Recall .0.1

If k is a field of characteristic zero then the elliptic curve $\mathcal{E} \subseteq \overline{k}^2$ is the solutions to

$$E(x,y) = y^2 - 4x^3 + g_2x + g_3,$$

where $\Delta = g_2^3 - 27g_3^2 \neq 0$ (aka the curve is nonsingular, aka not all formal partial derivatives vanish at some P).

Why do we require that if $(x,y) \in \mathcal{E}$ with $D_1E(x,y) = 0$, $D_2E(x,y) = 0$. $D_2E(x,y) = 2y$, so if this is zero $y = 0$.

Factor $y^2 = 4(x-x_1)(x-x_2)(x-x_3)$. Then $E(x,y) = 0$ when $x = x_1, x_2, x_3$ since $y = 0$, but then this gives that $D_1E(x,y)$ vanishing implies there is a non-distinct root, so then $\Delta = 0$. The converse is similar.

Note: from our discussion last time, if a tangent line through P goes through ∞, then P is a 2-torsion point since $P + P + \infty = \infty$, $P = -P$. If the coefficients lie in some field k then we can write down the equation of the addition in this group structure as rational functions with coefficients in k.

Remark .0.1

We can think of an ellitpic curve $E[x,y] = \mathcal{E}$ as a functor from k-algebras to groups

$$\mathcal{E} : R \mapsto \mathcal{E}(R) \subseteq R \times R.$$

Torsion! We will have that $E[N] \coloneqq \mathcal{E}(\overline{k})[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$, where $\mathcal{E}(L)[N] = \{x \in \mathcal{E}(L) \mid Nx = \infty\}$. Last time, we saw that if L/K is Galois then $\mathrm{Gal}(L/k)$ acts on $\mathcal{E}(L)$, and this gives an action on N-torsion as $\mathrm{Gal}(L/k)$ acting on $\mathcal{E}(L)[N]$:

$$\rho : \mathrm{Gal}(L/k) \to \mathrm{GL}_2(\mathbb{Z}/N\mathbb{Z}).$$

To see that $E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$

.1. Algebraic Curves and Function Fields

Let $I = \langle \varphi_1, \dots, \varphi_r \rangle \subseteq \overline{k}[x_1, \dots, x_n]$. Now consider

$$V \coloneqq \{p \in \overline{k}^n \mid \varphi(p) = 0 \text{ for all } \varphi \in I\},$$

We then know that I is prime, so the coordinate ring $\overline{k}[V] = \overline{k}[x_1, \dots, x_n]/I$ is an integral domain, and we can consider its field of fractions $\overline{k}(V)$. If $\overline{k}(V)$ is a finite dimensional extension of $\overline{k}(t)$, then we say V is an affine algebraic curve.

If $[D_j\varphi_i(p)]$ is rank $n-1$ for each $p \in V$, then we say that V is nonsingular. This is nice, but we really want to homogenize. Say if φ_1 was $x_1 + x_2^2$ we would take it to $x_0x_1 + x_2^2$. Under this replacement if V' is the corresponding subset of $\overline{k}^{n+1}$ then $x \in V'$ implies $\lambda x \in V'$ for any $\lambda \in \overline{k}$.

We would then define $\mathbb{P}^r(\overline{k})$ to be the quotient of $\overline{k}^{r+1}$ by the action of scaling by an element of $\overline{k}$. This is projective r-space over $\overline{k}$. We can then consider

$$I_{\mathrm{hom}} = \langle \varphi_{i,\mathrm{hom}} \rangle \subseteq \overline{k}[x_0, \dots, x_r]$$
$$V_{\mathrm{hom}} = \{\underbrace{[p_0 : \cdots : p_r]}_{p} \in \mathbb{P}^r(\overline{k}) \mid \varphi(p) = 0 \text{ for all } \varphi \in I_{\mathrm{hom}}\}.$$

This will make V_{hom} compact which will be nice! V_{hom} is then called a projective algebraic curve.

Definition .1.1

We'll define the tangent space $T_p(C)$ (C is an affine algebraic curve) to be

$$T_p(C) \coloneqq \{v \in \overline{k}^n \mid [D_j\varphi_i(p)]v = 0\}.$$

We'll also consider $\mathfrak{m}_p \subseteq \overline{k}[C]$, which is the maximal ideal at p, to be

$$\mathfrak{m}_p \coloneqq \{f \in \overline{k}[C] \mid f(p) = 0\}.$$

Then $\mathfrak{m}_p/\mathfrak{m}_p^2$ is called the cotangent space at p.

Lemma .1.1

$\mathfrak{m}_p/\mathfrak{m}_p^2$ is naturally dual to T_pC as a vector space.

Proof. We must construct a perfect pairing

$$\mathfrak{m}_p/\mathfrak{m}_p^2 \times T_pC \to \overline{k}.$$

This will take $(f, v) \mapsto \nabla f(p) \cdot v$.

We must check this is well-defined. If $f \in \mathfrak{m}_p^2$ then $f = \sum g_i h_i$, where $g_i(p), h_i(p) = 0$, then

$$\nabla f(p) = \sum g_i(p) \cdot \nabla h_i(p) + \nabla g_i(p) \cdot h_i(p) = 0.$$

Furthermore, this is the coordinate ring, so if $\varphi \in I$, we see

$$\nabla\varphi \cdot v = 0,$$

since $\nabla\varphi_i \cdot v = 0$ for all φ_i. Linearity is clear. To show this is a perfect pairing, suppose $v \in T_pC$ and $(f, v) = 0$ for all f. Then $\nabla x_i(p) \cdot V = 0$, so $v = 0$.

To see the other direction, if $\nabla f \cdot v = 0$ then all the first-order partials vanish at p, and we can write f as...

Local Rings. Consider the localization $\overline{k}[C]_p \coloneqq \{f/g \in \overline{k}(C) \mid g(p) \neq 0\}$, then $M_p = \mathfrak{m}_p\overline{k}[C]_p$ is the unique maximal ideal, and

$$M_p/M_p^2 \cong \mathfrak{m}_p/\mathfrak{m}_p^2,$$

Theorem .1.2

$\overline{k}[C]_p$ is a discrete valuation ring

Proof. First we show M_p is principal. Take $t \in M_p$ generating M_p/M_p^2. Now consider $N = \langle t \rangle$. We want to show M_t/N is zero. Thus by Nakayama's Lemma we can show $M_p \cdot M_p/N = M_p/N$. We see that

$$M_p \cdot \frac{M_p}{N} = \frac{M_p^2 + N}{N} = \frac{M_p}{N}.$$

Can write any $f \in \overline{k}[C]_p$ as $t^e v$, then we define the valuation as $v_p(f) = e$. We also let $v_p(0) = \infty$.

More generally, for $f/g \in \overline{k}(C)$ we let

$$v_p(f/g) = v_p(f) - v_p(g)$$

This gives $v_p : \overline{k}(C) \to \mathbb{Z} \cup \{\infty\}$.

Note: Each $f/g \in \overline{k}(C)$ gives a map

$$C \to \mathbb{P}^1(\overline{k})$$

$$p \mapsto \begin{cases} 0 & \text{if } v_p(f/g) > 0 \\ \infty & \text{if } v_p(f/g) < 0 \\ \frac{f(p)}{g(p)} & \text{if } v_p(f/g) = 0 \end{cases}.$$

Exercise .1.1

Let $E(x, y) : y^2 = 4x^3 - 4x$. We want to compute $v_{(0,0)}\left(\frac{x}{y}\right)$.