ELLIPTIC CURVES II (THE ASSOCIATIVITY)

FRANCESCO PAPPALARDI

#3 - THIRD LECTURE.

AUGUST 9TH 2016

Saigon University
Vietnam
August 1, 2016

Formulas for Addition on E (Summary for special equation)

$$E : y^2 = x^3 + Ax + B$$

$P_1 = (x_1, y_1), P_2 = (x_2, y_2) \in E(k) \setminus \{\mathcal{O}\}$,

Addition Laws for the sum of affine points

- If $P_1 \neq P_2$
  - $x_1 = x_2$ $\Rightarrow$ $P_1 +_E P_2 = \mathcal{O}$
  - $x_1 \neq x_2$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \qquad \nu = \frac{y_1 x_2 - y_2 x_1}{x_2 - x_1}$$

- If $P_1 = P_2$
  - $y_1 = 0$ $\Rightarrow$ $P_1 +_E P_2 = 2P_1 = \mathcal{O}$
  - $y_1 \neq 0$

$$\lambda = \frac{3x_1^2 + A}{2y_1}, \nu = -\frac{x_1^3 - Ax_1 - 2B}{2y_1}$$

Then

$$P_1 +_E P_2 = (\lambda^2 - x_1 - x_2, -\lambda^3 + \lambda(x_1 + x_2) - \nu)$$

Properties of the operation "$+_E$"

Theorem

The addition law on $E(k)$ has the following properties:

(a) $P +_E Q \in E(k)$ $\qquad \forall P, Q \in E(k)$

(b) $P +_E \mathcal{O} = \mathcal{O} +_E P = P$ $\qquad \forall P \in E(k)$

(c) $P +_E (-P) = \mathcal{O}$ $\qquad \forall P \in E(k)$

(d) $P +_E (Q +_E R) = (P +_E Q) +_E R$ $\qquad \forall P, Q, R \in E(k)$

(e) $P +_E Q = Q +_E P$ $\qquad \forall P, Q \in E(k)$

- $(E(k), +_E, \mathcal{O})$ commutative group
- $-P = -(x_1, y_1) = (x_1, -y_1)$
- All group properties are easy except associative law (d)
- Today we shall discuss three proofs:
  1. Computer assisted proof
  2. *Combinatorial incidence Geometry* proof
  3. Algebraic proof via the *Picard group*

- If L/k is a field extension, we can $E(L)$ also if E is defined over k; Theorem holds for $(E(L), +_E)$
- In particular, if E/k, can consider the groups $E(\bar{k})$.

Computer assited proof of the associativity

We need to explain to the computer how to check that:

$$P +_E (Q +_E R) = (P +_E Q) +_E R \quad \forall P, Q, R \in E$$

In the case when either one of $P, Q, R, P +_E Q$ or $Q +_E R$ equals $\mathcal{O}$ the above identity is clearly satisfied. Here we deal with the *generic case*. i.e. All the points $\pm P, \pm R, \pm Q, \pm(Q +_E R), \pm(P +_E Q)$ all different.We have the following

Lemma

Let $P_1 = (x_1, y_1), P_2 = (x_2, y_2), P_3 = (x_3, y_3) \in k^2$ distinct. Suppose there exists an elliptic curve E such that $P_1, P_2, P_2 \in E(k) \setminus \{\mathcal{O}\}$ and $P_1 + P_2 + P_3 = \mathcal{O}$

$$\Longrightarrow \det \begin{vmatrix} 1 & x_1 & x_1^3 - y_1^2 \\ 1 & x_2 & x_2^3 - y_2^2 \\ 1 & x_3 & x_3^3 - y_3^2 \end{vmatrix} = 0.$$

Mathematica code

```
L[x_,y_,r_,s_]:=(s-y)/(r-x);
M[x_,y_,r_,s_]:=(yr-sx)/(r-x);
A[{x_,y_},{r_,s_}]:={(L[x,y,r,s])^2-(x+r),
        -(L[x,y,r,s])^3+L[x,y,r,s](x+r)-M[x,y,r,s]}
Together[A[A[{x,y},{u,v}],{h,k}]-A[{x,y},A[{u,v},{h,k}]]]
det = Det[({{1,x1,x1^3-y1^2},{1,x2,x2^3-y2^2},{1,x3,x3^3-y3^2}})]
PolynomialQ[Together[Numerator[Factor[res[[1]]]]/det],
                      {x1,x2,x3,y1,y2,y3}]
PolynomialQ[Together[Numerator[Factor[res[[2]]]]/det],
                      {x1,x2,x3,y1,y2,y3}]
```

One more case:
$P +_E 2Q = (P +_E Q) +_E Q$

Combinatorial incidence Geometry

We specialize to the case $k = \mathbb{C}$
If $P \in \mathbb{C}[x, y]$ has degree d, we consider the *affine curve* $V_P = \{(x_0, y_0) \in \mathbb{C}^2 : \ P(x_0, y_0) = 0\}$ and the associated *projective curve*

$$\mathbb{P}V_{F_P} = \{[x_0, y_0, z_o] \in \mathbb{P}^2(\mathbb{C}) : \ F_P(x_0, y_0, z_0) = 0\}$$

where $F_P(X, Y, Z) := Z^d P(X/Z, Y/Z)$ is the corresponding *homogenized* polynomial.

1. A curve (affine or projective) of degree one is a *line* $\mathbb{P}V_{F_P} : aX + bY + cZ = 0$
2. A curve (affine or projective) of degree two is called a *quadric* $\mathbb{P}V_{F_P} : aX^2 + bXY + cXZ + dY^2 + eYZ + fZ^2 = 0$
3. A curve (affine or projective) of degree three is called a *cubic* $\mathbb{P}V_{F_P} : aX^3 + bX^2Y + cX^2Y + dXY^2 + eXYZ + fXZ^2 + gY^3 + hY^2Z + jYZ^2 + kZ^3 = 0$
4. A curve my have multiple components when P (or F_P) is *not* irreducible. When P is irreducible (so is F_P), V_P (and $\mathbb{P}V_{F_P}$) are called irreducible
5. **Examples:** $\mathcal{Q} : X^2 - XY = 0$ is a reducible quadric; $\mathcal{C} : X(X^2 + Y^2 + Z^2) = 0$ is a reducible cubic. In this case we write $\mathcal{Q} \cap \mathcal{C} = \ell$. Where $\ell : \{X = 0\}$ is a common component.
6. An irreducible quadric is called a *conic*
7. A cubic which is irreducible, smooth and is also called elliptic curve

Bézout Theorem

We shall use the fundamental:

Theorem (Bézout Theorem)

Any two (projective) curves with degrees d and d' without common components, meet in exactly dd' points counted with moltiplicity.

For example if there are no common components, a line meets a curve of degree d in d points and a quadric curve meets it in $2d$ points. Two cubic (irreducible or not) meet in 9 points and so on.

Note (Consequences of Linear Algebra)

A line depends on **3** parameters; A quadric depends on **6** parameters; A cubic depends on **10**,...A curve of degree **d**, depends on $(\mathbf{d}+\mathbf{1})(\mathbf{d}+\mathbf{2})/\mathbf{2}$ parameters.
Hence, applying linear algebra:

1. Through any **2** given points in $\mathbb{P}^2(\mathbb{C})$ it passes a line
2. Through any **5** given points in $\mathbb{P}^2(\mathbb{C})$ it passes a quadric
3. Through any **9** given points in $\mathbb{P}^2(\mathbb{C})$ it passes a cubic
4. Through any $\mathbf{d}(\mathbf{d}+\mathbf{3})/\mathbf{2}$ given in $\mathbb{P}^2(\mathbb{C})$ points it passes a curve of degree **d**

Note (Example)

Given $[X_j, Y_j, Z_j] \in \mathbb{P}^2(\mathbb{C}), j = 1, 2, 3, 4, 5$, solve for a, b, c, d, e, f the linear system:

$$\begin{cases} aX_1^2 + bX_1Y_1 + cX_1Z_1 + dY_1^2 + eY_1Z_1 + fZ_1^2 = 0 \\ aX_2^2 + bX_2Y_2 + cX_2Z_2 + dY_1^2 + eY_2Z_2 + fZ_2^2 = 0 \\ aX_3^2 + bX_3Y_3 + cX_3Z_3 + dY_3^2 + eY_3Z_3 + fZ_3^2 = 0 \\ aX_4^2 + bX_4Y_4 + cX_4Z_4 + dY_4^2 + eY_4Z_1 + fZ_4^2 = 0 \\ aX_5^2 + bX_5Y_5 + cX_5Z_5 + dY_5^2 + eY_5Z_5 + fZ_5^2 = 0 \end{cases}$$

1. For degree **1**, if the points are distinct, the line is unique
2. For degree **2**
   - if **5** points are collinear, then there are infinitely many quadric (all reducible) through the **5** points
   - if **3** points are collinear, then there exists no conic through the **5** points (Bezout Theorem) but only union of lines
3. For degree **3**
   - if **8** points are in a quadric, then there are infinitely many cubic (all reducible) through the **9** points
   - if **7** points are in a quadric, then there exists no irreducible cubic through the **9** points (Bezout Theorem) but only union of a quadric and a line
   - if **4** points are collinear, then there exists no irreducible cubic through the **9** points (Bezout Theorem) but only union of a quadric and a line

The notion of *General Position* may be introduced to recover uniqueness? For example: *If five point of $\mathbb{P}^2(\mathbb{C})$ are such that no three of them are collinear, then the quadric is unique and it is a conic.*

Theorem (Cayley-Bacharah)

Let $P_0, P_1 \in \mathbb{C}[X, Y, Z]$ be two cubic homogeneous polynomials and consider The two curves:

$$\mathcal{C}_0 : \{P_0 = 0\} \qquad \text{and} \qquad \mathcal{C}_1 : \{P_1(x, y) = 0\}.$$

*Assume that $\mathcal{C}_0$ and $\mathcal{C}_1$ intersect (over $\mathbb{C}$) in **precisely 9 distinct points** $A_1, A_2, \ldots, A_9 \in \mathbb{P}^2(\mathbb{C})$.*
If P is a cubic homogeneous polynomials that vanishes on eight of these points (say $A_1, A_2, \ldots, A_8$). Then P is a linear combination of P_0 and P_1 and in particular it vanishes also on the ninth point A_9.

Proof of the Cayley-Bacharah Theorem.

Some preliminary observations on the points $A_1, A_2, \ldots, A_9$:

(a) no 4 (**four**) of the **9** points are collinear (otherwise Bézout fails)

(b) no 7 (**seven**) of the **9** points lie on a quadric (otherwise Bézout fails)

(c) any 5 (**seven**) of the **9** points determine a unique quadric σ

if the quadrics were two σ and σ', then (by Bézout) they would share a common line ℓ.

such a line can contain most three points (by Bézout). So the line ℓ' through the other two points is such that $\sigma = \ell \cdot \ell' = \sigma'$

□

Proof of the Cayley-Bacharah Theorem (continues).

Further observations on the points $A_1, A_2, \dots, A_9$:

1. no 3 (**three**) of the first **8** points (say A_1, A_2, A_3) are collinear (lying on a line ℓ, say):

   Suppose $A_4, A_5, \dots, A_8$ do not lie on ℓ and let σ be the *unique* quadric containing them

   If B is another point on ℓ and C a point not on $\ell \cup \sigma$. By linear algebra we can find a cubic homogeneous polynomial $Q = aP + bP_0 + cP_1$ such that Q vanishes on B and C.

   Hence Q vanishes on A_1, A_2, A_3 and on B so it contains ℓ and a quadric curve.

   Such a quadric curve passes thought $A_4, A_5, \dots, A_8$ so in coincides with σ.

   This contradicts the fact that Q vanishes on C.

2. no 6 (**six**) of the first **8** points (say $A_1, \dots, A_6$) lie on a quadric σ.

   Note that σ would not be the union of two lines. Otherwise there would be three collinear points

   Let ℓ be the line through A_7 and A_8.

   If B is another point on σ and C a point not on $\ell \cup \sigma$. By linear algebra we can find a cubic homogeneous polynomial $Q = aP + bP_0 + cP_1$ such that Q vanishes on B and C.

   As $\mathcal{C}_Q$ vanishes on seven of its points, it contains σ as a component. Hence $\mathcal{C}_Q = \sigma \cdot \ell$ which contradicts the fact that C is in Q.

□

Proof of the Cayley-Bacharah Theorem (conclusion).

Let $\ell = \ell_{A_1,A_2}$ and $\sigma = \sigma_{A_3,\ldots,A_7}$ the unique quadric.

σ is a conic (otherwise three point are collinear) and $A_8 \notin \ell \cup \sigma$.

Let $B, C \in \ell \setminus \sigma$ and let $Q = aP + bP_0 + cP_1$ a cubic vanishing on B and C.

$\mathcal{C}_Q$ vanishes on four point of ℓ and goes through $A_3, \ldots, A_7$, hence $\mathcal{C}_Q = \ell \cup \sigma$. But then it does not pass through A_8 which is a cotraddiction.

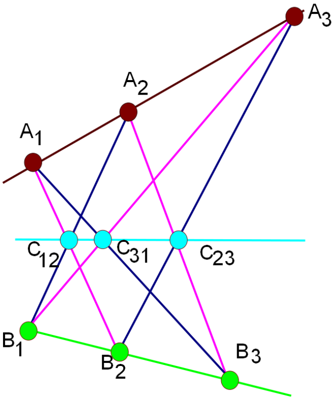
□

Theorem (Pappus)

Let ℓ and ℓ' be distinct lines. Let A_1, A_2, A_3 distict points of ℓ not on ℓ' and let B_1, B_2, B_3 distict points of ℓ' not on ℓ'. Then the three points

$$C_{12} = \ell_{A_1,B_2} \cap \ell_{A_2,B_1}, \quad C_{23} = \ell_{A_2,B_3} \cap \ell_{A_3,B_2}, \quad \textit{and} \quad C_{31} = \ell_{A_3,B_1} \cap \ell_{A1,B_3}$$

are collinear □



Assume C_{12}, C_{23} and C_{31} distinct otherwise the statement is obvious. Consider the three cubics:

$$\begin{aligned} \gamma_0 &= \ell_{A_1,B_2} \cdot \ell_{A_2,B_3} \cdot \ell_{A_3,B_1} \text{(purple lines)}, \\ \gamma_1 &= \ell_{A_2,B_1} \cdot \ell_{A_3,B_2} \cdot \ell_{A_1,B_3} \text{(dark blue lines)}, \\ \gamma_2 &= \ell \cdot \ell' \cdot \ell_{C_{12},C_{23}}. \end{aligned}$$

$A_1, A_2, A_3, B_1, B_2, B_3, C_{12}, C_{23}, C_{13}$ are in γ_0 and γ_1.

$A_1, A_2, A_3, B_1, B_2, B_3, C_{12}, C_{23}$ is in γ_2.

Cayley-Bacharah implies that C_{31} is also in γ_2.

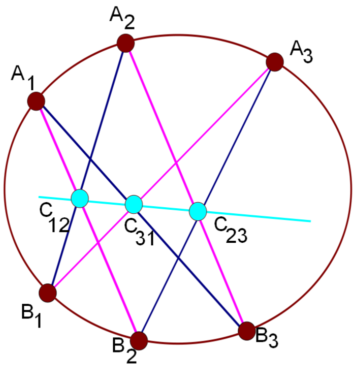
Finally, since C_{31} is not in ℓ and not in ℓ', C_{31} is in $\ell_{C_{12},C_{23}}$ which is the claim. □

Theorem (Pascal)

Let $A_1, A_2, A_3, B_1, B_2, B_3$ distict points of a conic σ. Then the three points

$$C_{12} = \ell_{A_1,B_2} \cap \ell_{A_2,B_1}, \quad C_{23} = \ell_{A_2,B_3} \cap \ell_{A_3,B_2}, \quad \text{and} \quad C_{31} = \ell_{A_3,B_1} \cap \ell_{A1,B_3}$$

are collinear



Assume C_{12}, C_{23} and C_{31} distinct otherwise the statement is obvious. Consider the three cubics:

$$\begin{aligned} \gamma_0 &= \ell_{A_1,B_2} \cdot \ell_{A_2,B_3} \cdot \ell_{A_3,B_1} \text{(purple lines)}, \\ \gamma_1 &= \ell_{A_2,B_1} \cdot \ell_{A_3,B_2} \cdot \ell_{A_1,B_3} \text{(dark blue lines)}, \\ \gamma_2 &= \sigma \cdot \ell_{C_{12},C_{23}}. \end{aligned}$$

$A_1, A_2, A_3, B_1, B_2, B_3, C_{12}, C_{23}, C_{13}$ are in γ_0 and γ_1.

$A_1, A_2, A_3, B_1, B_2, B_3, C_{12}, C_{23}$ is in γ_2.

Cayley-Bacharah implies that C_{31} is also in γ_2.

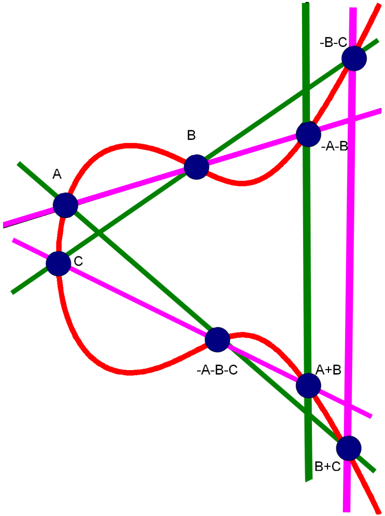
Finally, since C_{31} is not in σ since σ meets any line in at most two points, C_{31} is in $\ell_{C_{12},C_{23}}$ which is the claim. □

Pappus's Theorem is a degenerate case of Pascal's Theorem.

Theorem (Associativity of the elliptic curve law)

Let E be a projective elliptic curve where $\mathcal{O} = [0, 1, 0]$ is the point at infinity. Let A, B, C be points of an elliptic curve E. Then

$$A +_E (B +_E C) = (A +_E B) +_E C.$$



Assume that $\mathcal{O}$, A, B, C, $A + B$, $B + C$, $-(A + B)$, $-(B + C)$ are all distinct and all different from $-((A + B) + C)$ and from $-(A + (B + C))$.Let

$$\gamma_1 = \ell_{A,B} \cdot \ell_{C,(A+B)} \cdot \ell_{\mathcal{O},(B+C)} \text{(purple lines)},$$
$$\gamma_2 = \ell_{\mathcal{O},(A+B)} \cdot \ell_{B,C} \cdot \ell_{A,(B+C)} \text{(green lines)}$$

By construction, E and γ_1 are cubic with no common component that meet in nine distinct points $\mathcal{O}$, A, B, C, $A + B$, $B + C$, $-(A + B)$, $-(B + C)$, $-((A + B) + C)$. The cubic γ_2 goes through the first eight points. By **Cayley-Bacharah** also goes through the ninth point $-((A + B) + C)$.
The line $\ell_{A,(B+C)}$ (which is a component of γ_2) meets E both in $-((A + B) + C)$ and in $-(A + (B + C))$. So, this two points must be equal. □

Pappus's Theorem and Pascal's Theorem are degenerate cases of the above.

Facts about $A := k[x, y]/(w)$

Analogies with $\mathbb{Z}[i]$

Let $E : w = y^2 - x^3 - a_4x - a_6$ be an elliptic curve with $a_4, a_6 \in k$. Consider the ring

$$A := k[x, y]/(w)$$

if we set $v = x^3 + a_4x + a_6 \in k[x]$ and the coset $\mathbf{y} := y + (w)$. Hence

$$\mathbb{Z}[T]/(T^2 + 1) =: \mathbb{Z}[i] \quad = \quad \{a + ib : a, b \in \mathbb{Z}\}$$
$$A := k[x, y]/(w) = k[x][y]/(y^2 - v) \quad = \quad \{f + g\mathbf{y} : f, g \in k[x]\}.$$

Analogies:

1. *i and $\mathbf{y}$ satisfy:* $T^2 + 1 = (T - i)(T + i)$ $\qquad$ $T^2 - v = (T - \mathbf{y})(T - \overline{\mathbf{y}})$ where $\overline{\mathbf{y}} = u - \mathbf{y}$
2. *Conjugation map*: $a + ib \mapsto \overline{a + ib} = a - ib$ $\qquad$ $f + g\mathbf{y} \mapsto \overline{f + g\mathbf{y}} = f + g\overline{\mathbf{y}}$
3. *Norm functions*: $N(a + ib) = (a + ib)(a - ib) = a^2 + b^2$ $\qquad$ $N(f + g\mathbf{y}) = (f + g\mathbf{y})(f + g\overline{\mathbf{y}}) = f^2 - g^2v$
4. *Norm properties*: $N(\alpha) = |\mathbb{Z}[i]/(\alpha)| \forall \alpha \in \mathbb{Z}[i]$, $\qquad$ $\deg N(\alpha) = \dim_k(A/(\alpha)) \forall \alpha \in A$
5. $|\mathbb{Z}[i]/(\alpha)| = N(\alpha)$ $\qquad$ $\dim_k(A/(\alpha)) = \deg(N(\alpha))$

same proof: $R = \mathbb{Z}[i], S = \mathbb{Z}$ $\qquad$ $R = A, S = k[x]$

a) $|R/(\alpha)| = |R/(\overline{\alpha})|$ as $g + (\alpha) \mapsto \overline{g} + (\overline{\alpha})$ defines an isomorphism $R/(\alpha) \cong R/(\overline{\alpha})$;
b) $N(\alpha\beta) = N(\alpha)N(\beta)$ because of the exact sequence $0 \to R/(\alpha) \to R/(\alpha\beta) \to R/(\beta) \to 0$.
c) $\forall m \in S$, from $R/(m) \cong S/(m) \oplus S/(m)$
if $R = \mathbb{Z}[i]$, $N(m) = m^2$, $\qquad$ if $R = A$, $\dim_k(A/m) = 2 \deg m$
d) Finally $R/(\alpha)^2 \cong R/(\alpha) \oplus R/(\overline{\alpha}) \cong R/(\alpha\overline{\alpha})$,

The degree of the norm

It is quite simple to see that for $\alpha = f + g\mathbf{y} \in A$,

$$\dim_k(A/(\alpha)) = \deg(\alpha\overline{\alpha}) = \deg(f^2 - g^2 v) = \max\{2\deg f, 3 + 2\deg g\}.$$

This immediately implies that A is a *domain*. Furthermore

Theorem

The elements $\mathbf{e}_0, \mathbf{e}_2, \mathbf{e}_3, \mathbf{e}_4, \cdots$ *of* A *defined by*

$$\mathbf{e}_{2j} = x^j, \quad \mathbf{e}_{3+2j} = \mathbf{y}x^j \quad (j \geq 0)$$

form a k*–basis of* A *over* k *and for* $\alpha = \sum_{i \neq 1} c_j \mathbf{e}_j \in A$ *(with* $c_j \in K$ *not all zero), one has*
$\deg(N(\alpha)) = \max\{j : c_j \neq 0\}$

Note (The absense of $\mathbf{e}_1$ implies that A is not Eucledean with the norm N)

If A *euclidean* and $\beta \in A \setminus k$ of mininum norm, $\deg_k(A/(\beta)) = 1$ since $\forall \alpha \in A$, $\alpha = q\beta + \rho \Longrightarrow \rho \in k$. Hence $\deg N(\beta) = 1 \rightarrow\leftarrow$

The algebraic proof of associativity

(following H. Lenstra)

$\forall P = [\alpha : \beta : 1] \in E(k)$ a *ring homomorphism*

$$\varphi_P : A \longrightarrow k, X \mapsto \alpha, Y \mapsto \beta.$$

1. $\mathfrak{m}_P = \mathfrak{m} = \ker \varphi_P \quad \Longrightarrow \quad A/\mathfrak{m} \cong k \quad \Longrightarrow \quad \dim_k A/\mathfrak{m} = 1$
2. $P \mapsto \mathfrak{m}_P$ is one to one correspondence between $E(k) \setminus \{\mathcal{O} = [0 : 1 : 0]\}$ and the set of ideal $\mathfrak{m} \subset A$ s. t. $\dim_k A/\mathfrak{m} = 1$
3. We extended to all of $E(k)$ by $\mathcal{O} \mapsto (1) = A$
4. 1-1 map:

$$E(k) \longleftrightarrow \mathrm{P}(A) := \{\mathfrak{m} \subset A : \mathfrak{m} \text{ is an ideal and } \dim_k A/\mathfrak{m} \leq 1\}$$

5. Need to define a group ooperation on $\mathrm{P}(A)$ which is *compatible* with $+_E$
6. We are done!
7. in which sense *compatible*?

Compatibility with the group law of the elliptic curve

Proposition

(i) Let $P_1 = (x_1, y_1), P_2 = (x_2, y_2), P_3 = (x_3, y_3) \in E(k) \setminus \{\mathcal{O}\}$ and let $\mathfrak{m}_j = (X - x_j, Y - y_j) \in P(A)$ be the ideal associated to P_j.Then

$$P_1 +_E P_2 +_E P_3 = \mathcal{O} \quad \Longrightarrow \quad \mathfrak{m}_1 \cdot \mathfrak{m}_2 \cdot \mathfrak{m}_3 = (rX + sY + t) \subset A$$

where $rX + sY + t = 0$ is the line through P_1, P_2 and P_3.

(ii) Let $P = (x_P, y_P) \in E(k) \setminus \{\mathcal{O}\}$.Then

$$\mathfrak{m}_P \mathfrak{m}_{-P} = (x - x_P) \subset A$$

Proof.

(i): first assume P_j's distinct. Enough to show $m_j \supset (rX + sY + t)$ for $j = 1, 2, 3$. This implies

$$(rX + sY + t) \subseteq \mathfrak{m}_1 \mathfrak{m}_2 \mathfrak{m}_3.$$

Since $\dim_k(A/m_j) = 1$ and $\deg(N(rX + sY + t)) = 3$.
Just rite $(rX + sY + t) = ((y_j - y_{j'})(X - x_j) + (x_j - x_{j'})(Y - y_j))$.
Next assume $P_1 = P_2$ and let $2y_1(y - y_1) - (3x_1^2 + A)(x - x_1) = 0$ the tangent line to E at P_1. Argument above extends except that has to show that $\dim_k A/\mathfrak{m}^2 = 2$ or equivalently that $\dim_k \mathfrak{m}/\mathfrak{m}^2 = 1$. This follows from the fact that P_1 is non singular.
(ii): Analogue. Observing that $2y_P(X - x_P) = (Y + y_P)(X - x_P) - (Y - y_P)(X - x_P)$ □

The Picard group

Definition

Let B be a domain. Then

1. An ideal $\mathfrak{a} \subset A$ is said invertible if there exists some ideal $\mathfrak{b} \subset B$ such that $\mathfrak{a}\mathfrak{b} = (\alpha)$ for some $\alpha \in B$ non-zero.
2. Two ideals $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent ($\mathfrak{a} \sim \mathfrak{b}$) if there exists non-zero $\alpha, \beta \in B$ with $\beta\mathfrak{a} = \alpha\mathfrak{b}$.
3. The Picard group is the quotient

$$\mathrm{Pic}(B) = \{\mathfrak{a} \subset B : \mathfrak{a} \text{ invertible ideal}\}/\sim$$

4. The elements of $\mathrm{Pic}(B)$ are ideal classes $[\mathfrak{a}]$ and the multiplication of classes is defined by $[\mathfrak{a}][\mathfrak{b}] = [\mathfrak{a}\mathfrak{b}]$.
5. $\mathrm{Pic}(B)$ is an abelian group under the multiplication of classes of ideas with $[(1)]$ as the neutral element.

Corollary (The map $\Phi : E(k) \to \mathrm{Pic}(A)$, $P \mapsto [(X - x_p, Y - y_p]$, $\mathcal{O} \mapsto [(1)]$ is multiplicative)

Strategy

Note (Strategy)

1. First bijection

$$\Psi : E(k) \longrightarrow P(A) := \{\mathfrak{n} \subset A : \mathfrak{m} \text{ ideal with } \dim_k(A/\mathfrak{m}) \leq 1\}, P \mapsto \mathfrak{m}_P = (X - x_P, Y - y_P)$$

2. Second bijection

$$\Phi : P(A) \longrightarrow \mathrm{Pic}(A), \mathfrak{m} \mapsto [\mathfrak{m}]$$

3. The composition is compatible with the operations (i.e. $\Phi(\Psi(P +_E Q)) = [\mathfrak{m}_P][\mathfrak{m}_Q]$)
4. Need to show that Φ is a bijection.
5. Strategy:
   - -a- prove: $\dim_k(A/\mathfrak{m}) = 1 \implies \mathfrak{m}$ is invertible *(i.e. Φ is well defined)*
     a technical Lemma
   - -b- prove: $\forall [\mathfrak{a}] \in \mathrm{Pic}(A), \exists! \mathfrak{m} \in S$ s.t. $([\mathfrak{a}][\mathfrak{m}] = 1)$ (i.e. $\mathfrak{a}\,\mathfrak{m}$ principal)
     poor man's Riemann–Roch Theorem

Poor Man's Riemann Rock

Theorem

$\forall \mathfrak{a} \subset A$ *ideal,* $\exists!$ *principal* $(\alpha) \subset \mathfrak{a}$*, s.t.* $\dim_k \mathfrak{a}/(\alpha) \leq 1$.

Proof.

1. $\dim_k(A/\mathfrak{a}) = m$ (say) is finite:
   Let $\beta \in \mathfrak{a}, \beta \neq 0$. Then $A/(\beta) \twoheadrightarrow A/\mathfrak{a}$. Since $\dim_k A/(\beta) = \deg(N(\beta)) < \infty$, $\dim_k A/\mathfrak{a} < \infty$
2. Since $\mathbf{e}_0, \mathbf{e}_2, \ldots, \mathbf{e}_{m+1}$ are linear independent in $A/\mathfrak{a}$. Let
   $$\alpha = \sum_{\substack{j \leq m+1 \\ j \neq 1}} c_j \mathbf{e}_j \quad c_j\text{'s not all zero}$$
   $\deg_k(N(\alpha)) \leq m+1 \implies \dim_k(\mathfrak{a}/(\alpha) = \dim_k(A/(\alpha)) - \dim_k(A/\mathfrak{a}) \leq 1$
3. α is unique: Suppose that there exists β with the same properties. If $\deg_k \mathfrak{a}/(\alpha) = \dim_k \mathfrak{a}/(\beta) = 0$, then necessarilty $(\alpha) = (\beta) = \mathfrak{a}$.
4. In can be excluded that $\deg_k \mathfrak{a}/(\alpha) = 0$ and $\dim_k \mathfrak{a}/(\beta) = 1$. In fact, if it was the case, then we would have $\dim_k(\alpha)/(\beta) = \dim_k(A/(\alpha/\beta) = \deg(N(\alpha/\beta)) = 1$ which is impossible.
5. if $\deg_k \mathfrak{a}/(\alpha) = \dim_k \mathfrak{a}/(\beta) = 1$, then write $\alpha = \sum \lambda_j \mathbf{e}_j$ and $\beta = \sum \mu_j \mathbf{e}_j$ with $\lambda_{m+1} \neq 0$ and $\mu_{m+1} \neq 0$. But this implies that $\tau = \mu_{m+1}\alpha - \lambda_{m+1}\beta \in \mathfrak{a}$ has degree $\leq m$. Finally we are lead to the impossible situation above.

□

From the above, one can deduce that A is a PID if and only if $E(k) = \{\mathcal{O}\}$ is the trivial group.

The technical Lemma

Theorem

Let $\mathfrak{m} = (\alpha, \beta) \subset$ *A maximal ideal, Then* $\mathfrak{m}$ *is invertible* $\Longleftrightarrow \dim_{A/\mathfrak{m}} \mathfrak{m}/\mathfrak{m}^2 = 1$.

Proof.

$\Longrightarrow$: use that $\mathfrak{a} \mapsto \mathfrak{a}\mathfrak{m}$ gives a bijection

□