

# The Bloch–Kato Selmer Group

Tony Feng

January 27, 2016

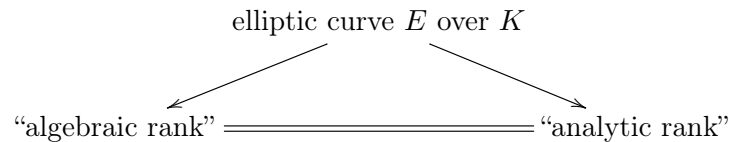
## 1 Overview

### 1.1 The baby Bloch–Kato conjecture

The “weak” BSD conjecture predicts that for an elliptic curve  $E$  over a number field  $K$ , we have

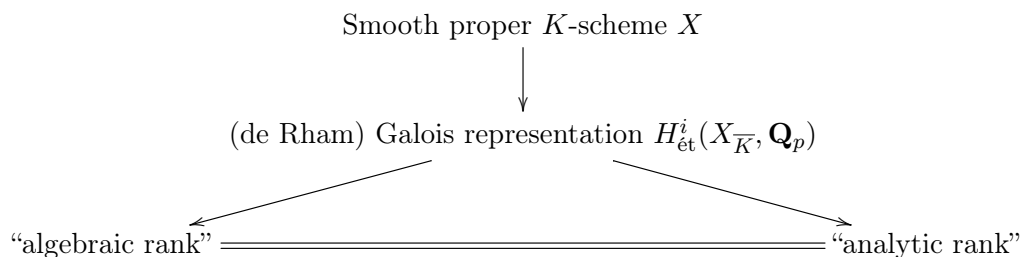
$$\text{rank } E(K) = \text{ord}_{s=1} L(E/K, s).$$

The miracle of this formula is that it relates two quantities with very different origins: the left hand side is an *algebraic* object while the right hand side is an *analytic* object. Furthermore, the algebraic rank is “global” in nature, while the analytic rank can be defined locally.



In the next two talks I will discuss a “generalization” of this conjecture to arbitrary smooth proper varieties over a number field  $K$  – this is a baby version of the Bloch–Kato conjecture (which in full generality applies to a much wider class of varieties, and also predicts the *leading coefficient* of the  $L$ -function in terms of periods and algebraic data).

For my purposes, the starting point for the Bloch–Kato conjecture is a Galois representation appearing in the étale cohomology of a *smooth proper*  $K$ -scheme  $X$ , and it predicts the agreement of a certain “algebraic rank” and an “analytic rank”.



Now, the natural question is what the “algebraic rank” and “analytic rank” are. You can probably guess what the analytic rank is: we have already defined the  $L$ -function attached to an  $\ell$ -adic representation of  $G_K$  unramified at all but finitely many primes, and up to non-trivial “independence of  $\ell$ ” and rationality issues for characteristic polynomials of Frobenius at *all* finite places, this definition makes sense without further comment. This  $L$ -function conjecturally admits an analytic continuation, and the analytic rank is defined to be its order of vanishing at a special point.

On the other hand, it is more challenging to define the “algebraic rank”, and in fact that is the subject of this entire first talk (and some of the second as well). It will turn out in the end to be essentially the  $\mathbf{Q}_p$ -rank of a certain vector space, which we call the “Bloch–Kato Selmer group”.

The ultimate statement of the conjecture is that for a  $p$ -adic Galois representation  $V$  coming from geometry:

$$\text{ord}_{s=0} L(s, V) = \dim H_f^1(G_K, V^*(1)) - \dim H^0(G_K, V^*(1)).$$

Here are three examples that show what kind of interesting statements we can expect the Bloch–Kato conjecture to encompass.

*Example 1.1.* For  $X = A$  an abelian variety over  $K$  and Galois representation  $H_{\text{ét}}^1(A_{\overline{K}}, \mathbf{Q}_p)$ , the rank of the Bloch–Kato Selmer group is equal to the rank of  $A$  if  $\text{III}_A$  is finite, which is of course conjecturally true (and necessary even to make sense of the strong BSD conjecture). Therefore, *assuming the finiteness of  $\text{III}_A$*  the baby Bloch–Kato conjecture for  $A$  is equivalent to the weak BSD conjecture for  $A$ .

*Example 1.2.* For the Galois representation  $\mathbf{Q}_p$  (with  $\mathbf{Q}_p(-1) = H_{\text{ét}}^2(\mathbf{P}_{\overline{K}}^1)$ ), the rank of the Bloch–Kato Selmer group is equal to the rank of  $\mathcal{O}_K^\times$ . A reasonable way to think about this is that  $H_f^1(G_K, \mathbf{Z}_p(1))$  is the  $p$ -adic completion of  $\mathcal{O}_K^\times$  and hence the right side of the conjecture is exactly  $\text{rank}(\mathcal{O}_K^\times) = r_1 + r_2 - 1$ .

On the other side we have the  $L$ -function of  $\mathbf{Q}_p(1)$ , and this has trivial Euler factor at the  $p$ -adic places but Euler factor at places  $v$  not over  $p$  given by  $(1 - q_v^{1-s})^{-1}$ , so

$$L(s, \mathbf{Q}_p(1)) = \zeta_K(s) \cdot \prod_{v|p} (1 - q_v^{1-s})^{-1}$$

and hence the vanishing order at  $s = 0$  is that same as that for  $\zeta_K$ . Thus, the baby Bloch–Kato conjecture for  $\mathbf{Q}_p(1)$  amounts Dirichlet’s Unit Theorem plus the analytic continuation of the Dedekind zeta function for  $K$ :

$$r_1 + r_2 - 1 = \text{ord}_{s=0} \zeta_K(s).$$

*Example 1.3.* In particular, the baby Bloch–Kato conjecture will predict the integer zeros of the Riemann zeta function  $\zeta(s)$ . This is fairly subtle! Recall that  $\zeta(s)$  vanishes at negative *even* integers  $-2, -4, \dots$ . Therefore, we’ll eventually have to

give a uniform algebraic definition that is sensitive to parity and sign in the special case of  $\mathbf{Q}_p$ . Since  $L(V(n), s) = L(V, s + n)$ , the conjecture will state that except for  $n = 0, 1$ :

$$\text{ord}_{s=0} \zeta(n) = \dim H_f^1(G_{\mathbf{Q}}, \mathbf{Q}_p(1 - n))$$

and so we should see that

$$\dim H_f^1(G_{\mathbf{Q}}, \mathbf{Q}_p(n)) = \begin{cases} 1 & n \text{ odd} > 1, \\ 0 & \text{otherwise.} \end{cases}$$

Keep these examples in mind throughout; they will serve as “sounding boards” for our definitions.

## 1.2 The classical Selmer group

The construction of the Bloch–Kato Selmer group is modelled on that for the usual Selmer group of an abelian variety  $A$  over  $K$ , so let’s recall how that goes. The point is to embed  $A(K)$  inside some cohomology group as in the proof of the Mordell–Weil Theorem. For an integer  $m > 0$ , we have a short exact sequence of smooth  $K$ -groups

$$0 \rightarrow A[m] \rightarrow A \xrightarrow{m} A \rightarrow 0. \quad (1.1)$$

From the long exact sequence for Galois (or equivalently étale) cohomology, we extract a short exact sequence

$$0 \rightarrow A(K)/mA(K) \rightarrow H^1(K, A[m]) \rightarrow H^1(K, A)[m] \rightarrow 0.$$

Thus we can realize  $A(K)/mA(K)$  inside  $H^1(K, A[m])$ . The group  $A(K)/mA(K)$  is isomorphic to  $(\mathbf{Z}/m\mathbf{Z})^{\oplus r}$  plus a *uniformly bounded* part (as  $m$  varies) arising from  $A(K)_{\text{tor}}$ , so this almost detects the rank. However, the group  $H^1(K, A[m])$  is too crude of a container; for instance, it is generally infinite! (For example, recall that  $H^1(K, \mu_m) = K^\times / (K^\times)^m$ , and this is huge.) One thing we must do is cut it down by local conditions, exactly as in the proof of the Mordell–Weil Theorem.

Recall the restriction maps  $H^1(K, A[m]) \rightarrow H^1(K_v, A[m])$  for any place  $v$  of  $K$ . Under this restriction, any class in  $H^1(K, A[m])$  in the image of  $A(K)/mA(K)$  certainly maps to a class of  $H^1(K_v, A[m])$  in the image of  $A(K_v)/mA(K_v)$ , and we have a similar exact sequence for each  $K_v$ , leading to a commutative diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A(K)/mA(K) & \longrightarrow & H^1(K, A[m]) & \longrightarrow & H^1(K, A)[m] & \longrightarrow & 0 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \longrightarrow & \prod_v A(K_v)/mA(K_v) & \longrightarrow & \prod_v H^1(K_v, A[m]) & \longrightarrow & \prod_v H^1(K_v, A)[m] & \longrightarrow & 0 \end{array}$$

The *m-Selmer group* is defined to be the subgroup of classes in  $H^1(K, A[m])$  whose image in  $H^1(K_v, A[m])$  comes from  $A(K_v)/mA(K_v)$  for every  $v$ , or alternatively whose image becomes trivial in  $\prod_v H^1(K_v, A)[m]$ . Basic finiteness results in

Galois cohomology and consideration of the valuative criterion for properness relative to an abelian scheme model for  $A$  over some ring of  $S$ -integers (exactly as in the proof of the Mordell–Weil Theorem) ensures that  $\text{Sel}_m(A)$  is finite for each  $m$ .

This leads to an exact sequence

$$0 \rightarrow A(K)/mA(K) \rightarrow \text{Sel}_m(A) \rightarrow \text{III}_A[m] \rightarrow 0.$$

We get compatible such sequences as  $m$  runs over powers of a fixed prime  $p$ . Consider taking the inverse limits of these sequences. If  $\text{III}_A$  were finite, then since  $A(K)$  is finitely generated we would get

$$0 \rightarrow A(K) \otimes \mathbf{Z}_p \rightarrow \varprojlim \text{Sel}_{p^n}(A) \rightarrow \text{III}_A[p^\infty] \rightarrow 0.$$

Since  $A(K) \otimes \mathbf{Q}_p$  has dimension equal to the rank of  $A(K)$ , we expect to have

$$\dim_{\mathbf{Q}_p} \varprojlim \text{Sel}_{p^n}(A) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p = \text{rank}_{\mathbf{Z}} A(K).$$

We have almost written down a description of  $\text{rank } A(K)$  as the dimension of some cohomology group, but the definition of the Selmer group depended on a Kummer sequence for  $A$ , which depends on a group structure for  $A$ .

The Bloch–Kato Selmer group for a general Galois representation, such as arising from the  $p$ -adic étale cohomology of a variety over  $K$  (generalizing the consideration of the linear dual  $H_{\text{ét}}^1(A_{\overline{K}}, \mathbf{Q}_p)$  of  $V_p(A)$ ) will be similarly defined as a subspace of some global Galois cohomology group cut out by local conditions. However, instead of using the Kummer sequence to cut out these local conditions we will need to find another method (to replace the role of “arising from local points via a Kummer connecting map”). The punchline will be that the cohomology classes need to land in certain “local Bloch–Kato Selmer groups” for each place; defining these local groups will be our focus today.

## 2 Some local Galois cohomology

We recall some facts from local Galois cohomology. Now let  $K$  be a finite extension of  $\mathbf{Q}_\ell$  and let  $V$  be a  $p$ -adic representation of  $G_K$  (always understood to be continuous and finite-dimensional over  $\mathbf{Q}_p$ ); we allow  $\ell = p$ . We may view  $V$  as a lisse  $p$ -adic étale sheaf on  $\text{Spec}(K)$ , in terms of which  $H^i(G_K, V) = H_{\text{ét}}^i(K, V)$ ; we denote this as  $H^i(K, V)$  as usual. The following result is a more-or-less formal consequence of Tate local duality for finite Galois modules and careful bookkeeping with passage to inverse limits.

**Theorem 2.1.** *The cohomology groups  $H^i(K, V)$  satisfy the following properties:*

- (Cohomological dimension)  $H^i(G_K, V) = 0$  if  $i > 2$ .

- (Duality) There is a canonical isomorphism  $H^2(K, \mathbf{Q}_p(1)) = \mathbf{Q}_p$ , and the pairing

$$H^i(K, V) \times H^{2-i}(K, V^*(1)) \rightarrow H^2(K, \mathbf{Q}_p(1)) = \mathbf{Q}_p$$

induced by the cup product is a perfect pairing for all  $i$ .

- (Euler characteristic formula) We have

$$h^0(K, V) - h^1(K, V) + h^2(K, V) = \begin{cases} 0 & \ell \neq p, \\ [K : \mathbf{Q}_p] \cdot \dim(V) & \ell = p. \end{cases}$$

In practice this formula allows us to compute the dimensions of the Galois cohomology groups  $H^i(K, V)$ .

- If  $i > 2$ , then of course  $h^i(K, V) = 0$ .
- If  $i = 0$ , then  $h^i(K, V)$  is the multiplicity of the trivial representation as a subrepresentation, and if  $i = 2$  then by using the duality we see that  $h^2(K, V)$  is the multiplicity of  $\mathbf{Q}_p$  as a subrepresentation of  $V^*(1)$ .
- Finally, using the Euler characteristic formula we can compute  $h^1(K, V)$ : it is number of appearances of  $\mathbf{Q}_p$  as a subrepresentation of  $V$  and  $\mathbf{Q}_p$  as subrepresentation of  $V^*(1)$ , plus  $[K : \mathbf{Q}_p] \cdot \dim(V)$  if  $\ell = p$ .

*Example 2.2.* Since  $V \mapsto V^*(1)$  exchanges subs and quotients, and  $\mathbf{Q}_p$  and  $\mathbf{Q}_p(1)$ , the formula enunciated evidently implies  $\dim H^1(K, V) = \dim H^1(K, V^*(1))$ , which had better be true because they are in perfect pairing.

*Example 2.3.* The dimension of  $H^0(K, \mathbf{Q}_p(n))$  is 0 unless  $n = 0$  (in which case it is 1). The dimension of  $H^2(K, \mathbf{Q}_p(n))$  is 0 unless  $n = 0$  (in which case it is 1). This let us easily compute  $h^1(K, \mathbf{Q}_p(n))$ . For  $n \neq 0, 1$  we have

$$h^1(K, \mathbf{Q}_p(n)) = \begin{cases} 0 & \ell \neq p, \\ [K : \mathbf{Q}_p] & \ell = p. \end{cases}$$

For the exceptional cases,

$$h^1(K, \mathbf{Q}_p) = h^1(K, \mathbf{Q}_p(1)) = \begin{cases} 1 & \ell \neq p, \\ 1 + [K : \mathbf{Q}_p] & \ell = p. \end{cases}$$

Consider the map

$$K^\times \otimes_{\mathbf{Z}_p} \mathbf{Q}_p \rightarrow H^1(K, \mathbf{Q}_p(1)) \quad (2.1)$$

coming from the Kummer sequence. We have  $K^\times \simeq \mathbf{Z} \times \mathcal{O}_{K^\times}$ , and  $\mathcal{O}_{K^\times}$  is essentially isomorphic to its Lie algebra  $\mathcal{O}_K$ , so we also see that  $K^\times \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$  has rank 1 if  $\ell \neq p$  and  $1 + [K : \mathbf{Q}_p]$  if  $\ell = p$ . This reflects the fact that the map (2.1) is an isomorphism.

*Example 2.4.* If  $V = V_p(A)$  for an abelian variety  $A$ , what is  $\dim H^1(K, V)$ ? Of course  $H^0(K, V) = 0$ , as  $A(K)_{\text{tor}}$  is finite (as we see via the logarithm of this compact  $\ell$ -adic Lie group). We have  $h^2(K, V) = h^0(K, V^*(1))$ , but  $V^*(1) = V_p(\widehat{A})$ , so that vanishes for the same reason. We conclude that  $h^1(K, V)$  is equal to 0 if  $\ell \neq p$  and  $2 \dim(A) \cdot [K : \mathbf{Q}_p]$  otherwise.

### 3 Local Bloch–Kato Selmer group, $\ell \neq p$

For the rest of this section  $K$  is a finite extension of  $\mathbf{Q}_\ell$  for some prime  $\ell \neq p$ . Let  $I_K \subset G_K$  denote the inertia subgroup, and note that  $G_K/I_K \simeq \widehat{\mathbf{Z}}$  (topologically generated by Frobenius).

We want to define the local Bloch–Kato Selmer group as a subspace of  $H^1(K, V)$ . What are reasonable conditions to cut it down? If  $V$  is the (geometric) étale cohomology of a smooth proper  $K$ -scheme  $X$  then it is *unramified* whenever  $X$  has good reduction (i.e., is the generic fiber of a smooth proper  $O_K$ -scheme), by the smooth and proper base change theorems. What condition does this impose on  $H^1(K, V)$ ? By inflation-restriction for  $H^1$ , we are led to

*Definition 3.1.* For any  $p$ -adic representation  $V$  of  $G_K$ ,

$$H_{\text{ur}}^1(K, V) := H^1(G_K/I_K, V^{I_K}) = \ker(H^1(K, V) \rightarrow H^1(I_K, V)).$$

*Remark 3.2.* Here is one “concrete” interpretation of the group  $H_{\text{ur}}^1(K, V)$ . Note that the group  $H^1(K, V)$  parametrizes extensions of  $\mathbf{Q}_p$  by  $V$  and  $p$ -adic representation spaces (including continuity of the Galois action):

$$0 \rightarrow V \rightarrow W \rightarrow \mathbf{Q}_p \rightarrow 0$$

The corresponding cohomology class  $\xi$  is the image of  $1 \in H^0(K, \mathbf{Q}_p)$  in  $H^1(K, V)$  under the boundary map. Then  $\xi \in H_{\text{ur}}^1(K, \mathbf{Q}_p)$  if and only if the sequence

$$0 \rightarrow V^{I_K} \rightarrow W^{I_K} \rightarrow \mathbf{Q}_p^{I_K} = \mathbf{Q}_p \rightarrow 0$$

is exact.

Being unramified is the only reasonable “geometric condition” in the case  $\ell \neq p$ , so  $H_{\text{ur}}^1(K, V)$  is the “local Bloch–Kato Selmer group at  $\ell \neq p$ .”

*Example 3.3.* For an abelian variety  $A$  with good reduction over an  $\ell$ -adic field  $K$  and a prime  $p \neq \ell$  (so  $A[p^n]$  is unramified for all  $n > 0$  by the “easy” direction of the Néron–Ogg–Shafarevich criterion), the image of the boundary map

$$\delta : A(K)/p^n A(K) \rightarrow H^1(K, A[p^n])$$

of the Kummer sequence lands inside  $H^1(G_K/I_K, A[p^n])$ .

Indeed, this map sends a point  $x \in A(K)/p^n A(K)$  to the  $A[p^n]$ -torsor its  $p^n$ th roots inside  $A$ , and since  $A$  extends to an abelian scheme  $\mathcal{A}$  over  $O_K$  this extends

to the  $\mathcal{A}[p^n]$ -torsor  $[p^n]^{-1}(\xi) \subset \mathcal{A}$  for  $\xi \in \mathcal{A}(\mathcal{O}_K) = A(K)$  corresponding to  $x$  (valuative criterion). But  $\mathcal{A}[p^n]$  is finite étale over  $\mathcal{O}_K$  since  $[p]_{\mathcal{A}} : \mathcal{A} \rightarrow \mathcal{A}$  is finite étale (as we may check on geometric fibers over  $\text{Spec}(\mathcal{O}_K)$  since  $p \neq \ell$ ), so its torsors are finite étale over  $\mathcal{O}_K$  and thus have unramified geometric generic fiber (as a  $G_K$ -set). Thus,  $\delta(x)$  arises from  $H^1(G_K/I_K, A[p^n])$  as claimed.

Hence, if we instead begin with an abelian variety  $A$  over a *number field*  $K$  and pick a finite place  $v$  of  $K$  not over  $p$  at which  $A$  has good reduction (so  $V_p(A)$  is unramified at  $v$ ) then the composition of the global Kummer map  $A(K) \otimes_{\mathbf{Z}} \mathbf{Q}_p \rightarrow H^1(K, V_p(A))$  with the localization map  $H^1(K, V_p(A)) \rightarrow H^1(K_v, V_p(A))$  lands inside  $H_{\text{un}}^1(K_v, V_p(A))$ .

The key theme for this whole talk is to have a good understanding of dimensions. The following result gives a good interpretation of  $h_{\text{ur}}^1(K, V) := \dim H_{\text{ur}}^1(K, V)$ .

**Lemma 3.4.** *For any  $p$  and  $\ell$ , we have  $\dim H_{\text{ur}}^1(K, V) = \dim H^0(K, V)$ .*

*Proof.* We have already noted that inflation-restriction provides an isomorphism  $H^1(G_K/I_K, V^{I_K}) \simeq H_{\text{ur}}^1(K, V)$ . But  $G_K/I_K \simeq \widehat{\mathbf{Z}}$  is pro-cyclic, and it is a general fact (proved in Serre's book *Local Fields*) that  $\widehat{\mathbf{Z}}$  has cohomological dimension 1 and  $h^0(\widehat{\mathbf{Z}}, W) = h^1(\widehat{\mathbf{Z}}, W)$  for any  $p$ -adic representation  $W$  of  $\widehat{\mathbf{Z}}$  (bootstrap from the case of finite discrete  $\widehat{\mathbf{Z}}$ -modules, which amounts to the study of Herbrand quotients in the cohomology of cyclic groups), so

$$h^1(G_K/I_K, V^{I_K}) = h^0(G_K/I_K, V^{I_K}) = h^0(K, V).$$

□

*Example 3.5.* Under the isomorphism  $\widehat{K^\times} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p \simeq H^1(K, \mathbf{Q}_p(1))$  induced by the Kummer exact sequence for  $\mathbf{G}_m$ , we claim that if  $\ell \neq p$  then the respective subspaces  $\widehat{\mathcal{O}_K^\times} \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$  and  $H_{\text{ur}}^1(K, \mathbf{Q}_p(1))$  in the two sides each vanish. Indeed, for the right side we have  $h_{\text{un}}^1(K, \mathbf{Q}_p(1)) = h^0(K, \mathbf{Q}_p(1)) = 0$  and for the left side it is a simple exercise using that  $\mathcal{O}_K^\times$  is pro- $\ell$  near 1.

**Proposition 3.6.** *If  $\ell \neq p$  then the duality between  $H^1(K, V)$  and  $H^1(K, V^*(1))$  makes  $H_{\text{ur}}^1(K, V)$  and  $H_{\text{ur}}^1(K, V^*(1))$  exact annihilators of each other.*

*Proof.* First let's make sure the dimensions add up correctly. By Lemma 3.4,

$$\begin{aligned} h_{\text{ur}}^1(K, V) + h_{\text{ur}}^1(K, V) &= h^0(K, V) + h^0(K, V^*(1)) \\ &= h^0(K, V) + h^2(K, V). \end{aligned}$$

Since we are assuming that  $\ell \neq p$ , this is in fact equal to  $h^1(K, V)$ . So it suffices to show that these two spaces annihilate each other.

As discussed in the proof of Lemma 3.4, we have

$$\begin{aligned} H_{\text{ur}}^1(K, V) &\simeq H^1(G_K/I_K, V^{I_K}), \\ H_{\text{ur}}^1(K, V^*(1)) &\simeq H^1(G_K/I_K, V^*(1)^{I_K}). \end{aligned}$$

Therefore, it suffices to show that the pairing induced by cup product

$$H^1(G_K/I_K, V^{I_K}) \times H^1(G_K/I_K, V^*(1)^{I_K}) \rightarrow H^2(K, \mathbf{Q}_p(1))$$

is zero. But this pairing obviously factors through  $H^2(G_K/I_K, \mathbf{Q}_p(1))$ , which vanishes because  $G_K/I_K \simeq \widehat{\mathbf{Z}}$  has cohomological dimension 1.  $\square$

Now let's study this definition for our favorite examples to see that something reasonable happens.

*Example 3.7.* Assume  $\ell \neq p$ . We already computed in Example 2.4 that for  $V = V_p(A)$  for an abelian variety  $A$  over an  $\ell$ -adic field  $K$ , we have  $H^1(K, V) = 0$ . But here's another proof (which is not really different). We have  $H_{\text{ur}}^1(K, V) = 0$  by Lemma 3.4, so by Proposition 3.6 (using that  $\ell \neq p!$ ) we have  $H_{\text{ur}}^1(K, V^*(1)) = H^1(K, V^*(1))$ . But  $V^*(1) = V_p(\widehat{A})$ . Hence, the same argument applies to show that this is 0. Double duality for abelian varieties then does the job.

## 4 Local Bloch–Kato Selmer group, $\ell = p$

### 4.1 Digression on $p$ -adic Hodge theory

The definition of the local Bloch–Kato Selmer group(s) for  $\ell = p$  draws technical ingredients and motivation from  $p$ -adic Hodge theory, so we give a very brief summary.

Let us briefly return to the setting of a Galois representation coming from the étale cohomology of a variety  $X$  over a number field  $K$ . The standard technique to study the étale cohomology groups  $H_{\text{ét}}^i(X_{\overline{K}}, \mathbf{Q}_\ell)$  is to restrict to the “decomposition group”  $G_{K_v}$ . If  $\ell$  is distinct from the residue characteristic  $p$  at  $v$  then this representation is *unramified* when  $X_{K_v}$  is the generic fiber of a smooth proper  $O_{K_v}$ -scheme. In particular, for a fixed prime  $\ell$ ,  $H_{\text{ét}}^i(X_{\overline{K}}, \mathbf{Q}_\ell)$  is unramified for all but finitely many places  $v$  of  $K$  when  $X$  is smooth and proper over  $K$  (and the same holds for any separated  $K$ -scheme  $X$  of finite type by Deligne’s “generic base change theorem” from SGA 4.5, but that is a story for another day). What happens when  $\ell = p$ ? The story gets *much* more complicated, but in a fascinating way.

Tate discovered that the  $p$ -adic étale cohomology groups  $H_{\text{ét}}^i(X_{\overline{K}}, \mathbf{Q}_p)$  possess properties at  $v$  analogous to those dictated by classical Hodge theory for smooth proper  $\mathbf{C}$ -schemes. Recall that if  $Z$  a compact Hausdorff Kähler manifold then its singular cohomology with  $\mathbf{C}$ -coefficients admits a decomposition

$$H^n(Z, \mathbf{C}) \simeq \bigoplus_{i+j=n} H^i(Z, \Omega_Z^j). \quad (4.1)$$

Tate proved was that if  $A$  is a an abelian variety over a  $p$ -adic field  $K$  and has good reduction then we have a canonical isomorphism of *semi-linear Galois modules*

$$H_{\text{ét}}^n(A_{\overline{K}}, \mathbf{Q}_p) \otimes \mathbf{C}_K \simeq \bigoplus_{i+j=n} H^i(A, \Omega^j)_{\mathbf{C}_K}(-j) \quad (4.2)$$



where  $\mathbf{C}_K$  denotes the completion of  $\overline{K}$ . (The essential case is  $n = 1$ , since  $A$  is an abelian variety.) Fontaine realized that the correct framework for generalizing these results to general smooth proper  $K$ -schemes in place of abelian varieties involves a formalism of “period rings”. Faltings proved, in terms of Fontaine’s formalism, that a similar decomposition holds for all smooth proper  $K$ -schemes (and Scholze generalized the result to arbitrary smooth proper rigid-analytic spaces over  $K$ , far beyond the analytification of smooth proper  $K$ -schemes).

The period rings of  $p$ -adic Hodge theory are the “coefficient rings” for defining precise *comparison isomorphisms* relating the  $p$ -adic étale and algebraic de Rham cohomology of smooth proper schemes over  $p$ -adic fields. In this context elements of period rings arise as entries of a matrix relating  $p$ -adic étale and algebraic de Rham cohomology, thereby explaining the name “period ring”.

*Example 4.1.* The simplest period ring is

$$B_{HT} := \bigoplus_{n \in \mathbf{Z}} \mathbf{C}_p(n) \stackrel{\text{non-can.}}{\simeq} \mathbf{C}_p[t, t^{-1}]$$

where  $t$  is a choice of basis of  $\mathbf{Z}_p(1)$  (i.e., a compatible system  $(\zeta_{p^n})$  of primitive  $p^n$ th roots of 1 for  $n \geq 1$ ). Note that  $g(t) = \chi(g)t$  where  $\chi$  is the cyclotomic character. We have canonically  $H_{\text{ét}}^2(\mathbf{P}_K^1, \mathbf{Q}_p) = \mathbf{Q}_p(-1) = \mathbf{Q}_p \cdot t^{-1}$  and canonically  $H_{\text{dR}}^2(\mathbf{P}_K^1/K) \simeq K$  via Serre duality. There is no canonical choice of  $t$ , so we cannot expect to canonically relate the  $p$ -adic and algebraic deRham cohomologies for  $\mathbf{P}_K^1$ ; the mechanism to pass between these two cohomologies will involve a “period ring” to cancel out the appearance of  $t^{-1}$ .

There is a general definition (due to Fontaine, and explained at length in Fontaine’s first article in the *Asterisque* volume “*Periodes  $p$ -adique*”) for what constitutes a “period ring”; this involves an action by  $G_K$  on  $B$  such that  $B^{G_K}$  is a field and some further properties hold to ensure that if  $V$  is any  $p$ -adic representation of  $G_K$  then  $(V \otimes_{\mathbf{Q}_p} B)^{G_K}$  is finite-dimensional over  $B^{G_K}$  and the natural map

$$B \otimes_{B^{G_K}} (V \otimes_{\mathbf{Q}_p} B)^{G_K} \rightarrow B \otimes_{\mathbf{Q}_p} V \tag{4.3}$$

is *injective* and

$$\dim_{B^{G_K}} (V \otimes_{\mathbf{Q}_p} B)^{G_K} \leq \dim_{\mathbf{Q}_p} V.$$

*Definition 4.2.* For any period ring  $B$ , let

$$D_B(V) = (V \otimes B)^{G_K}.$$

A  $p$ -adic representation  $V$  for  $G_K$  is *admissible with respect to  $B$*  if the inequality

$$\dim_{B^{G_K}} (V \otimes_{\mathbf{Q}_p} B)^{G_K} \leq \dim_{\mathbf{Q}_p} V$$

is an equality (in which case (4.3) is always an isomorphism).

Since  $D_B(V) = \text{Hom}_{G_K}(V^*, B)$ , we refer to the images in  $B$  of such  $G_K$ -equivariant homomorphisms as “periods of  $V^*$  and  $B$ -admissibility says that  $V^*$  has “enough  $p$ -adic periods”. The formalism ensures that  $V$  is  $B$ -admissible if and only if  $V^*$  is so.

*Remark 4.3.* If  $V$  is  $B$ -admissible then the periods for  $V^*$  are the  $B^{G_K}$ -linear combinations of the entries of the matrix for the natural  $G_K$ -equivariant  $B$ -linear isomorphism

$$B \otimes_{B^{G_K}} D_B(V) \simeq B \otimes_{\mathbf{Q}_p} V$$

with respect to fixed ordered bases for  $D_B(V)$  over  $B^{G_K}$  and for  $V$  over  $\mathbf{Q}_p$  respectively. This explains the use of the word “period” since for  $V = H_{\text{ét}}^n(X_{\overline{K}}, \mathbf{Q}_p)$  with a smooth proper  $K$ -scheme  $X$  it turns out that canonically  $D_B(V) \simeq H_{\text{dR}}^n(X/K)$  when  $B$  is the “deRham period ring” (and then  $B^{G_K} = K$ , with the above isomorphism under such a canonical identification of  $D_B(V)$  called the *deRham comparison isomorphism* for  $p$ -adic étale cohomology). Even the weaker property that  $\dim_K H_{\text{dR}}^n(X/K) = \dim_{\mathbf{Q}_p} H_{\text{ét}}^n(X_{\overline{K}}, \mathbf{Q}_p)$  is not at all obvious!

Fontaine constructed period rings (1)  $B_{\text{dR}}$ , (2)  $B_{\text{crys}}$ , and (3)  $B_{\text{st}}$  which are respectively the period rings for

1. smooth proper  $K$ -schemes,
2. generic fibers of smooth proper  $O_K$ -schemes,
3. smooth proper  $K$ -schemes admitting a semistable proper flat  $O_K$ -model.

In particular,  $B_{\text{crys}} \subset B_{\text{st}} \subset B_{\text{dR}}$  (although the last embedding is not canonical).

We say that a representation is (1) de Rham (2) crystalline (3) semistable if it is admissible for (1)  $B_{\text{dR}}$ , (2)  $B_{\text{crys}}$ , (3)  $B_{\text{st}}$ . What the above means is that if  $X$  is smooth proper  $K$ -scheme then  $H_{\text{ét}}^i(X_{\overline{K}}, \mathbf{Q}_p)$  is de Rham, if  $X$  furthermore has semistable reduction then  $H_{\text{ét}}^i(X_{\overline{K}}, \mathbf{Q}_p)$  is semistable, and if  $X$  furthermore has good reduction then  $H_{\text{ét}}^i(X_{\overline{K}}, \mathbf{Q}_p)$  is crystalline. In addition, the proofs of these deep results identify  $D_B(H_{\text{ét}}^n(X_{\overline{K}}, \mathbf{Q}_p))$  with a cohomology of  $X$  directly defined using sheaves of differential forms.

*Remark 4.4.* Strictly speaking, these rings contains periods for cohomology of other geometric objects, such as  $p$ -divisible groups over  $O_K$  and smooth proper rigid-analytic spaces over  $K$ .

We’re going to need the period rings  $B_{\text{dR}}$  and  $B_{\text{crys}}$ . The explicit constructions of  $B_{\text{dR}}$  and  $B_{\text{crys}}$  are too complicated to explain here. For our purposes, we will just explain their fundamental properties.

The ring  $B_{\text{dR}}$  has a *filtration* coming from its structure as a discretely valued field. The valuation subring is  $B_{\text{dR}}^+ := \text{Fil}^0 B_{\text{dR}}$ . The associated graded ring turns out to be the *Hodge–Tate period ring*

$$B_{HT} = \bigoplus_{n \in \mathbf{Z}} \mathbf{C}_K(n).$$

This implies that any representation which is de Rham is automatically Hodge–Tate, since

$$\dim_K(V \otimes B_{\mathrm{dR}})^{G_K} \leq \dim_K(V \otimes B_{\mathrm{HT}})^{G_K}.$$

This induces a filtration on  $D_{\mathrm{dR}}(V)$ , and the integers at which it jumps (with multiplicity) are called the *Hodge–Tate weights*.

*Example 4.5.* For a de Rham (or even Hodge–Tate) representation, a more intuitive definition of Hodge–Tate weight is that if

$$V \otimes \mathbf{C}_K \simeq \bigoplus \mathbf{C}_K(-j) \otimes_K V_j$$

where  $V_j := \mathrm{Hom}_{G_K}(\mathbf{C}_K(-j), V \otimes \mathbf{C}_K)$  is the associated  $j$ th “multiplicity space”, then the Hodge–Tate weights are  $j$  with multiplicity  $\dim_K V_j$ .

The Hodge–Tate weight of  $\mathbf{Q}_p(n)$  is  $-n$ . From Tate’s decomposition (4.2), the Hodge–Tate weights of  $H_{\mathrm{\acute{e}t}}^1(A_{\overline{K}}, \mathbf{Q}_p)$  for an abelian variety  $A$  over  $K$  with good reduction are 0 with multiplicity  $g$  and 1 with multiplicity  $g$ ; those of the dual  $V_p(A)$  are the negations. (The “good reduction” hypothesis can be dropped, but that requires methods going beyond those of Tate.)

The ring  $B_{\mathrm{crys}}$  has a  $G_K$ -equivariant *Frobenius endomorphism*  $\phi$  inspired by the crystalline–deRham comparison isomorphism for smooth proper  $O_K$ -schemes. There is also a canonical filtration inherited from  $B_{\mathrm{dR}}$  (inspired by the Hodge filtration on algebraic deRham cohomology), but there is no extra compatibility demanded between  $\phi$  on  $B_{\mathrm{crys}}$  and this filtration on the extension ring  $B_{\mathrm{dR}}$ .

Informally, the crystalline condition is the  $p$ -adic analogue of the notion of unramifiedness for  $\ell$ -adic representations of  $G_K$  for  $p$ -adic fields  $K$  when  $\ell \neq p$  (unramifiedness is much too restrictive to be useful in the study of  $p$ -adic representations arising from algebraic geometry over  $p$ -adic fields).

The deRham condition turns out (by deep results) to be equivalent to a “potentially semistable” property, inspired by the dream that smooth proper  $K$ -schemes should have “potentially semistable reduction” (proved in a useful weaker form in deJong’s work on alternations). For  $\ell \neq p$ , the analogous property is Grothendieck’s elementary result in the appendix to the Serre–Tate paper “Good reduction of abelian varieties” that every  $\ell$ -adic representation of the Galois group of a  $p$ -adic field  $K$  with  $p \neq \ell$  is unipotent on an open subgroup of  $I_K$ .

To summarize, here is a panorama of the important classes of  $p$ -adic representations and their properties.

Property	Period Ring	Structure	$\ell$ -adic analogue
Hodge–Tate	$B_{\mathrm{HT}}$	Hodge–Tate weights	N/A
de Rham	$B_{\mathrm{dR}}$	Filtration	pot. unipotent on inertia
Crystalline	$B_{\mathrm{crys}}$	Frobenius $\phi$	unramified

## 4.2 The local BK Selmer group

Now let  $K$  be a finite extension of  $\mathbf{Q}_p$  and  $V$  a  $p$ -adic representation of  $G_K$ . We are looking for a subspace  $L \subset H^1(K, V)$  which is analogous to  $H_{\text{ur}}^1(K, W)$  when  $W$  is an  $\ell$ -adic representation with  $\ell \neq p$ . By analogy with the  $\ell$ -adic situation, we seek a definition that provides an exact annihilator with respect to  $V \mapsto V^*(1)$ .

*Example 4.6.* The subspace  $H_{\text{ur}}^1(G_K, V)$  doesn't work, since by Lemma 3.4 and the Euler characteristic formula we have

$$\begin{aligned} h_{\text{ur}}^1(K, V) + h_{\text{ur}}^1(K, V^*(1)) &= h^0(K, V) + h^0(K, V^*(1)) \\ &= h^1(K, V) - [K : \mathbf{Q}_p] \dim V \\ &< h^1(K, V) \end{aligned}$$

whenever  $V \neq 0$ .

*Definition 4.7.* We define

$$H_f^1(G_K, V) = \ker (H^1(K, V) \rightarrow H^1(K, V \otimes_{\mathbf{Q}_p} B_{\text{crys}})).$$

*Remark 4.8.* As one sanity check, we have an analogue of Remark 3.2: a class  $\xi \in H^1(K, V)$  corresponds to an extension

$$0 \rightarrow V \rightarrow W \rightarrow \mathbf{Q}_p \rightarrow 0,$$

and  $\xi \in H_f^1(K, V)$  if and only if the sequence

$$0 \rightarrow D_{\text{crys}}(V) \rightarrow D_{\text{crys}}(W) \rightarrow D_{\text{crys}}(\mathbf{Q}_p) \rightarrow 0$$

is exact.

The ring  $B_{\text{dR}}$  is a discretely valued field with valuation ring  $B_{\text{dR}}^+$  (often called  $B_{\text{dR}}^0$ ). This inherits a filtration and its associated graded ring is  $B_{\text{HT}}$ , so it contains the integral powers of any basis  $t$  of  $\mathbf{Q}_p(1)$ .

**Proposition 4.9** (First fundamental exact sequence). *There is an exact sequence of  $G_K$ -modules*

$$0 \rightarrow \mathbf{Q}_p \xrightarrow{\alpha} B_{\text{crys}} \oplus B_{\text{dR}}^+ \xrightarrow{\beta} B_{\text{crys}} \oplus B_{\text{dR}} \rightarrow 0$$

where  $\alpha(x) = (x, x)$  and  $\beta(y, z) = (y - \phi(y), y - z)$ .

Given that I didn't even define the rings  $B_{\text{crys}}$  and  $B_{\text{dR}}$ , let's just accept this exact sequence as a black box.

**Proposition 4.10.** *If  $V$  is de Rham, then we have*

$$\dim_{\mathbf{Q}_p} H_f^1(K, V) = \dim_{\mathbf{Q}_p} (D_{\text{dR}}(V)/D_{\text{dR}}^+(V)) + \dim_{\mathbf{Q}_p} H^0(K, V). \quad (4.4)$$



counts (with multiplicities) the number of non-positive weights plus the number of negative weights of  $V$ , hence also equals  $\dim_{\mathbf{Q}_p} V$ . By dimension considerations, the desired surjectivity follows.  $\square$

*Example 4.12.* A variant of the same argument shows that if  $V$  is de Rham, then  $\dim_K D_{\text{dR}}^+(V) + \dim_K D_{\text{dR}}^+(V^*(1)) = \dim_{\mathbf{Q}_p} V$ .

Put another way,  $\dim H_f^1(G_K, V)$  is the sum of the multiplicity of the trivial representation in  $V$  and  $[K : \mathbf{Q}_p]$  times the number of negative Hodge–Tate weights of  $V$  (since  $\mathbf{Q}_p(n)$  has Hodge–Tate weight  $-n$ ).

*Example 4.13.* Recall that  $h^1(K, V) = h^0(K, V^*(1)) + [K : \mathbf{Q}_p] \dim(V)$ . Thus, if  $V$  is de Rham with all Hodge–Tate weights  $\leq -2$  (so  $h^0(K, V^*(1)) = 0$ ), then  $H_f^1(K, V) = H^1(K, V)$  by equality of dimensions.

*Example 4.14.* We have  $h_f^1(K, \mathbf{Q}_p(n)) = 0$  if  $n < 0$ , 1 if  $n = 0$ , and  $[K : \mathbf{Q}_p]$  if  $n \geq 1$ .

In particular, the only interesting inclusions occur for  $n = 0$  and  $n = 1$ . For  $n = 0$ , we have the inclusion of a line

$$H_f^1(K, \mathbf{Q}_p) \subset H^1(K, \mathbf{Q}_p) = \text{Hom}_{\text{cont}}(K^\times, \mathbf{Q}_p)$$

in an ambient space of dimension  $[K : \mathbf{Q}_p] + 1$ . We claim that it is generated by the valuation  $x \mapsto v_p(x)$ . The reason is that this corresponds to the *unramified* extension, and unramified implies crystalline.

**Theorem 4.15.** *Let  $V$  be de Rham. Then under the duality between  $H^1(K, V)$  and  $H^1(K, V^*(1))$  the subspaces  $H_f^1(K, V)$  and  $H_f^1(K, V^*(1))$  are mutual orthogonal.*

*Proof.* As usual, let's first do the dimension count. We have that

$$h_f^1(K, V) = h^0(K, V) + [K : \mathbf{Q}_p](\# \text{ negative Hodge–Tate weights})$$

while

$$\begin{aligned} h_f^1(K, V^*(1)) &= h^0(K, V^*(1)) + [K : \mathbf{Q}_p](\# \text{ negative HT weights of } V^*(1)) \\ &= h^0(K, V^*(1)) + [K : \mathbf{Q}_p](\# \text{ non-negative HT weights of } V) \end{aligned}$$

So in total we find that the sum of their dimensions is

$$h^0(K, V) + h^0(K, V^*(1)) + [K : \mathbf{Q}_p](\# \text{ Hodge–Tate weights})$$

but  $\#$  Hodge–Tate weights is  $\dim_{\mathbf{Q}_p} V$  since  $V$  is de Rham, and that gives exactly the description of  $h^1(K, V)$  furnished by the local Euler characteristic formula.

Now it suffices to show that the pairing

$$H_f^1(K, V) \times H_f^1(K, V^*(1)) \rightarrow H^2(K, \mathbf{Q}_p(1)) = \mathbf{Q}_p$$

vanishes identically.

Fix  $y \in H_f^1(K, V^*(1))$ , so it suffices to show that the cup product map

$$(\cdot) \cup y : H_f^1(K, V) \rightarrow H^2(K, V \otimes V^*(1))$$

vanishes. Tensoring the first fundamental exact sequence (4.4) against  $V$ , any  $x \in H_f^1(K, V)$  arises from a class

$$x' \in H^0(K, (B_{\text{crys}} \otimes V) \oplus (B_{\text{dR}} \otimes V)),$$

so by the compatibility of cup products and connecting maps in low-degree  $G_K$ -cohomology it follows that  $x \cup y$  is in the image of

$$x' \cup y \in H^1(K, (B_{\text{crys}} \otimes V \otimes V^*(1)) \oplus (B_{\text{dR}} \otimes V \otimes V^*(1)))$$

under the connecting map from tensoring  $V \otimes V^*(1)$  against the first fundamental exact sequence. Thus, it suffices to show that  $x' \cup y = 0$ .

But  $x' \cup y$  clearly only depends on the image of  $y$  in

$$H^1(K, (B_{\text{crys}} \otimes V^*(1)) \oplus (B_{\text{dR}} \otimes V^*(1))),$$

and that image vanishes by the analysis of  $\alpha^1$  in the proof of Proposition 4.10 (applied to  $V^*(1)$ , which inherits the deRham property of  $V!$ ).  $\square$

Let's now analyze our favorite examples.

**Proposition 4.16.** *The Kummer map  $\widehat{K}^\times \otimes_{\mathbf{Z}_p} \mathbf{Q}_p \rightarrow H^1(K, \mathbf{Q}_p(1))$  identifies  $\mathcal{O}_K^\times \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$  with  $H_f^1(K, \mathbf{Q}_p(1))$ .*

*Proof.* As usual, let's start by counting dimensions. Since  $\mathcal{O}_K^\times$  is a compact  $p$ -adic Lie group of dimension  $[K : \mathbf{Q}_p]$  (via the  $p$ -adic logarithm), we have

$$\dim_{\mathbf{Q}_p} \mathcal{O}_K^\times \otimes_{\mathbf{Z}_p} \mathbf{Q}_p = [K : \mathbf{Q}_p].$$

On the other hand, we computed in Example 4.14 that  $h_f^1(K, \mathbf{Q}_p(1)) = [K : \mathbf{Q}_p]$  as well. That means it suffices to show that  $\mathcal{O}_K^\times \otimes_{\mathbf{Z}_p} \mathbf{Q}_p$  lands in  $H_f^1(K, \mathbf{Q}_p(1))$ .

To see this inclusion, it is useful to use the perspective of  $H_f^1(K, V)$  as extensions

$$0 \rightarrow V \rightarrow W \rightarrow \mathbf{Q}_p \rightarrow 0$$

of  $p$ -adic  $G_K$ -representations with  $W$  crystalline (Remark 4.8). Thus, it suffices to prove that for any  $u \in \mathcal{O}_K^\times$ , the Kummer class

$$\delta(u) \in H^1(K, \mathbf{Q}_p(1)) = \text{Ext}_{G_K}^1(\mathbf{Q}_p, \mathbf{Q}_p(1))$$

viewed as a 2-dimensional  $p$ -adic representation of  $G_K$  ( $\mathbf{Q}_p$ -linear extension of  $\mathbf{Q}_p$  by  $\mathbf{Q}_p(1)$ ) is a crystalline representation.

Unraveling Kummer-theoretic constructions, this extension class is  $V_p(E)$  where  $E = \overline{K}^\times / u^{\mathbf{Z}}$  (a fake version of a Tate curve using the parameter  $u$  with  $|u|_K = 1$ ). This coincides with  $V_p(\mathcal{E}_K)$  where  $\mathcal{E} = (\mathcal{E}_n)$  is the  $p$ -divisible group over  $O_K$  whose  $p^n$ -torsion layer  $\mathcal{E}_n$  is the finite flat  $O_K$ -group scheme arising from the base change along

$$u : \mathrm{Spec}(O_K) \rightarrow \mathrm{Spec}(\mathbf{Z}[q, 1/q])$$

of the Katz–Mazur group scheme  $T_{p^n}$  over  $\mathbf{Z}[q, 1/q]$  that is the  $p^n$ -torsion of “ $\mathbf{G}_m/q^{\mathbf{Z}}$ ”. (These are analyzed very directly in §8.7 of the book *Arithmetic moduli of elliptic curves* by Katz and Mazur.) It is a (non-trivial) theorem of Fontaine that for any  $p$ -divisible group  $\Gamma$  over  $O_K$ ,  $V_p(\Gamma_K)$  is crystalline!  $\square$

**Proposition 4.17.** *Let  $A$  be an abelian variety over  $K$ . Then the image of the injective Kummer map*

$$\delta : A(K) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p \rightarrow H^1(K, V_p(A))$$

is  $H_f^1(K, V_p(A))$ .

Note that there is *no* good-reduction hypothesis on  $A$ . The injectivity of the Kummer map uses that the compact  $p$ -adic Lie group  $A(K)$  has a pro- $p$  neighborhood of 0 that is a finite free  $\mathbf{Z}_p$ -module, so the  $p$ -adic completion of  $A(K)$  is identified with an open subgroup of  $A(K)$ .

*Proof.* We again count dimensions. The logarithm map defines an isomorphism between an open finite-index subgroup of the compact  $p$ -adic Lie group  $A(K)$  and an open subgroup of its Lie algebra (which naturally coincides with  $\mathrm{Lie}(A)$ ), so

$$\dim_{\mathbf{Q}_p}(A(K) \otimes_{\mathbf{Z}_p} \mathbf{Q}_p) = [K : \mathbf{Q}_p]g.$$

On the other hand, since  $V_p(A)$  is deRham (being linear dual to  $H^1(A_{\overline{K}}, \mathbf{Q}_p)$ ), and in general each  $H^j(X_{\overline{K}}, \mathbf{Q}_p)$  is deRham for any smooth proper  $K$ -scheme  $X$ , or in the good reduction case it is crystalline by Fontaine’s theorem on Galois representations arising from  $p$ -divisible groups over  $O_K$ ) and it has Hodge–Tate weights 0 (with multiplicity  $g$ ) and  $-1$  (with multiplicity  $g$ ), we have  $\dim H_f^1(K, V_p(A)) = [K : \mathbf{Q}_p]g$  by Example 4.10.

Now it suffices to show that for any  $u \in A(K)$ , the Kummer class  $\delta(u)$  lies in  $H_f^1(K, V_p(A))$ . We will prove this only when  $A$  has good reduction, as then one can get by using  $p$ -divisible groups over  $O_K$  (and Fontaine’s hard theorem that the  $p$ -adic representations arising from the generic fiber of any such  $p$ -divisible group is crystalline).

Let  $\mathcal{A}$  be the abelian scheme over  $O_K$  with generic fiber  $A$ , so  $u \in A(K) = \mathcal{A}(O_K)$ . The pullback along  $u$  of the short exact sequence

$$0 \rightarrow \mathcal{A}[p^n] \rightarrow \mathcal{A} \xrightarrow{p^n} \mathcal{A} \rightarrow 0$$



for the fppf topology is an  $\mathcal{A}[p^n]$ -torsor  $\mathcal{T}_n$  over  $O_K$  for the fppf topology. By arguing in terms of fppf group sheaves and descent theory, for any finite flat  $O_K$ -group scheme  $G$  killed by an integer  $N$  every fppf  $G$ -torsor  $T$  over  $O_K$  arises from a *canonically* associated short exact sequence of  $N$ -torsion commutative finite flat  $O_K$ -groups

$$0 \rightarrow G \rightarrow E_T \rightarrow \mathbf{Z}/N\mathbf{Z} \rightarrow 0.$$

Naturally  $\mathcal{T}_{n+1}/\mathcal{A}[p] \simeq \mathcal{T}_n$  as torsors over  $\mathcal{A}[p^{n+1}]/\mathcal{A}[p] = \mathcal{A}[p^n]$ . Hence, by the *canonicity* of the construction of  $E_T$  from  $T$  (naturally in  $G$ ), there are compatible short exact sequences

$$0 \rightarrow \mathcal{A}[p^n] \rightarrow E_{\mathcal{T}_n} \rightarrow \mathbf{Z}/(p^n) \rightarrow 0$$

for  $n \geq 1$ , so  $E = (E_{\mathcal{T}_n})$  constitutes a  $p$ -divisible group over  $O_K$  (an extension of  $\mathbf{Q}_p/\mathbf{Z}_p$  by  $\mathcal{A}[p^\infty]$ ). By design,  $V_p(E_K) = \delta(u)$  as extensions of  $V_p(\mathbf{Q}_p/\mathbf{Z}_p) = \mathbf{Q}_p$  by  $V_p(\mathcal{A}[p^\infty]) = V_p(A)$ , so the same theorem of Fontaine ensures that this is a crystalline  $p$ -adic representation.  $\square$