

Option C

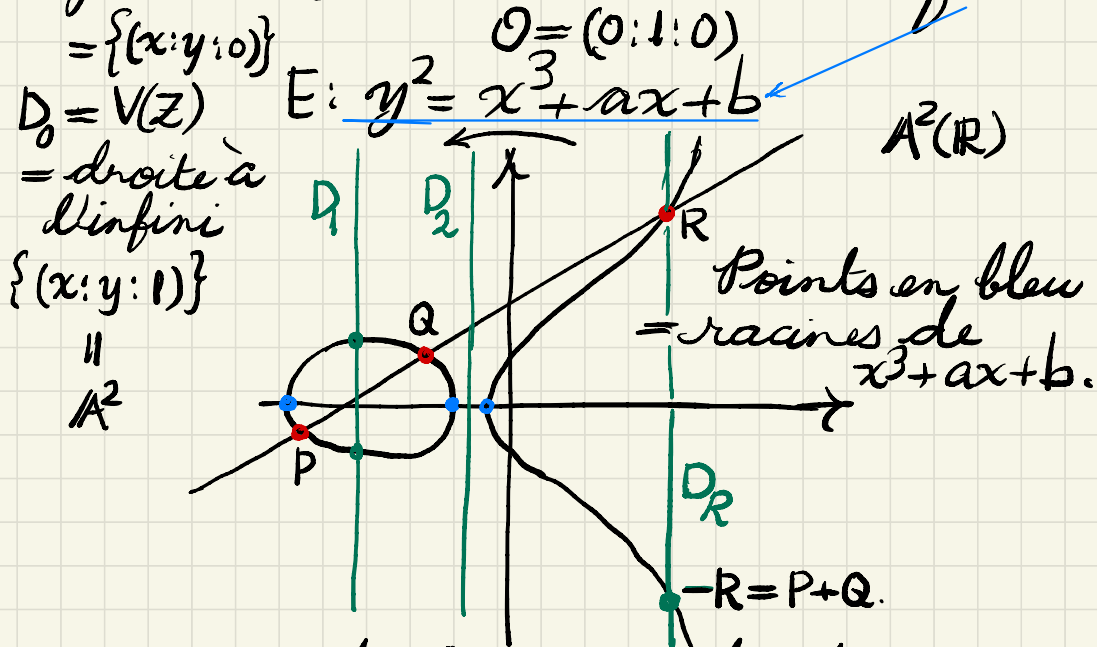
Courbes elliptiques
(un aperçu)

D Kohel

15/12/2020



Courbe elliptique : courbe cubique dans $\mathbb{P}^2$. La partie affine ($\subseteq \mathbb{A}^2$) peut être normalisée de la forme



Bézout : trois points d'intersection avec une droite.

Cas spéciaux : une droite verticale a une intersection à l'infini.

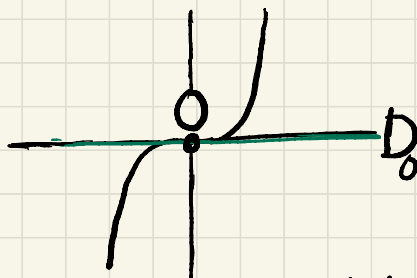
D_1 : 2 points affines avec $E(\mathbb{R})$ + le point O

D_2 : 2 points affines dans $E(\mathbb{C})$, conjugués, + le point O

D_0 : Le point à l'infini O avec mult 3.

(2)

à l'infini:



On obtient une loi d'addition sur E en utilisant Bézout:

Règle: Trois points d'intersection avec une droite somme à O (= le point à l'infini, vu comme le point neutre): $P+Q+R=O \Rightarrow P+Q=-R$.

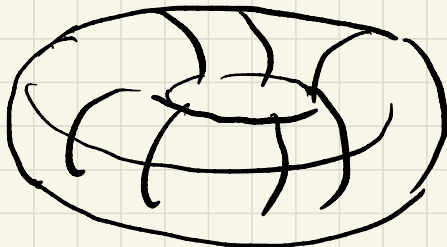
$$D_R: R+(-R)+O=0 \quad \nearrow$$

On peut vérifier que cette définition donne lieu à une structure de groupe abélien.

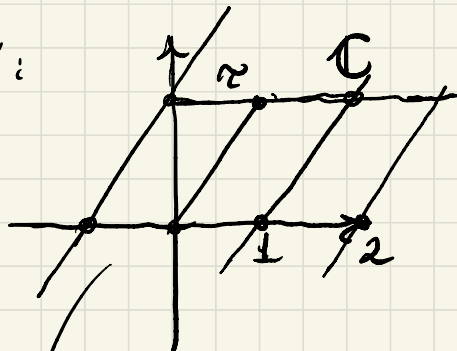
Sur $\mathbb{C}$: $E(\mathbb{C})$ ressemble:

On peut identifier

$$E(\mathbb{R}) \subseteq E(\mathbb{C})$$



18°

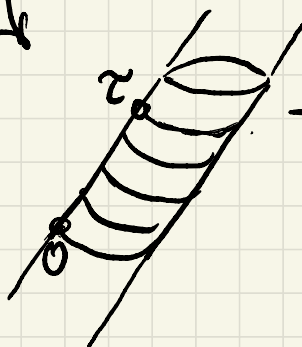


$\Lambda \parallel \langle 1, z \rangle = \mathbb{Z} + \mathbb{Z}z$

$\exists p(z) = p(z)$

mero-
morphe
& double-
ment
periodique

$\mathbb{C} / \langle 1, z \rangle \cong$



$g=1$

$p'(z)^2 = 4p(z)^3 + g_2(\Lambda)p(z) + g_3(\Lambda)$

$y = p'(z)$

$y^2 = 4x^3 + Ax + B$
 $x = p(z)$

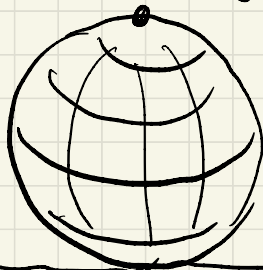
$A = g_2(\Lambda)$

$B = g_3(\Lambda)$

$g=0$:

$\mathbb{P}^1(\mathbb{C})$:

$\infty = (0:1)$



$\mathbb{C}$

Hierarchie des courbes

$g=0$: droites, coniques

$g=1$: courbes elliptiques