Yesterday: $f \in k[x,y]$ an irreducible polynomial

$$C = V(f) = \{ p \subset \mathbb{A}^2_k : f(p) = 0 \} \qquad \tilde{f}(x_0,x_1,x_2) = x_0^{\deg(f)} f\left(\frac{x_1}{x_0}, \frac{x_2}{x_0}\right)$$

$$\tilde{C} = V_+(f) = \{ p \in \mathbb{P}^2_k : \tilde{f}(p) = 0 \}$$

$\tilde{C}$ ↑ closure of C in $\mathbb{P}^2_k$

Prop. Suppose that $\tilde{C}$ is smooth. For $0 \le i+j \le d-3$ $(d = \deg(f))$ the meromorphic differential form

$$\omega_{ij} = x^i y^j \frac{dx}{\partial f/\partial y}$$ has no poles if $d \ge 3$.

Moreover, if $d=3$, then $\mathrm{ord}_p(\omega) = 0 \ \ \forall p \in \tilde{C}$.

Cor: If $\tilde{C}$ is smooth and $\deg(f) \ge 3$ then the genus of $\tilde{C}$ is $\ge \frac{(d-1)(d-2)}{2}$ with equality if $d=3$.

Rmk: This is always an equality (but I won't show it).

Proof: For $p \in C$,

$$\Omega_{C,p} \otimes_{\mathcal{O}_{C,p}} k(p) = \frac{k(p)\,dx \oplus k(p)\,dy}{\left(\frac{\partial f}{\partial x}(p)\,dx + \frac{\partial f}{\partial y}(p)\,dy\right)}.$$

If $\frac{\partial f}{\partial y}(p) \neq 0$, then the differential form

$$\mathrm{ord}_p\left(\frac{dx}{\partial f/\partial y}\right) = 0. \quad \left(\text{it is non-zero in } \Omega_{C,p} \otimes k(p).\right)$$

$$\Longrightarrow \quad \mathrm{ord}_p\left(x^i y^j \frac{dx}{\partial f/\partial y}\right) \ge 0.$$

If $\frac{\partial f}{\partial y}(p) = 0$, then $\frac{\partial f}{\partial x}(p) \neq 0$. As a meromorphic differential form

$$\frac{dx}{\partial f/\partial y} = -\frac{dy}{\partial f/\partial x} \qquad \Omega_{K(C)/k} = \frac{K(C)\,dx \oplus K(C)\,dy}{\left(\frac{\partial f}{\partial x}dx + \frac{\partial f}{\partial y}dy\right)}$$

By the same argument we see that

$$\omega_{00} = -\frac{dy}{\partial f/\partial x} \quad \Rightarrow \quad \mathrm{ord}_p(\omega_{00}) = \mathrm{ord}_p\left(\frac{dy}{\partial f/\partial x}\right) = 0.$$

$\mathrm{ord}_p(\quad) \quad \mathrm{ord}_p(x^i y^j \omega_{00}) \ge 0$

$\Longrightarrow \quad \mathrm{ord}_p(\omega_{ij}) = \mathrm{ord}_p(x^i y^j \omega) \geq 0.$

Look at the infinity. Up to renumbering variable, we may assume $p \in D_+(x_2)$

$$u = \frac{x}{y}$$

$$v = \frac{1}{y} \qquad dv = -\frac{dy}{y^2} \qquad dy = -\frac{dv}{v^2}.$$

The equation of $\tilde{C} \cap D_+(x_2)$ is

$$g(u,v) = v^d f\left(\frac{u}{v}, \frac{1}{v}\right)$$

$$\frac{\partial g}{\partial u} = v^d \frac{\partial f}{\partial x}\left(\frac{u}{v}, \frac{1}{v}\right) \cdot \frac{1}{v} = v^{d-1} \frac{\partial f}{\partial x}\left(\frac{u}{v}, \frac{1}{v}\right).$$

$$\omega_\infty = -\frac{dy}{\partial f/\partial x} = -\frac{dv}{v^2} \cdot \frac{v^{d-1}}{\partial g/\partial u} = -v^{d-3} \frac{dv}{\partial g/\partial u}.$$

If $\frac{\partial g}{\partial u}(p) \neq 0$, then the same argument shows

$$\mathrm{ord}_p(\omega_\infty) \geq 0 \quad \text{and it is } 0 \text{ if } d=3.$$

$$\omega_{ij} = -\left(\frac{u}{v}\right)^i \left(\frac{1}{v}\right)^j v^{d-3} \frac{dv}{\partial g/\partial u} = -u^i v^{d-3-i-j} \frac{dv}{\partial g/\partial u}$$

$$\mathrm{ord}_p(\omega_{ij}) \geq 0 \qquad \text{if} \qquad i+j \leq d-3.$$

If $\frac{\partial g}{\partial u}(p) = 0$, then $\frac{\partial g}{\partial v}(p) \neq 0$ and

$$\omega_\infty = -v^{d-3} \frac{dv}{\partial g/\partial u} = v^{d-3} \frac{du}{\partial g/\partial v}$$

$$\uparrow$$

$$\frac{\partial g}{\partial u} du + \frac{\partial g}{\partial v} dv = 0$$

The same argument shows: $\mathrm{ord}_p(\omega_\infty) \geq 0$ and it is 0 if $d=3$.

for $i+j \leq d-3 \qquad \mathrm{ord}_p(\omega_{ij}) \geq 0.$

Def. An elliptic curve (over k) is the datum of a smooth proj. curve E, of genus 1, together with a k-rational point $e \in E(k)$.

This is equivalent to giving: a projective plane curve $E \subset \mathbb{P}^2_k$ of degree 3

1) a smooth plane curve [illegible] together a k-rational point

or

2) a smooth projective plane curve $E \subseteq \mathbb{P}^2$ with Weierstrass equation

$$y^2 + b_1 xy + b_2 y = a_3 x^3 + a_2 x^2 + a_1 x + a_0 \qquad (a_3 \neq 0)$$

and $e = [0:0:1]$.

Group Law on an elliptic curve

Fix $E = V_+(f) \subseteq \mathbb{P}^2_k$ a smooth projective plane curve of genus 1 and with a k-rational point $e \in E(k)$.

$P, Q \in E(k)$ $\qquad L_{PQ} = \begin{cases} \text{the unique passing through } P,Q & \text{if } P \neq Q \\ \text{the tangent line at } E \text{ in } P. & \text{if } P = Q \end{cases}$

Let $C = V_+(g) \subseteq \mathbb{P}^2_k$ a smooth projective plane curve.

Let $\varphi \in k[x_0, x_1, x_2]$ homogeneous polynomial of degree d.

$P \in C$ $\qquad \operatorname{ord}_P(\varphi) = \operatorname{ord}_P\left(\frac{\varphi}{x_i^d}\right)$ with $P \in D_+(x_i) \cap C$

↖ does not depend on the chosen i.

If $C \not\subseteq V_+(\varphi)$, then

$$0 \leq \operatorname{div}(\varphi) = \sum_{P \in C} \operatorname{ord}_P(\varphi)\,[P] \in \operatorname{Div}(X).$$

Rmk: (Stupid Bezout) If $\deg \varphi = 1$, so $\{\varphi = 0\}$ is a line in $\mathbb{P}^2$, then $\deg(\operatorname{div}(\varphi)) = \deg(g)$

$\{\varphi = 0\} \cap k^8 = \langle v, w \rangle$ $\qquad a(\lambda, \mu) = g(\lambda v + \mu w)$

↑ homogeneous polynomial of degree $\deg(g)$ and two variables.

$$a(\lambda, \mu) = \prod_{i=0}^{\delta} h_i^{m_i}$$

h_i monic irreducible, $h_i \neq h_j$ for $i \neq j$.

and $\sum_{i=0}^{\delta} m_i \deg(h_i) = \deg(g)$

Lemma (Stupid Bezout) The line $\{\varphi = 0\}$ meets the curve C in exactly $\deg(\varphi)$ points counted with multiplicity and $\cong \mathbb{P}^1_k$

$$\mathrm{div}_C(\varphi) = \sum_{i=0}^{\delta} m_i [x_i] \qquad x_i \in \{\varphi = 0\} \cap C$$

$$\deg(m_i) = \deg(x_i)$$

is the point corresponding to the irreducible polynomial h

In otherwords, for $p, q \in E(k)$, L_{pq} is the unique line s.t.

$$\mathrm{div}_E(\varphi_{pq}) - [p] - [q] \quad \text{is effective.}$$

(φ_{pq}: equation for L_{pq})

$$\mathrm{div}_E(\varphi_{pq}) = [p] + [q] + [p*q]$$

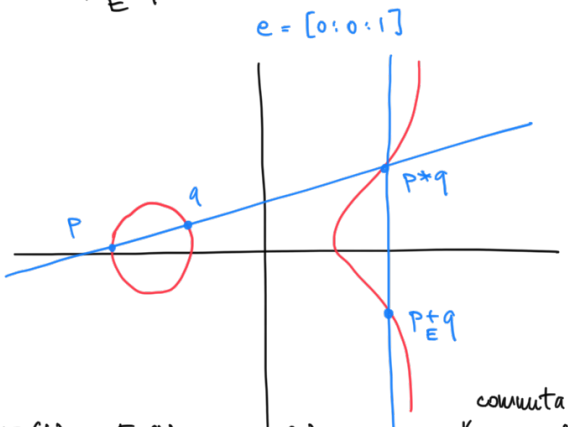
($[p*q]$: definition of $p*q$)

Def: $p*q$ is the "third" point of intersection of L_{pq} with E.

($p*q \in E(k)$)

Def: For $p, q \in E(k)$, define

$$p \overset{+}{_E} q := (p*q) * e$$



Th: The map $E(k) \times E(k) \to E(k)$ is a commutative group law with

$$(p, q) \mapsto p \overset{+}{_E} q$$

identity e and inverse $p \mapsto p * (e*e)$

Rmk: If e is an inflexion point (i.e. $e*e = e$), then the inverse is $p \mapsto p*e$.

Proof: • $p \overset{+}{_E} q = (p*q) * e = (q*p) * e = q \overset{+}{_E} p.$

($p*q = q*p$)

($L_{p*e,\, e}$)

- (identity) : $P \overset{+}{_E} e = (P * e) * \cdots$

$L_{p,e} = L_{p*e,e}$

$p*e$ is the "third" in $L_{p,e} \cap E$, so p is the third of $L_{p*e,e} \cap E$.

- (inverse) $P \overset{+}{_E} \big(p * (e*e) \big) = \Big(p * \big(\underbrace{p * (e*e)}_{L_{p,\, e*e}} \big) \Big) * e$

$L_{p,\, p*(e*e)} = L_{p,\, e*e}$

$= (e*e) * e = e.$

- (associative) $p, q, r \in E(k)$. It suffices to show :

$$(p \overset{+}{_E} q) * r = p * (q \overset{+}{_E} r)$$

$L = L_{p,q}$: p q $p*q$ $\lambda = 0$

$M = L_{p*q,e}$: $p*q$ e $p+q$ $\mu = 0$

$N = L_{p+q,r}$: $p+q$ r $(p+q)*r$ $\nu = 0$

$L' = L_{qr}$: q r $q*r$ $\lambda' = 0$

$M' = L_{q*r,e}$: $q*r$ e $q+r$ $\mu' = 0$

$N' = L_{q+r,p}$: $q+r$ p $p*(q+r)$

Let f be the equation of the curve E.

$$g := \lambda \mu' \nu$$

Consider the k-vector space V generated by f and g $\subseteq k[x_0, x_1, x_2]$

$$V = \{ \alpha f + \beta g : \alpha, \beta \in k \} \qquad \dim V = 2.$$

I want to show that $h = \lambda' \mu \nu'$ belongs to V. If so,

$$\operatorname{div}_E(h) \geq [p] + [q] + [p*q] + [q*r] + [e] + [q+r] + [p+q] + [r] + [(p+q)*r].$$

$\| \quad \| \quad \| \quad \| \quad \| \quad \| \quad \| \quad \| \quad \|$

$\operatorname{div}_E(\lambda') + \operatorname{div}_E(\mu) + \operatorname{div}_E(\nu')$

$\|$ stupid Bezout

$[q] + [r] + [q*r] + [p*q] + [e] + [p+q] + [p+(q+r)] + [p] + [(p+q)*r]$

$\Longrightarrow \quad p * (q+r) = (p+q) * r.$

Suppose $|k| \geq 2$, so $\# \mathbb{P}^1(k) \geq 3$. Pick $t \in L'(k) \setminus \{ q, r, q*r \}$.

Since $t \notin E$, the vector space

$$W = \{ \psi \in V : \psi(t) = 0 \} \subseteq V$$

is of dimension 1. Up to scalar scalar factor there is a unique $\psi \in V$ s.t. $\psi(t) = 0$.

Claim: $\psi = h$ (up to scalar factor).

Indeed

$$\mathrm{div}_{L'}(f) = [q] + [r] + [q*r]$$

$$\mathrm{div}_{L'}(g) \geq [q] + [r] + [q*r]$$

$$\Longrightarrow \quad \mathrm{div}_{L'}(\psi) \geq [q] + [r] + [q*r] + [t]$$

$$4 \leq \deg(\mathrm{div}_{L'}(\psi)) = \deg \psi = 3$$

(stupid Bezout)

if $L' \notin V_+(\psi) \Longrightarrow L' \subseteq V_+(\psi)$

This means that λ' divides ψ.

Let $\psi' = \frac{\psi}{\lambda'}$: it is homogeneous polynomial of degree 2

$$\mathrm{div}_M(\psi') \geq [p*q] + [e] + [p+q]$$

$$\Longrightarrow \quad M \subseteq V_+(\psi') \Rightarrow \mu \text{ divides } \psi'$$

(stupid Bezout)

Set $\psi'' = \frac{\psi'}{\mu}$: it is homogeneous polynomial of degree 1.

$$\mathrm{div}_{N'}(\psi'') \geq [p] + [q+r]$$

$$\Longrightarrow \quad N' \subseteq V_+(\psi'') \Longrightarrow \nu' \text{ divides } \psi''$$

(stupid Bezout)

$\nu' = \psi''$. scalar factor.

$$\Longrightarrow \quad h = \psi \text{ up to scalar factor.} \qquad \square$$

Rmk: (E, e) elliptic curve

$$i_{3[e]} : E \longrightarrow \mathbb{P}(H^0(3[e])^*).$$

$k=\bar{k}$ $\qquad e \longmapsto H_e = \{\varphi \in H^0(3[e]) : \operatorname{ord}_e(\varphi) > -3\}$

$\qquad\qquad\qquad\qquad\qquad\qquad\quad = H^0(2[e])$

In other words, if $f \in H^0(2[e]) \setminus H^0([e])$

$$g \in H^0(3[e]) \setminus H^0(2[e])$$

$$\begin{array}{ccc} k^3 & \longrightarrow & H^0(3[e]) \\ (x_0, x_1, x_2) & \longmapsto & x_0 + x_1 f + x_2 g \end{array}$$

$i_{3[e]}(e)$ is the hyperplane in k^3 generated by $1, f$.

so it is the linear form e_2^*

$$k^3 \longrightarrow H^0(3[e]) \longrightarrow k$$

$$(x_0, x_1, x_2) \longmapsto x_0 + x_1 f + x_2 g \longmapsto x_2.$$

$e_0, e_1, e_2 \in k^3$ canonical basis

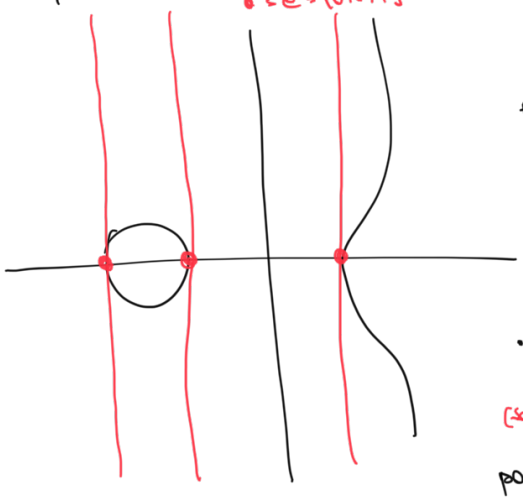
$e_0^*, e_1^*, e_2^* \in (k^3)^*$ dual basis

In $\mathbb{P}((k^3)^*)$ the point $i_{3[e]}(e)$ is $[e_2^*] = [0:0:1]$.

Example: look for 2-torsion points. Suppose $\operatorname{char}(k) \neq 2$ and $k = \bar{k}$.

$x \in E$ s.t. $x + x = 0_E$. Suppose we have a Weierstrass equation of the form

$$y^2 = a_3x^3 + a_2x^2 + a_1x + a_0 = q(x)$$



$P \underset{E}{+} P = e$ is equivalent to saying that

(*) $P * P = e$ (here we use that e is a flex, $e*e = e$).

- $e \underset{E}{+} e = e$

(*) says that the third point on the tangent at P is the point at infinity.

In other words, the tangent at P is vertical, i.e. $\frac{\partial f}{\partial y}(P) = 0$. where f is the equation of the curve

For the 2-torsion points

$\frac{\partial f}{\partial y} = 2y$. There [illegible]

are the points of intersection of E with $\{y=0\}$ and e.

$$\begin{cases} y^2 = q(x) \\ y = 0 \end{cases} \Rightarrow \begin{cases} q(x)=0 \\ y=0 \end{cases}$$

q is of degree 3

Since E is smooth, it has 3 distinct roots

There are exactly 4 points of 2-torsion (if $\mathrm{char}(k) \neq 2$, and $k=\bar{k}$).

. If k is not alg closed, then q may not have all its zeroes in k.

. If $\mathrm{char}(k)=2$,

$$E[2](k) = \{ x \in E : x+x=e \}$$

$$\Rightarrow \quad \# E[2](k) \leq 2.$$

Thm: Let $E \subseteq \mathbb{P}^2$ be a smooth proj. plane curve of deg 3 and $e \in E(k)$.

$$\mathrm{Div}^0(E) = \{ \text{divisors of degree 0 on } E \}$$

$$\| \text{or}$$

$$\{ \mathrm{div}(f) : f \in K(E)^* = K(E) \setminus \{0\} \} \leftarrow \text{this is a subgroup}$$

$$\mathrm{Pic}^0(E) = \mathrm{Div}^0(E) \Big/ \{ \mathrm{div}(f) : f \in K(E)^* \}.$$

The map $E(k) \longrightarrow \mathrm{Pic}^0(E)$ is an isomorphism of groups.

$$x \longmapsto [x] - [e]$$

In particular, it does not depend on the chosen embedding.

Proof: L_{pq} = line passing through p, q as before

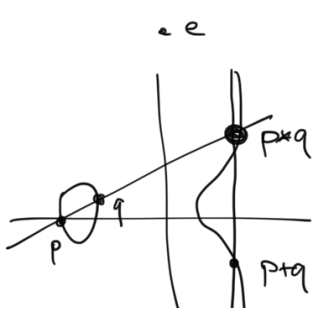
φ_{pq} = equation for $L_{p,q}$.

We have to show that the divisor

$$[p] - [e] + [q] - [e] - \left([p+q] - [e] \right)$$

is the divisor of some $f \in K(E)$.

$$\mathrm{div}\left(\frac{\varphi_{p,q}}{\varphi_{p+q,e}} \right) = \mathrm{div}\left(\frac{\varphi_{p,q}}{\varphi_{e,e}} \cdot \frac{\varphi_{e,e}}{\varphi_{p+q,e}} \right)$$



$[p] + [q] + [\cancel{p+q}] - 2[e] - [\cancel{e+e}]$

$= [p] + [q] + \cancel{[p*q]} \cdots$

$+ [e] + \cancel{[e]} + \cancel{[e*e]} - \cancel{[p*q]} - \cancel{[e]} - [p+q].$

$= \big([p] - [e]\big) + \big([q] - [e]\big) - \big([p+q] - [e]\big).$

(Injective) : Suppose $[p] - [e] = \mathrm{div}(f)$. Then

$f \in H^0([e]) = k \Rightarrow f$ is constant $\Longrightarrow \mathrm{div}(f) = 0.$

$\longrightarrow p = e.$

(Surjective) Let $D \in \mathrm{Div}^0(E)$ be a divisor of degree 0.

$D + [e]$ is a divisor of degree 1 on E

$\underset{RR}{\Longrightarrow} H^0(D + [e]) = kf.$

$\mathrm{div}(f) + D + [e] \geq 0$ is effective and of degree 1

$\Longrightarrow \exists\, x \in E(k)$ s.t. $[x] = \mathrm{div}(f) + D + [e]$

$\Longrightarrow \big([x] - [e]\big) - D = \mathrm{div}(f).$ $\square$