Haessig Elliptic Curves

Note Title 9/25/2009

1. Cubic plane curves defined by

$$ax^3 + bx^2y + \cdots + hx + iy + k = 0$$

Change of coordinates over $\mathbb{Z}[\frac{1}{6}]$

$$\rightsquigarrow y^2 = x^3 + Ax^2 + Bx + C = f(x)$$

or $y^2 = 4x^2 - g_2x - g_3$ WEIERSTRASS NORMAL FORM

The coordinate change is rational rather than linear.

This curve is elliptic if it is nonsingular.

$F(x,y) = y^2 - f(x)$.

$\frac{dy}{dx} = \frac{\partial F/\partial x}{\partial F/\partial y}$

Nonsingularity requires $(F_x, F_y) \neq (0,0)$ at any point on C.

$\frac{\partial F}{\partial x} = -f'(x)$, $\frac{\partial F}{\partial y} = -2y$

$F_y = 0 \Rightarrow f(x) = 0$

We get a singular pt $\Leftrightarrow$ $f(x)$ and $f'(x)$ have common root, i.e. $f(x)$ has a double root.

e.g. Legendre family

$$y^2 = x(x-1)(x-\lambda) \qquad \lambda \neq 0, 1$$

Discriminant

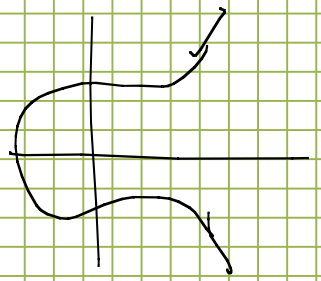
If $f(x) = (x-\alpha_1)(x-\alpha_2)(x-\alpha_3)$

$$D = (\alpha_1-\alpha_2)^2(\alpha_2-\alpha_3)^2(\alpha_1-\alpha_3)^2$$

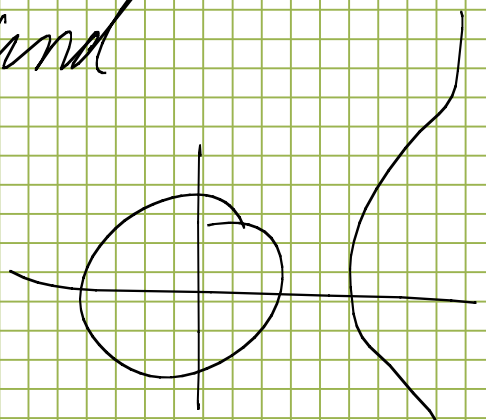
Then curve is nonsing $\iff D \neq 0$.

D is a fn of A, B, C.

Assume $K = \mathbb{R}$ and

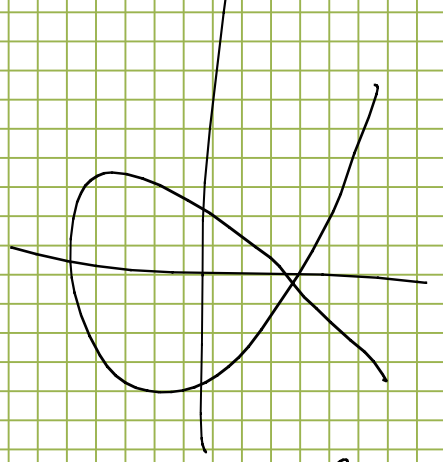


$f(x)$ has one real root



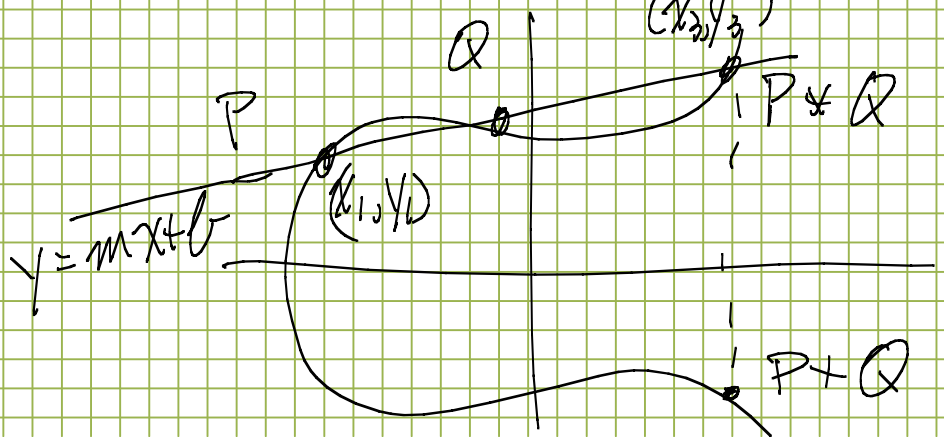
3 real roots

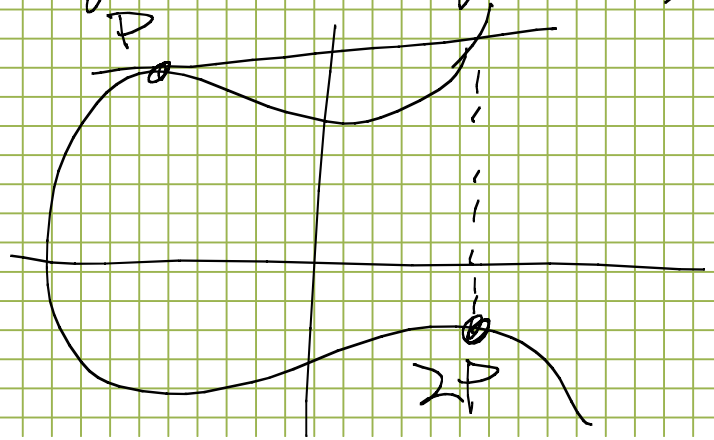
NOT ELLIPTIC



singular case

II The group law (not formal yet)





For $E(K): y^2 = x^3 + Ax^2 + Bx + C$,

$P = (x_1, y_1)$ $\quad Q = (x_2, y_2)$

$P * Q = (m^2 - A - x_1 - x_2,\ m x_3 + b) = (x_3, y_3)$

x_3 = rational fn of x_1, x_2, A, B, C

$P + Q = (m^2 - A - x_1 - x_2,\ -y_3)$

Thm. (skipping 2 sections) The f.g.l.

Let E be an elliptic curve over a complete local field K, s.t. $K = \mathbb{Q}_p$.

$E \rightsquigarrow F(Z_1, Z_2)$ $\quad |y| = 3,\ |x| = 2,\ |a_i| = 1$

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

Let $x = \frac{z}{w}$, $y = -\frac{1}{w}$, $\left(z = -\frac{x}{y}\right)$ Why?

$|z| = -1$
$|w| = -3$

$$w = z^3 + a_1 z w + a_2 z^2 w + a_3 w^2 + a_4 w^2 z + a_6 w^6$$

$$\rightsquigarrow$$

$$w = z^3 + a_1 z^4 + (a_1^2 + a_2) z^5 + \cdots$$

$$\in \mathbb{Z}[a_1, \cdots a_6][[z]]$$

$$x = z^{-2} - a_1 z^{-1} - a_2 - a_3 z + \cdots$$
$$y = -z^{-3} + a_1 z^{-2} + a_2 z^{-1} + a_3 + \cdots$$

} Formal solution

If E is defined over K

R = ring of integers

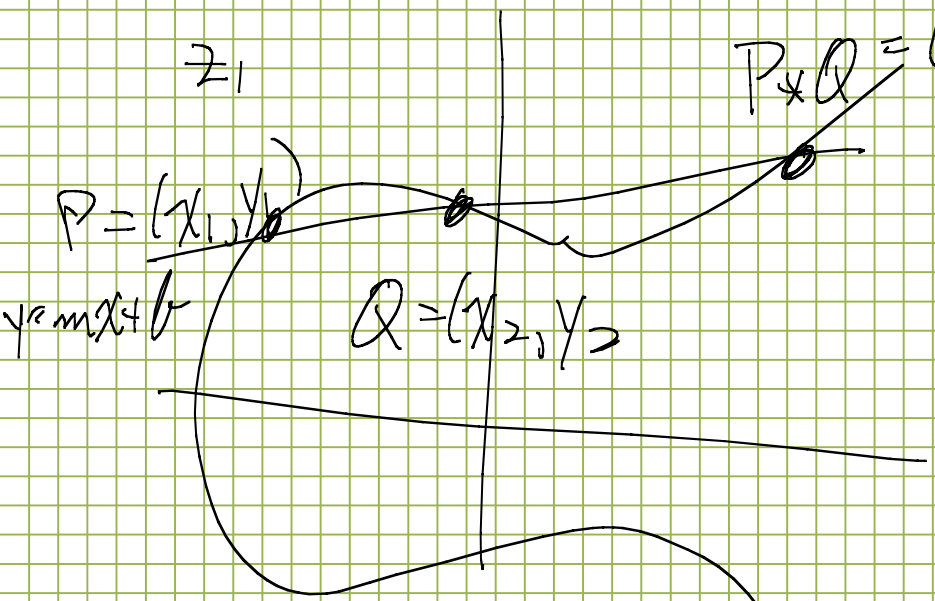
M = maximal ideal

If $z \in M$, then the power series of above converge. We get a map

$$M \longrightarrow E(K) = K\text{-valued points of } E$$

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

$z_i = x_i / y_i$



Want $\tilde{z}_3$ as $F(z_1, z_2)$

When $a_1 = a_3 = 0$, $\tilde{z}_3 = z_3$.

$$P + Q = \left(m^2 - A - x_1 - x_2, -(m x_3 + b)\right)$$

We get

$$\tilde{z}_3 = z_1 + z_2 - a_1 z_1 z_2 - a_2 (z_1^2 z_2 + z_1 z_2^2) \ldots$$