Math 6170 C, Lecture on March 30, 2020

Yongchang Zhu

Plan

(1) III. § 9. The Endomorphism Ring

(2) IV. A Brief Summary

(3) V. §1. The Number of Rational Points over Finite Fields

Recall that an **anti-involution** of a ring R is a map

$$\tau : R \to R$$

such that

$$\tau(a+b) = \tau(a) + \tau(b), \quad \tau(ab) = \tau(b)\tau(a), \quad \tau(1) = 1.$$

$$\tau^2 = \tau \circ \tau = \mathrm{Id}.$$

Example 1. $R = \mathbb{C}$, $\tau(z) = \bar{z}$ is an anti-involution.

Example 2. $R = M_n(k)$, $n \times n$ matrices over a field k,

$$\tau(a) = a^T$$

is an anti-involution.

Let E/K be an elliptic curve. The ring $\mathrm{End}(E)$ has the following properties:

(1) $\mathrm{End}(E)$ is a characteristic 0 integral domain, and $\mathrm{rank}_{\mathbb{Z}} \mathrm{End}(E) \leq 4$.

(2) There is an anti-involution on $\mathrm{End}(E)$, $\phi \mapsto \hat{\phi}$.

(3) $\phi\hat{\phi} \in \mathbb{Z}_{\geq 0}$, $\phi\hat{\phi} = 0$ iff $\phi = 0$.

The above properties implies that $\mathrm{End}(E)$ is isomorphic to one of the following rings:

(1) $\mathbb{Z}$.
(2) An order in a quadratic imaginary field $\mathbb{Q}(\sqrt{-d})$.
(3) An order in a quaternion algebra over $\mathbb{Q}$.

Definition. Let A be a finite dimensional $\mathbb{Q}$-algebra (not necessarily commutative). An **order** in A is a subring R (be definition, any subring contains 1) satisfying the following properties:

(1). R is a finitely generated $\mathbb{Z}$-module.

(2). $\mathrm{rank}_{\mathbb{Z}} R = \dim_{\mathbb{Q}} A$.

Example. $A = \mathbb{Q}$, $\mathbb{Z}$ is the unique order in $\mathbb{Q}$.

Example. $A = \mathbb{Q}(\sqrt{-d})$, where $d \in \mathbb{Z}_{>0}$ is a square free.

$\dim_{\mathbb{Q}} A = 2$.

For any positive integer N, $R_N = \mathbb{Z} + \mathbb{Z}N\sqrt{-d}$ is an order.

Example. $A = M_2(\mathbb{Q})$, $\dim_{\mathbb{Q}} A = 4$.

$M_2(\mathbb{Z})$ is an order.

$$L \stackrel{\text{def}}{=} \{\begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a, b, d \in \mathbb{Z}\}$$

is a subring, and finitely generated as $\mathbb{Z}$-module, but $\mathrm{rank}_{\mathbb{Z}} L = 3 \neq 4$, so it is **not** an order.

Definition. A definite quaternion algebra is a 4-dimensional algebra over $\mathbb{Q}$ of the form

$$A = \mathbb{Q} + \mathbb{Q}\alpha + \mathbb{Q}\beta + \mathbb{Q}\alpha\beta$$

with the multiplication rules:

$$\alpha^2, \beta^2 \in \mathbb{Q},\ \alpha^2 < 0,\ \beta^2 < 0,\ \alpha\beta = -\beta\alpha.$$

The above A is a division algebra over $\mathbb{Q}$.

Recall Hamilton's quaternion algebra is the algebra $\mathbb{H}$ over $\mathbb{R}$:

$$\mathbb{H} = \mathbb{R} + \mathbb{R}i + \mathbb{R}j + \mathbb{R}k$$

with multiplication rules

$$i^2 = -1, j^2 = -1, ij = -ji = k$$

A realization of $\mathbb{H}$ as a subalgebra of $M_2(\mathbb{C})$:

$$\mathbb{H} = \{ \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} \mid z, w \in \mathbb{C} \}$$

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

$$i \mapsto \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$$

$$j \mapsto \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$$

$$k \mapsto \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$$

Realization of A as a subring of $\mathbb{H}$:
Assume $\alpha^2 = -a, \beta^2 = -b, a \in \mathbb{Q}_{>0}, b \in \mathbb{Q}_{>0}$,

$$1 \mapsto \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$
$$\alpha \mapsto \begin{pmatrix} \sqrt{a}i & 0 \\ 0 & -\sqrt{a}i \end{pmatrix}$$
$$\beta \mapsto \begin{pmatrix} 0 & \sqrt{b} \\ -\sqrt{b} & 0 \end{pmatrix}$$

gives an embedding of A in $\mathbb{H} \subset M_2(\mathbb{C})$.

IV. The Formal Group of an Elliptic Curve. A Very Brief Summary.

Let R be a commutative ring. $R[[X]]$ be the ring of formal power series over R.
An element $c_0 + c_1 X + \cdots + c_n X^n + \ldots$ is a unit in $R[[X]]$ iff c_0 is a unit in R.

If $R = k$ is a field, then (X) is the unique maximal ideal of $k[[X]]$.
$\mathrm{Frac}\, k[[X]] = k((X))$, the field of formal Laurent power series over k.

$R[[X, Y]]$ be the ring of formal power series of two variables over R.
$R[[X, Y, Z]]$ be the ring of formal power series of three variables over R.

For k a field, $k[[X]], k[[X, Y]], k[[X, Y, Z]]$ are local rings.

Definition.

An **one parameter formal group over** R is a power series $F(X, Y) \in R[[X, Y]]$ satisfying

(a) $\quad F(X, Y) = X + Y + \text{higher terms.}$

(b) (associativity) $\quad F(X, F(Y, Z)) = F(F(X, Y), Z).$

(c) (commutativity) $\quad F(X, Y) = F(Y, X).$

(to be continued)

(d) (existence of inverse) There is a unique power series $i(X) \in R[[X]]$ such that

$$F(X, i(X)) = 0$$

(e) $F(X, 0) = X$ and $F(0, Y) = Y$.

Example. Let R be any commutative ring,

$$F(X, Y) = X + Y$$

is a formal group.

Example. Let R be any commutative ring,

$$F(X, Y) = X + Y + XY$$

is a formal group.

The behavior of an elliptic curve near O gives a formal group.

Let E be an elliptic curve over K given by the Weierstrass equation

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

To study the solution near O, we change coordinate:

$$z = -\frac{x}{y}, \quad w = -\frac{1}{y}$$

z is a local uniformizer at O. $\mathrm{ord}_O w = 3$.

The equation for E becomes

$$w = z^3 + a_1 zw + a_2 z^2 w + a_3 w^2 + a_4 zw^2 + a_6 w^3 \tag{1}$$

We consider the solution of (1) of the form

$$z = z_1, \quad w = z_1^3 + A_4 z_1^4 + A_5 z_1^5 + \dots$$

There are unique $A_4, A_5, \dots$ (depending on a_1, a_2, a_3, a_4, a_6) such that

$$(z_1, w_1) = (z_1, z_1^3 + A_4 z_1^4 + A_5 z_1^5 + \dots)$$

is a solution of (1).

This is a solution in ring $K[[z_1]]$.

Similarly we have a unique solution in $K[[z_2]]$ of the form

$$(z_2, w_2) = (z_2, z_2^3 + A_4 z_2^4 + A_5 z_1^5 + \dots)$$

Given solutions (z_1, w_1) and (z_2, w_2) as above, use the standard method, we get a solution $(z_1, w_1) + (z_2, w_2)$ of the form

$$(z, w) = (F(z_1, z_2), w)$$

$$F(z_1, z_2) = z_1 + z_2 + \cdots \in K[[z_1, z_2]]$$

This formal power series $F[z_1, z_2]$ is a formal group.

Chapter V. Elliptic Curves over Finite Fields

V. § 1. Number of Rational Points

Let K be a finite field with $|K| = q$, E be an elliptic curve given by the Weierstrass equation

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

For each $x = a \in K$, we have a quadratic equation of y, which has at most 2-solutions. So

$$|E(K)| \leq 2q + 1.$$

The better estimate is

$$|E(K)| \sim q + 1.$$

because the quadratic equation for y has $1/2$-chances of being solvable.

Theorem V 1.1.

Let E/K be an elliptic curves over a finite field F of q elements. Then

$$||E(K)| - q - 1| \leq 2\sqrt{q}.$$

Proof. The q-th power Frobenius morphism

$$\phi : E \to E, \ \ (x, y) \mapsto (x^q, y^q)$$

$P \in E$ is in $E(K)$ iff $\phi(P) = P$ iff $(1 - \phi)(P) = 0$. Thus

$$E(K) = \ker(1 - \phi).$$

Claim. The isogeny $1 - \phi$ is separable.
Because

$$(1 - \phi)^* \omega = 1^* \omega - \phi^* \omega = \omega \neq 0$$

Proof (continued).

Since $1 - \phi$ is separable,

$$|E(K)| = |\ker(1 - \phi)| = \deg(1 - \phi)$$

Recall $\deg : \operatorname{End}(E) \to \mathbb{R}$ is a positive definite quadratic form (Corollary III 6.3), so by the following lemma

$$|\deg(1 - \phi) - \deg(1) - \deg(\phi)| \leq 2\sqrt{\deg(1)\deg(\phi)}$$

that is

$$|\,|E(K)| - 1 - q| \leq 2\sqrt{q}.$$

Lemma V 1.2.

Let A be an abelian group and

$$\deg : A \to \mathbb{R}$$

is a positive definite quadratic form, then for all $a, b \in A$,

$$|\deg(a-b) - \deg(a) - \deg(b)| \leq 2\sqrt{\deg(a)\deg(b)}$$

We restrict deg to $L \overset{\text{def}}{=} \mathbb{Z}a + \mathbb{Z}b$, which is a positive definite quadratic form on a free abelian group of rank 1 or 2. deg extends to an inner product on vector space $L_{\mathbb{R}} = L \otimes_{\mathbb{Z}} \mathbb{R}$. The result follows from the Cauchy-Schwartz inequality on the inner product space $L_{\mathbb{R}}$.

Let K be a finite field with $|K| = q$. Let V be a projective variety. Let K_n be the degree n extension of K, so $|K_n| = q^n$.

Definition. The zeta function of V/K is the power series

$$Z(V/K, T) = \exp\Big(\sum_{n=1}^{\infty} |V(K_n)| \frac{T^n}{n}\Big)$$

$$|\mathbb{P}^N(K_n)| = \frac{q^{n(N+1)}-1}{q^n-1} = \sum_{i=0}^{N} q^{ni}$$

$$Z(\mathbb{P}^N/K, T) = \frac{1}{(1-T)(1-qT)\cdots(1-q^NT)}.$$

End