

DIOPHANTINE GEOMETRY
NOTES TAKEN 02/26/2008
NOTETAKER: PIPPA CHARTERS

First, let's recall some notation from last class. Let A be an abelian variety over K and $m \in \mathbb{Z}, m \geq 2$ where we assume that $A[m] \subseteq A(K)$. Then we defined the injective map

$$\delta : A(K)/mA(K) \rightarrow H_K = \text{Hom}(\text{Gal}(K_{sep}/K), A[m]).$$

We now assume that K is a global field, and M_K the set of places of K . Then for $v \in M_K$, we let K_v represent the corresponding completion. We can now look at the induced maps

$$\delta_v : A(K_v)/mA(K_v) \rightarrow H_{K_v}$$

and notice that we obtain a commutative diagram:

$$\begin{array}{ccc} \delta : A(K)/mA(K) & \longrightarrow & H_K \\ \downarrow & & \downarrow \\ \delta_v : A(K_v)/mA(K_v) & \longrightarrow & H_{K_v} \end{array}$$

We now define a new group. Let

$$S_m := \{h \in H_K \mid h \in \text{Im}(\delta_v) \text{ for all } v \in M_K\}.$$

Because of the diagram above, note that elements in $A(K)/mA(K)$ are in S_m , and in particular, δ induces an injective map $0 \rightarrow A(K)/mA(K) \hookrightarrow S_m$.

Theorem 1. S_m is finite.

Proof. While we do not go through the proof of this theorem here, it follows from much the same argument as the proof of the finiteness of $A(K)/mA(K)$. \square

Define

$$\text{III}_m = S_m/\delta(A(K)).$$

We want to figure out how to compute $A(K)$. In order to do this, we need to compute $A(K)/mA(K)$. It turns out that S_m is computable, but it's hard to determine the image of $A(K)/mA(K)$ in S_m , as it is not clear how to decide if an element of S_m actually comes from $A(K)/mA(K)$. It turns out that there is a way around this.

Let l be a prime, $l \neq p$ if $\text{char}K = p > 0$. Then the following commutative diagram holds:

$$\begin{array}{ccccccc} 0 & \longrightarrow & A(K)/lA(K) & \longrightarrow & S_l & \longrightarrow & \text{III}_l \longrightarrow 0 \\ & & \uparrow & & \uparrow & & \uparrow \\ 0 & \longrightarrow & A(K)/l^n A(K) & \longrightarrow & S_{l^n} & \longrightarrow & \text{III}_{l^n} \longrightarrow 0 \end{array}$$

We can look at the image of $S_{l^n} \rightarrow S_l$, which is a subgroup of S_l containing the image of $A(K)/lA(K)$. (Note: For this to make sense, we need to define $H_K, \delta, S_{l^n}, \dots$ even when $A[l^n] \not\subset A(K)$, which can be done using Galois cohomology).

Descent “algorithm”. We may now use the above to compute the image of $A(K)/lA(K)$ in S_l in the following manner. Consider two distinct parallel processes.

- (1) Compute elements of $A(K)$ and map them to S_l . In this manner, we will build up a larger and larger picture of the image of $A(K)/lA(K)$ in S_l .
- (2) Compute S_{l^n} and map it to S_l for $n = 1, 2, 3, \dots$. In this manner, we will find smaller and smaller subgroups of S_l containing the image of $A(K)/lA(K)$.

At some point, it is our hope that the subgroups obtained by following these two processes will be the same. That is, there will come a point where we can no longer build up our subgroup as in part 1, or restrict the subgroup further, as we are doing in part 2. At this point, we will have found the exact image of $A(K)/lA(K)$ in S_l as desired.

Theorem 2. *The descent “algorithm” will work if $|\text{III}_{l^m}|$ is bounded as $m \rightarrow \infty$.*

Consider

$$\text{III}_{l^\infty} := \varprojlim_n \text{III}_{l^n}.$$

We define the Tate-Shafarevich group by $\text{III} = \bigoplus_l \text{III}_{l^\infty}$.

Conjecture (Tate-Shafarevich). *III is finite.*

If this conjecture indeed holds true in all cases, then our algorithm is always valid. For now, the conjecture is known to be true only for some elliptic curves over \mathbb{Q} of small rank.

Example. Consider the abelian variety A over $K = \mathbb{Q}$ given by $y^2 = (x - e_1)(x - e_2)(x - e_3)$ where $e_i \in \mathbb{Z}$. Let $m = 2$. Then the map δ is given by:

$$\begin{aligned} \delta : A(\mathbb{Q}) &\rightarrow \mathbb{Q}^\times / (\mathbb{Q}^\times)^2 \oplus \mathbb{Q}^\times / (\mathbb{Q}^\times)^2 \\ (x, y) &\mapsto (x - e_1, x - e_2) \end{aligned}$$

Let μ be the restriction of the map δ to the first coordinate. That is,

$$\begin{aligned} \mu : A(\mathbb{Q}) &\rightarrow \mathbb{Q}^\times / (\mathbb{Q}^\times)^2 \\ (x, y) &\mapsto x - e_1 \end{aligned}$$

We want to know what it means if $b \in \mathbb{Q}^\times / (\mathbb{Q}^\times)^2$ is in the image of μ . First off, we know that $b \in \text{Im}(\mu)$ if and only if there exists some $(x, y) \in E(\mathbb{Q})$ with $x - e_1 = bu^2$ for some $u \in \mathbb{Q}^\times$. That is, there exists some solution to the equation

$$y^2 = bu^2(bu^2 - e_1 + e_2)(bu^2 - e_1 + e_3).$$

Letting $v = \frac{y}{u}$, this is the same as the statement that $b \in \text{Im}(\mu)$ if and only if the equation

$$v^2 = b(bu^2 + e_1 - e_2)(bu^2 + e_1 - e_3) \quad (*)$$

has a solution $(u, v) \in \mathbb{Q}^2$. Consider the set S_2 . We know $b \in S_2$ (i.e., $b \in \mu(A(\mathbb{Q}_p))$ for all p) if and only if the above equation $(*)$ has points in \mathbb{Q}_p for all p . In this example, III_2 measures how much bigger S_2 is than $\text{Im}(\mu)$. Specifically, III_2 is the set of equations $y^2 = bu^2(bu^2 - e_1 + e_2)(bu^2 - e_1 + e_3)$ for varying b which have

solutions in \mathbb{Q}_p for all p “modulo” the set of these equations that have solutions in \mathbb{Q} . What this means for us is that

$\text{III}_2 = 0 \iff$ the Hasse Principle holds for this particular set of equations.

For every curve C of genus 1 over a field K , one can associate an elliptic curve E/K called its Jacobian. If K is a global field and $C(K_v) \neq \emptyset$ for all $v \in M_K$, then C can be viewed as an element of $\text{III}(E/K)$. $\text{III}(E/K) = 0$ if and only if the Hasse Principle holds for curves of genus 1 over K with Jacobian E . If the conjecture of Tate and Shafarevich above holds then failure of the Hasse Principle is measured by a finite quantity.

Suppose C/K has genus 1. If $C(K_v) = \emptyset$ for some v , then $C(K) = \emptyset$. On the other hand, if $C(K_v) \neq \emptyset$ for all $v \in M_K$, then $[C] \in \text{III}(E/K)$. It follows that we have

$$C(K) \neq \emptyset \iff [C] = 0.$$

If $\text{III}(E/K)$ is finite, then we can verify whether $[C] = 0$ by a finite computation. To do this, we use a bilinear pairing (known as the Cassels pairing)

$$\beta : \text{III} \times \text{III} \rightarrow \mathbb{Q}/\mathbb{Z}$$

which is known to be nondegenerate if III is finite. From this pairing, we get $[C] = 0 \iff \beta([C], g) = 0$ for all $g \in \text{III}$. Note that this is true only for curves of genus 1, not for those of higher genus. It does, however, end up generalizing to “principal homogeneous spaces of abelian varieties.”