Elliptic curves

A rather restrictive def'n.

Def: An elliptic curve over a field k is a pair (E, O) where

- $E \subseteq \mathbb{P}^2_k$ a sm. plane curve which can be written as $V_{(f)}$ where $f = y^2z - (x^3 + ax^2z + bxz^2 + cz^3)$ for some $a, b, c \in k$;
- O is the point $x = z = 0$ (i.e. $[0,1,0]$) $\in E(k)$

Remarks:

- E does not determine f, but actually it almost does - see homework.
- Usually just write $E: y^2 = x^3 + ax^2 + bx + c$ - homogenization etc. implicit
- Rather restrictive! Actually, one can define $\in C$ as a sm. proper geom. conn. curve of genus 1 w. a marked pt, & show every such can be put in this form if $\mathrm{char}\, k \neq 2$. For this, need a notion of (iso)morphism of varieties, which we lack.
- How do we (quickly) tell if a given $V_{(f)}$ smooth? See next page!

1.10| When does an equation $y^2 = x^3 + ax^2 + bx + c$ (or $y^2 = x^3 + Ax + B$) define an EC? We just need to check that the curve V_f is smooth

Lemma: The curve V_f^P where

$$f = y^2 - x^3 - ax^2 - bx - c$$

is smooth iff $16(-4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2) \neq 0$

Δ_E, discriminant

Similarly, V_f^P for $f = y^2 - x^3 + Ax + B$ is smooth iff

$$-16(4A^3 + 27B^2) \neq 0$$

Δ_E

Pf: See Homework CHECK, esp. wt. mult. by 16. □

Let (E, o) be a Weierstrass EC. Recall that we have a composition law $*$ "defined" on $E(k)$. The aim of the next section is
- to make the def'n rigorous
- to upgrade this 'composition law on $E(k)$' to give a factorization

$$E: \mathrm{Fld}_k \longrightarrow \mathrm{Set}$$

(A6) ↘ ↗ ab. gps.

(i.e. for every $K \geq k$, give a gp. structure on $E(K)$, & do this in a 'consistent' way)

For this, we need a little intersection theory.

Intersection theory for plane curves

Def: A plane curve is a hypersurface $V_f^P \subset \mathbb{P}^2_k$, where $f \in k[x, y, z]$

- Let $C \subseteq \mathbb{P}^2_k$ a plane curve. An equation for C is a poly. $f \in k[x, y, z]$ such that $C = V_f^P$ and such that $(f) = \sqrt{(f)}$.

(Equivalently, $f = u f_1 \cdots f_n$ with $u \in k^\times$ and f_i distinct irreducibles in $k[x, y, z]$)

Note that such an f exists, & is unique upto mult. by elts of $k^\times$.

Def: Let $V, W \subseteq \mathbb{P}^n_k$. The naive intersection of V & W is defined to be the algebraic variety $V \cap W \subseteq \mathbb{P}^n_k$ given by

$$V \cap W : \mathrm{Fld}/_k \longrightarrow \mathrm{Set}$$

$$K \longmapsto V(K) \cap W(K) \text{ (as subsets of } \mathbb{P}^n(K)).$$

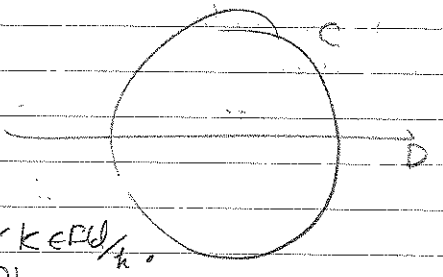
Lemma $V, W \subseteq \mathbb{P}^n_k$, say $V = V^p_I$, $W = V^p_J$. Then $V \cap W = V^p_{I+J}$ (sum of ideals in $k[x_0, \dots, x_n]$)

Pf: See Homework. □

Def A variety $V/_k$ is finite if $V(K)$ is a finite set $\forall K \in \mathrm{Fld}/_k$. (NOT enough that $V(k)$ be finite).

Def: Let $C, D \subseteq \mathbb{P}^2_k$ be plane curves. We say C, D meet properly if $C \cap D$ is finite.

eg: $C: x^2+y^2-1=0$, $D: y=0$.



$C \cap D$: $I(y, (x+1)(x-1))$

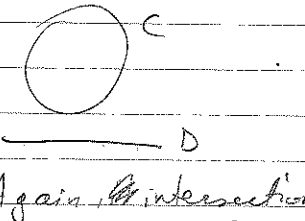
Then $(C \cap D)(K) = \{(1,0), (-1,0)\}$ $\forall K \in \mathrm{Fld}/_k$.

Guess: intersection number = 2?!

eg: $C: x^2+y^2-1=0$, $D: y-2=0$

$C \cap D$: $(y-2, x^2+3=0)$ Then

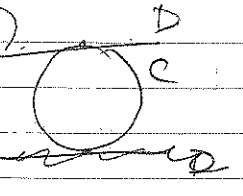
$$(C \cap D)(K) = \begin{cases} \phi & \text{if } \sqrt{-3} \notin K \\ \{(\sqrt{-3}, 2), (-\sqrt{-3}, 2)\} & \text{if } \sqrt{-3} \in K \end{cases}$$



Again, intersection number = 2?

eg: $C: x^2+y^2-1=0$, $D: y-1=0$; $C \cap D$: $(y=1, x^2=0)$

$(C \cap D)(K) = \{(0,1)\}$ $\forall K/_k$.



Idea: # still should be 2 - count multiplicity?!

cf. idea that, for composition law to work, every line in $\mathbb{P}^2$ should meet E in 3 pts w. mult.

1.12

SWAP!

Def: k a field, $C, D \subseteq \mathbb{P}^2_k$ curves which meet properly, $P \in C \cap D$ (closed). Let f an eqn for C, g an eqn for D. Let $\varphi_i : \mathbb{A}^2_k \to \mathbb{P}^2_k$ a standard chart s.t. P is in image of φ_i. Let $\tilde{f}, \tilde{g} \in k[x_0, \hat{x}_i, x_2]$ be restrictions of f, g under φ_i obtained by setting $x_i = 1$ in f, g. Let $\tilde{P} \in \mathbb{A}^2_k(k)$ best $\varphi_i(\tilde{P}) = P$.

Then define the intersection # of C, D at P by

$$i_P(C, D) = i_{\tilde{P}}(\tilde{f}, \tilde{g})$$

$k \supseteq k$

Def: k field, $P \in \mathbb{A}^2_k(K)$. Define the localization $\mathcal{O}_P$ as the localization of $k[x,y]$ at the max. ideal $(x - x_P, y - y_P)$. ($= (x_P, y_P)$)

Def: k a field, $f, g \in k[x,y]$ irred, s.t. $(f) \neq (g)$. Let $P \in \mathbb{A}^2_k(k)$ s.t. $f(P) = g(P) = 0$. Define

$$i_P(f, g) = \dim_k \frac{\mathcal{O}_P}{(f_P, g_P)}$$ (here f_P = image of f in $\mathcal{O}_P$)

Lemma: $i_P(f, g)$ is finite.

Pf. First, we observe that $(f_P) \neq (g_P)$. Indeed, suppose $(f_P) = (g_P)$. Then $f = g \cdot h$ for some $h \in \mathcal{O}_P^\times$, i.e. some $h \in k[x,y] \setminus (x - x_P, y - y_P)$. But since f, g irred we find $h \in k^\times$, so $(f) = (g)$, $\not\propto$.

Now $\mathcal{O}_P$ is regular, local, dim 2. Hence krull-dim $\frac{\mathcal{O}_P}{(f_P, g_P)}$ so krull dim $\frac{\mathcal{O}_P}{(f_P, g_P)} = 0$, so $\frac{\mathcal{O}_P}{(f_P, g_P)}$ Artinian, so $\dim_k \left(\frac{\mathcal{O}_P}{(f_P, g_P)}\right) < \infty$.

"Dimension theory of Noeth. local rings", A & M. □

It is easy to see $i_P(C, D)$ is indep. of choice of f & g – they are unique up to mult. by elts of $k^\times$. However, need to check independent of choice of coordinate chart φ_i.

This is rather easy. We will do 1 case – others identical.

To ease notation, say $k = \bar{k}$. Say P given by (x_P, y_P, z_P) & that $y_P \neq 0$ & $z_P \neq 0$. Then there are two φ_i to choose between

8/11

$\varphi_2 : \mathbb{A}^2 \longrightarrow \mathbb{P}^2$, $(x,y) \longmapsto (x,y,1)$ $\qquad$ $\varphi_1 : \mathbb{A}^2 \longrightarrow \mathbb{P}^2$, $(x,z) \longmapsto (x,1,z)$

Let $p_i \in \mathbb{A}^2(k)$ s.t. $\varphi_i(p_i) = p$, so $p_2 = \left(\frac{x_p}{z_p}, \frac{y_p}{z_p}\right)$, $p_1 = \left(\frac{x_p}{y_p}, \frac{z_p}{y_p}\right)$.

Then we have an isomorphism

$$\Psi : \mathcal{O}_{p_2} \xrightarrow{\sim} \mathcal{O}_{p_1}$$

$$\| \qquad\qquad \|$$

$$k[X,Y]_{(X-\frac{x_p}{z_p},\, Y-\frac{y_p}{z_p})} \qquad k[X,Z]_{(X-\frac{x_p}{y_p},\, Z-\frac{z_p}{y_p})}$$

$X \longmapsto X/Z$

$Y \longmapsto 1/Z$

$X/Y \longleftarrow X$

$1/Y \longleftarrow Z$

Now f corresponds to $f(x,y,1)$ under φ_2 & to $f(x,1,z)$ under φ_1, & it is easy to check that $\Psi(f(x,y,1)) = f(x,1,z) \cdot \text{unit} \in \mathcal{O}_{p_1}$, etc.

eg. $f = x+y+2z$. Then $f_1 = X+Y+Z$, & $f_2 = X+1+2Z$

Now $\Psi(f_1) = \frac{X}{Z} + \frac{1}{Z} + Z = \frac{1}{Z}(X+1+2Z)$

$= \frac{1}{Z} \cdot f_2$, & $Z \in \mathcal{O}_{p_1}^\times$.

Eg: $C: x^2+y^2-z^2=0$, $D: y-z=0$, $p: x=0, y=1, z=1$. Let's compute $i_p(C,D)$.

Well, p is contained in the patch given by $z=1$, so it's enough to compute

$i_q(f,g)$ with $f = x^2+y^2-1$, $g = y-1$, $q: x=0, y=1$.

Then $\frac{\mathcal{O}_q}{(f_q, g_q)} \simeq \frac{k[x,y]}{(y-1,\, x^2+y^2-1)} \simeq \frac{k[x]}{(x^2)}$, & $\dim_k \frac{k[x]}{(x^2)} = 2$ ☺.

Rk: Clearly $i_p(C,D) = i_p(D,C)$.

1.14

Def: k a field, $C, D \subseteq \mathbb{P}^2_k$ curves which meet properly. Define the intersection # of C & D as

$$i(C,D) = \sum_{P \in (C,D)(\bar{k})} i_P(C,D).$$

meeting properly

Lemma: k field, $C, D \subset \mathbb{P}^2_k$, $K \supseteq k$, $C_K, D_K \subset \mathbb{P}^2_K$ base-changes. Then $i(C,D) = i(C_K, D_K)$.

Pf sketch: enough to show $\dim_k \frac{k[x,y]}{(f,g)} = \dim_K \frac{K[x,y]}{(f_K, g_K)}$. comm. alg (ref).

Def: k a field, $C \subset \mathbb{P}^2_k$ a curve. Let f an eqn for C. We define the degree of C to be the homog. deg of f (clearly indep of f) (reduced).

Thm [Bezout]: k a field, $C, D \subset \mathbb{P}^2_{k=\bar{k}}$ meeting properly. Then

$$i(C,D) = \deg(C) \cdot \deg(D).$$

Pf: (assume $k = \bar{k}$.) We will only use this (I hope) in the case $\deg C = 1$ (or $\deg D = 1$). We'll only give a pf in this case. We'll even assume C given by $x = 0$ - the general case (with $\deg C = 1$) is similar, or can reduce to this case by showing $i(-,-)$ invariant under linear change of coords.

So C given by $x = 0$, & D given by $g = 0$, & $x \nmid g$.

Again adjusting coords, WMA that $(0:1:0) \notin D(k)$.
So every point in $(C,D)(\bar{k})$ is contained in the aff. patch $\psi_2 : \mathbb{A}^2 \to \mathbb{P}^2$, $(x,y) \mapsto (x:1:y)$

- the degree of g is equal to the degree of the univariate polynomial

$$g(0, y, 1) \in k[y].$$

Finally, it is an easy calculation that

$$i(C,D) = \#\text{roots of } g \text{ (in } k = \bar{k}) \text{ with multiplicities}$$
$$= \deg g$$

(□)

Def: k, C, D. Define $C \cdot D = \sum_{P \in (C,D)(\bar{k})} i_P(C,D) \cdot [P] \in$ free ab gp on $\mathbb{P}^2(\bar{k})$.
formal symbol

Group law on an elliptic curve

Def: Let k field. Let (V, O) be a pair of a variety over k & a pt $O \in V(k)$. A group law on (V, O) is a factorization

$$\mathrm{Fld}_k \xrightarrow{V} \mathrm{Set} \quad \text{s.t. } O \text{ is the identity elt}$$

$$V_g : \mathrm{Fld}_k \to \mathrm{GP}$$

(V, O, V_g) is called an algebraic gp.

Eg: $V = \mathbb{A}^n_k$, $O = (0, 0, \dots, 0)$. Define

$$\mathrm{Fld}_k \longrightarrow G_a$$

(if $n=1$, this is usually written $G_{a,k}$)

$$k \longmapsto (k^n, +).$$

eg $V = V(xy-1) \subset \mathbb{A}^2_k$, $O = (1, 1)$. Define

$$\mathrm{Fld}_k \longrightarrow G_m$$

$$k \longmapsto \big(V(k), (x_1, y_1)\cdot(x_2, y_2) = (x_1 x_2, y_1 y_2)\big).$$

(usually written $G_{m,k}$).

Def: k field, (E, O) ell. curve/k. Let $K \supseteq k$, & let $p, q \in E(K)$.

- if $p \neq q$, then let L be the unique degree-1 curve (line) in $\mathbb{P}^2_K$ such that $p, q \in L(K)$. Then

$$L \cdot E = [p] + [q] + [r] \text{ , some } r \in \mathbb{P}^2_K(\bar{K}) \text{ (maybe } p = r \text{ or } q = r).$$

Moreover, we see $r \in \mathbb{P}^2_K(K)$ since p, q are $\mathbb{P}^2_K(K)$ (naturally $\subseteq \mathbb{P}^2_K(\bar{K})$ by $K \subseteq \bar{K}$) (see Homework).

Define $p + q = r$.

- If $p = q$, let L be the unique line s.t. $L \cdot E = 2[p] + [r]$, some r (maybe $= p$).

Again, $r \in \mathbb{P}^2_K(K)$, & define $p + q = r$.

1.16 | This $*$ is not a grouplaw, it is just a rigorous version of ~~our~~ our earlier composition law.

Def ~~Def~~ Define $p+q = O*(p*q)$. (here O is the O on (E,O)).

Thm: ~~Defining~~ k field, (E,O) E/k. Defining

$$\underline{Fld}_k \longrightarrow \underline{Gp}$$
$$k \longmapsto (E(k),\ p\cdot q = p+q)$$

makes sense, giving a well-defined group law on (E,O). It is commutative.

~~Pf~~ Pf: Commutativity is clear (same holds for $*$). We should check $p+O=p$: well $p+O = O*(p*O)$.
~~p+O=p~~
Let L line through p & O, ~~so~~ & let r = third pt on line.
Then $p*O=r$, & $O*r=p$, ✓.

Define $-: E(k) \to E(k)$
$$p \longmapsto p*(O*O).$$

Then $p+(-p) = O*(p*-p) = O*(p*(p*(O*O)))$.
Let $s=O*O$, let $t=p*s$.
Again, let r = third pt on line joining p & O, then

~~$p*O=r$, so $p*r=O$, so $O*(p*(p*O)) = O*O$.~~

$p+(-p) = O*(p*(p*s)) = O*(p*t) = O*s = O$ ✓.

Other axioms similarly easy, except associativity. This ~~is~~ is possible, but is a real pain! Can do ~~it~~ in very tedious way, see proof [ST]. No fun!

Really correct way to prove assoc. (& even construct gp law) is to use Riemann-Roch to construct an iso $E(k) \simeq \mathrm{Pic}\, E_k$. This is beyond scope of course ~~see~~ ~~some HW~~ ~~exercise~~.

□