Introduction to Algebraic Number Theory
Lecture 36

Erin Bela

April 16, 2014

Definition 0.1 *Let C be a smooth projective curve. We define the* ***cotangent space****:*

$$\Omega_C = \frac{\{\bar{K}(C)-\text{ vector space generated by } df,\ f \in \bar{K}(C)\}}{\{d(f+g) = df + dg,\ d\ const\ = 0,\ d(fg) = f\,dg + g\,df\}}$$

If $\varphi : C_1 \to C_2$ is a morphism then we have a map $\varphi^* : \Omega_{C_2} \to \Omega_{C_1}$ given by:

$$\varphi^*\left(\sum f_i \cdot dg\right) = \sum \varphi^*(f_i)\, d\varphi(g_i).$$

Remark: φ is purely inseparable if $\varphi^* = 0$.

Proposition 0.2 *Pick $\omega \in \Omega_C$, where Ω_C is a 1-dimensional $K(C)$-vector space. Let P be a point on C, t_P a uniformizer at P. Then we can write $\omega = g\,dt_P$, for $g, t_P \in \bar{K}(C)$.*

Definition 0.3 *Define $\mathrm{ord}_P(\omega) := \mathrm{ord}_P(g)$. This is independent of the choice of t_P.*

Definition 0.4 *Define*

$$div(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega) \cdot [P].$$

We can show that for all but finitely many P, $\mathrm{ord}_P(\omega) = 0$ and so $div(\omega) \in Div(C)$. Now, $\omega_2 = f \cdot \omega$ is also a generator of Ω_C (1-dimensional) and $div(\omega_2) = div(f \cdot \omega) = div(f) + div(\omega)$. So, $div(\omega)$ depends on ω, but its projection to $\mathrm{Pic}(C) = \mathrm{Div}(C)/div(\bar{K}(C))$ does not.

Definition 0.5 *We define the* ***Canonical Class of*** *C to be $K_C = div(\omega) \in \mathrm{Pic}(C)$.*

Example Let $C = \mathbb{P}^1$. We have $\bar{K}(C) = \bar{K}(t)$, $\Omega_{\mathbb{P}^1} = \bar{K}(t)dt$, $df(t) = f'(t)dt$. Let $\omega = dt$. For all points $\lambda \neq \infty$ in $\mathbb{P}^1$, the uniformizer is $t_\lambda = t - \lambda$,

$$\frac{\omega}{dt_\lambda} = \frac{\omega}{d(t-\lambda)} = \frac{dt}{d(t-\lambda)} = 1,$$

and $\mathrm{ord}_\lambda(dt) = 0$. If $\lambda = \infty$, the uniformizer is $t_\infty = 1/t$,

$$\frac{\omega}{dt_\infty} = \frac{dt}{d(\frac{1}{t})} = -t^2,$$

so $\mathrm{ord}_\infty(dt) = \mathrm{ord}_\infty(-t^2) = -2$. Therefore, $K_{\mathbb{P}^1} = -2[\infty]$, $t^2 = t_\infty^{-2}$, so $K_{\mathbb{P}^1} = -2$, $\mathrm{Pic}(\mathbb{P}^1) \cong \mathbb{Z}$.

Example Let $C = y^2 = (x-e_1)(x-e_2)(x-e_3)$. $P_i = (e_i : 0 : 1)$.

$$\begin{aligned} div(y) &= [P_1] + [P_2] + [P_3] - 3[\infty] \\ div(x - e_i) &= 2[P_i] - 2[\infty] \end{aligned}$$

Let $w = dx$, $P = P_i$. We have $\mathrm{ord}_{P_i}(y) = 1$.

$$\begin{aligned} \mathrm{ord}_{P_i}(\omega) &= \mathrm{ord}_{P_i}\left(\frac{dx}{dy}\right) \\ 2ydy &= \sum_{i<j}(x-e_i)(x-e_j)dx \\ \implies \frac{dx}{dy} &= \frac{2y}{\sum_{i<j}(x-e_i)(x-e_j)} \\ \mathrm{ord}_{P_i}\left(\frac{dx}{dy}\right) &= \mathrm{ord}_{P_i}(y) - \mathrm{ord}_{P_i}\left(\sum_{i<j}(x-e_i)(x-e_j)\right) = 1 \end{aligned}$$

If $P \notin \{P_1, P_2, P_3, \infty\}$, $\mathrm{ord}_P(dx) = 0$.

Finally, if $P = \infty$ we use projective coordinates X, Y, Z with $x = X/Z$ and $y = Y/Z$. Then we previously computed that $\mathrm{ord}_\infty(Z) = 3$ and $\mathrm{ord}_\infty(X) = 1$ and so $\mathrm{ord}_\infty(x) = -2$. We choose $t_\infty = x^{-1/2}$ as a uniformizer. Then

$$\mathrm{ord}_\infty(\omega) = \mathrm{ord}_\infty \frac{dx}{dx^{-1/2}} = \mathrm{ord}_\infty - 2x^{3/2} = -3$$

and so we deduce that

$$div(\omega) = [P_1] + [P_2] + [P_3] - 3[\infty] = div(y)$$

Therefore $div(\omega) = 0$ in $\mathrm{Pic}(C)$ and the canonical class is therefore trivial.

1 Riemann-Roch

Definition 1.1 *$D = \sum n_P[P] \in \mathrm{Div}(C)$. Say $D \geq 0$ if $n_P \geq 0$ for all P.*

$$\begin{aligned} \mathscr{L}(D) &= \left\{f \in \bar{K}(C)^\times - 0 \,|\, div(f) \geq -D\right\} \\ &= \{f \,|\, \forall P, \mathrm{ord}_P(f) \geq -n_P\} \end{aligned}$$

If $n_P < 0$, f has a zero of order at least n_P at P. If $n_P > 0$, f has a pole of order at most n_P at P. $\mathscr{L}(D)$ is a finite-dimensional $\bar{K}$-vector space.

Remark: Let $s \in C(\bar{K})$,

$$\begin{aligned} \mathcal{O}_s &= \{f \,|\, f \text{ has a pole at } s\text{, no other pole}\} \\ D &= \sum_{P \in S}[P] \\ \mathscr{L}(nD) &= \{f \text{ pole of order at most } n \text{ at } P \in S,\ \text{no other pole}\} \\ \mathcal{O}_s &= \bigcup_{n \geq 1}\mathscr{L}(nD) \end{aligned}$$

Theorem 1.2 *Riemann-Roch Let $\ell(D) = \dim_{\bar{K}} \mathscr{L}(D)$.*

(1) $\ell(D)$ depends only on the image of D in $\mathrm{Pic}(C)$.

(2) $\ell(0) = 1$. *If* $\deg(D) < 0$, *then* $\ell(D) = 0$.

(3) There exists a $g \in \mathbb{Z}$ *called the genus of* C. *Furthermore,*

$$\ell(D) - \ell(K_C - D) = \deg(D) - g + 1$$

Proof (1)

$$\begin{aligned} \mathscr{L}(D) &\to \mathscr{L}(D + div(f)) \\ g &\mapsto g/f \end{aligned}$$

(2) $f \in \mathscr{L}(D)$, $f : C \to \mathbb{P}^1$. If $D = 0$, $div(f) \geq 0$ so there are no poles. f is not surjective if and only if f is constant. Thus, $\mathscr{L}(0) = \bar{K}$. Suppose $\deg D < 0$. Then $f \in \mathscr{L}(D)$, $div(f) \geq -D$, and $\deg(div(f)) \geq \deg(-D) > 0$ implies $f = 0$.

Corollary 1.3 *(1)* $\ell(K_C) = g$

(2) $\deg(K_C) = 2g - 2$

(3) If $\deg D > 2g - 2$, *then* $\ell(D) = \deg(D) - g + 1$.

Proof (1) $\ell(0) - \ell(K_C) = 0 - g + 1 \implies \ell(K_C) = g$.

(2) $\underbrace{\ell(K_C)}_{g} - \underbrace{\ell(0)}_{1} = \deg K_C - g + 1 \implies \deg K_C = 2g - 2$.

(3) We know $\ell(D) - \ell(K_C - D) = \deg D - g + 1$. Since $\deg(K_C - D) = \deg(K_C) - \deg(D) = 2g - 2 - \deg D < 0$. So $\ell(K_C - D) = 0$ and the result follows.

Example If $C = \mathbb{P}^1$, $g_{\mathbb{P}^1} = 0$, and $\deg(K_{\mathbb{P}^1}) = -2$. If E is an elliptic curve, $g_E = 1$, so $\deg(K_E) = 0$

Application of Riemann-Roch: If $s \neq 0$, $\mathcal{O}_S \supsetneq \bar{K}$. Pick $n > \frac{2g-2}{\#s}$. Then $\deg(nD) = n\#s > 2g - 2$. It follows $\ell(nD) = n\#s - g + 1 \geq g$. So for $n \gg 0$, $\dim_{\bar{K}} \mathscr{L}(nD) > 1$. So $\mathscr{L}(nD) \supsetneq \bar{K}$. $\mathscr{O}_s = \bigcup_{n \geq 1} \mathscr{L}(nD) \supsetneq \bar{K}$.

2 Elliptic Curves and Weierstrass Equations

Definition 2.1 *E is an elliptic curve over K is a smooth projective curve of genus 1 containing a point 0.*

Proposition 2.2 *There exists*

$$\begin{aligned} E &\hookrightarrow \mathbb{P}^2 \\ 0 &\mapsto \infty \end{aligned}$$

such that E is the vanishing of the Weierstrass equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

where $x = \frac{X}{Z}$, $y = \frac{Y}{Z}$ *are the affine coordinates of* $\mathbb{P}^2$ *(projective coordinates* $(X : Y : Z)$*).*

Proof We compute

$$\begin{aligned} \mathscr{L}(2[0]) &= 2. \\ \ell(3[0]) &= \deg[3 \cdot 0] - g + 1 \\ \mathscr{L}(2[0]) &= \bar{K} \oplus x \cdot \bar{K} \\ \ell(3[0]) &= \deg[3 \cdot 0] - g + 1 \\ \mathscr{L}(3[0]) &= \bar{K} \oplus x\bar{K} \oplus y\bar{K}, \ x, y \in \bar{K}(E) \end{aligned}$$

where the last line comes from the fact that $\mathscr{L}(2[0]) \subset \mathscr{L}(3[0])$.

Define the map:

$$\begin{aligned} &E \hookrightarrow \mathbb{P}^2 \\ &P \mapsto (x(P) : y(P) : 1) \text{ for } P \neq 0 \\ &0 \mapsto \infty = (0 : 1 : 0). \end{aligned}$$

Since $\div(x) \geq -2[0]$ and $\div(y) \geq -3[0]$ it follows that $1, x, x^2, x^3, xy, y, y^2 \in \mathscr{L}(6[0])$, where $\dim \mathscr{L}(6[0]) = 6$. Thus the 7 functions $1, x, x^2, x^3, xy, y, y^2$ satisfy a linear dependence. This linear dependence has the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

for some $a_i \in K$ and is called a Weierstrass equation for E.