

# Démonstration

Yann-Arby BEBBA

11 février 2022

## Table des matières

### Lecture 1: Lemme 7.1.

Sun 06 Feb 2022 02 :51

**Lemme .1.** Soit  $g$  un polynôme unitaire à coefficients dans  $K$  de degré  $n \geq 1$ . Soient  $\alpha_1, \dots, \alpha_n$  ses racines dans  $\overline{K}$  comptées avec multiplicités. Le discriminant  $\Delta$  de  $g$  est défini par l'égalité

$$\Delta = \prod_{i < j} (\alpha_i - \alpha_j)^2.$$

C'est un élément de  $K$ .

### Démonstration.

□

**Lemme .2.** Soit  $\Delta = -(4a^3 + 27b^2)$  le discriminant  $f : x^3 + ax + b$ . Les racines de  $f$  sont simples, si et seulement si  $\Delta \neq 0$ .

**Démonstration.** Montrons tout d'abord que le discriminant de  $f$  est  $\Delta = -(4a^3 + 27b^2)$ .

Soit  $\Delta$  le discriminant de  $f$ . Soient  $\alpha, \beta, \gamma$  les racines de  $f$  dans  $\overline{K}$  et  $f'$  le polynôme dérivé de  $f$ .

Tout d'abord montrons grâce au Lemme 1 que :

$$\begin{aligned} \Delta &= (-1)(\alpha - \beta)^2(\alpha - \gamma)^2(\beta - \gamma)^2 \\ &= -f(\alpha)'f(\beta)'f(\gamma)'. \end{aligned}$$

D'après le théorème de d'Alembert on peut écrire  $f$  sous la forme :

$$f = (X - \alpha)(X - \beta)(X - \gamma).$$

En dérivant  $f$  sous cette forme on obtient :

$$\begin{aligned} f &= (X - \alpha)((X - \beta)(X - \gamma))' + (X - \beta)(X - \gamma) \\ &= (X - \alpha)((X - \beta) + (X - \gamma)) + (X - \beta)(X - \gamma). \end{aligned}$$

---

Donc

$$f' = (X - \alpha)(X - \beta) + (X - \alpha)(X - \gamma) + (X - \beta)(X - \gamma).$$

On a alors successivement :

$$f(\alpha)' = (\alpha - \beta)(\alpha - \gamma), f(\beta)' = (\beta - \alpha)(\beta - \gamma) \text{ et } f(\gamma)' = (\gamma - \alpha)(\gamma - \beta).$$

En multipliant ces trois expressions, on obtient :

$$\begin{aligned} f(\alpha)' f(\beta)' f(\gamma)' &= (\alpha - \beta)(\alpha - \gamma)(\beta - \alpha)(\beta - \gamma)(\gamma - \alpha)(\gamma - \beta) \\ &= (X - \alpha)(\alpha - \gamma)(-1)(\alpha - \beta)(\beta - \gamma)(-1)(\alpha - \gamma)(-1)(\beta - \gamma) \\ &= (-1)^3 (\alpha - \beta)^2 (\alpha - \gamma)^2 (\beta - \gamma)^2 \\ &= -\Delta. \end{aligned}$$

Et donc

$$\Delta = -f'(\alpha)f'(\beta)f'(\gamma).$$

En partant de la forme  $f : x^3 + ax + b$ , on remarque que  $f' : 3x^2 + a$ . Par suite on obtient,

$$\begin{aligned} \Delta &= -f'(\alpha)f'(\beta)f'(\gamma) \\ &= -(3\alpha^2 + a)(3\beta^2 + a)(3\gamma^2 + a). \end{aligned}$$

Ce qui donne :

$$\begin{aligned} \Delta &= -((9\alpha^2\beta^2 + 3a(\alpha^2 + \beta^2) + a^2)(3\gamma^2 + a)) \\ &= -\left(27(\alpha\beta\gamma)^2 + 9a(\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2) + 3a^2(\alpha^2 + \beta^2 + \gamma^2) + a^3\right). \end{aligned}$$

D'après l'identité suivante :

$$a^2 + b^2 = (a + b)^2 - 2ab.$$

On peut écrire

$$\alpha^2 + \beta^2 + \gamma^2 = (\alpha + \beta + \gamma)^2 - 2(\alpha\beta + \alpha\gamma + \beta\gamma),$$

$$\alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2 = (\alpha\beta + \alpha\gamma + \beta\gamma)^2 - 2\alpha\beta\gamma(\alpha + \beta + \gamma).$$

Donc d'après les relations entre coefficients et racine (i.e relation de Viète), pour un polynôme de la forme  $ax^3 + bx^2 + cx + d$ , on a :

$$\alpha + \beta + \gamma = -\frac{b}{a},$$

$$\alpha\beta + \alpha\gamma + \beta\gamma = \frac{c}{a},$$

$$\alpha\beta\gamma = -\frac{d}{a}.$$

Donc pour  $f$  on a  $a = 1$ ,  $b = 0$ ,  $c = a$  et  $d = b$ .

D'où,

$$\alpha + \beta + \gamma = 0, \alpha\beta + \alpha\gamma + \beta\gamma = a \text{ et } \alpha\beta\gamma = -b.$$

Ce qui donne :

$$\begin{aligned}\alpha^2 + \beta^2 + \gamma^2 &= 0^2 - 2a = 2a \\ \alpha^2\beta^2 + \alpha^2\gamma^2 + \beta^2\gamma^2 &= a^2 + 2b \times 0.\end{aligned}$$

Donc le discriminant vaut :

$$\begin{aligned}\Delta &= -(27b^2 + 9a^3 - 6a^3 + a^3) \\ &= -(4a^3 + 27b^2).\end{aligned}$$

Maintenant, supposons que  $\Delta = 0$ . On a alors :

$$\begin{aligned}-(4a^3 + 27b^2) = 0 &\Leftrightarrow -f(\alpha)'f(\beta)'f(\gamma)' = 0 \\ &\Leftrightarrow (f(\alpha)' = 0) \vee (f(\beta)' = 0) \vee (f(\gamma)' = 0) \\ &\Leftrightarrow \alpha \text{ ou } \beta \text{ ou } \gamma \text{ est une racine multiple.}\end{aligned}$$

D'où le résultat. □

## Lecture 2: Lemme 7.2.

Mon 07 Feb 2022 10 :28

**Lemme .3.** Soient  $P = [a_1, a_2, a_3]$  et  $Q = [b_1, b_2, b_3]$  deux points distincts de  $\mathbb{P}^2$ .

Il existe une unique droite de  $\mathbb{P}^2$  passant par  $P$  et  $Q$ . C'est la droite  $D$  d'équation  $ux + vy + wz = 0$  avec  $[x, y, z] \in \mathbb{P}^2$  et

$$u = a_2b_3 - a_3b_2, \quad v = a_3b_1 - a_1b_3, \quad w = a_1b_2 - a_2b_1.$$

Énoncé originel :

Soient  $P = [a_1, a_2, a_3]$  et  $Q = [b_1, b_2, b_3]$  deux points distincts de  $\mathbb{P}^2$ . Il existe une unique droite de  $\mathbb{P}^2$  passant par  $P$  et  $Q$ . C'est l'ensemble des points  $[x, y, z] \in \mathbb{P}^2$  tels que le déterminant de la matrice

$$M = \begin{pmatrix} a_1 & b_1 & x \\ a_2 & b_2 & y \\ a_3 & b_3 & z \end{pmatrix}$$

soit nul. Autrement dit, c'est la droite d'équation  $ux + vy + wz = 0$ , avec

$$u = a_2b_3 - a_3b_2, \quad v = a_3b_1 - a_1b_3, \quad w = a_1b_2 - a_2b_1.$$

**Démonstration.** Montrons qu'il existe une droite  $D$  passant par  $P$  et  $Q$ .

Les éléments  $u$ ,  $v$  et  $w$  ne sont pas tous nuls car  $P$  et  $Q$  sont distincts.

En effet, si  $P = Q$  alors  $a_1 = b_1$ ,  $a_2 = b_2$  et  $a_3 = b_3$  donc  $u = v = w = 0$  or  $P \neq Q$  donc il existe  $x \in \{u, v, w\}$  tel que  $x \neq 0$ . □

---

**Lecture 3: Lemme 7.3.**

Mon 07 Feb 2022 20 :57

Soit

$$y^2z = x^3 + axz^2 + bz^3,$$

l'équation de  $E$ , où  $a, b \in K$ .

Notons

$$F = Y^2Z - (X^3 + aXZ^2 + bZ^3) \in K[X, Y, Z],$$

$$F_X = \frac{\partial F}{\partial X}, \quad F_Y = \frac{\partial F}{\partial Y}, \quad F_Z = \frac{\partial F}{\partial Z},$$

c'est-à-dire,

$$F_X = -(3X^2 + aZ^2), \quad F_Y = 2YZ, \quad F_Z = Y^2 - (2aXZ + 3bZ^2).$$

**Lemme .4.** Il n'existe pas de point  $P \in E$  tel que

$$F_X(P) = F_Y(P) = F_Z(P) = 0.$$

**Démonstration.** Supposons par l'absurde, qu'il existe un tel point  $P \in E$ . Remarquons que  $F_Z(O) = 1 \neq 0 = F_Z(P)$  donc par hypothèse  $P$  est distinct de  $O$ .Pour fixer les idées posons  $P = [x, y, 1]$ .Puisque  $\text{Car}(K) \neq 2$ , on a

$$(F_Y = 0) \Leftrightarrow (2YZ = 0) \Rightarrow (Y = 0),$$

donc  $y = 0$ .Donc  $P$  serait de la forme  $[x, 0, 1]$ .

On obtient alors

$$F_X = -(3X^2 + a) = 0 \text{ et } F_Z = -(2aX + 3b) = 0.$$

— Supposons  $a \neq 0$ , on alors à partir de  $F_Z$ 

$$X = -\frac{3b}{2a}.$$

Donc par  $F_X$ 

$$\begin{aligned} -\left(3\left(-\frac{3b}{2a}\right)^2 + a\right) &= 0 \\ -(27b^2 + 4a^3) &= 0. \end{aligned}$$

Ce qui est absurde car  $F$  est elliptique. (cite lemme 7.1)

— Supposons que  $a = 0$ , alors

$$(3b = 0) \underbrace{\Rightarrow}_{\text{Car}(K) \neq 3} (b = 0).$$

Donc on  $a = b = 0$  donc  $-(27b^2 + 4a^3) = 0$  absurde car  $F$  est elliptique.  
(lem 7.1)

D'où le résultat.

□

#### Lecture 4: Lemme 7.4.

Mon 07 Feb 2022 20 :59

**Lemme .5. 1)** L'équation de la tangente à  $E$  au point  $O$  est  $z = 0$ .

**2)** Soit  $P = [x_0, y_0, 1]$  un point de  $E$  distinct de  $O$ . L'équation de la tangente à  $E$  en  $P$  est

$$F_X(P)(x - x_0z) + F_Y(P)(y - y_0z) = 0.$$

**Démonstration. 1)** Soit  $O \in E$  le point à l'infini. D'après l'équation de la tangente à  $E$  au point  $O$ . On a successivement

$$F_X(O) = 0, F_Y(O) = 0 \text{ et } F_Z(O) = 1.$$

Ainsi on retrouve bien  $z = 0$ .

**2)** Soit  $P$  un tel point, d'après l'équation (cite ? set up snippet -nommé + cité) de la tangente et de l'égalité  $y_0^2 = x_0^3 + ax_0 + b$  on a,

$$\begin{aligned} & F_X(P)x + F_Y(P)y + F_Z(P)z = 0 \\ & -(3x_0^2 + a)x + (2y_0)y + (y_0^2 - (2ax_0 + 3b))z = 0 \\ & -3x_0^2x - ax + 2y_0y + y_0^2z - 2ax_0z - 3bz = 0 \\ & -3x_0^2x - ax + 2y_0y + y_0^2z - 2ax_0z - 3z(y_0^2 - x_0^3 - ax_0) = 0 \text{ (i.e } b = y_0^2 - (x_0^3 + ax_0)) \\ & -3x_0^2x - ax + 2y_0y + y_0^2z - 2ax_0z - 3y_0^2z + 3x_0^3z + 3ax_0z = 0 \\ & -(3x_0^2 + a)x + 2y_0y - 2y_0^2z + (3x_0^2 + a)x_0z = 0 \\ & -(3x_0^2 + a)(x - x_0) + 2y_0(y - y_0z) = 0. \end{aligned}$$

D'où le résultat.

□

#### Lecture 5: Proposition 7.1.

Mon 07 Feb 2022 21 :04

Dans cette proposition à l'aide du comportement de deux points du plan  $E$  et de la droite qui les intersectent. On veut construire une loi de composition interne

$$\begin{aligned} \top : E \times E &\longrightarrow E \\ (P, Q) &\longmapsto P \top Q \end{aligned}$$

Cette loi, comme on va le voir, n'est pas une loi de groupe. C'est ce qui va nous permettre cependant de donner, par la suite, de donner une structure de groupe au plan  $E$  à l'aide d'une symétrie bien choisie.

---

**Proposition .6.** Soient  $P$  et  $Q$  des points de  $E$ . Soit  $D$  la droite de  $\mathbb{P}^2$  passant par  $P$  et  $Q$  si  $P \neq Q$ , ou bien la tangente à  $E$  en  $P$  si  $P = Q$ . On a

$$D \cap E = \{P, Q, f(P, Q)\},$$

où  $f(P, Q)$  désigne le point de  $E$  défini par les conditions suivantes.

1) Supposons  $P \neq Q$ ,  $P \neq O$  et  $Q \neq O$ .

i) Supposons  $x_P \neq x_Q$ . Posons

$$\lambda = \frac{y_P - y_Q}{x_P - x_Q} \text{ et } \nu = \frac{x_P y_Q - x_Q y_P}{x_P - x_Q}.$$

On a

$$f(P, Q) = [\lambda - x_P - x_Q, \lambda(\lambda^2 - x_P - x_Q) + \nu, 1].$$

ii) Si  $x_P = x_Q$ , on a  $f(P, Q) = O$ .

2) Supposons  $P \neq O$  et  $Q = O$ . On a

$$f(P, O) = [x_P, -y_P, 1].$$

De même, si  $P = O$  et  $Q \neq O$ , on a  $f(O, Q) = [x_Q, -y_Q, 1]$

3) Si  $P = Q = O$ , on a  $f(O, O) = O$ .

4) Supposons  $P = Q$  et  $P \neq O$ .

i) Si  $y_P = 0$ , on a  $f(P, P) = O$ .

ii) Supposons  $y_P \neq 0$ . Posons

$$\lambda = \frac{3x_P^3 + a}{2y_P} \text{ et } \nu = \frac{-x_P^3 + ax_P + 2b}{2y_P}.$$

On a

$$f(P, P) = [\lambda^2 - 2x_P, \lambda(\lambda^2 - 2x_P) + \nu, 1].$$

Dans cette démonstration, on étudie le comportement des points  $P$  et  $Q$  selon qu'ils soient distincts ou égaux. Que ce soit pour la droite ou la tangente tous les deux vont éventuellement, soit recouper la courbe elliptique et rester dans le plan  $E$ , soit "couper" le point à l'infini  $O$ . C'est ce qu'on veut découvrir à l'aide du point que l'on a nommé  $f(P, Q)$  qui désigne le comportement par rapport à  $P$  et  $Q$  de ce troisième point.

**Démonstration.** Soient  $P = [x_P, y_P, 1]$  et  $Q = [x_Q, y_Q, 1]$  des points de  $E$  tels qu'ils sont distincts. Alors il existe une droite  $D \in \mathbb{P}^2$  qui passe par  $P$  et  $Q$ .

1) Supposons  $P \neq Q$ ,  $P \neq O$  et  $Q \neq O$ . Donc comme  $D$  existe, il existe un point  $M \in D \cap E$  et on cherche donc à connaître son comportement dans le plan  $E$ .

i) Supposons  $x_P \neq x_Q$ . Comme  $P, Q \neq O$ , le point à l'infini n'appartient pas à  $D$ . Comme  $M \in D$ , il est de la même forme que  $P$  et  $Q$ . Posons  $M = [x_0, y_0, 1]$  avec  $x_0, y_0$  des coordonnées sur  $\bar{K}$ .

---

Comme  $M \in E$ , on a la première égalité

$$y_0^2 = x_0^3 + ax_0 + b. \quad (1)$$

Ensuite avec  $M \in D$  d'après le lemme 7.2 on a la matrice suivante

$$\begin{pmatrix} x_P & x_Q & x_0 \\ y_P & y_Q & y_0 \\ 1 & 1 & 1 \end{pmatrix},$$

qui nous permet d'obtenir une seconde égalité.

$$\begin{aligned} (y_P - y_Q)x_0 - (x_P - x_Q)y_0 + (x_P y_Q - x_Q y_P) &= 0 \\ y_0 &= \frac{y_P - y_Q}{x_P - x_Q} x_0 + \frac{x_P y_Q - x_Q y_P}{x_P - x_Q}. \end{aligned}$$

Posons

$$\lambda = \frac{y_P - y_Q}{x_P - x_Q} \quad \text{et} \quad \nu = \frac{x_P y_Q - x_Q y_P}{x_P - x_Q}.$$

Donc l'équation de  $D$  est de la forme

$$y = \lambda x + \nu z,$$

c'est-à-dire dans notre cas on a

$$y_0 = \lambda x_0 + \nu.$$

En remplaçant dans (1), il vient

$$\begin{aligned} (\lambda x_0 + \nu)^2 &= x_0^3 + ax_0 + b \\ \lambda^2 x_0^2 + 2\lambda\nu x_0 + \nu^2 &= x_0^3 + ax_0 + b \\ x_0^3 - \lambda^2 x_0^2 + (a - 2\lambda\nu)x_0 + b - \nu^2 &= 0. \end{aligned}$$

Donc  $x_0$  est une racine du polynôme

$$H = X^3 - \lambda^2 X^2 + (a - 2\lambda\nu)X + b - \nu^2.$$

On remarque que  $H(x_P) = H(x_Q) = 0$  donc  $x_P$  et  $x_Q$  sont aussi des racines de  $H$ . Par les relations coefficients racines obtient la valeur de  $x_0$

$$\begin{aligned} x_0 + x_P + x_Q &= -(-\lambda^2) \\ x_0 &= \lambda^2 - x_P - x_Q. \end{aligned}$$

Ainsi les racines de  $H$  sont

$$x_P, \quad x_Q \quad \text{et} \quad \lambda^2 - x_P - x_Q.$$

Il en résulte que  $D \cap E$  est formé de  $P$ , et du point  $M = f(P, Q)$ .  
Donc

$$\begin{aligned} f(P, Q) &= [x_0, y_0, 1] \\ &= [\lambda^2 - x_P - x_Q, \lambda x_0 + \nu, 1] \\ &= [\lambda^2 - x_P - x_Q, \lambda(\lambda^2 - x_P - x_Q), 1]. \end{aligned}$$

D'où l'assertion.

- 
- ii) Supposons  $x_P = x_Q$ . Comme  $P$  et  $Q$  sont distincts, on a alors  $y_P = -y_Q$ . D'après le lemme 7.2, la matrice suivante

$$\begin{pmatrix} x_P & x_Q & x \\ y_P & -y_Q & y \\ 1 & 1 & z \end{pmatrix}.$$

D'où l'équation de la droite suivante

$$\begin{aligned} 2y_P x - 2y_P x_P z &= 0 \\ x &= x_P z. \end{aligned}$$

Donc le point  $O$  est aussi un point de la droite  $D$  donc de  $D \cap E$ . Soit  $M \in D \cap E$  distincts de  $O$ . Si  $M = [0, 1, 0]$ , d'après la situation on a  $x_0 = x_P$  et  $y_0 = \pm y_P$ , donc  $M = P$  ou  $M = Q$ . Or on a  $P, Q \neq O$ . Donc on a nécessairement  $M = O$ . Ainsi on a bien  $D \cap E = \{P, Q, f(P, Q) = O\}$ , d'où l'assertion dans ce cas ci.

- 2) Supposons  $P \neq O$  et  $Q = O$ . Donc d'après lemme 7.2, on a

$$\begin{pmatrix} x_P & 0 & x \\ y_P & 1 & y \\ 1 & 0 & z \end{pmatrix}.$$

À partir de la deuxième ligne on obtient l'équation de la droite suivante

$$\begin{aligned} x_P z - x &= 0 \\ x &= x_P z. \end{aligned}$$

Si  $M = [x_0, y_0, 1]$  est un point de  $D \cap E$ , on a donc  $x_0 = x_P$  d'où  $y_0 = \pm y_P$ . On a ainsi  $D \cap E = \{P, O, f(P, O)\}$ , où  $f(P, O) = [x_P, -y_P, 1]$ .

- 3) Supposons  $P = Q = O$ , par le lemme 7.4 la tangente  $D$  à  $E$  au point  $O$  à pour  $z = 0$ . Par suite,  $O$  est le seul point de  $D \cap E$ , d'où  $f(O, O) = O$ .
- 4) Supposons  $P = Q$  et  $P \neq O$ . L'équation de la tangente  $D$  à  $E$  en  $P$  a donc pour équation

$$F_X(P)(x - x_P z) + F_Y(P)(y - y_P z) = 0.$$

- i) Si  $y_P = 0$ , on a

$$x_P^3 + ax_P + b = 0.$$

Donc  $x_P$  est racine simple de ce polynôme. De plus,  $F_X(P) \neq 0$ . En effet, si  $F_X(P) = 0$  on a

$$\begin{aligned} -(3x_P^2 + a) &= 0 \\ x_P^2 &= -\frac{a}{3}, \end{aligned}$$

ce qui est absurde.

Ainsi à partir de l'équation de la tangente  $D$  on a

$$\begin{aligned} F_X(P)(x - x_P z) = 0 &\Rightarrow (F_X(P)) = 0 \vee (x - x_P z) = 0 \\ &\Rightarrow x - x_P z = 0. \end{aligned}$$



---

Donc pour  $D$  on a

$$D : x = x_P z.$$

Le seul point de  $D \cap E$  distinct de  $P$  est donc le point  $O$ , d'où  $D \cap E = (P, O)$ , d'où l'assertion.

- ii) Supposons  $y_P \neq 0$ . Du lemme 7.4 et de l'équation  $b = y_P^2 - x_P^3 - ax_P$  on obtient

$$\begin{aligned} & -(3x_P^2 + a)(x - x_P z) + 2y_P(y - y_P z) = 0 \\ & -3x_P^2 x + 3x_P^3 z - ax + ax_P z + 2y_P y - 2y_P^2 z = 0 \\ & 2y_P y = 3x_P^2 x - 3x_P^3 z + ax - ax_P z + 2y_P^2 z \\ & 2y_P y - ax_P z = 3x_P^2 x + ax - x_P^3 z + 2b \\ & y = \frac{3x_P^2 + a}{2y_P} x + \frac{-x_P^3 + ax_P + 2b}{2y_P} z. \end{aligned}$$

On pose  $\lambda = \frac{3x_P^2 + a}{2y_P}$  et  $\nu = \frac{-x_P^3 + ax_P + 2b}{2y_P}$  et on obtient l'équation de  $D$ , c'est-à-dire

$$y = \lambda x + \nu z.$$

Le point  $O$  n'est donc pas sur  $D$ . Soit  $M = [x_0, y_0, 1]$  un point de  $E \cap D$ . On a par le même raisonnement que dans le cas (1-i) (utilise ref?) les deux équations suivantes

$$y_0^2 = x_0^3 + ax_0 + b \quad \text{et} \quad y_0 = \lambda x_0 + \nu.$$

Par suite  $x_0$  est une racine du polynôme

$$G = X^3 - \lambda^2 X^2 + (a - 2\lambda\nu)X + b - \nu^2.$$

Le polynôme dérivé de  $G$  est

$$G' = 3X^2 - 2\lambda^2 X + a - 2\lambda\nu.$$

□