

# Diophantine Geometry Lecture Notes

March 27, 2008

Let  $K$  be a field of characteristic  $p > 0$ . Let  $f(x_1, x_2, \dots, x_n) \in K[x_1, x_2, \dots, x_n]$  given by

$$f(x_1, x_2, \dots, x_n) = \sum a_{i_1, i_2, \dots, i_n} x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}.$$

Define

$$f^{(p)}(x_1, x_2, \dots, x_n) = \sum a_{i_1, i_2, \dots, i_n}^p x_1^{i_1} x_2^{i_2} \dots x_n^{i_n}.$$

If  $X/K$  is a variety,  $X$  is the set of zeros of  $f_1, f_2, \dots, f_m \in K[x_1, x_2, \dots, x_n]$ . Define  $X^{(p)}$  to be the set of common zeroes of  $f_1^{(p)}, f_2^{(p)}, \dots, f_m^{(p)}$ . There is a map  $F : X \rightarrow X^{(p)}$  given by  $(x_1, x_2, \dots, x_n) \mapsto (x_1^p, x_2^p, \dots, x_n^p)$  because  $(f(x_1, x_2, \dots, x_n))^p = f^{(p)}(x_1^p, x_2^p, \dots, x_n^p)$ . (Follows from the fact that  $(x + y)^p = x^p + y^p$  in characteristic  $p$ ).

*Remark.* If  $X$  is defined over  $\mathbb{F}_p$ , then  $X^{(p)} = X$ . If  $X$  is defined over  $\mathbb{F}_{p^m}$ , then, if we define  $X^{(p^2)} = (X^{(p)})^{(p)}$ , etc. then  $X^{(p^m)} = X$ , and we get a map  $F^m : X \rightarrow X$  via

$$X \rightarrow X^{(p)} \rightarrow X^{(p^2)} \rightarrow \dots \rightarrow X^{(p^m)}$$

.

Let  $A/K$  be an abelian variety. Then we have the map  $F : A \rightarrow A^{(p)}$ . We also have the map  $[p] : A \rightarrow A$  defined by  $P \mapsto pP$ . Fact: There is a map  $V : A^{(p)} \rightarrow A$  such that  $[p] = V \circ F$ .

*Remark.* If  $\Phi : X \rightarrow Y$  is an onto map of varieties over  $K$ , we have an injection of function fields  $K(Y) \hookrightarrow K(X)$ . Then the map  $\Phi$  is separable if  $K(X)/K(Y)$  is separable.

*Definition.* An abelian variety  $A$  is called ordinary if  $V$  is separable.

**Theorem.** If  $K$  is a global field of characteristic  $p > 0$  and  $C/K$  is a curve of genus  $g \geq 2$  such that  $C$  is not defined over  $K^p$  and  $J = \text{Jac}(C)$  is ordinary, then  $C(K)$  is finite.

*Proof.* Mordell-Weil implies that  $J(K)$  is finitely generated, so  $J(K)/pJ(K)$  is finite. If  $C(K) = \emptyset$ , we are done. If not, we have  $\alpha : C \rightarrow J$  defined by  $P \mapsto P - P_0$ . We can assume  $C \subseteq J$ . So  $C(K) = C \cap (J(K))$ . If  $C(K)$  is infinite, then there is  $P_1 \in J(K)$  such that  $C \cap (P_1 + pJ(K))$  is infinite. Define  $\Phi : J^{(p)} \rightarrow J$  by  $\Phi(P) = V(P) + P_1$ . Define  $C' = \Phi^{-1}(C)$ , so that  $C'$  is a curve on  $J^{(p)}$ . Now we have  $P \in P_1 + pJ(K) \Leftrightarrow$  there is  $Q \in J(K)$  such that  $P = P_1 + pQ = P_1 + V(F(Q)) = \Phi(F(Q)) \Leftrightarrow \Phi^{-1}(P) \in F(J(K))$ . But  $F(J(K)) = J^{(p)}(K^p)$ . So  $C \cap (P_1 + pJ(K))$  infinite  $\Rightarrow C' \cap J^{(p)}(K^p)$  is infinite.  $J^{(p)}$  is defined over  $K^p$ . It can be shown that  $C' \cap J^{(p)}(K^p)$  being infinite implies  $C'$  is defined over  $K^p$ . But using the fact that  $J$  is ordinary, we can show  $C'$  defined over  $K^p$  implies  $C$  defined over  $K^p$ , giving a contradiction.  $\square$

*Remark.* The natural hypothesis for the Mordell conjecture is that  $C$  is not defined over  $\mathbb{F}_q$ . It can be shown that this is equivalent to  $C$  not defined over  $K^{p^m}$  for some  $m \geq 1$ : If  $K$  is a global field of characteristic  $p$ ,  $\bigcap_{m \geq 1} K^{p^m} = \mathbb{F}_q$ . The proof can be adapted to deal with this more general situation.

What happens over finite fields: Consider  $C/\mathbb{F}_q$ , with  $q = p^f$ . Let  $K$  be a global field of characteristic  $p$  with constant field  $\mathbb{F}_q$ . Suppose  $P \in C(K) - C(\mathbb{F}_q)$ . We can consider  $F^{fm}(P) \in C(K)$ , and we get infinitely many points with  $m = 1, 2, \dots$

*Example.*  $C : y^2 = x^5 + 1$  over  $\mathbb{F}_3$ . Take  $K = \mathbb{F}_3(t, s)$  where  $s^2 = t^5 + 1$ . Then  $(t^{3^m}, s^{3^m}) \in C(K)$ .

In place of  $J(K)$ , we could have used any subgroup  $\Gamma \subseteq J(K^{sep})$  with the property that  $\Gamma/p\Gamma$  is finite (e.g., one can take  $\Gamma$  to be the group of prime to  $p$  torsion points in  $J(K^{sep})$ ). A special case of the Manin-Mumford conjecture says that  $C \cap J_{tor}$  is finite.

Another example that one can take is to embed  $J(K)$  in  $J(K_v)$  for a completion  $K_v$  of  $K$  and take  $\overline{J(K)}$  in  $J(K)$ . (In the case of number fields, the Chabauty argument proves that  $\overline{J(K)} \cap C$  is finite if  $J(K) \subseteq J(K_v)$  and  $\text{rk}(J(K)) < \text{genus}(C)$ ). In characteristic  $p$ ,  $\overline{J(K)} \subseteq J(K_v)$  is always “small”, where “big” means that it “contains a neighborhood of 0,” and “small” means not “big.” In characteristic 0,  $\overline{J(K)} \subseteq J(K_v)$  is “small” if  $v$  is non-Archimedean and  $\text{rk}(J(K)) < \text{genus}(C)$ . Otherwise, it is usually “big.”