Elliptic Curves Lecture 1 (05/02)

Introduction to Elliptic Curves

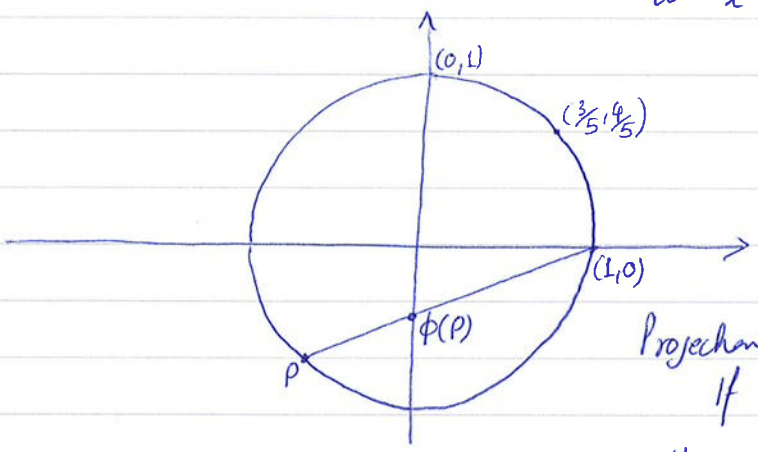
A Diophantine equation is a polynomial equation in several variables to which integer (or rational) solutions are sought.

e.g. $X^2 + Y^2 = Z^2$ has solutions $(0,0,0)$, $(1,0,1)$, $(3,4,5)$, $(5,12,13)$, ...

How many solutions are there?

Can we describe them?

One approach is to use geometry. Enough to study rational solutions to $x^2 + y^2 = 1$.



Projection onto the y-axis

If $P = (x_0, y_0)$ then the line is

$$y = \frac{y_0}{x_0 - 1}(x - 1)$$

So $\phi(P) = \left(0, \frac{y_0}{1 - x_0}\right)$.

We can also find the inverse of ϕ

line through $(0,t)$ and $(1,0)$ is $y = -t(x-1)$

Where does it meet the circle?

Substituting into the equation of the circle, $x^2 + t^2(x-1)^2 = 1$

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

We know that $x = 1$ is certainly a solution to this quadratic equation (because the line passes through $(1,0)$)

sum of roots

Dividing throughout by t^2+1,

$$x^2 - \underbrace{\frac{2t^2}{t^2+1}}_{\text{sum of roots}}x + \underbrace{\frac{t^2-1}{t^2+1}}_{\text{product of roots}} = 0$$

So the line meets the circle at

$$\Psi(0,t) = \left(\frac{t^2-1}{t^2+1}, \frac{2t}{t^2+1}\right)$$

ϕ and Ψ give a bijection

$$\left\{\begin{array}{l}\text{rational points on} \\ x^2+y^2=1 \\ \text{except } (1,0)\end{array}\right\} \underset{\Psi}{\overset{\phi}{\rightleftarrows}} \{(0,t) \mid t \in \mathbb{Q}\}$$

We deduce: Every rational solution to $x^2+y^2=1$ (except $(1,0)$) is of the form

$$x = \frac{t^2-1}{t^2+1}, \quad y = \frac{2t}{t^2+1} \quad \text{with } t \in \mathbb{Q}$$

(This is a parametrization of the solutions)

→ some work: primitive integer solutions to $X^2+Y^2=Z^2$ are $(u^2-v^2, 2uv, u^2+v^2)$ or $(2uv, u^2-v^2, u^2+v^2)$ with u, v coprime integers.

The same approach works for all conics.

What about more complicated curves?

→ use genus to measure "complicated"

$\{x^2+y^2=1\} \subset \mathbb{C}^2$

↳ looks like topological sphere

genus 0

We're interested in curves which have genus 1

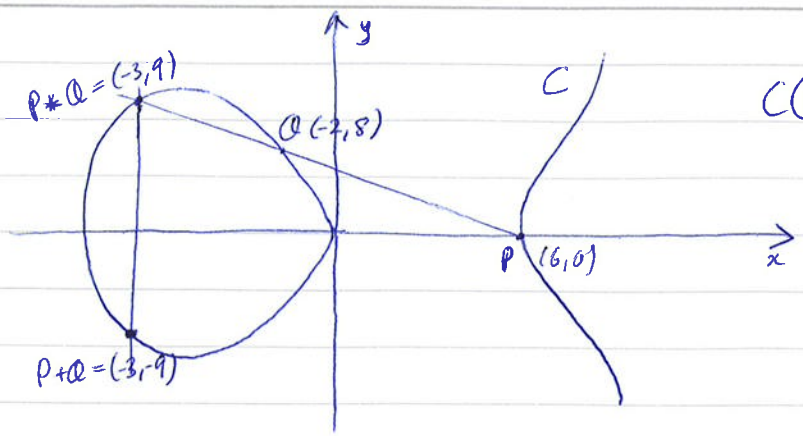
ie. complex solutions look like

These are elliptic curves

They look like $y^2 = x^3 + Ax + B$.

Example $y^2 = x^3 - 36x = x(x+6)(x-6)$

// looks like ↗



$C(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$.

Line through PQ is $y = -x + 6$

Find where it meets C

$$(-x+6)^2 = x^3 - 36x$$

$$\Rightarrow x^3 - x^2 - 24x - 36 = 0$$

(sum of roots $= -1$)

$\Rightarrow$ third solution is $x = -3$

So the curve intersects the line at the point $(-3, 9)$

This gives an operation $P * Q = (-3, 9)$ on the set $C(\mathbb{Q})$

↳ It is not a group operation (e.g. no identity)

But we can remedy this: • add a "point at infinity" $\mathcal{O}$ lying on every vertical line

• define $P + Q = (P * Q) * \mathcal{O}$

Can prove that $+$ makes $C(\mathbb{Q})$ into an abelian group (identity $= \mathcal{O}$).

e.g. $2(-3,9) = \left(\frac{25}{4}, -\frac{35}{8}\right)$

$$3(-3,9) = \left(\frac{-1581}{1369}, -\frac{321057}{50653}\right)$$

$2(6,0) = \mathcal{O}$ so $(6,0)$ is a torsion element in $C(\mathbb{Q})$.

$(-3,9)$ is non-torsion

* Theorem (Mordell, 1922): Let E be an elliptic curve over $\mathbb{Q}$. Then the group $E(\mathbb{Q})$ is a finitely generated Abelian group.

In the above example, $C(\mathbb{Q}) \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$.

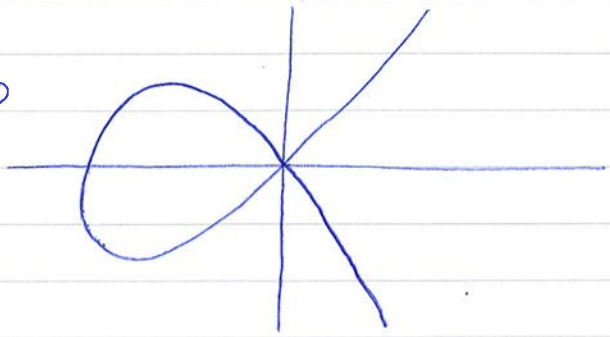
How can we find generators for $E(\mathbb{Q})$?
How can we find the rank?

Question: Can the rank be arbitrarily large?
e.g. explicit curve with rank ≥ 28 (Elkies, 2006).

One way to solve the problem of computing the rank would be to prove the conjecture of Birch and Swinnerton-Dyer (1965)
For each p, count $\#E(\mathbb{F}_p)$ and put them into a generating function $L(E,s)$, defined for $\mathrm{Re}\, s > \frac{3}{2}$.

Conjecture (BSD): $L(E,s)$ extends to a meromorphic function on $\mathbb{C}$, with a zero at $s=1$ of order $r = \mathrm{rank}\, E(\mathbb{Q})$.

Let k be a field. $\bar{k}$ denotes the algebraic closure of k. $k[\vec{x}] = k[x_1, x_2, \ldots, x_n]$.
Definition: affine n-dimensional space is $\mathbb{A}^n = \mathbb{A}^n(\bar{k}) = \bar{k}^n$.
It contains $\mathbb{A}^n(k) = k^n$.
for $S \subset \bar{k}[\vec{x}]$, let $V_S = \{P \in \mathbb{A}^n(\bar{k}) : \forall f \in S,\ f(P) = 0\}$
Example: $f = Y^2 - X^3 - X^2 \in \mathbb{Q}[X,Y]$
$C = V_f$
$C : f = 0$



Note: If $I = (S) \subset \bar{k}[\vec{x}]$ ideal generated by S, then $V_I = V_S$.

Recall: • R commutative ring (e.g. $k[\vec{x}]$). An ideal $I \subset R$ is called prime if R/I is an integral domain (i.e. if $x, y \in R$ such that $xy \in I$ then $x \in I$ or $y \in I$).
• If R is a UFD (e.g. $k[\vec{x}]$) and $0 \neq f \in R$. Then (f) is prime $\Leftrightarrow f$ is irreducible.

e.g. k any field, then $Y^2-X^3-X^2 \in \bar{k}[X,Y]$ is irreducible.
If it is reducible, then $Y^2-X^3-X^2 = (Y+a)(Y+b)$; $a,b \in \bar{k}[\bar{x}]$
$\Rightarrow$ $b=-a$, $a^2 = X^3+X^2$ which is impossible by degree in X.

$Y^2-2X^2 \in \mathbb{Q}[X,Y]$ is irreducible but
$Y^2-2X^2 = (Y-\sqrt{2}X)(Y+\sqrt{2}X) \in \bar{\mathbb{Q}}[X,Y]$

* Definition An (affine) algebraic variety (over $\bar{k}$) in $\mathbb{A}^n$ is a set V_I for a prime ideal $I \subset \bar{k}[\bar{x}]$
e.g. V_f for irreducible $f \in \bar{k}[\bar{x}]$.

for subset $V \subset \mathbb{A}^n(\bar{k})$, let $I(V) = \{f \in \bar{k}[\bar{x}] : \forall P \in V,\ f(P)=0\}$.
↳ ideal of $\bar{k}[\bar{x}]$

* Theorem: There is a bijection
$\{\text{varieties in } \mathbb{A}^n(\bar{k})\} \longleftrightarrow \{\text{prime ideals in } \bar{k}[\bar{x}]\}$
$V \longmapsto I(V)$
$V_I \longleftarrow I$

* Definition: The affine coordinate ring of a variety $V \subset \mathbb{A}^n(\bar{k})$ is
$\bar{k}[V] = \dfrac{\bar{k}[\bar{x}]}{I(V)}$. → is an integral domain

Its field of fractions $\bar{k}(V)$ is called the function field of V

e.g. $V: Y^2 = X^3+X^2$
($V = V_f$ for $f = Y^2-X^3-X^2$)
$\bar{k}[V] = \dfrac{\bar{k}[X,Y]}{(Y^2-X^3-X^2)} = \dfrac{\bar{k}[X][Y]}{(Y^2-X^3-X^2)} = \bar{k}[X] + \bar{y}\,\bar{k}[X]$
with $\bar{y}^2 = X^3+X^2$
$\bar{k}(V) = \bar{k}(X) + \bar{y}\bar{k}(X)$ with $\bar{y} = X^3+X^2$
$= \bar{k}(X)(\sqrt{X^3+X^2})$

* **Definition:** • V is *defined over k* if $\exists\, S \subset k[\vec{x}]$ such that S generates the $k[\vec{x}]$ ideal $I(V)$.

Notation: "V/k"

• If so, let $V(k) = V \cap \mathbb{A}^n(k)$

e.g. $C(\mathbb{Q})$, $V(\mathbb{R})$ etc.

• $k[V] = \text{image}(k[\vec{x}] \to \bar{k}[V])$

$\cong \dfrac{k[\vec{x}]}{I(V) \cap k[\vec{x}]}$

• $k(V)$ = field of fractions of $k[V] \subset \bar{k}[V]$.

Dimension

* **Definition:** For fields $\ell > k$, the *transcendence degree* of ℓ over k is $\#T$ when $T \subset \ell$ is algebraically independent over k and $\ell \supset k(T)$ is algebraic.

Then $\dim(V)$ = transcendence degree $(\bar{k}(V)/\bar{k})$

* **Definition:** curve = variety of dimension 1.

Example: $C: y^2 = x^3 + x^2$.

(ie. $C = V_f$, $f = y^2 - x^3 - x^2$)

Recall that $\bar{k}(C) = \bar{k}(x)(\sqrt{x^3+x^2}) = \ell$

Take $T = \{x\}$, then $\bar{k}(C)/k(x)$ is algebraic, so

$\dim(C) = \text{tr. deg.}\,(\bar{k}(C)/\bar{k}) = \#T = 1$.

e.g. $V = \mathbb{A}^n$.

$\bar{k}[V] = \bar{k}[\vec{x}]$

$\bar{k}(V) = \bar{k}(\vec{x})$

$T = \{x_1, x_2, \dots, x_n\}$

$\therefore \dim(\mathbb{A}^n) = n$.

* **Definition:** For $f_1, \dots, f_m \in \bar{k}[\vec{x}]$, let $V = V_{\{f_1, \dots, f_m\}}$ and $P \in V(\bar{k}) = V$

• Then V is *smooth / non-singular* at P if the $n \times n$ matrix ↗

$$M = \left(\frac{\partial f_i}{\partial x_j}(P) \right)_{i,j}$$

has rank $n - \dim(V)$

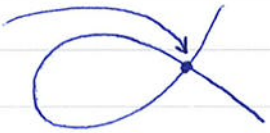
- V is smooth if it is smooth at all points $P \in V(k)$
- The <u>tangent space</u> of V at P is $T_P = \{ \vec{x} \in \hat{k}^n : M(\vec{x} - P) = \vec{0} \}$

$$= P + \ker(M)$$

$$\dim T_P = \dim(\ker(M)) = n - \operatorname{rank}(M).$$

So $\dim T_P = \dim(V) \iff \operatorname{rank}(M) = n - \dim(V)$.

Exercise: Show that $C: Y^2 = X^3 + X^2$ is smooth everywhere except here



Elliptic curves lecture 2 (12/02)

Vak: _____ Naam: _____

Datum: _____ Studierichting: _____

Docent: _____ Collegekaartnummer: _____

Projective Space

$k \to$ algebraically closed field.

Define *n-dimensional projective space* over k

$$\mathbb{P}^n(k) = \underbrace{k^{n+1} \setminus \{0,0,\dots,0\}}_{\sim}$$

where $(x_0,\dots,x_n) \sim (\lambda x_0,\dots,\lambda x_n)$ for $\lambda \in k^\times$.

A point $P \in \mathbb{P}^n(k)$ is given by $P = (x_0 : \dots : x_n)$ (not unique!)

The ratios x_i/x_j are well defined.

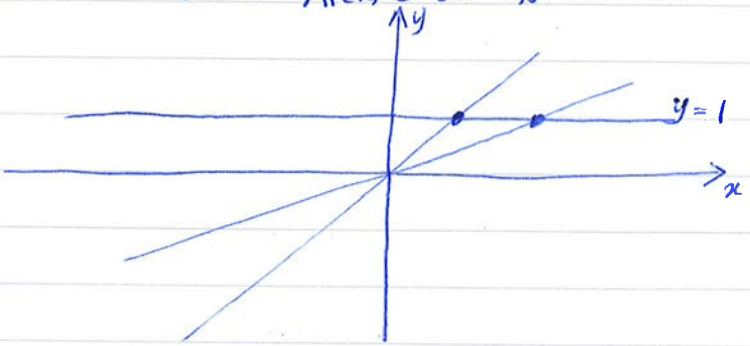
Example: $\mathbb{P}^1(k) = \underbrace{k^2 \setminus \{(0,0)\}}_{\sim}$

If $(x:y) \in \mathbb{P}^1(k)$ has $y \neq 0$, then $(x:y) = (x/y : 1)$

So we get a bijection $\{(x,y) \in \mathbb{P}^1(k) \mid y \neq 0\} \leftrightarrow \mathbb{A}^1(k)$.

The only other point is $(1:0) = (2:0) = \dots$.

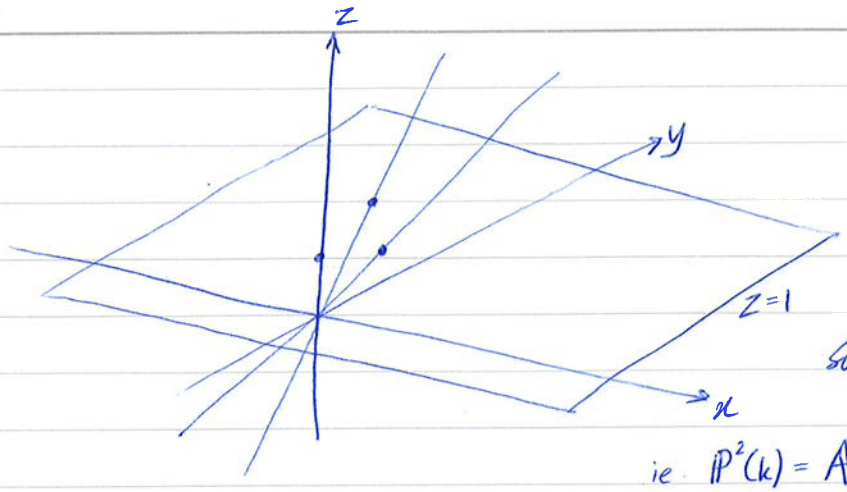
$\Rightarrow \mathbb{P}^1(k) = \mathbb{A}^1(k) \cup \{(1:0)\}$.



What about $\mathbb{P}^2(k)$?

If $(x:y:z) \in \mathbb{P}^2(k)$ has $z \neq 0$, then $(x:y:z) = (x/z : y/z : 1)$

$\Rightarrow$ bijection: $\{(x:y:z) \in \mathbb{P}^2(k) \mid z \neq 0\} \leftrightarrow \mathbb{A}^2(k)$



lines that do not meet $z=1$ are in the xy plane so they form a copy of $\mathbb{P}^1(k)$

ie $\mathbb{P}^2(k) = \mathbb{A}^2(k) \cup \mathbb{P}^1(k)$.

In general, $\{(x_0 : \cdots : x_n) \in \mathbb{P}^n(k) \mid x_i \neq 0\} \longleftrightarrow \mathbb{A}^n(k)$

We get $n+1$ subsets of $\mathbb{P}^n(k)$ each in bijection with $\mathbb{A}^n(k)$.

These are the affine pieces/patches of $\mathbb{P}^n(k)$.

Projective algebraic sets

Given $f \in k[x_0, \ldots, x_n]$, $P \in \mathbb{P}^n(k)$, the value $f(P)$ is not defined.

If f is homogeneous, then whether $f(P) = 0$ is well defined.

because $f(\lambda x_0, \ldots, \lambda x_n) = \lambda^d f(x_0, \ldots, x_n)$ for f homogeneous of degree d.

Define $V_f \subset \mathbb{P}^n(k)$ for f homogeneous

$V_f = \{P \in \mathbb{P}^n(k) \mid f(P) = 0\}$.

(more generally, define V_I where $I \subset k[x_0, \ldots, x_n]$ is an ideal generated by homogeneous polynomials).

Such a set is a projective algebraic set

→ If k is not algebraically closed a projective algebraic set over $\bar{k}$ is defined over k if it can be defined by polynomials with coefficients in k.

→ A point of $\mathbb{P}^n(\bar{k})$ is defined over k if it can be written as $(x_0 : \cdots : x_n)$ with $x_i \in k$.

A projective variety is an irreducible projective algebraic set.

Affine and projective

Consider $\mathbb{A}^n \subset \mathbb{P}^n$ by identifying $\mathbb{A}^n$ with $\{x_0 \neq 0\}$

We have

$k[x_1, \ldots, x_n]$ ⟷ {homogeneous polynomials in $k[x_0, \ldots, x_n]$}

$f(1, x_1, \ldots, x_n)$ ⟵ f

Homogenising: e.g. $X_1^2 + X_1X_2 + X_2^4$

$\downarrow$

$X_0^2X_1^2 + X_0^2X_1X_2 + X_2^4$.

Given an algebraic set $V \subset \mathbb{A}^n$, its projective closure $\bar{V} \subset \mathbb{P}^n$ is defined by homogenisations of all polynomials in $k[x_1, \dots, x_n]$ vanishing on V.

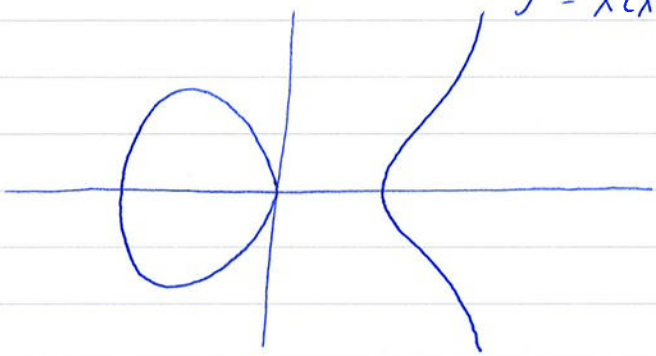
Proposition 2.6 (a) V affine variety $\Rightarrow V = \bar{V} \cap \mathbb{A}^n$.

(b) V projective variety $\Rightarrow V \cap \mathbb{A}^n = \emptyset$ or $\overline{V \cap \mathbb{A}^n} = V$.

(Note: $V \cap \mathbb{A}^n$ is an affine variety)

(c) A projective variety V is defined over k if and only if $V \cap \mathbb{A}^n$ is defined over k (with $V \cap \mathbb{A}^n \neq \emptyset$.)

Example: Take $V \subset \mathbb{A}^2$ defined by $y^2 = x(x^2 - 1)$ $(k = \mathbb{Q})$



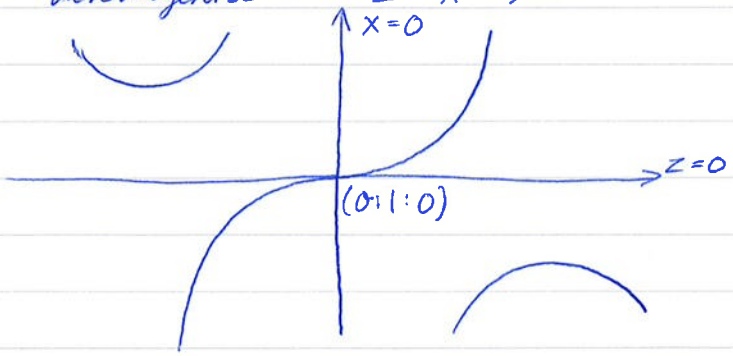
Its projective closure is $\bar{V} \subset \mathbb{P}^2$ defined by $y^2z = x^3 - xz^2$.

To find the points at infinity, set $z = 0$

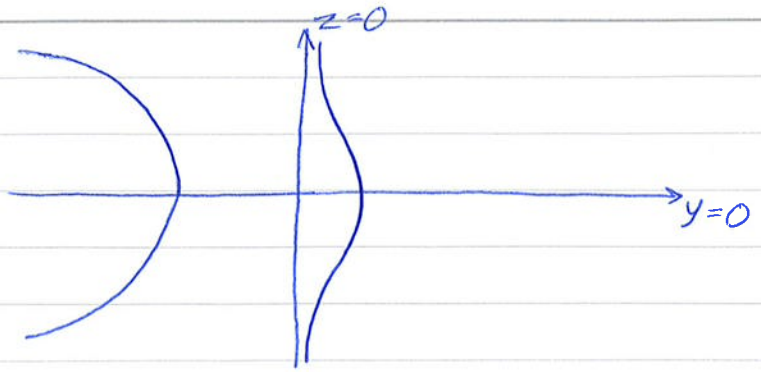
$z = 0 \Rightarrow x^3 = 0$ so $(0:1:0)$ is the unique point at infinity on $\bar{V}$

Other two affine patches?

$y \neq 0$ dehomogenise $\longrightarrow$ $z = x^3 - xz^2$



$x \neq 0$ dehomogenise $\longrightarrow$ $y^2z = 1 - z^2$



Funchan field

Consider $\frac{f}{g}$ where $f, g \in k[x_0, \dots, x_n]$ homogeneous of the same degree.

For $P \in \mathbb{P}^n(k)$, the value $\frac{f(P)}{g(P)}$ is defined whenever $g(P) \neq 0$.

Let $V \subset \mathbb{P}^n$ be a projective variety.

Then $\frac{f_1}{g_1}, \frac{f_2}{g_2}$ define the same funchan on V (wherever both defined)

if and only if $f_1 g_2 - f_2 g_1 \in I(V)$ ← ideal generated by homogeneous polynomials vanishing on V.

These form the funchan field $\hat{k(V)}$ of V.

Formally, $k(V) =$ frac $\left(\frac{k[x_0, \dots, x_n]}{I(V)} \right)_0$ ← homogeneous of degree 0.

Check $k(V) \cong$ (funchan field of an affine piece of V)

dehomogenise →

← homogenise

Dimension $\dim(V) = \text{tr. deg}_k(k(V))$

Maps between varieties

Two varieties $V_1, V_2 \subset \mathbb{P}^n$

Consider rational funchans $(f_0, \dots, f_n)$ with $f_i \in \bar{k}(V)$

At points where $f_i(P)$ are all defined and not all zero, we get

$(f_0(P) : \dots : f_n(P)) \in \mathbb{P}^n(k)$.

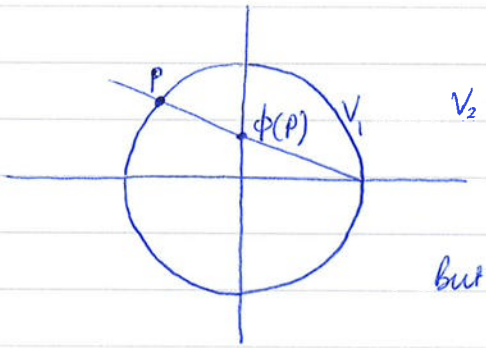
This defines a rational map $V_1 \longrightarrow \mathbb{P}^n$.

If the image is contained in V_2, it is a rational map $V_1 \longrightarrow V_2$
It is defined over k if the f_i (can be chosen to) have coefficients in k.

Example $V_1 \subset \mathbb{P}^2 : X^2+Y^2=Z^2$

$V_2 = \mathbb{P}^1$

$\phi : V_1 \longrightarrow V_2$ defined by $\left(1 : \frac{y}{x-z}\right) = \left(\frac{x-z}{y} : 1\right) = (x-z : y)$



$V_2 = y\text{-axis} \cong \mathbb{P}^1$

Looks like it's not defined at $(1:0:1) \in V_1$

But $\frac{x-z}{y} = \frac{(x-z)(x+z)}{y(x+z)} = \frac{x^2-z^2}{y(x+z)} = \frac{-y^2}{y(x+z)}$

$= \frac{-y}{x+z}$.

So $\phi = \left(\frac{-y}{x+z} : 1\right) = (-y : x+z)$ ...

$\phi(1:0:1) = (0:2) = (0:1)$.

Say a rational map $\phi : V_1 \longrightarrow V_2$ is defined or regular at $P \in V_1$ if there exists a representation $\phi = (f_0 : \cdots : f_n)$ with $f_i(P)$ all defined and not all zero.

A rational map that is defined everywhere on V_1 is a regular map or a morphism

A morphism that has an inverse morphism is an isomorphism

II. Curves

A curve is a projective variety of dimension 1.

Definition: V variety, $P \in V$ point

The local ring at P is $\bar{k}[V]_P = \{f \in \bar{k}(V) \mid f \text{ is defined at } P\}$

What does this look like? Work on an affine piece containing P

$$\bar{k}(V) = \left\{ \frac{f}{g} : f, g \in k[x_1, \dots, x_n],\ g \notin I(V) \right\} / \sim$$

where $\frac{f_1}{g_1} \sim \frac{f_2}{g_2}$ iff $f_1 g_2 = f_2 g_1 \in I(V)$.

An element of $\bar{k}(V)$ is defined at P iff it can be written as $\frac{f}{g}$ with $g(P) \neq 0$

Ideal $m_P \subset \bar{k}[V_P]$ consisting of functions evaluating to 0 at P.

This is a local ring: it has a unique maximal ideal (namely m_P).

Proposition 1.1: P is a smooth point of a curve $C \iff \bar{k}[C]_P$ is a DVR.

A generator for m_P is called a uniformizer or local parameter at P.

$\longrightarrow$ get $\mathrm{ord}_P : \bar{k}(C)^\times \longrightarrow \mathbb{Z}$

every non-zero $f \in \bar{k}(C)$ can be written as $f = t^n g$ with $g \in \bar{k}[C]_P$ a unit.

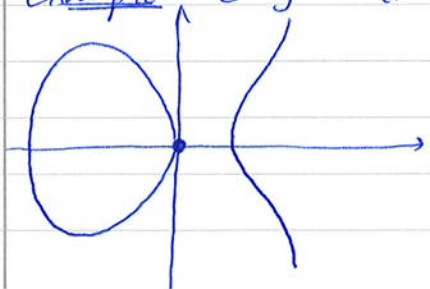
$n = \mathrm{ord}_P(f)$.

$\mathrm{ord}_P(f) \geq 0 \iff f$ is regular at P (or $f \in \bar{k}[C]_P$)

$\mathrm{ord}_P(f) = n > 0 \to$ say f has a zero of order n at P.

$\mathrm{ord}_P(f) = -n < 0 \to$ say f has a pole of order n at P.

Example $C: y^2 = x(x^2-1) \subset \mathbb{A}^2$, $P = (0,0)$



Claim: y is a local parameter at P.

Write the equation as $x + y^2 - x^3 = 0$

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

$\Rightarrow \quad x = \frac{-y^2}{1-x^2}$ in $\bar{k}[C]_p$

Why is y a local parameter?

m_p is generated by x, y but we've just shown $x = y^2 \times$ unit

so we don't need x so $m_p = (y)$.

(and $ord_{(0,0)}(x) = 2$).

Elliptic Curves Lecture 3
19/02.

Vak: _____ Naam: _____

Datum: _____ Studierichting: _____

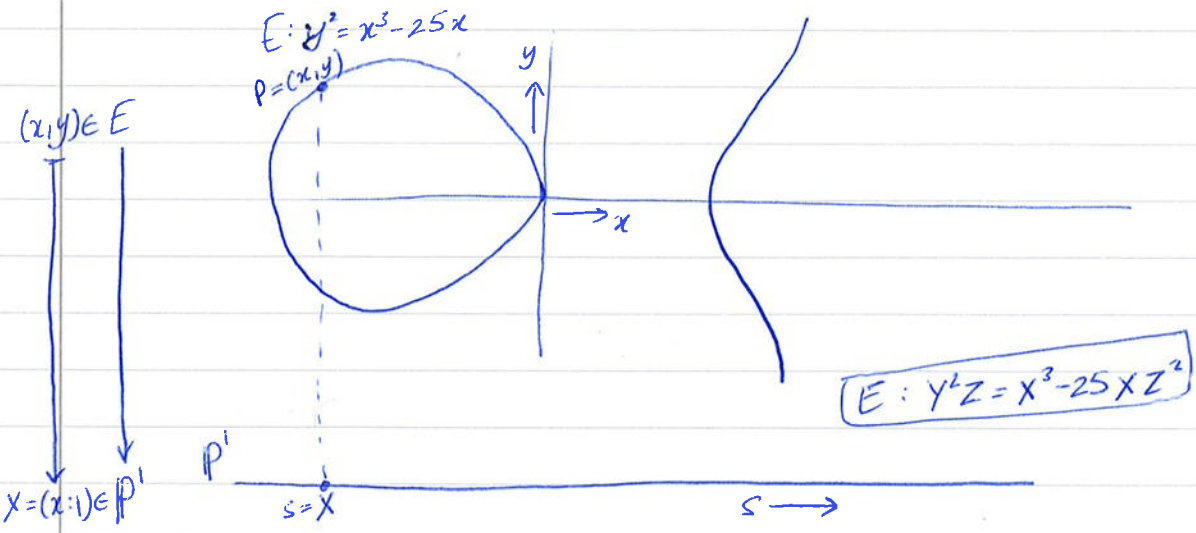
Docent: _____ Collegekaartnummer: _____

Recall: A rational map $\phi: V \to W \subset \mathbb{P}^n$ is $\phi = (f_0 : \dots : f_n) \in (k(V)^{n+1} \setminus \{0\})/\sim$ ($\sim$ = scaling by $k(V)^\times$) satisfying the defining equations of W.
It is **regular at $P \in V$** if it has a representative $(f_0, \dots, f_n)$ with $\forall i$ $f_i \in k[V]_P$ $\leftarrow \operatorname{ord}_P(f_i) \geq 0$ & $\exists i$ $f_i(P) \neq 0$ $\leftarrow \operatorname{ord}_P(f_i) = 0$
(Then $\phi(P) \in \mathbb{P}^n$ makes sense).

Theorem 2.1: $\phi: C \longrightarrow W \subset \mathbb{P}^n$
(C curve)
Then ϕ is regular at all smooth points of C. If C is smooth then ϕ is a morphism.

Proof: $\phi = (f_0 : \dots : f_n)$, $P \in C$ a smooth point. Let u be a uniformizer at P (local ring at P is a DVR). Let $m = \min\{\operatorname{ord}_P f_i : i = 0, \dots, n\}$
Note $\phi = (\underbrace{u^{-m} f_0}_{\operatorname{ord}_P \geq 0} : \dots : \underbrace{u^{-m} f_n}_{\operatorname{ord}_P \geq 0})$ & one of them has $\operatorname{ord}_P = 0$.

- morphism $\iff$ regular at all $P \in C$. □



Example: what is $\phi(O)$ for $O = (0:1:0)$?
More generally $f \in k(C)$, get $\phi: C \to \mathbb{P}^1$, $\phi = (f : 1)$.
Note: $\phi = (f:1) = (1 : \frac{1}{f})$ ($f \neq 0$, is boring!)
for $P \in C$,
$\operatorname{ord}_P f \geq 0 \rightsquigarrow \phi(P) = (f(P) : 1) \in \mathbb{P}^1$.

$\mathrm{ord}_P f \le 0 \rightsquigarrow \phi(P) = (1 : f(P))$
$(\mathrm{ord}_P \tfrac{1}{f} \ge 0)$

$\mathrm{ord}_P f > 0 \rightsquigarrow \phi(P) = (f(P) : 1) = (0:1) = 0 \in \mathbb{P}^1$.

$\mathrm{ord}_P f < 0 \rightsquigarrow \phi(P) = (1 : \tfrac{1}{f}(P)) = (1:0) = \infty \in \mathbb{P}^1$.

$\phi^{-1}(\{0\}) = \{\text{zeros of } f\} \subset C$

$\phi^{-1}(\{\infty\}) = \{\text{poles of } f\} \subset C$.

We write $\phi = f$.

$x(O)$, $O = (0:1:0)$?

$\mathrm{ord}_O(x) < 0$, so $x(O) = (1:0) = \infty$

In fact, $\mathrm{ord}_O(x) = -2$, $\mathrm{ord}_O(y) = -3$ } exercise!

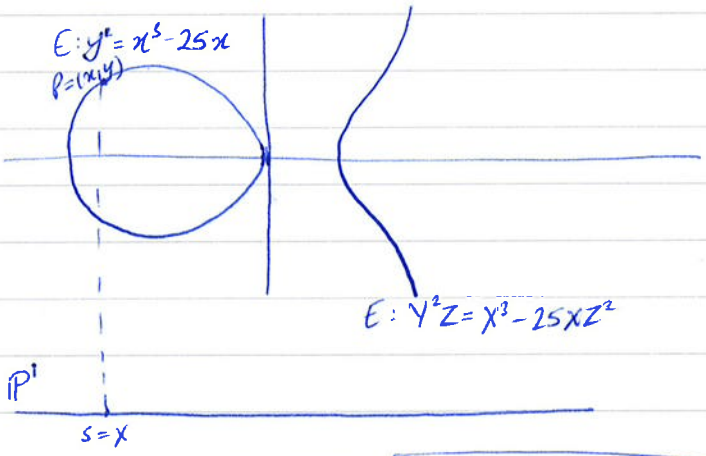
Recall: for non-constant $\phi : C_1 \longrightarrow C_2$

$\rightsquigarrow \phi^* : k(C_2) \longrightarrow k(C_1)$

$f \longmapsto f \circ \phi$.

If ϕ is constant
$\phi : C_1 \to \{Q\} \subset C_2$
Then
$\phi^* = \mathrm{eval}_Q$:
$k[C_2]_{\mathfrak{a}} \to k$

Example: $\phi : C_1 \longrightarrow C_2$
$\| \quad\quad \|$
$E \xrightarrow{x} \mathbb{P}^1$



$x^* : \phi^* : k(\mathbb{P}^1) \longrightarrow k(E)$

$\phi^* k(s) = k(x) \subset k(E)$

$k(s) \quad\quad k(x)[Y] / (Y^2 - x^3 + 25x)$

$\Downarrow \quad\quad \Downarrow$

$f(s) \longmapsto f(x)$

e.g. $\phi^*\left(\frac{s^2+1}{s}\right) = \frac{x^2+1}{x}$.

is a ring homomorphism, equivalently it is a field embedding
so $\phi^* k(C_2)$ is a subfield of $k(C_1)$

Definition:

$$\deg(\phi) = \begin{cases} 0 & \text{if } \phi \text{ is constant} \\ \underbrace{[k(C_1) : \phi^* k(C_2)]}_{\text{fact: } \in \mathbb{Z}_{\geq 1}} & \text{otherwise.} \end{cases}$$

In the previous example, $\deg(x : E \to \mathbb{P}^1) = 2$.

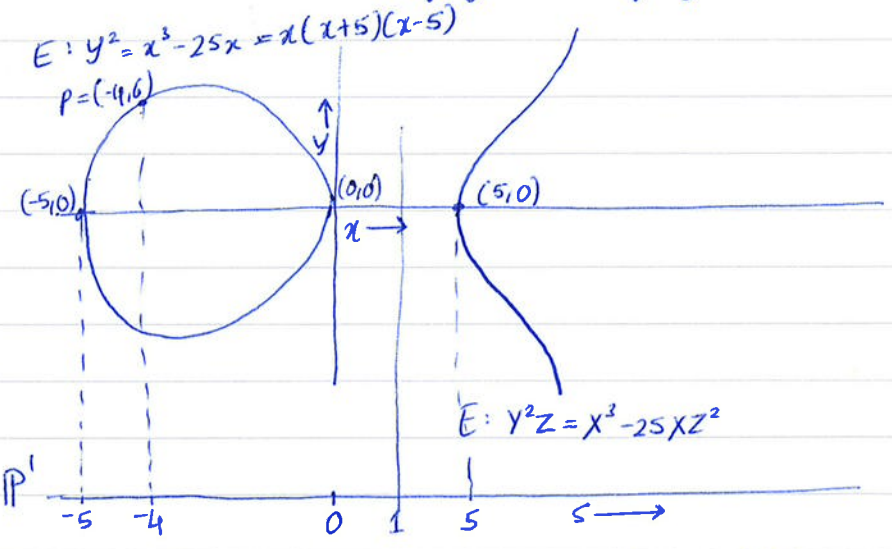
Theorem 2.4: Contravariant equivalence of categories

$$\left(\begin{array}{c}\text{objects: smooth projective curves over } k \\ \text{morphisms: non-constant morphisms over } k\end{array}\right) \longrightarrow \left(\begin{array}{c}\text{objects: field extensions over } k \text{ of transcendence degree } 1 \\ \text{morphisms: field embeddings that are the identity on } k\end{array}\right)$$

$$C \longmapsto k(C)$$

$$(\phi : C_1 \to C_2) \longmapsto (\phi^* : k(C_2) \to k(C_1))$$

Corollary 2.4.1 $\deg(\phi) = 1 \iff \phi$ is an isomorphism where $\phi : C_1 \to C_2$ is a rational map of smooth projective curves.



$(-1, \pm\sqrt{-24}) \in E(\overline{\mathbb{Q}})$

Observation

- for most $a \in \mathbb{P}^1$ $\exists$ *two* points in $E(\overline{\mathbb{Q}})$ mapping to a
- finitely many $a \in \mathbb{P}^1$ with one $P \in E(\overline{\mathbb{Q}})$ mapping to it.

Definition: for $\phi : C_1 \xrightarrow{P} C_2$ non-constant, the *ramification index* of ϕ at P is $e_\phi(P) = \operatorname{ord}_P(\phi^* t)$ where t is a uniformizer at $\phi(P)$. $\in \mathbb{Z}_{\geq 1}$

• ϕ is unramified at P if $e_\phi(P) = 1$

Example: In the curve (on the previous page)

$s - x(P) \to$ uniformizer at $x(P)$

$e_x(P) = ord_P(x - x(P)) = \begin{cases} 1 & \text{if tangent to } E \text{ at } P \text{ is non-vertical} \\ 2 & \text{for } P = (\dots, 0). \end{cases}$

Proposition 2.6 $\phi: C_1 \longrightarrow C_2$ non-constant

(a) $\forall Q \in C_2$:

$$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg(\phi).$$

(b) If $\psi: C_2 \longrightarrow C_3$, then $e_{\psi\circ\phi}(P) = e_\phi(P)\, e_\psi(\phi(P))$

Are all ϕ unramified almost everywhere?

No! Take $k = \overline{\mathbb{F}_p}$

Frobenius $\phi: \mathbb{P}^1 \longrightarrow \mathbb{P}^1$

$x \longmapsto x^p$

$(x:z) \longmapsto (x^p : z^p)$

Call coordinates s $\quad$ t

$s \longmapsto s^p$

$\phi^* t = s^p$

$\forall a \in \overline{\mathbb{F}_p} \subset \mathbb{P}^1$, $\phi(a) = a^p$

Then $t - a^p$ is a uniformizer

$\phi^*(t - a^p) = s^p - a^p = (s-a)^p$

$e_\phi(a) = p \Rightarrow$ ramified everywhere!

$k = \overline{\mathbb{F}_p}$ $\qquad$ $\overline{\mathbb{F}_p}(s) \xleftarrow{\phi^*} \overline{\mathbb{F}_p}(t)$

$s^p \longleftarrow t$

$\overline{\mathbb{F}_p}(s) / \overline{\mathbb{F}_p}(s^p)$ is purely inseparable.

Fact: $\forall$ finite extension of fields $L \supset K$ $\exists$ L^{sep} such that

$L \supset L^{sep} \supset K$ $\qquad$ $[L:K]_s = [L^{sep}:K]$, $[L:K]_i = [L:L^{sep}]$

(purely inseparable, separable)

$\deg_s \phi = [L^{sep} : K]$ (separable degree)
$\deg_i \phi = [L : L^{sep}]$ (inseparable degree)

Proposition 2.6 (c) For all but finitely many $Q \in C_2$,
$\#\phi^{-1}(Q) = \deg_s(\phi)$.

Divisors

k algebraically closed, $C \to$ smooth curve over k.
$\mathrm{Div}(C) =$ (free abelian group generated by points of C)
$= \left\{ \sum_{P \in C} n_P (P) : \forall P \in C,\ n_P \in \mathbb{Z} : \text{for all but finitely many } P, n_P = 0 \right\}$

e.g. $D = 7(O) - 5(P) + (R)$; $P, Q, R \in C$.

$\deg : \mathrm{Div}(C) \longrightarrow \mathbb{Z}$
$\sum_P n_P (P) \longmapsto \sum_P n_P$

$\mathrm{Div}^0(C) = \ker(\deg : \mathrm{Div}(C) \longrightarrow \mathbb{Z})$.

Given $f \in k(C)^\times$, let $\mathrm{div}(f) = \sum_P \mathrm{ord}_P(f)(P)$.

$\mathrm{ord}_P(f) > 0 \iff f(P) = 0$
$\mathrm{ord}_P(f) < 0 \iff f$ has a pole at P.

Example: $E : y^2 = (x - e_1)(x - e_2)(x - e_3)$
$P_i = (e_i, 0) \in E$.
$\mathrm{div}(x - e_i) = 2P_i - 2O$ ($O = (1:0)$ pt. at ∞).
↑ exercise: $\mathrm{ord}_x O = -2$.

homomorphism:

$$k(C)^\times \longrightarrow \mathrm{Div}(C).$$

Definition:
- image = {principal divisors}
- $D_1, D_2 \in \mathrm{Div}(C)$ are called <u>linearly equivalent</u> (notation $D_1 \sim D_2$) if $\exists f \in k(C)^\times : D_1 = D_2 + \mathrm{div}(f)$.
- $\mathrm{Pic}(C) = \dfrac{\mathrm{Div}(C)}{\mathrm{div}(k(C)^\times)}$

$\sum_{P \in \phi^{-1}(Q)} e_\phi(P) = \deg \phi$ so ϕ is surjective

Proposition 3.1 (a) $\mathrm{div}(f) \iff f \in k^\times$.
(b) $\deg(\mathrm{div}(f)) = 0$

Proof of (a): $\Leftarrow$ is clear
$\Rightarrow \mathrm{div}(f) = 0 \rightarrow$ no poles
$\Rightarrow (f : L) : C \longrightarrow \mathbb{P}^1$
does not have ∞ in its image.
$\Rightarrow$ non-surjective
$\Rightarrow$ constant
$\Rightarrow f$ is constant, ie. $f \in k^\times$. ∎

$$\therefore \mathrm{Pic}^0(C) = \frac{\mathrm{Div}^0(C)}{\mathrm{div}(k(C)^\times)}$$

[we will see for elliptic curves
$E \xrightarrow{\text{bijection}} \mathrm{Pic}^0(E)$]

Exact sequence: $1 \longrightarrow k^\times \longrightarrow k(C)^\times \xrightarrow{\mathrm{div}} \mathrm{Div}^0(C) \twoheadrightarrow \mathrm{Pic}^0(C) \longrightarrow 0$
for curves C

for number fields K, there is also an exact sequence

$$1 \longrightarrow \mathcal{O}_K^\times \longrightarrow K^\times \longrightarrow \left(\begin{array}{c}\text{non-zero}\\ \text{fractional ideals}\\ \text{of } \mathcal{O}_K\end{array}\right) \longrightarrow Cl(K) \longrightarrow 0$$

$$x \longmapsto x\mathcal{O}_K$$

What if k is not algebraically closed?

If k is perfect

Galois theory $\quad \mathrm{Div}_k(C) = \mathrm{Div}(C_{\bar{k}})^{\mathrm{Gal}(\bar{k}/k)}$

If k is not perfect...

points

primes

Elliptic Curves Lecture 4 (26/02)

Vak: _____ Naam: _____

Datum: _____ Studierichting: _____

Docent: _____ Collegekaartnummer: _____

Differentials

$k \to$ algebraically closed field

$C \to$ smooth curve over k.

Define the space of differential forms on C : a vector space Ω_C over $k(C)$ with generators $\{dx : x \in k(C)\}$

Relations: (i) $d(x+y) = d(x) + d(y)$

(ii) $d(xy) = x\,dy + y\,dx$

(iii) $da = 0$ for all $a \in k$.

Can deduce other properties, e.g. $d(x^n) = n x^{n-1} dx$, quotient rule etc.

Example: $C : X^2 + Y^2 = Z^2 \subset \mathbb{P}^2_k$

$k(C)$ generated by $x = X/Z$, $y = Y/Z$.

So Ω_C is generated by dx and dy.

But $x^2 + y^2 = 1$ so $2x\,dx + 2y\,dy = 0$

$\therefore dy = -\frac{x}{y}\,dx$.

So Ω_C is 1-dimensional generated by dx (or dy).

Proposition 4.2 (a) Ω_C is a 1-dimensional vector space over $k(C)$.

(b) Ω_C is generated by dx (i.e. $dx \neq 0$) iff $k(C)/k(x)$ is a finite separable extension.

(c) A non-constant morphism $\phi : C_1 \to C_2$ induces $\phi^* : \Omega_{C_2} \to \Omega_{C_1}$ by $\phi^*(f\,dx) = \phi^* f\, d(\phi^* x)$ and ϕ is separable iff ϕ^* is non-zero.

Let P be a point of C, and $\omega \in \Omega_C$.

Take $t \to$ uniformizer at P, then Prop. 4.2(b) $\Rightarrow$ can write $\omega = g\,dt$, $g \in k(C)$.

Define $\mathrm{ord}_P(\omega) = \mathrm{ord}_P(g)$.

* does not depend on choice of uniformizer t

$\omega \neq 0 \Rightarrow$ * $\operatorname{ord}_P(\omega) = 0$ for all but finitely many $P \in C$.

Define $\operatorname{div}(\omega) = \sum_{P \in C} \operatorname{ord}_P(\omega)\, P$.

Say ω is <u>regular</u> if $\operatorname{ord}_P(\omega) \geq 0$ for all P.

Fact: If $\omega_1, \omega_2 \overset{\text{non-zero}}{\in} \Omega_C$ then $\omega_1 = f\omega_2$ for some $f \in k(C)^\times$

So $\operatorname{div}(\omega_1) = \operatorname{div}(f) + \operatorname{div}(\omega_1)$

ie. $\operatorname{div}(\omega_1) \sim \operatorname{div}(\omega_2)$ (They are linearly equivalent)

The <u>canonical divisor class</u> is the class in $\operatorname{Pic} C$ of $\operatorname{div}(\omega)$ for any $0 \neq \omega \in \Omega_C$. Write K_C for any $\operatorname{div}(\omega)$ "canonical divisor".

Given $D \in \operatorname{Div}(C)$, define (as in hw)

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

This is a sub-k-vector space of $k(C)$

e.g. $C = \mathbb{P}^1$, $D = (2:1)$

$(x:y) \in \mathbb{P}^1 \rightarrow \mathcal{L}(D) = \left\{ \dfrac{ax+by}{(x-2y)} : a, b \in k \right\}$

↳ 2-dimensional vector space.

If $D = 2(2:1)$, $\mathcal{L}(D) = \left\{ \dfrac{ax^2+bxy+cy^2}{(x-2y)^2} : a, b, c \in k \right\}$

↳ 3-dimensional vector space.

If C is projective, then $\mathcal{L}(D)$ is finite dimensional for all $D \in \operatorname{Div}(C)$

Define $\ell(D) = \dim_k \mathcal{L}(D)$.

$\mathcal{L}(K_C) \cong$ k-vector space of <u>regular</u> differentials on C.

$f \in \mathcal{L}(K_C) \iff \operatorname{div}(f) + \operatorname{div}(\omega) \geq 0$

$\iff \operatorname{div}(f\omega) \geq 0$

$\iff f\omega$ is a regular differential.

Example: There are <u>no</u> non-zero regular differentials on $\mathbb{P}^1$.

$\mathbb{P}^1 = \{(x:y)\}$, $t = x/y$

Take t = coordinate on $\mathbb{P}^1$ ie. $k(\mathbb{P}^1) = k(t)$

What is $\operatorname{div}(dt)$?

At $(\alpha:1)$, $t - \alpha$ is a uniformizer.

$d(t-\alpha) = dt - d\alpha = dt.$

So $\mathrm{ord}_{(\alpha:1)}\, dt = 0.$

At $(1:0) \in \mathbb{P}^1$, $s = 1/t$ is a uniformizer

$s = y/x$

$\therefore dt = d(1/s) = -\frac{1}{s^2}\, ds$ so $\mathrm{ord}_{(1:0)}(dt) = -2$

$\therefore \mathrm{div}(dt) = -2(1:0).$

So $\mathcal{L}(\mathrm{div}(dt)) = \{0\}$

$(\deg(D) = 0 \Rightarrow \mathcal{L}(D) = \{0\})$

Definition: $g = \ell(K_C)$ is the genus of the curve C.

e.g. $\mathbb{P}^1$ has genus 0.

Theorem (Riemann-Roch): Let C be a smooth projective curve over a field k. K_C canonical divisor on C, g genus of C.

For $D \in \mathrm{Div}(C)$,

$$\ell(D) - \ell(K_C - D) = \deg D - g + 1.$$

Proposition 5.8 C curve over a field k

D divisor on C defined over k.

$\mathcal{L}(D)$ vector space over $\bar{k}$.

This vector space has a basis consisting of functions over k

e.g. $C = \mathbb{P}^1$, $k = \mathbb{Q}$, $D = (0)$

$\mathcal{L}(D)$ has basis $1, 1/x$ over $\mathbb{Q}$ or over $\bar{\mathbb{Q}}$

$\Rightarrow$ Riemann-Roch over $\bar{k}$ $\Rightarrow$ Riemann-Roch over k.

Also we can always take K_C to be a divisor defined over k.

(take $K_C = \mathrm{div}(df)$ for $f \in k(C)$)

Application of Riemann-Roch

$D = K_C \Rightarrow \ell(K_C) - \ell(0) = \deg(K_C) - g + 1$

($\ell(K_C) = g$, $\ell(0) = 1$: constant functions)

$\Rightarrow \deg(K_C) = \underline{2g-2}.$

e.g. $g=0 \quad \therefore \deg(K_C) = -2$

$\ell(D) - \ell(K_C - D) = \deg D + 1$

If $\deg D \geq -1$ then $\deg(K_C - D) < 0$ so $\ell(K_C - D) = 0$.

Proposition III.3.1 k field, E smooth projective curve of genus 1, $O \in E(k)$ a chosen point

Then there is an isomorphism $\phi: E \longrightarrow C$ with $C \subset \mathbb{P}^2$ defined by $Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$ $a_1, a_2, a_3, a_4, a_6 \in k$, and $\phi(O) = (0:1:0)$

Proof Use Riemann-Roch $\ell(K_C - nO) = 0$ for $n \geq 1$

n	$\ell(nO)$	elements of $\mathcal{L}(nO)$
1	1	constants
2	2	$1, x$
3	3	$1, x, y$
4	4	$1, x, y, x^2$
5	5	$1, x, y, xy, x^2$
6	6	$1, x, y, x^2, xy, y^2, x^3$

x some non-constant function with $\operatorname{ord}_O(x) = -2$.

y " " " " " $\operatorname{ord}_O(y) = -3$

linearly dependent

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

for some $A_1, \dots, A_7 \in k$ with A_6, A_7 both not zero.

Change of variable $x \longmapsto -A_6A_7x$

$y \longmapsto A_6A_7^2y$

and divide by $A_6^3A_2^4$ gives an equation as claimed.

Define $\phi: E \longrightarrow \mathbb{P}^2$ by $[x:y:1]$ and let $C = \phi(E)$

Note $\phi(O) = (0:1:0)$

Claim: $\deg(\phi) = 1$

Compose with projection to the x-axis to get

$\phi_x = [x:1] : E \longrightarrow \mathbb{P}^1$

with $\deg(\phi_x) = 2$. since $\phi^{-1}((1:0)) = O$

and $e_{\phi_x}(O) = 2$.

$\Rightarrow \deg\phi \mid \deg\phi_x = 2$

Similarly by projection to y-axis, $\deg\phi \mid 3$

Claim: C is smooth

If not, C is either nodal i.e. 

or cuspidal i.e. 

These both have rational maps ψ to $\mathbb{P}^1$ of degree 1.
Then $\psi \circ \phi : E \longrightarrow \mathbb{P}^1$ would give an isomorphism, but E has genus 1 and $\mathbb{P}^1$ has genus 0.
So C must be smooth as claimed.
$\therefore$ E and C are both smooth and $\phi : E \longrightarrow C$ is a rational map of degree 1, so it is an isomorphism. □

Second application of Riemann-Roch

Proposition: E smooth curve of genus 1 over k
$O \in E(k)$
Then $P \longmapsto [P - O]$
$E(k) \longrightarrow \mathrm{Pic}\, E$
gives a bijection $E(k) \longrightarrow \mathrm{Pic}^0 E$.

Proof: Injectivity
Suppose $[P - O] = [Q - O]$ for $P, Q \in E(k)$
Then $[P] = [Q]$ ie. $P \sim Q$
ie. $\exists f \in k(E)$ with $\mathrm{div}(f) = P - Q$
Then $[f : 1]$ defines an isomorphism $E \longrightarrow \mathbb{P}^1$ which is a contradiction.

Surjectivity
Let $D \in \mathrm{Div}(E)$, $\deg(D) = 0$
Apply Riemann-Roch to $D + O$:

$$\ell(D+O) - \underbrace{\ell(K_E - D - O)}_{\| \; 0} = 1 - 1 + 1 = 1$$

$\Rightarrow \exists\, f \in k(C)^\times$ with $\underline{div(f) + D + O} = 0.$

$P =$ effective divisor of degree 1

$\therefore div(f) + D + O = P$

$\Rightarrow D \sim P - O.$ □

Elliptic Curves Lecture 5
05/03.

Vak: _____ Naam: _____

Datum: _____ Studierichting: _____

Docent: _____ Collegekaartnummer: _____

(General) Weierstrass equation:

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

Weierstrass curve:

projective curve given by a Weierstrass equation.

Elliptic Curve over k: pair $E = (E, O)$

E: smooth projective curve over k (irreducible over $\bar{k}$) of genus 1

$O \in E(k)$

Homomorphism of elliptic curves $\phi : E \to E'$:

morphism of curves $\phi : E \to E'$ such that $\phi(O_E) = O_{E'}$

("isogeny" in the book)

Isogeny: surjective homomorphism of elliptic curves

↖ equivalently: non constant O_E (?)

III 3.1 Let k be a field.

(a) $\forall$ E/k elliptic curve $\exists$ smooth Weierstrass curve C and $\phi : E \xrightarrow{\sim} C$ such that $\phi(O_E) \longrightarrow (0:1:0)$

Proof (a): Last week

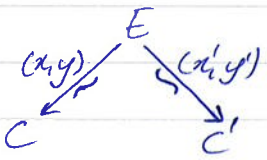
(c) For every smooth Weierstrass curve, the pair $(C, (0:1:0))$ is an elliptic curve

Proof: Homework 5, Problem 4.

(b) Every isomorphism over k between elliptic curves given by Weierstrass equations is of the form: $(x, y) \longmapsto (x', y')$ where

$x = u^2x' + r$, $y = u^3y' + su^2x' + t$ with $u \in k^\times$; $r, s, t \in k$.

Proof (b) Have



(In fact, can take $E = C$ or $E = C'$)

Then $x, y, x', y' \in K(E)$

Recall $1, x$ is a basis of $\mathcal{L}(2(O)) \to$ dimension = 2 by Riemann-Roch.

Same way $1, x'$ is a basis of $\mathcal{L}(2(O))$

So $x = u_1 x' + r$ with $u_1 \in k^\times$, $r \in k$

Similarly: $y \in \mathcal{L}(3(O))$ with basis $1, x', y'$

So $y = u_2 y' + s_2 x' + t$ for some $u_2, s_2, t \in k$ and $u_2 \neq 0$ since $\mathrm{ord}_O y = -3$.

Note: $C: y^2 + \dots = x^3 + \dots$

$\downarrow$

$u_2^2 y'^2 + \dots = u_1^3 x'^3 + \dots$

But $C': y'^2 + \dots = x'^3 + \dots$

So $u_2^2 = u_1^3$. Let $u = u_2/u_1$, $s = s_2/u^2$

Then $u^2 = u_2^2/u_1^2 = u_1$, $u^3 = u_2^3/u_1^3 = u_2$

So $x = u_1 x' + r \Rightarrow x = u^2 x' + r$

and $y = u_2 y' + s_2 x' + t \Rightarrow y = u^3 y' + s u^2 x' + t$ $\Big\}$ $(*)$ $\square$

3.1 $\forall$ Weierstrass curve and all $u \in k^\times$; $r, s, t \in k$, the change of variables $(*)$ gives another Weierstrass curve.

Short Weierstrass equations

If $\mathrm{char}(k) \neq 2$ Let $y' = y + \frac{1}{2}(a_1 x + a_3)$

Then $(y')^2 = y^2 + a_1 xy + a_3 y + \frac{1}{4}(a_1 x + a_3)^2$

$= x^3 + (\dots) x^2 + (\dots) x + (\dots)$

So every Weierstrass curve is isomorphic to a Weierstrass curve with $a_1 = a_3 = 0$.

If also $\mathrm{char}(k) \neq 3$ complete the cube

$x' = x + \frac{1}{3} a_2$

So every Weierstrass equation is isomorphic to Weierstrass equation with $a_1 = a_2 = a_3 = 0$

Short Weierstrass equation: $y^2 = x^3 + Ax + B$.

Still assuming $\mathrm{char} \neq 2, 3$ Every isomorphism between elliptic curves given by short Weierstrass equations is of the form $x = u^2 x'$, $y = u^3 y'$ with $u \in k^\times$.

P. T. O.

$$y^2 = x^3 + Ax + B$$

$x = u^2x',\ y = u^3y'$ ↦ $u^6y'^2 = u^6x'^3 + Au^2x' + B$

Divide throughout by u^6 $\Rightarrow$ $y'^2 = x'^3 + Au^{-4}x' + Bu^{-6}$

$A = u^4A'$, $B = u^6B'$ & we are done.

Singular Weierstrass equations

Suppose S is a singular point on a Weierstrass curve E.

$O = (0:1:0)$ is always non-singular (HW 5, Problem 1(a))

So $S = (x_0, y_0)$

Change of variables $x' = x - x_0$, $y' = y - y_0$

So without loss in generality $S = (0,0)$

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

$a_6 = 0$ as $S \in E$

$\frac{\partial f}{\partial y}(0,0) = a_3 = 0$ $\quad$ $\frac{\partial f}{\partial x}(0,0) = a_4 = 0$ (where f is the equation of the curve)

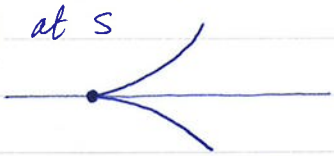
So $E: f = 0$ for $f = \boxed{y^2 + a_1xy - a_2x^2} - x^3$

↑ "2nd order approximation of E around $(0,0)$"

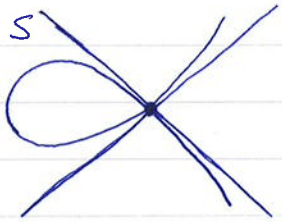
$= (y - \alpha x)(y - \beta x)$ for some $\alpha, \beta \in \bar{k}$

↓ two "tangent" lines.

Definition: If $\alpha = \beta$, then E has a cusp at S



If $\alpha \neq \beta$ then E has a node at S



Discriminant & j-invariant

Definition: $c_4, \Delta \in \mathbb{Z}[a_1, a_2, a_3, a_4, a_6]$ are defined by general formulas in [Silverman, III.1], but also uniquely determined by

- for short Weierstrass equation E $\quad y^2 = x^3 + Ax + B$,

$$c_4(E) = -2^4 \cdot 3 \cdot A$$

$$\Delta(E) = -2^4(4A^3 + 27B^2)$$

• for change of Weierstrass equation (*),

$$c_4(E) = u^4 c_4(E')$$
$$\Delta(E) = u^{12}\Delta(E')$$

Definition: $j = c_4^3/\Delta \in \mathbb{Q}(a_1, \ldots, a_6)$

e.g. for short Weierstrass equation, $j(E) = 1728\,\frac{4A^3}{4A^3+27B^2}$.

III.1.4

(a) Given a Weierstrass curve:

(i) smooth $\iff \Delta \neq 0$

(ii) node $\iff \Delta = 0,\ c_4 \neq 0$

(iii) cusp $\iff \Delta = 0,\ c_4 = 0$.

(b) Two elliptic curves E, E' given by Weierstrass equations, then E and E' are isomorphic over $\bar{k} \iff j(E) = j(E')$

(c) $\forall\, j_0 \in k\ \exists$ elliptic curve E/k such that $j(E) = j_0$.

Proof: Assume $\mathrm{char}(k) \neq 2, 3$

General case: book.

By changes of variables & using (**) we may assume without loss in generality that all Weierstrass equations are short.

(a) 2 cases: $\Delta \neq 0$; $\Delta = 0$

↓ smooth by one of the homework exercises.

for short Weierstrass equation $y^2 = x^3 + Ax + B$,

$c_4 = -2^4 \cdot 3 \cdot A$, $\Delta = -2^4(4A^3 + 27B^2)$

for changes of Weierstrass equation, $c_4(E) = u^4 c_4(E')$

$\Delta(E) = u^{12}\Delta(E')$

$\Delta = 0$: Homework 1 ex 3 (c)

$x^3 + Ax + B = (x-c)^2(x-d)$ for some $c, d \in \bar{k}$

$= x^3 - (c+c+d)x^2 + (cd+cd+c^2)x - ccd$

so $d = -2c$; $A = c^2 + 2cd = c^2 - 4c^2 = -3c^2$.

Let $x' = x - c$; then $y^2 = (x')^2(x' - (d-c)) \to E$

So E: $y^2 - (c-d)x'^2 - x'^3 = 0$ ie. $y^2 - 3cx'^2 - x'^3 = 0$

(since $d = -2c$)

$(y - \sqrt{3c}\,x')(y + \sqrt{3c}\,x')$

So cusp $\iff c=0 \iff A=0 \iff c_4=0$ □(a)

(b) $E: y^2=x^3+Ax+B$, $E': y^2=x^3+A'x+B'$

$$j(E)=1728\frac{4A^3}{4A^3+27B^2}$$

If $E\cong E'$ over $\bar{k}$, then $j(E)=u^{12}/u^{12}\,j(E') \to j(E)=j(E')$

If $j(E)=j(E')$, then $1728\frac{4A^3}{4A^3+27B^2}=1728\frac{4A'^3}{4A'^3+27B'^2}$

so $A^3(4A'^3+27B'^2)=A'^3(4A^3+27B^2)$

so $A^3B'^2=A'^3B^2$ (#)

Goal: Find u such that $A=u^4A'$, $B=u^6B'$.

Case 1 $A=0$, then $B\neq 0$, so $A'=0$

Take $u=(B/B')^{1/6}$.

Case 2 $B=0$, similar, take $u=(A/A')^{1/4}$

Case 3 $A,B\neq 0$. Then $A',B'\neq 0$ (If $A'=0$ then $B'=0$, $\Delta'=0$; If $B'=0$ then $A'=0$, $\Delta'=0$)

Take $u=\left(\frac{A'B}{AB'}\right)^{1/2}$

Then $u^4A'=\frac{A'^3B^2}{A^2B'^2}=A$ (by (#))

similarly $u^6B'=B$. □(b)

Proof (c) formula in book.

Now to find a formula yourself?

Solve for $j_0=1728\cdot\frac{4A^3}{4A^3+27B^2}$

Set $B=A$ and then

$$\Rightarrow j_0=1728\cdot\frac{4A}{4A+27}$$

Solution: [redacted] $A=\frac{27\cdot j_0}{4(1728-j_0)}$

$\Delta=2^6\cdot 3^{12}\cdot\frac{j_0^2}{1728-j_0}$ ok if $j_0\neq 0, 1728$.

for $j=0$, we get an elliptic curve as

$y^2 = x^3 + 1$ has $j=0$

for $j=1728$, we get an elliptic curve as

$y^2 = x^3 + x$ has $j=1728$ □ (c)

III.2 Chord-and-tangent addition

E Weierstrass curve

for $P, Q \in E_{ns}(k) = \{$non-singular points in $E(k)\}$

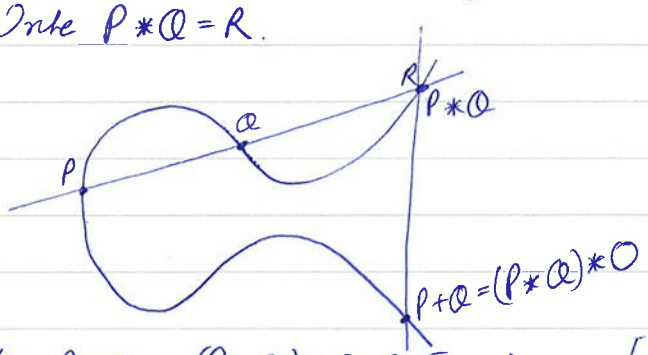
let L line through P & Q

(tangent to E if $P=Q$)

Then $\exists!$ 3rd point of intersection $R \in E_{ns}(k)$

(counted with multiplicity) (HW5 problem 7)

Write $P * Q = R$.



Let $P+Q = (P*Q)*O \in E_{ns}(k)$ [$O \to$ point at infinity $(0:1:0)$]

Claim: $(E_{ns}(k), +)$ is a group

Smooth case

bijection $\kappa : E(\bar{k}) \longrightarrow Pic^0(E_{\bar{k}})$

$P \longmapsto [(P)-(O)]$

HW4, ex 4 $\longrightarrow$ $\kappa(P+Q) = \kappa(P) + \kappa(Q)$

$E(k) \subset E(\bar{k})$ is a subgroup.

Singular case

HW5, ex 5.

Elliptic Curves lecture 6

12/02

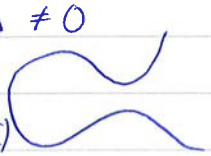
Vak: _____ Naam: _____

Datum: _____ Studierichting: _____

Docent: _____ Collegekaartnummer: _____

E weierstrass curve

$\rightsquigarrow$ 3 cases:

	$\Delta \neq 0$	$\Delta = 0, c_4 \neq 0$	$\Delta = 0$ $c_4 = 0$
	smooth, $E(k) \cong \mathrm{Pic}^0_k(E)$  elliptic curve	node $E^{ns}(\bar{k}) \cong \bar{k}^\times$  multiplicative	cusp $E^{ns}(k) \cong (k,+)$ additive
If $\mathrm{char}(k) \neq 2$ and $E: y^2 = f(x)$ $\deg f = 3$	f has 3 distinct roots in $\bar{k}$	f has a double root and a single root	f has a triple root.

Goal: understand $E(\mathbb{Q}) \cong E(\mathbb{Q})^{tors} \oplus \mathbb{Z}^r$ (group of rational points of E)

later ↑ today using $E(\mathbb{Q}) \to E(\mathbb{F}_p)$

VII, 1-3

Let $R = \mathbb{Z}$, $Q = \mathbb{Q}$, $\pi = p$ prime number, $k = \mathbb{F}_p$, $v = \mathrm{ord}_p$, ie. for $x = p^n \frac{a}{b}$ with $p \nmid a, b$, $v(x) = n$.

Define $v(0) = \infty$, $v(\infty) = -\infty$.

OR, R = DVR, valuation v

$Q = \mathrm{Frac}(R)$ (field of fractions of R)

π = uniformizer

$k = R/\pi R$ residue field

$p = \mathrm{char}(k)$

e.g. $R = \mathbb{C}[[z]]$

For $x \in R$, let $\tilde{x} = x \bmod \pi \in k$

Given $P = (x_0 : \dots : x_n) \in \mathbb{P}^n(Q)$, write it with $x_0, \dots, x_n \in R$ not all common

Let $\tilde{P} = (\tilde{x}_0 : \dots : \tilde{x}_n) \in \mathbb{P}^n(k)$

Get map $\mathbb{P}^n(Q) \longrightarrow \mathbb{P}^n(k)$, $P \longmapsto \tilde{P}$

For $E: f = 0$, f Weierstrass equation with coefficients in R.

Let $\tilde{E}: \tilde{F}=0$, $\tilde{F}$ Weierstrass equation with coefficients in k

Get map $E(\mathbb{Q}) \longrightarrow \tilde{E}(k)$

e.g. $E: y^2 = x^3 + 2x + 4$ over $\mathbb{Q}$

$$P = \left(\frac{1}{4}, -\frac{17}{8}\right) \in E(\mathbb{Q})$$

$$P = \left(\frac{1}{4} : \frac{17}{8} : 1\right) = (2 : -17 : 8)$$

so $P \bmod 2 = (0:1:0)$ on $\tilde{E}(\mathbb{F}_2)$

& $P \bmod 3 = (2:1:2) = (1:2:1) = (1,2) \in \tilde{E}(\mathbb{F}_3)$

Let $E_\pi^0(\mathbb{Q}) = \{P \in E(\mathbb{Q}) : \tilde{P} \in \tilde{E}^{ns}(k)\}$

$[= E(\mathbb{Q})$ if $\tilde{E}$ is smooth$]$

HW problem 4: In this situation $E_\pi^0(\mathbb{Q})$ is a subgroup of $E^{ns}(\mathbb{Q})$ and

$E_\pi^0(\mathbb{Q}) \longrightarrow \tilde{E}^{ns}(k)$ is a homomorphism.
$P \longmapsto \tilde{P}$

Proof: In the book (Silverman).

We say that the Weierstrass equation has good, multiplicative, additive reduction if $\pi \nmid \Delta$; $\pi \mid \Delta$, $\pi \nmid C_4$; $\pi \mid \Delta$, $\pi \mid C_4$ respectively.
(smooth) (node) (cusp)

e.g. $\Delta(E) = -2^8 \cdot 29$, $C_4(E) = -2^5 \cdot 3$

E has good reduction at all primes $\neq 2, 29$

It has multiplicative reduction at $p = 29$

It has additive reduction at $p = 2$

Example: $E: y^2 = x^3 + 1000000$, $p = 5$

has additive reduction at 5.

$F: y^2 = x^3 + 1$ has good reduction at 5

But these are two Weierstrass equations for the same elliptic curve:

$$E \longrightarrow F : (x, y) \longmapsto (10^{-2}x, 10^{-3}y)$$

Definition: A Minimal Weierstrass equation of an elliptic curve E is a Weierstrass equation with coefficients in R such that $v(\Delta)$ is

minimal among all Weierstrass equations for E with coefficients in R.

Reduction of an elliptic curve means reduction of a minimal Weierstrass equation.

Theorem: This does not depend on the choice of a minimal Weierstrass equation.

$$\left.\begin{aligned}\Delta &= u^{12}\Delta' \\ c_4 &= u^4 c_4'\end{aligned}\right\} u \text{ unit mod } \pi$$

if $v(\Delta) < 12$, then Weierstrass equation is minimal
if $v(c_4) < 4$, then Weierstrass equation is minimal

$P \in \ker\left(E_\pi^0(Q) \longrightarrow \tilde{E}^{ns}(k)\right)$

$\Updownarrow$ (for $P \neq 0$)

$v(x(P)) < 0 \iff v(y(P)) < 0$

And if so, then, by $y^2 + \cdots = x^3 + \cdots$ $\quad 2v(y) = 3v(x)$

so $\exists\, n \in \mathbb{Z}_{\geq 1}$ such that $v(y) = -3n$ & $v(x) = -2n$

Definition: for $n \in \mathbb{Z}_{\geq 1}$, let

$$E_\pi^n(Q) = \{0\} \cup \{P \in E(Q) : v(x(P)) \leq -2n\}$$

VII, 2.1 So $E(Q) \supset E^0(Q) \supset E^1(Q) \supset E^2(Q) \supset \cdots$

& $E^1(Q) = \ker\left(E^0(Q) \longrightarrow E^{ns}(k)\right)$

& $E^0(Q)/E^1(Q) \hookrightarrow E^{ns}(k)$

$P \longmapsto \tilde{P}$.

Theorem $\forall n \in \mathbb{Z}_{\geq 1}$: $E_\pi^n(Q)$ is a group, and $\exists$ embedding

$$E_\pi^n(Q)/E_\pi^{n+1}(Q) \hookrightarrow (k, +)$$

VII 2.2 & IV 3.2 & Milne II 4.1

Proof: [Milne] If $E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, $a_i \in R$.

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

where $x' = \pi^{2n}x$, $y' = \pi^{3n}y$

$a_i' = \pi^{in}a_i$

So $f: E \xrightarrow{\sim} E'$

$(x,y) \longmapsto (x',y')$

Claim: $P \in E^n(\mathbb{Q}) \iff f(P) \in (E')^0(\mathbb{Q})$

Claim: $P \in E^{n+1}(\mathbb{Q}) \iff f(P) \in (E')^1(\mathbb{Q})$

So $f: \dfrac{E^n(\mathbb{Q})}{E^{n+1}(\mathbb{Q})} \xrightarrow{\sim} \dfrac{E'^0(\mathbb{Q})}{E'^1(\mathbb{Q})} \hookrightarrow \tilde{E}'^{ns}(k)$

$y^2 = x^3$

$\cong (k,+)$

$P \in E^n(\mathbb{Q})$ $\quad$ $f(P) \in (E')^0(\mathbb{Q})$

$\Updownarrow$ $\quad$ $\Updownarrow$

$v(x(P)) \le -2n \iff v(x'(P)) \le 0 \iff \tilde{x}'(P) \neq 0$

so the 1st claim is proved.

$P \in E^{n+1}(\mathbb{Q})$ $\quad$ $f(P) \in (E')^1(\mathbb{Q})$

$\Updownarrow$ $\quad$ $\Updownarrow$

$v(x(P)) \le -2n-2 \iff v(x'(P)) \le -2$

so the second claim is proved and we are done. □

Theorem VII 3.1 Let $E \to$ Weierstrass equation over $\mathbb{Q}$ and $m \in \mathbb{Z}_{\ge 1}$ such that $p \nmid m$

Then $E(\mathbb{Q})[m] \xhookrightarrow{\varphi} E(\mathbb{Q})/E'(\mathbb{Q})$

(case of good reduction $\hookrightarrow \tilde{E}(k)$)

Proof: Given $P \in \ker \varphi$, $P \neq O$.

Then $v(x(P)) = -2n$ for some $n \in \mathbb{Z}_{\ge 1}$,

so

$$0 \neq [P] \in \frac{E^n(\mathbb{Q})}{E^{n+1}(\mathbb{Q})} \hookrightarrow (k,+)$$

Have $mP = O$, hence $p = \mathrm{char}(k) \mid m$

contradicts the assumption! □

Corollary: For $E/\mathbb{Q}$: $E(\mathbb{Q})^{tors}$ is finite

↑ torsion subgroup.

Proof: HW Problem 5. □

Application: Compute $E(\mathbb{Q})^{tors}$

Example VII 3.3.1

$E: y^2+y = x^3+x+1$ over $\mathbb{Q}$. (f)

$\Delta = -13\cdot 47$, hence good reduction at $p=2$.

So for odd m,

$$E(\mathbb{Q})[m] \hookrightarrow \tilde{E}(\mathbb{F}_2) = \{O\}$$ (only the point at infinity)

$\tilde{E}(\mathbb{F}_2)$: $y^2+y=0$, $x^3+x+1=1$

So $E(\mathbb{Q})$ has no (non-trivial) points of odd order.

If $E(\mathbb{Q})$ has a point of even order, then it has a point of order 2.

$E(\mathbb{Q})[2] = \{O\}$ ⇒ no point of order 2

$\frac{\partial f}{\partial y} = 2y+1$, $x^3 - x + 5/4 = 0$ (irreducible over $\mathbb{Q}$)

So $E(\mathbb{Q})^{tors} = \{O\}$.

Example 3.3.3

$E: y^2 = x^3+x$, $\Delta = -64$

$\#\tilde{E}(\mathbb{F}_3) = 4$ ⇝ torsion points have order dividing $3^a\cdot 4$ for some a

$\#\tilde{E}(\mathbb{F}_5) = 4$ ⇝ torsion points have order dividing $5^b\cdot 4$ for some b.

So torsion points have order dividing 4.

($m \mid n$, p has order n, then $(m/n)p$ has order m)

$\#\tilde{E}(\mathbb{F}_7) = 8$

Note: $(0,0) \in E(\mathbb{Q})[2]$

Note: $E(\mathbb{Q})^{tors} \subseteq E(\mathbb{Q})[4] \hookrightarrow \tilde{E}(\mathbb{F}_p)$ for all odd primes. (Theorem 3.1)

$\tilde{E}(\mathbb{F}_3) \cong \mathbb{Z}/4\mathbb{Z}$

$\tilde{E}(\mathbb{F}_5) \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$

So $E(\mathbb{Q})^{tors} = \langle (0,0) \rangle \cong \mathbb{Z}/2\mathbb{Z}$.

What else is known?

Theorem VII 3.4

Suppose $\mathrm{char}(Q) = 0$ & $p \neq 0$

Let $e_p = v(p)$ ($= 1$ if $K = Q$)

(1) If $n > \frac{e_p}{p-1}$ then $E^n(Q)$ is torsion-free.

(2) Given $P \in E(Q)^{tors}$ of order $m \neq 1$

If m is not a power of p, then $v(x(P)) \geq 0$

If $m = p^n$, then $v(x(P)) \geq -2\left\lfloor \frac{e_p}{p-1} \right\rfloor$

Proof sketch: (1) Switch to completion Q_π, construct power series $\exp_F$, $\log_F$

$$E^n(Q) \subset E^n(Q_\pi) \xrightarrow{\sim} (\pi^n R_\pi, +)$$
$$P \longmapsto \log_F(P)$$
$$\exp_F(z) \longleftarrow z$$

Corollary: E/Q, elliptic curve,

All torsion points $P \in E(Q)$ have integer x & y coordinates except 2-torsion points, and possibly $\left(\frac{a}{2^2}, \frac{b}{2^3}\right)$

Proof: $\left\lfloor \frac{e_p}{p-1} \right\rfloor = 1$ for $p = 2$, 0 for $p > 2$.

Example: $y^2 + xy = x^3 + 4x + 1$

$$\left(-\tfrac{1}{4}, \tfrac{1}{8}\right) \in E(Q)[2]$$

Theorem Lutz-Nagell (VIII 7.2)

$E : y^2 = x^3 + Ax + B$, $A, B \in \mathbb{Z}$ (Short Weierstrass equation!)

$P = (x, y) \in E(Q)^{tors}$

Then $x, y \in \mathbb{Z}$ & $(y = 0$ or $y^2 \mid 4A^3 + 27B^2)$

Mazur's theorem VIII 7.5

P. T. O.

$$E(\mathbb{Q})^{tors} \cong \begin{cases} \mathbb{Z}/m\mathbb{Z} & 1 \le m \le 10 \text{ or } m = 12 \\ (\mathbb{Z}/m\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) & 1 \le m \le 4 \end{cases}$$

Elliptic Curves Lecture 1
19/03

Vak: _____ Naam: _____

Datum: _____ Studierichting: _____

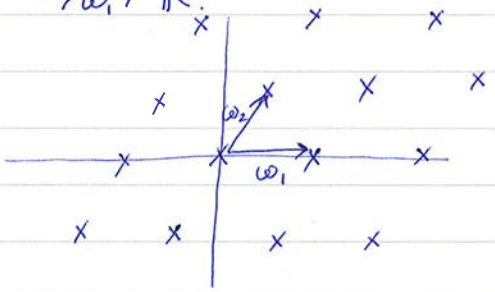
Docent: _____ Collegekaartnummer: _____

Elliptic curves over $\mathbb{C}$

Lattices and complex tori

Definition: A lattice in $\mathbb{C}$ is a discrete subgroup of rank 2 ($\cong \mathbb{Z}^2$)

If Λ is a lattice, then $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ for some $\omega_1, \omega_2 \in \mathbb{C}$ with $\omega_2/\omega_1 \notin \mathbb{R}$.

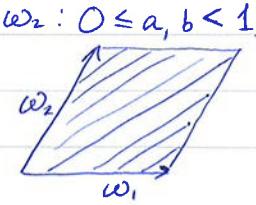


Definition: A complex torus is the quotient of $\mathbb{C}$ by a lattice

It is a Riemann surface in the obvious way.
Any two complex tori are diffeomorphic as real manifolds but are not in general isomorphic as Riemann surfaces.

We are interested in meromorphic functions on complex tori or, equivalently, meromorphic functions on $\mathbb{C}$ that are invariant under the action by translation of a lattice.
These are called elliptic functions or doubly periodic functions.
(Liouville's theorem $\Rightarrow$ there are no non-constant holomorphic elliptic functions).

A fundamental domain for a lattice Λ is, e.g. if $\Lambda = \langle \omega_1, \omega_2 \rangle$ then $D = \{a\omega_1 + b\omega_2 : 0 \le a, b < 1\}$ or any translate of this.



Proposition: Let f be a non-zero elliptic function for Λ, and D a fundamental domain for Λ such that f has no zeros/poles on the boundary of D.

Then: (i) $\sum_{w \in D} \operatorname{res}_w(f) = 0$;

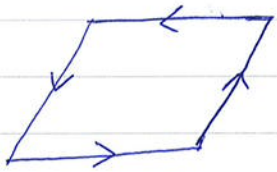
(ii) $\sum_{w \in D} \operatorname{ord}_w(f) = 0$;

(iii) $\sum_{w \in D} \operatorname{ord}_w(f) \cdot w = 0 \bmod \Lambda$.

(all finite sums)

Proof: (i) $\sum_{w \in D} \operatorname{res}_w(f) = \frac{1}{2\pi i} \int_{\partial D} f(z)\,dz = 0$

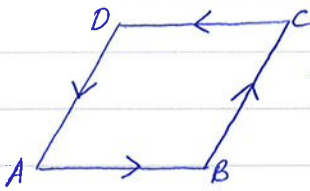
f is periodic $\Rightarrow$ { top & bottom cancel; left & right cancel }



(ii) $\sum_{w \in D} \operatorname{ord}_w(f) = \frac{1}{2\pi i} \int_{\partial D} \frac{f'(z)}{f(z)}\,dz = 0$

(same argument).

(iii) $\sum_{w \in D} \operatorname{ord}_w(f) \cdot w = \frac{1}{2\pi i} \int_{\partial D} \frac{f'(z)}{f(z)}\, z\,dz$



$\frac{1}{2\pi i} \int_{AB} \frac{f'(z)}{f(z)}\, z\,dz + \frac{1}{2\pi i} \int_{CD} \frac{f'(z)}{f(z)}\, z\,dz$

$= \frac{1}{2\pi i} \int_{AB} \frac{f'(z)}{f(z)}\, z\,dz - \frac{1}{2\pi i} \int_{AB} \frac{f'(z)}{f(z)} (z + \omega_2)\,dz$

$\Lambda \Rightarrow = -\omega_2 \cdot \underbrace{\frac{1}{2\pi i} \int_{AB} \frac{f'(z)}{f(z)}\,dz}$

winding number of $f(AB)$ around 0

$f(A) = f(B)$

Similarly, contribution from left + right is an integer multiple of ω_1 and we're done. □

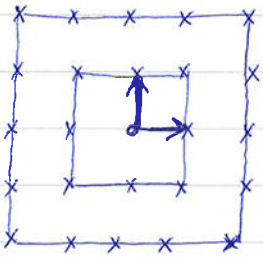
In particular, a non-constant elliptic function must have ≥ 2 zeros and poles (counting multiplicity).

The Weierstrass $\wp$-function

Lemma: Let $\Lambda \subset \mathbb{C}$ be a lattice. The sum

$$\sum_{\substack{w \in \Lambda \\ w \neq 0}} \frac{1}{|w|^3} \quad \text{converges.}$$

Proof: Pick a basis ω_1, ω_2 for Λ



Sum over parallelograms

$P_n = \{a\omega_1 + b\omega_2 : a, b \in \mathbb{R},\ \max\{|a|, |b|\} = n\}$

$B = \min\{|w| : w \in P_1\}$

Then $\min\{|w| : w \in P_n\} = nB$.

$|P_n \cap \Lambda| = 8n$

So $\sum_{w \in P_n \cap \Lambda} \frac{1}{|w|^3} \leq \frac{8n}{(nB)^3}$

and our sum $u \leq \sum_{n=1}^{\infty} \frac{8}{B^3 n^2} = \frac{8}{B^3} \sum_{n=1}^{\infty} \frac{1}{n^2} < \infty$. □

Corollary: The series $G_k(\Lambda) = \sum_{\substack{w \in \Lambda \\ w \neq 0}} \frac{1}{w^k}$ converges absolutely for $k \geq 3$

This is called an Eisenstein series of weight k associated to Λ.

Remarks:
- $G_k(\Lambda) = 0$ for k odd
- $G_2(\Lambda)$ diverges.
- $G_k(\Lambda)$ is a "holomorphic function of Λ" (modular form).

Consider the series $\sum_{w \in \Lambda} \frac{1}{(z-w)^2}$

This looks as if it might define an elliptic function for Λ, but unfortunately it diverges (for $z \in \Lambda$, it looks like G_2 for large w)

So "subtract" G_2 ...

Definition: Let $\Lambda \subset \mathbb{C}$ be a lattice. The Weierstrass $\wp$-function is

$$\wp_\Lambda = \frac{1}{z^2} + \sum_{\substack{w \in \Lambda \\ w \neq 0}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2} \right)$$

Proposition: This series converges normally on compact subsets of $\mathbb{C}$ to a meromorphic elliptic function for Λ.

- f_n holomorphic functions: $\sum f_n$ converges normally on $A \subset \mathbb{C}$ if $\sum_n \left(\sup_{z \in A} |f_n(z)| \right)$ converges.

- If f_n are meromorphic, we allow ourselves to throw away finitely many terms with poles in A.

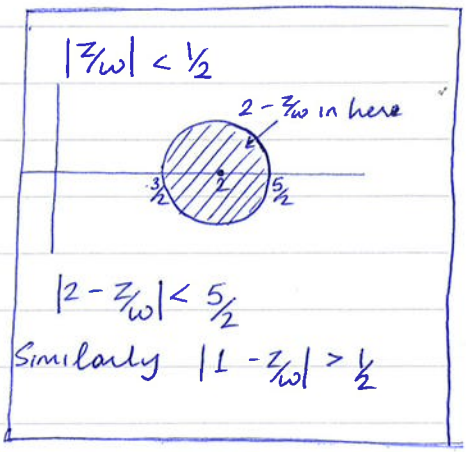
Proof: We'll show that it converges normally on $|z| \leq r$, after discarding terms for $|w| \leq 2r$.

$$\left| \frac{1}{(z-w)^2} - \frac{1}{w^2} \right| = \left| \frac{w^2 - z^2 + 2zw - w^2}{w^2(z-w)^2} \right|$$

$$= \left| \frac{wz(2 - z/w)}{w^4(z/w - 1)^2} \right|$$

$$= \frac{|z(2 - z/w)|}{|w|^3 |1 - z/w|^2}$$

$$< \frac{r \cdot 5/2}{|w|^3 \cdot 1/4} = \frac{10r}{|w|^3}$$



Lemma $\Rightarrow \wp(z)$ converges normally on $|z| \leq r$ for all $r > 0$.

In particular, $\wp(z)$ is meromorphic.

Derivative is $\wp'(z) = \sum_{w \in \Lambda} \frac{-2}{(z-w)^3}$.

$\wp'(z)$ is clearly periodic w.r.t Λ.

For $w \in \Lambda$, $\wp(z+w)$ and $\wp(z)$ have the same derivative $\Rightarrow$ differ by a constant.

But $\wp(w/2) = \wp(-w/2) \Rightarrow$ the constant is 0. ∎

Theorem: Let $\Lambda \subset \mathbb{C}$ be a lattice. Then any elliptic function on Λ is a rational function of $\wp_\Lambda$ and $\wp'_\Lambda$.

Proof: Any function is a combination of an even function and an odd function:

$$2f(z) = (f(z) + f(-z)) + (f(z) - f(-z))$$

If $f(z)$ is odd, then $\wp'(z)f(z)$ is even.

→ sufficient to prove it for even functions.

Let f be an even elliptic function for Λ.

If f has a zero/pole of order n at $z \in \mathbb{C}$, then f also has a zero/pole of order n at $-z$.

Special points where $z \equiv -z \pmod{\Lambda}$ ie. $z = 0, \frac{\omega_1}{2}, \frac{\omega_2}{2}, \frac{\omega_1+\omega_2}{2} \bmod \Lambda$

$(\Lambda = \langle \omega_1, \omega_2 \rangle)$

Here, the odd derivatives of f are odd and periodic, so zero at these points.

⇒ Taylor series has only even terms ⇒ f has even order.

(If f has a pole at w, multiply by a power of $(z-w)$ and then use this argument).

So f has a zero/pole of order m_i at z_i and $-z_i$ $(1 \le i \le r)$ $z_i \not\equiv -z_i \pmod{\Lambda}$ and a zero/pole of order $2n_i$ at z_i' $(1 \le i \le s)$ with $z_i' \equiv -z_i' \pmod{\Lambda}$

Define

$$g(z) = \prod_{i=1}^{r} \underbrace{(\wp(z) - \wp(z_i))^{m_i}}_{\text{zeros of order } m_i \text{ at } \pm z_i} \prod_{i=1}^{s} \underbrace{(\wp(z) - \wp(z_i'))^{n_i}}_{\text{zero of order } 2n_i \text{ at } z_i'}$$

Thus has the same zeros/poles as f away from Λ ⇒ also at points of Λ (by lemma at beginning).

∴ $\frac{f}{g}$ is holomorphic and elliptic, so constant. □

In particular, $(\wp'(z))^2$ must be a rational function of $\wp$.

Define $g_2(\Lambda) = 60 G_4(\Lambda)$

$g_3(\Lambda) = 140 G_6(\Lambda)$

Theorem: $(\wp'(z))^2 = 4\wp(z)^3 - g_2(\Lambda)\wp(z) - g_3(\Lambda)$

Vak: _____ Naam: _____

Datum: _____ Studierichting: _____

Docent: _____ Collegekaartnummer: _____

Theorem Let $\Lambda \subset \mathbb{C}$ be a lattice.
The function $\wp_\Lambda(z)$ satisfies

$$(\wp_\Lambda'(z))^2 = 4\wp_\Lambda(z)^3 - g_2(\Lambda)\wp_\Lambda(z) - g_3(\Lambda)$$

Proof Look at Laurent series
we have $\frac{1}{(1-t)^2} = \sum_{n=0}^{\infty} (n+1)t^n$ for $|t|<1$.

For $|z|<|w|$,

$$\frac{1}{(z-w)^2} - \frac{1}{w^2} = \frac{1}{w^2}\left(\frac{1}{(1-z/w)^2} - 1\right)$$

$$= \sum_{n=1}^{\infty} (n+1)\frac{z^n}{w^{n+2}}$$

So, for $|z|$ sufficiently small and $z \neq 0$,

$$\wp(z) = \frac{1}{z^2} + \sum_{\substack{w\in\Lambda \\ w\neq 0}} \left(\frac{1}{(z-w)^2} - \frac{1}{w^2}\right)$$

$$= \frac{1}{z^2} + \sum_{n=1}^{\infty} (n+1) z^n \sum_{\substack{w\in\Lambda \\ w\neq 0}} \frac{1}{w^{n+2}}$$

$$= \frac{1}{z^2} + \sum_{k=1}^{\infty} (2k+1) G_{2k+2}(\Lambda) z^{2k}$$

Now consider $(\wp')^2 - 4\wp^3 + g_2(\Lambda)\wp + g_3(\Lambda) = g$
Look at Laurent series

$\Rightarrow$ g is holomorphic near $z=0$
and $g(z)=0$

But g is periodic (wrt Λ)
(meromorphic)

with no poles except possibly on Λ.

$\Rightarrow$ g has no poles, so constant

$\Rightarrow$ $g=0$. $\square$

Algebraically: $M(\mathbb{C}/\Lambda) \cong \mathbb{C}(x)[y] / (y^2 - 4x^3 + g_2 x + g_3)$

($M(\mathbb{C}/\Lambda)$: meromorphic elliptic functions for Λ)

Theorem: Let $\Lambda \subset \mathbb{C}$ be a lattice.

The function $\phi : \mathbb{C}/\Lambda \longrightarrow \mathbb{P}^2(\mathbb{C})$

$$[z] \longmapsto \begin{cases} (\wp(z) : \wp'(z) : 1) & z \neq 0 \\ (0:1:0) & z = 0 \end{cases}$$

gives a bijection between $\mathbb{C}/\Lambda$ and the algebraic curve $E_\Lambda \subset \mathbb{P}^2(\mathbb{C})$ defined by

$$Y^2 Z = 4X^3 - g_2(\Lambda) X Z^2 - g_3(\Lambda) Z^3.$$

Proof: We've shown $\mathrm{im}(\phi) \subset E_\Lambda(\mathbb{C})$.

Need to show ϕ is a bijection.

$\phi(0) = (0:1:0)$ and there are no other points at infinity on E_Λ.

Look at $Z \neq 0$. Take $(x:y:1) \in E_\Lambda(\mathbb{C})$

Then $\wp(z) - x$ is periodic, with a double pole at 0.

So it has two zeros at $\pm z_0$, i.e. $\wp(\pm z_0) = x$.

If $z_0 \not\equiv -z_0 \pmod{\Lambda}$ then

$$0 \neq \wp'(z_0) \neq -\wp'(z_0) = \wp'(-z_0)$$

So $\phi(z_0), \phi(-z_0)$ are two distinct points on $E_\Lambda(\mathbb{C})$, namely $(x : \pm y : 1)$. (2 pts $\longleftrightarrow$ 2 pts)

If $z_0 \equiv -z_0 \pmod{\Lambda}$, then $\wp'(z_0) = 0$.

So $x = \wp(z_0)$ is a root of $4x^3 - g_2 x - g_3 = 0$

So $y = 0$. (1 pt $\longleftrightarrow$ 1 pt.) □

Define $\Delta(\Lambda) = g_2(\Lambda)^3 - 27 g_3(\Lambda)^2$

(= discriminant of $4x^3 - g_2(\Lambda)x - g_3(\Lambda)$).

Remark: This is a "holomorphic function of Λ" i.e. a modular form.

Lemma $\Delta(\Lambda) \neq 0$, i.e. E_Λ is an elliptic curve.

Proof: Roots of $4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ are

$$e_1 = \wp(\omega_1/2), \quad e_2 = \wp(\omega_2/2), \quad e_3 = \wp\left(\frac{\omega_1+\omega_2}{2}\right)$$

where $\Lambda = \langle \omega_1, \omega_2 \rangle$

We must show that these are distinct.

e.g. $\wp(z) - e_1$ has a double pole at 0

and a zero at $\omega_1/2$, double since $\wp'(\omega_1/2) = 0$

$\Rightarrow$ It has no other zeros. □

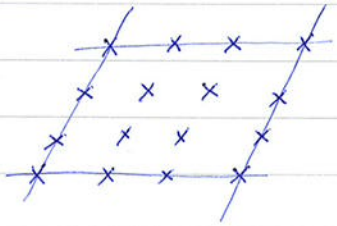
In fact, ϕ is more than just a bijection

- ϕ is an isomorphism of Riemann surfaces.
- ϕ is an isomorphism of groups. (homework exercise)

Remark: e.g. this tells us

$$E(\mathbb{C})[m] \cong (\mathbb{Z}/m\mathbb{Z})^2$$

$\uparrow$ P such that $mP = O$



Thm: The functor $\mathbb{C}/\Lambda \longmapsto E_\Lambda$

complex tori $\longrightarrow$ elliptic curves / $\mathbb{C}$

holomorphic maps $\longrightarrow$ algebraic maps

is an equivalence of categories.

What are the holomorphic maps between two complex tori?

Let Λ, Λ' be two lattices in $\mathbb{C}$.

Any continuous function $\phi: \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$ lifts to a continuous function $\tilde{\phi}: \mathbb{C} \longrightarrow \mathbb{C}$.

Define ϕ to be holomorphic if $\tilde{\phi}$ is.

A function $\tilde{\phi}: \mathbb{C} \longrightarrow \mathbb{C}$ descends to $\phi: \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$ iff, for all $\lambda \in \Lambda$, we have $\tilde{\phi}(z+\lambda) - \tilde{\phi}(z) \in \Lambda'$ for all $z \in \mathbb{C}$.

Example: translation $z \longmapsto z + \alpha$ defines a holomorphic map $\mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda$

If $\phi: \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$ is holomorphic, then after composing with a translation, we may assume $\phi(0) = 0$.

Proposition: Let $\phi: \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$ be holomorphic with $\phi(0) = 0$. Then there exists $\alpha \in \mathbb{C}$ such that $\phi([z]) = [\alpha z]$, for all $z \in \mathbb{C}$, and $\alpha\Lambda \subset \Lambda'$.

Conversely, any such α defines a holomorphic map.

Proof: Clearly, for any $\alpha \in \mathbb{C}$ with $\alpha\Lambda \subset \Lambda'$, multiplication by α defines such a map. Conversely, take $\phi: \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda$ holomorphic, and lift to $\tilde{\phi}: \mathbb{C} \longrightarrow \mathbb{C}$.

For any $w \in \Lambda$, $\tilde{\phi}(z+w) = \tilde{\phi}(z)$ is continuous and takes values in Λ', so is constant.

$\therefore \tilde{\phi}'(z+w) = \tilde{\phi}'(z)$.

$\tilde{\phi}$ is holomorphic and elliptic, so constant

$\to \tilde{\phi}(z) = \alpha z + \beta$ for some $\alpha, \beta \in \mathbb{C}$.

$\tilde{\phi}(0) = 0 \Rightarrow \beta = 0$.

$\tilde{\phi}$ takes Λ into Λ', so $\alpha\Lambda \subset \Lambda'$. □

* A holomorphic map $\phi: \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$ with $\phi(0) = 0$ is called an isogeny

→ We've just proved that every isogeny is also a homomorphism of groups.

→ Two complex tori are isogeneous if there exists an isogeny between them.

Corollary: $\mathbb{C}/\Lambda$ and $\mathbb{C}/\Lambda'$ are isomorphic (i.e. $\exists$ mutually inverse holomorphic maps between them) iff $\Lambda' = \alpha\Lambda$ for some $\alpha \in \mathbb{C}^\times$.

Λ, Λ' are homothetic

Lemma: Under the bijection $\mathbb{C}/\Lambda \longrightarrow E_\Lambda(\mathbb{C})$, $\mathbb{C}/\Lambda' \longrightarrow E_{\Lambda'}(\mathbb{C})$, every holomorphic map $\phi: \mathbb{C}/\Lambda \longrightarrow \mathbb{C}/\Lambda'$ gives rise to an algebraic mapping $E_\Lambda \longrightarrow E_{\Lambda'}$.

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \xrightarrow{\phi} & \mathbb{C}/\Lambda' \\ \downarrow \sim & & \downarrow \sim \\ E_\Lambda(\mathbb{C}) & \xrightarrow{\text{algebraic}} & E_{\Lambda'}(\mathbb{C}) \end{array}$$

Proof:

$$\begin{array}{ccc} \mathbb{C} & \xrightarrow{\tilde{\phi}} & \mathbb{C} \\ \downarrow & & \downarrow \\ \mathbb{C}/\Lambda & \xrightarrow{\phi} & \mathbb{C}/\Lambda' \\ \downarrow \sim & & \downarrow \sim \\ E_\Lambda(\mathbb{C}) & \xrightarrow[\psi]{\text{algebraic}} & E_{\Lambda'}(\mathbb{C}) \end{array}$$

We know $\tilde{\phi}(z) = \alpha z + \beta$, with $\alpha\Lambda \subset \Lambda'$.

Consider $z \longmapsto \wp_{\Lambda'}(\alpha z + \beta)$

For $w \in \Lambda$, $\wp_{\Lambda'}(\alpha(z+w)+\beta) = \wp_{\Lambda'}(\alpha z + \beta + \underbrace{\alpha w}_{\in \Lambda'})$

$= \wp_{\Lambda'}(\alpha z + \beta)$

So $z \longmapsto \wp_{\Lambda'}(\alpha z + \beta)$ is an elliptic function for Λ

$\therefore$ it is a rational function in $\wp_\Lambda, \wp_\Lambda'$.

i.e. x-coordinate $(\Psi(P)) =$ rational function $(x(P), y(P))$

similarly for y-coordinate. □

So we do indeed have a functor

F: complex tori $\longrightarrow$ elliptic curves / $\mathbb{C}$

holomorphic maps algebraic maps.

To show that it is an equivalence of categories it must be full, faithful and essentially surjective.

Faithful

$$\begin{array}{ccc} \mathbb{C}/\Lambda & \longrightarrow & \mathbb{C}/\Lambda' \\ \sim\downarrow & & \sim\downarrow \\ E_\Lambda(\mathbb{C}) & \longrightarrow & E_{\Lambda'}(\mathbb{C}) \end{array}$$

these are maps of sets of points.

Full: need to show every algebraic map between algebraic curves over $\mathbb{C}$ is holomorphic when the curves are considered as Riemann surfaces.

Essentially surjective: need to show that any elliptic curve / $\mathbb{C}$ is isomorphic to E_Λ for some lattice Λ.

Recall: $E: y^2 = x^3 + Ax + B$ has j-invariant

$$j(E) = \frac{1728\,(4A^3)}{4A^3 - 27B^2}.$$

And over $\mathbb{C}$, $j(E_1) = j(E_2) \Rightarrow E_1 \cong E_2$.

If $\Lambda \subset \mathbb{C}$ is a lattice, define

$$j(\Lambda) = \frac{g_2(\Lambda)^3}{g_2(\Lambda)^3 - 27 g_3(\Lambda)^2}$$

Then $j(E_\Lambda) = j(\Lambda)$.

Exercise: If Λ, Λ' are homothetic, then $j(\Lambda) = j(\Lambda')$.

Every lattice is homothetic to $\mathbb{Z} + \mathbb{Z}\tau$ for some
$\tau \in \mathcal{H} = \{z \in \mathbb{C} \mid \operatorname{Im}(z) > 0\}$.

Define $j(\tau) = j(\mathbb{Z} + \mathbb{Z}\tau)$

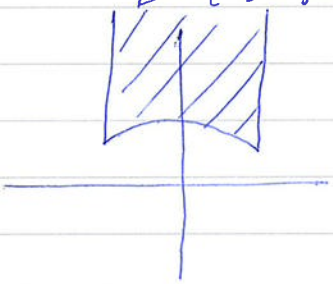
Theorem: $j : \mathcal{H} \longrightarrow \mathbb{C}$ is surjective.

$SL_2(\mathbb{Z})$ acts on $\mathcal{H}$ by $\begin{pmatrix} a & b \\ c & d \end{pmatrix}(z) = \dfrac{az+b}{cz+d}$.

All τ in one orbit under $SL_2(\mathbb{Z})$ define homothetic lattices. $\Rightarrow$ j invariant under $SL_2(\mathbb{Z})$

A fundamental domain for the action of $SL_2(\mathbb{Z})$ is

$$D = \{\tau \in \mathcal{H} : -\tfrac{1}{2} \le \operatorname{Re}(\tau) \le \tfrac{1}{2},\ |\tau| \ge 1\}$$



Proof (sketch - see Stevenhagen)

- j is holomorphic
- $j(\mathcal{H}) \subset \mathbb{C}$ is open
- to show $j(\mathcal{H})$ is closed.

Take a convergent sequence $j(z_1), j(z_2), \ldots$ with $z_i \in D$.

If the z_i converge or have a convergent subsequence, done.

Otherwise, $\operatorname{Im}(z_i) \longrightarrow \infty$ for some subsequence

$$G_{2k}(z_n) = \sum_{\substack{(a,b) \in \mathbb{Z}^2 \\ (a,b) \neq (0,0)}} \frac{1}{(a+bz_n)^{2k}} \longrightarrow 2\sum_{a \ge 1} \frac{1}{a^{2k}} = 2\zeta(2k).$$

so $g_2(\Lambda)^3 - 27 g_3(\Lambda)^2 \longrightarrow 0$

so $j \longrightarrow \infty$ $\square$

Elliptic Curves — Lecture 9.

Vak: _____ Naam: _____

Datum: _____ Studierichting: _____

Docent: _____ Collegekaartnummer: _____

Isogenies

E_1, E_2 elliptic curves over k

An isogeny is a morphism $\phi: E_1 \longrightarrow E_2$ such that $\phi(O_{E_1}) = O_{E_2}$.

$\deg(\phi)$, $\deg_s(\phi)$, $\deg_i(\phi)$, separability etc. defined as for morphisms of curves.

(define $\deg(0\text{map}) = 0$)

$\mathrm{Hom}(E_1, E_2)$ = set of isogenies $E_1 \longrightarrow E_2$.

If $\phi_1, \phi_2: E_1 \longrightarrow E_2$ are isogenies, then define $(\phi_1 + \phi_2)(P) = \phi_1(P) + \phi_2(P)$ (addition on E_2)

This is also an isogeny.

(why? $E_1 \xrightarrow{(\phi_1, \phi_2)} E_2 \times E_2 \xrightarrow{+} E_2$, with $\phi_1 + \phi_2$.)

So $\mathrm{Hom}(E_1, E_2)$ is an abelian group.

If $E_1 = E_2$ $\mathrm{End}(E) = \mathrm{Hom}(E, E)$ is a ring (under composition).

$\mathrm{Aut}(E) = (\mathrm{End}(E))^\times$ group under composition.

Silverman: Hom, End, Aut for isogenies over $\bar{k}$

Hom_k, End_k, Aut_k for isogenies defined over k.

Examples: $[m]: E \longrightarrow E$

$$P \longmapsto mP = \begin{cases} \underbrace{P + \cdots + P}_{m} & m > 0 \\ -(\underbrace{P + \cdots + P}_{-m}) & m < 0 \\ O & m = 0 \end{cases}$$

Clearly $[m] \circ [n] = [mn]$

So we get $[\ ]: \mathbb{Z} \longrightarrow \mathrm{End}_k(E)$ homomorphism of rings.

$m \longmapsto [m]$

(last week/homework: if $k = \mathbb{C}$ then we can transfer to category of complex tori to see $\mathrm{End}(E) \cong \mathbb{Z}$ most of the time
$\mathrm{End}(E) \cong$ order in imaginary quadratic field, in special cases)

Proposition (a) $m \neq 0 \Rightarrow [m] : E \longrightarrow E$ is not constant.

(b) $\mathrm{Hom}(E_1, E_2)$ is a torsion-free abelian group
i.e. if $\phi \neq 0$ then $\phi + \cdots + \phi \neq 0$.

(c) $\mathrm{End}(E)$ has characteristic zero and no (non-zero) zero divisors

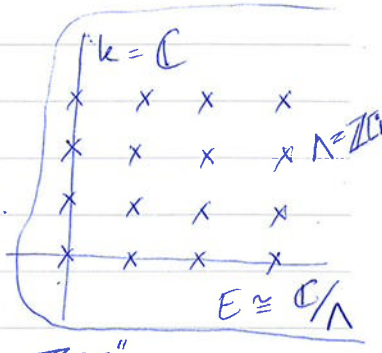
Proof:- (a) Only finitely many points on E satisfy $[2]P = P + P = O$. (apart from O)
(use explicit formula: these are the points with vertical tangent line and there are ≤ 3 of them over $\bar{k}$. Take care if $\mathrm{char}\, k = 2$).
$\Rightarrow [2] \neq [0]$
If $\mathrm{char}\, k \neq 2$ there are points $P \neq O$ with $[2]P = O$
(use formula). Then for odd m, $[m]P = P$, so $[m] \neq [0]$ for m odd.
Now use $[mn] = [m] \circ [n]$
(If $\mathrm{char}\, k = 2$, start instead with a non-trivial 3-torsion point).

(b) If $[m] \circ \phi = \underbrace{\phi + \cdots + \phi}_{m} = 0$ then $\deg[m] \cdot \deg(\phi) = 0$

$\Rightarrow m = 0$ or $\phi = [0]$.

(c) (b) $\Rightarrow \mathrm{char}\, \mathrm{End}(E) = 0$
If $\phi \circ \psi = [0]$ then $\deg\phi \cdot \deg\psi = 0 \therefore \deg\phi = 0$ or $\deg\psi = 0$
i.e $\phi = [0]$ or $\psi = [0]$. □

An isogeny not of the form $[m]$: take $\mathrm{char}\, k \neq 2$ with $i \in k$ such that $i^2 = -1$.
let $E : y^2 = x^3 - x$
define $[i](x, y) = (-x, iy)$
Check $[i]$ is an endomorphism of E, of degree 1.
$[i]$ has order 4 in $\mathrm{Aut}(E)$.
So $\mathrm{End}(E) \neq \mathbb{Z}$. In fact, $\mathrm{End}(E) \cong \mathbb{Z}[i]$
"E has complex multiplication by $\mathbb{Z}[i]$".



Example $k = \mathbb{F}_q$ $(x,y) \longmapsto (x^q, y^q)$ defines the Frobenius endomorphism $E \to E$.

It is purely inseparable of degree q.

It defines a bijection $E(\overline{\mathbb{F}}_q) \to E(\overline{\mathbb{F}}_q)$ of which the fixed points are precisely $E(\mathbb{F}_q)$.

What other morphisms are there between elliptic curves?

Not many: Given E, $Q \in E(k)$,

define $T_Q : E \to E$ by $P \longmapsto P+Q$, translation by Q.

If $\psi : E_1 \to E_2$ is any morphism,

then $T_{\psi(0)} \circ \psi$ is an isogeny.

Theorem 4.8: An isogeny is a homomorphism of groups.

i.e., if $\phi : E_1 \to E_2$ is an isogeny, then

$\phi(P \overset{\uparrow}{+} Q) = \phi(P) + \phi(Q)$ for all $P, Q \in E_1$

addition on E_1 ; addition on E_2.

Proof: Assume $k = \bar{k}$. Recall

$$E(k) \xrightarrow{\sim} Pic^0(E)$$
$$P \longmapsto [P - O]$$

Recall $\phi_* : Div E_1 \to Div E_2$.

$$\sum n_i P_i \longmapsto \sum n_i \phi(P_i)$$

This induces a map $Pic^0(E_1) \to Pic^0(E_2)$

(check ϕ(principal divisor) is principal)

So
$$\begin{array}{ccc} E_1(k) & \xrightarrow{\sim} & Pic^0(E_1) \\ \downarrow \phi & & \downarrow \phi_* \\ E_2(k) & \xrightarrow{\sim} & Pic^0(E_2) \end{array}$$

It commutes: $\phi_*([P-O]) = [\phi(P) - \phi(O)] = [\phi(P) - O]$. ∎

Define $\ker(\phi) = \phi^{-1}(O)$. It is a finite subgroup of $E_1(k)$ (if $\phi \neq [0]$)

Theorem 4.10 $\phi : E_1 \to E_2$ a non-constant isogeny over $k = \bar{k}$.

(a) (i) for all $Q \in E_2$, $\#\phi^{-1}(Q) = \deg_s \phi$.

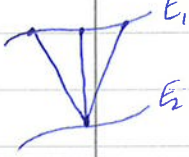
(ii) for all $P \in E_1$, $e_\phi(P) = \deg_i \phi$

(b) There is an isomorphism $\ker \phi \xrightarrow{\sim} \mathrm{Aut}(k(E_1)/\phi^* k(E_2))$

$$T \longmapsto T_T^*$$

(c) If ϕ is separable, then ϕ is unramified and $k(E_1)/\phi^* k(E_2)$ is Galois.

Proof: (a)(i) We already know this for almost all $Q \in E_2$.
Apply translation to show it holds for all $Q \in E_2$.



(ii) If $\phi(P) = \phi(P')$, let $R = P' - P$, so $\phi(R) = 0$.

We have $E_1 \xrightarrow{\tau_R} E_1$ ie. $\phi(P+R) = \phi(P)$ for all $P \in E_1$.

ϕ, ϕ : $E_1 \to E_2$

$$\Rightarrow e_\phi(P) = e_{\phi \circ \tau_R}(P) = e_\phi(\tau_R(P))\, e_{\tau_R}(P) = e_\phi(P') \cdot 1$$

(b) If $T \in \ker(\phi)$, then $E_1 \xrightarrow{\tau_T} E_1$

ϕ, ϕ : $E_1 \to E_2$

So on function fields, τ_T induces $\tau_T^* : k(E_1) \longrightarrow k(E_1)$, automorphism, restricts to id on $\phi^* k(E_2)$

i.e. $\tau_T^* \in \mathrm{Aut}\left(k(E_1)/\phi^* k(E_2)\right)$

The map $T \longmapsto \tau_T^*$ is a homomorphism

$$(\tau_{(T+T')} = \tau_T + \tau_{T'})$$

and it is injective $(T \neq 0 \Rightarrow \tau_T \neq 0)$.

Since $\#\mathrm{Aut}\left(k(E_1)/\phi^* k(E_2)\right) \leq \deg_s(\phi) \overset{(a)}{=} \#\ker(\phi)$.

$\therefore$ the map is an isomorphism.

(c) follows from (a) and (b). □

Corollary: $E_1 \xrightarrow[\text{sep}]{\phi} E_2$ with $\ker\phi \subset \ker\psi$

$\phi, \psi \to$ isogenies

$\psi : E_1 \to E_3$

then $\exists$ isogeny $\lambda : E_2 \longrightarrow E_3$ making the diagram commute.

Proof: $\ker(\phi)$ acts on $k(E_1)$, fixing $\psi^* k(E_3)$

$\longrightarrow$ field extensions

$$\begin{array}{ccc} k(E_1) & & \\ \cup & & \\ k(E_1)^{\ker\phi} & = & \phi^* k(E_2) \\ \cup & & \\ \psi^* k(E_3) & & \end{array}$$

This inclusion of fields makes λ.

□

Proposition 4.12 Let E be an elliptic curve over $k = \bar{k}$.
$\Phi \subset E$ a finite subgroup. Then there exists a separable isogeny $\phi : E \longrightarrow E'$ with $\ker(\phi) = \Phi$.

Proof Φ acts on $k(E)$ by translation as above.
$\rightarrow$ subfield $k(E)^{\Phi}$
which corresponds to a morphism of curves
$\phi : E \longrightarrow C$, with $k(C) \cong k(E)^{\Phi}$
ϕ is unramified: by construction, for $T \in \Phi$

$$\begin{array}{ccc} E & \xrightarrow{T} & E \\ & {\scriptstyle\phi}\searrow \quad \swarrow{\scriptstyle\phi} & \\ & C & \end{array}$$

so if $\phi(P) = Q$, then $\phi(P+T) = Q$ for all $T \in \Phi$
so $\#\phi^{-1}(Q) \geq \#T = \deg\phi$
Riemann-Hurwitz formula gives $g(C) = 1$. □

The invariant differential

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

$$\omega = \frac{dx}{2y + a_1x + a_3} \quad \text{satisfies } \operatorname{div}(\omega) = 0.$$

Since $\ell(K_E) = g(E) = 1$,
ω is up to scalar multiplication by $k^{\times}$ the unique regular differential on E.

Proposition 5.1: For $Q \in E$, $\tau_Q^*\omega = \omega$.

Proof $\operatorname{div}(\tau_Q^*\omega) = \tau_Q^*\operatorname{div}(\omega) = \tau_Q^*(0) = 0$.
So $\tau_Q^*\omega = a_Q\omega$ for some $a_Q \in k^{\times}$.
We want $a_Q = 1$. Idea: a_Q is a rational function of Q with no zeros or poles, so constant. Take $Q = O$ to see $a_Q = 1$ for all Q.
(why? $(P, Q) \longmapsto (P+Q, Q)$

$$\begin{array}{ccc} E \times E & \xrightarrow{\tau} & E \times E \\ (P,Q) \longmapsto Q \quad {\scriptstyle\pi_2}\downarrow & \nearrow_{\pi_2} & \text{acts as a } \tau_Q \text{ on } \pi_2^{-1}(Q) \cong E \\ E & & \end{array}$$

take $\bar{\omega} = \pi_1^* \omega$ ($= \omega$ on every fibre)

with $f = \pi_2^*$ (natural function on E)

$f(a) = a_a$ }.