Courbes algébriques

(Introduction à la géométrie algébrique)

Introduction : qu'est-ce que c'est que la géométrie algébrique ?

L'étude des solutions de systèmes d'équations polynomiales en plusieurs variables

$$f_1 = \cdots = f_r = 0 \quad \text{où} \quad \underbrace{f_1, \ldots, f_r}_{\text{polynômes}} \in \underset{\text{(un corps)}}{k}[\underbrace{t_1, \ldots, t_n}_{\text{indéterminées (=variables)}}]$$

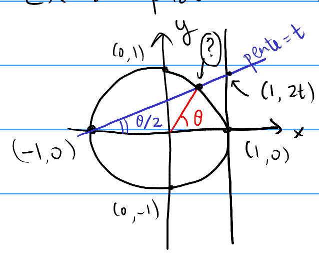
$$Z(f_1, \ldots, f_r)(k) := \{\underbrace{(x_1, \ldots, x_n)}_{=:\underline{x}} \in k^n \mid f_1(\underline{x}) = \cdots = f_r(\underline{x}) = 0\}$$

à travers la géométrie des objets qu'ils définissent.

P.ex. en géométrie euclidienne, $\{(x,y) \in \mathbb{R}^2 \mid x^2+y^2-1=0\}$ est un cercle.

On distingue la situation "géométrique" où on cherche des solutions à valeurs dans un corps algébriquement clos (p.ex. $\mathbb{C}$), et la situation "arithmétique", plus générale (p.ex. sur $\mathbb{Q}$). (Les corps finis ($\mathbb{F}_q$) sont un peu intermédiaires.)

Ex de problème : paramétrage rationnel du cercle $\{x^2+y^2=1\}$



Paramétrage ~~"transcendant"~~ : $\theta \longmapsto (\cos\theta, \sin\theta)$

fonctionne uniquement sur $\mathbb{R}$.

Points rationnels ? Pas évidents à trouver. P.ex. $\left(\frac{3}{5}, \frac{4}{5}\right)$ (triplet pythagoricien)

$3^2+4^2=5^2$

Paramétrage par la droite de pente $t = \tan\frac{\theta}{2}$: si (x,y) est le point d'intersection de la droite de pente t par $(-1,0)$ $\{y = t(x+1)\}$ et du cercle $\{x^2+y^2=1\}$, on a

$$x^2 + t^2(x+1)^2 = 1 \qquad x^2 + t^2x^2 + 2t^2x + t^2 = 1$$

$$(t^2+1)x^2 + 2t^2x + (t^2-1) = 0 \qquad \text{ceci admet } x=-1 \text{ comme solution}$$

l'autre solution est alors $x = \frac{1-t^2}{1+t^2}$ et alors $y = \frac{2t}{1+t^2}$

Bref, $\boxed{t \longmapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)}$ fournit un paramétrage de $\{x^2+y^2=1\}$ $(x \neq -1)$ $(t^2 \neq -1)$ par des fonctions rationnelles. Intérêt : ceci fonctionne sur "n'importe quel" corps. $(2 \neq 0)$

(P.ex. $t = \frac{1}{2} \in \mathbb{Q}$ donne $\left(\frac{3}{5}, \frac{4}{5}\right)$)

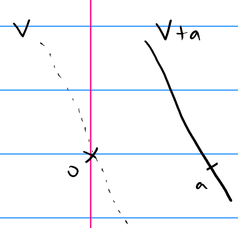
Ceci permet aussi de calculer le cardinal $\#\{(x,y) \in \mathbb{F}_q \mid x^2+y^2=1\} = \begin{cases} q+1 & \text{si } q \equiv 3 \pmod 4 \\ q-1 & \text{si } q \equiv 1 \pmod 4 \end{cases}$

Rq : $\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ est une solution de $x^2+y^2=1$ avec $x,y \in k(t)$.

Espace affine et espace projectif

Déf : si k est un corps, on appelle "espace affine de dimension n" sur k et on note $\mathbb{A}^n(k)$ l'ensemble k^n.

Généralement, on notera $\underline{x} := (\underbrace{x_1, \dots, x_n}_{\text{coordonnées (affines) de } \underline{x}})$ un élément de $\mathbb{A}^n(k)$



* $\overbrace{\text{Sous-espaces affines}}^{\text{"s.e.a."}}$ de $\mathbb{A}^n(k)$: ce sont les $\underbrace{V+a}_{\text{(translaté)}}$ avec V un k-s.e.v. de k^n et $a \in k^n$

= translatés des sous-espaces vectoriels ("s.e.v") et l'ensemble vide

La dimension d'un tel s.e.a. est par définition celle de V.

P. ex. une droite affine est un $\{\lambda u + a \mid \lambda \in k\}$, $u \in k^n \setminus \{0\}$, $a \in k^n$

(= s.e.a. de dimension 1).

Les singletons $\{a\} = \{0\} + a$ $(a \in k^n)$ sont les s.e.a de dimension 0.

Description "implicite" = $V = \{\varphi_i - c_i = 0\}$ où $\varphi_1, \dots, \varphi_r$ sont des formes linéaires sur V (= élément du dual V^*) qui engendrent V^*

et $c_1, \dots, c_r$ sont des constantes (= éléments de k)

$\varphi_i - c_i$ peut être vu comme un polynôme de degré 1. (degré total)

Sous-espace affine engendré par $a_1, \dots, a_r \in \mathbb{A}^n(k)$

c'est $\{\underbrace{\lambda_1 a_1 + \dots + \lambda_r a_r}_{\text{"combinaison affine"}} \mid \lambda_1, \dots, \lambda_r \in k$ vérifiant $\lambda_1 + \dots + \lambda_r = 1\}$

= le plus petit sous-espace affine contenant $a_1, \dots, a_r$.

Transformations affines (inversibles) : ce sont les $\underline{x} \mapsto M\underline{x} + b$, $k^n \to k^n$

où $M \in GL_n(k)$ (matrice $n \times n$ inversible), $b \in k^n$

= composée d'une transformation linéaire inversible et d'une translation $(y \mapsto y + b)$

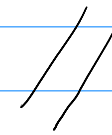
Les transformations affines inversibles (de k^n) forment un groupe appelé groupe (général ?) affine $GA_n(k) = k^n \rtimes GL_n(k)$.

Ce sont les transformations bijectives qui préservent les combinaisons affines.

(Idée : la "géométrie affine" est celle qui connaît la notion de droite, plan, etc., et de parallélisme, mais pas d'angle, distance, ...)

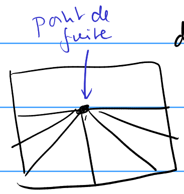
Géométrie projective et espace projectif.

Idée : on voudrait supprimer la notion de parallélisme :



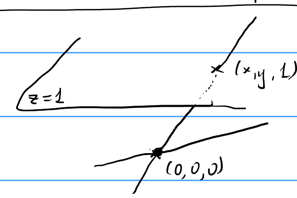
Notion apparue à la renaissance avec le développement et l'étude des lois de la perspective

(inventer un point d'intersection "à l'infini".



Plan projectif :

on va vouloir regarder les points (x,y) du plan



affine $\mathbb{A}^2(k)$ comme $(x,y,1)\in\mathbb{A}^3(k)$ et les identifier à la droite reliant l'origine $(0,0,0)=O$ et $(x,y,1)$: toutes les droites par O correspondent à des points de $\mathbb{A}^2$ sauf celles qui sont parallèles à $\{z=1\}$ qui vont donner naissance aux "points à l'infini".

Déf (variante 1) : l'espace projectif de dimension n sur un corps k, noté $\mathbb{P}^n(k)$, est l'ensemble des droites vectorielles (= s.e.v. de dimension 1) de k^{n+1}.

Plutôt que considérer les droites elles-mêmes on peut considérer la relation d'équivalence "définir la même droite" :

le point $(x_0,\dots,x_n)\in k^{n+1}$, différent de $(0,\dots,0)$, définit la droite vectorielle $\{(\lambda x_0,\dots,\lambda x_n)\mid\lambda\in k\}$

et $(x_0,\dots,x_n)$ et $(y_0,\dots,y_n)$ définissent la même ssi

$$\exists\lambda\in k^\times\ (\underline{y}=\lambda\underline{x}\quad(\text{c'est-à-dire } y_i=\lambda x_i \text{ pour tout } i))$$

$k^\times := \{z\in k\mid z\neq 0\}$ (plus généralement, $A^\times := \{z\in A\mid z \text{ inversible}\}$) anneau

Bref, on définit une relation d'équivalence $\sim$ sur $k^{n+1}\setminus\{(0,\dots,0)\}$ par $(x_0,\dots,x_n)\sim(y_0,\dots,y_n)$

$$:\Leftrightarrow \exists\lambda\in k^\times\ (\underline{y}=\lambda\underline{x})$$

$$\Leftrightarrow \underline{y} \text{ et } \underline{x} \text{ sont colinéaires}$$

$$\Leftrightarrow x_i y_j = x_j y_i \text{ pour tous } i \text{ et } j$$

Et alors (les classes d'équivalence par $\sim$ sont des droites moins l'origine).

Déf (variante 2) : $\mathbb{P}^n(k) := (k^{n+1}\setminus\{0\})/\sim$

est l'ensemble des classes d'équivalence dans $k^{n+1}\setminus\{0\}$ (origine) par la relation en question.

deux points

On notera $(x_0 : \cdots : x_n)$ l'élément de $\mathbb{P}^n(k)$ défini comme classe d'équivalence de $(x_0, \dots, x_n)$ par $\sim$ (ou comme droite vectorielle qu'il engendre)

⚠ Ceci n'a de sens que si au moins une des coordonnées x_i est $\neq 0$.

On a $(x_0 : \cdots : x_n) = (y_0 : \cdots : y_n)$ ssi $\exists \lambda \in k^\times \; \forall i \; (y_i = \lambda x_i)$

Ex: dans $\mathbb{F}_5$: $(1:0:2) = (2:0:-1) = (-1:0:-2)$

Les $x_0, \dots, x_n$ s'appellent des coordonnées homogènes du point en question.

⚠ La valeur de x_i n'a pas de sens en soi.
En revanche, la question de savoir si $x_i = 0$ en a une.
et si $x_i \neq 0$, la valeur $\frac{x_j}{x_i}$ a un sens.

Convention: on peut distinguer deux sortes de points dans $\mathbb{P}^n$, à savoir:

- ceux pour lesquels $x_0 \neq 0$, qu'on peut écrire (quitte à diviser toutes les coordonnées par $\frac{1}{x_0}$) sous la forme $(1 : x_1 : \cdots : x_n)$: on identifiera un tel point avec le point $(x_1, \dots, x_n) \in \mathbb{A}^n(k)$
- ceux pour lesquels $x_0 = 0$, qui sont de la forme $(0 : x_1 : \cdots : x_n)$: ces points sont appelés "points à l'infini" et forment collectivement un "$\mathbb{P}^{n-1}$ à l'infini"

Bref, on peut écrire "$\mathbb{P}^n(k) = \underbrace{\mathbb{A}^n(k)}_{\{x_0 \neq 0\}} \cup \underbrace{\mathbb{P}^{n-1}(k)}_{\{x_0 = 0\}}$"

"points affines"
"points finis" (?)
"points à distance finie"

union disjointe

"à l'infini"

Remarque: cette distinction "points à l'infini" / "points finis" n'est pas intrinsèque à $\mathbb{P}^n$: pour $\mathbb{P}^n$, tous les points se valent, c'est le choix d'un espace affine $\mathbb{A}^n$ ici vu comme $\{x_0 \neq 0\}$ qui fait naître cette distinction.

* Nombre de points de $\mathbb{P}^n(\mathbb{F}_q)$? → corps fini à q éléments

Deux méthodes de calcul :

→ $\#(\mathbb{F}_q^{n+1}\setminus\{0\}) = q^{n+1}-1$

chaque classe par $\sim$ a $q-1$ éléments (droite vectorielle moins l'origine)

donc $\#\mathbb{P}^n(\mathbb{F}_q) = \dfrac{q^{n+1}-1}{q-1}$

→ on vient de voir que $\mathbb{P}^n(\mathbb{F}_q) = \underbrace{\mathbb{A}^n(\mathbb{F}_q)}_{q^n} \overset{\circ}{\cup} \mathbb{P}^{n-1}(\mathbb{F}_q)$

donc par récurrence $\#\mathbb{P}^n(\mathbb{F}_q) = q^n + q^{n-1} + \cdots + q + 1$

Ceci permet au passage de retrouver la valeur de la somme géométrique.

* Notion de sous-espace projectif de $\mathbb{P}^n$:

si V est un sous-espace vectoriel de k^{n+1}, disons de dimension $m+1$,

on note $\mathbb{P}(V) := (V\setminus\{0\})/\sim$ l'ensemble des classes d'équivalence par $\sim$ des points (non nuls) de V.

Ce $\mathbb{P}(V)$ s'appellera (un) sous-espace projectif de dimension m de $\mathbb{P}^n$.

(Pour $m=0$, on retrouve les points de $\mathbb{P}^n$:

si V est la droite vectorielle engendrée par $(x_0,\dots,x_n)\neq 0$

alors $\mathbb{P}(V) = \{(x_0:\cdots:x_n)\}$.)

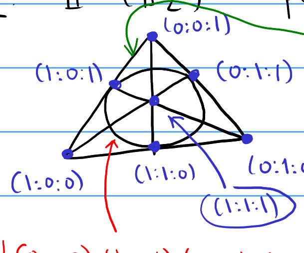
Pour $m=1$ on parle de droite projective, pour $m=2$ de plan projectif, etc.

Remarque : par deux points distincts de $\mathbb{P}^n$ passe une unique droite [projective]

à savoir $\mathbb{P}(V)$ où V est le plan vectoriel engendré par x, y

les vecteurs de coordonnées des points en question

Ex : $\underset{\underset{(\mathbb{F}_2^3\setminus\{0\})/\sim}{\parallel}}{\mathbb{P}^2(\mathbb{F}_2)}$ "plan de Fano" a 7 points.



$V = \{(0,0,0), (1,0,1), (0,1,1), (1,1,0)\}$

$x+y+z=0$

Ex : la droite passant par $(x:y:z) = (1:0:0)$ et $(x:y:z) = (0:0:1)$ $\boxed{y=0}$

est $\mathbb{P}(V)$ avec V le plan engendré par $(1,0,0)$ et $(0,0,1)$

$V = \{(0,0,0), (1,0,0), (0,0,1), (1,0,1)\}$

Une droite projective $\underset{(k^2\setminus\{0\})/\sim}{\mathbb{P}^1(k)}$ s'identifiera à $\underset{\mathbb{A}^1(k)}{k} \cup \{\infty\}$ ← "point à l'infini"

en identifiant $(x_0:x_1)$ à $\dfrac{x_1}{x_0}\in k$ si $x_0\neq 0$ $\quad \underbrace{(1:t)}_{t\in k}$ $\quad (0:1)$

"∞" si $x_0=0$ ($x_1\neq 0$ forcément)

Équations polynomiales dans l'espace projectif :

si $(x_0 : \cdots : x_n) \in \mathbb{P}^n(k)$, la valeur des coordonnées homogènes x_i n'a pas de sens en soi.
(car on peut toutes les multiplier par une même constante).

Déf : un polynôme $f \in k[t_0, \ldots, t_n]$ (en $n+1$ indéterminées) est dit **homogène de degré ℓ** lorsque tous ses monômes sont de degré total ℓ. [Ex : $t_0^3 + t_1^2 t_2 + t_1 t_2 t_3 + t_0 t_4^2$ est homogène de degré 3)

Rqe : dans ce cas, $f(\lambda x_0, \ldots, \lambda x_n) = \lambda^\ell f(x_0, \ldots, x_n)$ quels que soient $x_0, \ldots, x_n, \lambda \in k$

$x_0 - 1$ pas homogène
$(1:0:2) \in \mathbb{P}^2(\mathbb{R})$
$\shortparallel$
$(2:0:4)$
dépend du choix des coordonnées

Par conséquent, la question de savoir si $f(x_0, \ldots, x_n) = 0$ ou non a un sens pour $(x_0 : \cdots : x_n) \in \mathbb{P}^n(k)$.

On peut donc définir, si f est homogène

$$Z_{\mathbb{P}^n}(f)(k) := \{(x_0 : \cdots : x_n) \in \mathbb{P}^n(k) \mid f(x_0, \ldots, x_n) = 0\}$$

(ce qui a bien un sens d'après ce qu'on vient de dire)

ou juste $Z(f)$, ou encore "$\{f = 0\}$".

Si on a plusieurs polynômes homogènes (pas supposés de même degré) on note $Z(f_1, \ldots, f_r) := Z(f_1) \cap \cdots \cap Z(f_r) = $ "$\{f_1 = \cdots = f_r = 0\}$"

Remarque : les sous-espaces projectifs de $\mathbb{P}^n$ sont précisément les lieux définis par des équations linéaires, c'est-à-dire des f_i homogènes de degré 1 (= forme linéaire)

[polynôme $c_0 t_0 + \cdots + c_m t_n \longleftrightarrow$ forme linéaire $(x_0, \ldots, x_n) \longmapsto c_0 x_0 + \cdots + c_n x_n$]

En effet, $\mathbb{P}(V)$, si V est un s.e.v. de k^{n+1} est égal à $Z(\varphi_1, \ldots, \varphi_r)$ où $\varphi_1, \ldots, \varphi_r$ sont des formes linéaires sur k^{n+1} telles que $\ker(\varphi_1) \cap \cdots \cap \ker(\varphi_r) = V$

($\varphi_1, \ldots, \varphi_r$ engendrent $\underbrace{V^\perp}_{\{\text{formes linéaires s'annulant sur } V\}}$ dans le dual de k^{n+1})