sequence of Galois lattices

$$0 \to k_s[T]^*/k_s^* \to \mathrm{Div}_\infty(X \times_k k_s) \to \mathrm{Pic}(X \times_k k_s) \to 0.$$

Flasque tori over a field have the remarkable property that a principal homogeneous space of S over an open set U of a smooth k-variety extends to the whole of X : there is no ramification (CT-Sansuc).

The theory of flasque tori and flasque resolutions extends to tori over noetherian schemes.

In particular if X is a regular scheme and S/X a flasque torus, for any open set $U \subset X$ the restriction map $H^1_{et}(X, S) \to H^1_{et}(U, S)$ is surjective : principal homogeneous spaces under S extend.

Given an algebraic group G over k, the group $G(k)/R$ is the quotient of the group $G(k)$ of rational points by R-equivalence, which is generated by the elementary relation : for any k-morphism $V \to G$ with $V \subset \mathbb{P}^1_k$ all points in the image of $V(k)$ are related.

For a k-torus T, a flasque resolution

$$1 \to S \to Q \to T \to 1$$

induces an isomorphism $T(k)/R \simeq H^1(k, S)$ (CT-Sansuc thesis) – in a functorial way.

For G reductive over F, the HHK theorem is :

$$Ш_{\mathcal{P}}(F,G) \simeq \prod_{P} G(F_P) \Big\backslash \prod_{U,P} G(F_{U,P}) \Big/ \prod_{U} G(F_U) .$$

For an arbitrary connected reductive group G over F, the pointed set $Ш_{\mathcal{P}}(F,G)$ admits the pointed double coset

$$\prod_{P} G(F_P)/R \Big\backslash \prod_{U,P} G(F_{U,P})/R \Big/ \prod_{U} G(F_U)/R$$

as a quotient.

For a torus T over F and a flasque resolution

$$1 \to S \to Q \to T \to 1$$

one can do better. One has isomorphisms of abelian groups

$$Ш_{\mathcal{P}}(F,T) \simeq \prod_P T(F_P)/R \Big\backslash \prod_{U,P} T(F_{U,P})/R \Big/ \prod_U T(F_U)/R$$

and

$$Ш_{\mathcal{P}}(F,T) \simeq \prod_P H^1(F_P,S) \Big\backslash \prod_{U,P} H^1(F_{U,P},S) \Big/ \prod_U H^1(F_U,S)$$

Using the good properties of flasque tori over regular local rings, one proves :

Theorem. If T is a *torus* over $\mathcal{X}$, and $\mathcal{P}$ is as above, then one has

$$Ш_{\mathcal{P}}(F,T) = Ш_{dvr}(F,T) = Ш_{dvr,\mathcal{X}}(F,T).$$

Using the double coset formula, we shall now discuss how to compute this group.

One must get some control on the individual maps $H^1(F_P,S) \to H^1(F_{U,P},S)$ and $H^1(F_U,S) \to H^1(F_{U,P},S)$, and then combine this with the properties of the graph of components of the special fibre of $\mathcal{X}/R$.

Here are some of the key points.

Let $1 \to S \to Q \to T \to 1$ be a flasque resolution of the $\mathcal{X}$-torus T.

Let $\kappa(P)$ denote the residue field at a (schematic) point P of $\mathcal{X}$.

The map $H^1(F_P, S) \to H^1(F_{U,P}, S)$ for a given branch (U, P)

Both fields F_P and $F_{U,P}$ are fields of fractions of complete regular local rings. Using the fact that S is flasque, one shows :

• At any point $P \in \mathcal{P}$ there is a natural specialisation map $H^1(F_P, S) \to H^1(\kappa(P), S)$ and it is an isomorphism.

• At any branch (U, P) we have natural isomorphisms

$$H^1(F_P, S) \simeq H^1(F_{U,P}, S) \simeq H^1(\kappa(P), S).$$

The map
$H^1(F_U, S) \to \prod_{(U,P)} H^1(F_{U,P}, S) \simeq \prod_{(U,P)} H^1(\kappa(P), S)$
for a given U**, with** P **running through all points** $P \in \mathcal{P}$ **in the closure of** U**.**

If $\overline{U} \subset Y^{red}$ denotes the smooth integral projective curve over k which is the closure of U and $k(U)$ its field of fractions, the image of the above map coincides with the image of specialisation maps

$$H^1(k(U), S) \to \prod_{(U,P)} H^1(\kappa(P), S)$$

and even better

$$H^1(\overline{U}, S) \to \prod_{(U,P)} H^1(\kappa(P), S)$$

Let us give easy consequences.

Proposition A. Let $\mathcal{X}/R$ be as above. Assume that the residue field k of R has cohomological dimension at most 1. If T is an $\mathcal{X}$-torus, then $\text{Ш}_{dvr}(F, T) = 0$.

Indeed the hypothesis on k implies $H^1(\kappa(P), S) = 0$, hence each $H^1(F_{U,P}, S) = 0$.

Note that in the CPS16 counterexample the residue field k is the complex field. But there the torus T over F had bad reduction over $\mathcal{X}$.

Theorem B. Let $\mathcal{X}/R$ be as above. Assume that the special fibre Y/k of $\mathcal{X}/R$ is a simple normal crossing divisor all reduced components of which are isomorphic to $\mathbb{P}^1_k$ and that these components intersect at k-points. Assume that T is an R-torus, and let $1 \to S \to Q \to T \to 1$ be a flasque resolution of T over R. Let Γ denote the reduction graph associated to the special fibre. Let m denote the number of cycles of that graph, i.e. the rank of $H_1(\Gamma_{\mathrm{top}}, \mathbb{Z})$. Then

$$Ш(F, T) \simeq H^1(k, S)^m.$$

If we drop just the hypothesis that the components intersect at rational points, we still have a nice formula.

Theorem C. Assume that the special fibre Y/k of $\mathcal{X}/R$ is a simple normal crossing divisor all components of which are isomorphic to $\mathbb{P}^1_k$ and that T is an R-torus. Then there is an exact sequence

$$0 \to \mathrm{Hom}(H_1(\Gamma_{\mathrm{top}}, \mathbb{Z}), H^1(k, S)) \to Ш(F, T)$$

$$\to \prod_{\mathcal{P}} [H^1(\kappa(P), S)/H^1(k, S)] \to 0.$$

Suppose we are given a field k and a k-torus T_0 with a flasque resolution

$$1 \to S_0 \to Q_0 \to T_0 \to 1,$$

such that $T_0(k)/R \simeq H^1(k, S_0) \neq 0$.
To produce examples of $\mathcal{X}, T/R$ such that $Ш(F, T) \neq 0$ it is then enough to take $\mathcal{X}/R$ a model as in Theorem B (all reduced components $\mathbb{P}^1_k$, transversal intersections defined over k) with a loop in the reduced fibre, and to take for T/R the obvious lift of the k-torus T_0.
It is well known how to choose T_0/k as above. One may produce a biquadratic extension of number fields, or even of p-adic fields ℓ/k with $T_0 = R^1_{\ell/k}\mathbb{G}_m$ such that $T_0(k)/R \neq 0$. Note that here we have $cd(k) \geq 2$.
One variant of this construction provides examples over a big field k with $Ш(F, T)$ infinite.

The previous results are detailed in a recent preprint on arXiv. Another result (CHHKPS 2018), to be included in a future paper, is :

Theorem *There exists a field* k*, a semisimple simply connected group* G *over* k *and a regular proper curve* $\mathcal{X}$ *over* $R = k[[t]]$*, with function field* F*, such that* $Ш_{div}(F, G) \neq \{*\}$*.*

More precisely, we may take
$k = \mathbb{C}((a))((b))((c))((d))$
$G = SL(1, D)$ with $D = (a, b) \otimes (c, d)$ (tensor product of quaternion algebras)
$\mathcal{X}/R$ a regular model with special fibre Y/k consisting of two $\mathbb{P}^1_k$'s intersecting transversally in two k-points.

Note that $cd(F) = 6$.

Proof. For an arbitrary connected reductive group G over F, recall that the pointed set $Ш_{\mathcal{P}}(F, G)$ admits the pointed double coset

$$\prod_P G(F_P)/R \Big\backslash \prod_{U,P} G(F_{U,P})/R \Big/ \prod_U G(F_U)/R$$

as a quotient. We assume that G comes from an *anisotropic* reductive group over k, and that the special fibre Y/k is a (reduced) union of $\mathbb{P}^1_k$'s meeting transversally at k-rational points. We then prove that there are surjective specialisation maps
$sp_P : G(F_P)/R \to G(k)/R$
$sp_U : G(F_U)/R \to G(k)/R$
$sp_{U,P} : G(F_{U,P})/R \to G(k)/R$
which are compatible with the maps $G(F_P) \to G(F_{U,P})$ and $G(F_U) \to G(F_{U,P})$.

To prove this, one lemma is :
Let G/k be an *anisotropic* reductive group.
Let $\theta_{x,y}$ denote the composition of $G(k((x,y))) \subset G(k((x))((y)))$ with the series of specialisation maps (at the obvious points)

$$G(k((x))((y))) = G(k((x))[[y]]) \to G(k((x))) = G(k[[x]]) \to G(k)$$

and finally the map $G(k) \to G(k)/R$.
And let $\theta_{y,x}$ denote the map obtained by permuting x and y. Then $\theta_{x,y} = \theta_{y,x}$.

This uses the fact that in iterated blow-ups at a k-point P of a smooth k-surface all k-points on the exceptional divisor are R-equivalent.

One then finds that $Ш_{\mathcal{P}}(F, G)$ has a natural quotient of the shape

$$\prod_P G(k)/R \Big\backslash \prod_{U,P} G(k)/R \Big/ \prod_U G(k)/R$$

where all maps $G(k)/R \to G(k)/R$ are identity maps.
If for instance the special fibre consists of two $\mathbb{P}^1_k$'s intersecting transversally at two k-rational points, then one finds that elements of the shape $(a, b, c, d) \in \prod_{U,P} G(k)/R$ (in a suitable order) which do not satisfy $a.d^{-1}.b.c^{-1} = 1$ represent nontrivial elements in the quotient.

To produce the required counterexamples to the local-global principle for a simply connected group over the field $F = \mathbb{C}((a))((b))((c))((d))((t))(x)$, it remains to recall the following results from the 70s.

(Platonov) Let $k = \mathbb{C}((a))((b))((c))((d))$. Let $D = (a, b) \otimes (c, d)$ (tensor product of two quaternion algebras). Then the quotient $SK_1(D)$ of D^{*1} (elements of reduced norm 1) by the commutator subgroup is non-zero.

(Voskresenskiĭ, using a result of Platonov) Let D/k be a central simple algebra over a field k. Let $G = SL(1, D)$. Then $SK_1(D) = G(k)/R$.