

DIOPHANTINE GEOMETRY

FELIPE VOLOCH

FEB 19, 2008

(NOTES BY YUAN YAO)

Lemma 0.1. *Let K be a field of characteristic p , $p = 0$ or a prime number, A be an abelian variety over K , m be an integer with $m \geq 2$ and $p \nmid m$. Then $A[m] := \{P \in A \mid mP = 0\}$ is a finite set of points defined over a finite extension of K .*

Proof. For any abelian variety, the group law is defined by rational functions of coordinates, so $mP = P + P + \dots + P$ is a rational function of P , and so $A[m]$ is an algebraic set. By algebraic geometry, we know $A[m]$ has a finite number of irreducible components, each defined over a finite extension of K . Let X be an irreducible component of $A[m]$, take a point $Q \in X$, then for any $P \in X$, we have $m(P - Q) = mP - mQ = 0 - 0 = 0$, which implies $X - Q \subseteq A[m]$, and $0 = Q - Q \in X - Q$.

Now consider the property of $A[m]$ near $0 \in A$. Let t_1, \dots, t_n be local coordinates at 0 , then near 0 , the group law $\mu : A \times A \rightarrow A$ can be considered as a rational map $\mu(t_1, \dots, t_n, t'_1, \dots, t'_n) = (F_1(t_1, \dots, t_n, t'_1, \dots, t'_n), \dots, F_n(t_1, \dots, t_n, t'_1, \dots, t'_n))$. Since $0+0 = 0$, we have $F_i(0, \dots, 0, 0, \dots, 0) = 0$ for all $1 \leq i \leq n$; since $t+0 = 0+t = t$, we have $F_i(t_1, \dots, t_n, 0, \dots, 0) = t_i$ and $F_i(0, \dots, 0, t'_1, \dots, t'_n) = t'_i$, for all $1 \leq i \leq n$. It follows that $F_i(t_1, \dots, t_n, t'_1, \dots, t'_n) = t_i + t'_i + \text{higher order terms}$ (as a power series) and hence, $m(t_1, \dots, t_n) = (t_1, \dots, t_n) + \dots + (t_1, \dots, t_n) = (mt_1 + \text{higher order terms}, \dots, mt_n + \text{higher order terms})$. By assumption, $\text{char}K \nmid m$, so $m(t_1, \dots, t_n) \neq 0$ for (t_1, \dots, t_n) close but unequal to 0 , which implies 0 is an isolated point in $A[m]$.

Combine the two results, we see each irreducible component X must be a single point, so $A[m]$ is a finite set of points. □

Example 0.2. Let A be an elliptic curve $y^2 = x^3 + ax + b$, $m = 2$. By the addition on elliptic curves, a point $(x, y) \in A$ satisfies $2(x, y) = 0$ if and only if $y = 0$. So

$$A[2] = \{(x, y) \in A \mid y = 0\} \cup \{0\} = \{(x, 0) \mid x^3 + ax + b = 0\} \cup \{0\}$$

consists of 4 points, each defined over the splitting field of $x^3 + ax + b$ over K .

Remark: Given this lemma and the so-called **Weak Mordell-Weil Theorem:** **Let K be a global field of characteristic p , $p = 0$ or a prime number, A be an abelian variety over K , m be an integer with $m \geq 2$ and $p \nmid m$, and suppose $A[m] \subseteq A(K)$, then the quotient group $A(K)/mA(K)$ is finite**, we can prove Mordell-Weil Theorem by working in the extension of K which contains coordinates of $A[m]$. By the lemma, there exists L/K finite such that $A[m] \subseteq A(L) \implies A(L)/mA(L)$ is finite. Then using height function, we can deduce $A(L)$ is finitely generated, so $A(K) \subseteq A(L)$ is also finitely generated.

Now suppose K is a field of characteristic p , $p = 0$ or a prime number, A is an abelian variety over K , m is an integer with $m \geq 2$ and $p \nmid m$, and assume $A[m] \subseteq A(K)$. Denote the group

$H = \text{Hom}(\text{Gal}(K^{sep}/K), A[m])$, then H has a bijection to the set

$$\{(L, \lambda) \mid L/K \text{ is a finite Galois extension, } \lambda \text{ is a group monomorphism from } \text{Gal}(L/K) \text{ to } A[m]\}$$

by sending φ to $((K^{sep})^{\ker \varphi}, \bar{\varphi})$. Define a map δ from $A(K)$ to H as follows: let $P \in A(K)$, choose $Q \in A(K^{sep})$ such that $mQ = P$, let $L = K(Q)$. We **Claim** that L/K is Galois, and the map $\lambda : \text{Gal}(L/K) \rightarrow A[m] : \sigma \mapsto \sigma Q - Q$ is a group monomorphism. Now $(L, \lambda) \in H$, and is defined to be the image of P under δ . Then δ is a well-defined (independent of the choice of Q) group homomorphism, and $\ker \delta = mA(K)$. Henceforth, δ induces a homomorphism from $A(K)/mA(K)$ to H .

Proof of Claim: Firstly, suppose $\sigma \in \text{Gal}(K^{sep}/K)$, then $m(\sigma Q) = \sigma(mQ) = \sigma(P) = P$, so $m(\sigma Q - Q) = P - P = 0$, so $\sigma Q - Q \in A[m] \subseteq A(K)$, and so $\sigma Q = Q + (\sigma Q - Q) \in A(K(Q)) = A(L)$. This shows L/K is Galois.

Secondly, for any $\sigma, \tau \in \text{Gal}(L/K)$, we have $\lambda(\sigma\tau) = \sigma\tau Q - Q = \sigma\tau Q - \sigma Q + \sigma Q - Q = \sigma(\tau Q - Q) + (\sigma Q - Q) = \sigma(\lambda(\tau)) + \lambda(\sigma)$. As $\lambda(\tau)$ is an element in $A[m] \subseteq A(K)$, it is fixed by $\sigma \in \text{Gal}(L/K)$, and so $\lambda(\sigma\tau) = \lambda(\tau) + \lambda(\sigma)$. Besides, suppose $\lambda(\sigma) = 0$, then $\sigma(Q) = Q \implies L = K(Q)$ is fixed by $\sigma \implies \sigma = 1$. This shows λ is a group monomorphism.