I Isomorphisms of elliptic curves

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

be an elliptic curve given by a long Weierstrass equation.

A linear isomorphism is an isomorphism $\phi: E \to E'$ given by an affine change of coordinates where E' is still given by a long Weierstrass equation

they are of the form $(x,y) \mapsto (u^2 x + r,\ u^3 y + s x + t)$

prop: if $\mathrm{char}\, k > 3$, there is a linear isomorphism $\phi: E \to E'$ where

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

is a short Weierstrass equation

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

$$\begin{cases} y = y' - \frac{a_1}{2} x - \frac{a_3}{2} \\ x = x' \end{cases} \quad \leftarrow \mathrm{char}\, k \neq 2$$

$$\Rightarrow \left(y' - \frac{a_1}{2} x - \frac{a_3}{2}\right)^2 + a_1 x \left(y' - \frac{a_1}{2} x - \frac{a_3}{2}\right) + a_3 \left(y' - \frac{a_1}{2} x - \frac{a_3}{2}\right) = \dots$$

$$\Leftrightarrow y'^2 - a_1 x y' - a_3 y' + a_1 x y' + a_3 y' + \dots x = \dots$$

$$\Leftrightarrow y'^2 = x^3 + a_2' x^2 + a_4' x + a_6'$$

$$x = x' - \frac{a_2'}{3}$$

$$\Rightarrow y^2 = \left(x' - \frac{a_2}{3}\right)^3 + a_2' \left(x' - \frac{a_2}{3}\right)^2 + a_4' \left(x' - \frac{a_2}{3}\right) + a_6' + \dots x + \dots$$

$$\Leftrightarrow y^2 = x'^3 + a_4'' x + a_6''$$ ∎

remark: linear isomorphisms preserving short Weierstrass equations are of the form

$$(x, y) \longmapsto (u^2 x, u^3 y) \qquad u \neq 0$$

corollary: (a, b) and $(u^4 a, u^6 b)$ correspond to isomorphic curves

definition: $$j(E: y^2 = x^3 + ax + b) = 1728 \frac{4a^3}{4a^3 + 27b^2}$$

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

theorem: 1) $j(E) = j(E') \iff E$ and E' are isomorphic over $\bar{k}$

2) for any $j \in k$, there is a E/k with $j(E) = j$

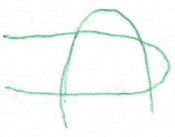
so $j(E)$ fully determines the isomorphism class of E (over $\bar{k}$)

VI Addition law

theorem (Bezout): let φ and φ' be two irreductible projective plane curves of degree d and d' respectively

then if $\varphi \neq \varphi'$ over $\bar{k}$, $\#(\varphi \cap \varphi') = dd'$ (counting multiplicity)

example:



2 curves of degree 2

4 points of intersection

corollary: let E be an elliptic curve and L any line.

then $E \cap L = \{P_1, P_2, P_3\}$ over $\bar{k}$ (possibly with multiplicity)

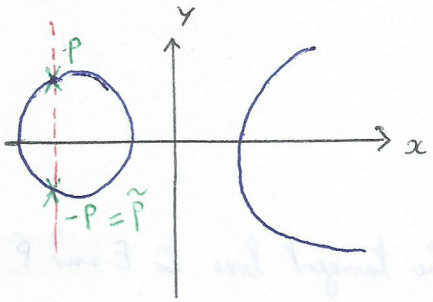
definition: $P_1 + P_2 + P_3 = O_E$

lemma 1: O is $(0:1:0)$ the point at infinity O_E

proof: take L the tangent line at O_E. We saw that L is $z=0$, the line at infinity. So $L \cap E = \{O_E, O_E, O_E\}$, so $O_E + O_E + O_E = O$

So O_E is a point of 3-torsion. We admit that in fact $O_E = O$ ∎

lemma 2: if $P = (x;y)$ then $-P = (x;-y)$



proof: let $L = v_P$ the vertical line going through P

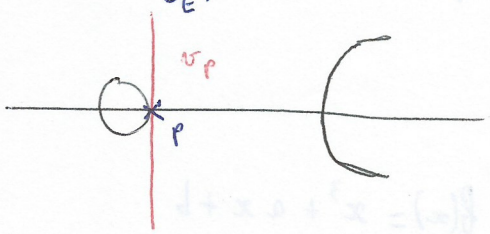
$v_P = " x = x_P "$

$v_P \cap E = \{P, \tilde{P}, O_E\}$

$P + \tilde{P} + O_E = O_E \Rightarrow \tilde{P} = -P$ ∎

remark: $P = -P \iff y_P = 0 \iff 2P = O$

we say that P is a Weierstrass point. Indeed in this case x_P is a root of the Weierstrass equation $y^2 = x^3 + ax + b$



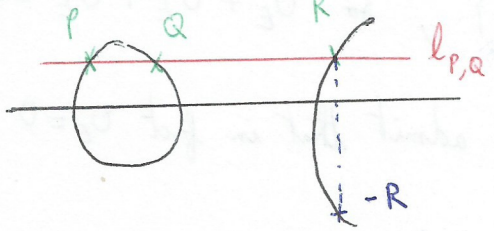
in this case, v_P is tangent to E at P

lemma 3: let $P, Q \in E(k)$ $\quad P, Q \neq \mathcal{O}_E$

a) if $P = -Q$, $P + Q = \mathcal{O}_E$

otherwise

b) if $P \neq Q$, Let $L = \ell_{P,Q}$ the line going through P and Q

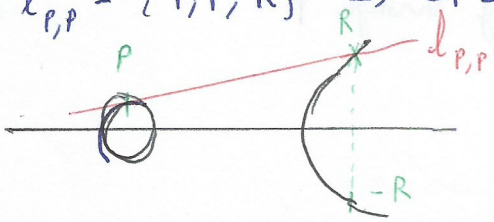


$$\ell_{P,Q} \cap E = \{P, Q, R\}$$

$$P + Q + R = \mathcal{O}_E$$
$$\Rightarrow P + Q = -R$$

c) if $P = Q$ then we take $\ell_{P,P}$ = the tangent line to E at P

$$E \cap \ell_{P,P} = \{P, P, R\} \Rightarrow 2P = -R$$



remark: $\ell_{P,Q} = \ell_{Q,P}$ so + is commutative

formula: * $-P = (x_P ; -Y_P)$

* $\ell_{P,Q}$: $Y - Y_P = \alpha (x - x_P)$

where α is the slope $\alpha = \dfrac{Y_Q - Y_P}{x_Q - x_P}$

* $\ell_{P,P}$: $Y - Y_P = \alpha (x - x_P)$

where $\alpha = \dfrac{f'(x_P)}{2 Y_P}$ with $f(x) = x^3 + a x + b$

$y^2 = f(x)$

$2 y_P (y - y_P) = f'(x)(x - x_P)$

I have a line $y = \alpha x + \beta$ that intersects E at P and Q (where $Q = P$ in case (C))

I want to compute the third point of intersection

$$(\alpha x + \beta)^2 = f(x) = x^3 + a x + b$$

$$\Rightarrow x^3 - \alpha^2 x^2 - 2\alpha x - \beta^2 + a x + b = 0$$

but we know that $x_P + x_Q + x_R = - - \alpha^2 = \alpha^2$

$$\begin{cases} x_R = \alpha^2 - x_P - x_Q \\ y_R - y_P = \alpha (x_R - x_P) \end{cases}$$

$$\Rightarrow P + Q = - R = (x_R ; - y_R)$$

VII Elliptic curves over finite fields

if $E/_{\mathbb{F}_q}$ is an elliptic curve over $\mathbb{F}_q$, then $E(\mathbb{F}_q)$ is a finite abelian group

definition : $E/_k$ $E[n]$ the group of n-torsion : $\{ P \in E(\bar{k}),\ nP = O_E \}$

remark : we saw that $E[2] = \{ O_E \} \cup \{$ the 3 Weierstrass points $\}$
$= (x_\alpha, 0), (x_\beta, 0), (x_\gamma, 0)$

where $x_\alpha, x_\beta, x_\gamma$ are the 3 roots of $f(x) = 0$
distincts

prop: if $\mathrm{char}\, k \nmid n$ (or $\mathrm{char}\, k = 0$)

$$E[n](\bar{k}) \simeq \left(\mathbb{Z}/n\mathbb{Z}\right)^2$$

in general, $\#E[n](\bar{k}) \leq n^2$

corolary: if $k = \mathbb{F}_q$, $E(\mathbb{F}_q) \simeq \mathbb{Z}/d_1\mathbb{Z} \times \mathbb{Z}/d_2\mathbb{Z}$

with $d_1 \mid d_2$ and $d_1 \mid q-1$ and $d_1 d_2 = \#E(\mathbb{F}_q)$ (note we may have $d_2 = 1$)

proof: we have $E(\mathbb{F}_q) \simeq \mathbb{Z}/d_1\mathbb{Z} \times \dots \times \mathbb{Z}/d_k\mathbb{Z}$ $\quad d_1 \mid d_2 \mid \dots \mid d_k$

with $d_1 \neq 1$

then $\#E[d_1](\mathbb{F}_q) = d_1^k > d_1^2 \Rightarrow$ contradiction ▨

prop: if $q = p^m$, $E/\mathbb{F}_q$

either $E[p](\bar{\mathbb{F}}_q) \simeq \left(\mathbb{Z}/p\mathbb{Z}\right)$ in which case E is ordinary and

$$E[p^n](\bar{\mathbb{F}}_q) \simeq \mathbb{Z}/p^n\mathbb{Z}$$

or $E[p](\bar{\mathbb{F}}_q) \simeq 0$ in which case E is supersingular

and $E[p^n](\bar{\mathbb{F}}_q) \simeq 0$

number of points

$E/\mathbb{F}_q$, $\quad y^2 = f(x) = x^3 + ax + b$

$$\#E(\mathbb{F}_q) = \underset{\{O_E\}}{1} + \#\left\{(x,y) \in \mathbb{F}_q,\ y^2 = x^3 + ax + b\right\}$$

if $x \in \mathbb{F}_q$

- if $x^3 + ax + b$ is a square, $y^2 \neq 0$ in $\mathbb{F}_q$

  we have two points (x,y) and $(x,-y)$ in $E(\mathbb{F}_q)$

- if $x^3 + ax + b = 0$
  we have one point $(x, 0)$ in $E(\mathbb{F}_q)$

- if $x^3 + ax + b$ is not a square in $\mathbb{F}_q$
  we have no point

if $q = p$, $\mathbb{F}_q = \mathbb{Z}/p\mathbb{Z}$

recall the Jacobi symbol

$$\left(\frac{x}{p}\right) = \begin{cases} 1 & \text{if } x \text{ is a square mod } p \\ 0 & \text{if } x = 0 \bmod p \\ -1 & \text{if } x \text{ is not a square mod } p \end{cases}$$

$$\#E(\mathbb{F}_q) = 1 + \sum_{x \in \mathbb{F}_q} \left[1 + \left(\frac{x^3 + ax + b}{p}\right)\right]$$

prop: there are exactly $\frac{q-1}{2}$ squares in $\mathbb{F}_q^*$

proof: $\mathbb{F}_q^*$ is cyclic

heuristic: for a "random x", the probability that $x^3 + ax + b$ is a square is $\frac{1}{2}$

so the esperance of the number of points above x is $2 \times \frac{1}{2} = 1$

so we expect $\#E(\mathbb{F}_q) \simeq 1 + q$

theorem (Hasse - Weil): $|\#E(\mathbb{F}_q) - 1 - q| \leq 2\sqrt{q}$

definition: $\pi : E \longrightarrow E$ the Frobenius
$P \longmapsto \pi(P) = (x_P^q, y_P^q)$

recall that if $x \in \overline{\mathbb{F}_q}$, $\pi(x) = x^q$

if $P \in E(\bar{\mathbb{F}}_q)$, $P \in E(\mathbb{F}_q) \Leftrightarrow \pi(P) = P$

$E(\mathbb{F}_q) = \mathrm{Ker}(\pi - 1)$

but π has a characteristic polynomial : $X_\pi = X^2 - tX + q$

where $t = \pi + \bar{\pi}$ is the trace of the Frobenius

and Hasse-Weil proved that $|t| \leq 2\sqrt{q}$

and so $\#E(\mathbb{F}_q) = \deg(\pi - 1) = X_\pi(1) = 1 - t + q$

so $\#E(\mathbb{F}_q) - 1 - q = -t$