Visibility of Galois Cohomology and Mordell-Weil Groups

William Stein

November 20, 2003

Contents

1 Visibility of $\mathrm{H}^1(K, A)$

Let K be a number field. (There should be a similar theory for function fields over a finite field.)

1.1 Motivation and Philosophy

Suppose

$$0 \to A \to B \to C \to 0$$

is an exact sequence of abelian varieties over K. (Thus each of A, B, and C is a complete group variety over K, whose group is automatically abelian.) Then there is a corresponding long exact sequence of cohomology for the group $\mathrm{Gal}(\overline{\mathbf{Q}}/K)$:

$$0 \to A(K) \to B(K) \to C(K) \to \mathrm{H}^1(K, A) \to \mathrm{H}^1(K, B) \to \mathrm{H}^1(K, C) \to \cdots$$

The study of the Mordell-Weil group $C(K) = \mathrm{H}^0(K, C)$ is popular in arithmetic geometry. For example, the Birch and Swinnerton-Dyer conjecture (BSD conjecture), which is one of the million dollar Clay Math Problems, asserts that the dimension of $C(K) \otimes \mathbf{Q}$ equals the ordering vanishing of $L(C, s)$ at $s = 1$.

The group $\mathrm{H}^1(K, A)$ is also of interest in connection with the BSD conjecture, because it contains the Shafarevich-Tate group

$$Ш(A) = Ш(A/K) = \mathrm{Ker}\left(\mathrm{H}^1(K, A) \to \bigoplus_v \mathrm{H}^1(K_v, A)\right) \subset \mathrm{H}^1(K, A),$$

where the sum is over all places v of K (e.g., when $K = \mathbf{Q}$, the fields K_v are $\mathbf{Q}_p$ for all prime numbers p and $\mathbf{Q}_\infty = \mathbf{R}$).

The group $A(K)$ is *fundamentally different* than $\mathrm{H}^1(K, C)$. The Mordell-Weil group $A(K)$ is finitely generated, whereas the first Galois cohomology $\mathrm{H}^1(K, C)$ is far from being finitely generated—in fact, every element has finite order and there are infinitely many elements of any given order.

This talk is about "dimension shifting", i.e., relating information about $\mathrm{H}^0(K, C)$ to information about $\mathrm{H}^1(K, A)$.

1.2 Definitions

1.2.1 What are Elements of Galois Cohomology?

Elements of $\mathrm{H}^0(K, C)$ are simply points, i.e., elements of $C(K)$, so they are relatively easy to "visualize". In contrast, elements of $\mathrm{H}^1(K, A)$ are Galois cohomology classes, i.e., equivalence classes of set-theoretic (continuous) maps $f : \mathrm{Gal}(\overline{\mathbf{Q}}/K) \to A(\overline{\mathbf{Q}})$ such that $f(\sigma\tau) = f(\sigma) + \sigma f(\tau)$. Two maps are equivalent if their difference is a map of the form $\sigma \mapsto \sigma(P) - P$ for some fixed $P \in A(\overline{\mathbf{Q}})$. From this point of view H^1 is more mysterious than H^0.

1.2.2 Principal Homogeneous Spaces

There is an alternative way to view elements of $\mathrm{H}^1(K, A)$. The WC group of A is the group of isomorphism classes of principal homogeneous spaces for A, where a principal homogeneous space is a variety X and a map $A \times X \to X$ that satisfies the same axioms as those for a simply transitive group action. Thus X is a twist as variety of A, but $X(K) = \emptyset$, unless $X \approx A$. Also, the nontrivial elements of $Ш(A)$ correspond to the classes of X that have a K_v-rational point for all places v, but no K-rational point.

1.2.3 Visibility of $\mathrm{H}^1(K, A)$

Barry Mazur introduced the following definition in order to help unify diverse constructions of principal homogeneous spaces:

Definition 1.1. The *visible subgroup* of $\mathrm{H}^1(K, A)$ in B is

$$\begin{aligned} \mathrm{Vis}_B \mathrm{H}^1(K, A) &= \mathrm{Ker}(\mathrm{H}^1(K, A) \to \mathrm{H}^1(K, B)) \\ &= \mathrm{Coker}(B(K) \to C(K)). \end{aligned}$$

Remark 1.2. Note that $\mathrm{Vis}_B \mathrm{H}^1(K, A)$ *does* depend on the embedding of A into B. For example, suppose $B = B_1 \times A$. Then there could be nonzero visible elements if A is embedding into the first factor, but there will be no nonzero visible elements if A is embedded into the second factor. Here we are using that $\mathrm{H}^1(K, B_1 \times A) = \mathrm{H}^1(K, B_1) \oplus \mathrm{H}^1(K, A)$.

The connection with the WC group of A is as follows. Suppose

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

is an exact sequence of abelian varieties and that $c \in \mathrm{H}^1(K, A)$ is visible in B. Thus there exists $x \in C(K)$ such that $\delta(x) = c$. Then $X = \pi^{-1}(x) \subset B$ is a translate of A in B, so the group law on B gives X the structure of principal homogeneous space for A, and one can show that the class of X in the WC group of A corresponds to c.

1.2.4 Finiteness of the Visible Subgroup

Lemma 1.3. *The group* $\mathrm{Vis}_B \mathrm{H}^1(K, A)$ *is finite.*

Proof. By the Mordell-Weil theorem $C(K)$ is finitely generated. The group $\mathrm{Vis}_B \mathrm{H}^1(K, A)$ is a homomorphic image of $C(K)$ so it is finitely generated. On the other hand, it is a subgroup of $\mathrm{H}^1(K, A)$, so it is a torsion group. The lemma follows since a finitely generated torsion abelian group is finite. □

1.3 Every Element of $\mathrm{H}^1(K, A)$ is Visible Somewhere

Proposition 1.4. *Let $c \in \mathrm{H}^1(K, A)$. Then there exists an abelian variety $B = B_c$ and an embedding $A \hookrightarrow B$ such that c is visible in B. Moreover, B can be chosen to be a twist of a power of A.*

Proof. By definition of Galois cohomology, there is a finite extension L of K such that $\mathrm{res}_L(c) = 0$. Thus c maps to 0 in $\mathrm{H}^1(L, A_L)$. By a slight generalization of the Shapiro Lemma from group cohomology (which is proved by dimension shifting; see, e.g., Atiyah-Wall in Cassels-Frohlich), there is a canonical isomorphism

$$\mathrm{H}^1(L, A_L) \cong \mathrm{H}^1(K, \mathrm{Res}_{L/K}(A_L)) = \mathrm{H}^1(K, B),$$

where $B = \mathrm{Res}_{L/K}(A_L)$ is the Weil restriction of scalars of A_L back down to K. The restriction of scalars B is an abelian variety of dimension $[L : K] \cdot \dim A$ that is characterized by the existence of functorial isomorphisms

$$\mathrm{Mor}_K(S, B) \cong \mathrm{Mor}_L(S_L, A_L),$$

for any K-scheme S, i.e., $B(S) = A_L(S_L)$. In particular, setting $S = A$ we find that the identity map $A_L \to A_L$ corresponds to an injection $A \hookrightarrow B$. Moreover, $c \mapsto \mathrm{res}_L(c) = 0 \in \mathrm{H}^1(K, B)$.

The assertion about the structure of B follows from general facts about restriction of scalars, which won't be proved here. □

1.4 Other Results in the Context of Modularity

Usually one focuses on visibility of elements in $Ш(A)$. There are a number of other results about visibility in various special cases, and large tables of examples in the context of elliptic curves and modular abelian varieties. There are also interesting modularity questions/conjectures in this context. I will not go into these further right now, except to note one example.

Motivated by the notion of visibility, I developed (with input from Mazur, Cremona, and Agashe) computational techniques for unconditionally constructing Shafarevich-Tate groups of modular abelian varieties $A \subset J_1(N)$. For example, if $A \subset J_0(389)$ is the 20-dimensional simple factor, then

$$\mathbf{Z}/5\mathbf{Z} \times \mathbf{Z}/5\mathbf{Z} \subset Ш(A),$$

as predicted by the Birch and Swinnerton-Dyer conjecture. I found a few dozen other examples like this, where the computational construction of the Shafarevich-Tate group would be hopeless using any other known technique. See [AS, AS02] for more details, and [CM00] for examples when $\dim A = 1$.

2 Visibility of Mordell-Weil Groups

2.1 Motivation and Philosophy

The previous section was about understanding elements of H^1 in terms of Mordell-Weil groups. The BSD conjecture implies the following conjecture:

Conjecture 2.1. *If $L(C,1) = 0$, then $C(\mathbf{Q})$ is infinite.*

We know by the Gross-Zagier formula that if C is an elliptic curves over $\mathbf{Q}$ and $\mathrm{ord}_{s=1} L(C,s) = 1$, then $C(\mathbf{Q})$ is infinite, but little more is known toward Conjecture 2.1. More generally, the conjecture is known when $C \subset J_0(N)$ and $\mathrm{ord}_{s=1} L(C,s) = \dim(C)$, and there are other results over totally real number fields. People also seem to have a reasonable (but not good enough!) understanding of $Ш(C)$ when $L(C,1) \neq 0$.

2.1.1 Rank > 1: A New Idea is Needed

Suppose C is an elliptic curve over $\mathbf{Q}$ and $\mathrm{ord}_{s=1} L(C,s) = 2$. Conjecture 2.1 asserts that $C(\mathbf{Q})$ is infinite, but this is currently a difficult open problem. Nick Katz told me at dinner once that "a new idea is needed." It seems that nobody knows a good analogue of Gross-Zagier for rank two elliptic curves. (I've noticed that Mazur has been working on this question, in one way or another, since I've been at Harvard...)

Visibility of Mordell-Weil groups is an idea I came up which might have some relevance.

2.2 Definition

Suppose

$$0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$$

is an exact sequence of abelian varieties over a number field K, with corresponding long exact sequence

$$0 \to A(K) \to B(K) \to C(K) \xrightarrow{\delta} \mathrm{H}^1(K, A) \to \cdots$$

of $\mathrm{Gal}(\overline{\mathbf{Q}}/K)$-cohomology.

Definition 2.2. Let $x \in C(K)$ and suppose $m \in \mathbf{Z}_{>0}$ is a divisor of $\mathrm{order}(x)$ (everything divides ∞). Then x is *m-visible in* $\mathrm{H}^1(K, A)$ if the order of $\delta(x) \in \mathrm{H}^1(K, A)$ is divisible by m.

Motivated by Proposition 1.4, I made the following conjecture at a talk at MSRI in August 2000.

Conjecture 2.3 (Stein). *Suppose $x \in C(K)$ and $m \mid \mathrm{order}(x)$. Then there exists an exact sequence $0 \to A \to B \to C \to 0$ such that x is m-visible in $\mathrm{H}^1(K, A)$.*

2.3 Visibility for Elliptic Curves over Q

The following theorem provides evidence for the conjecture in general.

Theorem 2.4. *Let C be an elliptic curve over $\mathbf{Q}$. Then Conjecture 2.3 is true when m a prime power.*

Proof. Suppose m is a power of a prime p. Let $\mathbf{Q}_\infty$ be the cyclotomic $\mathbf{Z}_p$ extension of $\mathbf{Q}$, so $\mathbf{Q}_\infty$ is the Galois subfield of $\mathbf{Q}(\zeta_{p^n}, n \geq 1)$ of index $p-1$. By [BCDT01], C is a modular elliptic curve. Rohrlich [Roh84] proved that all but finitely many special values $L(C, \chi, 1)$ are nonzero, where χ varies over Dirichlet characters of p-power order. Kato recently proved using his Euler system (see, e.g., [Sch98]) that if $L(C, \chi, 1) \neq 0$, then the χ part of $C(\mathbf{Q}) \otimes \mathbf{Q}$ is 0. Combining these two results, we see that $C(\mathbf{Q}_\infty)$ is finitely generated.

Because $C(\mathbf{Q}_\infty)$ is finitely generated, there is an integer n such that $C(\mathbf{Q}_\infty) = C(\mathbf{Q}_n)$. Let

$$B = \mathrm{Res}_{\mathbf{Q}_n/\mathbf{Q}}(C_{\mathbf{Q}_n}).$$

Then trace induces an exact sequence

$$0 \to A \to B \xrightarrow{f} C \to 0,$$

with A an abelian variety. Then for any integer $j \geq n$ we have

$$\begin{aligned} \mathrm{Im}\left(\delta : C(\mathbf{Q}) \to \mathrm{H}^1(\mathbf{Q}, A)\right) &\cong C(\mathbf{Q})/f(B(\mathbf{Q})) \\ &= C(\mathbf{Q})/\operatorname{Tr}_{\mathbf{Q}_j/\mathbf{Q}}(C(\mathbf{Q}_j)) \\ &= C(\mathbf{Q})/p^{j-n}\operatorname{Tr}_{\mathbf{Q}_n/\mathbf{Q}}(C(\mathbf{Q}_n)) \\ &\twoheadrightarrow C(\mathbf{Q})/p^{j-n}C(\mathbf{Q}), \end{aligned}$$

where the last map is a surjection since

$$\mathrm{Tr}_{\mathbf{Q}_n/\mathbf{Q}}(C(\mathbf{Q}_n)) \subset C(\mathbf{Q}).$$

Suppose $x \in C(\mathbf{Q})$ has order divisible by $m = p^r$. Then for j sufficiently large the image of x in $C(\mathbf{Q})/p^{j-n}C(\mathbf{Q})$ will have order order divisible by m, which proves the theorem. □

Remark 2.5. This theorem is probably true with the same proof with C replaced by any modular abelian variety over $\mathbf{Q}$, i.e., quotient of $J_1(N)$. However, I'm not certain the details of the relevant theorems by Kato and Rohrlich have all been written down in this more general case. Also, one should investigate conjectures of Mazur about finite generatedness of $C(\mathbf{Q}_\infty)$ for general C (see [Maz72]).

2.4 Visibility of Mordell-Weil in Shafarevich-Tate Groups

Let $0 \to A \to B \to \mathbf{C} \to 0$ be an exact sequence of abelian varieties.

Definition 2.6. Let $x \in C(K)$ and suppose $m \in \mathbf{Z}_{>0}$ is a divisor of $\text{order}(x)$. Then x is *m-visible in* $Ш(A)$ if $\delta(x) \in Ш(A)$ and the order of $\delta(x) \in \mathrm{H}^1(K, A)$ is divisible by m.

The following conjecture strengthens Conjecture 2.3.

Conjecture 2.7 (Stein). *Suppose $x \in C(K)$ and $m \mid \text{order}(x)$. Then there exists an exact sequence $0 \to A \to B \to C \to 0$ such that x is m-visible in $Ш(A)$.*

2.4.1 Spiced Up Version of the Conjecture

We spice the conjecture up a little by requiring in addition that A be modular and $L(A, 1) \neq 0$, motivated by the fact that this is the most general class of abelian varieties for which $Ш(A)$ is known to be finite (by work of Kato).

Conjecture 2.8 (Stein). *Suppose C is a modular abelian variety (i.e., C is a quotient of $J_1(N)$ for some N). Suppose $x \in C(K)$ and $m \mid \text{order}(x)$. Then there exists a modular abelian variety A with $L(A, 1) \neq 0$ and an exact sequence $0 \to A \to B \to C \to 0$ such that x is m-visible in $Ш(A)$.*

We offer the following evidence for the conjecture, which I prove in [Ste].

Theorem 2.9. *Let C be the rank 1 elliptic curve $y(y+1) = x(x-1)(x+1)$ of conductor 37, and let x be a generator of $C(\mathbf{Q})$. Then for all* primes *$m < 25000$ with $m \neq 2, 37$, Conjecture 2.8 is true.*

Let $f = \sum a_n q^n$ be the newform associated to C. Suppose m is one of the primes in the theorem. Then there exists a surjective Dirichlet character $\chi : (\mathbf{Z}/\ell\mathbf{Z})^* \to \mu_m$ such that $L(f \otimes \chi, 1) \neq 0$. Moreover, the A of the theorem is the (up to isogeny) abelian variety $A_{f\otimes\chi}$ associated to $f \otimes \chi$ by Shimura, which has dimension $m - 1$.

2.4.2 Nonsquare Shafarevich-Tate Groups

A surprising observation that comes out of the proof is that

$$\#Ш(A) = m \cdot (\text{perfect square}),$$

so we obtain the first ever examples of abelian varieties whose Shafarevich-Tate groups have order neither a square nor twice a square.

References

[AS] A. Agashe and W. A. Stein, *Visible Evidence for the Birch and Swinnerton-Dyer Conjecture for Modular Abelian Varieties of Analytic Rank* 0, To appear in Math. of Computation.

[AS02] ———, *Visibility of Shafarevich-Tate groups of abelian varieties*, J. Number Theory **97** (2002), no. 1, 171–185. MR 2003h:11070

[BCDT01] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, *On the modularity of elliptic curves over* $\mathbf{Q}$*: wild 3-adic exercises*, J. Amer. Math. Soc. **14** (2001), no. 4, 843–939 (electronic). MR 2002d:11058

[CM00] J. E. Cremona and B. Mazur, *Visualizing elements in the Shafarevich-Tate group*, Experiment. Math. **9** (2000), no. 1, 13–28. MR 1 758 797

[Maz72] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18** (1972), 183–266. MR 56 3020

[Roh84] D. E. Rohrlich, *On L-functions of elliptic curves and cyclotomic towers*, Invent. Math. **75** (1984), no. 3, 409–423. MR 86g:11038b

[Sch98] A. J. Scholl, *An introduction to Kato's Euler systems*, Galois Representations in Arithmetic Algebraic Geometry, Cambridge University Press, 1998, pp. 379–460.

[Ste] W. A. Stein, *Shafarevich-tate groups of nonsquare order*, Proceedings of MCAV 2002, Progress of Mathematics (to appear).