Math 6170 C, Lecture on March 11, 2020

Yongchang Zhu

Plan.

(1) Review of Chapter III § 1.

(2) Chapter III § 2. The Group Law (continued)

(3). Chapter III § 3. Elliptic Curves

Reivew of III § 1.

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 a **Weierstrass equation.**

Conversely if

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$$

is smooth, then it is an elliptic curve with $O = [0, 1, 0]$.

If $\mathrm{Char}(\bar{K}) \neq 2, 3$, the equation of E can simplified to

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

A curve defined by the above equation is smooth iff

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

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.

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

Example: the affine lines $X + Y - 1 = 0$ and $X + Y - 2 = 0$ don't intersect. Their projective closures

$$L_1 : X + Y - Z = 0, \quad L_2 : X + Y - 2Z = 0$$

intersect at $[1, -1, 0]$.

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).

This follows from the following theorem:
Theorem. If $G(X, Y)$ is a homogeneous polynomial of degree d, then

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

has exactly d solutions in $\mathbb{P}^1$ (counting multiplicity).

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

Solutions are $[-B_i, A_i]$.

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

$$F(a_1 s + b_1 t, a_2 s + b_2 t, a_3 s + b_3 t) = 0 \tag{1}$$

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.

The multiplicity of a point P in the intersection is the multiplicity of its corresponding solution $[s, t]$ of (1).

Let (E, O) be an elliptic curve over K given by a Weierstrass equation. So $E \in \mathbb{P}^2$ with equation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ + a_6Z^3.$$

For any line $L \subset \mathbb{P}^2$, L and E intersect at 3 points (counting with multiplicity).

If E and L are both defined over K, and if two of intersection points are defined over K, then the remaining intersection point is also defined over K.

Tangent Line of a Smooth Curve.

If a smooth curve $C \subset \mathbb{P}^2$ is given by

$$C : F(X, Y, Z) = 0$$

where F is a homogeneous irreducible polynomial.

If $P = [x_0, y_0, z_0]$ is a point in C, the **tangent line** of C at P is defined as

$$L : \partial_X F(x_0, y_0, z_0)X + \partial_Y F(x_0, y_0, z_0)Y + \partial_Z F(x_0, y_0, z_0)Z = 0.$$

Proof of P is in L

:

Assume $F(X,Y,Z)$ has degree m, we have

$$F(tX,tY,tZ)=t^mF(X,Y,Z)$$

Take ∂_t and set $t=1$, we get

$$\partial_X F(X,Y,Z)X+\partial_Y F(X,Y,Z)Y+\partial_Z F(X,Y,Z)Z=mF(X,Y,Z)$$

Put $(X,Y,Z)=(x_0,y_0,z_0)$, we get

$$\partial_X F(x_0,y_0,z_0)x_0+\partial_Y F(x_0,y_0,z_0)y_0+\partial_Z F(x_0,y_0,z_0)z_0=mF(x_0,y_0,z_0)=0.$$

Our definition agrees with the affine case:

If (x_0, y_0) is a smooth point of the affine curve $f(X, Y) = 0$ in $\mathbb{A}^2$. The tangent line at (x_0, y_0) is

$$\partial_X f(x_0, y_0)(X - x_0) + \partial_Y f(x_0, y_0)(Y - y_0) = 0.$$

Lemma. Let $P = [x_0, y_0, z_0]$ be a point in the elliptic curve $E \subset \mathbb{P}^2$ with a Weierstrass equation $F(X, Y, Z) = 0$, L be the tangent line of E at P, then multiplicity of P in the intersection $E \cap L$ is at least 2.

Proof.

L has equation

$$F_X(x_0, y_0, z_0)X + F_Y(x_0, y_0, z_0)Y + F_Z(x_0, y_0, z_0)Z = 0.$$

Without loss of generality, we may assume $F_Z(x_0, y_0, z_0) = C \neq 0$. The points in L are parameterized by

$$[X, Y, Z] = [X, Y, -C^{-1}F_X(x_0, y_0, z_0)X - C^{-1}F_Y(x_0, y_0, z_0)Y]$$

Substitute this to the equation of E, we have

$$F(X, Y, -C^{-1}F_X(x_0, y_0, z_0)X - C^{-1}F_Y(x_0, y_0, z_0)Y) = 0$$

Proof (continued).

We need to prove $[X, Y] = [x_0, y_0]$ is a solution of $G(X, Y) = 0$ with multiplicity ≥ 2, where

$$G(X, Y) = F(X, Y, -C^{-1}F_X(x_0, y_0, z_0)X - C^{-1}F_Y(x_0, y_0, z_0)Y)$$

It is equivalent to prove

$$G_X(x_0, y_0) = G_Y(x_0, y_0) = 0$$

which can be proved by a direct computation.

Tangent Line of E at O

The elliptic curve (E, O) with equation

$$E : Y^2Z + a_1XYZ + a_3YZ^2 - (X^3 + a_2X^2Z + a_4XZ + a_6Z^3) = 0$$

and $O = [0, 1, 0]$. The tangent line at O is

$$L : Z = 0$$

The points in L are $[X, Y, 0]$.
To find $L \cap E$, we solve the equation

$$G(X, Y) = -X^3 = 0$$

The solution is $X = 0$ with multiplicity 3.

$$L \cap E = \{O, O, O\}$$

$P \in E(K)$, let L be the line connect O and P (if $P = O$, L is the tangent line at O). Let

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

We define $Q = -P$.

By the previous example, we have

$$-O = O.$$

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 (if $P = Q$, L is the tangent line at P),

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

We define $P + Q = -R$.

Proposition III.2.2.

$E(K)$ is an abelian group under $+$ and O is the identity element. The inverse of P is $-P$.

If E is a curve defined by a Weierstrass equation $F(X, Y, Z) = 0$ that is NOT smooth. Then $O = [0, 1, 0] \in E$ is a smooth point and there is only one singular point, the set $E_{ns}(K)$ of smooth points over K is an abelian group under $+$ with identity element O.

One first define $Q \mapsto -Q$ and then define $+$ as before.

To prove $E_{ns}(K)$ is closed under $-$ and $+$, we use the follow Exercise.

Exercise. If a line L intersects E at the singular point P, then the multiplicity is at least 2.

Recall Riemann-Roch Theorem.

Let C be a smooth curve with genus g, $D \in \mathrm{Div}(C)$, $K \in \mathrm{Div}(C)$ is a canonical divisor. Then

$$l(D) - l(K - D) = \deg D + 1 - g.$$

If C is defined over $K \subset \bar{K}$. A divisor $D \in \mathrm{Div}(C)$ is rational over K if it $G_{\bar{K}/K}$-invariant.

Then

$$\mathcal{L}(D) = \{f \in \bar{K}(C) \mid \mathrm{div}(f) \geq -D\}$$

is K-rational, that is,

$$\mathcal{L}_K(D) = \{f \in K(C) \mid \mathrm{div}(f) \geq -D\}$$

$$\dim_K \mathcal{L}_K(D) = \dim_{\bar{K}} \mathcal{L}(D).$$

Proposition III 3.1.

Let (E, O) be an elliptic curve defined over K.
(a) There exist functions $x, y \in K(C)$ such that the map

$$\phi : E \to \mathbb{P}^2 : \qquad \phi(P) = [x(P), y(P), 1]$$

gives an isomorphism of E/K onto a curve given by a Weierstrass equation

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

with coefficients $a_1, \ldots, a_6 \in K$ and such that $\phi(O) = [0, 1, 0]$.

(b) (c) (skipped)

Proof.

Consider divisor $D = n(O)$, $g = 1$, so $\deg K = 2g - 2 = 0$. By R-R theorem

$$l(D) - l(K - D) = \deg D + 1 - g = n$$

Because $\deg(K - D) = -n < 0$, so $l(K - D) = 0$. So $l(n(O)) = n$. That is

$$\mathcal{L}_K(n(O)) = \{f \in K(C) \,|\, \operatorname{div} f \geq -n(O)\}$$

is n-dimensional over K.

It is clear that

$$\mathcal{L}_K(1(O)) \subset \mathcal{L}_K(2(O)) \subset \mathcal{L}_K(3(O)) \subset \dots$$

and

$$f \in \mathcal{L}_K(m(O)), \quad g \in \mathcal{L}_K(n(O))$$

implies that

$$fg \in \mathcal{L}_K((m+n)O)$$

1 is a basis for $\mathcal{L}_K(1(O))$, let $x, y \in K(E)$ be such that

$$\{1, x\}$$

is a basis of $\mathcal{L}_K(2(O))$, and

$$\{1, x, y\}$$

is a basis of $\mathcal{L}_K(3(O))$.

$$\mathrm{ord}_O(x) = -2, \quad \mathrm{ord}_O(y) = -3.$$

Then

$$1, x, y, x^2, xy, y^2, x^3$$

are in $\mathcal{L}_K(6(O))$ which has dimension 6.

So we have

$$A_1 + A_2x + A_3y + A_4x^2 + A_5xy + A_6y^2 + A_7x^3 = 0$$

for some A_i's in K.

It is easy see that that $A_6 \neq 0$ and $A_7 \neq 0$. By replacing x with cx and y with dy, we assume $A_6 = 1$ and $A_7 = -1$.

So x, y satisfy a Weierstrass equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6. \tag{2}$$

We denote by C the projective curve in $\mathbb{P}^2$ defined by the equation (2).

We have a morphism

$$\phi : E \to \mathbb{P}^2, \quad \phi(P) = [x(P), y(P), 1]$$

The image is in C, we have a morphism

$$\phi : E \to C.$$

The function field of C is $K(x, y) \subset K(C)$.

$$[K(C) : K(x)] = 2$$

$$[K(C); K(y)] = 3$$

so

$$[K[C] : K(x, y)]$$

is a common divisor of 2 and 3, so $[K[C] : K(x, y)] = 1$.

This proves $K(C) = K(x, y)$.

To prove ϕ is an isomorphism, it remains to prove C is smooth.

If not, there is a morphism $\psi : C \to \mathbb{P}^1$ of degree one 1.

this means $\phi \circ \psi : E \to \mathbb{P}^1$ has degree one. because E and $\mathbb{P}^1$ are both smooth, so E is isomorphic to $\mathbb{P}^1$. Contradicts to $g(E) = 1$.

$\square$

Lemma 3.3.

Let E be a curve of genus one, $P, Q \in E$, then $(P) \sim (Q)$ iff $P = Q$.

Proof. If $(P) \sim (Q)$, there is $f \in \bar{K}(C)^*$ such that

$$\mathrm{div}(f) = (P) - (Q)$$

so $f \in \mathcal{L}((Q))$, by R-R, $\dim \mathcal{L}((Q)) = 1$, $1 \in \mathcal{L}((Q))$ so $f \in \bar{K}^*$. So $P = Q$.

Proposition III 3.4.

The abelian group E and $\mathrm{Pic}^0(E)$ are isomorphic. The isomorphism $\kappa : E \to \mathrm{Pic}^0(E)$ is given as

$$P \mapsto \text{class of } (P) - (O).$$

The proof needs the following result:

$$V \stackrel{\text{def}}{=} \{aX + bY + cZ \mid a, b, c \in \bar{K}\}$$

For each $0 \neq f = aX + bY + cZ \in V$, $P \in E$, we define $\mathrm{ord}_P f$ as follows.

We choose $g \in V$ such that $g(P) \neq 0$, then $f/g \in \bar{K}(E)$,

$$\mathrm{ord}_P(f/g)$$

is independent of the choice of g, we define

$$\mathrm{ord}_P f \stackrel{\text{def}}{=} \mathrm{ord}_P(f/g).$$

It is easy to see that for almost all $P \in E$, $\mathrm{ord}_P f = 0$.
We define

$$\mathrm{div}(f) = \sum_{P \in E} \mathrm{ord}_P f \ (P)$$

$$\mathrm{div}(f) \in \mathrm{Div}(E).$$

Lemma. If $0 \neq f = aX + bY + cZ$ and the line $L : aX + bY + cZ = 0$ intersects to E at P, Q, R (counting with multiplicity), then

$$\operatorname{div} f = (P) + (Q) + (R).$$

This lemma is used to prove $\kappa : E \to \mathrm{Pic}^0(E)$ is a group homomorphism.

End