Any two Weierstrass equations for the same elliptic curve E over K are related by substitutions of the form

$$\begin{aligned} x &= u^2x' + r \\ y &= u^3y' + u^2sx' + t \end{aligned}$$

where $u, r, s, t \in K$ with $u \neq 0$. The coefficients a_i' of the new Weierstrass equation are related to the coefficients a_i of the old via

$$\begin{aligned} ua_1' &= a_1 + 2s \\ u^2a_2' &= a_2 - sa_1 + 3r - s^2 \\ u^3a_3' &= a_3 + ra_1 + 2t \\ u^4a_4' &= a_4 - sa_3 + 2ra_2 - (rs+t)a_1 + 3r^2 - 2st \\ u^6a_6' &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1. \end{aligned} \tag{3}$$

The various associated quantities are transformed by

$$\begin{aligned} u^2b_2' &= b_2 + 12r \\ u^4b_4' &= b_4 + rb_2 + 6r^2 \\ u^6b_6' &= b_6 + 2rb_4 + r^2b_2 + 4r^3 \\ u^8b_8' &= b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \end{aligned} \tag{4}$$

and $u^4c_4' = c_4$, $u^6c_6' = c_6$, $u^{12}\Delta' = \Delta$, $j' = j$.

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on (1) with $P_1, P_2, P_1 + P_2 \neq 0_E$. Then $P_3 = P_1 + P_2 = (x_3, y_3)$ is given by

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\ y_3 &= -(\lambda + a_1)x_3 - \nu - a_3 \end{aligned}$$

where if $x_1 \neq x_2$ then

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1},$$

and if $x_1 = x_2$ then

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}$$

and

$$\nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}.$$

It is sometimes convenient to work with formulae in x only. Specialising to the shorter Weierstrass form (2), assuming $P_1 \neq P_2$, and putting $P_4 = P_1 - P_2 = (x_4, y_4)$, we obtain

$$\begin{aligned} x_3 + x_4 &= \frac{2(x_1x_2 + a)(x_1 + x_2) + 4b}{(x_1 - x_2)^2}, \\ x_3x_4 &= \frac{x_1^2x_2^2 - 2ax_1x_2 - 4b(x_1 + x_2) + a^2}{(x_1 - x_2)^2}. \end{aligned}$$

PART III ELLIPTIC CURVES
FORMULA SHEET

A Weierstrass equation, over a field K, is an equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

with coefficients $a_1, \dots, a_6$ in K. If $\mathrm{char}(K) \neq 2$ then we may replace y by $\frac{1}{2}(y - a_1x - a_3)$ to obtain an equation of the form

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

where

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6.$$

If further $\mathrm{char}(K) \neq 3$ then we may replace x by $\frac{1}{36}(x - 3b_2)$ and y by $\frac{1}{108}y$ to obtain

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

where

$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

The discriminant $\Delta \in \mathbb{Z}[a_1, \dots, a_6]$ is defined by

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

where

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.$$

It can be shown that (1) defines a smooth projective curve (and hence an elliptic curve, with origin the point at infinity) if and only if $\Delta \neq 0$. If $\mathrm{char}(K) \neq 2$ then this already follows from the usual formula for the discriminant of a cubic polynomial. A separate argument is required in the case $\mathrm{char}(K) = 2$.

The following relations may also be verified

$$4b_8 = b_2b_6 - b_4^2, \quad c_4^3 - c_6^2 = 1728\Delta.$$

The j-invariant is $j = c_4^3/\Delta$.

If $\mathrm{char}(K) \neq 2, 3$ it suffices to consider elliptic curves of the form

$$y^2 = x^3 + ax + b \tag{2}$$

in which case

$$\Delta = -16(4a^3 + 27b^2), \quad j = \frac{1728(4a^3)}{4a^3 + 27b^2}.$$

Date: 17th October 2013.

Elliptic Curves ①

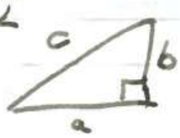
Books

1. Silverman, "The Arithmetic of Elliptic Curves", Springer 1986
2. Cassels, "Lectures on Elliptic Curves", CUP 1991
3. Silverman and Tate, "Rational Points on Elliptic Curves",
~~4.~~ Springer 1992
4. Milne, "Elliptic Curves", Booksurge 2006, available online.

1 covers some of the useful algebraic-geometry background

1. Fermat's Method of Descent

Let Δ be a triangle.



$a^2 = b^2 + c^2$ $\qquad$ $\text{area}(\Delta) = \frac{1}{2}ab$

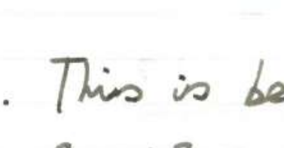
Definition

Δ is *rational* if $a, b, c \in \mathbb{Q}$.

Δ is *primitive* if $a, b, c \in \mathbb{Z}$, coprime.

Lemma 1.1

Every primitive Δ is of the form



for some $u, v \in \mathbb{Z}$, $u > v > 0$.

Proof

WLOG, a is odd and b is even. This is because if a, b are even, so is c since $a^2 + b^2 = c^2$, so a, b, c have common factor 2. Further, if a, b are both odd, $a^2 + b^2 \equiv 2 \equiv c^2 \ (4)$ $\#$

So we take a odd, b even, and c is odd.

Then $\left(\frac{b}{2}\right)^2 = \left(\frac{c+a}{2}\right)\left(\frac{c-a}{2}\right)$.

$\frac{c+a}{2}$ and $\frac{c-a}{2}$ are positive (as $c^2 = b^2 + a^2$ so $c > a$), integers (since c, a are both odd) and coprime (since $d \mid \frac{c+a}{2}, \frac{c-a}{2} \Rightarrow d \mid a, c$).

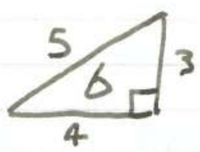
Therefore, by unique factorisation in $\mathbb{Z}$, $\frac{c+a}{2} = u^2$, $\frac{c-a}{2} = v^2$ for some $u, v \in \mathbb{Z}$.

Then $a = u^2 - v^2$, $b = 2uv$, $c = u^2 + v^2$ $\square$

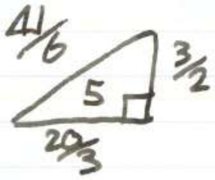
Definition

$D \in \mathbb{Q}_{>0}$ is congruent if $\exists$ a rational, right-angled triangle with area D. Scaling side lengths of a triangle by k gives area $k^2 D$. Then if $D = p/q$, $p, q \in \mathbb{Z}$, $(p,q) = 1$, $k = q$ gives area pq, and WLOG we consider $D \in \mathbb{Z}_{>0}$, squarefree.

$D = 5, 6$ are congruent.



$3^2 + 4^2 = 5^2$, $\frac{1}{2} \cdot 3 \cdot 4 = 6$



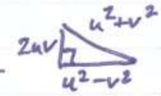
$\left(\frac{3}{2}\right)^2 + \left(\frac{20}{3}\right)^2 = \left(\frac{41}{6}\right)^2$, $\frac{1}{2} \cdot \frac{3}{2} \cdot \frac{20}{3} = 5$

Lemma 1.2

$D \in \mathbb{Q}_{>0}$ is congruent $\Leftrightarrow Dy^2 = x^3 - x$ for some $x, y \in \mathbb{Q}$, $y \neq 0$

Elliptic Curves ①

Proof

Lemma 1.1 shows that D is congruent 

just calculate the area of

$\Leftrightarrow Dw^2 = uv(u^2-v^2)$ for some $u, v, w \in \mathbb{Q}$, $w \neq 0$

Put $x = u/v$, $y = w/v^2$ $\square$

Fermat showed that 1 is not a congruent number.

Theorem 1·3

There are no solutions to $w^2 = uv(u-v)(u+v)$ $(*)$

for $u, v, w \in \mathbb{Z}$, $w \neq 0$

Proof

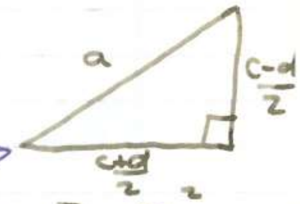
WLOG, u, v are coprime (or we can divide $(*)$ by a factor and begin again), $u > 0$ (or we switch the signs of both u and v), and $w > 0$ (or we simply switch the sign).

- If $v < 0$, replace (u, v, w) by $(-v, u, w)$
- If $u \equiv v (2)$, replace (u, v, w) by $\left(\frac{u+v}{2}, \frac{u-v}{2}, \frac{w}{2}\right)$

Then, $u+v$, $u-v$, u, v are coprime positive integers with product a square. Unique factorisation in $\mathbb{Z}$:

$\Rightarrow u = a^2$, $v = b^2$, $u+v = c^2$, $u-v = d^2$

for some $a, b, c, d \in \mathbb{Z}_{>0}$



Since $u \not\equiv v (2)$, c and d are odd.

Now $\left(\frac{c+d}{2}\right)^2 + \left(\frac{c-d}{2}\right)^2 = \frac{c^2+d^2}{2} = u = a^2$

This gives a primitive triangle, of area $\frac{c^2-d^2}{8} = \frac{v}{4} = \left(\frac{b}{2}\right)^2$

Let $w_1 = \frac{b}{2}$ (at least one of u, v is even, so WLOG,

v is even and hence b is)

Lemma 1·1 $\Rightarrow$ $w_1^2 = u_1 v_1 (u_1^2 - v_1^2)$

for some $u_1, v_1 \in \mathbb{Z}$.

$w_1^2 = u_1 v_1 (u_1^2 - v_1^2)$, another solution to $(*)$.

$4w_1^2 = b^2 = v \mid w^2 \Rightarrow w_1 \leq \frac{1}{2} w$

So by Fermat's Method of Infinite Descent, there are no solutions to $(*)$. $\square$

<u>A Variant for Polynomials</u>

(In Chapter 1, k a field, $\mathrm{char}(k) \neq 2$, algebraic closure $\bar{k}$.

<u>Lemma 1·4</u>

Let $u, v \in k[t]$ be coprime.

If $\alpha u + \beta v$ is a square for 4 distinct $(\alpha : \beta) \in \mathbb{P}^1$, then $u, v \in k$.

via Möbius transformation

<u>Proof</u>

WLOG $k = \bar{k}$. Changing coordinates on $\mathbb{P}^1$, the ratios $(\alpha : \beta)$ are $\overset{(i)}{(1:0)}$, $\overset{(ii)}{(0:1)}$, $\overset{(iii)}{(1:-1)}$ and $\overset{(iv)}{(1:-\lambda)}$ for some $\lambda \in k \setminus \{0, 1\}$.

$\Theta : (z ; 1) \mapsto (\Theta(z) ; 1)$

Mobius transformation: $\dfrac{z - \frac{\alpha_2}{\beta_2}}{z - \frac{\alpha_1}{\beta_1}} \cdot \dfrac{\frac{\alpha_1}{\beta_1} - \frac{\alpha_3}{\beta_3}}{\frac{\alpha_3}{\beta_3} - \frac{\alpha_2}{\beta_2}}$ for example

Then $u \overset{(i)}{=} a^2$, $v \overset{(ii)}{=} b^2$, $u - v \overset{(iii)}{=} (a+b)(a-b)$

$\lambda = \mu^2$, $\mu \in k$ since $k = \bar{k}$, $u - \lambda v \overset{(iv)}{=} (a + \mu b)(a - \mu b)$

Elliptic Curves ①

By unique factorisation in $K[t]$,

$a+b$, $a-b$, $a+\mu b$, $a-\mu b$ are all squares. consider (iii), (iv)

But $\max\{\deg(a), \deg(b)\} \leq \frac{1}{2}\max\{\deg(u), \deg(v)\}$

So by Fermat's Method of Descent, we have $u, v \in K$ $\square$

<u>Definition</u>

i) An elliptic curve E/K is the <u>projective closure</u> of a plane affine curve $y^2 = f(x)$ (**) where $f \in K[x]$ is a monic, cubic polynomial with distinct roots in $\bar{K}$.

(**) is called the <u>Weierstrass Equation</u>.

ii) For any field extension L/K,

$E(L) = \{(x, y) \in L^2 \mid y^2 = f(x)\} \cup \{0\}$

<u>Fact</u>

$E(L)$ is naturally an abelian group. We will study this group for L a finite field, a <u>local field</u> (finite extension of $\mathbb{Q}_p$) and a number field (finite extension of $\mathbb{Q}$).

Lemma 1·2 and 1·3

$\Rightarrow$ If $E: y^2 = x^3 - x$ then $E(\mathbb{Q}) = \{0, (0,0), (\pm 1, 0)\}$

<u>Corollary</u>

Let E/K be an elliptic curve. Then $E(K(t)) = E(K)$.

Elliptic Curves (2)

<u>Corollary 1.6</u>

Let E/k be an elliptic curve. Then $E(k(t)) = E(k)$

<u>Proof</u>

WLOG $k = \bar{k}$. By a change of coordinates, we may assume $E: y^2 = x(x-1)(x-\lambda)$, $\lambda \in k \setminus \{0,1\}$

(Change two of the roots of $f(x)$ to $0, 1$ and rescale)

Suppose $(x, y) \in E(k(t))$

Then $x = \frac{u}{v}$, for some $u, v \in k[t]$ coprime

$\Rightarrow uv(u-v)(u-\lambda v) = w^2$ for some $w \in k[t]$

(since $x = \frac{u}{v}$, $y = \frac{a}{b}$, $a, b, u, v \in k[t]$,

$\frac{a^2}{b^2} = \frac{u}{v}\left(\frac{u}{v} - 1\right)\left(\frac{u}{v} - \lambda\right)$

$\frac{a^2 v^4}{b^2} = uv(u-v)(u-\lambda v) \in k[t] \Rightarrow b = 1,\ w = av^2$)

Unique factorisation in $k[t]$

$\Rightarrow u, v, u-v, u-\lambda v$ are all squares

Lemma 1.4 $\Rightarrow u, v \in k \Rightarrow x, y \in k$ $\square$

<u>2 Some Remarks on Algebraic Curves</u>

(We assume that $k = \bar{k}$ and $\mathrm{char}(k) \neq 2$)

<u>Definition 2.1</u>

A plane affine algebraic curve $C = \{(x,y) \in \mathbb{A}^2 \mid f(x,y) = 0\}$

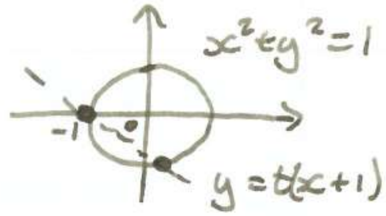
is <u>rational</u> if it has a rational parametrisation.

i.e. $\exists\ \varphi(t), \psi(t) \in k(t)$ such that

i) $\mathbb{A}^1 \to \mathbb{A}^2$, $t \mapsto (\varphi(t), \psi(t))$ is injective on $\mathbb{A}^1 \setminus \{\text{finite set}\}$

ii) $f(\varphi(t), \psi(t)) = 0$

Example 2.2



a) Any non-singular plane conic is rational.

We solve for the 2^{nd} point in the diagram:

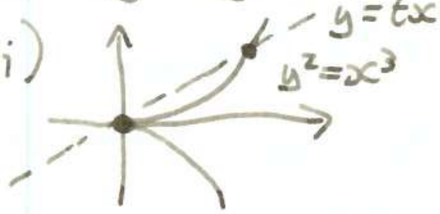
$y = t(x+1)$, $x^2+t^2(x+1)^2 = 1$

$\Rightarrow (x+1)(x-1+t^2(x+1)) = 0$

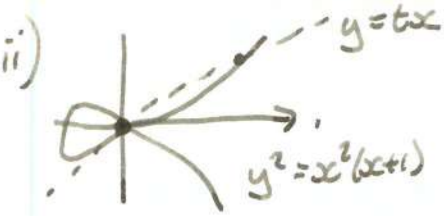
$\Rightarrow x = -1$ or $x = \frac{1-t^2}{1+t^2}$, $y = \frac{2t}{1+t^2}$

b) Any singular plane cubic is rational:

i)



ii)



As before, we solve for the 2^{nd} labelled point.

i) has parametrisation $(x,y) = (t^2, t^3)$

Corollary 1·6 shows that elliptic curves are not rational.

Remark 2.3

The genus $g(C) \in \mathbb{Z}_{\geq 0}$ is an invariant of a smooth projective curve C.

- If $k = \mathbb{C}$ then $g(C)$ = genus of the Riemann Surface
- A smooth plane curve of degree d has genus $\frac{1}{2}(d-1)(d-2)$

Proposition 2.4 ($k=\bar{k}$)

Let C be a smooth projective curve.

i) C is rational (c.f. Def 2·1) $\Leftrightarrow g(C) = 0$

ii) C is an elliptic curve (c.f. Def 1·5) $\Leftrightarrow g(C) = 1$

Elliptic Curves ②

Proof

i) Omitted

ii) "$\Rightarrow$" is Remark 2·3. "$\Leftarrow$" is covered later in the course.

Coordinate Ring $= K[X,Y]/(\text{Elliptic Curve Equation})$

Function Field $=$ Frac (Coordinate Ring)

Order of Vanishing

Let C be an algebraic curve with function field $k(C)$.

Let $P \in C$ be a smooth point (i.e. $\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}$ not both zero)

Write $\text{ord}_P(f)$ for the order of vanishing of $f \in k(C)$ at P, negative if f has a pole.

Fact

$\text{ord}_P : k(C)^* \to \mathbb{Z}$ is a discrete valuation i.e.

i) $\text{ord}_P(f_1 f_2) = \text{ord}_P(f_1) + \text{ord}_P(f_2)$

ii) $\text{ord}_P(f_1 + f_2) \geq \min(\text{ord}_P(f_1), \text{ord}_P(f_2))$

Definition

$t \in k(C)$ is a uniformiser at P if $\text{ord}_P(t) = 1$.

Example 2·5

$C = \{(x,y) \in \mathbb{A}^2 \mid g(x,y) = 0\}$ for $g \in k[\cancel{X}, Y]$, irreducible

$k(C) = \text{Frac}\, k[X,Y]/(g)$

$g = g_0 + g_1(x,y) + g_2(x,y) + \ldots$

(g_i are homogeneous polynomials of degree i)

Suppose $P = (0,0) \in C$ is a smooth point.

Then $g_0 = 0$ and $g_1(x,y) = \alpha x + \beta y$ with $\alpha, \beta \in k$, not both 0 (for smoothness).

Let $\gamma, \delta \in k$.

Fact

$\gamma x + \delta y$ is a uniformiser at $P \Leftrightarrow \alpha\delta - \beta\gamma \neq 0$

Example 2.6

$C = \{ (x,y) \in \mathbb{A}^2 \mid y^2 = x(x-1)(x-\lambda) \}$, $\lambda \in k \setminus \{0,1\}$

Projective Closure : $Y^2 Z = X(X-Z)(X-\lambda Z) \subset \mathbb{P}^2$

Let $P = (\overset{X}{0} : \overset{Y}{1} : \overset{Z}{0})$

Aim : compute $\mathrm{ord}_P(x)$, $\mathrm{ord}_P(y)$

Put $w = \frac{Z}{Y}$, $t = \frac{X}{Y}$, $w = t(t-w)(t-\lambda w)$ (*)

Now P is the point $(t, w) = (0,0)$

It is smooth and $\mathrm{ord}_P(t) = 1$.

Likewise, $\mathrm{ord}_P(t-w) = \mathrm{ord}_P(t-\lambda w) = 1$.

(*) $\Rightarrow \mathrm{ord}_P(w) = 3$

But $x = \frac{X}{Z} = \frac{t}{w} \Rightarrow \mathrm{ord}_P(x) = \mathrm{ord}_P(t) - \mathrm{ord}_P(w) = -2$

$y = \frac{Y}{Z} = \frac{1}{w} \Rightarrow \mathrm{ord}_P(y) = -\mathrm{ord}_P(w) = -3$

Projective Closure

Projective Plane:

$\mathbb{P}^2(k) = \{$equivalence classes of $(x,y,z) \in k^3$ under $(x,y,z) \sim (\lambda x, \lambda y, \lambda z), \lambda \in k \}$

Example: $F(x,y) = y^2 - x^3 + n^2 x$

"Homogenise" $\tilde{F}(x,y,z) = y^2 z - x^3 + n^2 x z^2$

Note that for $z \neq 0$,

$\tilde{F}(x,y,z) = 0 \iff F(\frac{x}{z}, \frac{y}{z}) = 0$

But using $\tilde{F}$ we can extend F to points at infinity, i.e. when $z = 0$.

This gives a "line at infinity" when x, y vary and $z = 0$

To work with normal points we use F, $F(x,y) = \tilde{F}(x,y,1)$ but to work with these new points, we put the tuple in the form $(x,1,0)$ or $(y,1,0)$ and consider points on the curve $\tilde{F}(x,1,z) = 0$ or $\tilde{F}(1,y,z) = 0$

xz plane $\qquad$ yz plane

Coordinate Ring

V an affine algebraic variety defined by equations $\{f_j(x_1, \dots, x_m) = 0 \mid j \in J\}$

Coordinate ring $R(V)$:

The quotient ring of $k[x_1, \dots, x_m]$ by $(f_1, f_2, \dots)$ (ideal generated by f_j)

50 35 15 5 0

$$5 = 35 - 2 \cdot 15$$
$$= 35 - 2(50 - 35)$$
$$= 3 \cdot 35 - 2 \cdot 50$$

Elliptic Curves ③

Riemann-Roch Spaces

Let C be a smooth projective curve.

Definition

A *divisor* is a formal sum of points on C, say $D = \sum_{P \in C} n_P P$ with $n_P \in \mathbb{Z}$, and $n_P = 0$ for all but finitely many P.

$\deg D = \sum_{P \in E} n_P$

D is *effective* (written $D \geq 0$) if $n_P \geq 0 \ \forall P$.

If $f \in k(C)^*$ then $\operatorname{div}(f) = \sum_{P \in C} \operatorname{ord}_P(f)\, P$

The Riemann-Roch space of $D \in \operatorname{div}(C)$ is   divisors of C

$\mathcal{L}(D) = \{ f \in k(C)^* \mid \operatorname{div}(f) + D \geq 0 \} \cup \{0\}$

i.e. the k-vector space of rational functions on C with "poles no worse than specified by D".

Riemann-Roch Theorem for Curves of Genus 1

$$\dim \mathcal{L}(D) = \begin{cases} \deg D & \text{if } \deg D > 0 \\ 0 \text{ or } 1 & \phantom{\text{if }} = 0 \\ 0 & \phantom{\text{if }} < 0 \end{cases}$$

Example

Let C be an elliptic curve with Weierstrass equation $y^2 = f(x)$, with P the point at ∞.

Example 2.6 $\Rightarrow \mathcal{L}(3P) = \langle 1, x, y \rangle$ → by 2.6

because these are in $\mathcal{L}(3P)$ and this has the correct dimension

Lemma 2.7

Let $C \subset \mathbb{P}^2$ be a smooth plane cubic and $P \in C$ a point of inflection. Then we can change coordinates such that

$C : Y^2 Z = X(X - Z)(X - \lambda Z)$, $\lambda \neq 0, 1$, $P = (\overset{X}{0} : \overset{Y}{1} : \overset{Z}{0})$

Proof:

We can change coordinates so that $P = (0:1:0)$ and by a translation

By rotation $T_P C = \{Z = 0\}$ (tangent line to C at P).

$C: \{F(X,Y,Z) = 0\} \subset \mathbb{P}^2$

$P \in C$ a point of inflection $\Rightarrow F(t,1,0) = \text{constant} \times t^3$

$\therefore$ no terms X^2Y, XY^2, Y^3

(because a non-zero t-term means the 'tangent line' intersects C, clearly a non-zero t^2-term will not give a point of inflection.

The constant term is 0 since $F(0,1,0) = 0$)

$F \in \langle Y^2Z, XYZ, YZ^2, X^3, X^2Z, XZ^2, Z^3 \rangle$

coefficient $\neq 0$ or $p \in C$ would be singular

coefficient $\neq 0$ otherwise C contains the line $\{Z=0\}$

We are free to rescale X, Y, Z, F.

WLOG $C: \underbrace{Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3}_{\text{(Weierstrass Form)}}$

Substituting $Y \mapsto Y - \frac{1}{2}a_1X - \frac{1}{2}a_3Z$ $(\operatorname{char} k \neq 2)$,

We may assume that $a_1 = a_3 = 0$

i.e. $C: Y^2Z = Z^3 f(X/Z)$, f some cubic polynomials

C smooth $\Rightarrow f$ has distinct roots.

WLOG, these roots are $0, 1$ and λ (by X translation and scaling)

$C: Y^2Z = X(X-Z)(X-\lambda Z)$ Legendre Form $\square$

The Degree of a Morphism

A morphism $\varphi: C_1 \to C_2$ between smooth projective curves is defined by a polynomial mapping

$\Phi: (X:Y:Z) \mapsto (\varphi_0(X,Y,Z), \varphi_1(X,Y,Z), \varphi_2(X,Y,Z))$

where the φ_i are homogeneous polynomials over K satisfying the defining equation of C_2.

Let $\varphi : C_1 \to C_2$ be a non-constant morphism of smooth projective curves. Let $\varphi^* : k(C_2) \to k(C_1)$, $f \mapsto f \circ \varphi$

Consider ideals. φ^* is a field embedding.

φ^* clearly a map $k[X,Y,Z] \hookrightarrow k[X,Y,Z]$. If f is zero in $k(C_2)$ i.e. f vanishes on C_2 then $f \circ \varphi$ vanishes on C_1 so $\varphi^* : k(C_2) \to k(C_1)$

Definition

i) $\deg \varphi = [k(C_1) : \varphi^* k(C_2)]$

ii) φ is separable if $k(C_1) / \varphi^* k(C_2)$ is separable (automatic if char $k = 0$).

N.B. φ is an isomorphism $\iff \deg \varphi = 1$

Suppose $P \in C_1$, $Q \in C_2$, $\varphi(P) = Q$

(P a point in the fibre of φ above Q).

Let $t \in k(C_2)$ be a uniformiser at Q.

Definition c.f. Riemann Surfaces ramification indices

$e_\varphi(P) = \mathrm{ord}_P(\varphi^* t)$ (always ≥ 1, independent of choice of t.)

Theorem 2·8

Let $\varphi : C_1 \to C_2$ be a non-constant morphism of smooth projective curves. Then

c.f. Riemann Surfaces

$$\sum_{P \in \varphi^{-1}(Q)} e_\varphi(P) = \deg \varphi \qquad \forall Q \in C_2.$$

Moreover, if φ is separable then $e_\varphi = 1$ for all but finitely many P. In particular

i) φ is surjective (N.B. $k=\bar{k}$)

ii) $\#\varphi^{-1}(Q) \leq \deg\varphi$ and if φ is separable then we have equality for all but finitely many $Q \in C_2$.

<u>Remark 2.9</u>

Let C be an algebraic curve.

A rational map $C \dashrightarrow \mathbb{P}^n$ is given by

$P \mapsto (f_0(P) : f_1(P) : \dots : f_n(P))$

where $f_0, f_1, \dots, f_n \in k(C)$, not all zero.

<u>Fact</u>

If C is smooth then this is automatically a morphism.

- char$(k)=p$, can take p^{th} roots

<u>3 Weierstrass Equations</u> (k a perfect field, all finite extensions are separable)

An elliptic curve E/k is a smooth projective curve of genus 1 defined over k, with a specified rational point $O_E \in E(k)$.

<u>Example</u>

$\{X^3 + pY^3 + p^2Z^2 = 0\} \subset \mathbb{P}^2$ (for p a given prime) is not an elliptic curve over $\mathbb{Q}$ since it has no $\mathbb{Q}$-rational points (descen
has to have at least one point

<u>Theorem 3.1</u>

Every elliptic curve E is isomorphic over k to a curve in Weierstrass form, via an isomorphism mapping $O_E \mapsto (0:1:0)$

<u>Remark</u>

Lemma 2.7 was the special case. E is a smooth plane cubic and O_E is a point of inflection.

Elliptic Curves 3

<u>Fact</u>

Let D be a divisor on E i.e. a formal sum of $\bar{K}$ points on E. If D is defined over K (i.e. D is fixed by the action of $Gal(\bar{K}/K)$) then $\mathcal{L}(D)$ has a basis consisting of rational functions in $K(E)$ (not just in $\bar{K}(E)$).

17/10/13

Elliptic Curves ④

Theorem 3·1

Every elliptic curve E is isomorphic over k to a curve in Weierstrass form via an isomorphism taking O_E to $(0:1:0)$

Proof

$\mathcal{L}(2O_E) \subset \mathcal{L}(3O_E)$. Pick bases:

$1, x \qquad\qquad 1, x, y$

The 7-elements $1, x, y, x^2, xy, x^3$ and y^2 in the 6 dimensional space $\mathcal{L}(6O_E)$ must satisfy a dependence relation. Leaving out either x^3 or y^2 gives a basis for $\mathcal{L}(6O_E)$ since each term has different order poles at O_E.

$\therefore$ coefficients of x^3 and y^2 are non-zero in the dependence relation

Rescaling x, y, we get

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

for some $a_i \in K$.

There is a morphism $\varphi : E \to E' \subset \mathbb{P}^2$, $P \mapsto (x(P) : y(P) : 1)$

$$\deg(E \xrightarrow{x} \mathbb{P}^1) \; (= [k(E) : k(x)]) = \operatorname{ord}_{O_E}\left(\tfrac{1}{x}\right) = 2$$

$$\deg(E \xrightarrow{y} \mathbb{P}^1) \; (= [k(E) : k(y)]) = \operatorname{ord}_{O_E}\left(\tfrac{1}{y}\right) = 3$$

because they are uniformisers

$$\begin{tikzcd} & K(E) \arrow[dl, dash, "2"'] \arrow[d, dash] \arrow[dr, dash, "3"] & \\ k(x) & k(x,y) \arrow[l, dash] \arrow[r, dash] & k(y) \end{tikzcd}$$

Tower Law $\Rightarrow K(E) = k(x, y)$

dependence relation gives $[k(x,y) : k(x)]$ and $[k(x,y) : k(y)]$

$\therefore \varphi^* K(E') = K(E)$

$\Rightarrow \deg \varphi = 1$

$\Rightarrow \varphi$ is birational.

If E' is singular, then E and E' are rational ※

So E' is smooth and φ is an isomorphism (by Remark 2·9).

$\varphi : E \to E'$, $P \mapsto \left(\frac{x}{y}(P) : 1 : \frac{1}{y}(P)\right)$

$O_E \mapsto (0:1:0)$ Have shown isomorphic to a plane cubic i.e. reduced to special case. $\square$

Proposition 3.2

Let E, E' be elliptic curves over k in Weierstrass form. Then $E \cong E'$ over $k \iff$ their equations are related by substitutions of the form:

$x = u^2 x' + r$, $y = u^3 y' + u^2 s x' + t$

for some $r, s, t, u \in k$, $u \neq 0$.

Proof $\Leftarrow$ is already clear

$\langle 1, x \rangle = \mathcal{L}(2O_E) = \langle 1, x' \rangle$

$\Rightarrow x = \lambda x' + r$, for some $\lambda, r \in k$, $\lambda \neq 0$

$\langle 1, x, y \rangle = \mathcal{L}(3O_E) = \langle 1, x', y' \rangle$

$\Rightarrow y = \mu y' + \sigma x' + t$, for some $\mu, \sigma, t \in k$, $\mu \neq 0$

Looking at coefficients of y^2 and $x^3 \Rightarrow \lambda^3 = \mu^2$

$\Rightarrow \lambda = u^2$, $\mu = u^3$, some $\underset{= \mu/\lambda}{u} \in k$

Put $s = \sigma/u^2$. $\square$

A Weierstrass equation defines an elliptic curve

$\iff$ it defines a smooth curve.

$\iff \Delta(a_1, \dots, a_6) \neq 0$

where $\Delta \in \mathbb{Z}[a_1, \dots, a_6]$ is a certain polynomial.

If $\mathrm{char}(k) \neq 2, 3$ we can reduce to the case

$y^2 = x^3 + ax + b$

with discriminant $\Delta = -16(4a^3 + 27b^2)$

17/10/13 Elliptic Curves ④

Corollary 3·3

Assume char$(k) \neq 2, 3$. Elliptic curves

$E : y^2 = x^3 + ax + b$, $E' : y^2 = x^3 + a'x + b'$

are isomorphic over $k \iff \begin{cases} a' = u^4 a \\ b' = u^6 b \end{cases}$ for some $u \in k^*$.

Proof:

E, E' are related by a substitution as in Proposition 3·2 with $r = s = t = 0$ □

Definition

The j-invariant of E is $j(E) = \frac{1728(4a^3)}{4a^3 + 27b^2}$

Corollary 3·4

$E \cong E' \Rightarrow j(E) = j(E')$

The converse holds when $k = \bar{k}$.

Proof:

$E \cong E' \iff \begin{cases} a' = u^4 a \\ b' = u^6 b \end{cases}$ for some $u \in k^*$.

$\Rightarrow (a^3 : b^2) = ((a')^3 : (b')^2)$

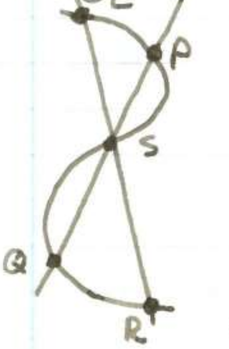
$\updownarrow$ Möbius map

$\Rightarrow j(E) = j(E')$

The converse holds if $k = \bar{k}$ (we can extract necessary roots) □

4. The Group Law

$E \subset \mathbb{P}^2$ smooth plane cubic. $O_E \in E(k)$.



$S = 3^{rd}$ point of intersection of E and line PQ

$R = 3^{rd}$ point of intersection of E and $O_E S$

We define $P \oplus Q = R$

If $P = Q$ take $T_P E$ instead of PQ and so on...

This is called the "chord and tangent Process".

Theorem 4·1

$(E, \oplus)$ is an abelian group.

Proof

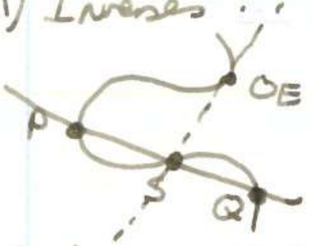
i) Commutativity is obvious since line(PQ) = line(QP).

ii) O_E is the identity: S is 3^{rd} point of intersection of E and $O_E P$.

P is 3^{rd} point of intersection of E and $O_E S$.

$O_E \oplus P = P$.

iii) Inverses: S is 3^{rd} point of intersection of E and $T_{O_E} E$



Q is 3^{rd} point of intersection of E and PS

$P \oplus Q = O_E$

iv) Associativity: Much harder!

Definition

$D_1, D_2 \in Div(E)$ are linearly equivalent (written $D_1 \sim D_2$) if

equivalence relation

$\exists f_2 \in \bar{K}(E)^*$ with $div(f) = D_1 - D_2$

Write $[D] = \{ D' \in Div(E) : D' \sim D \}$

Definition

N.B. rational functions have divisors of degree 0

$$Pic(E) = \frac{Div(E)}{\sim}, \quad Pic^\circ(E) = \frac{Div^\circ(E)}{\sim}$$

where $Div^\circ(E)$ is the group of divisors on E of degree 0.

We define $\varphi : E \to Pic^\circ(E)$, $P \mapsto [P - O_E]$

Proposition 4·2

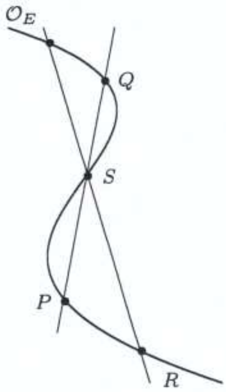
i) $\varphi(P \oplus Q) = \varphi(P) + \varphi(Q)$

ii) φ is a bijection.

Chapter 4

The Group Law

Let $E \subset \mathbb{P}^2$ be a smooth plane cubic with $\mathcal{O}_E \in E$.



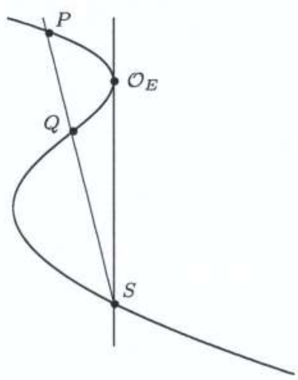
By Bezout's Theorem, E meets any line in three points, counted with multiplicity. Let $P, Q \in E$. Let $S = \overline{PQ} \cap E$, let $R = \overline{\mathcal{O}_E S} \cap E$. Define $P \oplus Q = R$. If $P = Q$, take $T_P E$ instead of $\overline{PQ}$ etc. This process is called the *chord-and-tangent process.*

Theorem 4.1. $(E, \oplus)$ is an abelian group.

Proof. (i) $P \oplus Q = Q \oplus P$.

(ii) $\mathcal{O}_E$ is the identity.

(iii) Given P, let $S = T_{\mathcal{O}_E} E \cap E$ and $Q = \overline{PS} \cap E$ then $\ominus P = Q$, i.e., $P \oplus Q = \mathcal{O}_E$.



Note that if $\mathcal{O}_E$ is a flex then $S = \mathcal{O}_E$ in the above.

(iv) Associativity is much harder to prove. □

Now assume that $K = \bar{K}$.

Definition. $D_1, D_2 \in \mathrm{Div}(E)$ are *linearly equivalent* if there exists $f \in K(E)^*$ such that $\mathrm{div}(f) = D_1 - D_2$. Write $D_1 \sim D_2$, and $[D] = \{D' : D' \sim D\}$.

Remark. Theorem 2.8 applied to $f\colon E \to \mathbb{P}^1$ shows $\deg(\mathrm{div}(f)) = 0$, so $D_1 \sim D_2$ implies $\deg(D_1) = \deg(D_2)$.

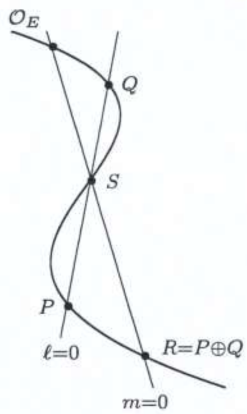
The principal divisors, i.e., $\mathrm{div}(f)$ for $f \in K(E)^*$ are a subgroup of $\mathrm{Div}(E)$ since $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$.

Definition. We define the groups $\mathrm{Pic}(E) = \mathrm{Div}(E)/\sim$ and $\mathrm{Pic}^\circ(E) = \mathrm{Div}^\circ(E)/\sim$ where $\mathrm{Div}^\circ(E) = \{D \in \mathrm{Div}(E) : \deg(D) = 0\}$. For the moment, we also define the map $\phi\colon E \to \mathrm{Pic}^\circ(E), P \mapsto [P - \mathcal{O}_E]$.

Proposition 4.2. (i) $\phi(P \oplus Q) = \phi(P) + \phi(Q)$.
(ii) ϕ is a bijection.

Note $\mathrm{Div}^\circ(E)$ is non-empty. Take any rational functio[n]

Proof. (i) Consider the lines $l = 0$ and $m = 0$. as specified by the diagram



Then $l/m \in K(E)^*$ and

$$\begin{aligned}\mathrm{div}\Big(\frac{l}{m}\Big) &= P + S + Q - \mathcal{O}_E - S - R \\ &= P + Q - \mathcal{O}_E - R \\ &= P + Q - \mathcal{O}_E - P \oplus Q\end{aligned}$$

because l/m is rational

so $P + Q \sim P \oplus Q + \mathcal{O}_E$, hence $P \oplus Q - \mathcal{O}_E \sim P - \mathcal{O}_E + Q - \mathcal{O}_E$ and finally $\phi(P \oplus Q) = \phi(P) + \phi(Q)$.

(ii) (*Injective.*) If $\phi(P) = \phi(Q)$ then $P - Q \sim 0$ so $P \sim Q$. So there exists $f \in K(E)^*$ such that $\mathrm{div}(f) = P - Q$, then $\deg\big(E \xrightarrow{f} \mathbb{P}^1\big) = 1$ and hence $E \cong \mathbb{P}^1$, which contradicts E being an elliptic curve unless f is constant so $P = Q$.
(*Surjective.*) Take $D \in \mathrm{Div}^\circ(E)$. Then $\deg(D + \mathcal{O}_E) = 1$. By Riemann–Roch, $\dim \mathcal{L}(D + \mathcal{O}_E) = 1$ so there exists $f \in K(E)^*$ such that $\mathrm{div}(f) + D + \mathcal{O}_E \geq 0$. The left-hand side also has degree 1. Therefore, $\mathrm{div}(f) + D + \mathcal{O}_E = P$ for some $P \in E$. Then $D + \mathcal{O}_E \sim P$ so $D \sim P - \mathcal{O}_E$ and finally $[D] = [P - \mathcal{O}_E] = \phi(P)$. □

Riemann-Roch for Curves of Genus 1:

$$\dim \mathcal{L}(D) = \begin{cases} \deg(D) & \text{if } \deg(D) > 0 \\ 0 \text{ or } 1 & = 0 \\ 0 & < 0 \end{cases}$$

Define sum: $\mathrm{Div}(E) \to E, P_1 + \cdots P_r - (Q_1 + \cdots + Q_s) \mapsto (P_1 \oplus \cdots \oplus P_r) \ominus (Q_1 \oplus \cdots \oplus Q_s)$. If $D \in \mathrm{Div}^\circ(E)$, say $D = \sum n_i P_i$, then $D = \sum n_i (P_i - \mathcal{O}_E)$ so

$$[D] = \sum n_i [P_i - \mathcal{O}_E] = \sum n_i \phi(P_i) = \phi(\mathrm{sum}(D))$$

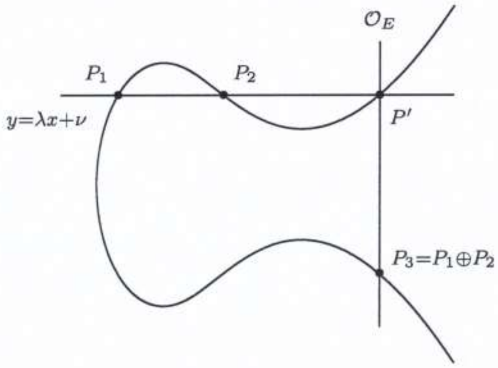
by Proposition 4.2 (i). So $D \sim 0$ if and only if $\mathrm{sum}(D) = \mathcal{O}_E$.

Corollary 4.3. If $D \in \mathrm{Div}(E)$ then $D \sim \mathcal{O}_E$, i.e., D is principal, if and only if $\deg(D) = 0$ and $\mathrm{sum}(D) = \mathcal{O}_E$.

4.1 Formlae for E in Weierstrass Form

We consider an elliptic curve with general Weierstrass equation

$$E \colon y^2 = a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6. \qquad (*)$$



The inverse of (x, y) is $(x, -(a_1 x + a_3) - y)$. Substituting $y = \lambda x + \nu$ into $(*)$ and taking coefficients of x^2 gives $\lambda^2 + a_1\lambda - a_2 = x_1 + x_2 + x' = x_1 + x_2 + x_3$ so

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2, \\ y' &= \lambda x' + \nu, \\ y_3 &= -(a_1 x_3 + a_3) - \lambda x_3 - \nu = -(a_1 + \lambda) x_3 + a_3 - \nu. \end{aligned}$$

It remains to give formulae for λ and ν.

Case 1. $x_1 = x_2$, $P_1 \neq P_2$. Then $P_1 \oplus P_2 = \mathcal{O}_E$.

Case 2. $x_1 \neq x_2$. Then

$$\lambda = \frac{y_1 - y_2}{x_1 - x_2}, \qquad \nu = y_1 - \lambda x_1 = \frac{x_1 y_2 - x_2 y_1}{x_1 - x_2}.$$

Case 3. $P_1 = P_2$. Use the tangent line, see formula sheet.

Theorem 4.4. Elliptic curves are group varieties, i.e., the group operations

$$[-1] \colon E \to E, P \mapsto \ominus P, \qquad \oplus \colon E \times E \to E$$

are morphisms of algebraic varieties.

Proof. (i) $[-1] \colon E \to E$ is a rational map and hence a morphism.

by default because
E is smooth

(ii) We need to show that $\oplus$ is a morphism. The formulae in Case 2 show it is a rational map regular on $U = \{(P,Q) : P, Q, P \oplus Q, P \ominus Q \neq \mathcal{O}_E\}$. Fix $P \in E$ and define the translation $\tau_P \colon E \to E, X \mapsto P \oplus X$. Note that τ_P is rational so a morphism. We can factor $\oplus$ as

$$E \times E \xrightarrow{\tau_A \times \tau_B} E \times E \xrightarrow{\oplus} E \xrightarrow{\tau_{\ominus A \ominus B}} E$$

$$(P, Q) \longmapsto (P+A, Q+B) \mapsto (P+A+Q+B) \longmapsto (P+Q)$$

for any $A, B \in E$. So $\oplus$ is regular on all translations of U, and these cover all of $E \times E$. Thus $\oplus$ is a morphism. $\square$

Let K be any field and E an elliptic curve over K. Set

$$E(K) = \{(x,y) \in K^2 : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\} \cup \{\mathcal{O}_E\}.$$

Lemma 4.5. $(E(K), \oplus)$ is an abelian group.

4.2 Statement of Results

(i) $K = \mathbb{C}$, $E(\mathbb{C}) \cong C/\Lambda \cong \mathbb{R}/\mathbb{Z} \times \mathbb{R}/\mathbb{Z}$, where Λ is a rank 2 lattice, and the isomorphisms are isomorphims of topological groups.

To add further brief remarks, note that the meromorphic functions on $\mathbb{C}/\Lambda$ correspond precisely to the Λ-invariant meromorphic functions on $\mathbb{C}$. The function field $\mathbb{C}/\Lambda$ is generated by $\wp(z)$ and $\wp'(z)$ where $\wp$ is the Weierstrass function. One shows that $\mathbb{C}/\Lambda \cong E(\mathbb{C})$ for some elliptic curve $E/\mathbb{C}$. The Uniformisation Theorem gives that every elliptic curve $E/\mathbb{C}$ arises this way.

(ii) $K = \mathbb{R}$,

$$E(\mathbb{R}) = \begin{cases} \mathbb{Z}/2\mathbb{Z} \times \mathbb{R}/\mathbb{Z} & \Delta > 0, \\ \mathbb{R}/\mathbb{Z} & \Delta < 0. \end{cases}$$

(iii) $K = \mathbb{F}_q$, $|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}$, which is Hasse's Theorem.

(iv) $[K : \mathbb{Q}_p] < \infty$, $\mathcal{O}_K$ the ring of integers. Then $E(K)$ contains a subgroup of finite index isomorphic to $(\mathcal{O}_K, +)$.

(v) $[K : \mathbb{Q}] < \infty$, $E(K)$ is a finitely generated abelian group, which is the Mordell–Weil Theorem. From basic group theory, we know that if A is a finitely generated group then $A \cong F \times \mathbb{Z}^r$ where F is a finite group and r is the rank of A. If K is a number field then proof of the Mordell–Weil Theorem gives an upper bound for $\operatorname{rank}(E)$. But there is no algorithm proven to compute the rank in all cases.

22/10/13

Elliptic Curves ⑥

Statement of Results (continued)

iii) $k = \mathbb{F}_q$, $|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}$ (Hasse's Theorem)

iv) $[k : \mathbb{Q}_p] < \infty$, ring of integers $\mathcal{O}_k$. $E(k)$ contains a subgroup of finite index isomorphic to $(\mathcal{O}_k, +)$

v) $[k : \mathbb{Q} < \infty]$. $E(k)$ is a finitely generated abelian group (Mordell - Weil Theorem)

Basic group theory: If A is a finitely generated abelian group then $A \cong$ (finite group) $\times \mathbb{Z}^r$ (r the rank of A).

The proof of Mordell-Weil gives an upper bound for the rank of $E(k)$. But there is no known algorithm proven to compute the rank in all cases.

Brief remarks on the case $k = \mathbb{C}$

$\Lambda = \{a\omega_1 + b\omega_2 : a, b \in \mathbb{Z}\}$ where ω_1, ω_2 are a basis for $\mathbb{C}$ as an $\mathbb{R}$-vector space. We consider meromorphic functions:

$$\left\{\begin{matrix}\text{meromorphic functions on}\\ \text{the Riemann surface } \mathbb{C}/\Lambda\end{matrix}\right\} \Longleftrightarrow \left\{\begin{matrix}\Lambda\text{-invariant meromorphic}\\ \text{functions on } \mathbb{C}\end{matrix}\right\}$$

The function field of $\mathbb{C}/\Lambda$ is generated by $\wp(z)$ and $\wp'(z)$, where $\wp(z) = \frac{1}{z^2} + \sum_{0 \neq \lambda \in \Lambda} \left(\frac{1}{(z-\lambda)^2} - \frac{1}{\lambda^2}\right)$

$$\wp'(z) = -2 \sum_{\lambda \in \Lambda} \frac{1}{(z-\lambda)^3}$$

These satisfy $\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3$ for some $g_2, g_3 \in \mathbb{C}$, depending on Λ.

One shows that $\mathbb{C}/\Lambda \underset{\nearrow}{\cong} E(\mathbb{C})$ where $E : y^2 = 4x^3 - g_2 x - g_3$

isomorphism of Riemann Surfaces

Uniformisation Theorem : Every elliptic curve $E/\mathbb{C}$ arises in this way.
(One proof uses modular forms)

5 Isogenies

Let E_1, E_2 be elliptic curves.

Definitions

i) An isogeny $\phi : E_1 \to E_2$ is a non-constant morphism with $\phi(O_{E_1}) = O_{E_2}$

$\updownarrow$ Theorem 2.8
surjective (on $\bar{k}$ points)

ii) We say then that E_1, E_2 are isogenous.

iii) $\mathrm{Hom}(E_1, E_2) := \{\text{isogenies } E_1 \to E_2\} \cup \{0\}$

is an abelian group under $(\phi + \psi)(P) = \phi(P) \oplus \psi(P)$

If $E_1 \xrightarrow{\phi} E_2 \xrightarrow{\psi} E_3$ then $\psi\phi$ is an isogeny.

Tower Law $\Rightarrow \deg(\psi\phi) = \deg(\psi)\deg(\phi)$

iv) For $n \in \mathbb{Z}$ let $[n] : E \to E$, $P \mapsto \underbrace{P \oplus \dots \oplus P}_{n \text{ times}}$ if $n > 0$.

$[-1] : P \mapsto \ominus P$, $[n] = [-1] \circ [-n]$ for $n < 0$.

Theorem 4.4 $\Rightarrow$ $[n]$ is a morphism.

v) The n-torsion subgroup of E is $E[n] = \ker(E \xrightarrow{[n]} E)$

If $k = \mathbb{C}$, then $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$

$\Rightarrow E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$, $\deg[n] = n^2$

We will prove that $\deg[n] = n^2$ holds over any field k and $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ holds provided that $\mathrm{char}(k) \nmid n$.

Lemma 5.1

Assume that $\mathrm{char}(k) \neq 2$. $E : y^2 = f(x) = (x - e_1)(x - e_2)(x - e_3)$

$e_1, e_2, e_3 \in \bar{k}$, distinct.

22/10/13 Elliptic Curves ⑥

Then $E[2] = \{O_E, (e_1,0), (e_2,0), (e_3,0)\} \cong (\mathbb{Z}/2\mathbb{Z})$

Proof

Let $O \neq P \in E$, $P = (x_P, y_P)$

can see this by taking partial derivatives to the equation of the curve

$T_P E = \{ 2y_P(y - y_P) = f'(x_P)(x - x_P) \}$

$P \in E[2] \Leftrightarrow [2]P = O \Leftrightarrow T_P E = \{x = x_P\}$

$\Leftrightarrow y_P = 0$ □

Proposition 5·2

If $0 \neq n \in \mathbb{Z}$, then $[n] : E \to E$ is an isogeny

Proof

We must show that $[n] \neq [0]$. Assume that $char(k) \neq 2$.

When $n = 2$, Lemma 5·1 $\Rightarrow E[2] \neq E \Rightarrow [2] \neq [0]$

When n is odd, Lemma 5·1 $\Rightarrow \exists\, O \neq T \in E[2]$

Then $nT = T \neq O$, so $[n] \neq [0]$

Now, since $[mn] = [m] \circ [n]$, we are done for even n.

If $char(k) = 2$, we could replace 5·1 with an explicit lemma on 3-torsion points. □

Corollary

$Hom(E_1, E_2)$ is a torsion-free $\mathbb{Z}$-module.

Theorem 5·3

Let $\phi : E_1 \to E_2$ be an isogeny. Then $\phi(P \oplus Q) = \phi(P) \oplus \phi(Q)$ $\forall P, Q \in E_1$.

Proof (sketch)

ϕ induces a map $\phi_* : Div^0(E_1) \to Div^0(E_2)$

$$\sum n_P P \mapsto \sum_{P \in E} n_P \phi(P)$$

$$\begin{array}{c} k(E_1) \\ | \\ k(E_2) \end{array} \Big\} \text{ norm map}$$

Recall that $\phi_*: k(E_2) \hookrightarrow k(E_1)$

Fact : If $f \in k(E_1)^*$, $\mathrm{div}(\underbrace{N_{k(E_1)/k(E_2)}}_{\text{norm}} f) = \phi_*(\mathrm{div}(f))$

So ϕ_* takes principal divisors to principal divisors.

$\therefore \phi_* : \mathrm{Pic}^0(E_1) \to \mathrm{Pic}^0(E_2)$

Since $\phi(O_{E_1}) = O_{E_2}$ the following diagram commutes :

$$\begin{array}{ccccc} P & E_1 & \xrightarrow{\phi} & E_2 & Q \\ \downarrow & \wr\downarrow & & \wr\downarrow & \downarrow \\ [P - O_{E_1}] & \mathrm{Pic}^0(E_1) & \xrightarrow{\phi_*} & \mathrm{Pic}^0(E_2) & [Q - O_{E_2}] \end{array}$$

ϕ_* a group homomorphism $\Rightarrow \phi$ is a group homomorphism $\square$

$$\begin{tikzcd} E_1 \arrow[r, "\phi"] \arrow[d, "\wr"'] & E_2 \arrow[d, "\wr"] \\ \mathrm{Pic}^0(E_1) \arrow[r, "\phi^*"] & \mathrm{Pic}^0(E_2) \end{tikzcd}$$

24/10/13

Elliptic Curves 7

Example

Let E/k be an elliptic curve, $0 \neq T \in E(k)[2]$

W.L.O.G. $E : y^2 = x(x^2 + ax + b)$

$a, b \in k$, $b(a^2 - 4b) \neq 0$ (for distinct roots)

$T = (0,0)$. Let $P = (x, y)$.

$P' = P + T = (x', y')$

Calculation $\Rightarrow (x', y') = \left(\frac{b}{x}, -\frac{by}{x^2}\right)$

Check: the line PT has slope $\lambda = y/x$

$\lambda^2 = y^2/x^2 = \frac{x^2 + ax + b}{x} = x + a + b/x$

$x' = \lambda^2 - a - x = b/x$, $y' = -\lambda x' = -\frac{by}{x^2}$

Let $\xi = x + x' + a = \frac{x^2 + ax + b}{x} = \left(\frac{y}{x}\right)^2$

and $\eta = y + y' = \frac{y}{x}\left(x - \frac{b}{x}\right)$

Then $\eta^2 = \frac{y^2}{x^2}\left(\left(x + \frac{b}{x}\right)^2 - 4b\right)$

$= \xi((\xi - a)^2 - 4b) = \xi(\xi^2 - 2a\xi + a^2 - 4b)$

Let $E' : y^2 = x(x^2 + a'x + b')$

where $a' = -2a$, $b' = a^2 - 4b$

There is an isogeny $\phi : E \to E'$, $(x, y) \mapsto (\xi, \eta) = \left(\left(\frac{y}{x}\right)^2, \frac{y(x^2}{x}\right.$

We check that $\phi(O_E) = O_{E'}$

$(x, y) \mapsto \left(\left(\frac{y}{x}\right)^2 : \frac{y(x^2 - b)}{x^2} : 1\right)$

ord_{O_E}: $-2 \quad -3 \quad 0$

$(0 : 1 : 0) = O_{E'}$ multiply through by cube of a uniformiser

What is the degree of ϕ?

Lemma 5.5 → Gives a practical way to find the degree of an isogeny

Let $\phi : E_1 \to E_2$ be an isogeny. Then $\exists$ a morphism $\xi : \mathbb{P}^1 \to \mathbb{P}^1$ such that the following diagram commutes:

$$\begin{tikzcd} E_1 \arrow[r, "\phi"] \arrow[d, "x_1"'] & E_2 \arrow[d, "x_2"] \\ \mathbb{P}^1 \arrow[r, "\xi"] & \mathbb{P}^1 \end{tikzcd}$$

x_i = take the x coordinate on the Weierstrass equation for E_i.

Moreover if $\xi(t) = \frac{r(t)}{s(t)}$, $r, s \in k[t]$ coprime, then

$\deg(\phi) = \deg(\xi) = \max(\deg(r), \deg(s))$

Proof

For $i = 1, 2$, $k(E_i)/k(x_i)$ is a degree 2 Galois extension with Galois group generated by $[-1]^*$

Theorem 5.3 $\Rightarrow \phi \circ [-1] = [-1] \circ \phi$

So if $f \in k(x_2)$,

because $[-1]^*$ in the Galois Group, f in the base field

$[-1]^*(\phi^* f) = \phi^*([-1]^* f) = \phi^* f$

$\therefore \phi^* f \in k(x_1)$.

$$\begin{tikzcd} & k(E_1) = k(x_1, y_1) \arrow[dl, dash, "2"'] \arrow[d, dash, "\deg(\phi)"] \\ k(x_1) \arrow[d, dash, "\deg\xi"'] & k(E_2) = k(x_2, y_2) \arrow[dl, dash, "2"] \\ k(x_2) & \end{tikzcd}$$

Now $k(x_2) \hookrightarrow k(x_1)$, $x_2 \mapsto \xi(x_1) = \frac{r(x_1)}{s(x_1)}$ ↑ coprime

Tower Law $\Rightarrow \deg \phi = \deg \xi$

The min. poly. of x_1 over $k(x_2)$ is $f(X) = r(X) - s(X)x_2$ and $f(X) \in k(x_2)[X]$

Check : x_1 is a root of f (clear), and f is irreducible in $k[x_2, X]$ (since r, s coprime) hence irreducible in $k(x_2)[X]$ by Gauss' Lemma.

$$\therefore \deg(\xi) = [k(x_1) : k(x_2)]$$
$$= \deg(f) = \max(\deg(r), \deg(s)) \qquad \square$$

So in example 5·4, $\xi(x) = \left(\frac{y}{x}\right)^2 = \frac{x^2+ax+b}{x}$

Since $b \neq 0$, x^2+ax+b and x are coprime.

$\therefore \deg(\phi) = 2$. We say that ϕ is a 2-isogeny.

Example 5·6

Assume char$(k) \neq 2, 3$. $E: y^2 = x^3 + ax + b = f(x)$

$[2]: E \to E$, $(x, y) \mapsto \left(\underbrace{\left(\frac{3x^2+a}{2y}\right)^2 - 2x}_{\xi(x)}, \dots \right)$

$$\xi(x) = \frac{(3x^2+a)^2 - 8x(x^3+ax+b)}{4(x^3+ax+b)}$$
$$= \frac{x^4 + \dots}{4(x^3+ax+b)}$$

We must check that the numerator and denominator are coprime.

Indeed, otherwise $\exists\, \theta \in \bar{k}$ such that $f(\theta) = f'(\theta) = 0$

$\Rightarrow f$ has a double root $\Rightarrow E$ is singular ※

$\therefore \deg[2] = 4$.

has degree 0 by convention.

Recall : $\mathrm{Hom}(E_1, E_2) = \{\text{isogenies } E_1 \to E_2\} \cup \{0\}$

If $\phi \in \mathrm{Hom}(E_1, E_2)$ then $\deg(-\phi) = \deg([-1]\circ\phi) = \deg(\phi)$

$\deg(2\phi) = \deg([2]\circ\phi) = 4\deg\phi$.

Lemma 5·7

Let $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$. Then

$\deg(\phi+\psi) + \deg(\phi-\psi) = 2\deg(\phi) + 2\deg(\psi)$

(The "Parallelogram Law").

Proof

Next lecture.

Lemma 5·8

$\deg[n] = n^2 \quad \forall n \in \mathbb{Z}$.

Uses Parallelogram Law for induction step

Proof

By induction on n. Trivial for $n = 0, 1$.

Put $\phi = [n]$, $\psi = [1]$ in Lemma 5·7.

$\deg[n+1] + \deg[n-1] = 2\deg[n] + 2\deg[1]$

Induction hypothesis $\Rightarrow \deg[n+1] = 2n^2 + 2 - (n-1)^2 = (n+1)^2$

If $n < 0$ then use $[n] = [-1] \circ [-n] \Rightarrow \deg[n] = (-n)^2 = n^2$ □

Theorem 5·9

$\deg : \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$ is a positive-definite quadratic form.

i.e. i) $\deg([n]\phi) = n^2 \deg(\phi) \quad \forall n \in \mathbb{Z}$

ii) $(\phi, \psi) \mapsto \deg(\phi + \psi) - \deg(\phi) - \deg(\psi)$

is $\mathbb{Z}$-bilinear.

iii) $\deg(\phi) \geq 0$ with equality $\Leftrightarrow \phi = 0$.

Proof

i) Use Lemma 5·8.

ii) Exercise. Use Lemma 5·7. See Sheet 2.

iii) Trivial, since an isogeny always has degree ≥ 1, leaving only 0 with degree 0 □

26/10/13

Elliptic Curves ⑧

Lemma 5·7

Let $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$. Then $\deg(\phi+\psi) + \deg(\phi-\psi) = 2\deg(\phi) + 2\deg(\psi)$

Proof

We may assume that $\phi, \psi, \phi+\psi, \phi-\psi \neq 0$. Otherwise the result is trivial, or use $\deg[2] = 4$. Assume for simplicity that $\mathrm{char}(k) \neq 2, 3$.

$E_2 : y^2 = x^3 + ax + b$

$\phi : (x, y) \mapsto (\xi_1(x), \eta_1(x,y))$

$\psi : (x, y) \mapsto (\xi_2(x), \eta_2(x,y))$

$\phi+\psi : (x, y) \mapsto (\xi_3(x), \eta_3(x,y))$

$\phi-\psi : (x, y) \mapsto (\xi_4(x), \eta_4(x,y))$

Group law on E_2: $\xi_3 = \left(\frac{\eta_1 - \eta_2}{\xi_1 - \xi_2}\right)^2 - \xi_1 - \xi_2$

$\xi_4 = \left(\frac{\eta_1 + \eta_2}{\xi_1 - \xi_2}\right)^2 - \xi_1 - \xi_2$

We also have $\eta_i^2 = \xi_i^3 + a\xi_i + b, \quad i = 1, 2$

$$(1 : \xi_3 + \xi_4 : \xi_3\xi_4) = \left((\xi_1 - \xi_2)^2 : 2(\xi_1\xi_2 + a)(\xi_1 + \xi_2) + 4b : \xi_1^2\xi_2^2 - 2a\xi_1\xi_2 - 4b(\xi_1+\xi_2) + a^2\right)$$

Write $\xi_i(x) = \frac{r_i(x)}{s_i(x)}$ where $r_i, s_i \in k[x]$, coprime

$$(s_3 s_4 : r_3 s_4 + r_4 s_3 : r_3 r_4) = (\overset{W_0}{(r_1 s_2 - r_2 s_1)^2} : \ldots \underset{\text{Exercise}}{W_1} \ldots : \ldots W_2 \ldots)$$

W_0, W_1, W_2 each have degree 2 in r_1 and s_1 and have degree 2 in r_2 and s_2.

$$\begin{aligned}
\deg(\xi_3) + \deg(\xi_4) &= \max(\deg(r_3), \deg(s_3)) + \max(\deg(r_4), \deg(s_4)) \\
&= \max(\deg(s_3 s_4), \deg(r_3 s_4 + r_4 s_3), \deg(r_3 r_4))
\end{aligned}$$

these have no common factor in $k[x]$

$$\begin{aligned}
&\leq \max(\deg(W_0), \deg(W_1), \deg(W_2)) \\
&\leq 2\max(\deg(r_1), \deg(s_1)) + 2\max(\deg(r_2), \deg(s_2)).
\end{aligned}$$

1

$= 2\deg(\xi_1) + 2\deg(\xi_2)$

$\therefore \ \deg(\phi + \psi) + \deg(\phi - \psi) \leq 2\deg(\phi) + 2\deg(\psi) \qquad (*)$

Replacing ϕ and ψ with $\phi+\psi$, $\phi-\psi$, we obtain

$4\deg(\cancel{2}\phi) + 4\deg(\cancel{2}\psi) \leq 2\deg(\psi+\phi) + 2\deg(\phi-\psi)$

Since $\mathrm{char}(k) \neq 2$, $\quad 2\deg(\phi) + 2\deg(\psi) \leq \deg(\phi+\psi) + \deg(\phi-\psi)$

This is the inequality reverse to $(*)$ $\square$

6 Invariant Differential

Let C be a smooth projective curve over $k = \bar{k}$.

The space of differentials Ω_C is the $k(C)$-vector space generated by df for $f \in k(C)$ subject to relations:

$$\left.\begin{array}{l} i)\ d(f+g) = df + dg \\ ii)\ d(fg) = f\,dg + df\,g \end{array}\right\} \forall f, g \in k(C)$$

iii) $da = 0 \quad \forall a \in k$

Fact

Ω_C is a 1-dimensional $k(C)$-vector space.

Let $\omega \in \Omega_C$, $\omega \neq 0$. Let $P \in C$, $t \in k(C)$ a uniformiser at P. Then $\omega = f\,dt$ for some $f \in k(C)$

We define $\mathrm{ord}_P(\omega) = \mathrm{ord}_P(f)$. This is independent of choice of t. Moreover $\mathrm{ord}_P(\omega) = 0$ for all but finitely many $P \in C$.

We define $\mathrm{div}(\omega) = \sum_{P \in C} \mathrm{ord}_P(\omega) P$

Definition

$$g(C) = \dim_k \underbrace{\{\omega \in \Omega_k \mid \overbrace{\mathrm{div}(\omega) \geq 0}^{\text{is effective}}\}}_{\text{space of regular differentials}}$$

26/10/13

Elliptic Curves ⑧

A consequence of Riemann Roch:

$\deg(\operatorname{div}(\omega)) = 2g(C) - 2$

Fact

Suppose that $f \in k(C)^*$, $\operatorname{ord}_P(f) = n \neq 0$.

If $\operatorname{char}(k) \nmid n$ then $\operatorname{ord}_P(df) = n-1$.

Lemma 6·1

Assume that $\operatorname{char}(k) \neq 2$. $E : y^2 = (x-e_1)(x-e_2)(x-e_3)$

Then $\omega = \frac{dx}{y}$ is a differential on E with no zeros or poles.

($\Rightarrow g(E) = 1$). In particular, ω is a basis for the 1-dimensional k-vector space of regular differentials on E.

Proof

Let $T_i = (e_i, 0)$. $E[2] = \{0, T_1, T_2, T_3\}$

$\operatorname{div}(y) = (T_1) + (T_2) + (T_3) - 3(0)$ ①

If $P \in E \setminus E[2]$, $\operatorname{ord}_P(\underbrace{x - x_P}_{x_P \text{ not a double root}}) = 1 \Rightarrow \operatorname{ord}_P(dx) = 0$

If $P = T_i$, $\operatorname{ord}_P(x - e_i) = 2 \Rightarrow \operatorname{ord}_P(dx) = 1$

If $P = \underset{\text{point at } \infty}{0}$ $\underbrace{\operatorname{ord}_P(x) = -2}_{\text{See earlier}}$ $\Rightarrow \operatorname{ord}_P(dx) = -3$

using the 'Fact' above

$\operatorname{div}(dx) = (T_1) + (T_2) + (T_3) - 3(0)$ ②

①, ② $\Rightarrow \operatorname{div}\left(\frac{dx}{y}\right) = 0$, zero so no zeros or poles □

Definition

If $\phi : C_1 \to C_2$ is a non-constant morphism

$\phi^* : \Omega_{C_2} \to \Omega_{C_1}$, $f\,dg \longmapsto \phi^*(f)\, d(\phi^* g)$

(Remember : $\phi : C_1 \to C_2$ a non-constant morphism,

$\phi^* : k(C_2) \to k(C_1)$, $f \mapsto f \circ \phi$

ϕ^* a field embedding)

Example

$E: y^2 = x(x^2+ax+b)$, $T=(0,0)$

$\tau_T : (x,y) \mapsto \left(\frac{b}{x}, -\frac{by}{x^2}\right)$

Then $\tau_T^*\left(\frac{dx}{y}\right) = \frac{d(b/x)}{-by/x^2} = \frac{-b/x^2\,dx}{-by/x^2} = \frac{dx}{y}$

Lemma 6·2

Let E/k be an elliptic curve. $P \in E$. $\tau_P : E \to E$, $X \mapsto X \oplus P$

$\omega = \frac{dx}{y}$. Then $\tau_P^* \omega = \omega$

Proof

$\tau_P^*\omega$ is a regular differential on $E \Rightarrow \tau_P^*\omega = \lambda_P \omega$ for some $\lambda_P \in k^*$. The map $E \to \mathbb{P}^1$, $P \mapsto \lambda_P$ is a morphism of smooth projective curves, but not surjective. as $\lambda_P \in k^*$, does not hit 0

$\therefore$ it is constant. i.e. $\lambda_P = \lambda$ Taking $P = 0 \Rightarrow \lambda = 1$ $\square$

i.e. $\tau_P = id$

29/10/13

Elliptic Curves (9)

$E: y^2 = f(x)$, char$(k) \neq 2$

$\omega = \frac{dx}{y}$ <u>invariant differential</u> $\Leftrightarrow \tau_P^* \omega = \omega \quad \forall P \in E$

<u>Aside</u>

If $k = \mathbb{C}$ then $\mathbb{C}/\Lambda \xrightarrow{\sim} E$, $z \mapsto (\wp(z), \wp'(z))$

$\frac{dx}{y} = \frac{\wp'(z)dz}{\wp'(z)} = dz$, obviously invariant under $z \mapsto z + c$

<u>Lemma 6·3</u>

Let $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$, ω the invariant differential on E_2.

Then $(\phi + \psi)^* \omega = \phi^* \omega + \psi^* \omega$

<u>Proof</u>

Write $E = E_2$. $\quad E \times E \to E$

$\mu : (P, Q) \mapsto P \oplus Q$

$pr_1 : (P, Q) \mapsto P$, $pr_2 : (P, Q) \mapsto Q$

<u>Fact</u>

$\Omega_{E \times E}$ is a 2-dimensional vector space over $k(E \times E)$, with basis $pr_1^* \omega$ and $pr_2^* \omega$. $(*)$

$\therefore \mu^* \omega = f\, pr_1^* \omega + g\, pr_2^* \omega$ for some $f, g \in k(E \times E)$

For $Q \in E$ let $i_Q : E \to E \times E$, $P \mapsto (P, Q)$

Applying i_Q^* to $(*)$ gives

id map so $(pr_1 \circ i_Q)^* \omega = \omega$

$i_Q^* \mu^* = (\mu \circ i_Q)^*$

$(\mu \circ i_Q)^* \omega = (i_Q^* f)(pr_1 \circ i_Q)^* \omega + (i_Q^* g)(pr_2 \circ i_Q)^* \omega$

$\mu \circ i_Q = \tau_Q$

$\Rightarrow \tau_Q^* \omega = (i_Q^* f) \omega + 0$

This maps any point to Q so $(pr_2 \circ i_Q)^* \omega = 0$

Lemma 6·2 $\Rightarrow i_Q^* f = 1 \quad \forall Q \in E$.

$\Rightarrow f(P, Q) = 1 \quad \forall P, Q \in E$.

Similarly, $g(P, Q) = 1 \quad \forall P, Q \in E$.

(*) becomes $\mu^*\omega = pr_1^*\omega + pr_2^*\omega$

Now pull back by $E_1 \xrightarrow{\mu_0} E_2 \times E_2$, $P \overset{\mu_0}{\mapsto} (\phi(P), \psi(P))$

to get $\underline{(\phi+\psi)^*\omega} = \phi^*\omega + \psi^*\omega$ $\square$

$E_1 \xrightarrow{\mu_0} E_2 \times E_2 \xrightarrow{\mu} E_2$

because $\mu \circ \mu_0 = \phi + \psi$, $pr_1 \circ \mu_0 = \phi$, $pr_2 \circ \mu_0 = \psi$

Lemma 6.4

$\phi : C_1 \to C_2$ a non-constant morphism.

ϕ is separable $\Leftrightarrow$ $\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ is non-zero.

Proof

Omitted.

Example

$\mathbb{G}_m = \mathbb{A}^1 \setminus \{0\}$ multiplicative group

$\phi : \mathbb{G}_m \to \mathbb{G}_m$, $x \mapsto x^n$, $0 \neq n \in \mathbb{Z}$.

$\phi^*(dx) = d(x^n) = nx^{n-1}dx$

If $\mathrm{char}(k) \nmid n$ then ϕ is separable.

$\Rightarrow \#\phi^{-1}(Q) = \deg(\phi)$ for all but finitely many $Q \in \mathbb{G}_m$.

But ϕ is a group homomorphism

$\therefore \#\phi^{-1}(Q) = \#\ker\phi \quad \forall Q$

$\therefore \#\ker\phi = \deg\phi = n$.

This shows that k $(=\bar{k})$ contains exactly n n^{th} roots of unity.

Theorem 6.5

If $\mathrm{char}(k) \nmid n$ then $E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$

Proof

Lemma 6.3 and Induction $\Rightarrow [n]^*\omega = n\omega$

Since $\mathrm{char}(k) \nmid n$, it follows that $[n]$ is separable.

$\Rightarrow \#[n]^{-1}(Q) = \deg[n]$ for all but finitely many $Q \in E$.

But $[n]$ is a group homomorphism

$\Rightarrow \#[n]^{-1}(Q) = \#E[n] \quad \forall Q \in E$.

$\therefore \#E[n] = \deg[n] = n^2$

Group Theory $\Rightarrow E[n] \cong \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z} \times \dots \times \mathbb{Z}/d_t\mathbb{Z}$

with $d_1 | d_2 | \dots | d_t | n$ ← Structure Theorem says n^2
Can reduce to n as group elements have order $\leq n$

If p is a prime divisor of d_1, then $E[p] \cong (\mathbb{Z}/p\mathbb{Z})^t$

But $\#E[p] = p^2$, so $t=2$ and $d_1 = d_2 = n$

$\therefore E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$ □

<u>Remark</u>

If $\mathrm{char}(k) = p$, then $[p]$ is inseparable. It can be shown that <u>either</u> $\underset{\text{"ordinary"}}{E[p^r] \cong \mathbb{Z}/p^r\mathbb{Z}} \quad \forall r \geq 1$ <u>or</u> $\underset{\text{"supersingular"}}{E[p^r] = 0} \quad \forall r \geq 1$.

<u>Lemma 6.6</u>

Let A be an abelian group (or $\mathbb{Z}$-module)

Let $q: A \to \mathbb{Z}$ be a positive definite quadratic form.

If $\phi, \psi \in A$, then $|\underbrace{q(\phi+\psi) - q(\phi) - q(\psi)}_{\text{"}\langle\phi,\psi\rangle\text{"}}| \leq 2\sqrt{q(\phi)q(\psi)}$ Think Cauchy Schwartz

<u>Proof</u>

We may assume that $\phi \neq 0$, otherwise it is clear.

Let $m, n \in \mathbb{Z}$. $0 \leq q(m\phi + n\psi) = \frac{1}{2}\langle m\phi+n\psi, m\phi+n\psi\rangle$

$\langle\sigma,\sigma\rangle = 2q(\sigma)$ $\quad = m^2 q(\phi) + mn\langle\phi,\psi\rangle + n^2 q(\psi)$

$$= q(\phi)\left(m + \frac{\langle\phi,\psi\rangle}{2q(\phi)}n\right)^2 + n^2\left(q(\psi) - \frac{\langle\phi,\psi\rangle^2}{4q(\phi)}\right)$$

Take $m = -\langle\phi,\psi\rangle$, $n = 2q(\phi)$ to deduce

$$q(\psi) - \frac{\langle\phi,\psi\rangle^2}{4q(\phi)} \geq 0 \Rightarrow \langle\phi,\psi\rangle^2 \leq 4q(\phi)q(\psi)$$

$$\Rightarrow |\langle\phi,\psi\rangle| \leq 2\sqrt{q(\phi)q(\psi)}$$

□

<u>Theorem 6·7</u> (Hasse)

$E/\mathbb{F}_q$ an elliptic curve. Then $|\#E(\mathbb{F}_q) - (q+1)| \leq 2\sqrt{q}$

<u>Proof</u>

Recall $\mathrm{Gal}(\mathbb{F}_{q^r}/\mathbb{F}_q)$ is cyclic of order r, generated by $\mathrm{Fr}: x \mapsto x^q$. Let E have Weierstrass equation with coefficients $a_1, a_2, \ldots, a_6 \in \mathbb{F}_q$ ($\Rightarrow a_i^q = a_i$). Define a Frobenius endomorphism $\phi: E \to E$, $(x,y) \mapsto (x^q, y^q)$, an isogeny of degree q. Then $E(\mathbb{F}_q) = \{P \in E \mid \phi(P) = P\} = \ker(1-\phi)$

$$\phi^*\omega = \phi^*\left(\frac{dx}{y}\right) = \frac{d(x^q)}{y^q} = \frac{qx^{q-1}dx}{y^q} = 0$$

Lemma 6·3 $\Rightarrow (1-\phi)^*\omega = \omega - \phi^*\omega = \omega \neq 0$.

$\therefore \#\ker(1-\phi) = \deg(1-\phi)$

Theorem 5·9 $\Rightarrow \deg: \mathrm{Hom}(E,E) \to \mathbb{Z}$ is a +ve definite quadratic form

Lemma 6·6 $\Rightarrow |\underset{\#E(\mathbb{F}_q)}{\underset{\shortparallel}{\deg(1-\phi)}} - \underset{q}{\underset{\shortparallel}{\deg(\phi)}} - \underset{1}{\underset{\shortparallel}{\deg(1)}}| \leq 2\sqrt{\underbrace{\deg(\phi)\deg(1)}_{q}}$

□

31/10/13 Elliptic Curves 10

7 Formal Groups

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

Affine piece $Y \neq 0$, $t = -\frac{X}{Y}$, $w = -\frac{Z}{Y}$

$E: w = t^3 + a_1tw + a_2t^2w + a_3w^2 + a_4tw^2 + a_6w^3 = f(t,w)$

We will construct a power series $w \in \mathbb{Z}[a_1, \dots, a_6][[t]]$ $= t^3(1 + A_1t + A_2t^2 + \dots)$

such that $w(t) = f(t, w(t))$

In fact, $A_1 = a_1$, $A_2 = a_1^2 + a_2$, $A_3 = a_1^3 + 2a_1a_2 + a_3, \dots$

Definitions

1. Let R be a ring, I an ideal. The I-adic topology is the topology on R with basis $\{r + I^n \mid r \in R, n \geq 0\}$

2. R is complete if

i) $\bigcap_{n \geq 0} I^n = \{0\}$ → define a metric by $d(x,y) = \{$least n with $x - y \in I^n\}$

ii) Every Cauchy sequence converges

Remark

If $x \in I$, $\frac{1}{1-x} = 1 + x + x^2 + \dots \Rightarrow 1 - x \in R^*$

Lemma 7.1 (Hensel's Lemma)

Let R be an integral domain, complete with respect to $I \subset R$.

$F \in R[x]$, $s \in \mathbb{Z}_{\geq 1}$.

so F has finite length

Suppose that $a \in R$ satisfies $\begin{cases} F(a) \equiv 0 \pmod{I^s} \\ F'(a) \in R^* \end{cases}$

Then $\exists!$ $b \in R$ such that $\begin{cases} F(b) = 0 \\ b \equiv a \pmod{I^s} \end{cases}$

Proof

Pick any $\alpha \in \cancel{R^*}$ R with $F'(a) \equiv \alpha \pmod{I}$ (then $\alpha \in R^*$).

Replacing F by $\frac{F(x+a)}{\alpha}$, we may assume $a = 0$, $\alpha = 1$.

We have $F(0) \equiv 0 \pmod{I^s}$, $F'(0) \equiv 1 \pmod{I}$ — c.f. Newton Raphson

We put $x_0 = 0$, $x_{n+1} = x_n - F(x_n)$ ① $\forall n \geq 0$.

Easy induction $\Rightarrow x_n \equiv 0 \pmod{I^s}$. ②

<u>Claim</u> $x_{n+1} \equiv x_n \pmod{I^{n+s}}$

<u>Proof of Claim</u> (Induction on n)

$n=0$ is done. Suppose $x_n \equiv x_{n-1} \pmod{I^{n+s-1}}$

$$F(X) - F(Y) = (X-Y)\left(F'(0) + XG(X,Y) + YH(X,Y)\right) \qquad (\dagger)$$

for some $G, H \in R[X,Y]$. $\equiv 0 \pmod{I^{n+s-1}}$ $\quad \equiv 1 \pmod{I}$ $\quad \equiv 0 \pmod{I^s}$ when $X = x_n$, $Y = x_{n-1}$

Then $F(x_n) - F(x_{n-1}) \equiv x_n - x_{n-1} \pmod{I^{n+s}}$ ← think about $(\dagger)$

$\Rightarrow x_n - F(x_n) \equiv x_{n-1} - F(x_{n-1}) \pmod{I^{n+s}}$

$\Rightarrow x_{n+1} \equiv x_n \pmod{I^{n+s}}$

This proves the claim. $\therefore (x_n)_{n \geq 0}$ is a Cauchy sequence

R complete $\Rightarrow x_n \to b$ as $n \to \infty$ for some $b \in R$.

Taking the limit as $n \to \infty$ of ① gives $b = b - F(b)$, $F(b) = 0$

② gives $b \equiv 0 \pmod{I^s}$

Uniqueness follows from $(\dagger)$ and the assumption that R is an integral domain. $F(b_1) - F(b_2) = 0$, RHS of $(\dagger)$ non-zero if non unique ※ $\square$

We apply Hensel's Lemma with $R = \mathbb{Z}[a_1, \dots, a_6][[t]]$, $I = (t)$.

$F(X) = X - f(t, X)$, $s = 3$, $a = 0$

$F(0) = -t^3 \equiv 0 \pmod{I^3}$, $F'(0) = 1 - a_1 t - a_2 t^2 \in R^*$

$\Rightarrow \exists$ unique $w(t) \in R$ such that $\begin{cases} f(t, w(t)) = w(t) \\ w(t) \equiv 0 \pmod{t^3} \end{cases}$

Elliptic Curves ⑪

Remark

Taking $\alpha = 1$ in the proof, $w = \lim w_n$ where $w_0 = 0$

$$w_{n+1} = f(t, w_n)$$

Lemma 7.2

$R \subset K$

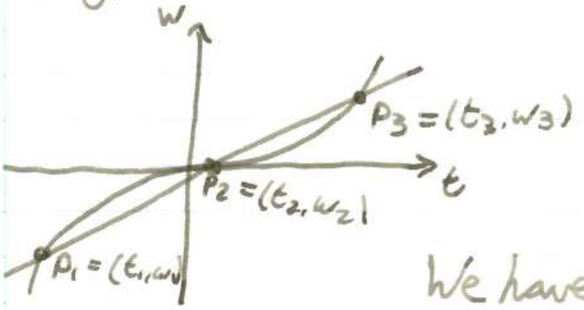
Let R be an integral domain, complete with respect to $I \leq R$. (ideal)

$a_1, \dots, a_6 \in R$. $K = \mathrm{Frac}(R)$

Then $\hat{E}(I) = \{(t, w(t)) \in E(k) \mid t \in I\}$

is a subgroup of $E(k)$.

Proof



Taking $t = 0$ shows $0 \in E(k)$ ($\hat{E}(I)$)

It suffices to show that

$P_1, P_2 \in \hat{E}(I) \Rightarrow -P_1 - P_2 \in \hat{E}(I)$

We have $t_1, t_2 \in I$, $w_1 = w(t_1) \in I$,

$w_2 = w(t_2) \in I$. $w(t) = t^3(1 + A_1 t + A_2 t^2 + \dots)$

$$\lambda = \frac{w_2 - w_1}{t_2 - t_1} = \sum_{n=3}^{\infty} A_{n-3} \frac{t_2^n - t_1^n}{t_2 - t_1} \in I$$

$\nu = w_1 - \lambda t_1 \in I$ $\longrightarrow$ P_1, P_2, P_3 lie on $w = \lambda t + \nu$

Substituting $w = \lambda t + \nu$ into $w = f(t, w)$,

$$\lambda t + \nu = t^3 + a_1 t(\lambda t + \nu) + a_2 t^2(\lambda t + \nu) + a_3(\lambda t + \nu)^2 + a_4 t(\lambda t + \nu)^2 + a_6(\lambda t + \nu)^3$$

$A = \text{coefficient of } t^3 = 1 + a_2\lambda + a_4\lambda^2 + a_6\lambda^3 \in R^*$

$B = \text{coefficient of } t^2 = a_1\lambda + a_2\nu + a_3\lambda^2 + 2a_4\lambda\nu + 3a_6\lambda^2\nu \in I$

$\therefore\ t_3 = -\frac{B}{A} - t_1 - t_2 \in I$. ← t_1, t_2, t_3 are roots of some expression and second coefficient $= t_1 + t_2 + t_3$

$w_3 = \lambda t_3 + \nu \in I$. Uniqueness is given by Lemma 7.1
$\Rightarrow w_3 = w(t_3)$

$\therefore\ -P_1 - P_2 = P_3 = (t_3, w(t_3)) \in \hat{E}(I)$ $\square$

02/11/13 Elliptic Curves 12

R a ring, $I \subset R$ an ideal

Definition

A sequence $(x_n)_{n \geq 0}$ in R is Cauchy if $\forall k$, $\exists N$ such that $x_m - x_n \in I^k$ $\forall m, n \geqslant N$.

$w(t) \in \mathbb{Z}[a_1, \dots, a_6][[t]]$

Lemma 7·2

R an integral domain complete w.r.t. I. $k = \mathrm{Frac}(R)$. $a_1, \dots, a_6 \in R$.

$\hat{E}(I) = \{(t, w(t)) \in E(k) \mid t \in I\} \leq E(k)$

We apply Lemma 7·2 for R a power series ring.

Take $R = \mathbb{Z}[a_1, \dots, a_6][[t]]$, $I = (t)$ gives

$\iota(t) \in \mathbb{Z}[a_1, \dots, a_6][[t]]$ with $\iota(0) = 0$ such that

$[-1](t, w(t)) = \cancel{(\iota(t), w(\iota(t)))}\ (\iota(t), w(\iota(t)))$

Taking $R = \mathbb{Z}[a_1, \dots, a_6][[t_1, t_2]]$, $I = (t_1, t_2)$

gives $F(t_1, t_2) \in \mathbb{Z}[a_1, \dots, a_6][[t_1, t_2]]$ with $F(0,0) = 0$

such that $(t_1, w(t_1)) \oplus (t_2, w(t_2)) = (F(t_1, t_2), w(F(t_1, t_2)))$

In fact, $\iota(X) = -X - a_1 X^2 - a_2 X^3 - (a_1^3 + a_3) X^4 + \dots$

$F(X, Y) = X + Y - a_1 XY - a_2 (X^2 Y + XY^2) + \dots$

By properties of the group law, we deduce

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

ii) $F(X, 0) = X$, and $F(0, Y) = Y$

iii) $F(F(X, Y), Z) = F(X, F(Y, Z))$

iv) $F(X, \iota(X)) = 0$

Definition

Let R be a ring. A <u>formal group</u> over R is a power series $F \in R[[X,Y]]$ satisfying conditions i), ii) and iii).
commutativity, identity, associativity

Exercise: Show that for any formal group $\exists!\, \imath(X) = -X + \ldots \in R[[X]]$ such that $F(X, \imath(X)) = 0$.

Examples

additive group $\mathbb{G}_a$ — formal group $\hat{\mathbb{G}}_a$

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

ii) $F(X,Y) = X + Y + XY = (1+X)(1+Y) - 1$ — $\hat{\mathbb{G}}_m$ multiplicative group

iii) $F(X,Y) = $ (See above) — $\hat{E}$

Definition

Let F, G be formal groups over R.

i) A morphism $f : F \to G$ is a power series $f \in R[[T]]$ with $f(0) = 0$ satisfying $f(F(X,Y)) = G(f(X), f(Y))$ i.e. a homomorphism

ii) $F \cong G$ if $\exists$ morphisms $f : F \to G$, $g : G \to F$ such that $f(g(T)) = T = g(f(T))$

Theorem 7.3

If $\text{char}(R) = 0$ then every formal group F over R is isomorphic to $\hat{\mathbb{G}}_a$ over $R \otimes \mathbb{Q}$. More precisely

i) There is a unique power series $\log(T) = T + \frac{a_2}{2}T^2 + \frac{a_3}{3}T^3 + \ldots$ with $a_i \in R$. $\log(F(X,Y)) = \log(X) + \log(Y)$ $(*)$

ii) There is a unique power series $\exp(T) = T + \frac{b_2}{2!}T^2 + \frac{b_3}{3!}T^3 + \ldots$ with $b_i \in R$, satisfying $\exp(\log(T)) = T$ and $\log(\exp(T)) = T$

Proof

$F_1(X,Y) = \frac{\partial F}{\partial X}(X,Y)$.

Uniqueness : Let $p(T) = \frac{d}{dT}\log(T) = 1 + a_2 T + a_3 T^2 + \dots$

$\frac{\partial}{\partial X}(*) \Rightarrow \underline{p(F(X,Y))F_1(X,Y)} = p(X)$

$T = F(X,Y)$

$\frac{\partial}{\partial X}\log(F(X,Y)) = \frac{\partial}{\partial X}\log T = \frac{\partial T}{\partial X}\frac{\partial}{\partial T}\log T$

Put $X = 0$ gives $p(Y)F_1(0,Y) = 1$

$\Rightarrow p(Y) = (F_1(0,Y))^{-1}$ $p(0) = 1$

$\log(0) = 0$, so $p(T)$ specifies log uniquely

Existence : Let $p(T) = (F_1(0,T))^{-1} = 1 + a_2 T + a_3 T^2 + \dots$ some $a_i \in R$

Define $\log(T) := T + \frac{a_2}{2}T^2 + \frac{a_3}{3}T^3 + \dots$

$F(F(X,Y),Z) = F(X, F(Y,Z))$ ①

$\frac{\partial}{\partial X}① \Rightarrow F_1(F(X,Y),Z)F_1(X,Y) = F_1(X, F(Y,Z))$ use chain rule if unsure

$X = 0 \Rightarrow F_1(Y,Z)F_1(0,Y) = F_1(0, F(Y,Z))$

$\Rightarrow F_1(Y,Z)p(Y)^{-1} = p(F(Y,Z))^{-1}$

$\Rightarrow F_1(Y,Z)p(F(Y,Z)) = p(Y)$

integrate w.r.t Y $\Rightarrow \log(F(Y,Z)) = \log(Y) + h(Z)$, $h(Z)$ some power series

By symmetry between Y, Z, $h(Z) = \log(Z)$.

For ii) we use

Lemma 7.4

Let $f(T) = aT + \dots \in R[[T]]$ with $a \in R^*$. Then $\exists!\, g(T)$, $g(T) = a^{-1}T + \dots \in R[[T]]$ such that $f(g(T)) = T = g(f(T))$

important for base case of induction

Proof

We construct polynomials $g_n(T) \in R[T]$ such that

i) $f(g_n(T)) \equiv T \pmod{T^{n+1}}$

ii) $g_{n+1}(T) \equiv g_n(T) \pmod{T^{n+1}}$

Then let $g(T) = \lim_{n\to\infty} g_n(T)$. To start the induction, let $g_1(T) = a^{-1}T$. Now suppose $n \geq 2$ and g_{n-1} exists.

$\Rightarrow f(g_{n-1}(T)) \equiv T \pmod{T^n}$, $f(g_{n-1}(T)) \equiv T + bT^n \pmod{T^{n+1}}$

We put $g_n(T) = g_{n-1}(T) + \lambda T^n$ ($\lambda \in R$ to be chosen)

Then $f(g_n(T)) = f(g_{n-1}(T) + \lambda T^n) \equiv f(g_{n-1}(T)) + \lambda a T^n \pmod{T^{n+1}}$

$\equiv T + (b + \lambda a)T^n \pmod{T^{n+1}}$

Idea: Solve for the infinitely many coefficients one by one by induction.

So we take $\lambda = -\frac{b}{a}$ (N.B $a \in R^*$)

We get $g(T) = a^{-1}T + \ldots \in R[[T]]$

such that $f(g(T)) = T$ ① — Hensel's Lemma

Applying the same argument to g gives $h(T) = aT + \ldots \in R[[T]]$

such that $g(h(T)) = T$ ②

Then $f(T) \overset{②}{=} f(g(h(T))) \overset{①}{=} h(T)$

Theorem 7.3 ii) now follows except for showing $b_i \in R$ (not just $R \otimes \mathbb{Q}$).

Hint: Repeatedly differentiate $f(g(T)) = T$ and put $T = 0$.

Shows that each coefficient is an R-combination of the last

05/11/13

Notation

Let $\mathcal{F}$ (e.g. $\hat{G}_a$, $\hat{G}_m$, $\hat{E}$) be a formal group, given by a power series $F \in R[[X, Y]]$. Suppose that R is complete with respect to some ideal I. For $x, y \in I$, we define $x \oplus_{\mathcal{F}} y = F(x, y) \in I$. Then $\mathcal{F}(I) = (I, \oplus_{\mathcal{F}})$ is an abelian group.

Examples

i) $\hat{G}_a(I) = (I, +)$

ii) $\hat{G}_m(I) \cong (1+I, \times)$

In Lemma 7.2 we saw $\hat{E}(I) \overset{\text{subgroup}}{\subset} E(k)$.

Corollary 7.5

Let $\mathcal{F}$ be a formal group over R. Let $n \in \mathbb{Z}$ and suppose $n \in R^*$. Then:

i) $[n] : \mathcal{F} \to \mathcal{F}$ is an isomorphism.

ii) If R is complete with respect to I an ideal, then $\mathcal{F}(I) \xrightarrow{\times n} \mathcal{F}(I)$ is an isomorphism.

In particular, $\mathcal{F}(I)$ has no n-torsion.

Proof

We have $[1](T) = T$. For $n \geq 2$ we put $[n](T) = F([n-1](T), T)$

By induction, we find that $[n](T) = nT + \ldots$

(also works for $n < 0$ e.g. $[-1](T) = \iota(T) = -T + \ldots$)

Lemma 7.4 shows that if $\underbrace{n \in R^* \text{ then } [n]}_{\text{because we can invert the}}$ is an isomorphism. □

8 Elliptic Curves over Local Fields

Let k be a field.

Definition 8·1

$v : k^* \to \mathbb{Z}$ is a discrete valuation iff

i) $v(xy) = v(x) + v(y)$

ii) $v(x+y) \geq \min(v(x), v(y))$ ($v(0)$ is either infinite or undefined)

Examples

i) $k = \mathbb{Q}$, p prime. $v = v_p$ where $v_p(p^r \frac{a}{b}) = r$ with $a, b \in \mathbb{Z}$ coprime to p.

ii) $[k:\mathbb{Q}] < \infty$, ring of integers $\mathcal{O}_k$. $\mathfrak{p} \subset \mathcal{O}_k$ a prime ideal. $v = v_\mathfrak{p}$ where $v_\mathfrak{p}(x)$ is the power of $\mathfrak{p}$ in the factorisation in the factorisation of $x\mathcal{O}_k$ into prime ideals.

Remark

Let $x, y \in k$. Definition 8·1 $\Rightarrow \begin{cases} v(x+y) \geq \min(v(x), v(y)) \\ v(x) \geq \min(v(x+y), \underbrace{v(y)}_{=v(-y)}) \end{cases}$

So if $v(x) < v(y)$ then $v(x+y) = v(x)$.

Hence if $v(x) \neq v(y)$, then $v(x+y) = \min(v(x), v(y))$.

Lemma 8·2

Let E/k be an elliptic curve with Weierstrass equation

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

Assume that $v(a_i) \geq 0$ $\forall i$. Let $0_E \neq P = (x, y) \in E(k)$.

Then either

i) $v(x), v(y) \geq 0$ or

ii) $v(x) = -2r$, $v(y) = -3r$ for some $r \in \mathbb{Z}_{\geq 1}$.

Notation

Let $\mathcal{F}$ (e.g. $\hat{\mathbb{G}}_a$, $\hat{\mathbb{G}}_m$, $\hat{E}$) be a formal group, given by a power series $F \in R[[X,Y]]$. Suppose that R is complete with respect to some ideal I. For $x, y \in I$, we define $x \oplus_{\mathcal{F}} y = F(x,y) \in I$. Then $\mathcal{F}(I) = (I, \oplus_{\mathcal{F}})$ is an abelian group.

Examples

i) $\hat{\mathbb{G}}_a(I) = (I, +)$

ii) $\hat{\mathbb{G}}_m(I) \cong (1+I, \times)$

In Lemma 7.2 we saw $\hat{E}(I) \overset{\text{subgroup}}{\subset} E(K)$.

Corollary 7.5

Let $\mathcal{F}$ be a formal group over R. Let $n \in \mathbb{Z}$ and suppose $n \in R^*$. Then:

i) $[n] : \mathcal{F} \to \mathcal{F}$ is an isomorphism.

ii) If R is complete with respect to I an ideal, then $\mathcal{F}(I) \xrightarrow{\times n} \mathcal{F}(I)$ is an isomorphism.

In particular, $\mathcal{F}(I)$ has no n-torsion.

Proof

We have $[1](T) = T$. For $n \geq 2$ we put $[n](T) = F([n-1](T), T)$

By induction, we find that $[n](T) = nT + \ldots$

(also works for $n < 0$ e.g. $[-1](T) = \iota(T) = -T + \ldots$)

Lemma 7.4 shows that if $\underbrace{n \in R^* \text{ then } [n]}_{\text{because we can invert the}}$ is an isomorphism. □

8 Elliptic Curves over Local Fields

Let k be a field.

Definition 8.1

$v : k^* \to \mathbb{Z}$ is a discrete valuation if

i) $v(xy) = v(x) + v(y)$

ii) $v(x+y) \geq \min(v(x), v(y))$ ($v(0)$ is either infinite or undefined)

Examples

i) $k = \mathbb{Q}$, p prime. $v = v_p$ where $v_p\left(p^r \frac{a}{b}\right) = r$ with $a, b \in \mathbb{Z}$ coprime to p.

ii) $[k:\mathbb{Q}] < \infty$, ring of integers $\mathcal{O}_k$. $\mathfrak{p} \subset \mathcal{O}_k$ a prime ideal. $v = v_{\mathfrak{p}}$ where $v_{\mathfrak{p}}(x)$ is the power of $\mathfrak{p}$ in the factorisation in the factorisation of $x\mathcal{O}_k$ into prime ideals.

Remark

Let $x, y \in k$. Definition 8.1 $\Rightarrow \begin{cases} v(x+y) \geq \min(v(x), v(y)) \\ v(x) \geq \min(v(x+y), \underbrace{v(y)}_{=v(-y)}) \end{cases}$

So if $v(x) < v(y)$ then $v(x+y) = v(x)$.

Hence if $v(x) \neq v(y)$, then $v(x+y) = \min(v(x), v(y))$.

Lemma 8.2

Let E/k be an elliptic curve with Weierstrass equation

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

Assume that $v(a_i) \geq 0$ $\forall i$. Let $0 \neq P = (x, y) \in E(k)$.

Then either

i) $v(x), v(y) \geq 0$ or

ii) $v(x) = -2r$, $v(y) = -3r$ for some $r \in \mathbb{Z}_{\geq 1}$.

05/11/13

Proof

of Weierstrass Equation

The case $v(x) \geq 0$: Suppose $v(y) < 0$. Then $v(LHS) = 2v(y) < 0$ and $v(RHS) \geq 0$ ※ Hence $v(y) \geq 0$.

The case $v(x) < 0$: $v(LHS) \geq \min(2v(y), v(x)+v(y), v(y))$ (*)

$v(LHS) = v(RHS) = 3v(x)$ → Sub $v(y) \geq v(x)$ into (*) gives $3v(x) \geq 2v(x)$, $v(x) \geq 0$ ※

$\therefore v(y) < v(x) < 0$. Then $v(LHS) = 2v(y)$.

→ 2, 3 coprime

Hence $v(x) = -2r$, $v(y) = -3r$, some $r \in \mathbb{Z}_{\geq 1}$ $\square$.

Notation

not to be confused with ring of integers of a number field, though it plays the same role

Valuation ring $\mathcal{O}_K = \{x \in K^* \mid v(x) \geq 0\} \cup \{0\}$

Unit group $\mathcal{O}_K^* = \{x \in K^* \mid v(x) = 0\} \cup \{0\}$

Maximal ideal $\pi\mathcal{O}_K = \{x \in K^* \mid v(x) \geq 1\}$

(i.e. pick $\pi \in K$ with $v(\pi) = 1$) — v surjective after scaling etc.

The residue field $k = \mathcal{O}_K / \pi\mathcal{O}_K$

Definition

A Weierstrass equation for E with coefficients $a_1, \dots, a_6 \in K$ is

i) integral if $a_1, \dots, a_6 \in \mathcal{O}_K$.

ii) minimal if $v(\Delta)$ is minimal among all integral models for E.

Remark

i) Putting $x = u^2 x'$, $y = u^3 y'$ gives $a_i = u^i a_i'$

$\therefore$ integral models exist.

ii) $a_1, \dots, a_6 \in \mathcal{O}_K \Rightarrow \Delta \in \mathcal{O}_K \Rightarrow v(\Delta) \in \mathbb{Z}_{\geq 0}$.

Fix $0 < c < 1$. We define a metric on K by

$$d(x,y) = \begin{cases} c^{v(x-y)} & x \neq y \\ 0 & x = y \end{cases}$$

Definition 8·1 ii) $\Rightarrow d(x,z) \leq \max(d(x,y), d(y,z))$

This is called the Ultra-metric inequality, much stronger than the triangle inequality.

Let $\hat{K}$ be the completion of K with respect to d. By continuity,

i) $+, \times$ extend to functions on $\hat{K}$ making $\hat{K}$ a field

ii) v extends to $\hat{K}$ and is also a discrete valuation

N.B. the residue field does not change.

In Examples i) and ii), we write $\hat{K} = \mathbb{Q}_p$, $K_{\mathfrak{p}}$ respectively.

For the rest of this section, K is a field complete with respect to a discrete valuation $v : K^* \to \mathbb{Z}$. $\mathcal{O}_K$, π, k defined as before.

Further, assume $\mathrm{char}(K) = 0$, $\mathrm{char}(k) = p > 0$.

(e.g. $K = \mathbb{Q}_p$, $\mathcal{O}_K = \mathbb{Z}_p$, $\pi\mathcal{O}_K = p\mathbb{Z}_p$, $k = \mathbb{F}_p$)

K complete $\Rightarrow \mathcal{O}_K$ complete with respect to $\pi^r\mathcal{O}_K$ (any $r \geq 1$)

In Section 7, we put $t = -\frac{x}{y}$, $w = -\frac{1}{y}$

$$\hat{E}(\pi^r\mathcal{O}_K) = \{(x,y) \in E(K) \mid -\tfrac{x}{y}, -\tfrac{1}{y} \in \pi^r\mathcal{O}_K\} \cup \{0\}$$

$$= \{(x,y) \in E(K) \mid v(\tfrac{x}{y}), v(\tfrac{1}{y}) \geq r\} \cup \{0\}$$

Lemma 8·2 $$= \{(x,y) \in E(K) \mid v(x) \leq -2r, v(y) \leq -3r\} \cup \{0\}$$

By Lemma 7·2 this is a subgroup of $E(K)$, say $E_r(K)$

because $\pi^r\mathcal{O}_K$ is an ideal

$v(x) \leq -2r$
$v(y) \leq -3r$
$\Rightarrow v(\frac{x}{y}), v(\frac{1}{y}) \geq r$

$v(x) = -2r_0$
$v(y) = -3r_0$
$v(\frac{x}{y}) \geq r$
$\Rightarrow r_0 \geq r$
$\Rightarrow v(x) \leq -2r$
$v(y) \leq -3r$

$$E_r(K) = \{(x,y) \in E(K) \mid {v(x) \le -2r \atop v(y) \le -3r}\} \cup \{0\}$$

$\hat{E}(\pi\mathcal{O}_K)$ char $(K) = 0$, char $(k) = p$

$\parallel$ $E_1(K) \supset E_2(K) \supset \dots$

More generally, if $\mathcal{F}$ is a formal group over $\mathcal{O}_K$ then

$\mathcal{F}(\pi\mathcal{O}_K) \supset \mathcal{F}(\pi^2\mathcal{O}_K) \supset \dots$

Remember $\hat{G}_a(I) = (I, +)$

<u>Proposition 8.3</u>

Let $\mathcal{F}$ be a formal group over $\mathcal{O}_K$. Let $e = v(p)$. If $r > \frac{e}{p-1}$ then $\log : \mathcal{F}(\pi^r\mathcal{O}_K) \to \hat{G}_a(\pi^r\mathcal{O}_K)$

and $\exp : \hat{G}_a(\pi^r\mathcal{O}_K) \to \mathcal{F}(\pi^r\mathcal{O}_K)$

are inverse group homomorphisms.

Recall properties of log and exp

<u>Proof</u>

Let $x \in \pi^r\mathcal{O}_K$. We must show that the power series exp and log of Theorem 7.3 converge.

Recall $\exp(T) = T + \frac{b_2}{2!}T^2 + \frac{b_3}{3!}T^3 + \dots$ for some $b_2, b_3, \dots \in \mathcal{O}_K$

$$v(n!) = e\,v_p(n!) = e\sum_{j=1}^{m} \left\lfloor \frac{n}{p^j} \right\rfloor \quad , \quad p^m \le n < p^{m+1}$$

$$\le e\sum_{j=1}^{m} \frac{n}{p^j} = en\frac{\frac{1}{p} - \frac{1}{p^{m+1}}}{1 - \frac{1}{p}} = \frac{e}{p-1}\,n\,(1 - p^{-m})$$

$$\le \frac{e}{p-1}(n-1)$$

$v(b_n) \ge 0$ — by hypothesis

$$\therefore v\left(\frac{b_n}{n!}x^n\right) \ge \underbrace{nr}_{\text{from } x^n} - \underbrace{\frac{e}{p-1}(n-1)}_{\text{from } n!} = (n-1)\overbrace{\left(r - \frac{e}{p-1}\right)}^{>0} + r$$

This is $\ge r$ and $\to \infty$ as $n \to \infty$.

$\therefore \exp(x)$ converges and belongs to $\pi^r\mathcal{O}_K$.

Likewise, $\log(x)$ converges and belongs to $\pi^r\mathcal{O}_K$. $\square$

So for r sufficiently large, $\mathcal{F}(\pi^r\mathcal{O}_K) \cong \hat{G}_a(\pi^r\mathcal{O}_K)$

$$\cong (\pi^r\mathcal{O}_K, +) \cong (\mathcal{O}_K, +)$$

F a formal group over R. $F \in R[[X,Y]]$
$\mathcal{F}(I) = (I, \oplus_F)$
$x \oplus_F y := F(x,y)$

Lemma 8.4

If $r \geq 1$, then $\mathcal{F}(\pi^r \mathcal{O}_K) / \mathcal{F}(\pi^{r+1}\mathcal{O}_K) \cong (k, +)$

Proof

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

If $x, y \in \mathcal{O}_K$ then $F(\pi^r x, \pi^r y) \equiv \pi^r(x+y) \pmod{\pi^{r+1}}$

$\mathcal{F}(\pi^r \mathcal{O}_K) \to k \quad , \quad \pi^r x \mapsto x \bmod \pi$

is a group homomorphism. Moreover, it is surjective and has kernel $\mathcal{F}(\pi^{r+1}\mathcal{O}_K)$.

$\therefore \quad \mathcal{F}(\pi^r \mathcal{O}_K) / \mathcal{F}(\pi^{r+1}\mathcal{O}_K) \cong (k, +)$ $\square$

Corollary

If $|k| < \infty$, then $\mathcal{F}(\pi \mathcal{O}_K)$ has a subgroup of finite index isomorphic to $(\mathcal{O}_K, +)$.

For large enough r, $\mathcal{F}(\pi^r \mathcal{O}_K) \cong (\mathcal{O}_K, +)$
If $|k| < \infty$, previous lemma $\Rightarrow$ finite index

Notation

Reduction mod π is $\mathcal{O}_K \to \mathcal{O}_K / \pi \mathcal{O}_K = k$, $x \mapsto \tilde{x}$

Let E/K be an elliptic curve.

Proposition 8.5

The reductions mod π of two minimal Weierstrass equations for E define isomorphic curves over k.

Proof

see formula sheet

Say the Weierstrass equations are related by $[u; r, s, t]$ where $u \in K^*$ and $r, s, t \in K$. Then $\Delta_1 = u^{12}\Delta_2$

Both equations are minimal $\Rightarrow v(\Delta_1) = v(\Delta_2)$

$\Rightarrow v(u) = 0$ i.e. u is a unit, $u \in \mathcal{O}_K^*$.

Transformation formulae for a_i's and b_i's $\Rightarrow r, s, t \in \mathcal{O}_K$.

e.g. $u^2 b_2' = b_2 + 12r$. The Weierstrass equations for the reduction

Clear when not in char 2 or 3

π are now related by $[\tilde{u}^{*0}; \tilde{r}, \tilde{s}, \tilde{t}]$ $\square$

Definition

The reduction $\tilde{E}/k$ of E/K is defined by the reduction of a minimal Weierstrass equation mod π. E has good reduction if $\tilde{E}$ is non-singular ($\Leftrightarrow \tilde{E}$ is an elliptic curve) otherwise bad reduction.

For an integral Weierstrass equation $v(\Delta) = 0 \Rightarrow$ good reduction

$0 < v(\Delta) < 12 \Rightarrow$ bad reduction

$v(\Delta) \geq 12 \Rightarrow$ Weierstrass equation might not be minimal.

There is a well defined map $\mathbb{P}^2(K) \to \mathbb{P}^2(k)$, $(x:y:z) \mapsto (\tilde{x}:\tilde{y}:\tilde{z})$

Note that before reduction we choose a representative $(x:y:z)$ so that $\min(v(x), v(y), v(z)) = 0$.

We restrict this map to get $E(K) \to \tilde{E}(k)$, $P \mapsto \tilde{P}$

Lemma 8.2 $\Rightarrow E_1(K) = \{P \in E(K) \mid \tilde{P} = 0\}$ $= \hat{E}(\pi\mathcal{O}_K) = \{P \in E(K) : v(x) \leq -2, v(y) \leq -3\}$

$0 = 0_E = (0:1:0)$

Let $\tilde{E}_{ns} = \begin{cases} \tilde{E} & \text{if } E \text{ has good reduction} \\ \tilde{E} \setminus \{\text{singular points}\} & \text{if } E \text{ has bad reduction} \end{cases}$

non singular

The chord and tangent process defines a group law on $\tilde{E}_{ns}$.

In the case of bad reduction

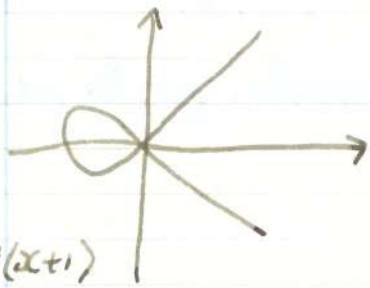
$\underset{\text{over } \bar{k}}{\tilde{E}_{ns} \cong} \ \mathbb{G}_a$ or $\mathbb{G}_m$

additive reduction — multiplicative reduction

For simplicity, assume char$(k) \neq 2$.

$\tilde{E}: y^2 = f(x)$, $\deg(f) = 3$.

Double Root

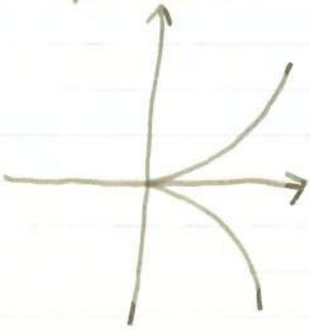


$y^2 = x^2(x+1)$

Curve with node

Multiplicative Reduction

Triple Root

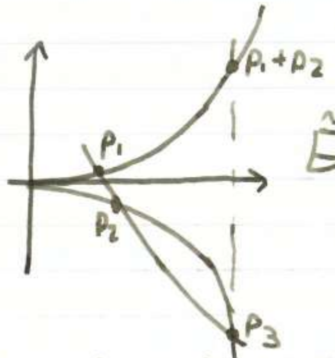


$y^2 = x^3$

Curve with cusp

Additive Reduction

09/11/13 Elliptic Curves (15)



$\tilde{E} : y^2 = x^3$

$\mathbb{G}_a \xrightarrow{\sim} \tilde{E}_{ns}$, $t \mapsto (t^{-2}, t^{-3})$

$0 \mapsto 0_{\tilde{E}}$

$x/y \longleftarrow (x, y)$

We check that this is a group homomorphism:

Let P_1, P_2, P_3 lie on the line $ax + by = 1$. Let $P_i = (x_i, y_i)$.

$\Rightarrow x_i^3 = y_i^2 = y_i^2 (a x_i + b y_i)$

$\Rightarrow t_i = x_i / y_i$ is a root of $X^3 - aX - b = 0$

$\Rightarrow t_1 + t_2 + t_3 = 0$ The same check but for multiplicative reduction is on an ex. sheet

<u>Definition</u>

$E_0(K) := \{ P \in E(K) \mid \tilde{P} \in \tilde{E}_{ns}(k) \}$

<u>Proposition 8.6</u>

$E_0(K) \subset E(K)$ is a subgroup and reduction mod π is a surjective group homomorphism $E_0(K) \to \tilde{E}_{ns}(k)$.

<u>Proof</u>

(group homomorphism) A line in $\mathbb{P}^2$ defined over K is given by $aX + bY + cZ = 0$ with $a, b, c \in K$ not all 0. We may assume that $\min(v(a), v(b), v(c)) = 0$ (by scaling a, b, c by π)

Reduction mod π gives a line $\tilde{a}X + \tilde{b}Y + \tilde{c}Z = 0$.

At least one of a, b, c is a unit, hence non-zero, so this defines a line.

If $P_1, P_2, P_3 \in E(K)$ with $P_1 + P_2 + P_3 = 0$, then they lie on a line L. Then $\tilde{P}_1, \tilde{P}_2, \tilde{P}_3 \in \tilde{E}(k)$ lie on the line $\tilde{L}$.

If $\tilde{P}_1, \tilde{P}_2 \in \tilde{E}_{ns}(k)$ then $\tilde{P}_3 \in \tilde{E}_{ns}(k)$. So if $P_1, P_2 \in E_0(K)$

then $P_3 \in E_0(k)$ and $\tilde{P}_1 + \tilde{P}_2 + \tilde{P}_3 = 0$.

(Surjective) $f(x,y) = y^2 + a_1 xy + a_3 y - x^3 - a_2 x^2 - a_4 x - a_6$

Let $\tilde{P} \in \tilde{E}_{ns}(k) \setminus \{0\}$, say $\tilde{P} = (\tilde{x}_0, \tilde{y}_0)$ for some $x_0, y_0 \in \mathcal{O}$

$\tilde{P}$ non-singular $\Rightarrow$ either $\frac{\partial f}{\partial x}(x_0, y_0) \not\equiv 0 \pmod{\pi}$ (i)

or $\frac{\partial f}{\partial y}(x_0, y_0) \not\equiv 0 \pmod{\pi}$ (ii)

Case (i): Let $g(t) = f(t, y_0) \in \mathcal{O}_K[t]$

Then $g(x_0) \equiv 0 \pmod{\pi}$, $g'(x_0) \in \mathcal{O}_K^*$ (since $g'(x_0) \not\equiv 0 \pmod{\pi}$)

Hensel's Lemma $\Rightarrow \exists b \in \mathcal{O}_K$ such that

Lift x_0 to b $\rightarrow g(b) = 0$, $b \equiv x_0 \pmod{\pi}$. Then $P = (b, y_0) \in E(K)$

reduces to $\tilde{P} = (\tilde{x}_0, \tilde{y}_0)$ (In fact, $P \in E_0(K)$ because $\tilde{P} \in \tilde{E}_{ns}(k) \setminus \{0\}$).

Case (ii) works similarly. □

$$\begin{array}{ccccccccc}
\hat{E}(\pi^r \mathcal{O}_K) & & & & \hat{E}(\pi \mathcal{O}_K) & & & & \\
\wr\wr & & & & \wr\wr & & & & \\
E_r(K) & \subset \ldots\ldots \subset & E_2(K) & \subset & E_1(K) & \subset & E_0(K) & \subset & E(K) \\
\wr\wr & & & & & & & & \\
(\mathcal{O}_K, +) & & & & & & & & \\
(\text{if } r > \frac{e}{p-1}) & & & & & & & &
\end{array}$$

quotient $\cong (k, +)$ $\qquad$ $E_0(K)/E_1(K) \cong \tilde{E}_{ns}(k)$

<u>Lemma 8·7</u>

If $|k| < \infty$ then $\mathbb{P}^2(K)$ is compact (wrt π-adic topology)

<u>Proof</u>

$$\pi^r \mathcal{O}_K / \pi^{r+1} \mathcal{O}_K \cong \mathcal{O}_K / \pi \mathcal{O}_K \cong k$$

$$\pi^r x \pmod{\pi^{r+1}} \mapsto x \bmod \pi$$

k finite $\Rightarrow \mathcal{O}_K / \pi^r \mathcal{O}_K$ finite $\forall r$.

Let (x_n) be a sequence in $\mathcal{O}_K$. (x_n) has a subsequence $(x_n^{(1)})$ that is constant mod π (since $\mathcal{O}_K/\pi\mathcal{O}_K$ finite). Similarly, this has a subsequence $(x_n^{(2)})$, constant mod π^2. Continuing inductively, we find that $(x_n^{(n)})$ is a Cauchy sequence, hence converges.

$\therefore \mathcal{O}_K$ is sequentially compact, hence compact.

$\mathbb{P}^n(K)$ is the union of the compact sets of the form

scale by π $\Rightarrow \{ (a_0 : a_1 : \dots : a_{i-1} : 1 : a_{i+1} : \dots : a_n) \mid a_j \in \mathcal{O}_K \}$

compact since it is a direct product of copies of $\mathcal{O}_K$. □

Hence $\mathbb{P}^n(K)$ is compact.

Lemma 8.8 $(|k| < \infty)$

closed subspace of a compact space is compact

$E_0(K) \subset E(K)$ has finite index.

check that group operations are continuous

Proof

$E(K) \subset \mathbb{P}^2(K)$ is a closed subset and hence is a compact topological group.

If $\tilde{E}$ has singular point $(\tilde{x}_0, \tilde{y}_0)$

$E(K) \setminus E_0(K) = \left\{ (x,y) \in E(K) \;\middle|\; \begin{matrix} v(x-x_0) \geq 1 \\ v(y-y_0) \geq 1 \end{matrix} \right\}$

points which map to singular points under reduction

This is a closed subset, so $E_0(K) \subset E(K)$ is an open subgroup.

The cosets of $E_0(K)$ in $E(K)$ are an open cover.

$E(K)$ compact $\Rightarrow [E(K) : E_0(K)] < \infty$. □

Remark $c_K(E)$, the Tamagawa Number

Good reduction $\Rightarrow c_K(E) = 1$

But the converse is false.

Fact

Either $c_K(E) = v(\Delta)$

or $c_K(E) \leq 4$

Lemma 8.8 : Group Ops are continuous

~~Need only check around O~~

Inverses $(x,y) \mapsto (x,-y)$
Clearly continuous

Theorem 8.9

Let K be a field complete with respect to a discrete valuation, with $\mathrm{char}(K) = 0$, finite residue field. Then $E(K)$ contains a subgroup of finite index $\cong (\mathcal{O}_K, +)$.

In particular $E(K)_{tors}$ is finite.

Remark

The fields in Theorem 8.9 are the finite extensions of $\mathbb{Q}_p$.

because

$$H = E(K) / (\mathcal{O}_K, +) \text{ is finite}$$

$$P \in E(K)_{tors} \Rightarrow P + (\mathcal{O}_K, +) \text{ is non-zero in } H$$

If $P - Q \in (\mathcal{O}_K, +)$, $P, Q \in E(K)_{tors}$

then $P - Q = t \in \mathcal{O}_K$

P, Q torsion $\Rightarrow Nt = 0$, $N = \mathrm{lcm}(\mathrm{order}(P), \mathrm{order}(Q))$

$\times$ as $t \in (\mathcal{O}_K, +)$, torsion free

$\therefore$ $E(K)_{tors}$ injects into H

$\therefore$ $E(K)_{tors}$ finite

12/11/13

Elliptic Curves (16)

Let K be a finite extension of $\mathbb{Q}_p$.

N.B K is complete with respect to v_K.

$$\begin{array}{ccc} K^* & \overset{v_K}{\twoheadrightarrow} & \mathbb{Z} \\ \cap & & \downarrow \times e \\ L^* & \overset{v_L}{\twoheadrightarrow} & \mathbb{Z} \end{array}$$

Let L/K be a finite extension. $[L:K] = ef$ where $f = [k':k]$ and k, k' are the residue fields of K and L respectively. $\mathrm{char}(k) = p$

If L/K is Galois then there is a natural group homomorphism

$\mathrm{Gal}(L/K) \to \mathrm{Gal}(k'/k)$

This map is surjective, with kernel of order e.

Definition

L/K is <u>unramified</u> if $e = 1$.

Fact

For each $m \geq 1$,

i) k has a unique extension of degree m

ii) K has a unique <u>unramified</u> extension of degree m.

These extensions are Galois, with cyclic Galois group.

c.f. Algebraic Number Theory

Theorem 8·10

$[K:\mathbb{Q}_p] < \infty$. Suppose E/K has good reduction, and $p \nmid n$.
If $P \in E(K)$ then $K([n]^{-1}P)/K$ is unramified.

Notation

i) $[n]^{-1}P = \{Q \in E(\bar{K}) : nQ = P\}$

ii) $K(\{P_1, \dots, P_r\}) = K(x_1, \dots, x_r, y_1, \dots, y_r)$, $P_i = (x_i, y_i)$

__Proof__

$[n] : \tilde{E} \to \tilde{E}$ is a separable isogeny since $p \nmid n$.

$\therefore \ \#[n]^{-1}\tilde{P} = \deg[n] = n^2 \quad \left([n]^{-1}\tilde{P} = \{Q' \in \tilde{E}(\bar{k}) : nQ' = \tilde{P}\}\right)$

$k' = k([n]^{-1}\tilde{P})$. Let $m = [k' : k]$. Let L/K be the unramified extension of degree m (so L has residue field k'). We claim that each $Q' \in \tilde{E}(k')$ with $nQ' = \tilde{P}$ is the reduction of some $Q \in E(L)$ with $nQ = P$.

reduces to $0_{\tilde{E}}$

Proposition 8.6 $\Rightarrow \exists\, Q_0 \in E(L)$ reducing to Q'. Then $nQ_0 - P \in E_1(L)$.

$E_0(K) \to \tilde{E}_{ns}(k)$ surjective

Corollary 7.5 $\Rightarrow nQ_0 - P = nQ_1$ for some $Q_1 \in E_1(L)$. important

$p \nmid n$

$\Rightarrow P = n(Q_0 + Q_1)$. Taking $Q = Q_0 + Q_1$ proves the claim.

says $[n]$ is an isomorphism

$E_1(L) \cong \hat{E}(\pi_L\mathcal{O}_L)$ has no n-torsion

Therefore all n^2 points $[n]^{-1}P$ are defined over L.

$\Rightarrow K([n]^{-1}P) \subset L \quad \Rightarrow K([n]^{-1}P)/K$ is unramified $\square$

9 The Torsion Subgroup

$[K : \mathbb{Q}] < \infty$.

__Notation__

i) $\underline{p}$ a prime ideal of K (i.e. of $\mathcal{O}_K$)

ii) $K_{\underline{p}}$ = completion of K wrt $\underline{p}$-adic valuation.

Residue field $k_{\underline{p}} = \mathcal{O}_K/\underline{p}$

__Definition__

E has __good reduction__ at $\underline{p}$ if $E/K_{\underline{p}}$ has good reduction.

__Lemma 9.1__

E/K has only finitely many bad primes.

12/11/13 Elliptic Curves (16)

Proof

Take a Weierstrass equation for E with $a_1, \dots, a_6 \in \mathcal{O}_K$.

E non-singular $\Rightarrow 0 \neq \Delta \in \mathcal{O}_K$.

Write $(\Delta) = \underline{p_1}^{\alpha_1} \dots \underline{p_r}^{\alpha_r}$, factorisation into prime ideals.

Let $S = \{\underline{p_1}, \dots, \underline{p_r}\}$. If $\underline{p} \notin S$ then $v_{\underline{p}}(\Delta) = 0$

$\Rightarrow E/K_{\underline{p}}$ has good reduction.

$\therefore \{\text{bad primes for } E\} \subset S$ □

Remark

If K has class number 1 (e.g. $K = \mathbb{Q}$) then we can find a Weierstrass equation for E with $a_1, \dots, a_6 \in \mathcal{O}_K$ which is minimal at all primes $\underline{p}$.

Lemma 9.2

$E(K)_{tors}$ is finite.

Proof

Take any prime $\underline{p}$. $K \subset K_{\underline{p}} \Rightarrow E(K) \subset E(K_{\underline{p}})$

$\Rightarrow E(K)_{tors} \subset E(K_{\underline{p}})_{tors}$. Then apply Theorem 8.9. □
Says $E(K_{\underline{p}})_{tors}$ is finite

Lemma 9.3

Let $\underline{p}$ be a prime of good reduction, with $\underline{p} \nmid (n)$. Then reduction mod $\underline{p}$ gives an injection $E(K)[n] \hookrightarrow \tilde{E}(k_{\underline{p}})[n]$.

Proof

$\rightarrow E_0(K_{\underline{p}}) \twoheadrightarrow \tilde{E}_{ns}(k_{\underline{p}})$

Proposition 8.6 $\Rightarrow E(K_{\underline{p}}) \rightarrow \tilde{E}(k_{\underline{p}})$ is a group homomorphism, with kernel $E_1(K_{\underline{p}})$. Corollary 7.5 $\Rightarrow E_1(K_{\underline{p}})$ has no n-torsion. □

$\underline{p} \nmid n$ $\quad n \in K_{\underline{p}}^* \Rightarrow \hat{E}(\pi \mathcal{O}_{K_{\underline{p}}})$ has no n-torsion

Examples

1. $E/\mathbb{Q} : y^2 + y = x^3 - x^2$. $\Delta = -11$

E has good reduction at all $p \neq 11$.

p	2	3	5	7	11	13
$\#\tilde{E}(\mathbb{F}_p)$	5	5	5	10	–	10

Hence $\#E(\mathbb{Q})_{tors} \mid 5 \cdot 2^a$ for some $a \geq 0$. ($p=2$)

and $\#E(\mathbb{Q})_{tors} \mid 5 \cdot 3^b$, for some $b \geq 0$. ($p=3$)

$\Rightarrow \#E(\mathbb{Q})_{tors} \mid 5$. Let $T = (0,0) \in E(\mathbb{Q})$. Calculation $\Rightarrow 5T = ($

$\therefore E(\mathbb{Q})_{tors} \cong \mathbb{Z}/5\mathbb{Z}$

2. $E/\mathbb{Q} : y^2 + y = x^3 + x^2$. $\Delta = -43$.

E has good reduction at all $p \neq 43$.

p	2	3	5	7	11	13
$\#\tilde{E}(\mathbb{F}_p)$	5	6	10	8	9	19

Hence $\#E(\mathbb{Q})_{tors} \mid 5 \cdot 2^a$ some $a \geq 0$ ($p=2$)

$\#E(\mathbb{Q})_{tors} \mid 9 \cdot 11^b$ some $b \geq 0$ ($p=11$)

$\therefore E(\mathbb{Q})_{tors} = \{0_E\}$

$\therefore T = (0,0) \in E(\mathbb{Q})$ is a point of infinite order.

$\Rightarrow \operatorname{rank} E(\mathbb{Q}) \geq 1$.

Works by 9.3. $E/\mathbb{Q}$

E has good reduction at p

$\Rightarrow$ the p-free part of the torsion subgroup injects into $\tilde{E}(\mathbb{F}_p)$

the p-part is a p-group

So $\#E(\mathbb{Q})_{tors} \mid \tilde{E}(\mathbb{F}_p) \times p^a$, some $a \in \mathbb{Z}_{\geq 0}$

14/11/13 Elliptic Curves (17)

Examples

3. $E_D : y^2 = x^3 - D^2 x$, D squarefree, $\Delta = 2^6 D^6$

$E_D(\mathbb{Q})_{tors} \supset \{0, (0,0), (\pm D, 0)\} \cong (\mathbb{Z}/2\mathbb{Z})^2$

Let $f(x) = x^3 - D^2 x$. If $p \nmid 2D$ so that E_D has good reduction

$\# \tilde{E}_D(\mathbb{F}_p) = 1 + \sum_{x \in \mathbb{F}_p} \left(\left(\frac{f(x)}{p} \right) + 1 \right)$

If $p \equiv 3 \ (4)$, then since f is an odd function,

$\left(\frac{f(-x)}{p} \right) = \left(\frac{-f(x)}{p} \right) = \left(\frac{-1}{p} \right) \left(\frac{f(x)}{p} \right) = -\left(\frac{f(x)}{p} \right)$

$\therefore \ \# \tilde{E}_D(\mathbb{F}_p) = p + 1$

Let $m = \# E(\mathbb{Q})_{tors}$. We have $4 \mid m \mid p+1$ for all sufficiently large primes p with $p \equiv 3 \ (4)$.

$\Rightarrow m = 4$ otherwise we contadict Dirichlet's Theorem on primes in Arithmetic Progressions. So $E_D(\mathbb{Q})_{tors} \cong (\mathbb{Z}/2\mathbb{Z})^2$

$\hookrightarrow$ it would mean that $\forall p >> 0$, $p \equiv 3(4)$, we have $p \equiv -1 \ (m)$ ※

Note

rank $E_D(\mathbb{Q}) \geq 1 \iff \exists x, y \in \mathbb{Q}, y \neq 0$ such that $y^2 = x^3 - D^2 x$

(Lecture 1) $\iff D$ is a congruent number.

Lemma 9.4

Let $E/\mathbb{Q}$ be given by a Weierstrass equation with coefficients $a_1, \ldots, a_6 \in \mathbb{Z}$. Suppose $0 \neq T \in E(\mathbb{Q})_{tors}$, say $T = (x, y)$.

Then

i) $4x, 8y \in \mathbb{Z}$. idea: look modulo each prime p different result for $p=2$

ii) If $2 \mid a_1$, or $2T \neq 0$, then $x, y \in \mathbb{Z}$.

Proof

i) The Weierstrass equation for E defines a formal group $\hat{E}$ over $\mathbb{Z}$.

$\hat{E}(p^r \mathbb{Z}_p) \cong \left\{ (x,y) \in E(\mathbb{Q}_p) \;\middle|\; \begin{matrix} v_p(x) \leq -2r \\ v_p(y) \leq -3r \end{matrix} \right\} \cup \{0\}$

Proposition 8·3 $\Rightarrow \hat{E}(p^r \mathbb{Z}_p) \cong (\mathbb{Z}_p, +)$ for $r > \frac{1}{p-1}$ (c.f. $\frac{e}{p-1}$, $e = v(p)$)

$\Rightarrow \begin{cases} \hat{E}(4\mathbb{Z}_2) & r > 1 \\ \hat{E}(p\mathbb{Z}_p) \ \forall \text{odd } p \end{cases}$ are torsion-free. $r \geq 1$

So by Lemma 8·2, $v_2(x) \geq -2$, $v_2(y) \geq -3$. since $P = (x,y)$ is torsion and ~~torsion~~ $v_p(x) \leq -4$, $v_p(y) \leq -6$ are torsion free

Similarly, $v_p(x) \geq 0$, $v_p(y) \geq 0$ $\forall$ odd primes p.

This proves i).

$v_2(x) \leq -2$, $v_2(y) \leq -3$ — but we have equality by part (i)

ii) Suppose $T \in \hat{E}(2\mathbb{Z}_2)$. Since $\hat{E}(2\mathbb{Z}_2) / \hat{E}(4\mathbb{Z}_2) \cong (\mathbb{F}_2, +)$ (Lemma 8·4)

and $\hat{E}(4\mathbb{Z}_2)$ is torsion-free, We deduce that $2T = 0$. as $T \notin \hat{E}(4\mathbb{Z}_2)$ because T is torsion

i.e. $(x,y) \notin \mathbb{Z}^2$

$\Rightarrow (x,y) = T = -T = (x, -y - a_1 x - a_3)$

$\Rightarrow 2y + a_1 x + a_3 = 0$

$\Rightarrow \underbrace{8y}_{\text{odd}} + a_1 \underbrace{(4x)}_{\text{odd}} + \underbrace{4a_3}_{\text{even}} = 0 \quad \Rightarrow a_1$ is odd.

So if a_1 is even, or $2T \neq 0$, then we deduce $x, y \in \mathbb{Z}$. $\square$

because we must have $v_2(x), v_2(y) \geq 0$

Example

$y^2 + xy = x^3 + 4x + 1$, $\left(-\frac{1}{4}, \frac{1}{8}\right) \in E(\mathbb{Q})[2]$.

Corollary 9·5 (Lutz - Nagell)

$E/\mathbb{Q}$ an elliptic curve given by a Weierstrass equation $y^2 = x^3 + ax + b$,

$a, b \in \mathbb{Z}$. Suppose that $0 \neq T \in E(\mathbb{Q})_{tors}$, say $T = (x,y)$.

Then $x, y \in \mathbb{Z}$, and either $y = 0$ or $y^2 \mid (4a^3 + 27b^2)$

Proof

because $a_1 = 0$ hence a_1 even

Lemma 9.4 $\Rightarrow x, y \in \mathbb{Z}$. If $2T = 0$ then $y = 0$. Suppose that $2T \neq 0$, say $2T = (x_2, y_2)$. Let $f(x) = x^3 + ax + b$

$x_2 = \left(\frac{f'(x)}{2y}\right)^2 - 2x$.

Lemma 9.4 $\Rightarrow x_2, y_2 \in \mathbb{Z}$. $\therefore y \mid f'(x)$.

E non-singular $\Rightarrow f(x), f'(x)$ are coprime $\Rightarrow f(x), f'(x)^2$ are coprime.

$\Rightarrow \exists g, h \in \mathbb{Q}[x]$ such that $g(x)f(x) + h(x)f'(x)^2 = 1$.

A calculation gives $(3X^2+4a)f'(X)^2 - 27(X^3+aX-b)f(X) = 4a^3 + 27b$

Since $y \mid f'(x)$, $y^2 = f(x) \Rightarrow y^2 \mid (4a^3 + 27b^2)$ $\square$

Remark

Mazur has shown that if $E/\mathbb{Q}$ is an elliptic curve, then

$$E(\mathbb{Q})_{tors} \cong \begin{cases} \mathbb{Z}/n\mathbb{Z} & 1 \leq n \leq 12,\ n \neq 11 \\ \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2n\mathbb{Z} & 1 \leq n \leq 4 \end{cases}$$

Moreover, all of these possibilities occur.

10 Kummer Theory

K a field, $\mathrm{char}(K) \nmid n$, and assume that $\mu_n \subset K$.

Lemma 10.1

means adjoin n^{th} roots of each coset representative of Δ

Let $\Delta \subset K^*/(K^*)^n$ be a finite subgroup. Let $L = K(\sqrt[n]{\Delta})$

Then L/K is Galois and $\mathrm{Gal}(L/K) \cong \mathrm{Hom}(\Delta, \mu_n)$

Proof

normality — separability

L/K is Galois since $\mu_n \subset K$ and $\mathrm{char}(K) \nmid n$.

Define the Kummer pairing $\langle\ ,\ \rangle : \mathrm{Gal}(L/K) \times \Delta \to \mu_n$
$$(\sigma, x) \mapsto \frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}}$$

Well-defined: Suppose that $\alpha^n = \beta^n = x$.

$\Rightarrow \left(\frac{\alpha}{\beta}\right)^n = 1 \Rightarrow \frac{\alpha}{\beta} \in \mu_n \subset k$, so fixed by $\mathrm{Gal}(L/k)$.

$\Rightarrow \sigma\left(\frac{\alpha}{\beta}\right) = \frac{\alpha}{\beta} \Rightarrow \underbrace{\frac{\sigma(\alpha)}{\alpha} = \frac{\sigma(\beta)}{\beta}}_{}$ $= \frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}}$ since the map is well defined as above

Bilinear: $\langle \sigma\tau, x\rangle = \frac{\sigma\tau(\sqrt[n]{x})}{\sqrt[n]{x}} = \frac{\sigma\tau(\sqrt[n]{x})}{\tau(\sqrt[n]{x})}\frac{\tau(\sqrt[n]{x})}{\sqrt[n]{x}} = \langle \sigma, x\rangle\langle \tau, x\rangle$

$\langle \sigma, xy\rangle = \frac{\sigma(\sqrt[n]{xy})}{\sqrt[n]{xy}} = \frac{\sigma(\sqrt[n]{x})\,\sigma(\sqrt[n]{y})}{\sqrt[n]{x}\ \sqrt[n]{y}} = \langle \sigma, x\rangle\langle \sigma, y\rangle$

Non-degenerate: If $\langle \sigma, x\rangle = 1 \ \forall x \in \Delta$, then

$\sigma(\sqrt[n]{x}) = \sqrt[n]{x} \ \forall x \in \Delta \Rightarrow \sigma$ fixes L pointwise, i.e. $\sigma = 1$.

If $\langle \sigma, x\rangle = 1 \ \forall \sigma \in \mathrm{Gal}(L/k)$

$\Rightarrow \sigma(\sqrt[n]{x}) = \sqrt[n]{x} \ \forall \sigma \in \mathrm{Gal}(L/k)$

$\Rightarrow \sqrt[n]{x} \in k^* \Rightarrow x \in (k^*)^n$ i.e. $x(k^*)^n = 1$ in Δ

We get injective group homomorphisms

$$\mathrm{Gal}(L/k) \hookrightarrow \mathrm{Hom}(\Delta, \mu_n)$$

$$\Delta \hookrightarrow \mathrm{Hom}(\mathrm{Gal}(L/k), \mu_n)$$

16/11/13

Elliptic Curves (18)

$\mathrm{char}(k) \nmid n$, $\mu_n \subset k$.

Lemma 10·1

If $L = k(\sqrt[n]{\Delta})$ then L/k Galois, $\mathrm{Gal}(L/k) \cong \mathrm{Hom}(\Delta, \mu_n)$

Proof (continued)

The Kummer pairing induces group homomorphisms

i) $\mathrm{Gal}(L/k) \xhookrightarrow{\theta_1} \mathrm{Hom}(\Delta, \mu_n)$ $\quad \theta_1(\sigma) = \langle \sigma, \cdot \rangle$

ii) $\Delta \xhookrightarrow{\theta_2} \mathrm{Hom}(\mathrm{Gal}(L/k), \mu_n)$ $\quad \theta_2(x) = \langle \cdot, x \rangle$

use Structure Theorem

A a finite abelian group $|\mathrm{Hom}(A, \mathbb{C}^*)| = |A|$

By i) $\mathrm{Gal}(L/k)$ is an abelian group of exponent dividing n. so we can use

smallest +ve integer n such that $g^n = e$ $\forall g \in G$, G a group

So $|\mathrm{Gal}(L/k)| \overset{(i)}{\leq} |\Delta| \overset{(ii)}{\leq} |\mathrm{Gal}(L/k)|$

use properties of the pairing

$\therefore$ Both i), ii) are isomorphisms. $\square$

Theorem 10·2

There is a bijection

$$\left\{ \begin{array}{l} \text{finite subgroups} \\ \text{of } k^*/(k^*)^n \end{array} \right\} \leftrightarrow \left\{ \text{finite abelian extensions of } L/k \text{ of exponent dividing } n \right\}$$

$$\Delta \longmapsto k(\sqrt[n]{\Delta})$$

$$\frac{(L^*)^n \cap k^*}{(k^*)^n} \longleftarrow L$$

Proof

Let L/k be an abelian extension of exponent dividing n.

Let $\Delta = \frac{(L^*)^n \cap k^*}{(k^*)^n}$. Then $k(\sqrt[n]{\Delta}) \subset L$.

then proof of 10·1 shows that Δ is finite

Let $G = \mathrm{Gal}(L/k)$. The Kummer pairing gives an injection

$\Delta \xhookrightarrow{\theta} \mathrm{Hom}(G, \mu_n)$. $\quad \theta : \Delta \hookrightarrow \mathrm{Hom}(G, \mu_n)$, $x \mapsto \langle \cdot, x \rangle$

Aim: to show that this map is surjective.

Let $\chi : G \to \mu_n$ be a group homomorphism.

fact from Galois Theory

Since distinct automorphisms are linearly independent, $\exists a \in L$ with

$y = \sum_{\tau \in G} \chi(\tau)^{-1}\tau(a) \neq 0$. Let $\sigma \in G$. otherwise this is a linear dependence

Then $\sigma(y) = \sum_{\tau \in G} \chi(\tau)^{-1}\sigma\tau(a)$ fixed by σ, $\mu_n \in K$.

$= \sum_{\tau \in G} \chi(\sigma^{-1}\tau)^{-1}\tau(a)$ ⟵ change variable of summation

$= \chi(\sigma)\sum_{\tau \in G}\chi(\tau)^{-1}\tau(a) = \chi(\sigma)\, y$

$\Rightarrow \sigma(y^n) = y^n \ \forall \sigma \in G.$ ⟵ $\chi(\sigma) \in \mu_n$

$\Rightarrow x = y^n \in K^* \cap (L^*)^n$

Then $x \in \Delta$ (x is a coset representative for an element of Δ)

and $\chi : \sigma \mapsto \frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}}$ as $\chi(\sigma) = \frac{\sigma(y)}{y}$. So Θ hits χ $\therefore \Theta$ surjective

Now $\Delta \xrightarrow{\sim} \mathrm{Hom}(G, \mu_n) \Rightarrow |\Delta| = |G|$. use Lemma 10·1

$\Rightarrow [K(\sqrt[n]{\Delta}) : K] = [L : K]$

But $K(\sqrt[n]{\Delta}) \subset L$, hence $L = K(\sqrt[n]{\Delta})$ → So each L arises from a Δ

It remains to show that if $\Delta \subset \frac{K^*}{(K^*)^n}$ a finite subgroup,

$L = K(\sqrt[n]{\Delta})$ and $\Delta' = \frac{(L^*)^n \cap K^*}{(K^*)^n}$, then $\Delta = \Delta'$.

It is clear that $\Delta \subset \Delta'$ $x \in \Delta \Rightarrow \sqrt[n]{x} \in L \Rightarrow x \in (L^*)^n \Rightarrow x \in \Delta'$

$\Rightarrow L = K(\sqrt[n]{\Delta}) \subset K(\sqrt[n]{\Delta'}) \subset L.$

$\Rightarrow K(\sqrt[n]{\Delta}) = K(\sqrt[n]{\Delta'}) \Rightarrow |\Delta| = |\Delta'|$ by Lemma 10·1.

Since $\Delta \subset \Delta'$, we have $\Delta = \Delta'$. → So different Δ produces different L $\square$

<u>Proposition 10·3</u>

Let K be a number field, $\mu_n \subset K$. Let S be a finite set of prime ideals of K (really $\mathcal{O}_K$). There are only finitely many extensions L/K such that

16/11/13 Elliptic Curves (18)

i) L/K is abelian of exponent dividing n. (finite)

ii) L/K is unramified at all primes $\underline{p} \notin S$.

Proof

Theorem 10·2 $\Rightarrow L = K(\sqrt[n]{\Delta})$ for some finite subgroup $\Delta \subset K^*/(K^*)^n$

Let $\underline{p}$ be a prime of K.

$\underline{p}\mathcal{O}_K = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_r^{e_r}$, $\mathfrak{P}_i$ primes of L.

Let $x \in K^*$ represent an element of Δ.

$n v_{\mathfrak{P}_i}(\sqrt[n]{x}) = v_{\mathfrak{P}_i}(x) = e_i v_{\underline{p}}(x)$

If $\underline{p} \notin S$ then all $e_i = 1$, so $v_{\underline{p}}(x) \underset{= n v_{\mathfrak{P}_i}(\sqrt[n]{x})}{\equiv} 0 \ (n)$.

$\therefore \Delta$ is contained in $K(S,n) = \{x \in K^*/(K^*)^n \mid v_{\underline{p}}(x) \equiv 0 (n) \ \forall \underline{p} \notin S\}$

We complete the proof with a Lemma:

Lemma 10·4

$K(S,n)$ is finite. So there are only finitely many possible Δs.

Proof

The map $K(S,n) \rightarrow (\mathbb{Z}/n\mathbb{Z})^{|S|}$

$$x(K^*)^n \mapsto (v_{\underline{p}}(x) \bmod n)_{\underline{p} \in S}$$

has kernel $K(\phi, n)$. So it suffices to prove the lemma for $S = \phi$. which has finite index in $K(S,n)$ so $K(\phi,n)$ finite $\Leftrightarrow K(S,n)$ finite

If $x(K^*)^n \in K(\phi, n)$ then $(x) = \underline{a}^n$ for some ideal $\underline{a}$.
$K(\phi,n) = \{x \in K^*/(K^*)^n \mid v_{\underline{p}}(x) \equiv 0 (n) \ \forall \underline{p}\}$

There is a short exact sequence

$$0 \rightarrow \mathcal{O}_K^*/(\mathcal{O}_K^*)^n \rightarrow K(\phi,n) \xrightarrow{\Phi} Cl_K[n] \rightarrow 0$$

$$x(K^*)^n \mapsto [\underline{a}]$$

3 For exactness: $\ker \Phi = \{x \in K(\phi,n) \mid (x) \sim (y)^n, \text{ some } y \in \mathcal{O}_K\}$

$|Cl_K| < \infty$ for a number field.

$\mathcal{O}_K^*$ is finitely generated (Dirichlet's unit theorem). So $\mathcal{O}_K^* / (\mathcal{O}_K^*)^n$ finite

Hence $K(\phi, n)$ is finite. $\square$

II The Weak Mordell-Weil Theorem

K a number field, E/K an elliptic curve, $n \geq 2$.

Theorem II·1 (Weak Mordell-Weil)

$$\left| \frac{E(K)}{nE(K)} \right| < \infty$$

Lemma II·2

Assume that $E[n] \subset E(K)$. Let $S = \{$primes of bad reduction for $E\}$ $\cup \{\mathfrak{p} \mid n\}$

Let $L = K([n]^{-1}P)$ for some $P \in E(K)$.

Then

i) L/K is an abelian extension of exponent dividing n.

ii) L/K is unramified at all $\mathfrak{p} \notin S$.

Proof

by assumption

Let $Q \in \underset{E(\bar{K})}{E}$ with $nQ = P$. Since $E[n] \subset E(K)$ we have

$K([n]^{-1}P) = L = K(Q)$. Let M/K be the Galois closure of L/K.

If $\sigma \in \mathrm{Gal}(M/K)$ then we have $\sigma(Q) - Q \in E[n] \subset E(K)$

because $[n]$ is defined over K
$nQ = P \Rightarrow n\sigma(Q) = \sigma(P) = P$
$\Rightarrow \sigma(Q) - Q \in E[n]$

$\Rightarrow \sigma(Q) \in E(L)$.

$\Rightarrow \sigma(L) \subset L \quad \forall \sigma \in \mathrm{Gal}(M/K)$. $\quad \therefore L/K$ is Galois.

Define $f : \mathrm{Gal}(L/K) \to E[n]$

$$\sigma \longmapsto \sigma Q - Q$$

We will check that f is an injective group homomorphism.

19/11/13

Elliptic Curves (19)

E/k an elliptic curve, $E[n] \subset E(k)$.

$P \in E(k)$, $Q \in [n]^{-1}P$, $L = k(Q)$.

Define $f : \mathrm{Gal}(L/k) \to E[n]$, $\sigma \mapsto \sigma Q - Q$

f is a group homomorphism:

$$f(\sigma\tau) = \sigma\tau Q - Q = \sigma(\tau Q - Q) + (\sigma Q - Q)$$

$$= \sigma f(\tau) + f(\sigma) = f(\sigma) + f(\tau)$$ since $E[n] \subset E(k)$ so $f(\tau)$ is fixed by σ

f is injective:

$f(\sigma) = 0 \Rightarrow \sigma Q = Q \Rightarrow \sigma = 1$ since $L = k(Q)$

So $\mathrm{Gal}(L/k) \hookrightarrow E[n] \cong (\mathbb{Z}/n\mathbb{Z})^2$

$\therefore$ $\mathrm{Gal}(L/k)$ is abelian and of exponent dividing n.

same result for p-adic fields.

For ii), see Theorem 8·10. Gives what we need □

$$\begin{array}{ccc} L_{\mathfrak{P}} & - & L \\ | & & | \\ k_{\mathfrak{p}} & - & k \end{array}$$

$\mathfrak{P} \mid \mathfrak{p}$, primes of L and k

In fact, if $k[\alpha_1, \dots, \alpha_r] = L$ then $k_{\mathfrak{p}}[\alpha_1, \dots, \alpha_r] = L_{\mathfrak{P}}$

<u>Remark</u>

If $E[n] \subset E(k)$ and L/k is a finite Galois extension, then analogous to the Kummer pairing

c.f. μ_n

$$\frac{E(k) \cap nE(L)}{nE(k)} \hookrightarrow \mathrm{Hom}(\mathrm{Gal}(L/k), E[n])$$

c.f. $\dfrac{k^* \cap (L^*)^n}{(k^*)^n}$

$$P \longmapsto (\sigma \mapsto \sigma Q - Q), \text{ where } nQ = P.$$

c.f. $x \longmapsto \left(\sigma \mapsto \dfrac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}}\right)$

<u>Lemma 11·3</u>

If L/k is a finite Galois extension, then the natural map

$$\alpha : E(k)/nE(k) \to E(L)/nE(L)$$ has finite kernel.

1

Proof

n^{th} roots of $P \in E(K)$ which are in $E(L)$

n^{th} powers of $P \in E[L]$ which are in $E(K)$

There is a injective group homomorphism

$$\frac{E(L) \cap [n]^{-1}E(K)}{E(K)} \xrightarrow{\times n} \frac{E(K) \cap nE(L)}{nE(K)} = \ker \alpha$$

For X a set, A an abelian group, $\mathrm{Map}(X, A) = \{\text{all maps } X \to A\}$ is a group under pointwise operations. There is an injection

$$\frac{E(L) \cap [n]^{-1}E(K)}{E(K)} \hookrightarrow \mathrm{Map}(\mathrm{Gal}(L/K), E[n])$$

$$Q \mapsto (\sigma \mapsto \sigma Q - Q)$$

condition to be in the kernel

Indeed, if $\boxed{\sigma Q = Q \ \ \forall \sigma \in \mathrm{Gal}(L/K)}$ then $Q \in E(K)$.

$\mathrm{Gal}(L/K)$ and $E[n]$ are finite, so $\mathrm{Map}(\mathrm{Gal}(L/K), E[n])$ is finite $\Rightarrow \ker \alpha$ is finite. $\square$

Proof of Theorem 11·1

Lemma 11·3 $\Rightarrow$ we are free to replace K by any finite Galois extension. So WLOG,

i) $\mu_n \subset K$

ii) $E[n] \subset E(K)$ (In fact ii) $\Rightarrow$ i) by properties of the Weil pairing)

Let L be the composite (inside $\bar{K}$) of all the extensions $K([n]^{-1}P)$ for $P \in E(K)$.

These are finite, abelian, exponent dividing n

Lemma 11·2 and Proposition 10·3 $\Rightarrow$ there are only finitely many such extensions $\Rightarrow [L:K] < \infty$.

finitely many such extensions

Then $\frac{E(K)}{nE(K)} \to \frac{E(L)}{nE(L)}$ is the zero map.

all points of $E(K)$ are n^{th} roots of $E(L)$ by definition of L.

Lemma 11·3 $\Rightarrow |E(K)/nE(K)| < \infty$. $\square$

since all of $E(K)/nE(K)$ is the kernel and the kernel is finite.

19/11/13

Elliptic Curves (19)

<u>Remark</u>

If $K = \mathbb{R}$, or $\mathbb{C}$, or $[K : \mathbb{Q}_p] < \infty$, then $\left|\frac{E(K)}{nE(K)}\right| < \infty$, yet $E(K)$ is <u>not</u> finitely generated (in fact, uncountable).

<u>Fact</u>

If K is a number field, then $\exists$ a quadratic form (the <u>canonical height</u>) $\hat{h} : E(K) \to \mathbb{R}_{\geq 0}$ with the property that for any $B \geq 0$, $\{P \in E(K) : \hat{h}(P) \leq B\}$ is finite $\quad (*)$

<u>Theorem 11·4</u> (Mordell-Weil)

For K a number field, E/K an elliptic curve, then $E(K)$ is a finitely generated abelian group.

<u>Proof</u>

Fix an integer $n \geq 2$. Weak Mordell-Weil $\Rightarrow \frac{E(K)}{nE(K)}$ is finite.

Pick coset representatives $P_1, \ldots, P_r$.

Let $\Sigma = \{P \in E(K) \mid \hat{h}(P) \leq \max_{1 \leq i \leq r} \hat{h}(P_i)\}$

Claim: Σ generates $E(K)$. If not, $\exists\, P \in E(K) \setminus \{\text{subgroup generated by } \Sigma\}$ of minimal height (exists by $(*)$). Then $P = P_i + nQ$ ($Q \notin \langle \Sigma \rangle$ or done), for some $Q \in E(K)$ and $1 \leq i \leq r$ since P_i are a set of coset reps.

Minimality of $P \Rightarrow 4\hat{h}(P) \leq 4\hat{h}(Q) \leq n^2 \hat{h}(Q) = \hat{h}(nQ) = \hat{h}(P - P_i)$

$\leq \hat{h}(P - P_i) + \hat{h}(P + P_i) \underset{\text{parallelogram law}}{=} 2\hat{h}(P) + 2\hat{h}(P_i)$

$\Rightarrow \hat{h}(P) \leq \hat{h}(P_i) \quad \Rightarrow P \in \Sigma$ by definition of Σ ※

This proves the claim. By $(*)$, Σ is finite. $\square$

12 Heights

For simplicity, we take $K = \mathbb{Q}$.

Write $P \in \mathbb{P}^n(\mathbb{Q})$ as $P = (a_0 : a_1 : \dots : a_n)$ with $a_0, \dots, a_n \in \mathbb{Z}$

and $\gcd(a_0, \dots, a_n) = 1$. ← i.e. minimal

Definition

$$H(P) = \max_{0 \leq i \leq n} |a_i|$$

Lemma 12·1

Let $f_1, f_2 \in \mathbb{Q}[X_1, X_2]$ be coprime, homogeneous polynomials of degree d. Let $F : \mathbb{P}^1 \to \mathbb{P}^1$, $(x_1 : x_2) \mapsto (f_1(x_1, x_2) : f_2(x_1, x_2))$.

Then $\exists c_1, c_2 > 0$ such that $c_1 H(P)^d \leq H(F(P)) \leq c_2 H(P)^d$ $\forall P \in \mathbb{P}^1(\mathbb{Q})$. → constants independent of P

Proof

WLOG $f_1, f_2 \in \mathbb{Z}[X_1, X_2]$.

Upper bound: Write $P = (a : b)$, $a, b \in \mathbb{Z}$ coprime

$$H(F(P)) \leq \max(|f_1(a,b)|, |f_2(a,b)|)$$

$$\leq c_2 \max(|a|^d, |b|^d)$$ where $c_2 = \max_{i=1,2}(\sum \text{abs. values of coeffs of } f_i)$

$$\therefore H(F(P)) \leq c_2 H(P)^d.$$

Easy direction

21/11/13

$F : \mathbb{P}^1 \to \mathbb{P}^1$, $(x_1 : x_2) \mapsto (f_1(x_1, x_2) : f_2(x_1, x_2))$

Lower bound : We claim that that $\exists g_{ij} \in \mathbb{Z}[X_1, X_2]$ homogeneous of degree $d-1$ and an integer $K > 0$ such that

$\sum_{j=1}^{2} g_{ij} f_j = K X_i^{2d-1}$ for $i = 1, 2$. $(*)$

Indeed, running Euclid's Algorithm on $f_1(X, 1)$ and $f_2(X, 1)$ $(\dagger)$
coprime by hypothesis
gives $r, s \in \mathbb{Q}[X]$ of degree $< d$ such that

$r(X) f_1(X, 1) + s(X) f_2(X, 1) = 1$.

Clearing denominators and homogenising gives $(*)$ for $i = 2$.

$i = 1$ is obtained similarly by swapping variables at $(\dagger)$.

Write $P = (a_1 : a_2)$, $a_1, a_2 \in \mathbb{Z}$, coprime.

$(*) \Rightarrow \sum_{j=1}^{2} g_{ij}(a_1, a_2) f_j(a_1, a_2) = K a_i^{2d-1}$ for $i = 1, 2$.

$\therefore$ $\gcd(f_1(a_1, a_2), f_2(a_1, a_2))$ divides $\gcd(K a_1^{2d-1}, K a_2^{2d-1}) = K$.

But also $|K a_i^{2d-1}| \le \underbrace{\max_{j=1,2} |f_j(a_1, a_2)|}_{\le K H(F(P))} \underbrace{\sum_{j=1}^{2} |g_{ij}(a_1, a_2)|}_{\le r_i H(P)^{d-1}}$ Δ-inequality

$K \in \mathbb{Z}_{>0}$

where $r_i = \sum_{j=1}^{2}$ (sum of absolute values of coefficients of g_{ij}) > 0

$\therefore$ $|a_i|^{2d-1} \le r_i H(P)^{d-1} H(F(P))$ $\quad i = 1, 2$

$\therefore$ $H(P)^{2d-1} \le \max(r_1, r_2) H(P)^{d-1} H(F(P))$

$\Rightarrow \underbrace{\frac{1}{\max(r_1, r_2)}}_{= c} H(P)^d \le H(F(P))$

so ok to divide by

$\square$

<u>Definition</u>

i) The height of $x \in \mathbb{Q}$ is $H(x) = H((x : 1))$

ii) $E/\mathbb{Q}$ an elliptic curve. $y^2 = x^3 + ax + b$.

Height $H : E(\mathbb{Q}) \to \mathbb{R}_{\geq 1}$, $P \mapsto \begin{cases} H(x) & \text{if } P = (x, y) \\ 1 & \text{if } P = 0_E \end{cases}$

Logarithmic height $h : E(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$, $P \mapsto \log H(P)$.

<u>Lemma 12·2</u>

Let $\phi : E \to E'$ be an isogeny of elliptic curves over $\mathbb{Q}$. Then $\exists c > 0$ such that $|h(\phi(P)) - (\deg \phi) h(P)| < c \quad \forall P \in E(\mathbb{Q})$

<u>Note</u>

c depends on E, E', ϕ but not on P.

<u>Proof</u>

Recall Lemma 5·5
$$\begin{array}{ccc} E & \xrightarrow{\phi} & E' \\ {\scriptstyle x}\downarrow & & \downarrow{\scriptstyle x} \\ \mathbb{P}^1 & \xrightarrow{\xi} & \mathbb{P}^1 \end{array} \qquad \deg(\phi) = \deg(\xi)$$

Lemma 12·1 $\xrightarrow{\text{applied to } \xi}$ $\Rightarrow \exists$ constants $c_1, c_2 > 0$ such that

$c_1 H(P)^d \leq H(\phi(P)) \leq c_2 H(P)^d$

$\log c_1 H(P)^d \leq h(\phi(P)) \leq \log c_2 H(P)^d$

Taking logs gives $|h(\phi(P)) - d\, h(P)| \leq \underbrace{\max\left(\log c_2, \log \tfrac{1}{c_1}\right)}_{= c}$ $\square$

<u>Example</u>

$E/\mathbb{Q}$ an elliptic curve. Then $\exists c > 0$ such that

$$|h(2P) - 4h(P)| < c \quad \forall P \in E(\mathbb{Q})$$

<u>Definition</u>

The canonical height is $\hat{h}(P) = \lim_{n \to \infty} \frac{1}{4^n} h(2^n P)$

We check convergence. Let $m \geq n$.

triangle inequality

$$\left|\frac{1}{4^m} h(2^m P) - \frac{1}{4^n} h(2^n P)\right| \leq \sum_{r=n}^{m-1} \left|\frac{1}{4^{r+1}} h(2^{r+1} P) - \frac{1}{4^r} h(2^r P)\right|$$
$$= \sum_{r=n}^{m-1} \frac{1}{4^{r+1}} |h(2^{r+1}P) - 4h(2^r P)| \leq c \sum_{r=n}^{m-1} \frac{1}{4^{r+1}} \leq \frac{c}{4^{n+1}} \frac{1}{1 - \frac{1}{4}}$$
$$= \frac{c}{3 \cdot 4^n} \to 0 \text{ as } n \to \infty$$

So the sequence is Cauchy, and $\hat{h}(P)$ exists.

Lemma 12·3

$|h(P) - \hat{h}(P)|$ is bounded for $P \in E(\mathbb{Q})$.

Proof

Put $n = 0$ in the above calculation.

$\left|\frac{1}{4^m} h(2^m P) - h(P)\right| \leq c/3$

Letting $m \to \infty$ gives the result. □

Lemma 12·4

Let $\phi : E \to E'$ be an isogeny defined over $\mathbb{Q}$.

Then $\hat{h}(\phi(P)) = (\deg \phi)\, \hat{h}(P) \quad \forall P \in E(\mathbb{Q})$.

Proof

Lemma 12·2 $\Rightarrow \exists c > 0$ such that $|h(\phi(P)) - (\deg \phi) h(P)| < c$

Replace P by $2^n P$ and divide by 4^n.

$\left|\frac{1}{4^n} h(2^n \phi(P)) - (\deg \phi) \frac{1}{4^n} h(2^n P)\right| < c/4^n$

Letting $n \to \infty$ gives the result. □

Remark

Lemma 12·4 shows that $\hat{h}$ is independent of choice of Weierstrass equation for E (different equations $\Leftrightarrow$ isogeny of degree 1)

Lemma 12·5

$\#\{P \in E(\mathbb{Q}) : \hat{h}(P) \leq B\} < \infty$ → Key ingredient of Mordell-Weil

Proof

$\hat{h}$ bounded $\underset{\text{Lemma 12·3}}{\Rightarrow}$ h bounded $\Rightarrow$ only finitely many choices for x

$h = \log H$, $H(P) = \max_{P = (a_1 : a_2) \in \mathbb{Z}^2,\ \gcd(a_1, a_2) = 1} (|a_i|)$

y satisfies a quadratic in x

Given x, there are ≤ 2 choices for y. $\square$

Lemma 12·4 $\Rightarrow \hat{h}(nP) = n^2 \hat{h}(P) \quad \forall\, n \in \mathbb{Z}$.

$\hat{h}(\phi(P)) = (\deg \phi)\, \hat{h}(P)$

<u>Lemma 12·6</u>

$E/\mathbb{Q}$ an elliptic curve. $\exists\, C > 0$ such that

$$H(P+Q)\,H(P-Q) \leq C\, H(P)^2 H(Q)^2$$

for all $P, Q \in E(\mathbb{Q})$ with $P, Q, P+Q, P-Q \neq O_E$.

<u>Proof</u>

$P = (\xi_1, \eta_1)$, $Q = (\xi_2, \eta_2)$, $P+Q = (\xi_3, \eta_3)$, $P-Q = (\xi_4, \eta_4)$

$\xi_i = r_i/s_i$, $r_i, s_i \in \mathbb{Z}$, coprime.

(See proof of Lemma 5·7)

$y^2 = x^3 + ax + b$

$\exists$ formulae for $\xi_3 + \xi_4$, $\xi_3 \xi_4$ in terms of ξ_1, ξ_2, a, b.

$$(\underbrace{s_3 s_4 : r_3 s_4 + r_4 s_3 : r_3 r_4}_{\text{coprime}}) = (\underset{(r_1 s_2 - r_2 s_1)^2}{\overset{\shortparallel}{W_0}} : W_1 : W_2)$$

W_0, W_1, W_2 each have degree 2 in r_1, s_1, and degree 2 in r_2, s_2.

$$\begin{aligned} H(P+Q)\,H(P-Q) &= \max(|r_3|, |s_3|)\max(|r_4|, |s_4|) \\ &\leq 2\max(|s_3 s_4|, \underbrace{|r_3 s_4 + r_4 s_3|}, |r_3 r_4|) \\ &\leq 2\max(|W_0|, |W_1|, |W_2|) \\ &\leq \text{constant} \times H(P)^2 H(Q)^2 \end{aligned}$$

$\square$

works because of the factor of 2

23/11/13 # Elliptic Curves 21

Theorem 12·7

$\hat{h} : E(\mathbb{Q}) \to \mathbb{R}_{\geq 0}$ is a quadratic form.

Proof

take logs then take limits

Lemma 12·6 and $|h(2P) - 4h(P)|$ bounded

$\Rightarrow h(P+Q) + h(P-Q) \leq 2h(P) + 2h(Q) + c$

$\forall P, Q \in E(\mathbb{Q})$.

Replacing P, Q by $2^n P$, $2^n Q$ and dividing by 4^n, we let $n \to \infty$ and obtain $\hat{h}(P+Q) + \hat{h}(P-Q) \leq 2\hat{h}(P) + 2\hat{h}(Q)$

Replace P, Q by $P+Q$, $P-Q$ and use $\hat{h}(2P) = 4\hat{h}(P)$ to get the reverse inequality.

$\therefore \hat{h}$ satisfies the Parallelogram law, so it is a quadratic form. $\square$

13 Dual Isogenies and the Weil Pairing

Let K be a perfect field (e.g. $\mathrm{char}(K) = 0$ or $K = \mathbb{F}_q$)

Let E/K be an elliptic curve.

Proposition 13·1

Let $\Phi \subset E(\bar{K})$ be a finite Galois $(\bar{K}/K)$-stable subgroup.
Then $\exists$ an elliptic curve E'/K and a separable isogeny $\phi : E \to E'$ defined over K, with kernel Φ, such that every isogeny $\psi : E \to E''$ with $\Phi \subset \ker \psi$ factors uniquely via ϕ.

$$\begin{tikzcd} E \arrow[rr, "\psi"] \arrow[dr, "\phi"'] & & E'' \\ & E' \arrow[ur, dotted, "\exists!\text{ map}"'] & \end{tikzcd}$$

Proof

Omitted. The basic idea is to set $E' = E/\Phi$, which has function field $k(E)^{\Phi}$ (where $P \in \Phi$ acts as $\tau_P^* : k(E) \to k(E)$) — fixed field under Φ $\square$

<u>Proposition 13·2</u>

Let $\phi : E \to E'$ be an isogeny of degree n. Then $\exists !$ isogeny $\hat{\phi} : E' \to E$ such that $\hat{\phi}\phi = [n]$. $\hat{\phi}$ is called the dual isogeny.

<u>Proof</u>

In the case where ϕ is separable $\# E[\phi] = \deg \phi = n$

So $E[\phi] \subseteq E[n]$. Apply Proposition 13·1 with $\psi = [n]$.

$$\begin{tikzcd} E \arrow[rr, "{[n]}"] \arrow[dr, "\phi"'] & & E \\ & E' \arrow[ur] & \end{tikzcd}$$

The case where ϕ is inseparable is omitted.

For uniqueness, $\psi_1 \phi = \psi_2 \phi \Rightarrow (\psi_1 - \psi_2)\phi = 0$

$\Rightarrow \psi_1 = \psi_2$ by taking degrees. $\square$

<u>Remarks</u>

i) $\deg [n] = n^2 \Rightarrow \deg \phi = \deg \hat{\phi}$, and $\widehat{[n]} = [n]$

ii) $\phi \hat{\phi} \phi = \phi [n]_E = [n]_{E'} \phi \Rightarrow \phi \hat{\phi} = [n]_{E'}$

integer maps commute with isogenies

In particular, $\hat{\hat{\phi}} = \phi$.

iii) If $\phi, \psi \in \mathrm{Hom}(E_1, E_2)$ it can be shown that $\widehat{\phi + \psi} = \hat{\phi} + \hat{\psi}$. Proving this gives another way of showing that $\deg : \mathrm{Hom}(E_1, E_2) \to \mathbb{Z}$ is a quadratic form.

<u>Definition</u>

$\mathrm{sum} : \mathrm{Div}(E) \to E$

(a formal sum) $\sum n_P P \mapsto \sum n_P P$ (add up using group law)

Recall that $E \xrightarrow{\cong} \mathrm{Pic}^0(E)$

$$P \longmapsto [(P) - (0)]$$

If $D \in \mathrm{Div}^0(E)$, $\mathrm{sum}(D) \to [D]$

23/11/13

Elliptic Curves (21)

<u>Lemma 13.3</u>

If $D \in \mathrm{Div}^0(E)$, $D \sim 0 \iff \mathrm{sum}\, D = 0$

Let $\phi : E \to E'$ be an isogeny of degree n with dual isogeny $\hat{\phi} : E' \to E$. Assume that $\mathrm{char}(K) \nmid n$. We define the Weil pairing $e_\phi : E[\phi] \times E'[\hat{\phi}] \to \mu_n$

Let $T \in E'[\hat{\phi}]$. Then $nT = 0$.

by Lemma 13.3 since $\mathrm{sum}(nT - 0) = 0$

So $\exists f \in \bar{K}(E')$ such that $\mathrm{div}(f) = n(T) - n(0)$.

Pick $T_0 \in E(\bar{K})$ with $\phi(T_0) = T$. Then $\phi^*(T) - \phi^*(0) = \sum_{P \in E[\phi]} (P + T_0) - \sum_{P \in E[\phi]} (P)$ has sum $nT_0 = \hat{\phi}(\phi T_0) = \hat{\phi} T = 0$

So $\exists g \in \bar{K}(E)$ such that $\mathrm{div}(g) = \phi^*(T) - \phi^*(0)$

Then $\mathrm{div}(\phi^* f) = \phi^*(\mathrm{div} f) = n(\phi^*(T) - \phi^*(0))$

$= n \,\mathrm{div}\, g = \mathrm{div}(g^n)$

$\Rightarrow \phi^* f = c g^n$, for some $c \in \bar{K}^*$.

Rescaling $f \Rightarrow$ WLOG $c = 1$, $\therefore \quad \phi^* f = g^n$

If $S \in E[\phi]$ then $\tau_S^*(\mathrm{div}\, g) = \mathrm{div}\, g$

$\Rightarrow \mathrm{div}(\tau_S^* g) = \mathrm{div}(g) \Rightarrow \tau_S^* g = \zeta g$ for some $\zeta \in \bar{K}$

i.e. $\zeta = \dfrac{g(X+S)}{g(X)}$ independent of choice of $X \in E(\bar{K})$.

$\zeta^n = \dfrac{g(X+S)^n}{g(X)^n} = \dfrac{f(\phi(X+S))}{f(\phi(X))} = 1$ since $S \in E[\phi]$.

$\therefore \zeta \in \mu_n$. We define $e_\phi(S, T) = \dfrac{g(X+S)}{g(X)} = \zeta$

<u>Proposition 13.4</u>

e_ϕ is bilinear and non-degenerate.

<u>Proof</u>

i) Linear in first argument

3

$$e_\phi(S_1+S_2, T) = \frac{g(x+S_1+S_2)}{g(x)} = \frac{g(x+S_1+S_2)}{g(x+S_2)} \frac{g(x+S_2)}{g(x)}$$
$$= e_\phi(S_1, T)\, e_\phi(S_2, T)$$

---

ii) Linear in second argument:

$T_1, T_2 \in E'[\hat{\phi}]$

$f_1 \in \bar{K}(E')$, $\operatorname{div}(f_1) = n(T_1) - n(0)$

$f_2 \in \bar{K}(E')$, $\operatorname{div}(f_2) = n(T_2) - n(0)$

$\phi^* f_1 = g_1^n$, $\phi^* f_2 = g_2^n$

$\exists h \in \bar{K}(E')$ such that $\operatorname{div}(h) = (T_1) + (T_2) - (T_1 + T_2) - (0)$

Put $f = \frac{f_1 f_2}{h^n}$, $g = \frac{g_1 g_2}{\phi^* h}$

Check: $\operatorname{div}(f) = n(T_1 + T_2) - n(0)$

$$\phi^* f = \frac{\phi^* f_1\, \phi^* f_2}{(\phi^* h)^n} = \left(\frac{g_1 g_2}{\phi^* h}\right)^n = g^n$$

$$e_\phi(S, T_1 + T_2) = \frac{g(x+S)}{g(x)}$$
$$= \frac{g_1(x+S)}{g_1(x)} \frac{g_2(x+S)}{g_2(x)} \cancel{\frac{h(\phi(x))}{h(\phi(x+S))}}$$ — since $S \in E[\phi]$

$$= e_\phi(S, T_1)\, e_\phi(S, T_2)$$

$\phi : E \to E'$ an isogeny of degree n. $\mathrm{char}(k) \nmid n$.

$e_\phi : E[\phi] \times E[\hat{\phi}] \to \mu_n$, $(S, T) \mapsto \frac{\tau_S^* g}{g}$

where $\mathrm{div}(f) = n(T) - n(0)$

$\mathrm{div}(g) = \phi^*(T) - \phi^*(0)$ $\qquad \phi^* f = g^n$

iii) We show that e_ϕ is non-degenerate. Let $T \in E'[\hat{\phi}]$.

Suppose that $e_\phi(S, T) = 1 \quad \forall S \in E[\phi]$.

$\Rightarrow \tau_S^* g = g \qquad \forall S \in E[\phi]$ — finite because $\deg \phi = n$, Galois because $E[\phi]$ maps to all conjugates and has correct size

$\bar{K}(E)$

$\phi^* \bar{K}(E')$ — This is a Galois extension with Galois group $E[\phi]$.

$\therefore g = \phi^* h$ for some $h \in \bar{K}(E')$.

$\Rightarrow \phi^* f = g^n = \phi^*(h^n) \qquad \Rightarrow f = h^n$

$\Rightarrow \mathrm{div}(h) = (T) - (0) \Rightarrow T = 0$ (for principal divisors, sum is 0)

We have shown that $E'[\hat{\phi}] \hookrightarrow \mathrm{Hom}(E[\phi], \mu_n)$.

This is also an isomorphism since $n = \deg \phi = \deg \hat{\phi}$. $\square$

<u>Remark</u>

If E, E', ϕ are defined over K, then e_ϕ is <u>Galois Equivariant</u>

i.e. $e_\phi(\sigma S, \sigma T) = \sigma(e_\phi(S, T))$

$\forall \sigma \in \mathrm{Gal}(\bar{K}/K)$, $S \in E[\phi]$, $T \in E[\hat{\phi}]$.

Taking $\phi = [n] : E \to E$ (so that $\hat{\phi} = [n]$) gives

$e_n : E[n] \times E[n] \to \mu_n$.

<u>Corollary 13.5</u>

If $E[n] \subset E(K)$ then $\mu_n \subset K$.

Proof

e_n is non-degenerate $\Rightarrow \exists S, T \in E[n]$ such that

$e_n(S,T) = \zeta_n$ is a primitive n^{th} root of unity.

Then $\sigma(\zeta_n) = \sigma(e_n(S,T)) = e_n(\sigma S, \sigma T)$

$= e_n(S,T) = \zeta_n \quad \forall \sigma \in Gal(\bar{K}/K)$

$\Rightarrow \zeta_n \in K. \quad \Rightarrow \mu_n \subset K$ $\square$.

Example

$\nexists$ an elliptic curve $E/\mathbb{Q}$ with $E(\mathbb{Q})_{tors} \cong (\mathbb{Z}/3\mathbb{Z})^2$

since in this case, $E(\mathbb{Q})_{tors} = E(\mathbb{Q})[3]$
$\Rightarrow \mu_3 \subset \mathbb{Q}$ ※

Remark

In fact $e_n : E[n] \times E[n] \to \mu_n$ is alternating

i.e. $e_n(T,T) = 1 \quad \forall T \in E[n]$

$(\Rightarrow e(S,T) = e_n(T,S)^{-1})$

14 Galois Cohomology

Let G be a group, A a G-module (c.f. $\mathbb{Z}[G]$-module)

i.e. an abelian group with an action of G

Definition

$H^0(G,A) = A^G = \{a \in A \mid \sigma(a) = a \ \forall \sigma \in G\}$

$C^1(G,A) = \{\text{maps } G \to A\}$ "cochains" $\to$ a map $G \to A$ with $\sigma \mapsto a_\sigma$

$\cup$

$Z^1(G,A) = \{(a_\sigma)_{\sigma \in G} \mid a_{\sigma\tau} = \sigma(a_\tau) + a_\sigma, \ \forall \sigma, \tau \in G\}$ "co-cycles"

$\cup$

$B^1(G,A) = \{(\sigma(b) - b)_{\sigma \in G} : b \in A\}$ "co-boundaries"

this containment is easy to see

Definition

$$H^1(G,A) = \frac{Z^1(G,A)}{B^1(G,A)}$$

Remark

If G acts trivially on A then $H^1(G,A) = Hom(G,A)$.

26/11/13 Elliptic Curves (22)

Theorem 14.1

A short exact sequence of G-modules $0 \to A \xrightarrow{f} B \xrightarrow{g} C \to 0$ gives rise to a long exact sequence of Abelian groups:

$$0 \to A^G \xrightarrow{f} B^G \xrightarrow{g} C^G \xrightarrow{\delta} H^1(G,A) \xrightarrow{f_*} H^1(G,B) \xrightarrow{g_*} H^1(G,C)$$

Proof

Omitted, but we discuss the definition of $\delta : C \to H^1(G,A)$.

$\exists\, b \in B$ such that $g(b) = c$. Then $g(\underbrace{\sigma(b) - b) = \sigma(c) - c}) = 0$

as we are working in B^G, C^G and $\sigma \in G$

$\Rightarrow \sigma(b) - b = f(a_\sigma)$, some $a_\sigma \in A$.

We can check that $(a_\sigma)_{\sigma \in G} \in Z^1(G,A)$.

$\delta(c) =$ class of $(a_\sigma)_{\sigma \in G}$ in $H^1(G,A)$. $\square$

Theorem 14.2

Let A be a G-module and $H \triangleleft G$ a normal subgroup. There is an inflation - restriction exact sequence.

$$0 \to H^1(G/H, A^H) \xrightarrow{\text{inflation}} H^1(G,A) \xrightarrow{\text{restriction}} H^1(H,A)$$

Proof

Omitted. $\square$

Let K be a perfect field. $\mathrm{Gal}(\bar{K}/K)$ is a topological group with basis of open subgroups the $\mathrm{Gal}(\bar{K}/L)$ for $[L:K] < \infty$.

If $G = \mathrm{Gal}(\bar{K}/K)$ we modify the definition of $H^1(G,A)$ by insisting

i) The stabiliser of each $a \in A$ is an open subgroup of G.

ii) All cochains $G \to A$ are continuous, where A is given the discrete topology.

Then $H^1(\mathrm{Gal}(\bar{K}/K), A) = \varinjlim_{L} H^1(\mathrm{Gal}(L/K), A^{\mathrm{Gal}(\bar{K}/L)})$

L/K a finite Galois extension, and the direct limit is with respect to inflation maps.

Hilbert's Theorem 90

Let L/K be a finite Galois extension. Then $H^1(\mathrm{Gal}(L/K), L^*) = 0$.

Proof — note change from additive to multiplicative notation

Let $\{a_\sigma\} \in Z^1(G, L^*)$, $G = \mathrm{Gal}(L/K)$.

Distinct automorphisms are linearly independent.

$\Rightarrow \exists\, y \in L$ such that $\sum_{\tau \in G} a_\tau^{-1}\tau(y) = x \neq 0$

c.f. Theorem 10.2 Kummer Theory

Then $\sigma(x) = \sum_{\tau \in G} \sigma(a_\tau)^{-1}\sigma\tau(y)$

$= a_\sigma \sum_{\tau \in G} a_{\sigma\tau}^{-1}\sigma\tau(y)$ since $a_{\sigma\tau} = \sigma(a_\tau)a_\sigma$

$\Rightarrow \sigma(x) = a_\sigma \sum_{\tau \in G} a_\tau^{-1}\tau(y)$.

$\Rightarrow a_\sigma = \frac{\sigma(x)}{x} \quad \Rightarrow (a_\sigma)_{\sigma \in G} \in B^1(G, L^*)$

$\therefore H^1(G, L^*) = 0$ $\square$

Corollary

$H^1(\mathrm{Gal}(\bar{K}/K), \bar{K}^*) = 0$. $\quad \varinjlim_{L} H^1(\mathrm{Gal}(L/K), \bar{K}^*) = \varinjlim_{L} 0 = 0$

Application

Assume that $\mathrm{char}(K) \nmid n$. There is an exact sequence of $\mathrm{Gal}(\bar{K}/K)$-modules

$0 \to \mu_n \to \bar{K}^* \to \bar{K}^* \to 0$ — exact clear

$x \mapsto x^n$

We get a long exact sequence. by 14.1

$K^* \to K^* \to H^1(\mathrm{Gal}(\bar{K}/K), \mu_n) \to \underbrace{H^1(\mathrm{Gal}(\bar{K}/K), \bar{K}^*)}^{=0}$

$x \mapsto x^n$

$\Rightarrow H^1(\mathrm{Gal}(\bar{K}/K), \mu_n) \cong K^*/(K^*)^n$

By properties of the exact sequence

28/11/13

Elliptic Curves (23)

$H^1(\mathrm{Gal}(\bar{K}/K), \mu_n) \cong K^*/(K^*)^n$

If $\mu_n \subset K$, this becomes $\mathrm{Hom}_{cts}(\mathrm{Gal}(\bar{K}/K), \mu_n) \cong K^*/(K^*)^n$
continuous

This has finite subgroups of the form $\mathrm{Hom}(\mathrm{Gal}(L/K), \mu_n)$

for L/K a finite abelian extension of exponent dividing n.

Compare this with Proposition 10·2.

<u>Notation</u>

We write $H^1(K, -)$ for $H^1(\mathrm{Gal}(\bar{K}/K), -)$.

Let $\phi : E \to E'$ be an isogeny of elliptic curves over K.

We start with a short exact sequence of $\mathrm{Gal}(\bar{K}/K)$ modules.

$$0 \to E[\phi] \to E \xrightarrow{\phi} E' \to 0$$

Taking a long exact sequence by 14·1

$$\dots \to E(K) \xrightarrow{\phi} E'(K) \xrightarrow{\delta} H^1(K, E[\phi]) \to H^1(K, E) \xrightarrow{\phi_*} H^1(K, E) \to \dots$$

$$0 \to \frac{E'(K)}{\phi E(K)} \xrightarrow{\delta} H^1(K, E[\phi]) \to H^1(K, E)[\phi_*] \to 0$$

Now take K a number field.

$M_K = \{\text{places of } K\} = \{\text{finite places}\} \cup \{\text{infinite places}\}$

prime ideals in $\mathcal{O}_K$.

real, respectively complex conjugate pairs of embeddings $K \hookrightarrow \mathbb{C}$.

For $v \in M_K$, $K \subset K_v$, completion w.r.t. v-adic topology.

$$\begin{tikzcd}
0 \arrow[r] & \frac{E'(K)}{\phi E(K)} \arrow[r, "\delta"] \arrow[d] & H^1(K, E[\phi]) \arrow[r] \arrow[d, "\mathrm{res}_v"] & H^1(K, E)[\phi_*] \arrow[r] \arrow[d, "\mathrm{res}_v"] & 0 \\
0 \arrow[r] & \frac{E'(K_v)}{\phi E(K_v)} \arrow[r, "\delta_v"] & H^1(K_v, E[\phi]) \arrow[r] & H^1(K_v, E)[\phi_*] \arrow[r] & 0
\end{tikzcd}$$

We fix an embedding $\bar{K} \subset \bar{K}_v$. Then, by restriction,

$\mathrm{Gal}(\bar{K}_v/K_v) \subset \mathrm{Gal}(\bar{K}/K)$ (so now δ_v and cocycle definitions make sense)

Definition

i) The ϕ-Selmer group is

$$S^{(\phi)}(E/k) = \ker\left(H^1(k, E[\phi]) \longrightarrow \prod_{v \in M_k} H^1(k_v, E)\right)$$
$$= \{ \alpha \in H^1(k, E[\phi]) \mid \mathrm{res}_v(\alpha) \in \mathrm{Im}(\delta_v) \ \forall v \in M_k \}$$

ii) The Tate-Shafarevich group is

$$Ш(E/k) = \ker\left(H^1(k, E) \to \prod_{v \in M_k} H^1(k_v, E)\right)$$

We get

$$0 \longrightarrow \frac{E'(k)}{\phi E(k)} \to \underbrace{S^{(\phi)}(E/k)}_{\text{finite and effectively computable.}} \longrightarrow Ш(E/k)[\phi_*] \to 0$$

Conjecture

$Ш(E/k)$ is finite.

N.B. This would give an effective Algorithm for computing the rank $E(k)$.

If $\phi = [n] : E \to E$, then

$$0 \to \frac{E(k)}{nE(k)} \to S^{(n)}(E/k) \longrightarrow Ш(E/k)[n] \to 0$$

The proof of Weak Mordell-Weil can be rephrased as a proof that $S^{(n)}(E/k)$ is finite.

By the inflation - restriction exact sequence, we are free to extend our number field, so WLOG $\mu_n \subset k$, $E[n] \subset E(k)$

$E[n] \cong \mu_n \times \mu_n$ as $Gal(\bar{k}/k)$ modules.

$$H^1(k, E[n]) \cong \underset{\substack{\text{\rotatebox{90}{$\cong$}} \\ k^*/(k^*)^n}}{H^1(k, \mu_n)} \times \underset{\substack{\text{\rotatebox{90}{$\cong$}} \\ k^*/(k^*)^n}}{H^1(k, \mu_n)}$$

28/11/13

One shows that $S^{(n)}(E/K) \subset K(S,n) \times K(S,n)$

where $S = \{\text{primes of bad reduction for } E\} \cup \{\mathfrak{p} \mid n\}$

15 Descent by Cyclic Isogeny

E, E' elliptic curves / a number field K.

$\phi : E \to E'$ an isogeny defined over K.

Suppose $E'[\hat\phi] \cong \mathbb{Z}/n\mathbb{Z}$ generated by $T \in E'(K)$.

Then $E[\phi] \cong \mu_n$ as $\mathrm{Gal}(\bar K/K)$-modules.

maps $G \to A$ $\cup$ co-cycles

$S \mapsto e_\phi(S,T)$.

$H^1(G,A) = \dfrac{Z^1(G,A)}{B^1(G,A)} = \dfrac{\{(a_\sigma)_{\sigma\in G} \mid a_{\sigma\tau} = \sigma(a_\tau) + a_\sigma\}}{\{(\sigma(b)-b)_{\sigma\in G} \mid b \in A\}}$ co-boundaries

We have a short exact sequence of $\mathrm{Gal}(\bar K/K)$ modules

$0 \to \mu_n \to E \xrightarrow{\phi} E' \to 0.$ 14.1

$E(K) \to E'(K) \xrightarrow{\delta} H^1(K, \mu_n) \to H^1(K, E) \to \dots$

definition of δ as in 14.1

$\xrightarrow{\alpha}$ $\cong$ $K^*/(K^*)^n$ From Hilbert 90 application

α defined here ?

Proposition 15.1

Let f be a rational function on E', g a rational function on $K(E)$, with $\mathrm{div}(f) = n(T) - n(O)$, and

$\phi^* f = g^n$. Then $\alpha(P) = f(P) \bmod (K^*)^n$

for all $P \in E'(K) \setminus \{O, T\}$

Proof

Pick $Q \in E(\bar K)$ with $\phi(Q) = P$.

Then $\delta(P)$ is the class of the cocycle $\sigma \mapsto \sigma Q - Q \in E[\phi] \cong \mu_n$

$e_\phi(\sigma Q - Q, T) = \dfrac{g(\sigma Q - Q + X)}{g(X)}$ for any $X \in E(\bar K)$ avoiding zeroes, poles of g.

$e_\phi : (S,T) \mapsto \dfrac{\tau_S^* g}{g}$

$= \dfrac{g(\sigma Q)}{g(Q)}$ (take $X = Q$)

$= \dfrac{\sigma(g(Q))}{g(Q)} \in \mu_n$ since g is defined over K

as $E[\phi] \cong \mu_n$, $S \mapsto e_\phi(S,T)$ — suitable T

$$= \frac{\sigma(\sqrt[n]{f(P)})}{\sqrt[n]{f(P)}} \quad \text{since } f(P) = (\phi^* f)(Q) = g(Q)^n$$

But $H^1(K, \mu_n) \cong K^*/(K^*)^n$

$$\left(\frac{\sigma(\sqrt[n]{x})}{\sqrt[n]{x}}\right)_\sigma \longleftarrow\!\!\shortmid \; x$$

$\therefore \; \alpha(P) \equiv f(P) \mod (K^*)^n$ $\square$

$E: \; y^2 = x(x^2 + ax + b)$

$E': \; y^2 = x(x^2 + a'x + b')$ $\quad a' = -2a, \; b' = a^2 - 4b$

$$\phi : E \to E' \; ; \quad (x, y) \mapsto \left(\left(\frac{y}{x}\right)^2, \; \frac{y(x^2 - b)}{x^2}\right)$$

30/11/13 Elliptic Curves 24

Descent by 2-Isogeny

$E: \ y^2 = x(x^2+ax+b)$ $\qquad a' = -2a$, $b' = a^2-4b$

$E': \ y^2 = x(x^2+a'x+b')$

$\phi: E \to E', \quad (x,y) \mapsto \left(\left(\frac{y}{x}\right)^2, \frac{y}{x^2}(x^2-b) \right)$

$\hat{\phi}: E' \to E, \quad (x,y) \mapsto \left(\frac{y^2}{4x^2}, \frac{y}{8x^2}(x^2-b) \right)$

$E[\phi] = \{0, T\}, \quad T = (0,0) \in E(k)$

$E'[\hat{\phi}] = \{0, T'\}, \quad T' = (0,0) \in E'(k)$

Proposition 15·2

There is a group homomorphism

$$\alpha: E'(k) \longrightarrow k^*/(k^*)^2$$

$$(x,y) \longmapsto \begin{cases} x \bmod (k^*)^2 & \text{if } x \neq 0 \\ b' \bmod (k^*)^2 & \text{if } x = 0 \end{cases}$$

with kernel $\phi E(k)$.

Proof $\phi(x,y) = \left(\left(\frac{y}{x}\right)^2, \frac{y(x^2-b)}{x^2} \right)$ correct kernel by exactness of sequence

Either apply Proposition 15·1) with $f = x \in k(E')$ and

$g = y/x \in k(E)$. (or direct calculation). → c.f. example sheet $\square$

$$\alpha_E: \frac{E(k)}{\hat{\phi}E'(k)} \hookrightarrow k^*/(k^*)^2$$

$$\alpha_{E'}: \frac{E'(k)}{\phi E(k)} \hookrightarrow k^*/(k^*)^2$$

Lemma 15·3

$$2^{\operatorname{rank} E(k)} = \frac{1}{4} |\operatorname{Im}(\alpha_E)| |\operatorname{Im}(\alpha_{E'})|$$

Proof

Since $\hat{\phi}\phi = [2]_E$, there is an exact sequence

$$0 \to E(k)[\phi] \to E(k)[2] \xrightarrow{\phi} E'(k)[\hat{\phi}] \to \frac{E'(k)}{\phi E(k)} \xrightarrow{\hat{\phi}} \frac{E(k)}{2E(k)} \to \frac{E(k)}{\hat{\phi}E'(k)} \to 0$$

← projection to $\frac{E'(k)[\hat{\phi}]}{\phi E(k)}$ and inclusion into $\frac{E'(k)}{\phi E(k)}$

$\operatorname{Im}(\alpha_{E'}) \cong \frac{E'(k)}{\phi E(k)}$ $\qquad$ $\frac{E(k)}{\hat{\phi}E'(k)} \cong \operatorname{Im}(\alpha_E)$

$$\therefore \quad \frac{|E(k)/2E(k)|}{|E(k)[2]|} = \frac{1}{4} |\mathrm{Im}(\alpha_E)||\mathrm{Im}(\alpha_{E'})|$$

Mordell-Weil $\Rightarrow E(k) \cong \Delta \times \mathbb{Z}^r$ for some finite group Δ.

$\frac{E(k)}{2E(k)} \cong \frac{\Delta}{2\Delta} \times \left(\frac{\mathbb{Z}}{2\mathbb{Z}}\right)^r$

$E(k)[2] \cong \Delta[2]$ same order since Δ is finite.

$$\therefore \quad \frac{|E(k)/2E(k)|}{|E(k)[2]|} = 2^r \qquad \square$$

<u>Lemma 15.4</u>

If K is a number field, and $a, b \in \mathcal{O}_K$ then $\mathrm{Im}(\alpha_E) \subset K(S,2)$ where $S = \{\text{primes dividing } b\}$

$K(S,2) = \{x \in \frac{K^*}{(K^*)^2} \mid v_{\mathfrak{p}}(x) \equiv 0\ (2)\ \forall \mathfrak{p} \notin S\}$

<u>Proof</u>

We must show that if $(x,y) \in E(K)$ and $v_{\mathfrak{p}}(b) = 0$ then $v_{\mathfrak{p}}(x) \equiv 0\ (2)$.

In the case where $v_{\mathfrak{p}}(x) < 0$:

Lemma 8.2 $\Rightarrow v_{\mathfrak{p}}(x) = -2r$, $v_{\mathfrak{p}}(y) = -3r$, some $r \geq 1$.
so $v_{\mathfrak{p}}(x) \equiv 0\ (2)$

In the case where $v_{\mathfrak{p}}(x) > 0$:

since $v_{\mathfrak{p}}(b) = 0$

Then $v_{\mathfrak{p}}(x^2 + ax + b) = 0 \Rightarrow v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}(x(x^2+ax+b))$

$\Rightarrow v_{\mathfrak{p}}(x) = v_{\mathfrak{p}}(y^2) = 2v_{\mathfrak{p}}(y) \equiv 0\ (2) \qquad \square$

<u>Lemma 15.5</u>

If $b_1 b_2 = b$ then

$b_1 (K^*)^2 \in \mathrm{Im}(\alpha_E) \iff w^2 = b_1 u^4 + a u^2 v^2 + b_2 v^4 \quad (*)$
is soluble for $u, v, w \in K$ not all zero

<u>Proof</u>

If $b_1 \in (K^*)^2$ (u=1, v=0) or $b_2 \in (K^*)^2$ (u=0, v=1) then both conditions are satisfied.

N.B. $\alpha_E((0,0)) = b \bmod (K^*)^2$ $(\dagger)$

Then, we may assume that $b_1, b_2 \notin (K^*)^2$.

$b_1 (K^*)^2 \in \mathrm{Im}(\alpha_E) \iff \exists (x,y) \in E(K)$ such that $x = b_1 t^2$ for some $t \in K^*$

$\Rightarrow y = b_1 t^2 ((b_1 t^2)^2 + a(b_1 t^2) + b)$

$\Rightarrow \left(\frac{y}{b_1 t}\right)^2 = b_1 t^4 + a t^2 + b_2$

Then $(*)$ has solution $u = t$, $v = 1$, $w = \frac{y}{b_1 t}$.

Conversely, if (u, v, w) is a solution of $(*)$ then $uv \neq 0$ (since we assume b_1, b_2 not square, see $(\dagger)$).

$\left(b_1 \left(\frac{u}{v}\right)^2, b_1 \frac{uw}{v^3}\right) \in E(K)$. $\square$

Now we take $K = \mathbb{Q}$.

<u>Examples</u>

1. $E : y^2 = x^3 - x$, $a = 0$, $b = -1$

$\mathrm{Im}(\alpha_E) = \langle -1 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$E' : y^2 = x^3 + 4x$, $a' = 0$, $b' = 4$

$\mathrm{Im}(\alpha_{E'}) \subset \langle -1, 2 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$b_1 = -1$ $w^2 = -u^4 - 4v^4$ insoluble over $\mathbb{R}$

$b_1 = 2$ $w^2 = 2u^4 + 2v^4$ solution $(u,v,w) = (1,1,2)$

$b_1 = -2$ $w^2 = -2u^4 - 2v^4$ insoluble over $\mathbb{R}$

$\therefore \mathrm{Im}(\alpha_{E'}) = \langle 2 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

Lemma 15.3 $\Rightarrow$ rank $E(\mathbb{Q}) = 0 \Rightarrow 1$ not a congruent number.

2. $E : y^2 = x^3 + px$, p prime, $p \equiv 5 \ (8)$.

$b_1 = -1$, $w^2 = -u^4 - pv^4$ insoluble over $\mathbb{R}$

$\therefore \mathrm{Im}(\alpha_E) = \langle p \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$E' : y^2 = x^3 - 4px$

$\mathrm{Im}(\alpha_{E'}) \subset \langle -1, 2, p \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

N.B. $\alpha_{E'}((0,0)) = (-p)(\mathbb{Q}^*)^2$

$b_1 = 2 \qquad w^2 = 2u^4 - 2pv^4 \qquad ①$

$b_1 = -2 \qquad w^2 = -2u^4 + 2pv^4 \qquad ②$

$b_1 = p \qquad w^2 = pu^4 - 4v^4 \qquad ③$

① Suppose this has a solution. WLOG, $u, v, w \in \mathbb{Z}$ and $\gcd(u,v) = 1$.

If $p \mid u$ then $p \mid w$, so $p \mid v$ ※

$\therefore w^2 \equiv 2u^4 \not\equiv 0 \ (p) \Rightarrow \left(\frac{2}{p}\right) = +1$ ※ since $p \equiv 5 \ (8)$

② is also insoluble, since this gives $\left(\frac{-2}{p}\right) = +1$ by the same method but $p \equiv 5 \ (8) \Rightarrow \left(\frac{-2}{p}\right) = -1$.

$\therefore \mathrm{Im}(\alpha_{E'}) \subset \langle -1, p \rangle$

$\therefore \operatorname{rank} E(\mathbb{Q}) = \begin{cases} 0 & \text{③ soluble over } \mathbb{Q} \\ 1 & \text{③ not soluble over } \mathbb{Q}. \end{cases}$

03/11/13

Elliptic Curves (25)

Tuesday 21st January 2-15 MR15

$E : y^2 = x(x^2+ax+b)$

$\phi : E \to E'$ a 2-isogeny $\qquad w^2 = b_1u^4 + au^2v^2 + b_2v^4$ (*) $\qquad b_2 = b/b_1$

$$0 \to \frac{E'(\mathbb{Q})}{\phi E(\mathbb{Q})} \to S^{(\phi)}(E/\mathbb{Q}) \to Ш(E/\mathbb{Q})[\phi_*] \to 0$$

$$\frac{E'(\mathbb{Q})}{\phi E(\mathbb{Q})} \xrightarrow{\alpha_{E'}} \mathbb{Q}^*/(\mathbb{Q}^*)^2 \supseteq S^{(\phi)}(E/\mathbb{Q})$$

$\mathrm{Im}(\alpha_{E'}) = \{ b_1(\mathbb{Q}^*)^2 \in \mathbb{Q}^*/(\mathbb{Q}^*)^2 \mid$ (*) soluble over $\mathbb{Q} \}$

$\cap$

$S^{(\phi)}(E/\mathbb{Q}) = \{ b_1(\mathbb{Q}^*)^2 \in \mathbb{Q}^*/(\mathbb{Q}^*)^2 \mid$ (*) soluble over $\mathbb{R}$ and $\mathbb{Q}_p\ \forall p \}$

Fact

If $a, b_1, b_2 \in \mathbb{Z}$ and $p \nmid 2b(a^2-4b)$ then (*) is soluble over $\mathbb{Q}_p$.

Example 2 (continued)

$y^2 = x^3 + px \qquad p$ prime, $p \equiv 5\ (8)$

$w^2 = pu^4 - 4v^4 \qquad$ ③

$\mathrm{rank}\, E(\mathbb{Q}) = \begin{cases} 0 & \text{③ insoluble over } \mathbb{Q} \\ 1 & \text{③ soluble over } \mathbb{Q} \end{cases}$

use Hensel's Lemma

③ is soluble over $\mathbb{Q}_p$ since $\left(\frac{-1}{p}\right) = 1 \Rightarrow -1 \in (\mathbb{Z}_p^*)^2$

③ is also soluble over $\mathbb{Q}_2$ since $p-4 \equiv 1\ (8) \Rightarrow p-4 \in (\mathbb{Z}_2^*)^2$

③ is soluble over $\mathbb{R}$ since $\sqrt{p} \in \mathbb{R}$.

By the fact above, ③ is also soluble for other primes.

p	u	v	w
5	1	1	1
13	1	1	3
29	1	1	5
37	5	3	151
53	1	1	7

Conjecture

Rank $E(\mathbb{Q}) = 1 \quad \forall$ primes $p \equiv 5\ (8)$

<u>Example 3</u> (Lind)

$E: y^2 = x^3 + 17x$. $\mathrm{Im}(\alpha_E) = \langle 17 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$E': y^2 = x^3 - 68x$. $\mathrm{Im}(\alpha_{E'}) \subset \langle -1, 2, 17 \rangle \subset \mathbb{Q}^*/(\mathbb{Q}^*)^2$

$b_1 = 2$: $w^2 = 2u^4 - 34v^4$

Replace w by $2w$ and get $2w^2 = u^4 - 17v^4$

<u>Notation</u>

$C(K) = \{(u, v, w) \in K^3 \setminus (0,0,0) \mid 2w^2 = u^4 - 17v^4\}/\sim$

where $(u, v, w) \sim (\lambda u, \lambda v, \lambda^2 w)$ for $\lambda \in K^*$.

$C(\mathbb{Q}_2) \neq \emptyset$ since $17 \in (\mathbb{Z}_2^*)^4$

Hensel's Lemma

$C(\mathbb{Q}_{17}) \neq \emptyset$ since $\left(\frac{2}{17}\right) = +1 \Rightarrow 2 \in (\mathbb{Z}_{17}^*)^2$

$C(\mathbb{R}) \neq \emptyset$ since $\sqrt{2} \in \mathbb{R}$.

So $C(\mathbb{Q}_v) \neq \emptyset \;\; \forall v \in M_{\mathbb{Q}}$.

Suppose that $(u, v, w) \in C(\mathbb{Q})$

W.L.O.G. $u, v, w \in \mathbb{Z}$, $\gcd(u, v) = 1$, $w > 0$.

If $17 \mid w$ then $17 \mid u$ and $17 \mid v$ ※

So if $p \mid w$, then $p \neq 17$ and $u^4 \equiv 17v^4 \ (p)$

$\Rightarrow p = 2$ or $\left(\frac{17}{p}\right) = +1$.

If p is odd, $\left(\frac{p}{17}\right) = \left(\frac{17}{p}\right)$ by Quadratic Reciprocity

$= +1$. Also note that $\left(\frac{2}{17}\right) = +1$.

$\therefore$ w is a square mod 17.

We have $2w^2 \equiv u^4 \ (17)$

$\Rightarrow 2 \in (\mathbb{F}_{17}^*)^4 = \{\pm 1, \pm 4\}$ ※

$\therefore C(\mathbb{Q}) = \emptyset$, i.e. C represents a non-trivial element in Ш$(E/\mathbb{Q})$

03/11/13 Elliptic Curves 25

Birch and Swinnerton-Dyer Conjecture

$E/\mathbb{Q}$ an elliptic curve.

Definition

$$L(E,s) = \prod_p L_p(E,s)$$

trace of Frobenius

$$\text{where } L_p(E,s) = \begin{cases} (1-a_p p^{-s} + p^{1-2s})^{-1} & p \text{ has good reduction} \\ (1-p^{-s})^{-1} & \text{split. mult. reduction} \\ (1+p^{-s})^{-1} & \text{non-split mult. reduction} \\ 1 & \text{additive reduction} \end{cases}$$

where $\# \tilde{E}(\mathbb{F}_p) = 1 + p - a_p$

Hasse $\Rightarrow |a_p| \leq 2\sqrt{p} \Rightarrow L(E,s)$ converges for $Re(s) > 3/2$.

Theorem (Wiles, Breuil, Conrad, Diamond, Taylor)

$L(E,s)$ is the L-function of a weight two modular form, and hence has an analytic continuation to all of $\mathbb{C}$.

(and a functional equation $L(E,s) \Leftrightarrow L(E,2-s)$)

Weak BSD

$$\text{ord}_{s=1} L(E,s) = \text{rank } E(\mathbb{Q}) \overset{\shortparallel}{=} r.$$

Strong BSD

$$\lim_{s\to 1} \frac{1}{(s-1)^r} L(E,s) = \frac{\Omega_E \, Reg(E(\mathbb{Q})) \, |Ш(E/\mathbb{Q})| \prod_p c_p}{|E(\mathbb{Q})_{tors}|^2}$$

where c_p = Tamagawa number of $E/\mathbb{Q}_p$

$$= [E(\mathbb{Q}_p) : E_0(\mathbb{Q}_p)]$$

$$E(\mathbb{Q})/E(\mathbb{Q})_{tors} = \langle P_1, \dots, P_r \rangle$$

$$Reg\, E(\mathbb{Q}) = \det([P_i, P_j])_{i,j=1,\dots,r}$$

where $[P,Q] = \hat{h}(P+Q) - \hat{h}(P) - \hat{h}(Q)$

$$\Omega_E = \int_{E(\mathbb{R})} \frac{dx}{|2y + a_1 x + a_3|}$$

, a_i coefficients of a globally minimal weierstrass equation.

3