

Diophantine Geometry

Notes for February 21, 2008

Felipe Voloch
Transcribed by Salman Butt

March 3, 2008

Our goal today is prove the Weak Mordell-Weil Theorem. Recall our map δ :

$$\delta : A(K) \longrightarrow \text{Hom}(\text{Gal}(K_{sep}/K), A[m]) = H$$

We can also identify H with the (a priori) set

$$\{(L, \lambda) : L/K \text{ Galois}, \lambda : \text{Gal}(L/K) \hookrightarrow A[m]\},$$

(in fact, this set has a group structure), and we will often go back and forth between these two interpretations of H . We will also assume $A[m] \subseteq A(K)$. We defined δ by the following: given $P \in A(K)$, let Q be a point on our abelian variety such that $mQ = P$. Then we set $\lambda(\sigma) = \sigma Q - Q$ and $L = K(Q)$, where $K(Q)$ is the extension of K gotten by adjoining the coordinates of Q . We first want to prove some claims from last time.

Claim 1. δ is independent of the choice of Q .

Proof. Suppose Q, Q' satisfy $mQ = mQ' = P$. Then $m(Q - Q') = \mathcal{O}$, and by our assumption that $A[m] \subseteq A(K)$, we see that $Q - Q' \in A(K)$. This immediately tells us that $K(Q) = K(Q') = L$ since Q and Q' differ by an element of $A(K)$. Moreover for any $\sigma \in \text{Gal}(L/K)$, $\sigma(Q - Q') = Q - Q'$. Rearranging, we find that for any $\sigma \in \text{Gal}(L/K)$, $\sigma Q - Q = \sigma Q' - Q'$. Hence $\lambda(\sigma)$ is independent of Q , as is L . \square

Claim 2. λ is an injection.

Proof. $\lambda(\sigma) = \mathcal{O}$ if and only if $\sigma Q = Q$ if and only if σ when restricted to L is the identity, i.e. σ is the identity in $\text{Gal}(L/K)$. \square

Claim 3. δ is a homomorphism.

Proof. Let $P = P_1 + P_2$. Choose Q_i such that $mQ_i = P_i$ for $i = 1, 2$. Let $Q = Q_1 + Q_2$, then $mQ = P$. Let $\lambda_i(\sigma) = \sigma Q_i - Q_i$ for $i = 1, 2$. Then

$$(\lambda_1 + \lambda_2)(\sigma) = \sigma Q_1 + \sigma Q_2 - Q_1 - Q_2 = \sigma(Q_1 + Q_2) - (Q_1 + Q_2) = \sigma Q - Q = \lambda(\sigma),$$

so $\lambda = \lambda_1 + \lambda_2$ as desired. \square

Claim 4. $\ker \delta = mA(K)$.

Proof. We first show that $mA(K) \subseteq \ker \delta$: say $P \in mA(K)$, then there exists a $Q \in A(K)$ satisfying $mQ = P$, so let us choose this Q . Then $L = K$ so λ is the zero map, so $P \in \ker \delta$.

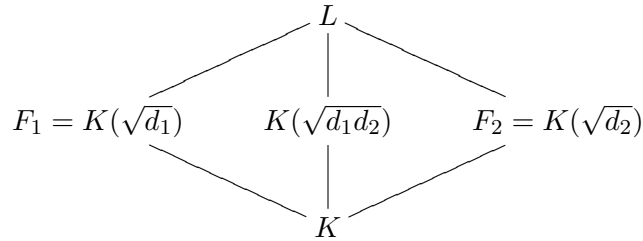
Now assume $P \in \ker \delta$, so $\lambda(\sigma) = \mathcal{O}$ for all σ . Then $\sigma Q = Q$ for all σ , hence $Q \in A(K)$ and, since $mQ = P$, we see that $P \in mA(K)$. \square

Using this last claim, we see that $\delta : A(K)/mA(K) \hookrightarrow H$.

Example. Let $A = E : y^2 = x^3 + ax + b$ be an elliptic curve and $m = 2$. We are assuming that $E[2] \subseteq E(K)$, so the points of order 2 (i.e. those points with y -coordinate 0) are in $E(K)$. Thus our cubic factors over K :

$$y^2 = (x - e_1)(x - e_2)(x - e_3), \quad e_i \in K.$$

As discussed last time, $E[2] = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. We want to know what extensions L/K are possible. Considering the possible maps $\text{Gal}(L/K) \hookrightarrow \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and noting that $\text{char}(K) \neq 2$, we readily see the only possible field diagram is



From this, the possible λ 's are easily determinable. Noting that we can adjust $K(\sqrt{d})$ by a square (i.e. $K(\sqrt{d}) = K(\sqrt{r^2 d})$), we readily see that $H \cong K^\times / (K^\times)^2 \oplus K^\times / (K^\times)^2$, where $(K^\times)^2$ is the subgroup of squares in K^\times . Choosing the basis $\{(e_1, 0), (e_2, 0)\}$ for $E[2]$, for $(x, y) \neq (e_1, 0), (e_2, 0)$, we see that

$$\delta : (x, y) \mapsto (x - e_1, x - e_2) \in E[2].$$

For $(x, y) = (e_1, 0), (e_2, 0)$, one can readily work out δ by considering what to do in order to divide by 2. \square

Remark 0.1. In general, if $p \nmid m$, $A[m] = (\mathbb{Z}/m\mathbb{Z})^{2 \dim A}$, so $H \cong (K^\times / (K^\times)^m)^{2 \dim A}$.

So far we had not assumed any conditions on our field K . We will now restrict our arguments to a global field K . Let M_K be the set of places (i.e. equivalence classes of absolute values) of K , K_v be the completion of K with respect to a place $v \in M_K$, $\mathcal{O}_v = \{x \in K_v : |x|_v \leq 1\} \subseteq K_v$, and $\mathcal{M}_v = \{x \in K_v : |x|_v < 1\}$ the unique maximal ideal in \mathcal{O}_v . By clearing denominators, we can view A as being defined over \mathcal{O}_v and reduce modulo \mathcal{M}_v to get a variety A_v defined over the finite field $\mathcal{O}_v/\mathcal{M}_v$. If A_v is an abelian variety, we say A has *good reduction* at v ; otherwise we say A has *bad reduction* at v .

We next define a set $S \subset M_K$ such that S contains the archimedean places, all places of bad reduction for A , and all places $v \mid m$ (i.e. $|m|_v < 1$). We claim without proof that S is finite. This can be shown by extending techniques from a previous lecture. We will need the following definitions to prove the Weak Mordell-Weil Theorem:

Definition 1. Let K be a field, L/K a finite extension, and $|\cdot|$ an absolute value on L . We say that $|\cdot|$ is *unramified in L* if $\{|x| : x \in K\} = \{|x| : x \in L\}$.

Definition 2. A place $v \in M_K$ is **unramified in L** if for all $|\cdot|$ of L that are in the class of v when restricted to K are unramified in L .

Example. Let $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{D})$ with D a square-free integer. Observe that for odd p , the p -adic absolute value in \mathbb{Q} is ramified in $\mathbb{Q}(\sqrt{D})$ if and only if $p \mid D$. (We say $|\cdot|/\mathbb{Q}$ is **ramified** in L if there exists an absolute value in L that restricts to $|\cdot|$ in \mathbb{Q} which is not unramified.) If $p \mid D$, $D = pc$ where $(c, p) = 1$ (since D is square-free). So $|\sqrt{D}|_p^2 = |D|_p = |pc|_p = 1/p$. Thus $|\sqrt{D}|_p = 1/\sqrt{p} \notin \{|x|_p : x \in \mathbb{Q}\} = p^{\mathbb{Z}} \cup \{0\}$. On the other hand if p does not divide D , then we have $|\sqrt{D}|_p = 1$. Thus $\{|x|_p : x \in \mathbb{Q}(\sqrt{D})\} = \{|x|_p : x \in \mathbb{Q}\}$. We also note that 2 ramifies in $\mathbb{Q}(\sqrt{D})$ if and only if D is even or $D \equiv 3 \pmod{4}$. \square

We will make use of the following important theorem:

Theorem 1. If $P \in A(K)$, $mQ = P$. Then $K(Q)/K$ is unramified outside of S .

Note that S depends on the abelian variety A and the field K . So as you vary $P \in A(K)$, the theorem tells us that the extensions $K(Q)/K$ are *all* unramified outside the *same* set S . We will also need the following theorem:

Theorem 2 (Hermite). If K is a global field, $S \subset M_K$ finite, $d \geq 2$ an integer (with $p \nmid d$ if $p = \text{char}K > 0$), then the set $\{L/K : L \text{ unramified outside of } S, [L : K] = d\}$ is finite.

Theorem 3. Theorem 1 and 2 imply the Weak Mordell-Weil Theorem.

Proof. By Theorem 1, if $P \in A(K)$, $K(Q)$ is unramified outside of S for any $mQ = P$. We also know that $[K(Q) : K] \leq \#A[m]$. Then by Theorem 2, there are only finitely many choices for such $K(Q)$ and only finitely many $\lambda : \text{Gal}(K(Q)/K) \hookrightarrow A[m]$. Thus the image of δ is finite. Thus $A(K)/mA(K)$ is finite, giving us the Weak Mordell-Weil Theorem. \square

Thus we are only left with proving Theorems 1 and 2. We will only do the case of an elliptic curve over \mathbb{Q} and $m = 2$, leaving the general case to one of the standard texts.

Proof of Theorem 1. We have

$$E : y^2 = x^3 + ax + b = (x - e_1)(x - e_2)(x - e_3)$$

where we may assume without loss of generality that $e_i \in \mathbb{Z}$ (performing a change of coordinates if necessary). As discussed before,

$$\delta(x, y) = (x - e_1, x - e_2) \in \mathbb{Q}^\times / (\mathbb{Q}^\times)^2 \times \mathbb{Q}^\times / (\mathbb{Q}^\times)^2.$$

Considering the possible linear change of variables, we observe that a point (x, y) on E must be of the form $(u/z^2, v/z^3)$ with $u, v, z \in \mathbb{Z}$ and $(u, z) = 1$, $(v, z) = 1$. Thus

$$x - e_i = \frac{u - e_i z^2}{z^2}.$$

So if p is an odd prime ($2 \in S$ since $m = 2$) which ramifies in $\mathbb{Q}(Q)$, then $p \mid (u - e_i z^2)$. (Note that we do not know if $u - e_i z^2$ is square-free, so we do not have an if and only if in the previous statement.) Plugging $(x, y) = (u/z^2, v/z^3)$ into the equation for E , we get

$$v^2 = (u - e_1 z^2)(u - e_2 z^2)(u - e_3 z^2).$$

Say $p \mid (u - e_1z^2)$ but $p \nmid (u - e_2z^2)(u - e_3z^2)$, then an even power of p divides exactly $(u - e_1z^2)$, since $p \mid v^2$. So p does not ramify in $\mathbb{Q}(\sqrt{x - e_1})$.

So the primes that ramify divide two of the factors of the cubic. So suppose without loss of generality that $p \mid (u - e_1z^2)$ and $p \mid (u - e_2z^2)$. Then $p \mid (e_1 - e_2)z^2$. But if $p \mid z$, then $p \mid u$, but this cannot happen since $(z, u) = 1$. Thus $p \nmid z$, hence $p \mid (e_1 - e_2)$. So the primes that ramify in $\mathbb{Q}(Q)$ are contained inside the set

$$S = \{2, \infty\} \cup \underbrace{\left\{ p : p \mid \prod_{i \neq j} (e_i - e_j) \right\}}_{\text{primes of bad reduction}}.$$

Thus $\mathbb{Q}(Q)$ is unramified outside of S . □

Proof of Theorem 2. We want to count the number of quadratic extensions of \mathbb{Q} unramified outside of $S = \{2, p_1, \dots, p_r\}$. These extensions are those $\mathbb{Q}(\sqrt{D})$ such that D is square-free and for all $p \notin S$, $p \nmid D$. Thus for $\epsilon_i = 0, 1$,

$$D = \pm \prod_{p_i \in S} p_i^{\epsilon_i}.$$

There are finitely many such D , so there are finitely many extensions $\mathbb{Q}(D)$. □

The general case of these theorems requires finiteness of class numbers and Dirichlet's Unit Theorem, but we will leave it at that.