

S08 DIOPHANTINE GEOMETRY
CLASS NOTE ON 3/18/08

We start with a theorem, which was conjectured by Mordell.

Theorem 1. *If K is a global field and C/K is a curve of genus ≥ 2 , then $C(K)$ is finite except if K is a function field over \mathbb{F}_q and C is defined over \mathbb{F}_q .*

Remark. In particular, if K is a number field, then $C(K)$ is finite. The number field case is solved by Faltings in 1983. The function field case was done by Samuel in the 60's.

Before we embark on the arithmetic of curves we need to do some geometry. We begin by defining divisors and Jacobians.

Suppose F is algebraically closed and C/F is a smooth irreducible projective curve. In general $C(F)$ is not finite.

Definition. *A divisor on C is a formal sum $D := \sum_{P \in C(F)} n_P P$ where $n_P : C(F) \rightarrow \mathbb{Z}$ is supported on finitely many points.*

Given two divisors $D = \sum_P n_P P, D' = \sum_P n'_P P$ define $D + D' := \sum_P (n_P + n'_P) P$. Denote the set of all divisors on C by $\text{Div}(C)$. In other words, $\text{Div}(C)$ is a free abelian group generated by $C(F)$.

We also define a map $\text{deg} : \text{Div}(C) \rightarrow \mathbb{Z}$ by $\text{deg}(D) := \sum_P n_P$ where $D = \sum_P n_P P$. Set $\text{Div}^0(C) := \ker(\text{deg})$.

Recall that the function field $F(C)$ is defined as a field of fractions of

$$R := F[x_1, \dots, x_n]/(f_1, \dots, f_m)$$

where $f_1 = \dots = f_m = 0$ is a system of equations for a non-empty affine open subset of C . For example, if C is defined by $f(x, y) = 0$ then $R = F[x, y]/(f(x, y))$ and $F(C)$ is a field of fractions of R .

Let $h \in F(C)$. Define $(h) \in \text{Div}(C)$ by

$$(h) := \sum_P \text{ord}_P(h) P$$

where $\text{ord}_P(h)$ is the order of zero or pole of h at P . We have the following fact.

Proposition 1. *$\text{deg}((h)) = 0$ for any $h \in F(C)$, that is, any function has as many zeros as poles with multiplicities.*

Verify this for a couple of examples. If $F = \mathbb{C}$, then C is a compact Riemann surface. Take any function $h \in F(C)$, that is, a meromorphic function on the surface. Then there are only finitely many zeros and poles on C . We can take a closed path γ on C enclosing a disk that does not contain any zeros or poles of h . By the residue theorem we have that

$$0 = \int_{\gamma} \frac{dh}{h} = \sum_P \text{ord}_P(h).$$

If $C = \mathbb{P}^1$, then $F(C) = F(x)$. For $h = \frac{A(x)}{B(x)}$, we have $\text{ord}_\infty(h) = \deg(B) - \deg(A)$ hence the proposition holds.

Definition. $\text{Prin}(C) := \{(h) : h \in F(C)\}$.

Remark. By proposition 1, $\text{Prin}(C) \subset \text{Div}^0(C) \subset \text{Div}(C)$. Also for any $h_1, h_2 \in F(C)$, $(h_1 h_2) = (h_1) + (h_2)$.

We are now in position to define the Jacobian of C .

Definition. The Jacobian of C is the group $\text{Div}^0(C)/\text{Prin}(C)$.

Definition. We say divisors D, D' on C are linearly equivalent if $D - D' \in \text{Prin}(C)$ and denote $D \sim D'$ if those are equivalent. In other words, $D \sim D'$ if and only if there exists $h \in F(C)$ so that $D - D' = (h)$.

Here are a couple of examples.

Suppose $D \in \text{Div}^0(\mathbb{P}^1)$. Then D is a form of $\sum_{\alpha \in F} n_\alpha [\alpha] + n_\infty [\infty]$. Note that $\sum n_\alpha + n_\infty = 0$. Define a function

$$h := \prod_{\alpha \in F} (x - \alpha)^{n_\alpha}.$$

Then $(h) = D$ and this implies that $\text{Jac}(\mathbb{P}^1) = 0$.

Now consider an elliptic curve $E : y^2 = x^3 + ax + b$. We claim that $\text{Jac}(E) \cong E(F)$. The isomorphism is given by $E(F) \ni P \mapsto P - O \in \text{Jac}(E)$ where O is the point at ∞ on E . This map is well-defined because $P - O \in \text{Div}^0(E)$. We are going to show first that this is surjective. Later we will see that this is injective and a homomorphism.

Let $P, Q \in E$ and L be the line \overline{PQ} . Then by definition,

$$(L) = P + Q + R - 3O$$

unless the line L is vertical, where R is another intersection point on E by L . Hence

$$P + Q - 2O \sim O - R \sim \overline{R} - O$$

where $\overline{R} = -R$ in the group law on E . Therefore

$$P + Q \sim \overline{R} + O.$$

This can be used iteratively on a divisor to trade two arbitrary points by a pair of points one of which is O . Let $D = \sum n_i P_i - \sum m_i Q_i$ where $n_i, m_i > 0$ and $\sum n_i = \sum m_i$. Then, applying this procedure gives:

$$D \sim \left(Q + \left(\sum n_i - 1 \right) O \right) - \left(R + \left(\sum m_i - 1 \right) O \right) = Q - R$$

Now, $Q - R \sim Q + \overline{R} - 2O \sim O - P \sim \overline{P} - O$. This shows that our map is surjective.