AN INTRODUCTORY LECTURE ON WC-GROUPS

1. The two definitions of a WC-group

Let k be a field[1] and let A be an abelian variety defined over k, i.e., a projective nonsingular, geometrically connected group variety defined over the field k. In particular, an elliptic curve is an abelian variety of dimension one.

Definition: The **Weil-Chatelet group** $WC(A/k)$ of an abelian variety is an abelian group whose elements are equivalence classes of principal homogeneous spaces for $A_{/k}$. This means that we are given a k-variety V together with a k-morphism $\mu : A \times V \to V$ such that

$$\mu(\overline{k}) : A(\overline{k}) \times V(\overline{k}) \to V(\overline{k})$$

is a simply transitive group action in the usual sense.

Suppose P is a point of V which is rational over some field extension l. Then the map $\varphi_P = \mu(-, P) : A_{/l} \to V_{/l}$ is an l-rational morphism which gives a bijection on geometric points, so it is an isomorphism $A_{/l} \to V_{/l}$. Moreover, viewing A as a principal homogeneous space over itself, φ_P is equivariant with respect to the two actions of A, i.e., (V, μ) is isomorphic to $(A, +)$ as a principal homogeneous space. Such a principal homogeneous space is called **trivial**.

Given two principal homogeneous spaces (V_i, μ_i), we can form a third space, as follows: we define an action $\mu_{+,-}$ of A on $V_1 \times V_2$, by $\mu_{+,-}(a, p_1 \times p_2) = \mu_1(a, p_1) \times \mu_2([-1]a, p_2)$, where $[-1]$ denotes inversion on the abelian variety A. We also have the more obvious diagonal action $\mu_{+,+}$ of A on $V_1 \times V_2$, and this action descends to the quotient $V_1 \times V_2/\mu_{+,-}$ and endows it with the structure of a principal homogeneous space, called the Baer sum $V_1 + V_2$ of V_1 and V_2.

Exercise 1: Show that the Baer sum gives a group law on the set of equivalence classes of principal homogeneous spaces for $A_{/k}$, in which the inverse of (V, μ) is $(V, \mu([-1] \circ -, -))$.

Exercise 2:
a) Show that the Baer sum V_3 of V_1 and V_2 has the property that there exists a morphism $\varphi : V_1 \times V_2 \to V$ with the property that

$$\varphi(\mu_1(a_1, p_1), \mu_2(a_2, p_2)) = \mu_3(a_1 + a_2, \varphi(p_1, p_2))$$

for all $a_i \in A(\overline{k})$, $p_i \in V_i(\overline{k})$, and that this property characterizes V_3 uniquely as a phs for A.
b) Use part a) to show that for all $n \in \mathbb{Z}$, $\mathbf{Alb}^n(V)$ represents the element $n[V] \in WC(k, A)$.

[1]Let us assume that k is perfect, mostly so as not to have to use a separate notation for the separable closure. We will denote $\overline{k}$ by a choice of algebraic closure of k.

This gives our first definition of the Weil-Chatelet group.

It follows from the above discussion that any nonzero element of $WC(k, A))$ is represented by (V, μ) with $V(k) = \emptyset$. In particular, when $A = E$ is an elliptic curve, the underlying variety of a nontrivial element of $WC(k, E)$ is a genus one curve without k-rational points.

Note that this construction is functorial in k: if $k \hookrightarrow l$ is a field embedding, then just by extending the base of a principal homogeneous space defined over k to a principal homogeneous space defined over l, we get a homomorphism of groups

$$r_{l/k} : WC(k, A) \to WC(l, A).$$

Let us define the kernel of this map as $WC(l/k, A)$. This is the subgroup of phs's $(V, \mu)_{/k}$ such that $V(l) \neq \emptyset$. For an abelian variety $A_{/k}$, one would like to compute not just $WC(k, A)$ but $WC(l, A)$ for all finite extensions l/k and the restriction maps $r_{l/k}$, and especially their kernels. I (and only I) refer to this as the **WCA problem**.

Remark: Notice that the construction goes through verbatim with A replaced by any commutative algebraic group.

2. Can we forget about the μ?

Let us now admit that it is somewhat unnatural that our WC-groups classify varieties together with a principal homogeneous space structure: it is arguably more natural to classify algebraic varieties $V_{/k}$ such that $V_{/\overline{k}} \cong A_{/\overline{k}}$. This raises two natural questions:

(Q1) If $V_{/k}$ is any variety which becomes isomorphic to $A_{/k}$ over the algebraic closure, can V be endowed with the structure of a phs over A?
(Q2) If so, is the resulting phs structure unique up to isomorphism?

The answer to both questions is "No, but..."

If $V_{/k}$ becomes isomorphic to an abelian variety over the algebraic closure, then it is canonically isomorphic to its own Albanese torsor $\mathbf{Alb}^1(V)$ (the parameter space of zero-cycles of degree one on V modulo a certain equivalence relation), which is a principal homogeneous space of the abelian variety $A' = \mathbf{Alb}^0(V)$, in an obvious way: given a zero-cycle of degree 0 and a zero-cycle of degree 1, we can just add them to get another zero-cycle of degree 1! The slight catch is that comparing A and A', we can say precisely that they are two abelian varieties defined over k which become isomorphic over $\overline{k}$. This usually does not imply that $A \cong A'$ (more on this later).

But this is fine: we still get that every variety which is a twisted form of an abelian variety is a principal homogeneous space of its Albanese variety. In particular, every curve of genus one is canonically a principal homogeneous space of its Jacobian $J(E) = \mathrm{Alb}^0(C) = \mathrm{Pic}^0(C)$.

Similarly, if (V, μ) is a principal homogeneous space over A, then the subtraction map ν induces an isomorphism $\mathrm{Alb}^0(V) \xrightarrow{\sim} A$. Thus:

Exercise 3: For an abelian variety A and a principal homogeneous space (V, μ) of A, the elements $(W, \mu_W$ of $WC(k, A)$ with $V \cong W$ as an algebraic variety form a single orbit under the action of $\mathrm{Aut}(A)$.

For instance, if $E_{/k}$ is an elliptic curve with j-invariant not 0 or 1728, then $\mathrm{Aut}(E) = \pm 1$, so that the set of isomorphism classes of genus one curves $C_{/k}$ whose Jacobian is isomorphic to E is $WC(k, E)/\pm 1$.

Exercise 4 (Poonen): Let V be a principal homogeneous space of $A = \mathrm{Alb}^0(V)$, with function field $k(V)$. Like any irreducible algebraic variety, V has a $k(V)$-rational point, i.e., the class of V lies in $WC(k(V)/k, A)$. Let M be the $\mathbb{Z}[\mathrm{Aut}(A)]$-submodule of $WC(k, A)$ generated by V.[2] Show that $M = WC(k(V)/k, A)$. (Hint: the containment $\subset$ is easy. For the converse, note that a $k(V)$-rational point on a principal homogeneous space W is equivalent to a rational map from V into W. Since over the algebraic closure, this is a map from a complete variety into an abelian variety, it is a morphism. Now show that if $V \to W$ is a morphism of phs's of a common abelian variety A, then $W \in M$.)

3. Connections with Galois cohomology

For A an abelian variety defined over k, $A(\overline{k})$ is naturally a $\mathfrak{g}_k = \mathrm{Gal}(\overline{k}/k)$-module, so we have the Galois cohomology groups $H^i(k, A) := H^i(\mathfrak{g}_k, A(\overline{k}))$.

For the topologists, recall that Galois cohomology is very nearly group cohomology where the group is $\mathfrak{g}_k$, but not quite: we need to use the structure of $\mathfrak{g}_k$ as a profinite group, i.e., as an inverse limit of Galois groups of finite Galois extensions $\mathfrak{g}(l/k)$. We can then define $H^i(\mathfrak{g}_k, A(\overline{k})) = \varinjlim_l H^i(\mathfrak{g}(l/l), A(l))$, or as the cohomology of $\mathfrak{g}_k$ as a topological group – i.e., continuous cochains modulo continuous coboundaries (and these are equivalent definitions).

Theorem 1. *There is a canonical isomorphism $H^1(k, A) \cong WC(k, A)$.*

Proof: Indeed, more is true: for any Galois extension l/k, we have $H^1(l/k, A) \cong WC(l/k, A)$. First, note that although we cannot add points on a phs V, we can subtract them: there is a natural map $\nu : V \times V \to A$ characterized by $\nu(v_1, v_2) = a \iff a + v_2 = v_1$. Now if V is a phs with an l-rational point P, then $a_\sigma := \sigma(P) - P$ gives a one-cycle with coefficients in $A(l)$. Moreover, the different choices of $P \in V(l)$ correspond exactly to the set of all elements of $Z^1(l/k, A)$ cohomologous to a_σ. If V and V' are isomorphic as phs's, then choosing points P and P' which correspond under the isomorphism, we get the same cocycle a_σ. Similarly, if V and V' give rise to cohomologous cocycles, we can choose $P \in V$ and $P' \in V'$ such that the cocycles are equal. Then the map $v \mapsto (v - P) + P'$ gives an isomorphism of V onto V', *a priori* defined over l, but easily seen to be $\mathfrak{g}(l/k)$-invariant, so defined over k. Thus we have defined an injective map $\Phi : WC(l/k, A) \to H^1(l/k, A)$.
The converse goes as follows: given cocycle $a_\sigma \in H^1(l/k, A)$, we can define $f_\sigma : A_{/l} \to A_{/l}$ by addition of a_σ. That a_σ is a cocycle is equivalent to the identity $f_\sigma \circ \sigma(f_\tau) = f_{\sigma\tau}$, and we appeal to Weil's descent conditions.

The isomorphism of the previous theorem respects the group structures, and is such

[2]For most abelian varieties A, $\mathrm{Aut}(A) = \pm 1$, so $M = \langle V \rangle$.

that for an algebraic field extension l/k, the geometric restriction map $WC(k,A)$ becomes the usual cohomological restriction map corresponding to $\mathfrak{g}_l \hookrightarrow \mathfrak{g}_k$. In other words, the exact sequence

$$0 \to WC(l/k,A) \to H^1(k,A) \to H^1(l,A)$$

is the usual inflation-restriction sequence in Galois (or group) cohomology.

Remark: This is a special case of a much more general principal of descent: namely, let V be an "object" defined over k, and let $\mathrm{Aut}(V)$ be the automorphism group of $V_{\overline{k}}$ (which is a not-necessarily commutative $\mathfrak{g}_k$-module). Then the set of $\overline{k}/k$-twisted forms of V – namely, those objects $W_{/k}$ which upon basechange to $\overline{k}$ become isomorphic to V, are parameterized by $H^1(\mathfrak{g}_k, \mathrm{Aut}(V))$. If $\mathrm{Aut}(V)$ is noncommutative, this is in general a pointed set (the distinguished point being given by V itself), but in our case, we are requiring V to be isomorphic to A as a phs, so the relevant automorphism group is A itself. As another example, $H^1(k, \mathrm{Aut}((A,0)))$ gives the abelian varieties $A'_{/k}$ which are isomorphic to A over the algebraic closure. Again, when $A = E$ is an elliptic curve with j-invariant not 0 or 1728, then $\mathrm{Aut}((E,0)) = \pm 1$, and $H^1(k, \pm 1) = k^\times/k^{\times 2}$, and we recover the notion of quadratic twists.[3]

Remark: This descent principle is (of course?) valid in much more generality, e.g. for sheaves of groups in many a Grothendieck topology. For instance, on a (paracompact, I suppose) topological space X, if G is a topological group, and $\underline{G}$ is the sheaf of continuous (or smooth, or holomorphic, or locally constant ...) G-valued functions on X, this principle tells us that fiber bundles with structure group G can be given by transition functions, with equivalence taking place in the Cech cohomology group $H^1(X, \underline{G})$.

4. Elementary examples of WC-groups

In this section we will see what can be said about WC-groups using only "general knowledge" together with one tool, the all-important Kummer sequence: for any positive integer n, we have a short exact sequence of Galois modules

$$0 \to A[n] \to A(\overline{k}) \xrightarrow{n} A(\overline{k}) \to 0.$$

Technical remark: Here we are defining $A[n]$ to be the Galois module $A[n]$. When the characteristic of k divides n, this group has cardinality smaller than n^{2g}, which seems to indicate that it is the wrong definition of $A[n]$ (rather we learn that we should take $A[n]$ to be the scheme-theoretic kernel of $[n]$, which is a finite flat group scheme of order n^{2g}). Nevertheless, this "naive" $A[n]$ will give the right answers in characteristic dividing n in the following discussion (unless I have made some terrible mistake).

Anyway, taking $\mathfrak{g}_k$-cohomology, we get the **Kummer sequence**:

$$0 \to A(k)/nA(k) \to H^1(k, A[n]) \to H^1(k,A)[n] \to 0. \tag{1}$$

[3]Note that by convention, when one speaks of automorphisms of an abelian variety, one invariably means automorphisms fixing the origin, whereas the automorphism group of the underlying algebraic variety is the semidirect product of A with $\mathrm{Aut}(A,0)$.

Remark: The Kummer sequence is valid with A replaced by any commutative algebraic group G in which $[n]$ is surjective on geometric points (e.g. any connected commutative group). Indeed, the classical case is $G = \mathbb{G}_m$; in conjunction with Hilbert 90 – $H^1(k, \mathbb{G}_m) = 0$ – we get $H^1(k, \mu_n) = k^\times / k^{\times n}$.

Let us just sit back and stare at this sequence for a moment. The middle term $H^1(k, A[n])$ is Galois cohomology with coefficients in a finite Galois module with underlying abelian group $(\mathbb{Z}/n\mathbb{Z})^a$, for some $a \leq 2g$ (with equality $\iff$ n is indivisible by the characteristic of k), where g is the dimension of A. Of course $H^1(k, A[n])$ depends upon the Galois-module structure of $A[n]$, but we have a right to expect that this group is larger the more complicated the field k becomes.

At least this is what happens in the most easily understood case where $\mathrm{char}(k)$ does not divide n and $A[n] \cong (Z/n\mathbb{Z})^{2g}$ has trivial $\mathfrak{g}_k$-module structure. Then by Kummer theory, $H^1(k, A[n]) \cong (k^\times / k^{\times n})^{2g}$. This group is infinite when k is any Hilbertian field (e.g. a number field) and in many other cases as well. There is also a correction factor, the **weak Mordell-Weil group** $A(k)/nA(k)$, a quantity which has a dependence on k, but especially when $A(k)$ is finitely generated, a very deep dependence on A itself. (When $A(k)$ is not finitely generated, $A(k)/nA(k)$ can well be small when $A(k)$ is itself large; we will see examples shortly.)

Example 0: If $k = \overline{k}$ is algebraically closed, then $WC(k, A) = 0$. Indeed, this is obvious both on the geometric side and the cohomological side. Note also that all three terms in the Kummer sequence vanish.

(Example ϵ: If k is separably closed, then $WC(k, A) = 0$, since every absolutely irreducible variety has a point over a separable field extension.)

4.1. $k = \mathbb{F}_q$. If we first look at the case of elliptic curves, then an element of $H^1(\mathbb{F}_q, E)$ is a genus one curve $C_{/\mathbb{F}_q}$. By the Weil bounds, C must have at least $(\sqrt{q} - 1)^2 \geq (\sqrt{2} - 1)^2$ rational points. Since this quantity is positive, in fact C must have at leat one rational point, so represents the trivial homogeneous space: $H^1(\mathbb{F}_q, E) = 0$. This suggests the following

Theorem 2. *For any abelian variety $A_{/\mathbb{F}_q}$, $H^1(\mathbb{F}_q, A) = 0$.*

Proof: It is enough to show $H^1(\mathbb{F}_q, A)[n] = 0$ for all n (or even all primes). Using the Kummer sequence then, it is enough to show that $\#A(k)/nA(k) = \#H^1(k, A[n])$. In fact both quantities equal $\#A[n](k)$. The equality $\#A(k)/nA(k) = \#A[n](k)$ is left to the reader as an easy exercise. Now a standard result in the cohomology of procyclic groups [**?**, §$XIII$.1] gives

$$H^1(k, A[n]) = A[n]/(F - 1)A[n],$$

where F is the q-power Frobenius map. But

$$\#(F - 1)A[n] = \#A[n]/\ker(F - 1)A[n] = \#A[n]/\#A[n](k).$$

The result follows.

Remark: The above proof works for any connected commutative algebraic group.

Exercise 5: Where was the connectedness used in the proof?

Remark: This is not the standard proof of this result. Rather, more traditional is to apply the cited cohomological fact to get

$$H^1(k, A) = A(\overline{k})/(F-1)A(\overline{k}),$$

and we are reduced to showing that $F-1$ is surjective on $\overline{k}$-points of A. Since F is purely inseparable, its derivative is zero (indeed, this is just the observation that $\frac{d}{dx}x^q = qx^{q-1} = 0$ in characteristic p!), so the morphism $F-1$ induces an isomorphism on the (co/)tangent space at the identity. Its image is therefore a Zariski-open subgroup which, since A is connected, must be A itself.

As a matter of fact, commutativity is not necessary:

Theorem 3. *(Lang) Let $G_{/\mathbb{F}_q}$ be a connected algebraic group, and let $X_{/\mathbb{F}_q}$ be an algebraic variety endowed with a transitive action of G. Then $X(\mathbb{F}_q) \neq \emptyset$.*

Remark: Again the essential point of the proof is to show that the morphism $\varphi : G \to G$, $x \mapsto x^{-1}Fx$ is geometrically surjective. This is (slightly) complicated by the fact that if G is noncommutative, φ is not a homomorphism of groups, so the tangent space argument gives us that it is generically surjective. To see how to derive the surjectivity, see [**?**, §VI.1.4, Prop. 3].

As an example where it is useful to have the theorem for noncommutative groups, one gets that $H^1(\mathbb{F}_q, PGL_n) = 0$ for all n, and it follows that the Brauer group $\mathrm{Br}(\mathbb{F}_q) = H^2(\mathbb{F}_q, \mathbb{G}_m) = 0$.

Final remark: I came up with the proof of Theorem 2 when preparing these notes (although indubitably it must appear in many other places), and at first I it seemed to me that it was "more elementary" than Lang's proof. But in fact Lang's proof comes down to showing that $F - [1]$ is surjective, whereas our proof implicitly uses that $[n]$ is surjective. When the characteristic of k divides n, this is arguably a deeper fact.

4.2. $k = \mathbb{R}$**.** For every genus $g \geq 0$, the smooth curve associated to the equation

$$y^2 = -(x^{2g+2} + 1)$$

has genus g and no $\mathbb{R}$-rational points. In particular, there exists some genus one curve C with $C(\mathbb{R}) = \emptyset$, which represents a nontrivial element of the WC-group of its Jacobian.

We can say a lot more. First, define the **index** of an element $V \in H^1(k, A)$ to be the gcd of all degrees of finite field extensions l/k such that $V \in WC(l/k, A)$, and the **period** of V to be its order in $WC(k, A) = H^1(k, A)$ (a direct limit of finite abelian groups, hence an abelian torsion group).

Proposition 4. *The period divides the index and the two quantities have the same prime divisors.*

Proof: See e.g. [**?**].

In our case, since $\mathfrak{g}_{\mathbb{R}} = \mathrm{Gal}(\mathbb{C}/\mathbb{R}) = \mathbb{Z}/2\mathbb{Z}$, any nontrivial class $\eta \in H^i(\mathbb{R}, M)$ has index and period equal to 2. In particular, $H^1(\mathbb{R}, A) = H^1(\mathbb{R}, A)[2]$.

Coming back to the case of $k = \mathbb{R}$, suppose that E has full 2-torsion defined over $\mathbb{R}$. Then the standard picture of $E(\mathbb{R})$ shows that $E(\mathbb{R}) \cong S^1 \oplus S^1$, so that $E(\mathbb{R})/2E(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$. On the other hand $H^1(\mathbb{R}, E[2])$ has order 4, and we conclude that $H^1(\mathbb{R}, E) \cong \mathbb{Z}/2\mathbb{Z}$, so has a unique nontrivial element. (It can be written down explicitly in terms of a Weierstrass equation for E; see [**?**, Example X.3.7].)

The other possibility is that $E_{/\mathbb{R}}$ has a single nontrivial 2-torsion point (a cubic equation defining E has either 1 or 3 real roots), and in this case $E(\mathbb{R}) \cong S^1$, so that $E(\mathbb{R})/2E(\mathbb{R}) = 0$ and $H^1(\mathbb{R}, E) \cong H^1(\mathbb{R}, E[2])$. Whenever the Galois module structure on $E[2]$ is nontrivial, it is nontrivial to say what $H^1(\mathbb{R}, E[2])$ is. In this particular case, it is of course a finite problem:

Exercise 6: Suppose $E_{/\mathbb{R}}$ is such that $E[2](\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$. Show that $H^1(\mathbb{R}, E) = 0$.

Of course the computation does not "explain why" $H^1(\mathbb{R}, E)$ should be trivial. There are several very nice explanations. For the first, we mention a result of Cassels. First, given an elliptic curve E over a field k of characteristic not equal to 2 or 3, represent it as $y^2 = f(x)$, where $f \in k[x]$ is a cubic polynomial (with distinct roots in $\overline{k}$). Define $l := k[x]/(f)$, a cubic étale algebra. (Note that although the polynomial f is not intrinsically determined by E, the algebra l is, as we leave it to the reader to check.) As in any separable algebra, there is a norm map $N : l^\times \to k^\times$. Let T be the kernel of N; it is a two-dimensional torus defined over k.

Theorem 5. *(Cassels) There is a canonical isomorphism $H^1(k, E[2]) \cong T/2T$.*

In the ("split") case in which $E[2] = E[2](k)$, $l = k \times k \times k$, $N \cong (k^\times)^2$ is a *split* torus, and the theorem is telling us what we already know. Suppose next that E has a single k-rational point of order 2 ("semisplit case"). Then $l \cong m \times k$, where m/k is a quadratic extension, the kernel of the norm map is isomorphic to $m^\times$, so $H^1(k, E[2]) \cong m^\times/m^{\times 2}$.

In the semisplit case of $k = \mathbb{R}$ we must have $m = \mathbb{C}$ (what else?), so $H^1(\mathbb{R}, E[2]) \cong \mathbb{C}^\times/\mathbb{C}^{\times 2} = 0$.

What about higher-dimensional real abelian varieties?

Theorem 6. *(Tate) Let $A_{/\mathbb{R}}$ be an abelian variety. $H^1(\mathbb{R}, A)$ is isomorphic to the component group $\pi_0(A) = A(\mathbb{R})/A(\mathbb{R})^0$.*

Remark: In particular, $\pi_0(A)$ is 2-torsion, since $H^1(\mathbb{R}, A)$ is. This part of the result is not hard to verify, since the norm map $N : A(\mathbb{C}) \to A(\mathbb{R})$ has as its image a closed, connected Lie subgroup containing $N(A(\mathbb{R})) = 2A(\mathbb{R})$. (Therefore it has finite index so is also open, and it follows that $N(A(\mathbb{C})) = A(\mathbb{R})^0$.) As far as I know, there is no truly elementary proof of this theorem. We will revisit it, along with its p-adic analogue, a bit later.

Remark: The results hold with $\mathbb{R}$ replaced by any real-closed field R. One can make sense of the component group in this context (semi-analytic connected components) or just use $N(A(C))$ in its place, where C is the algebraic closure of R.

4.3. $k = \mathbb{C}((t))$**.** If we order fields k by complexity of their WC-groups and draw a line so that on one side of the line we can compute the WC-groups in an explicit and functorial way and on the other side we cannot, then the case of $\mathbb{C}((t))$ is one of the last fields on the easy side of the line. Recall that the algebraic closure of $\mathbb{C}((t))$ is generated by $t^{\frac{1}{n}}$ for $n \geq 2$, and the absolute Galois group is $\hat{\mathbb{Z}}$. (In particular, like $\mathbb{F}_q$, this is a field of cohomological dimension one.)

Theorem 7. *(Ogg, Shafarevich) Let $k = \mathbb{C}((t))$ and $A_{/k}$ be an abelian variety with good reduction. Then $H^1(k, A) \cong (\mathbb{Q}/\mathbb{Z})^{2g}$.*

Proof (sketch): The point is that the hypothesis of good reduction implies that $A(k)$ is n-divisible for all n and $A[n]$ has the same Galois module structure as its reduction, i.e., trivial structure. Thus $H^1(k, A)[n] \cong H^1(k, A[n]) \cong (k^\times/k^{\times n})^{2g} \cong (\mathbb{Z}/n\mathbb{Z})^{2g}$, where we have also used the cyclicity of the absolute Galois group of k. Passing to the limit on n gives the desired result.

Corollary 8. *Under the hypotheses of the previous theorem, for any finite extension l/k of degree n, the restriction map $H^1(k, A) \to H^1(l, A)$ can be viewed as multiplication by n on the group $(\mathbb{Q}/\mathbb{Z})^{2g}$.*

So the kernel of the restriction map $H^1(\mathbb{C}((t)), A) \to H^1(\mathbb{C}((t^{\frac{1}{n}})), A)$ is precisely the n-torsion subgroup $H^1(\mathbb{C}((t)), A)[n]$. In particular, every principal homogeneous space has period equal to its index.

Exercise 7 (Ogg, Shafarevich): For an abelian variety $A_{/\mathbb{C}((t))}$, let α, μ and β be, respectively, the dimensions of the unipotent, multiplicative and abelian parts of the connected component of the Néron special fiber. Show that $H^1(k, A) \cong (\mathbb{Q}/\mathbb{Z})^{\mu+2\beta}$.

Remark: These results use (only) that $\mathbb{C}((t))$ is complete, discretely valued, with residue field $\tilde{k}$ algebraically closed of characteristic 0, but conversely any such field is isomorphic to $\tilde{k}((t))$.

Exercise X: Let k be any complete discretely valued field with algebraically closed residue field $\tilde{k}$ of characteristic $p > 0$.
a) For n prime to p, the above arguments still work: e.g. $H^1(k, A)[n] \cong (\mathbb{Z}/n\mathbb{Z})^{\mu+2\beta}$.
b) Try to compute the group $H^1(k, A)[p^\infty]$. (This has been done by Ogg, Shafarevich and Serre.)
c) Let $E_{/\mathbb{Q}_p}$ be an elliptic curve with good reduction, and fix $\ell \neq p$. Show that there is some unramified extension $k/\mathbb{Q}_p$ such that $H^1(k, E)[\ell] \neq 0$.

Remark: Note that $\mathbb{C}((t))$ is a field of dimension 1, i.e., all finite extensions have vanishing Brauer groups. This shows that WC-groups are in a sense more complicated than Brauer groups. ...

4.4. $k = \mathbb{R}((t))$**.** This case is even closer to the boundary. Work of Ducros computes $H^1(k, E)$ explicitly for any elliptic curve over k; the answer depends on the structure of the Néron special fiber (including the component group). When E has good reduction, $H^1(k, E)$ is $\mathbb{Q}/\mathbb{Z}$ in the semisplit case (i.e., one rational 2-torsion point) and is $\mathbb{Q}/\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})$ in the split case. In this case all the interesting behavior

is in the 2-torsion, so Cassels' theorem is quite relevant. In an as-yet uncompleted[4] preprint, I solved the WCE problem for elliptic curves over $\mathbb{R}((t))$ with good reduction. The general case remains open, although I do not think it is terribly difficult (it might be appropriate for a senior honors thesis or a master's thesis topic). As a byproduct one gets the following result:

Theorem 9. *Let $E_{/\mathbb{R}((t))}$ be an elliptic curve with good reduction. The following are equivalent:*
a) Every principal homogeneous space of E has period equals index.
b) $E[2](\mathbb{R}((t))) \cong \mathbb{Z}/2\mathbb{Z}$.

This is the only example I know of a field k for which the equality of period and index for all elements of the WC-group $H^1(k, E)$ depends on the choice of E.

5. A result about large WC-groups

In this section, we fix an abelian variety A defined over a field k, and an integer $n \geq 2$ indivisible by the characteristic of k.

Shafarevich proved in 1957 that WC-groups over number fields are "large" in the following sense:

Theorem 10. *(Shafarevich) If k is a number field then $H^1(A, E)$ has infinitely many elements of order n.*

In this section, we will prove the following generalization:

Theorem 11. *Suppose k satisfies the following hypotheses:*
(i) k is Hilbertian.
(ii) $A(k)/nA(k)$ is finite.
Then $H^1(k, A)$ has infinitely many elements of order n.

The relevant property (essentially the definition) of Hilbertian fields is the following: if $K/k(t)$ is a finite regular (i.e., $\overline{k} \cap K = k$) Galois extension with Galois group G, there are infinitely many pairwise disjoint extensions l/k with Galois group G.

Every infinite, finitely generated (for short IFG) field is Hilbertian. Moreover, for an abelian variety A over an IFG field, $A(k)$ is a finitely generated abelian group (this extension of the Mordell-Weil theorem is due to Lang-Néron), and it follows that $A(k)/nA(k)$ is finite. (For a proof of this latter fact, see e.g. [**?**, Theorem 3].) Therefore Theorem **??** applies in particular to IFG fields.

Remark: There exist Hilbertian fields over which every absolutely irreducible variety has a rational point, so in particular with vanishing WC-groups. The theorem then shows that for such a field, $A(k)/nA(k)$ is infinite.

Proof of Theorem 11: Using the Kummer sequence and the assumed finiteness of $A(k)/nA(k)$, we are reduced to the following

Proposition 12. *For any Hilbertian field k, $H^1(k, A[n])$ has infinitely many elements of order n.*

[4]It has not been touched since November of 2004...

Note that this is true when $A[n] \cong \mu_n^g$, since then $H^1(k, A[n]) \cong (k^\times/k^{\times n})^{2g}$, and it is well-known that Hilbertian fields have infinitely many disjoint abelian extensions of fixed exponent n. We will reduce to this case via a cohomological argument: let $l = k(\mu_n, A[n])$, so that $A[n] \cong (\mathbb{Z}/n\mathbb{Z})^{2g} \cong \mu_n^{2g}$ as a $\mathfrak{g}_l$-module. Put $G = \mathfrak{g}_{l/k}$. The extended inflation-restriction sequence reads

$$(2) \quad 0 \to H^1(l/k, A[n](l)) \to H^1(k, A[n]) \xrightarrow{\alpha} H^1(l, A[n])^G \to H^2(l/k, A[n](l)$$

so that the map α has finite kernel and cokernel.[5] Thus we want to prove that $H^1(l, A[n])^G$ has infinitely many elements of order n. It is a standard fact (and a good exercise to show) that $H^1(l, A[n])^G$ parameterizes short exact sequences

$$1 \to A[n] \to \mathcal{G} \to G \to 1$$

in which the induced action of G on $A[n]$ agrees with the action of $\mathfrak{g}_k$ on $A[n]$ (which by construction factors through G). From (2), we get that the image of $H^1(k, A[n])$ consists precisely of those exact sequences which are *split*, i.e., such that $\mathcal{G} \cong A[n] \rtimes G$. One has the following general theorem:

Theorem 13. *(Uchida) Every split embedding problem over a Hilbertian field has infinitely many linearly disjoint proper solutions.*

In other words, if l/k is a Galois extension of Hilbertian fields with Galois group G, and is a finite abelian group endowed with a G-action ρ, then there are infinitely many linearly disjoint Galois extensions m/k such that $\mathfrak{g}_{m/l} \cong A$ and such that $\mathfrak{g}_{m/k} \cong A \rtimes_\rho G$. That is to say, we're done.

Remark: Uchida's theorem was proved in 1980, but the case of k a number field was proved by Scholz in 1929, and is used by Shafarevich in his proof of Theorem 10. (Nevertheless his proof is a bit different, using less group cohomology and more study of how the WC-group of k maps into the WC-groups of the various completions of k.)

Remark: B. Poonen has told me that his student, S. Sharif, has a proof of Shafarevich's theorem which constructs classes in $H^1(k, A[n])$ in a more explicit way.

6. WC-groups over local fields

For any abelian variety $A_{/k}$, let $A^\vee = \mathrm{Pic}^0(A)$ be its dual abelian variety. Then there is a bilinear pairing

$$T : H^1(k, A^\vee) \times H^0(k, A) \to H^2(k, \mathbb{G}_m) = \mathrm{Br}(k).$$

In this section we will not give the definition of the pairing, but only the following theorem due to Tate and Milne. Let us assume that k is a nondiscrete locally compact field. That is, either it is $\mathbb{C}$ (an entirely trivial case) or it is $\mathbb{R}$, or it is a finite extension of $\mathbb{Q}_p$, or it is a finite extension of $\mathbb{F}_p((t))$. Again write $\pi_0(A)$ for the quotient of the topological group $A(k)$ by its maximal connected subgroup. When $k = \mathbb{C}$, $A(\mathbb{C})$ is connected, so $\pi_0 = 0$. When $k = \mathbb{R}$, $\pi_0(A) = A(\mathbb{R})/N(A(\mathbb{C}))$ is a finite 2-torsion abelian group as above. When k is a non-Archimedean, $A(k)$ is totally disconnected, so that $\pi_0(A) = A$ (this is, of course, the case to keep your eye on).

In all cases we have a canonical injection from $\mathrm{Br}(k) \hookrightarrow \mathbb{Q}/\mathbb{Z}$. When $k = \mathbb{C}$

[5] In fact α is an isomorphism in many cases.

this is the zero map; when $k = \mathbb{R}$, it is an isomorphism onto $\mathbb{Q}/\mathbb{Z}[2] = \frac{1}{2}\mathbb{Z}/\mathbb{Z}$, and otherwise it is an isomorphism. Now hold on to your hat:

Theorem 14. *(Tate, Milne)*
a) The identity component A^0 of $H^0(k, A)$ pairs trivially with every element of $H^1(k, A^\vee)$.
b) The induced pairing $T : H^1(k, A^\vee) \times \pi_0(A) \to \mathbb{Q}/\mathbb{Z}$ puts $H^1(k, A^\vee)$ and $\pi_0(A)$ in Pontrjagin duality.

Remarks: 1) $H^1(k, A^\vee)$ is the direct limit of the finite groups $H^1(k, A^\vee)[n]$, and $\pi_0(A)$ is the inverse limit of the finite quotients $\pi_0(A)/n\pi_0(A) = A(k)/nA(K)$. In particular, it follows from the theorem that these finite abelian groups are put into a canonical duality. Thus we get the following

Corollary 15. *The finite abelian groups $H^1(k, A^\vee)[n]$ and $A(k)/nA(k)$ are isomorphic.*

Conversely, knowing the duality at each level n is essentially equivalent to knowing the full duality, by passing to the limit.

Remark: At least in the case where $A \cong A^\vee$ (e.g. elliptic curves), this result gives us the beautiful fact the first and last terms of the Kummer sequence are isomorphic. In general, $A[n]$ and $A^\vee[n]$ are **Cartier dual $\mathfrak{g}_k$**-modules.

Corollary 16. *Let k be a locally compact discretely valued field with residue characteristic p, and $A_{/k}$ any abelian variety. Then $H^1(k, A)[p^\infty]$ is infinite, while for any prime $\ell \neq p$, $H^1(k, A)[\ell^\infty]$ is finite.*

The duality pairing has nice functorial properties:

Theorem 17. *Let l/k be a finite extension of discretely valued locally compact fields, and let $r : H^1(k, A) \to H^1(l, A)$ be the natural restriction map. Let $r^\vee : \mathrm{Hom}(H^1(l, A), \mathbb{Q}/\mathbb{Z}) \to \mathrm{Hom}(H^1(k, A), \mathbb{Q}/\mathbb{Z})$ be the dual map. Then $r^\vee$ fits into a commutative diagram*

$$INSERT$$

where $N : A(l) \to A(k)$ is the norm map.

For any finite extension l/k, we have $H^1(l/k, A) \subset H^1(k, A)[l : k]$. In particular, when k is a p-adic field, $H^1(l/k, A)$ is finite.

Corollary 18. *The finite abelian groups $H^1(l/k, A)$ and $A(k)/NA(l)$ are in duality, so are isomorphic.*

This gives at least a formal solution to the WCA problem over p-adic fields. Of course, this will be more or less useful according to how easily the cokernel of the norm map can be computed. Here is a special case:

Theorem 19. *Let k be a finite extension of $\mathbb{Q}_p$, and $A_{/k}$ an abelian variety. Suppose that n is a positive integer prime to p and to the order of the component group Φ of the Néron special fiber of $B = A^\vee$. Let l/k be a finite extension with relative ramification index e. Then $H^1(l/k, A)[n] = H^1(k, A)[\gcd(n, e)]$.*

Proof: In other words, suppose that V is a principal homogeneous space of order n prime to $\#\Phi \cdot p$. Then we must show that $V(l) \neq \emptyset \iff n \mid e$. Let $\tilde{k}$ denote the residue field of k. Recall that we have a filtration on $A(k)$, whose successive

quotients are: a subgroup of $\Phi(\tilde{k})$, the identity component $A^0(\tilde{k})$ of the Néron special fiber, and the kernel of reduction $\mathcal{K}$, on which the multiplication by n map is surjective. This filtration is functorial in k and is preserved by the norm map. By duality, we have $H^1(l/k, A)[n] \cong B(k)/nNB(l)$, and by our choice of n this latter quantity is isomorphic to $B^0(\tilde{k})/N_{l/k}B^0(\tilde{l})$. But

$$N_{l/k}B^0(\tilde{l}) = eN_{\tilde{l}/\tilde{k}}(B^0(\tilde{l})),$$

where the latter norm is for the residue extension $\tilde{l}/\tilde{k}$. We claim that $N_{\tilde{l}/\tilde{k}}(B^0(\tilde{l})) = B^0(\tilde{k})$; in fact this claim is valid for any connected commutative algebraic group G defined over a finite field k. For this, the quotient $G(k)$ by the image of the norm map is $\hat{H}^0(l/k, G(l))$, and by a standard result in the cohomology of finite cyclic groups (triviality of the Herbrand quotient: [**?**,]), this group has the same order as $H^1(l/k, G(l))$. Inflation injects this group into $H^1(k, G)$ which we have seen is equal to 0. This completes the proof.

In the special case in which A (hence also $A^\vee$) has good reduction, the theorem says that for a principal homogeneous space V for A whose order is prime to the residue characteristic, a field l/k is a splitting field if and only if $n \mid e(l/k)$. In this case the result is due to Lang and Tate [**?**], a paper which predates Tate's work on local duality. In fact this is an especially tractable case: Exercise X: Let A be an abelian variety over a p-adic field with good reduction, and n prime to p. Show that the finite abelian groups $A(k)/nA(k)$ and $H^1(k, A)[n]$ are isomorphic.

It is not hard to deduce the following result:

Corollary 20. *Let A be an abelian variety over a p-adic field, and let n prime to p be such that k does* not *contain the nth roots of unity. Suppose there exists a principal homogeneous space V over A of order n. Then V is not split by any abelian extension of k.*

Using this I was able to show:

Theorem 21. *Let k be either a p-adic field or a number field. Then there exists a genus one curve C defined over $\mathbb{Q}$ without any points rational over the maximal abelian extension of k.*

Problem X: Let k be the maximal unramified extension of $\mathbb{Q}_p$ (it is obtained by adjoining all roots of unity of order prime to p). Let A be an abelian variety defined over k and V a principal homogeneous space of A. Must V have an abelian splitting field?