Math 6170 C, Lecture on March 9, 2020

Yongchang Zhu

Plan.

(1) Computations about curve $y^2 = (x - e_1)(x - e_2)(x - e_3)$

(2). Chapter III, $\S$ 1. Weierstrass Equations

(3). Chapter III, $\S$ 2. The Group Law

Computations about Curve $C : y^2 = (x - e_1)(x - e_2)(x - e_3)$

Assume $\mathrm{Char}\, K \neq 2$, e_1, e_2, e_3 are distinct.

$$P_1 = (e_1, 0), \quad P_2 = (e_2, 0), \quad P_3 = (e_3, 0)$$

Finite points but not P_1, P_2, P_3:

$$(a, b), \quad a \neq e_1, e_2, e_3, \quad b^2 = (a - e_1)(a - e_2)(a - e_3).$$

Points at infinite: $[0, 1, 0]$

$$y^2 z = (x - e_1 z)(x - e_2 z)(x - e_3 z)$$

Set $z = 0$, $0 = x^3$, $x = 0$. We get $[0, 1, 0]$.

C is a smooth curve.

The function field of C is

$$\mathrm{Frac}\,\bar{K}[x,y]/(y^2-(x-e_1)(x-e_2)(x-e_3)).$$

It is a quadratic extension of $\bar{K}(x)$ by the equation:

$$y^2=(x-e_1)(x-e_2)(x-e_3)$$

Uniformizers:

At P_i, $i = 1, 2, 3$, y is a uniformizer.

At a finite point $(a, b) \neq P_1, P_2, P_3$,

$$x - a$$

is a uniformizer.

At $\infty = [0,1,0]$, x/y is a unifomizer.

Set $y = 1$ in $y^2 z = (x - e_1 z)(x - e_2 z)(x - e_3 z)$, we get

$$z = (x - e_1 z)(x - e_2 z)(x - e_3 z)$$

$x = 0, z = 0$ corresponds to ∞.

The function field is

$$\operatorname{Frac} \bar{K}[x, z]/(z - (x - e_1 z)(x - e_2 z)(x - e_3 z))$$

x is a uniformizer. This x corresponds to x/y in

$$\operatorname{Frac} \bar{K}[x, y]/(y^2 - (x - e_1)(x - e_2)(x - e_3)).$$

Another proof that x/y is uniformizer at ∞:

Using $\deg \operatorname{div}(x) = 0$, we get $\operatorname{ord}_\infty x = -2$,

Using $\deg \operatorname{div}(y) = 0$, we get $\operatorname{ord}_\infty y = -3$,

so

$$\operatorname{ord}_\infty (x/y) = \operatorname{ord}_\infty x - \operatorname{ord}_\infty y = 1.$$

Computation of $\mathrm{div}(dx/y)$

By definition,

$$\mathrm{div}(dx/y) = \sum_{P \in C} \mathrm{ord}_P(dx/y)(P).$$

To compute

$$\mathrm{ord}_P(\omega)$$

we find a uniformizer t at P,
and write

$$\omega = fdt$$

Then

$$\mathrm{ord}_P(\omega) \stackrel{\mathrm{def}}{=} \mathrm{ord}_P(f)$$

For $P = (a, b)$, $a \neq e_1, e_2, e_3$, $b \neq 0$.

$x - a$ is a uniformizer at P, $d(x - a) = dx$,

$$dx/y = \frac{1}{y} d(x - a),$$

$$1/y|_P = 1/b$$

so $\mathrm{ord}_P(dx/y) = 0$.

For $P = (e_1, 0)$, y is a uniformizer at P.

$$y^2 = (x - e_1)(x - e_2)(x - e_3)$$

implies that

$$2ydy = ((x - e_1)(x - e_2)(x - e_3))' \, dx$$

$$dx/y = \frac{2dy}{((x - e_1)(x - e_2)(x - e_3))'}$$

So we see that

$$\mathrm{ord}_P(dx/y) = 0.$$

Similarly for $P = (e_2, 0), (e_3, 0)$,

$$\mathrm{ord}_P(dx/y) = 0.$$

For $P = \infty$, x/y is a uniformizer.

$$d(x/y) = y^{-1}dx - y^{-2}dy = \left(1 - \frac{1}{2}y^{-2}\left((x-e_1)(x-e_2)(x-e_3)\right)'\right) dx/y$$

$$dx/y = \left(1 - \frac{1}{2}y^{-2}\left((x-e_1)(x-e_2)(x-e_3)\right)'\right)^{-1} d(x/y)$$

$$\left(1 - \frac{1}{2}y^{-2}\left((x-e_1)(x-e_2)(x-e_3)\right)'\right)|_{\infty} = 1$$

$$\mathrm{ord}_{\infty}(dx/y) = 0$$

This proves $\mathrm{ord}_P(dx/y) = 0$ for all $P \in C$.

So $\mathrm{div}(dx/y) = 0$.

Recall that $\mathrm{div}(f\omega) = \mathrm{div}(f) + \mathrm{div}(\omega)$

$$\mathrm{div}(fdx/y) = \mathrm{div}(f)$$

Recall that $\omega \in \Omega_C$ is called a holomorphic differential if $\mathrm{div}(\omega) \geq 0$.

The space of holomorphic differentials on C is a vector space over $\bar{K}$.

The space of holomorphic differentials on C is $\{f dx/y\}$ with $\mathrm{div}(f) \geq 0$.

It is $\bar{K} dx/y$, one dimensional. So the genus of C is $g = 1$.

The curve C: the projective closure of $y^2 = (x - e_1)(x - e_2)(x - e_3)$
$(e_1, e_2, e_3$ are distinct, $\mathrm{char}\,\bar{K} \neq 2)$
is an example elliptic curve over $\bar{K}$.

The Geometry of Elliptic Curves.

Definition. An **elliptic curve** over $\bar{K}$ is a pair (E, O), where E is a smooth curve with genus one and $O \in E$.

The elliptic curve (E, O) is defined over K if E is defined over K and $O \in E(K)$.

Proposition III 3.1.

Let (E, O) be an elliptic curve over K. Then E is isomorphic to the curve in $\mathbb{P}^2$ defined by an equation

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

with coefficients $a_1, \ldots, a_6 \in K$ and $O = [0, 1, 0]$.

The above equation is called **Weierstrass equation.**

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

If $\mathrm{char}(\bar{K}) \neq 2$, we complete the square of

$$\begin{aligned} y^2 + a_1xy + a_3y \quad &= y^2 + 2y(\frac{1}{2}x + \frac{1}{2}a_3) \\ &= (y + \frac{1}{2}x + \frac{1}{2}a_3)^2 - (\frac{1}{2}x + \frac{1}{2}a_3)^2 \end{aligned}$$

We replace y by $y - \frac{1}{2}x - \frac{1}{2}a_3$, and the equation is simplified to

$$E : y^2 = x^3 + b_2x^2 + 2b_4x + b_6$$

b_i's are polynomials of a_i's

For example: $b_6 = a_3^2 + 4a_6$.

If further $\mathrm{Char}(\bar{K}) \neq 2, 3$,

We replace x by $x - \frac{1}{3}b_2$, the equation is simplified to

$$E : y^2 = x^3 - 27c_4x - 54c_6.$$

Recall for a cubic equation

$$x^3 + px + q = 0$$

has multiple roots iff

$$-4p^3 - 27q^2 = 0$$

which is a multiple of $c_4^3 - c_6^2$ up to a product of powers of 2 and 3.

For

$$E : y^2 = x^3 - 27c_4x - 54c_6.$$

$\mathrm{char}(\bar{E}) \neq 2, 3.$
We define $\Delta = \Delta(E)$ as

$$1728\Delta = c_4^3 - c_6^2$$

$$1728 = 3^2 2^6$$

E is smooth iff $\Delta(E) \neq 0$. And (E, O) is an elliptic curve, where $O = \infty$.

Theorem If $\mathrm{Char}(K) \neq 2, 3$, then every elliptic curve over K can be expressed in the form (E, O), where E is given by the equation

$$E : y^2 = x^3 - 27c_4x - 54c_6$$

with

$$\Delta = 1728^{-1}(c_4^3 - c_6^2) \neq 0$$

and $O = \infty$.

The j-invariant of above E is defined as

$$j = j(E) = \frac{c_4^3}{\Delta}.$$

Proposition.

Two elliptic curves are isomorphic over $\bar{K}$ iff their j-invariant are equal.

A line in $\mathbb{P}^2$ is the variety defined by a homogeneous linear equation

$$AX + BY + CZ = 0$$

A, B, C are not all 0.

Two equations

$$AX + BY + CZ = 0, \quad A'X + B'Y + C'Z = 0$$

gives the same line iff

$$(A, B, C) = \lambda(A', B', C')$$

Example:

$$2X + Y - Z = 0$$

defines a line in $\mathbb{P}^2(\mathbb{C})$.

Its points are affine line $2X + Y - 1 = 0$ together with the extra point

$$[1, -2, 0]$$

at infinity.

Theorem. Two different lines in $\mathbb{P}^2$ intersects at a unique point.

Theorem.

Suppose $C : F(X, Y, Z) = 0$ (in $\mathbb{P}^2$, F is irreducible) is a smooth curve over $\bar{K}$ defined by a homogeneous equation of degree $d > 1$, then any line intersect with C at exactly d points (counting multiplicity).

It follows from

Theorem.

$$x^d + a_{n-1}x^{d-1} + \cdots + a_0 = 0$$

has exactly d solutions (counting multiplicity).

Homogeneous version of the above theorem:

Theorem. If $G(X, Y)$ is a homogeneous polynomial of degree d, then

$$G(X, Y) = 0$$

has exactly d solutions in $\bar{K}$ (counting multiplicity).

Proof. We have factorization $G(X, Y) = \Pi_{i=1}^{d}(A_i X + B_i Y)$.

A line can be expressed as

$$(X, Y, Z) = s(a_1, a_2, a_3) + t(b_1, b_2, b_3)$$

substitute it to $F(X, Y, Z) = 0$, we get

$$F(a_1 s + b_1 t, a_2 s + b_2 t, a_3 s + b_3 t) = 0$$

Because F is irreducible, $F(a_1 s + b_1 t, a_2 s + b_2 t, a_3 s + b_3 t) \neq 0$ and is a homogeneous polynomial of s, t with degree d, so it has d solutions.

If $\deg F = 2,\ C : F(X, Y, Z) = 0$,
and we know one solutions (a_1, a_2, a_3), then we know all the solutions.

Take a line $L(b_1, b_2, b_3) : (X, Y, Z) = s(a_1, a_2, a_3) + t(b_1, b_2, b_3)$,

$$L(b_1, b_2, b_3) \cap C$$

$$F(a_1 s + b_1 t, a_2 s + b_2 t, a_3 s + b_3 t) = 0$$

We already know one solution $s = 1, t = 0$, we can find the other solution.

If $\deg F = 3,\ C : F(X, Y, Z) = 0$,
and we know twos solutions $[a_1, a_2, a_3], [b_1, b_2, b_3]$, then we can find new solutions using the intersection.

Take a line $L : (X, Y, Z) = s(a_1, a_2, a_3) + t(b_1, b_2, b_3)$,

$$L \cap C$$

$$F(a_1 s + b_1 t, a_2 s + b_2 t, a_3 s + b_3 t) = 0$$

We already know one solution $(s, t) = (1, 0)$ and $(s, t) = (0, 1)$, we can find the other solution.

Definition.

Let (E, O) be an elliptic curve over K given by a Weierstrass equation. $P \in E(K)$, let L be the line connect O and P,

$$L \cap E = (O, P, Q)$$

We define $Q = -P$.

Definition.

Let (E, O) be an elliptic curve over K given by a Weierstrass equation. $P, Q \in E(K)$, let L be the line connect P and Q,

$$L \cap E = (P, Q, R)$$

We define $P + Q = -R$.

Theorem

. $E(K)$ is an abelian group under $+$ and O is the identity element.

When $P, Q \in E$, and $P = Q$, "the line connecting P and Q means the tangent line at P.

End