Elliptic Curves

Chris Dare, Stephen Timmel

Virginia Polytechnic Institute and State University

July 20, 2019

Sections

I - Canonical Bundle

I - Canonical Bundle

Module of Rel. Differentials

Let $f : \operatorname{Spec} R \to \operatorname{Spec} S$ be a morphism of affine schemes and define the R-module $\Omega_{R/S}$ to be the free R-module generated by $\{dr : r \in R\}$ modulo the relations

(i) $d(r_1 + r_2) = dr_1 + dr_2$ for $r_1, r_2 \in R$

(ii) **(Leibniz Rule)** $d(r_1 r_2) = r_1 dr_2 + dr_1 r_2$ for $r_1, r_2 \in R$

(iii) $ds = 0$ for all $s \in S$

I - Canonical Bundle

More generally:

Sheaf of Rel. Differentials

Let $f : X \to Y$ be a morphism of schemes. Let $\Delta : X \to X \times_Y X$ be the diagonal morphism and $\mathcal{I}$ its ideal sheaf. Then the **Sheaf of Relative Differentials** is the sheaf $\Omega_{X/Y} = \Delta^*(\mathcal{I}/\mathcal{I}^2)$

Note: The Module of Relative Differentials and Sheaf of Relative Differentials are the same on affine open sets.

I - Canonical Bundle

Tangent + Canonical Bundle

Let X be a smooth n-dimensional scheme, and suppose X is smooth (i.e. $\Omega_{X/k}$ is locally free of rank n). We define the **tangent bundle** $\mathcal{T}_X = \Omega_{X/k}^{\vee}$ and the **canonical bundle** $\omega_X = \bigwedge^n \Omega_{X/k}$.

I - Canonical Bundle

Lemma

Let $X = Z(f)$ *be a smooth hyper-surface of degree* d *in* $\mathbb{P}^n$*. Then the cotangent bundle* Ω_X *is determined by the short exact sequence*

$$0 \to \mathcal{O}_X(-d) \to i^*\Omega_{\mathbb{P}^n/k} \xrightarrow{i^*} \Omega_{X/k} \to 0$$

The tangent bundle $\mathcal{T}_X$ *is determined by the short exact sequence*

$$0 \to \mathcal{T}_X \to i^*\mathcal{T}_{\mathbb{P}^n} \to \mathcal{O}_X(d) \to 0$$

I - Canonical Bundle

Idea of Proof

- *The first map is given by* $\phi \mapsto d(f\phi)$. *If* $d(f\phi) = 0$ *then* $fd\phi = \phi df \Rightarrow f$ *is a factor of* $\phi \Rightarrow \phi \equiv 0$ *on* $\mathcal{O}_X(-d)$. i^* *is known to be surj. by previous examples. Since* $f = 0$ *on* X *we know* $\ker(\textit{first map}) = \textit{im}\, i^*$.

I - Canonical Bundle

Idea of Proof

- *The first map is given by* $\phi \mapsto d(f\phi)$. *If* $d(f\phi) = 0$ *then* $fd\phi = \phi df \Rightarrow f$ *is a factor of* $\phi \Rightarrow \phi \equiv 0$ *on* $\mathcal{O}_X(-d)$. i^* *is known to be surj. by previous examples. Since* $f = 0$ *on* X *we know* $\ker(\mathit{first\ map}) = \mathit{im}\, i^*$.
- *Taking duals gives second short exact sequence.*

I - Canonical Bundle

Recall the following lemma from [2]:

Lemma

Let X be a smooth curve. Then there is an isomorphism of Abelian groups

$$\{Line\ bundles\ \mathcal{L}\ on\ X\} \leftrightarrow Pic X$$

I - Canonical Bundle

Using previous lemma

- One commonly refers to K_X as the **canonical divisor** of ω_X, mapped to under this isomorphism

I - Canonical Bundle

Using previous lemma

- One commonly refers to K_X as the **canonical divisor** of ω_X, mapped to under this isomorphism
- We define the geometric genus p_g to be $\dim_k \Gamma(X, \omega_X)$

I - Canonical Bundle

Normal Bundle

Let $Y \subset X$ be an irreducible closed subscheme defined by sheaf of ideals $\mathcal{I}$. If Y is non-singular, $\mathcal{I}/\mathcal{I}^2$ is locally free and we refer to

$$\mathcal{N}_{Y/X} = (\mathcal{I}/\mathcal{I}^2)^\vee = \mathrm{Hom}_{\mathcal{O}_Y}(\mathcal{I}/\mathcal{I}^2, \mathcal{O}_Y)$$

as the **Normal Bundle** [3]

I - Canonical Bundle

Adjunction Formula

There is an exact sequence

$$0 \to \mathcal{I}/\mathcal{I}^2 \xrightarrow{\delta} \Omega_{X/k} \otimes \mathcal{O}_Y \to \Omega_{Y/k} \to 0$$

where δ sends germ of function to germ of differential.
By taking dual,

$$0 \to \mathcal{T}_Y \to \mathcal{T}_X \otimes \mathcal{O}_Y \to \mathcal{N}_{Y/X} \to 0$$

I - Canonical Bundle

Adjunction Formula

Taking top dimensional powers,

$$\bigwedge^n \mathcal{T}_X \otimes \mathcal{O}_Y \simeq \bigwedge^n \mathcal{T}_Y \otimes \mathcal{N}_{Y/X}$$

But dual commutes with exterior powers, so

$$\bigwedge^n \mathcal{T}_Y \simeq \bigwedge^n \mathcal{T}_X \otimes \mathcal{O}_Y \otimes \mathcal{I}/\mathcal{I}^2 \tag{1}$$

I - Canonical Bundle

Adjunction Formula

If $\mathcal{L}$ is invertible sheaf on X then $\mathcal{I}_Y \simeq \mathcal{L}^{-1}$ so

$$\mathcal{I}/\mathcal{I}^2 \simeq \mathcal{L}^{-1} \otimes \mathcal{O}_Y \Rightarrow \mathcal{N}_{Y/X} \simeq \mathcal{L} \otimes \mathcal{O}_Y$$

Taking duals in (1) gives adjunction formula

$$\omega_Y \simeq \omega_X \otimes \mathcal{N}_{Y/X}$$

I - Canonical Bundle

From 3264 [1]:

Corollary

If $Y \subset X$ *is a non-singular curve in a complete surface* X *then*

$$deg\, K_Y = deg\left((K_X + [Y])[Y]\right)$$

I - Canonical Bundle

Example

- Take $X = \mathbb{P}^n$ and $U_i = \{x_i \neq 0\}$. If $X_0, \ldots, X_n$ coordinates for $\mathbb{P}^n$, $x_k = \frac{X_k}{X_i}$ on U_i (for $k \neq i$), then top dimensional form $\omega|_{U_i}$ is

$$\omega|_{U_i} = dx_0 \wedge \cdots \wedge dx_n$$

I - Canonical Bundle

Example

- Take $X = \mathbb{P}^n$ and $U_i = \{x_i \neq 0\}$. If $X_0, \ldots, X_n$ coordinates for $\mathbb{P}^n$, $x_k = \frac{X_k}{X_i}$ on U_i (for $k \neq i$), then top dimensional form $\omega|_{U_i}$ is

$$\omega|_{U_i} = dx_0 \wedge \cdots \wedge dx_n$$

- If $y_k = \frac{X_k}{X_j}$ on U_j, we have transition functions

$$g_{i,j}(x_k) = \begin{cases} y_k/y_i & k \neq j \\ 1/y_i & k \neq j \end{cases}$$

I - Canonical Bundle

Example

- Gives differential

$$dg_{i,j}(x_k) = \begin{cases} \frac{1}{y_i} dy_k - \frac{y_k}{y_i^2} dy_i & k \neq j \\ \frac{-1}{y_i^2} dy_i & k = j \end{cases}$$

I - Canonical Bundle

Example

- Gives differential

$$dg_{i,j}(x_k) = \begin{cases} \frac{1}{y_i} dy_k - \frac{y_k}{y_i^2} dy_i & k \neq j \\ \frac{-1}{y_i^2} dy_i & k = j \end{cases}$$

- Gives pushforward

$$\begin{aligned} g^*(\omega|_{U_i}) &= g^*(dx_1 \wedge \cdots \wedge dx_n) \\ &= \frac{(-1)^n}{y_i^{n+1}} dy_1 \wedge \cdots \wedge dy_n \end{aligned}$$

I - Canonical Bundle

Example

- If $H = Z(X_i) \subset X = \mathbb{P}^n$ is any hyperplane, we have

$$\mathrm{Div}\,(\omega) = (-n-1)H$$

and

$$K_{\mathbb{P}^n} = (-n-1)\zeta$$

where $\zeta \in A^1(\mathbb{P}^n)$ is class of hyperplane, and lastly

$$\omega_{\mathbb{P}^n} \simeq \mathcal{O}_{\mathbb{P}^n}(-n-1)$$

I - Canonical Bundle

Alternatively: [3]

- For $X = \mathbb{P}^n$ and $Y = \operatorname{Spec} A$, Euler's exact sequence is

$$0 \to \Omega_{X/Y} \to \mathcal{O}_X(-1)^{\oplus n+1} \to \mathcal{O}_X \to 0$$

I - Canonical Bundle

Alternatively: [3]

- For $X = \mathbb{P}^n$ and $Y = \operatorname{Spec} A$, Euler's exact sequence is

$$0 \to \Omega_{X/Y} \to \mathcal{O}_X(-1)^{\oplus n+1} \to \mathcal{O}_X \to 0$$

- Taking dual gives us

$$0 \to \mathcal{O}_X \to \mathcal{O}_X(1)^{\oplus n+1} \to \mathcal{T}_X \to 0$$

since $\omega_X = \bigwedge^{n+1} \Omega_{X/Y}$, we take $n+1$ exterior product of first sequence to give us isomorphism $\omega_{\mathbb{P}^n} \simeq \mathcal{O}_{\mathbb{P}^n}(-n-1)$

II - Characterization of Elliptic Curve

II - Characterization of Elliptic Curve

Definition (Elliptic Curve)

A **curve** over a field k is an integral scheme C of finite type with $\dim C = 1$.

We say that C is an **elliptic curve** if $\deg C = 3$.

- In particular, we consider elliptic plane curves $C \subset \mathbb{P}^2$

II - Characterization of Elliptic Curve

Canonical Bundle of Elliptic Curve

- Adjunction Formula: for a non-singular irreducible closed subscheme $Y \subset X$ of codimension 1, have

$$\omega_Y \simeq \omega_X \otimes \mathcal{N}_{Y/X} \simeq \omega_X \otimes \mathcal{O}_X(Y)|_Y$$

II - Characterization of Elliptic Curve

Canonical Bundle of Elliptic Curve

- Adjunction Formula: for a non-singular irreducible closed subscheme $Y \subset X$ of codimension 1, have

$$\omega_Y \simeq \omega_X \otimes \mathcal{N}_{Y/X} \simeq \omega_X \otimes \mathcal{O}_X(Y)|_Y$$

- [3] When $X = \mathbb{P}^n$ ($n \geq 2$) and Y is non-singular hypersurface of degree d,

$$\omega_Y \simeq \omega_{\mathbb{P}^n}(Y)|_Y = \mathcal{O}_Y(d - n - 1)$$

II - Characterization of Elliptic Curve

Canonical Bundle of Elliptic Curve

Since any elliptic plane curve $C \subset \mathbb{P}^2$ has $d = \deg C = 3$ then

$$\omega_C \simeq \mathcal{O}_C$$

and

$$p_g(C) = \dim \Gamma(C, \omega_C) = \dim \Gamma(C, \mathcal{O}_C) = 1$$

II - Characterization of Elliptic Curve

Application to Physics

- A separated, smooth scheme X of finite type is said to be **Calabi-Yau** if

$$c_1(\mathcal{T}_X) = 0 \Leftrightarrow \omega_X \simeq \mathcal{O}_X$$

II - Characterization of Elliptic Curve

Application to Physics

- A separated, smooth scheme X of finite type is said to be **Calabi-Yau** if

$$c_1(\mathcal{T}_X) = 0 \Leftrightarrow \omega_X \simeq \mathcal{O}_X$$

- The only complex Calabi-Yau 1-folds are elliptic curves

II - Characterization of Elliptic Curve

First Chern Class of Curve

Let $X \subset \mathbb{P}^2$ be a curve and $\mathcal{E} = \mathcal{L}(D)$ be the invertible sheaf associated to some divisor D

- By definition we have $\Omega_{X/k} = \mathcal{L}(K_X) \Rightarrow \mathcal{T}_X = \Omega_{X/k}^{\vee} = \mathcal{L}(-K_X)$

II - Characterization of Elliptic Curve

First Chern Class of Curve

Let $X \subset \mathbb{P}^2$ be a curve and $\mathcal{E} = \mathcal{L}(D)$ be the invertible sheaf associated to some divisor D

- By definition we have $\Omega_{X/k} = \mathcal{L}(K_X) \Rightarrow \mathcal{T}_X = \Omega_{X/k}^\vee = \mathcal{L}(-K_X)$
- Recall $c_1(\mathcal{E}^\vee) = -c_1(\mathcal{E})$ for locally free sheaf $\mathcal{E}$

II - Characterization of Elliptic Curve

First Chern Class of Curve

Let $X \subset \mathbb{P}^2$ be a curve and $\mathcal{E} = \mathcal{L}(D)$ be the invertible sheaf associated to some divisor D

- By definition we have $\Omega_{X/k} = \mathcal{L}(K_X) \Rightarrow \mathcal{T}_X = \Omega^{\vee}_{X/k} = \mathcal{L}(-K_X)$
- Recall $c_1(\mathcal{E}^{\vee}) = -c_1(\mathcal{E})$ for locally free sheaf $\mathcal{E}$
- Since $\dim X = 1$, have $\Omega_{X/k} = \omega_x$

II - Characterization of Elliptic Curve

First Chern Class of Curve

Then

$$c_1(\mathcal{T}_X) = c_1(\mathcal{L}(-K_X)) = -c_1(\mathcal{L}(K_X)) = -c_1(\omega_X) = -K_X$$

From above (and [1]) we know that

$$K_X = (d - n - 1)\zeta$$

where $\zeta = c_1(\mathcal{O}_X(1)) \in A^1(X)$ class of hyperplane section.
Then

$$c_1(\mathcal{T}_X) = (n + 1 - d)\zeta$$

III - Riemann-Roch

III - Riemann-Roch

- So far, we have characterized elliptic curves as the simplest members of the broader space of Calibi-Yau schemes.
- There are more specific things we can say about elliptic curves, but we will need to rely heavily on the Riemann-Roch Theorem to prove anything useful (also Riemann-Hurwitz).
- Notation in this section will blend Perrin [4], Gathmann [2] and Hartshorne [3]

III - Riemann-Roch

Sheaf Cohomology

As described in [4], taking global sections of the exact sequence of $\mathcal{O}_X$-modules

$$0 \to \mathcal{F} \to \mathcal{G} \to \mathcal{H} \to 0$$

yields an exact sequence

$$0 \to \Gamma(X, \mathcal{F}) \to \Gamma(X, \mathcal{G}) \xrightarrow{\pi} \Gamma(X, \mathcal{H})$$

where π need not be a surjection.

III - Riemann-Roch

Čech complexes

- Given a sheaf $\mathcal{F}$ on the scheme X and fixed open cover $\{U_i\}$, define an abelian group

$$C^P(\mathcal{F}) = \prod_{i_0 < \ldots < i_p} \mathcal{F}(U_{i_0} \cap U_{i_1} \cap \ldots \cap U_{i_p})$$

where $\alpha \in C^p$ is a collection of independent sections $\alpha_{i_0,\ldots,i_p}$ of $\mathcal{F}$.

III - Riemann-Roch

Čech complexes

- Define a boundary operator $d^p : C^p \to C^{p+1}$ composed of the sections

$$(d^p\alpha)_{i_0,i_1,\dots,i_{p+1}} = \sum_{k=0}^{p+1} (-1)^k \alpha_{i_0,\dots,i_{k-1},i_{k+1},\dots,i_{p+1}}\Big|_{U_{i_1}\cap U_{i_2}\cap\dots\cap U_{i_{p+1}}}$$

- The $(-1)^k$ term guarantees that $d^{p+1} \circ d^p = 0$, so we know $\ker(d^{p+1}) \subset \mathrm{im}(d^p)$
- In general, this inclusion is strict, so no exact sequence yet.

III - Riemann-Roch

Čech complexes

- We can force the d^p to form an exact sequence by taking a quotient
- Defining $H^p(X, \mathcal{F}) = \ker(d^p)/\mathrm{im}(d^{p-1})$ and defining the degenerate cases $p < 0$ using $C^p = 0$ and $d^p = 0$, we get $H^0(X, \mathcal{F}) = \Gamma(\mathcal{F})$ and the exact sequence

$$0 \to \Gamma(\mathcal{F}) \to \Gamma(\mathcal{G}) \to \Gamma(\mathcal{H}) \to H^1(X, \mathcal{F}) \to H^1(X, \mathcal{G}) \to \ldots$$

  (proved by diagram chasing)
- This embeds the exact sequence we wanted in an infinite sequence of unknown terms.

III - Riemann-Roch

Additional Remarks

- This construction gives the same result independent of open cover
- Proof idea from §8.5 of [2]
  - First show that affine schemes satisfy $H^i(X, \mathcal{F}) = 0$ for $i > 0$

III - Riemann-Roch

Additional Remarks

- This construction gives the same result independent of open cover
- Proof idea from §8.5 of [2]
  - First show that affine schemes satisfy $H^i(X, \mathcal{F}) = 0$ for $i > 0$
  - The restriction map from $\tilde{H}^p(X, F)$ defined on the open cover $\{U_0, U_1, \ldots, U_n\}$ to $H^p(X, F)$ defined on the open cover $\{U_1, U_2, \ldots, U_n\}$ is an isomorphism

III - Riemann-Roch

Additional Remarks

- This construction gives the same result independent of open cover
- Proof idea from §8.5 of [2]
  - First show that affine schemes satisfy $H^i(X, \mathcal{F}) = 0$ for $i > 0$
  - The restriction map from $\tilde{H}^p(X, F)$ defined on the open cover $\{U_0, U_1, \ldots, U_n\}$ to $H^p(X, F)$ defined on the open cover $\{U_1, U_2, \ldots, U_n\}$ is an isomorphism
  - By repeated application of the above, we can add and remove any number of open sets from the cover.

III - Riemann-Roch

Motivation

- Since curves have dimension 1, we know that $\dim_k H^i(X, \mathcal{F}) = 0$ for $i > 1$ [4]
- To use our long exact sequence, we need some knowledge of $\dim_k H^1(X, \mathcal{F})$
- Riemann-Roch will help us evaluate the difference $\dim_k H^0(X, \mathcal{F}) - \dim_k H^1(X, \mathcal{F})$
- We will need some additional knowledge of $\dim_k H^1(X, \mathcal{F})$ when we apply the formula [2]

III - Riemann-Roch

The Riemann-Roch Theorem

If C is an irreducible projective curve of degree d and genus g, we have for all n the relation of graded components

$$\dim_k H^0(C, \mathcal{O}_C(n)) - dim_k H^1(C, \mathcal{O}_C(n)) = nd + 1 - g$$

III - Riemann-Roch

Proof (mostly from [4] VIII.1.5)

- Let $A = k[X_0, \dots, X_n]/I(C)$ and note that A has associated sheaf $\mathcal{O}_C$
- Let H be some hyperplane not containing C, and suppose the equation of H corresponds to $h \in A$
- Defining ϕ to be multiplication by h, we get the exact sequence

$$0 \to A(-1) \xrightarrow{\phi} A \to A/(h) \to 0$$

III - Riemann-Roch

- Mapping this sequence to sheaves and shifting by n, we get

$$0 \to \mathcal{O}_C(n-1) \xrightarrow{\phi} \mathcal{O}_C(n) \to \mathcal{O}_{C\cap H}(n) \to 0$$

- If we define for convenience

$$\chi(\mathcal{O}_C(n)) = dim_k H^0(C, \mathcal{O}_C(n)) - dim_k H^1(C, \mathcal{O}_C(n))$$

our exact sequence gives us the relation

$$\chi(\mathcal{O}_C(n)) = \chi(\mathcal{O}_C(n-1)) + \chi(\mathcal{O}_{C\cap H}(n))$$

III - Riemann-Roch

- Since C has dimension 1, the intersection $C \cap H$ has dimension 0 and consists of finitely many points
- By dimensionality, $dim_k H_1(C, \mathcal{O}_C) = 0$ and we know that $dim_k H_0(C, \mathcal{O}_C) = dim_k \Gamma(\mathcal{O}_C) = d$.
- Simplifying and using induction, we get

$$\chi(\mathcal{O}_C(n)) = \chi(\mathcal{O}_C(n-1)) + d$$

$$\chi(\mathcal{O}_C(n)) = \chi(\mathcal{O}_C) + nd$$

III - Riemann-Roch

- This leaves the expansion of $\chi(\mathcal{O}_C)$.
- We have the identity

$$H^0(C, \mathcal{O}_C) = \Gamma(\mathcal{O}_C) = k$$

since the only functions over all of $\mathcal{O}_C$ are constant.

- Therefore, $dim_k H^0(C, \mathcal{O}_C) = 1$.

III - Riemann-Roch

- The last term $dim_k H^1(C, \mathcal{O}_C)$ is sometimes used as an alternate definition of the arithmetic genus
- We are used to the arithmetic genus being the constant term of the Hilbert Polynomial.
- To relate these two forms, we start with another form of the Hilbert polynomial $P(n)$ given in [3]

$$P(n) = \chi(\mathcal{F}(n)) = \sum_i (-1)^i dim_k H^i(X, \mathcal{F}(n))$$

III - Riemann-Roch

- The constant term of this expression can be calculated as

$$g = \sum_{i=0}^{r-1} (-1)^i dim_k H^{r-i}(C, \mathcal{O}_C)$$

- In dimension 1, this simplifies to $g = H^1(C, \mathcal{O}_X)$
- Combining the terms we have already described, we get

$$dim_k H^0(C, \mathcal{O}_C(n)) - dim_k H^1(C, \mathcal{O}_C(n)) = nd + 1 - g$$

III - Riemann-Roch

Related Theorems

There are a number of equivalent statements that are commonly associated to Riemann-Roch (most easily proved using Serre duality)

- Let K be a canonical divisor

$$dim_k H^0(D) - dim_k H^0(K - D) = deg(D) + 1 - g$$

- (Riemann) For large n, we have

$$dim_k(C, \mathcal{O}_C(n)) = nd + 1 - g$$

IV - Rieman-Hurwitz

IV - Rieman-Hurwitz

Motivation

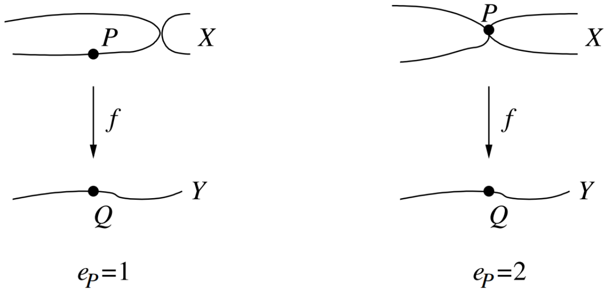
- So far, we have developed tools for understanding the dimension of global sections over sheaves
- Riemann-Hurwitz gives a similar set of tools for individual points through the ramification divisor.

IV - Rieman-Hurwitz

Ramification

- Recall that for smooth curves the Picard group of divisors is isomorphic to the set of line bundles Pic'
- Given a smooth map $f : X \to Y$ we can define a pullback map on divisors by pulling back the associated line bundles
- Given a point P, we can treat its image $f(P)$ as a divisor. This lets us compute the subscheme $f^{-1}(f(P))$
- The dimension of this subscheme is the ramification index e_P at P.

IV - Rieman-Hurwitz



- A point is unramified if its index is 1, and ramified otherwise.
- We will assume a field of characteristic 0 in this section

IV - Rieman-Hurwitz

Ramification Divisor

- Define $\Omega_{X/Y}$ as before
- The Ramification Divisor is defined to be

$$R = \sum_{P \in X} len(\Omega_{X/Y})_P \cdot P$$

- We will demonstrate that this formal sum contains ramified points counted with their ramification.

IV - Rieman-Hurwitz

Riemann-Hurwitz

(Riemann-Hurwitz) Let $f : X \to Y$ be a finite separable morphism of curves and $n = degf$. Then

$$2g(X) - 2 = n \cdot (2g(Y) - 2) + degR$$

Additionally, $degR$ satisfies

$$degR = \sum_{P \in X} (e_P - 1)$$

IV - Rieman-Hurwitz

Proof idea

- The following sequence is exact

$$0 \to f^*\Omega_Y \to \Omega_X \to \Omega_{X/Y} \to 0$$

- From this sequence, $\Omega_{X/Y}$ is supported on the ramification points of f.

IV - Rieman-Hurwitz

If f has ramification index e at P we substitute $t = au^e$ for unit a and differentiate

$$dt = aeu^{e-1}du + u^e da$$

Finding the highest power with nonzero coefficient gives

$$length(\Omega_{X/Y})_P = e - 1$$

Note: We just proved the second part of the theorem

IV - Rieman-Hurwitz

- Let K_X, K_Y be canonical divisors. Using the same kind of local calculation as before, we can show (as in [2]) that

$$K_X = f^* K_Y + R$$

IV - Rieman-Hurwitz

- To convert this equation into the first part of the theorem, note by Riemann-Roch that the canonical divisor has degree $2g-2$ (substitute $D=K$ into the alternate form)

$$dim_k H^0(K) - dim_k H^0(K-K) = deg(K) + 1 - g$$

- Noting that f^* multiplies degrees by $n = deg(f)$, we expand

$$degK_X = deg(f^*K_Y) + deg(R)$$

$$2g(X) - 2 = n(2g(Y)-2) + deg(R)$$

V - Properties of Elliptic Curves

V - Properties of Elliptic Curves

- So far, we have largely avoided discussing elliptic curves
- The general theorems we have proved can be applied to demonstrate some interesting properties of elliptic curves
- We conclude by showing that the family of elliptic curves over $\mathbb{P}^n$ is indexed by k

V - Properties of Elliptic Curves

The j-invariant

- The canonical parameterization $\phi : P^1 \rightarrow K$ onto an elliptic curve has ramified points where the curve has branch points.
- Given a branch point P_0, consider the divisor $2P_0$.
- The linear system of equivalent divisors has dimension 1 by Riemann-Roch (alternate form), so it induces a map $f : X \rightarrow P^1$ with degree 2.
- Applying Riemann-Hurwitz to the map f gives four ramified points.

V - Properties of Elliptic Curves

The j-invariant

- We change coordinates to fix $f(P^1) = \infty$.
- If the other two points are a, b we apply the following transformation, which fixes ∞ and sends a, b to $0, 1$

$$x' = \frac{x - a}{b - a}$$

V - Properties of Elliptic Curves

The j-invariant

- We now have an elliptic curve with branch points $0, 1, \infty, \lambda$ for some λ
- Define a function on λ

$$j(\lambda) = 2^8 \frac{(\lambda^2 - \lambda + 1)^3}{\lambda^2(\lambda - 1)^2}$$

- The 2^8 is a convenience that produces non-singular values over characteristic 2, and the remaining terms are chosen so j is an invariant, unique property of the curve K

V - Properties of Elliptic Curves

Claim

1. The value j does not depend on the choice of λ for a given curve K
2. The value j is unique to a curve K (two curves are isomorphic iff they have the same j)
3. The family of elliptic curves covers all possible j

V - Properties of Elliptic Curves

Proof Idea

1. Consider two morphisms f_1, f_2. By diagram chasing, we can find automorphisms τ_1, τ_2 so that f_1 and $\tau_2^{-1} f_2 \tau_1$ send the same branch point to infinity.
   To check permutations of the other three branch points, we can permute $0, 1, \lambda$ by σ and find a map ϕ to transform $\sigma 0, \sigma 1$ back to $0, 1$. The values $\phi(\sigma(\lambda))$ are generated by the actions
   $$\lambda \to 1/\lambda \qquad \lambda \to 1 - \lambda$$
   so we check that j preserves these actions

V - Properties of Elliptic Curves

3 Given a $j' \in K$, we can solve the original equation to find a value of λ with $j(\lambda) = j'$. The equation $y^2 = x(x-1)(x-\lambda)$ is an elliptic curve with $j(\lambda) = j'$

V - Properties of Elliptic Curves

2 We proceed by proving an important lemma that will render the original assertion trivial.

Lemma: Fix a branch point P_0. There is a closed immersion $K \to \mathbb{P}^2$ whose image is

$$y^2 = x(x-1)(x-\lambda)$$

This map sends P_0 to infinity, and this λ is the same as before up to the transformation $\phi \circ \sigma$ described earlier.

V - Properties of Elliptic Curves

Proof of Lemma

- We start by generating a map from the closed immersion sending the set of divisors equivalent to $3P_0$ to P^2 (this has dimension 2 by Riemann-Roch)
- We also know by the alternate form of Riemann-Roch that $dimH^0(\mathcal{O}(nP^0)) = n$ (taking nP^0 as a divisor).
- Considering the inclusion

$$H^0(\mathcal{O}(2P_0)) \subset H^0(\mathcal{O}(3P_0) \subset H^0(\mathcal{O}(6P_0)$$

we can choose x, y so $1, x$ is a basis for $H^0(\mathcal{O}(2P_0))$ and $1, x, y$ is a basis for $H^0(\mathcal{O}(3P_0))$

V - Properties of Elliptic Curves

- The monomials that can show up in an elliptic curve are $1, x, y, x^2, xy, x^3, y^2$ and are all contained in $H^0(\mathcal{O}(6P_0))$, so they cannot be linearly independent
- Our monomials only describe an elliptic curve when x^3, y^2 both appear with nonzero coefficient, and we can scale the coordinate system so both have coefficient 1.
- Writing down an arbitrary linear dependence and completing the square gives

$$y^2 = (x-a)(x-b)(x-c)$$

V - Properties of Elliptic Curves

- We can apply the same linear transformation used to derive j to send a, b to $0, 1$. This gives the final result

$$y^2 = x(x-1)(x-\lambda)$$

- Both curves have a pole at P_0 by construction, which is sent to ∞.
- Projecting from P_0 to the x-axis gives a morphism sending P_0 to infinity and ramified at the points $0, 1, \lambda, \infty$, so λ is one of the branch points in our other derivation.

V - Properties of Elliptic Curves

Using the Lemma

Finishing our proof of (2):

- j is a rational function of degree 6 which induces a map $\lambda \to j$ of degree 6.
- This covering is Galois because the functional spaces have automorphism group S_3.
    - We already noted that specific elements of the automorphism group correspond to permutations of the finite branch points.
- Therefore, $j(\lambda) = j(\lambda')$ iff λ, λ' are related by an automorphism and the proof is complete.

David Eisenbud and Joe Harris.
3264 & All That Intersection Theory in Algebraic Geometry.
Cambridge: Cambridge University Press, 2016.

Andreas Gathmann.
Algebraic Geometry.
University of Kaiserslautern, 2002.

Robin Hartshorne.
Algebraic Geometry.
Springer-Verlag New York, 1977.

Daniel Perrin.
Algebraic geometry: an introduction.
Springer Science & Business Media, 2007.