2021-02-10 — ACCQ205

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

$f_1 = \cdots = f_r = 0$ où $f_1, \dots, f_r \in k[t_1, \dots, t_n]$

(polynômes (sur un corps) indéterminées (=variables))

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

$=: \underline{x}$

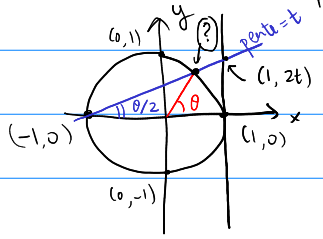
à travers la géométrie des objets qu'ils définissent.

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. $(\frac{3}{5}, \frac{4}{5})$ ← (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

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

$$(t^2+1)x^2 + 2t^2x + (t^2-1) = 0$$

ceci admet $x=-1$ 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 $\{x^2+y^2=1\}$ $(x \neq -1)$ par des fonctions rationnelles. Intérêt: ceci fonctionne sur "n'importe quel" corps. $(t^2 \neq -1)$ $(2 \neq 0)$

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

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

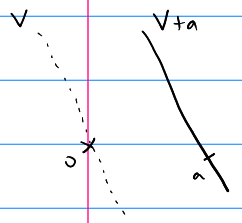
Déf: si k est un corps, on appelle "espace affine de dimension n" sur k et on note $\mathbb{A}^n(k)$ l'ensemble k^n.

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

$x_1, \dots, x_n$ = coordonnées (affines) de $\underline{x}$.

* **Sous-espaces affines** ("s.e.a.") de $\mathbb{A}^n(k)$: ce sont les $V + a$ avec V un k-s.e.v. de k^n (et l'ensemble vide) et $a \in k^n$

= translatés ($V + a$) des sous-espaces vectoriels ("s.e.v.")



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 (= éléments 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 $\{\lambda_1 a_1 + \dots + \lambda_r a_r \mid \lambda_1, \dots, \lambda_r \in k$ vérifiant $\lambda_1 + \dots + \lambda_r = 1\}$

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

$\lambda_1 + \dots + \lambda_r = 1$: "combinaison affine"

Transformations affines (inversibles) : ce sont les $\underline{x} \longmapsto M\underline{x} + b$, $k^n \longrightarrow k^n$ (= composée d'une transformation linéaire inversible et d'une translation $(y \mapsto y + b)$)

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

$b \in k^n$

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

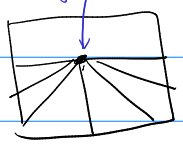
Ce sont les transformations bijectives qui préservent les combinaisons affines.

(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:

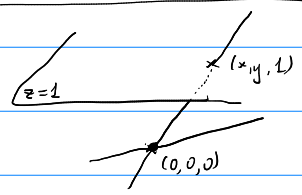
Notion apparue à la renaissance avec le développement et l'étude des lois de la perspective



→ 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 $(0,0,0)=0$ et $(x,y,1)$: toutes les droites par 0 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"



Def (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

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

$k^\times := \{z \in k \mid z \neq 0\}$ (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

$$(x_0,\dots,x_n) \sim (y_0,\dots,y_n)$$
$$:\Leftrightarrow \exists \lambda \in k^\times \ (y = \lambda \underline{x})$$
$$\Leftrightarrow \underline{y} \text{ et } \underline{x} \text{ sont colinéaires}$$
$$\Leftrightarrow x_i y_j = x_j y_i \text{ pour tous } i \text{ et } j.$$

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

Def (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) pour la relation en question.

On notera $(x_0 : \cdots : x_n)$ (deux points) l'élément de $\mathbb{P}^n(k)$ défini comme classe d'équivalence de $(x_0, \dots, x_n)$ pour $\sim$
(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 $(x_0 : \cdots : x_n) = (y_0 : \cdots : y_n)$ si $\exists \lambda \in k^\times \ \forall i \ (y_i = \lambda x_i)$

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 un.
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 "$\mathbb{P}^n(k) = \underbrace{\mathbb{A}^n(k)}_{x_0 \neq 0} \cup \underbrace{\mathbb{P}^{n-1}(k)}_{x_0 = 0}$"

$\mathbb{A}^n(k)$: "points affines" / "points finis" (?) / "points à distance finie"

$\cup$: union disjointe

$\mathbb{P}^{n-1}(k)$: "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 ou comme $\{x_0 \neq 0\}$ qui fait naître cette distinction.

→ corps fini à q éléments

* Nombre de point de $\mathbb{P}^n(\mathbb{F}_q)$?

Deux méthodes de calcul :

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

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

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

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

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 pour $\sim$ des points (non nuls) de V.

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

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

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

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

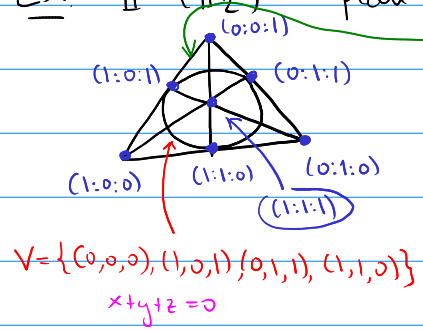
Par $m=1$ on parle de droite projective, par $m=2$ de plan projectif, etc.

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

à savoir $\mathbb{P}(V)$ si V est le plan vectoriel engendré par x, y les vecteurs de coordonnés des points en question

$\underbrace{(\mathbb{F}_2^3 \setminus \{0\})/\sim}_{=}$

Ex : $\mathbb{P}^2(\mathbb{F}_2)$ "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 $(x:y:z) = (0:0:1)$ (où $y=0$) est $\mathbb{P}(V)$ avec V le plan engendré par $(1,0,0)$ et $(0,0,1)$

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

$\underbrace{(k^2 \setminus \{0\})/\sim}_{=}$ $\quad \mathbb{A}^1(k)$ ← "point à l'infini"

Une droite projective $\mathbb{P}^1(k)$ s'identifiera à $k \cup \{\infty\}$

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

"∞" si $x_0 = 0$ $\quad (0:1)$ ($x_1 \neq 0$ 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 $f \in k[t_0, \dots, t_n]$ (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]

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

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

On peut donc définir, si f est homogène

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

(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 $Z(f_1, \dots, f_r) := Z(f_1) \cap \cdots \cap Z(f_r) = "\{f_1 = \cdots = f_r = 0\}"$

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

[polynôme $c_0 t_0 + \cdots + c_n t_n$ $\longleftrightarrow$ forme linéaire $(x_0, \dots, x_n) \mapsto c_0 x_0 + \cdots + c_n x_n$]

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

($\varphi_1, \dots, \varphi_r$ engendrent $V^\perp$ dans le dual de k^{n+1})

($V^\perp$ = {formes linéaires s'annulant sur V})

$x_0 - 1$ pas homogène

$(1 : 0 : 2) \in \mathbb{P}^2(\mathbb{R})$

$=$

$(2 : 0 : 4)$

dépend des deux coordonnées

2021-02-17

Rappel. espace projectif de dimension n sur un corps k

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

$\sim$: "être colinéaire"

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

($x_0, \ldots, x_n$ non tous nuls ; $y_0, \ldots, y_n$ non tous nuls)

On peut voir $\mathbb{P}^n(k) = \mathbb{A}^n(k) \cup H_\infty$

- $\mathbb{A}^n(k)$: espace affine k^n (on identifie $(x_1, \ldots, x_n) \in \mathbb{A}^n(k)$ avec $(1 : x_1 : \cdots : x_n) \in \mathbb{P}^n(k)$, i.e. $(x_0 : \cdots : x_n) \in \mathbb{P}^n(k)$ avec $x_0 \neq 0$ avec $(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0}) \in \mathbb{A}^n(k)$)
- H_∞ : "hyperplan à l'infini" $\{x_0 = 0\}$, identifiable à un $\mathbb{P}^{n-1}$

Cette construction ajoute un "point à l'infini" à toute direction de droites parallèles entre elles dans $\mathbb{A}^n$.

Sous-espaces projectifs de dim m de $\mathbb{P}^n(k)$: ce sont les $\mathbb{P}(V) := (V \setminus \{0\}) / \sim$ où V est un s.e.v de k^{n+1} de dimension $m+1$.

(Si $m = 1$, "droite", si $m = n-1$, "hyperplan")

Description "implicite" : $\{\varphi = 0\}$ définit un hyperplan si φ forme linéaire $\neq 0$ sur k^{n+1}

(application linéaire $k^{n+1} \to k$) $(x_0, \ldots, x_n) \longmapsto c_0 x_0 + \cdots + c_n x_n$

= polynôme homogène de degré 1 en $t_0, \ldots, t_n$

Transformations projectives ou groupe projectif linéaire :

Si $M \in GL_{n+1}(k)$ est une matrice $(n+1) \times (n+1)$ inversible, ou, ce qui revient au même, une application linéaire bijective $k^{n+1} \to k^{n+1}$, alors on peut définir $[M] : \mathbb{P}^n(k) \to \mathbb{P}^n(k)$

obtenue en appliquant M aux coordonnées $(x_0 : \cdots : x_n)$

autrement dit, si $M = (a_{ij})_{i=0,\ldots,n}^{j=0,\ldots,n}$,

$[M]$ envoie $(x_0 : \cdots : x_n)$ sur $\left(\sum_{j=0}^n a_{0j} x_j : \cdots : \sum_{j=0}^n a_{nj} x_j\right)$

Ces applications s'appellent "transformations projectives" ou "automorphismes linéaires" de $\mathbb{P}^n(k)$.

Une transformation projective envoie bien sûr les sous-espaces projectifs sur des sous-espaces projectifs.

(Notamment, une transformation projective envoie points alignés sur points alignés)

Bien sûr, $[M_1 M_2] = [M_1] \circ [M_2]$ si M_1, M_2 deux matrices inversibles.

Le groupe $PGL_{n+1}(k)$ des transformations projectives de $\mathbb{P}^n$ est donc $GL_{n+1}(k) / k^\times$ où $k^\times = \{$matrices λI_{n+1} d'homothétie avec $\lambda \neq 0\}$

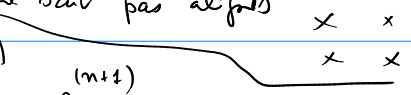
À quelle condition sur $n+1$ points de $\mathbb{P}^n$, disons $x^{(0)}, \dots, x^{(n)} \in \mathbb{P}^n(k)$, sont-ils situés sur un même hyperplan ? (un hyperplan = un $\mathbb{P}(V)$ avec V de dim $n \subset k^{n+1}$)

En remarquant que les coordonnés $x^{(i)} = (x_0^{(i)} : \dots : x_n^{(i)})$, ceci est le cas ssi les vecteurs $(x_j^{(i)})_j \in k^{n+1}$ ne sont pas libres c'est-à-dire $\boxed{\det (x_j^{(i)}) = 0}$

↑ cette condition ne dépend pas du choix des coordonnés représentant les $x^{(i)}$ grâce à la multilinéarité du déterminant

Base projective de $\mathbb{P}^n(k)$: c'est par définition $n+2$ points tels que $n+1$ quelconques d'entre eux ne soient pas situés sur un même hyperplan.

(Par exemple, pour $n=2$, une base projective = 4 points dont 3 quelconques ne sont pas alignés ; pour $n=1$, une base projective = 3 points distincts)



Exemple : la "base standard" de $\mathbb{P}^n(k)$, $e^{(0)}, \dots, e^{(n+1)}$ est formée des points $e^{(i)} := (0 : \dots : 0 : 1 : 0 : \dots : 0) \in \mathbb{P}^n$ pour $0 \le i \le n$ (1 à la i-ième coordonnée) et du point $e^{(n+1)} := (1 : \dots : 1)$

$$\begin{pmatrix} 1 & & 0 & 1 \\ & \ddots & & \vdots \\ 0 & & 1 & 1 \end{pmatrix}$$ (matrice $(n+1) \times (n+2)$)

← (vérifier : tout déterminant $(n+1)\times(n+1)$ obtenu en effaçant une colonne est $\neq 0$)

Rque : une transformation projective envoie une base sur une base.

Prop : si $x^{(0)}, \dots, x^{(n+1)}$ est une base de $\mathbb{P}^n$,

il existe $[M] \in PGL_{n+1}(k)$ unique (transformation projective) envoyant la base standard $e^{(0)}, \dots, e^{(n+1)}$ sur $x^{(0)}, \dots, x^{(n+1)}$ c'est-à-dire $[M]\, e^{(i)} = x^{(i)}$

Dém : puisque $\det(x_j^{(i)})_{i=0,\dots,n}^{j=0,\dots,n} \neq 0$, les $x_j^{(i)}$ définissent une matrice $(n+1)\times(n+1)$ inversible $P = (x_j^{(i)})$ donc une transformation projective, et on a $[P]\, e^{(i)} = x^{(i)}$ pour $0 \le i \le n$.

Il reste à fixer l'image de $e^{(n+1)}$ → $(1:\dots:1)$

Considérons $z := [P^{-1}]\, x^{(n+1)}$, disons $z = (z_0 : \dots : z_n)$. (qui contient $e^{(i)}$ pour $i \neq j$, $0 \le i \le n$)

Remarque : z n'est pas sur l'hyperplan $\{x_j = 0\}$ (i.e. $z_j \neq 0$).

En effet, si c'était le cas, l'image par $[P]$ de z, $e^{(i)}$ pour $i \neq j$ $(0 \le i \le n)$ c'est-à-dire $x^{(i)}$ pour $i \neq j$ $(0 \le i \le n+1)$, seraient sur un même hyperplan

connaissant le fait que $x^{(0)}, \dots, x^{(n+1)}$ est une base projective.

On appelle Q la matrice $\mathrm{diag}(z_0, \dots, z_n)$, $Q = \begin{pmatrix} z_0 & & 0 \\ & \ddots & \\ 0 & & z_n \end{pmatrix}$ inversible car on vient de voir $z_j \neq 0$. On pose $M = PQ$.

$[Q]e^{(n+1)} = z$ donc $[M]e^{(n+1)} = [P]z = x^{(n+1)}$, et $[Q]e^{(i)} = e^{(i)}$ donc $[M]e^{(i)} = x^{(i)}$

Unicité: si $[M]e^{(i)} = x^{(i)}$ et $[M']e^{(i)} = x^{(i)}$ aussi, alors $[M'^{-1}M]e^{(i)} = e^{(i)}$:

ceci montre que $M'^{-1}M$ est diagonale (sa i-ième colonne n'a qu'un élément $\neq 0$ sur la i-ième ligne) et comme $[M'^{-1}M]e^{(n+1)} = e^{(n+1)}$, on voit que cette diagonale est proportionnelle à $(1, \dots, 1)$, donc $M'^{-1}M$ est une matrice λI_n, qui est donc l'identité sur $\mathbb{P}^n$, $[M'^{-1}M] = 1 \in PGL_{n+1}(k)$. □

Corollaire: si $x^{(0)}, \dots, x^{(n+1)}$ et $y^{(0)}, \dots, y^{(n+1)}$ sont deux bases projectives de $\mathbb{P}^n$, il existe une unique transformation projective $[M] \in PGL_{n+1}(k)$ envoyant l'une sur l'autre.

(Ceci est utile par, par exemple, "envoyer des points à l'infini" ou au contraire éviter que des points soient à l'infini.)

Corollaire: (A) n'importe quel point de $\mathbb{P}^n(k)$ peut être complété en une base projective (si $x \in \mathbb{P}^n(k)$, il existe une base projective $x^{(0)}, \dots, x^{(n+1)}$ avec $x^{(0)} = x$)

(B) Si $x, y \in \mathbb{P}^n(k)$, il existe une transformation projective envoyant x sur y.

Dém: (A) Si $x = (x_0 : \dots : x_n)$, on peut compléter le vecteur $(x_0, \dots, x_n) \in k^{n+1}$ en une base de k^{n+1}, ceci forme une base $e^{(0)}, \dots, e^{(n)}$, quitte à effectuer une transformation linéaire, on peut supposer que c'est la base standard de k^{n+1}, qu'on peut alors compléter en base standard de $\mathbb{P}^n(k)$.

(B) On complète x et y en des bases $x^{(0)}, \dots, x^{(n+1)}$ et $y^{(0)}, \dots, y^{(n+1)}$ de $\mathbb{P}^n$ et d'après le corollaire précédent on peut envoyer l'une sur l'autre, donc en particulier x sur y par une transformation projective. □

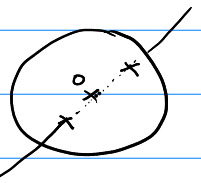
Moralité: $\mathbb{P}^n$ est "homogène" au sens où tous ses points sont semblables. ("tous ses points se valent")

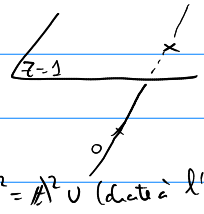
Comment visualiser $\mathbb{P}^2$? On l'a défini comme $(k^3 \setminus \{0\})/\sim$

(on implement l'ensemble des droites de k^3)

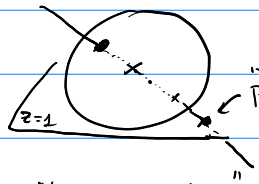
Si $k = \mathbb{R}$, on peut aussi voir $\mathbb{P}^2(\mathbb{R})$ comme la sphère unité sur laquelle on a identifié les points antipodaux.

("antipodaux" = "symétriques par rapport à l'origine"





$\mathbb{P}^2 = \mathbb{A}^2 \cup$ (droite à l'infini)



"projection gnomonique" de la sphère (modulo antipodie) (mais l'équateur) sur le plan (affine)

Cette projection envoie les "grands cercles" sur des droites du plan.

Calculs dans $\mathbb{P}^2(k)$

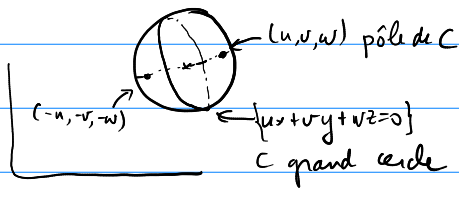
Les points de $\mathbb{P}^2(k)$ sont des triplets $(x:y:z)$ avec x, y, z non tous nuls modulo multiplication par une constante commune.

(Dans le cas de $\mathbb{P}^2(\mathbb{R})$, on peut normaliser par $x^2+y^2+z^2=1$ (c'est-à-dire diviser toutes les coordonnées par $\sqrt{x^2+y^2+z^2}$), ce qui revient justement à se ramener à la sphère)

Les droites dans $\mathbb{P}^2(k)$ sont de la forme $\{ux+vy+wz=0\}$ avec $u, v, w \in k$ non tous nuls, modulo multiplication par une constante. On écrira $[u:v:w]$ pour la droite en question.

Moralité : les droites de $\mathbb{P}^2$ peuvent se voir comme les points d'un autre $\mathbb{P}^2$ (appelé le $\mathbb{P}^2$ "dual").

Dans le cas de $\mathbb{P}^2(\mathbb{R})$ on comme une sphère modulo antipodie, ceci revient à voir un grand cercle à travers les coordonnées (u,v,w) de ses "pôles"



- Le point $(x:y:z)$ est sur la droite $[u:v:w]$ ssi $ux+vy+wz=0$ (← définition)
- La droite reliant $(x_1:y_1:z_1)$ et $(x_2:y_2:z_2)$ est donnée par:

$$\det\begin{pmatrix} x_1 & x_2 & x \\ y_1 & y_2 & y \\ z_1 & z_2 & z \end{pmatrix} = 0 \quad \text{c'est à dire} \quad [y_1z_2 - z_1y_2 : z_1x_2 - x_1z_2 : x_1y_2 - y_1x_2]$$

- Le point d'intersection de $[u_1:v_1:w_1]$ et $[u_2:v_2:w_2]$ est donné par:

$$(v_1w_2 - w_1v_2 : w_1u_2 - u_1w_2 : u_1v_2 - v_1u_2)$$

Le cas de $\mathbb{P}^1$: on peut voir $\mathbb{P}^1(k)$ comme les $(x_0:x_1)$ avec x_0, x_1 non tous deux nuls, modulo $\sim$

on préfère généralement ne retenir que $\frac{x_1}{x_0}$ qui peut être soit un élément de $\mathbb{A}^1(k)$, soit le symbole spécial "∞" pour le point à l'infini: $\mathbb{P}^1(k) = \mathbb{A}^1(k) \cup \{\infty\}$.

Les transformations projectives sont de la forme

$$(PGL_2(k)) \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} x_0 \\ x_1 \end{pmatrix} \longmapsto \begin{pmatrix} ax_0+bx_1 \\ cx_0+dx_1 \end{pmatrix}$$

$$\frac{x_1}{x_0} \longmapsto \frac{cx_0+dx_1}{ax_0+bx_1}$$

abus de notation

$$t \longmapsto \frac{c+dt}{a+bt} \qquad \text{"homographie" de } \mathbb{P}^1$$

$$(\infty \longmapsto \tfrac{d}{b} \text{ implicitement})$$

Birapport sur $\mathbb{P}^1$:

Déf: si a, b, c, d sont quatre points distincts de $\mathbb{P}^1$, le birapport $(a, b; c, d)$ de ces quatre points est (l'élément de $\mathbb{P}^1$) image de d par la transformation projective (unique!) envoyant a sur ∞, b sur 0 et c sur 1

(noter que a, b, c trois points distincts et $\infty, 0, 1$ sont des bases projectives de $\mathbb{P}^1$ $(0:1), (1:0), (1:1)$ (presque) la base standard)

Autrement dit,

$$\mathbb{P}^1 \longrightarrow \mathbb{P}^1$$
$$a \longmapsto \infty$$
$$b \longmapsto 0$$
$$c \longmapsto 1$$
$$d \longmapsto (a, b; c, d)$$

On a donc trivialement $(\infty, 0; 1, t) = t$ pour tout $t \in \mathbb{P}^1 \setminus \{\infty, 0, 1\}$.

Le birapport est invariant par transformations projectives

(si $[M] \in PGL_2(k)$, $([M]a, [M]b; [M]c, [M]d) = (a,b;c,d)$

en effet $\mathbb{P}^1 \xrightarrow{[M^{-1}]} \mathbb{P}^1 \longrightarrow \mathbb{P}^1$

$[M]a \longmapsto a \longmapsto \infty$
$[M]b \longmapsto b \longmapsto 0$
$[M]c \longmapsto c \longmapsto 1$
$[M]d \longmapsto d \longmapsto (a,b;c,d)$)

Formule explicite : $(a,b;c,d) = \dfrac{(c-a)(d-b)}{(d-a)(c-b)}$ ← abus de notation (formule vaut "en général" mais où il faut distinguer des cas particuliers par ∞, ...)

Un peu de géométrie sur $\mathbb{P}^2$:

on peut montrer que $\mathbb{P}^2(k)$ vérifie les "axiomes" suivants

- Par deux points distincts passe une unique droite.
- Deux droites distinctes se coupent en un unique point. (duaux)
- Il existe au moins trois points non alignés.
- Chaque droite contient au moins trois points.
- Théorème de Pappus

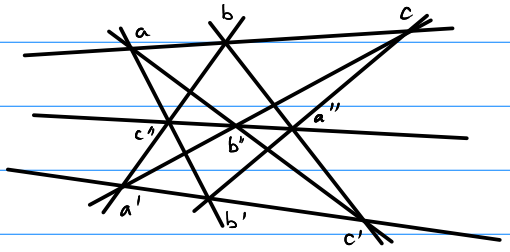
si a,b,c alignés

a',b',c' alignés

et $a'' := bc' \wedge b'c$ (intersection ; droite reliant b' à c)

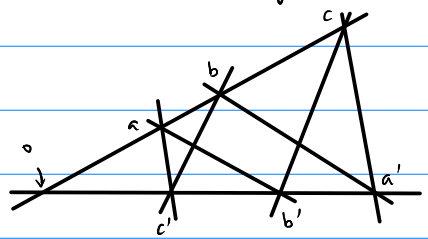
$b'' := ca' \wedge c'a$

$c'' := ab' \wedge a'b$ alors a'', b'', c'' alignés.



Ex de démonstration du théorème de Pappus en "envoyant à l'infini" certains points :

On choisit une transformation projective qui envoie a'' et b'' à l'infini :



on se ramène à montrer le théorème affine suivant :

si a,b,c alignés, a',b',c' alignés

et $bc' // b'c$, $ca' // c'a$ alors $ab' // a'b$

Dim affine : $\dfrac{oc}{ob} = \dfrac{ob'}{oc'}$ (Thalès) et $\dfrac{oc}{oa} = \dfrac{oa'}{oc'}$ (Thalès)

d'où $\dfrac{ob}{oa} = \dfrac{oa'}{ob'}$ (en divisant) d'où (Thalès réciproque) □

2021-03-03

Dualité projective

Il y a une "symétrie" (dualité) entre points et droites dans $\mathbb{P}^2$ et plus généralement, dans $\mathbb{P}^n$ entre points et hyperplans

(et plus généralement entre s.e.p. de dim r et $n-1-r$).

En effet, si V est un k-espace vectoriel (de dimension $n+1$, disons) on a un espace vectoriel dual $V^* := \{$formes linéaires φ sur $V\}$

↳ applications linéaires $V \to k$

à ce moment, on dira que $\mathbb{P}(V)$ et $\mathbb{P}(V^*)$ sont des espaces projectifs "duaux". ↳ $(V\setminus\{0\})/\sim$

Si on veut (si $V = k^{n+1}$) on peut dire entre $\mathbb{P}^n$ de coordonnés $(x_0 : \cdots : x_n)$ et $\mathbb{P}^n$ de coordonnés $[u_0 : \cdots : u_n]$

où $u_0, \dots, u_n$ sont les coordonnés de la forme linéaire

$$(x_0, \dots, x_n) \longmapsto \sum u_i x_i$$

Les points de $\mathbb{P}(V^*)$ correspondent exactement aux hyperplans ($\{\varphi = 0\}$) de $\mathbb{P}(V)$

par exemple $[u_0 : \cdots : u_n]$ décrivant l'hyperplan $\{u_0x_0 + \cdots + u_nx_n = 0\}$.

Mais symétriquement, les hyperplans de $\mathbb{P}(V^*)$ correspondent aux points de $\mathbb{P}(V)$

Et plus généralement, si on a un s.e.p. de $\mathbb{P}(V)$, disons $\mathbb{P}(W) \subset \mathbb{P}(V)$

où $W \subset V$ est un s.e.v. de dimension $r+1$,

alors on lui associe $W^\perp = \{\varphi \in V^* : \varphi|_W = 0\} = \{$f.l. s'annulant sur $W\}$

ceci définit un s.e.p. $\mathbb{P}(W^\perp) \subseteq \mathbb{P}(V^*)$

$W^\perp$ est de dimension $(n+1) - (r+1) = n-r$

$\mathbb{P}(W^\perp)$ est de dimension $n-r-1$

Si $W_1 \subset W_2$ alors $W_1^\perp \supseteq W_2^\perp$

$\mathbb{P}(W_1) \subset \mathbb{P}(W_2)$ alors $\mathbb{P}(W_1^\perp) \supseteq \mathbb{P}(W_2^\perp)$

Dualité : à un espace projectif $\mathbb{P}(V)$ on associe un "projectif dual" $\mathbb{P}(V^*)$,

et les s.e.p. de dimension r de $\mathbb{P}(V)$ correspondent bijectivement

aux s.e.p. de dimension $n-1-r$ de $\mathbb{P}(V^*)$,

les inclusions entre s.e.p. sont inversées.

En particulier, si on prend un théorème de géométrie projective de $\mathbb{P}^2$ et qu'on échange "points" et "droites"

"droite reliant deux points" et "point d'intersection de deux droites"

"trois points alignés" et "trois droites concourantes", etc.

on obtient un (nouveau) théorème de géométrie projective.

- Théorème de Pappus

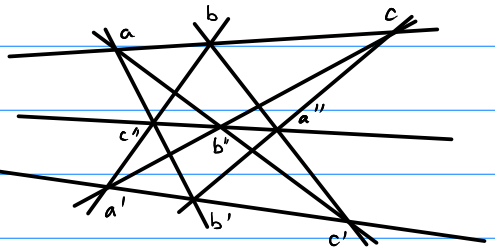
si a, b, c alignés

a', b', c' alignés

et $a'' := bc' \wedge b'c$ (intersection ; droite reliant b à c' ; droite reliant b' à c)

$b'' := ca' \wedge c'a$

$c'' := ab' \wedge a'b$ alors a'', b'', c'' alignés.



duaux

- Dual du théorème de Pappus.

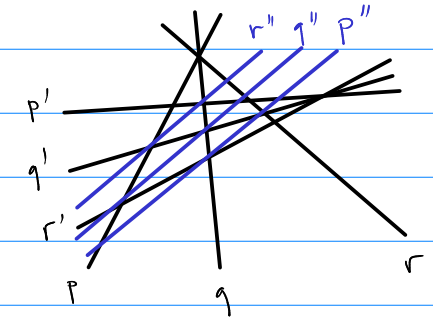
si p, q, r trois droites concourantes

p', q', r' trois droites concourantes

et $p'' = (q \wedge r') \vee (q' \wedge r)$

$q'' = (r \wedge p') \vee (r' \wedge p)$

$r'' = (p \wedge q') \vee (p' \wedge q)$ alors p'', q'', r'' concourants.



Retour sur le lien entre l'espace affine et l'espace projectif.

On a vu qu'on pouvait considérer

$$\mathbb{P}^n = \mathbb{A}^n \cup \mathbb{P}^{n-1}$$

($x_0 \neq 0$; disjoints ; $x_0 = 0$ "hyperplan à l'infini")

En fait, n'importe quel hyperplan peut être considéré comme "hyperplan à l'infini", par un découpage de ce genre.

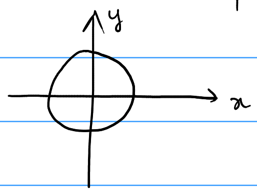
En effet, "tous les hyperplans se valent" car on a déjà vu que "tous les points se valent" (quels que soient $x, y \in \mathbb{P}^n$ il existe une transformation projective $[M] \in PGL_{n+1}(k)$ tq. $[M]x = y$)

("$PGL_{n+1}(k)$ agit transitivement sur $\mathbb{P}^n(k)$")

donc "tous les hyperplans se valent" par dualité.

Remarques sur cette décomposition "$\mathbb{P}^n = \mathbb{A}^n \cup$ (hyperplan à l'infini)".

Considérons l'équation $x^2+y^2=1$ dans $\mathbb{A}^2$ disons sur $k=\mathbb{R}$.



Si on veut maintenant voir $\mathbb{A}^2$ dans $\mathbb{P}^2$

$$(x,y) \longmapsto (1:x:y)$$

$$\left(\frac{X}{T},\frac{Y}{T}\right) \longleftarrow (T:X:Y) \qquad (T\neq 0)$$

$$(T:X:Y) = \left(1:\frac{X}{T}:\frac{Y}{T}\right)$$

l'équation $x^2+y^2=1$ du cercle se voit comme $\left(\frac{X}{T}\right)^2+\left(\frac{Y}{T}\right)^2=1$

soit, en chassant les dénominateurs, $X^2+Y^2-T^2=0$

polynôme homogène en T,X,Y

$\Longrightarrow$ définit un lieu dans $\mathbb{P}^2$

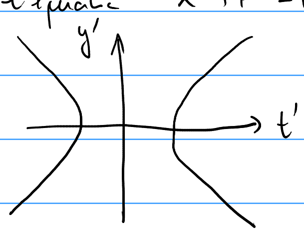
On l'appellera le "complété projectif" de $\{x^2+y^2=1\}$

Que se passe-t-il si on change d'hyperplan à l'infini ?

Disons qu'on prenne $X=0$ à la place de $T=0$ comme hyperplan à l'infini.

autrement dit, on veut considérer les coordonnées affines $\frac{T}{X}=:t'$ et $\frac{Y}{X}=:y'$

l'équation $X^2+Y^2-T^2=0$ est équivalente, pour $X\neq 0$, à $1+y'^2-t'^2=0$

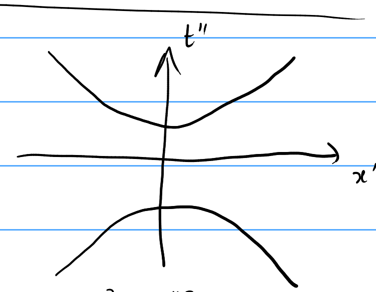


$t'^2-y'^2=1$

De même, si on prend $Y=0$ à l'infini

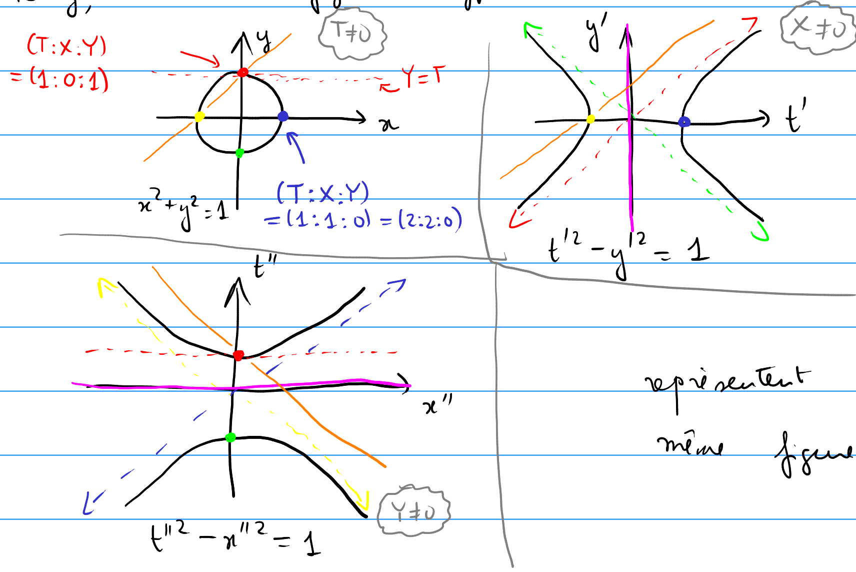
$t'':=\frac{T}{Y}$, $x'':=\frac{X}{Y}$

$x''^2+1-t''^2=1$



$t''^2-x''^2=1$

Bref, les trois figures affines suivantes



représentent trois {visions / morceaux} de la même figure projective $X^2+Y^2-T^2=0$

Remarques sur les transformations projectives par rapport à la décomposition

"$\mathbb{P}^n = \mathbb{A}^n \cup$ (hyperplan à l'infini)"

Si on a posé $H_\infty = \{x_0 = 0\}$, et $\mathbb{A}^n = \{x_0 \neq 0\}$ son complémentaire, quelles sont les transformations projectives $[M] \in PGL_{n+1}(k)$ qui stabilisent H_∞ ? (i.e. envoient H_∞ dans lui-même).

$M = \begin{pmatrix} * & 0 & \cdots & 0 \\ \vdots & & & \\ * & & & \end{pmatrix}$ quitte à multiplier par une constante $M = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ b & & A & \end{pmatrix}$

alors $M \begin{pmatrix} 1 \\ x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 1 \\ Ax+b \end{pmatrix}$ à $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$

autrement dit, on obtient une transformation affine (bijective) sur $\mathbb{A}^n$.

Les transformations affines (bijectives) de $\mathbb{A}^n$ sont exactement les transformations projectives de $\mathbb{P}^n$ qui stabilisent l'hyperplan à l'infini.

Morale : "la géométrie projective est celle des sous-espaces projectifs (par exemple pour $n=2$, des points et droites, alignement, concurrence, ...); et la géométrie affine est ce qui s'obtient en ajoutant l'idée d'un hyperplan à l'infini."

Équations algébriques dans l'espace affine et l'espace projectif

Pour l'instant, k est un corps qui sera bientôt supposé alg. clos.

Si $f \in k[t_1, \dots, t_n]$, on définit $Z(f)$ (ou $Z(f)(k)$ pour être précis) comme le lieu d'annulation de f, ("hypersurface $\{f=0\}$" dans $\mathbb{A}^n$),

à savoir : $Z(f)(k) := \{ \underline{x} := (x_1, \dots, x_n) \in k^n \mid f(x_1, \dots, x_n) = 0 \}$

Plus généralement, si $\mathcal{F} \subseteq k[\underline{t}] := k[t_1, \dots, t_n]$ est un ensemble de polynômes, on pose

$$Z(\mathcal{F}) := \bigcap_{f \in \mathcal{F}} Z(f) = \{ \underline{x} \in k^n \mid \forall f \in \mathcal{F} \ (f(\underline{x}) = 0) \}$$

Déf : une telle partie de $\mathbb{A}^n(k) := k^n$ s'appelle un <u>fermé de Zariski</u> ou <u>variété algébrique affine</u>.

Remarque évidente : si $\mathcal{F} \subseteq \mathcal{F}'$ alors $Z(\mathcal{F}) \supseteq Z(\mathcal{F}')$.

Rqe : si I est l'idéal engendré par $\mathcal{F}$, c'est-à-dire

$$I = \{ g_1 f_1 + \dots + g_s f_s \mid g_1, \dots, g_s \in k[\underline{t}] \text{ et } f_1, \dots, f_s \in \mathcal{F} \ (\text{et } s \in \mathbb{N}) \}$$

alors on a $Z(I) = Z(\mathcal{F})$.

[Dém : $Z(I) \subseteq Z(\mathcal{F})$ car $I \supseteq \mathcal{F}$, mais par ailleurs,

si $\underline{x} \in Z(\mathcal{F})$ et $f_1, \dots, f_s \in \mathcal{F}$ et $f = g_1 f_1 + \dots + g_s f_s \in I$

alors $f(\underline{x}) = 0$ car $f_i(\underline{x}) = 0$ pour $i = 1, \dots, s$, bref $\underline{x} \in Z(f)$.]

Bref, pour étudier les $Z(\mathcal{F})$ (fermés de Zariski), on peut se contenter d'étudier les $Z(I)$ avec $I \subseteq k[\underline{t}]$ <u>idéal</u>.

"Rappel" (Théorème de la base de Hilbert) :

tout idéal I de $k[\underline{t}]$ est engendré par un nombre fini d'éléments (il existe $f_1, \dots, f_s$ fixés tels que $I = \{ g_1 f_1 + \dots + g_s f_s \mid g_1, \dots, g_s \in k[\underline{t}] \}$)

↳ on a alors $Z(I) = Z(f_1, \dots, f_s) = Z(f_1) \cap \dots \cap Z(f_s)$

On peut donc aussi se contenter d'étudier les $Z(f_1, \dots, f_s)$.

On vient de définir $\mathcal{Z} : \{\text{ensemble de polynômes}\} \longrightarrow \{\text{ensemble de parts de } k^n\}$

On va maintenant définir une opération dans le sens contraire.

Si $E \subseteq k^n$ est une partie quelconque, on pose

$$\mathcal{I}(E) := \{ f \in k[\underline{t}] \mid \forall \underline{x} \in E \ (f(\underline{x}) = 0) \} = \{ f \in k[\underline{t}] \mid f|_E = 0 \}$$
$$= \{\text{polynômes s'annulant sur } E\}$$
$$= \bigcap_{\underline{x} \in E} \mathfrak{M}_{\underline{x}} \quad \text{où} \quad \mathfrak{M}_{\underline{x}} = \mathcal{I}(\{\underline{x}\}) = \{\text{polynômes s'annulant en } \underline{x}\}.$$

Remarque évidente : si $E \subseteq E'$ alors $\mathcal{I}(E) \supseteq \mathcal{I}(E')$.

Autre remarque : $\mathcal{I}(E)$ est un idéal de $k[\underline{t}]$ (car les $\mathfrak{M}_{\underline{x}}$ le sont :

si $f_1, \dots, f_s$ s'annulent en $\underline{x}$ alors $g_1 f_1 + \dots + g_s f_s$ aussi).

Quel est le rapport entre $\mathcal{Z}$ et $\mathcal{I}$???

Remarque-clé : dire que $E \subseteq \mathcal{Z}(F)$ signifie

"tous les éléments de F s'annulent en tous les points de E"

c'est-à-dire "$\forall f \in F \ \forall \underline{x} \in E \ (f(\underline{x}) = 0)$"

mais c'est aussi pareil que $F \subseteq \mathcal{I}(E)$.

Bref, $E \subseteq \mathcal{Z}(F) \iff F \subseteq \mathcal{I}(E)$

Manipulations formelles :

- si $F \subseteq k[\underline{t}]$, la remarque-clé appliquée à $E = \mathcal{Z}(F)$ donne $F \subseteq^{(1)} \mathcal{I}(\mathcal{Z}(F))$
- si $E \subseteq k^n$, la remarque-clé appliquée à $F = \mathcal{I}(E)$ donne $E \subseteq^{(2)} \mathcal{Z}(\mathcal{I}(E))$
- (1) + "$\mathcal{Z}$ renversant par l'inclusion" donne $\mathcal{Z}(F) \supseteq \mathcal{Z}(\mathcal{I}(\mathcal{Z}(F)))$

  (2) appliqué à $E = \mathcal{Z}(F)$ donne $\mathcal{Z}(F) \subseteq \mathcal{Z}(\mathcal{I}(\mathcal{Z}(F)))$ (par rel $F \subseteq k[\underline{t}]$)

  Bref, $\mathcal{Z}(F) = \mathcal{Z}(\mathcal{I}(\mathcal{Z}(F)))$
- De même, on a $\mathcal{I}(E) = \mathcal{I}(\mathcal{Z}(\mathcal{I}(E)))$ par rel $E \subseteq k^n$.

Ceci ne montre pas que $\mathcal{I}$ et $\mathcal{Z}$ sont des bijections réciproques en général.

Néanmoins ceci montre que $\mathcal{I}$ et $\mathcal{Z}$ sont des bijections réciproques entre

$$\left\{ \begin{array}{c} \text{les idéaux de } k[\underline{t}] \\ \text{de la forme } \mathcal{I}(E) \end{array} \right\} \underset{\mathcal{I}}{\overset{\mathcal{Z}}{\rightleftarrows}} \left\{ \begin{array}{c} \text{les fermés de Zariski} \\ \text{de } k^n \ (\text{les } \mathcal{Z}(F)) \end{array} \right\}$$

La question essentielle devient alors :

quels sont les idéaux de $k[\underline{t}]$ de la forme $\mathcal{I}(E)$?

peut-on les identifier ? les caractériser ?

(On vient de voir que I est un $\mathcal{I}(E)$ ssi $I = \mathcal{I}(\mathcal{Z}(I))$.)

Il y a au moins une condition nécessaire sur un idéal $I \subset k[t]$ pour vérifier cette condition ($I = \mathcal{I}(\mathcal{Z}(I))$) ou ce qui revient au même à savoir :

$$\exists E \subset k^n \ (I = \mathcal{I}(E))$$

Rappel : un idéal I d'un anneau A est un sous groupe $I \subset A$ pour l'addition ($0 \in I$, si $f_1, f_2 \in I$ alors $f_1 + f_2 \in I$ et si $f \in I$ alors $-f \in I$) qui vérifie de plus que si $g \in A$ et $f \in I$ alors $gf \in I$

On peut alors définir un anneau quotient dont les éléments sont les classes $h + I$ avec $h \in A$ ($h + I = \{h + f : f \in I\}$) avec l'addition $(h+I) + (h'+I) = (h+h') + I$ la multiplication $(h+I)(h'+I) = hh' + I$

On le note A/I.

anneau := anneau commutatif dans ce cours

On dit qu'un anneau A est

- (a) un corps lorsque $x \neq 0 \iff x$ est inversible ($\iff (\exists y \in A \ (xy = 1))$ $\iff$ $y \mapsto xy$ bijective $A \to A$)
- $\Downarrow$
- (b) intègre lorsque si $xy = 0$ alors $x = 0$ ou $y = 0$, et $0 \neq 1$; ou encore : $x \neq 0 \iff (y \mapsto xy$ est injective $A \to A)$
- $\Downarrow$
- (c) réduit lorsque $x^n = 0 \Rightarrow x = 0$ dans A ("pas de nilpotent autre que 0")

L'anneau "nul" (où l'unique anneau où $0 = 1$) n'est pas un corps

On en déduit trois conditions sur les idéaux :

on dit qu'un idéal $I \subset A$ est

- (a) maximal lorsque A/I est un corps
- $\Downarrow$
- (b) premier lorsque A/I est intègre
- $\Downarrow$
- (c) radical lorsque A/I est réduit.

Si on préfère, I est

- (a) maximal lorsque $(\forall x \in A)\ (x \notin I \iff \exists y \in A \ (xy - 1 \in I))$
- $\Downarrow$
- (b) premier lorsque $I \neq A$ et $(\forall x, y \in A)\ (xy \in I \Rightarrow x \in I$ ou $y \in I)$
- $\Downarrow$
- (c) radical lorsque $(\forall x \in A)(\forall n \in \mathbb{N})\ (x^n \in I \Rightarrow x \in I)$

Rque : il n'est pas difficile de voir que

I maximal $\iff I \neq A$ et I est maximal par l'inclusion

c'est-à-dire : si $I \subset J$ avec J idéal alors $\begin{cases} I = J \\ \text{ou} \\ J = A \end{cases}$

2021-03-10

Exemples d'idéaux :

(dans $\mathbb{Z}$) maximal : $5\mathbb{Z}$ est maximal car $\mathbb{Z}/5\mathbb{Z}$ est un corps ($\mathbb{F}_5$)

(plus généralement, $p\mathbb{Z}$ avec p un nombre premier) est maximal

premier : les mêmes, plus l'idéal $0 = \{0\} = (0) = 0\mathbb{Z}$

$\mathbb{Z}/0\mathbb{Z} = \mathbb{Z}$ est intègre (Kum. chinois)

radical : les mêmes, mais aussi $6\mathbb{Z}$ car $\mathbb{Z}/6\mathbb{Z} \simeq (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$

est réduit ; plus généralement, $p_1 \cdots p_r \mathbb{Z}$ avec p_i premiers distincts

est radical

(dans $k[x,y]$) maximal : $(x,y) = \{fx + gy : f, g \in k[x,y]\} = \{h \in k[x,y] : h$ n'a pas de terme constant$\}$

$= \{h \in k[x,y] : h(0,0) = 0\} = \{$polynômes s'annulant à l'origine$\}$

$k[x,y]/(x,y) \simeq k$ est un corps donc (x,y) est maximal

plus généralement, si $(x_0, y_0) \in k^2$, $(x - x_0, y - y_0) = \mathfrak{m}_{(x_0,y_0)}$

est l'idéal des polynômes s'annulant en (x_0, y_0)

$k[x,y]/\mathfrak{m}_{(x_0,y_0)} \simeq k$ par l'évaluation en (x_0, y_0)

$k[x,y] \ni f \longmapsto f(x_0, y_0) \in k$

Sont-ce les seuls ? En général non :

$\mathbb{R}[x,y]/(x^2+1, y) \simeq \mathbb{R}[x]/(x^2+1) \simeq \mathbb{C}$ est un corps

$\bar{x} \longmapsto \sqrt{-1}$ donc $(x^2+1, y) \subseteq \mathbb{R}[x,y]$ est maximal

(remarque : dans $\mathbb{C}[x,y]$, l'idéal (x^2+1, y) n'est pas maximal)

Idéaux premiers pas maximaux :

(y) : on a $k[x,y]/(y) \simeq k[x]$ intègre

(dans $k \neq 2$) (x^2+y^2-1) : on peut vérifier que x^2+y^2-1 est irréductible

et en déduire que $k[x,y]/(x^2+y^2-1)$ intègre

(remarque : $\mathbb{R}[x,y]/(x^2+y^2-1)$ peut s'identifier

à l'anneau des "polynômes trigonométriques"

$c + \sum_{k=1}^{N} a_k (\cos\theta)^k + \sum_{k=1}^{N} b_k (\sin\theta)^k$

par $\bar{x} \mapsto \cos\theta$, $\bar{y} \mapsto \sin\theta$)

Idéal radical pas premier : $(xy) = \{\sum c_{ij} x^i y^j : i \geq 1$ et $j \geq 1\}$

$k[x,y]/(xy)$ est réduit $= \{c + \sum_{i=1}^{N} a_i (\bar{x})^i + \sum_{i=1}^{N} b_i (\bar{y})^i\}$

Remarque essentielle: l'idéal $\mathcal{I}(E)$ est radical.

Autrement dit, si $f^m \in \mathcal{I}(E)$ alors $f \in \mathcal{I}(E)$

(C'est évident: si f^m est identiquement nul sur E alors f l'est.)

On appelle radical d'un idéal I (d'un anneau A) l'ensemble $\sqrt{I} := \{ f \in A \mid \exists m \geq 0 \ (f^m \in I) \}$

Il s'agit bien d'un idéal radical

Dém: $0 \in \sqrt{I}$; si $f, g \in \sqrt{I}$, donc $f^m \in I$, $g^n \in I$

$(f+g)^{m+n} \in I$ car en développant, tous les termes sont dans I

si $f \in \sqrt{I}$ et $g \in A$ alors $f^m \in I$ donc $(gf)^m = g^m f^m \in I$ donc $gf \in \sqrt{I}$

si $f^n \in \sqrt{I}$ alors $(f^n)^m = f^{mn} \in I$ donc $f \in \sqrt{I}$ □

Il s'agit du plus petit idéal radical contenant I.

Dém: si $J \supseteq I$ est un idéal radical, et si $f \in \sqrt{I}$, donc $f^m \in I$ alors $f^m \in J$ donc $f \in J$, bref $J \supseteq \sqrt{I}$. □

Bref, $\sqrt{I}$ est l'intersection de tous les idéaux radicaux contenant I.

(En fait on peut montrer que $\sqrt{I}$ est l'intersection de tous les idéaux premiers contenant I.)

Par ailleurs, si I est un idéal de $k[\underline{t}] := k[t_1, \dots, t_n]$ alors $\mathcal{Z}(I) = \mathcal{Z}(\sqrt{I})$ toujours parce que si f^m s'annule en $\underline{x}$ alors f s'annule en $\underline{x}$.

Bref, tout ceci montre qu'on a

$$\left\{ \begin{array}{c} \text{idéaux radicaux} \\ \text{de } k[\underline{t}] \end{array} \right\} \underset{\mathcal{I}}{\overset{\mathcal{Z}}{\rightleftarrows}} \left\{ \begin{array}{c} \text{fermés de Zariski} \\ \text{de } k^n \end{array} \right\}$$

$\mathcal{Z}$ est surjective et $\mathcal{Z} \circ \mathcal{I} = \mathrm{id}$

Malheureusement, si k n'est pas algébriquement clos, on n'a toujours pas des bijections réciproques.

Si k est algébriquement clos (rappel: ceci signifie que tout polynôme en une variable non constant a une racine, et donc se factorise en produit $c\prod_{x\in k}(t-x)^{n_x}$),

alors on a effectivement une bijection, en vertu du théorème suivant:

Théorème des zéros de Hilbert (Nullstellensatz)

(plusieurs formes)

Si k est un corps algébriquement clos

- "Nullstellensatz faible": si $\mathcal{Z}(I)=\emptyset$ pour $I\subset k[t]$ alors $I=(1)$ (idéal unité $k[t]$)

  De façon équivalente: si $\mathcal{Z}(f_1,\dots,f_r)=\emptyset$ (i.e. il n'existe pas x tq. $\forall i\ (f_i(x)=0)$) alors il existe $g_1,\dots,g_r\in k[t]$ tq. $g_1f_1+\dots+g_rf_r=1$.
- "Nullstellensatz fort": $\mathcal{Z}$ et $\mathcal{I}$ sont des bijections réciproques entre $\{$idéaux radicaux de $k[t]\}$ et $\{$fermés de Zariski de $k^n\}$
- "Lemme de Zariski" (?): les idéaux maximaux de $k[t]$ sont les $\mathfrak{m}_x:=\{f\in k[t]\mid f(x)=0\}=\mathcal{I}(\{x\})$ pour $x\in k^n$

L'hypothèse "k algébriquement clos" est essentielle.

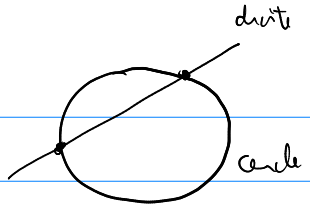
si k n'est pas algébriquement clos, il existe $f\in k[t]$ (une indéterminée) non constant et sans racine: on a alors $\mathcal{Z}(f)=\emptyset$ et pourtant l'idéal (f) engendré par f n'est pas (1).

Même si k n'est pas alg. clos, il existe une clôture algébrique c'est-à-dire un corps k^{alg} contenant k, alg. clos, et algébrique sur k c'est-à-dire que tout $x\in k^{alg}$ est racine d'un polynôme $f\in k[t]$ et $f\neq 0$. De plus, k^{alg} est unique à isomorphisme près par ces propriétés.

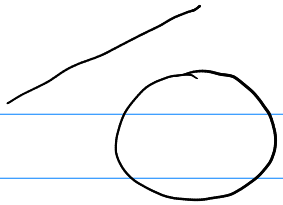
(Par exemple, la clôture algébrique de $\mathbb{R}$ est $\mathbb{C}$, celle de $\mathbb{Q}$ est $\{x\in\mathbb{C}: x \text{ est algébrique sur } \mathbb{Q}\}$ celle de $\mathbb{F}_q$ est $\bigcup_{n\geq 1}\mathbb{F}_{q^n}$.)

On va avoir tendance à étudier la géométrie algébrique sur k à travers k^{alg} (par avoir le NSS)

Ex:



2 points d'intersection réels



2 points d'intersection complexes conjugués

(Ex $\{x^2+y^2-1=0\}$ et $\{x=2\}$ se coupent en $(2, \sqrt{-3})$ et $(2, -\sqrt{-3})$)

$$Z(x^2+y^2-1,\ x-2)(\mathbb{C}) = \{(2,\sqrt{-3}),\ (2,-\sqrt{-3})\}$$

Si I est un idéal (radical) de $k[\underline{t}]$ avec k non alg. clos,

les éléments de $Z(I)(k) = \{\underline{x} \in k^n \mid \forall f \in I\ (f(\underline{x})=0)\}$

s'appelleront les k-points ou "points rationnels"

les éléments de $Z(I)(k^{alg}) = \{\underline{x} \in (k^{alg})^n \mid \forall f \in I\ (f(\underline{x})=0)\}$

s'appelleront les (k^{alg}-points) ou "points géométriques" de $Z(I)$. Le NSS assure que si $Z(I)$ n'a pas de point géométrique alors $I = (1)$

(en revanche, $Z(I)$ peut ne pas avoir de point rationnel, cf. ci-dessus).

Fonctions régulières et évaluation.

Soient I idéal radical de $k[\underline{t}]$ (k un corps quelconque).
Comment peut-on "voir" géométriquement l'anneau quotient $k[\underline{t}]/I$?
On a un morphisme d'anneaux "évaluation"

$$k[\underline{t}] \longrightarrow k^{Z(I)(k)} := \{\text{fonctions } Z(I)(k) \longrightarrow k\}$$
$$f \longmapsto \text{la fonction polynomiale définie par } f \text{ sur } Z(I)$$
$$(\underline{x} \longmapsto f(\underline{x}))$$

Si $f \in I$, par définition de $Z(I)$, l'évaluation est nulle
$(f(\underline{x}) = 0$ pour tout $\underline{x} \in Z(I))$

Ceci permet donc de passer au quotient et de définir

$$k[\underline{t}]/I \xrightarrow{ev} k^{Z(I)(k)}$$
$$f + I =: \overline{f} \longmapsto \text{idem } (\underline{x} \longmapsto f(\underline{x}))$$

Injectivité : si k est alg. clos, et si $f(\underline{x}) = 0$ pour tout $\underline{x} \in Z(I)$, alors $f \in \mathcal{I}(Z(I)) = I$ par le NSS, ce qui montre que ev ci-dessus est injective.

Bref, les éléments de $k[\underline{t}]/I$ peuvent se voir comme des fonctions sur $Z(I)$ (sur $Z(I)(k)$ sur $Z(I)(k^{alg})$...)
à savoir les restrictions à $Z(I)$ des fonctions polynomiales sur $\mathbb{A}^n$.
Les éléments de $k[\underline{t}]/I$ s'appellent aussi "fonctions régulières" sur $Z(I)$.

Ex : Les fonctions régulières sur $\{x^2+y^2-1\}$ sont les éléments de $k[x,y]/(x^2+y^2-1)$
(par exemple, sur $\mathbb{R}$, les restrictions des polynômes de $\mathbb{R}[x,y]$ au cercle $\{x^2+y^2=1\}$ sont les "polynômes trigonométriques", éléments de $\mathbb{R}[x,y]/(x^2+y^2-1) \simeq \mathbb{R}[\cos\theta, \sin\theta]$.

Retour sur les idéaux maximaux, premiers et radicaux.

On a vu que si k est alg. clos, on a des bijections réciproques

$$\{\text{idéaux radicaux de } k[\underline{t}]\} \underset{\mathcal{I}}{\overset{\mathcal{Z}}{\rightleftarrows}} \{\text{fermés de Zariski de } k^n\}$$

À quoi correspondent les idéaux $\begin{cases}\text{maximaux}\\ \text{premiers}\end{cases}$ dans cette correspondance ?

Pour les idéaux maximaux, on a vu la réponse (Lemme de Zariski) :

ils sont de la forme $\mathfrak{m}_{\underline{x}} := \mathcal{I}(\{\underline{x}\})$

(où $\mathcal{Z}(\mathfrak{m}_{\underline{x}}) = \{\underline{x}\}$)

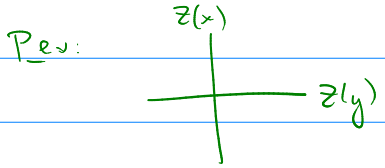
Bref, $\{\text{idéaux maximaux de } k[\underline{t}]\} \underset{\mathcal{I}}{\overset{\mathcal{Z}}{\rightleftarrows}} \{\text{singletons de } k^n\}$

Pour les idéaux premiers, on introduit la déf :

Déf : un fermé de Zariski E est dit **irréductible** lorsque si $E = E_1 \cup E_2$ où E_1, E_2 sont des fermés de Zariski alors soit $E_1 = E$ soit $E_2 = E$.

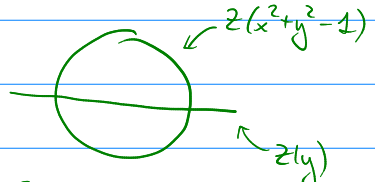
Contre-exemples : la réunion de deux fermés de Zariski non inclus l'un dans l'autre.

Ex :



$\mathcal{Z}(xy) = \mathcal{Z}(x) \cup \mathcal{Z}(y)$

pas irréductible



$\mathcal{Z}(x^2y+y^3-y) = \mathcal{Z}(x^2+y^2-1) \cup \mathcal{Z}(y)$

pas irréductible

En revanche, $\mathcal{Z}(x)$, $\mathcal{Z}(y)$, $\mathcal{Z}(x^2+y^2-1)$ sont irréductibles.

Prop : $E \subseteq k^n$ est irréductible ssi $\mathcal{I}(E)$ est un idéal premier.

Rque : l'idéal engendré par un seul $f \in k[\underline{t}]$ est premier ssi f est irréductible.

Bref, on a des bijections $\underset{\mathcal{I}}{\overset{\mathcal{Z}}{\rightleftarrows}}$ entre :

$\{\text{idéaux radicaux}\}$ et $\{\text{fermés de Zariski}\}$

$\Uparrow$ $\qquad$ $\Uparrow$

$\{\text{idéaux premiers}\}$ et $\{\text{fermés de Zariski irréductibles}\}$

$\Uparrow$ $\qquad$ $\Uparrow$

$\{\text{idéaux maximaux}\}$ et $\{\text{singletons}\}$

Topologie de Zariski :

Prop : les fermés de Zariski de k^n (k corps quelconque) vérifient les propriétés suivantes :

(i) $\emptyset$ et k^n sont des fermés

(ii) si $(F_i)_{i\in\Lambda}$ sont fermés alors $\bigcap_{i\in\Lambda} F_i$ est fermée

(iii) si $F_1, \dots, F_n$ sont fermés alors $F_1 \cup \dots \cup F_n$ est fermé.

Dém : (i) $\emptyset = Z(1)$, $k^n = Z(0)$

(ii) Si $F_i = Z(I_i)$ pour tout $i\in\Lambda$ avec I_i un idéal, on a $\bigcap_{i\in\Lambda} F_i = Z\left(\sum_{i\in\Lambda} I_i\right)$ où $\sum_{i\in\Lambda} I_i$ = idéal engendré par $\bigcup_{i\in\Lambda} I_i$
$= \left\{ \sum_{i\in\Lambda} f_i \text{ avec } f_i \in I_i \right.$ tous nuls sauf un nombre fini$\left.\right\}$

En effet, si $I := \sum_{i\in\Lambda} I_i$, on a
$I \supseteq I_i$ donc $Z(I) \subseteq Z(I_i)$ donc $Z(I) \subseteq \bigcap_{i\in\Lambda} Z(I_i)$

Réciproquement, si $\underline{x} \in \bigcap_{i\in\Lambda} Z(I_i)$ et $f \in I$,
donc $f = \sum_{i\in\Lambda} f_i$ avec $f_i \in I_i$, alors $f_i(\underline{x}) = 0$ $\forall i$ donc $f(\underline{x}) = 0$
donc $\underline{x} \in Z(I)$, ceci montre $\bigcap_{i\in\Lambda} Z(I_i) \subset Z(I)$,
bref, $Z(I) = \bigcap_{i\in\Lambda} Z(I_i)$ est bien un fermé de Zariski.

(iii) Par récurrence sur n, il suffit de montrer que si F_1 et F_2 sont fermés alors $F_1 \cup F_2$ est fermé.
Donc $F_1 = Z(I_1)$ et $F_2 = Z(I_2)$.
Montrons que $F_1 \cup F_2 = Z(I_1 I_2)$
où $I_1 I_2$ = l'idéal engendré par les $f_1 f_2$ pour $f_1 \in I_1$ et $f_2 \in I_2$.
On a $I_1 I_2 \subseteq I_1$ donc $Z(I_1 I_2) \supseteq Z(I_1) = F_1$
de même $Z(I_1 I_2) \supseteq F_2$
donc $Z(I_1 I_2) \supseteq F_1 \cup F_2$

Réciproquement, si $\underline{x} \in Z(I_1 I_2)$, et si $\underline{x} \notin F_1$
alors il existe $f_1 \in I_1$ tel que $f_1(\underline{x}) \neq 0$.
Si maintenant $f_2 \in I_2$, on a $(f_1 f_2)(\underline{x}) = 0$ car $f_1 f_2 \in I_1 I_2$
comme $f_1(\underline{x}) \neq 0$, on a $f_2(\underline{x}) = 0$ ($f_1(\underline{x}) f_2(\underline{x}) \in k$)
ceci montre $\underline{x} \in F_2$. Ceci montre $Z(I_1 I_2) \subseteq F_1 \cup F_2$.

Remarque : la démonstration marche aussi bien avec $I_1 \cap I_2$ qu'avec $I_1 I_2$ (on a $Z(I_1 I_2) = Z(I_1 \cap I_2)$). □

"Z."

Déf:
- un ouvert de Zariski est le complémentaire d'un fermé de Zariski,
- un voisinage (de Z.) de $x \in k^n$ est une partie de k^n contenant un ouvert contenant x.
- l'adhérence (de Z.) de $E \subseteq k^n$ est le plus petit fermé de Z. contenant E = l'intersection de tous les fermés de Z. contenant E

Rqe: l'adhérence de Z. de E est simplement $Z(J(E))$ [Dém: ceci est bien un fermé de Z. contenant E, et si $Z(I) \supseteq E$ alors $I \subseteq J(E)$ donc $Z(I) \supseteq Z(J(E))$.]

2021-03-24

Fermés et ouverts de Zariski dans $\mathbb{P}^n$ (espace projectif).

Rappel: un polynôme $f \in k[t_0, \dots, t_n] =: k[\underline{t}]$ est dit homogène de degré l lorsque tous ses monômes sont de degré total l.

On peut alors définir $Z(f) = \{(x_0 : \cdots : x_n) \in \mathbb{P}^n \mid f(x_0, \dots, x_n) = 0\}$

Si $f \in k[\underline{t}]$ et $l \in \mathbb{N}$ on appelle partie homogène de degré l de f la somme des termes de degré total l de f.

On la note $f^{[l]}$. Ex: si $f = x^2y - 2z^3 + x^2 + 1$ alors $f^{[3]} = x^2y - 2z^3$, $f^{[2]} = x^2$, $f^{[1]} = 0$, $f^{[0]} = 1$

Déf: un idéal $I \subset k[\underline{t}]$ est dit homogène lorsqu'il vérifie les deux conditions équivalentes suivantes:
- $*$ I est engendré par des polynômes homogènes (pas forcément de même degré)
- $*$ Si $f \in I$ et $l \in \mathbb{N}$ alors $f^{[l]} \in I$.

Déf: si I est un tel idéal (homogène), on définit $Z(I) \subseteq \mathbb{P}^n$ par (définitions équivalentes) $Z(I) = Z(f_1) \cap \cdots \cap Z(f_r)$ où $f_1, \dots, f_r$ sont homogènes engendrant I

ou si on préfère, $Z(I) = \bigcap_{\substack{f \in I \\ f \text{ homogène}}} Z(f)$

Ce $Z(I) \subset \mathbb{P}^n$ est appelé fermé de Zariski (projectif) défini par I.
On devrait le noter plus précisément $Z_{\mathbb{P}^n}(I)$,
par ailleurs, comme dans le cas affine, il faudrait distinguer

$$Z(I)(k) = \{\text{points "rationnels" (ou } k\text{-points)}\} = \{x \in \mathbb{P}^n(k) \mid f(x)=0 \text{ si } f \text{ homogène} \in I\}$$

(si k n'est pas algébriquement clos ($k \neq k^{alg}$))

et $Z(I)(k^{alg}) = \{\text{points "géométriques" (ou } k^{alg}\text{-points)}\}$
$= \text{idem sur } k^{alg}$ (clôture algébrique)

On définit aussi, si $E \subset \mathbb{P}^n(k)$, un idéal homogène

$J(E) :=$ idéal engendré par tous les $f \in k[\underline{t}]$ homogènes tels que $Z(f) \supseteq E$

En fait, on peut vérifier que $f \in k[\underline{t}]$ (quelconque) est dans $J(E)$
si $f^{[l]}$ s'annule sur E pour tout $l \in \mathbb{N}$.

Rque: si $I = (x_0, \dots, x_n)$ ou plus généralement $I = (x_0^l, \dots, x_n^l)$ alors $Z_{\mathbb{P}^n}(I) = \emptyset$
car les coordonnées d'un point de $\mathbb{P}^n$ sont non toutes nulles.

Déf: un idéal I homogène de $k[\underline{t}]$ est dit inélevant (ou:) lorsqu'il vérifie les conditions équivalentes suivantes:

* il existe $l \in \mathbb{N}$ tel que $\forall i \in \{0, \dots, n\}$, $t_i^l \in I$
* $\forall i \in \{0, \dots, n\}$ $\exists l_i \in \mathbb{N}$ t.q. $t_i^{l_i} \in I$
* il existe $l \in \mathbb{N}$ tel que tout monôme de degré $\geq l$ appartienne à I

Thm (Nullstellensatz projectif): si k est algébriquement clos,

* si I est un idéal homogène tel que $Z_{\mathbb{P}^n}(I) = \emptyset$
alors I est inélevant
* les fonctions $I \mapsto Z(I)$, $E \mapsto J(E)$ définissent des bijections réciproques (décroissantes pour l'inclusion) entre
{idéaux homogènes radicaux, autres que $(x_0, \dots, x_n)$}
et {fermés de Zariski de $\mathbb{P}^n$}

On définit la topologie de Zariski de $\mathbb{P}^n$ comme pour $\mathbb{A}^n$:
un ouvert de Zariski est le complémentaire d'un fermé...

Lien entre affine et projectif. (de coordonnés homogènes $(t_0 : \cdots : t_n)$)

Dans $\mathbb{P}^n$, on définit $n+1$ ouverts de Zariski

$D(t_0), \ldots, D(t_n)$ où $D(t_i) = \{t_i \neq 0\}$ (complémentaire de $Z(t_i)$)

on les appelle "cartes affines" de $\mathbb{P}^n$.

Chaque $D(t_i)$ peut être considéré comme un $\mathbb{A}^n$

de coordonnés $\left(\frac{t_0}{t_i}, \frac{t_1}{t_i}, \ldots, \cancel{\frac{t_i}{t_i}}, \ldots, \frac{t_n}{t_i}\right)$ (n coordonnées).

(le point $x = (x_0 : \cdots : x_n)$ de $\mathbb{P}^n$, où $x_i \neq 0$, c'est-à-dire $x \in D(t_i)$,

est égal à $\left(\frac{x_0}{x_i} : \frac{x_1}{x_i} : \cdots : \underset{\uparrow i}{1} : \cdots : \frac{x_n}{x_i}\right)$

et on l'identifie à : $\left(\frac{x_0}{x_i}, \frac{x_1}{x_i}, \ldots, \cancel{\frac{x_i}{x_i}}, \ldots, \frac{x_n}{x_i}\right) \in \mathbb{A}^n$).

On a par ailleurs $D(t_0) \cup \cdots \cup D(t_n) = \mathbb{P}^n$

($\mathbb{P}^n$ est recouvert par ces "cartes affines"). ("carte")

Moralité : l'espace projectif $\mathbb{P}^n$ est recouvert par $n+1$ ouverts affines

dans tout point de $\mathbb{P}^n$ a un voisinage qui est un $\mathbb{A}^n$

donc localement, $\mathbb{P}^n$ s'étudie comme $\mathbb{A}^n$.

Si $X = Z_{\mathbb{P}^n}(I)$ (où I idéal homogène) est un fermé de Zariski de $\mathbb{P}^n$,

peut-on décrire $X \cap D(t_i)$ comme un fermé de Zariski de $\mathbb{A}^n$?

(Projectif → Affine)

↳ une des cartes affines

Oui : il suffit de "déshomogénéiser" les équations de X

(générateurs de I) par rapport à la variable t_i,

autrement dit, $X \cap D(t_i) = Z_{\mathbb{A}^n}(I_{t_i})$ (déshomogénéisé total)

où I_{t_i} est l'idéal engendré par les $\frac{f}{t_i^{\ell}}$ où $\ell = \deg(f)$

et f parcourt des générateurs homogènes de I,

$\frac{f}{t_i^{\ell}}$ est considéré comme un polynôme en $\frac{t_0}{t_i}, \ldots, \frac{t_n}{t_i}$.

Ex. $\mathbb{P}^2$ de coordonnés $(x:y:z)$, $X = Z_{\mathbb{P}^2}(y^2 z - x^3 - x z^2)$

$X \cap D(z) = Z_{\mathbb{A}^2}\left(\left(\frac{y}{z}\right)^2 - \left(\frac{x}{z}\right)^3 - \left(\frac{x}{z}\right)\right) = Z_{\mathbb{A}^2}(v^2 - u^3 - u)$

où $u = \frac{x}{z}$ et $v = \frac{y}{z}$ sont les coordonnés affines sur $D(z)$

En fait, $X \subseteq \mathbb{P}^n$ est un fermé de Zariski si $X \cap D(t_i) \subseteq \mathbb{A}^n$

en est un pour tout $i \in \{0, \ldots, n\}$.

Aff → proj

Si $X \subset \mathbb{A}^n$ est un fermé de Zariski de $\mathbb{A}^n$, disons $X = Z(I)$ avec $I \subseteq k[\underline{T}] := k[T_1, \dots, T_n]$ idéal.

($T_i := \frac{t_i}{t_0}$)

alors on peut considérer X comme une partie de $\mathbb{P}^n$ en identifiant $\mathbb{A}^n$ à $\{(1 : T_1 : \dots : T_n)\} = D(t_0)$ de $\mathbb{P}^n$

Quelle est son adhérence de Zariski dans $\mathbb{P}^n$?

On peut la calculer comme $X^+ := Z(I^+)$

où I^+ est l'idéal homogène de $k[t_0, \dots, t_n]$

engendré par les $f^+ := \underbrace{t_0^{\deg f} f\left(\frac{t_1}{t_0}, \dots, \frac{t_n}{t_0}\right)}_{\text{polynôme homogène en } t_0, \dots, t_n}$

pour $f \in I$ (dans les)

("homogénéisé" de f par rapport à t_0)

Si I est engendré par un seul élément f

alors I^+ est engendré par f^+.

Ex: l'adhérence de Zariski de $Z_{\mathbb{A}^2}(v^2 - u^3 - u)$ ($\mathbb{A}^2$ coordonnés (u,v))

dans le $\mathbb{P}^2$ de coordonnés $(x : y : z)$ avec $u = \frac{x}{z}$, $v = \frac{y}{z}$

est $Z_{\mathbb{P}^2}(f^+)$ avec $f = v^2 - u^3 - u$

$$f^+ = z^3 \left[\left(\frac{y}{z}\right)^2 - \left(\frac{x}{z}\right)^3 - \left(\frac{x}{z}\right)\right]$$
$$= y^2 z - x^3 - x z^2$$

Topologie de Zariski relative à un fermé de Zariski X:

On dit que $Y \subseteq X$ est un fermé de X lorsque Y est un fermé inclus dans X

et que $V \subseteq X$ est un ouvert de X lorsque $Y := X \setminus V$ est un fermé de X

ce qui revient à dire que $V = X \cap U$ (($\mathbb{A}^n$ ou $\mathbb{P}^n$))

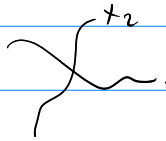
où U est un ouvert de l'espace ambiant (à savoir $U = \left(\begin{smallmatrix}\mathbb{A}^n \\ \text{ou} \\ \mathbb{P}^n\end{smallmatrix}\right) \setminus Y$)

Retour sur les irréductibles:

Si X est un fermé de Zariski, on dit que $E \subset X$ est dense dans X lorsque son adhérence est exactement X.

Prop: X est irréductible ssi **tout ouvert non vide de X est dense**

Dém: si X n'est pas irréductible, $X = X_1 \cup X_2$ avec X_1, X_2 deux fermés $\neq X$; alors $X \setminus X_1$ est un ouvert de X, qui est inclus dans X_2, donc n'est pas dense (son adhérence est incluse dans X_2).



Réciproquement, si U est un ouvert non vide et non dense de X, alors $X = (X \setminus U) \cup \text{adhérence}(U)$ est une écriture de X comme réunion de deux fermés plus petits. □

Intérêt: si X est irréductible, passer à l'ouvert $\{f \neq 0\} =: U$ revient à supposer que le polynôme f ne s'annule pas, le fait qu'un tel ouvert soit dense permet de dire que si g (un autre polynôme) s'annule sur U, alors g s'annule sur X (car $Z(g) \supseteq \text{adhérence}(U)$).

Bref, pour montrer une identité algébrique $(g=0)$ sur un irréductible, on peut supposer la non-annulation de n'importe quel polynôme f qui nous arrange. (à condition qu'il y ait au moins un pour $\neq 0 \ldots$)

(k alg. clos) On rappelle qu'on a vu que Z et I définissent des bijections entre $\{\text{idéaux premiers de } k[t_1, \ldots, t_n]\}$ et $\{\text{fermés irréductibles de } \mathbb{A}^n\}$

De même, on a des bijections entre $\{\text{idéaux homogènes premiers de } k[t_0, \ldots, t_n] \text{ autres que } (t_0, \ldots, t_n)\}$ et $\{\text{fermés irréductibles de } \mathbb{P}^n\}$.

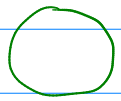
Déf: une variété algébrique affine, resp. projective,
resp. quasi-affine, resp. quasiprojective

est un fermé de Zariski de $\mathbb{A}^n$ ← "affine"

resp. un fermé de Zariski de $\mathbb{P}^n$ ← "projective"

resp. un ouvert de Zariski d'une variété affine (i.e. l'intersection d'un fermé et d'un ouvert de $\mathbb{A}^n$) } → "quasi-affine"

resp. un ouvert de Zariski d'une variété projective (i.e. l'intersection d'un fermé et d'un ouvert de $\mathbb{P}^n$) } → "quasi projective"

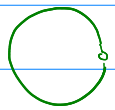
Ex: affine:  $\{x^2+y^2=1\} \subset \mathbb{A}^2 \quad (x,y)$

projective $\{X^2+Y^2=Z^2\} \subset \mathbb{P}^2 \quad (Z:X:Y)$ (même dessin)

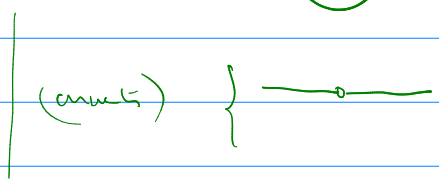
remarque: points à l'infini: $Z=0 \quad X^2+Y^2=0$

$(X+\sqrt{-1}Y)(X-\sqrt{-1}Y)=0$

deux points $(1:\sqrt{-1}:0)$ "points cycliques"
et $(1:-\sqrt{-1}:0)$

quasi-affine:  $\{x^2+y^2=1\} \cap \{x \neq 1\} \subset \mathbb{A}^2$

le cercle mais le pt $(1,0)$

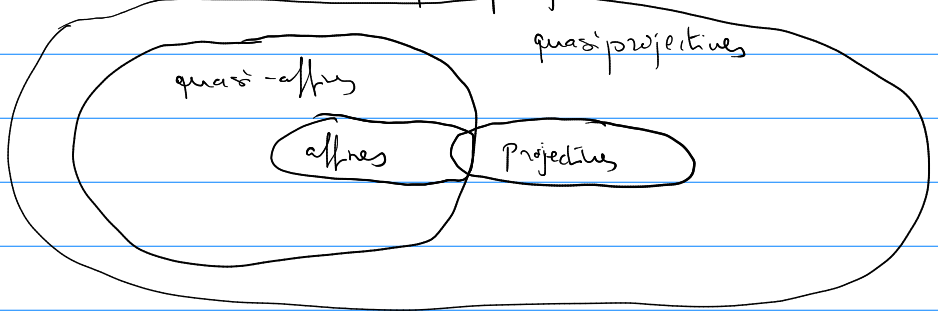


$\mathbb{A}^1 \setminus \{0\}$ la droite mais l'origine

$\mathbb{A}^n \setminus \{0\}$ ...

(courbe)

Rqe: comme $\mathbb{A}^n$ est un ouvert de $\mathbb{P}^n$ (c'est $D(t_0)$),
les variétés affines ou quasi-affines peuvent être
considérées comme quasiprojectives.



Fonctions et morphismes entre variétés algébriques.

Si k est un corps algébriquement clos,
on s'intéresse aux fonctions rationnelles sur $\mathbb{A}^n$
c'est-à-dire aux rapports entre deux polynômes $\frac{f}{g}$
avec $f, g \in k[t_1, \dots, t_n]$ et $g \neq 0$.

Si X est une partie de $\mathbb{A}^n$, on dit que $\frac{f}{g}$
est régulière sur X lorsque g ne s'annule pas sur X.
Elle définit alors une fonction $X \to k$.
"il ne s'annule pas" = "nulle part"

Si X est une variété affine ou quasi-affine,
un morphisme $X \to \mathbb{A}^d$ est une application de la forme
$\underline{x} \mapsto (h_1(\underline{x}), \dots, h_d(\underline{x}))$ h_i = "équations du morphisme"
où chaque h_i est une fonction rationnelle régulière sur X.
(le dénominateur ne s'annule pas sur X).

En fait, si X est affine, dit $X = Z(f_1, \dots, f_r)$
"le dénominateur g de h ne s'annule pas sur X"
signifie $Z(f_1, \dots, f_r, g) = \emptyset$, par le NSS
l'idéal $(f_1, \dots, f_r, g)$ est l'idéal entier,
il existe $u_1, \dots, u_r, v \in k[\underline{t}]$ tels que
$$u_1 f_1 + \dots + u_r f_r + vg = 1$$
donc v est l'inverse de g modulo $(f_1, \dots, f_r) =: I$
donc $h = \frac{f}{g}$ peut se réécrire sous $vf +$ (qqch s'annulant sur X)
ce qui permet de ne pas avoir de dénominateur.

Si Y est affine ou quasi-affine, un morphisme $X \to Y$
est un morphisme $X \to \mathbb{A}^d$ dont l'image est dans Y.
(ceci peut se vérifier en disant que les équations h_i
du morphisme satisfont à celles de Y)

Si maintenant X est projective ou quasi-projective $\subseteq \mathbb{P}^n$
$(t_0 : \cdots : t_n)$

Une fraction rationnelle homogène de degré total 0
c'est-à-dire un rapport f/g avec f et g
deux polynômes homogènes de même degré l
peut être considérée comme une fonction $\mathbb{P}^n \setminus Z(g) \longrightarrow k$
$(t_0 : \cdots : t_n) \mapsto \frac{f(t_0,\dots,t_n)}{g(t_0,\dots,t_n)}$

On dira que $\frac{f}{g}$ est régulière là où g ne s'annule pas.

Un morphisme $X \longrightarrow \mathbb{A}^d$ est une application de la forme
$\underline{x} \longmapsto (h_1(\underline{x}), \dots, h_d(\underline{x}))$ où $h_1, \dots, h_d$
(homogènes de degré 0)
sont des fonctions rationnelles régulières sur X.
(= dont le dénominateur ne s'annule pas sur X).

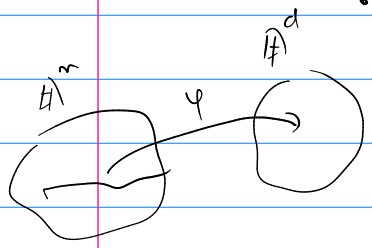
En fait, si X est projective, une fonction régulière
sur X tout entier est localement constante.
(Par exemple, si $X = \mathbb{P}^n$, il n'y a que les constantes.
En effet, si g ne s'annule pas sur $\mathbb{P}^n$, $Z(g) = \emptyset$
donc (g) serait un idéal inclus d'après le NSS projectif.
donc on doit pouvoir écrire $x_0^l = ug$ donc g divise x_0^l
$x_1^l = vg$ donc g divise x_1^l
donc g est une constante, donc f aussi
(le numérateur et dénominateur ont même degré).)

Un morphisme $X \longrightarrow \mathbb{P}^d$
sera défini par $\underline{x} \longmapsto (h_0(\underline{x}) : \cdots : h_d(\underline{x}))$
où $h_0(\underline{x}), \dots, h_d(\underline{x})$ sont des fonctions rationnelles
homogènes de même degré l (i.e. de la forme
$\frac{f}{g}$ avec f, g homogène, $\deg f = l + \deg g$)
avec $g_i \neq 0$ sur X mais aussi $f_0(\underline{x}), \dots, f_d(x)$
ne s'annulent pas simultanément.

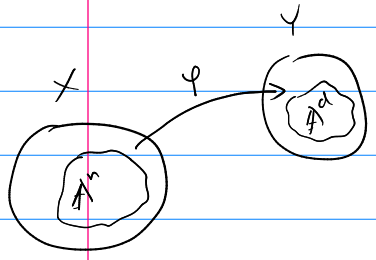
On peut simplifier ça : en "chassant" les dénominateurs
(on multiplie par le produit des g_i pour avoir des polynômes)

2021-03-31

Une autre façon de définir les morphismes dans le cas où on peut se ramener à/vers $\mathbb{P}^n$ et de travailler "localement" dans les cartes affines :



- si X est une var. alg. quasi-affine, un morphisme $\varphi : X \to \mathbb{A}^d$ est une fonction $X \to \mathbb{A}^d$ définie par la donnée de d fonctions rationnelles dont les dénominateurs ne s'annulent pas sur X (NB: si X est affine et pas juste quasi-affine, on peut supposer que ce sont des polynômes)
- si Y est une autre var. alg. quasi-affine, un morphisme $\varphi : X \to Y$ est juste un morphisme $X \to \mathbb{A}^d$ dont l'image est dans Y.
- Si X et Y sont deux variétés algébriques quasi-projectives, on dira qu'une application $\varphi : X \to Y$ est un morphisme si $X \subset \mathbb{P}^n$ et $Y \subset \mathbb{P}^d$, lorsqu'on peut écrire $X = \bigcup_{i=1}^{m} V_i$ où V_i est un ouvert de Zariski de X, contenu dans un $D(x_i) := \{x_i \neq 0\}$ (ouvert de $\mathbb{P}^n$ formé des points où la i-ième coordonnée ne s'annule pas, identifié à $\mathbb{A}^n$ de coordonnées $\left(\frac{x_0}{x_i}, \dots, \frac{x_n}{x_i}\right)$) et où φ restreinte à V_i a une image dans $Y \cap D(y_j)$ pour un certain $0 \leq j \leq d$ (idem : $D(y_j) := \{y_j \neq 0\} \cong \mathbb{A}^d$) et est un morphisme $V_i \to Y \cap D(y_j)$ (quasi-affine → quasi-affine)



En pratique, on retient les choses suivantes :

source $X \to Y$ cible

- Les morphismes sont définis par des fonctions rationnelles dont on impose que le dénominateur ne s'annule pas (sur la source). Si la source est affine ops. qu'il s'agit de polynômes.
- Si la source est quasi-projective, on demande l'indépendance du choix des coordonnées homogènes.
- Si la cible est quasi-projective, on demande que les coordonnées

ne s'annulent pas simultanément, et on peut "chasser" les dénominateurs.

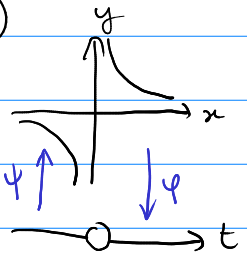
- La composition de morphismes (de variétés algébriques) donne encore un morphisme (si $X \xrightarrow{\varphi} Y$ et $Y \xrightarrow{\psi} Z$ sont deux morphismes alors $\psi \circ \varphi : X \to Z$ en est un)
- Les morphismes sont "locaux pour la topologie de Zariski" c'est-à-dire que si $X = \bigcup_{i \in I} V_i$ (généralement en nombre fini) avec V_i des ouverts de Zariski et $\varphi : X \to Y$ une application, alors φ est un morphisme ssi chaque $\varphi|_{V_i}$ (restriction de φ à V_i) en est un.

(Si on préfère: φ est un morphisme ssi φ en est un sur un voisinage ouvert de chaque point de X.)

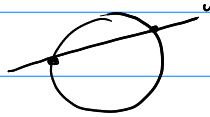
À la cible: si W est un ouvert de Y et $\varphi : X \to W$ une application, alors φ est un morphisme ssi $\varphi : X \to Y$ en est un.

Quelques exemples de morphismes entre variétés algébriques :

- Si $f \in k[t_1, \dots, t_n]$ est un polynôme, on peut identifier f à un morphisme $\mathbb{A}^n \to \mathbb{A}^1$ par $\underline{x} \mapsto f(\underline{x})$.
  (NB : k est algébriquement clos donc il est légitime d'identifier un polynôme avec la fonction qu'il définit).
- Si f, g sont deux polynômes, $g \neq 0$, alors f/g définit un morphisme $\{g \neq 0\} \to \mathbb{A}^1$
  ↳ ouvert de Zariski de $\mathbb{A}^n$.
- $U := \{t \neq 0\} \subseteq \mathbb{A}^1$ (ouvert complémentaire de l'origine)
  $H := \{xy = 1\} \subseteq \mathbb{A}^2$ (fermé de Zariski, "hyperbole")
  $\varphi : H \to U \quad (x, y) \mapsto x$
  $\psi : U \to H \quad t \mapsto (t, \frac{1}{t})$
  Ces deux morphismes et ils sont réciproques :
  on dira qu'il s'agit d'isomorphismes de variétés algébriques.



- Paramétrage rationnel du cercle :
  $C := \{(x, y) : x^2 + y^2 = 1\} \subseteq \mathbb{A}^2$
  $U := \{1 + t^2 \neq 0\} \subseteq \mathbb{A}^1$
  $\varphi : t \mapsto \left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$
  $U \to C$



car $k \neq 2$

en fait, il tombe dans l'ouvert complémentaire de $(-1, 0)$ dans C,

$\psi : (x, y) \mapsto \frac{y}{x+1}$
$C \setminus \{(-1,0)\} \to U$
$\psi \circ \varphi$ et $\varphi \circ \psi$ sont l'identité

on peut vérifier que c'est un isomorphisme entre $U := \{1 + t^2 \neq 0\} \subseteq \mathbb{A}^1$ et $C \setminus \{(-1,0)\} := \{x + 1 \neq 0\} \cap \{x^2 + y^2 = 1\} \subseteq \mathbb{A}^2$

- Complétion projective de l'exemple précédent :
  $C^+ := \{(Z : X : Y) \in \mathbb{P}^2 \mid X^2 + Y^2 - Z^2 = 0\}$ adhérence de C dans $\mathbb{P}^2$
  On définit $\varphi : \mathbb{P}^1 \to C^+$ par
  $(U : T) \mapsto (\underset{Z}{U^2 + T^2} : \underset{X}{U^2 - T^2} : \underset{Y}{2UT})$
  définie lorsque $U^2 + T^2 \neq 0$ ou $U^2 - T^2 \neq 0$ ou $2UT \neq 0$
  sont tous $\mathbb{P}^1$

Et $\psi_1 : C^+ \setminus \{(1:-1:0)\} \longrightarrow \mathbb{P}^1$ (Z:X:Y)

$(Z:X:Y) \longmapsto \underbrace{(X+Z : Y)}$ (X:Y)

↳ défini sauf si $X+Z = Y = 0$

coïncidence de $(1:-1:0)$

Mais remarquons que modulo $X^2+Y^2-Z^2$,

on a $(X+Z:Y) = ((X+Z)(X-Z) : Y(X-Z))$ (si $X-Z \neq 0$)

$= (X^2 - Z^2 : XY - YZ)$

$= (-Y^2 : XY - YZ)$ (si $Y \neq 0$)

$= (-Y : X-Z) = (Y : Z-X)$

Ceci montre que ψ_1 coïncide avec

$\psi_2 : C^+ \setminus \{(1:1:0)\} \longrightarrow \mathbb{P}^1$ (Z:X:Y)

$(Z:X:Y) \longmapsto (Y : Z-X)$

lorsque $X-Z \neq 0$, $X+Z \neq 0$ et $Y \neq 0$, c'est-à-dire

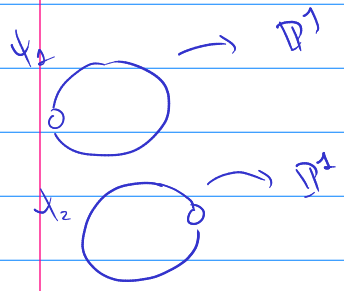
sur l'intersection $C^+ \setminus \{(1:1:0), (1:-1:0)\}$

des ouverts de définition de ψ_1 et ψ_2

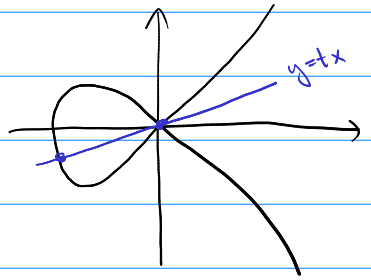
Ceci permet de "recoller" ψ_1 et ψ_2 en un morphisme

$\psi : C^+ \longrightarrow \mathbb{P}^1$

$(Z:X:Y) \longmapsto \left\{ \begin{matrix} (X+Z:Y) \\ \text{ou bien} \\ (Y:Z-X) \end{matrix} \right\}$ (qui coïncident si les deux sont définies)



(char $\neq 2$) • $C := \{y^2 = \underbrace{x^3 + x^2}_{x^2(x+1)}\} \subset \mathbb{A}^2$



"cubique nodale"

Morphisme $\mathbb{A}^1 \longrightarrow C$

$t \longmapsto (t^2-1, t^3-t)$

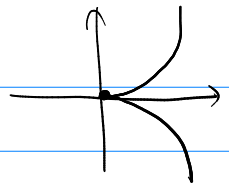
$(tx)^2 = x^3 + x^2$

$t^2 x^2 = x^3 + x^2$

$x = t^2 - 1$ $\quad y = t^3 - t$

(Paramétrage pas bijectif : le point $(0,0)$ de C est atteint deux fois : pour $t=+1$ et $t=-1$.)

- $C = \{y^2 = x^3\} \subset \mathbb{A}^2$



"cubique cuspidale"

Morphisme $\mathbb{A}^1 \xrightarrow{\varphi} C$

$t \longmapsto (t^2, t^3)$

φ est bijectif (i.e. définit une bijection entre les points génériques de $\mathbb{A}^1$ et ceux de C)

mais φ n'est pas un isomorphisme.

En effet, φ est bijectif car le point (x,y) de C s'obtient comme l'image de y/x si $(x,y) \neq (0,0)$ et comme l'image de 0 si $(x,y) = (0,0)$

Pourtant, l'application réciproque de φ n'est pas un morphisme au voisinage de l'origine. $C \setminus \{(0,0)\} \longrightarrow \mathbb{A}^1$

$(x,y) \longmapsto \frac{y}{x}$

est bien un morphisme,

mais il n'existe pas de polynôme $h \in k[x,y]$ tels que $(x,y) \longmapsto h(x,y)$, $C \longrightarrow \mathbb{A}^1$ soit la réciproque de φ :

en effet $h(t^2, t^3) = t$,

impossible par des raisons de degré ($(t^2)^i (t^3)^j = t^{2i+3j}$ et $2i+3j \neq 1$ si $(i,j) \in \mathbb{N}^2$)

Si k n'est pas algébriquement clos, par morphisme entre variétés algébriques $X \longrightarrow Y$ on entend un morphisme entre les variétés sur la clôture algébrique k^{alg} dont les équations peuvent être écrites avec des coefficients dans k.

Un tel morphisme définit naturellement une application $\underbrace{X(k)}_{\text{k-points de X}} \longrightarrow \underbrace{Y(k)}_{\text{k-points de Y}}$

(et bien sûr aussi $\underbrace{X(k^{alg})}_{\text{points génériques de X}} \longrightarrow \underbrace{Y(k^{alg})}_{\text{points génériques de Y}}$ restriction)

$X^2+Y^2+Z^2=0$

Ex: sur $k=\mathbb{R}$, $\{X^2+Y^2=-Z^2\}$ est un fermé de Zariski de $\mathbb{P}^2$ (donc une variété algébrique affine) sur $\mathbb{R}$ qui n'a pas de point réel.

Sur $\mathbb{C}$, il existe un isomorphisme $\mathbb{P}^1 \longrightarrow \{X^2+Y^2+Z^2=0\}$ obtenu en composant $\mathbb{P}^1 \longrightarrow \{X^2+Y^2-Z^2=0\}$ (paramétrage rationnel du cercle) et $(Z:X:Y) \longmapsto (\sqrt{-1}Z:X:Y)$ (transformation projective de $\mathbb{P}^2$)

En revanche, sur $\mathbb{R}$, $\{X^2+Y^2+Z^2=0\}$ n'est certainement pas isomorphe à $\mathbb{P}^1$ car $\mathbb{P}^1$ a des points réels alors que $\{X^2+Y^2+Z^2=0\}$ n'en a aucun, donc il n'y a pas de morphisme $\mathbb{P}^1 \longrightarrow \{X^2+Y^2+Z^2=0\}$ sur $\mathbb{R}$.

Fonctions régulières et fonctions rationnelles

Les fonctions régulières sur X forment un anneau, noté $\mathcal{O}(X)$

* Si X est une variété algébrique, une fonction régulière sur X est un morphisme $X \longrightarrow \mathbb{A}^1$ (si X est affine, disons $X=Z(I)$ avec I idéal radical de $k[t_1,\dots,t_n]$, on peut l'identifier à un élément de $k[t_1,\dots,t_n]/I$).
* Si X est de plus irréductible, une fonction rationnelle sur X est une fonction régulière sur un ouvert non vide (donc automatiquement dense) de X, qu'on appelle (un) ouvert de définition de cette fonction, et où on identifie f définie sur U et g définie sur V lorsque $f=g$ sur $U\cap V$. La réunion de tous les ouverts de définition est appelé l'ouvert de régularité de la fonction.

(Exemple: si f et g sont deux polynômes (en n variables, $g\neq 0$), $\frac{f}{g}$ est une fonction rationnelle sur $\mathbb{A}^n$, régulière sur l'ouvert $\{g\neq 0\}$.)

Les fonctions rationnelles (sur X irréductible) forment un corps. Si X est affine, ce corps est intègre d'ailleurs le corps des fractions de l'anneau $\mathcal{O}(X)$ des fonctions régulières.

[Si A est un anneau intègre, son "corps des fractions" est l'ensemble des quotients formels $\frac{a}{b}$ avec $a, b \in A$, $b \neq 0$ où on identifie $\frac{a}{b}$ et $\frac{a'}{b'}$ lorsque $ab' = a'b$ et avec l'addition

$$\frac{a}{b} + \frac{a'}{b'} = \frac{ab' + a'b}{bb'}$$

et la multiplication

$$\frac{a}{b} \cdot \frac{a'}{b'} = \frac{aa'}{bb'}$$]

Ce corps est noté $k(X)$.
^
des fonctions rationnelles sur X

Ex: $k(\mathbb{A}^n) = k(t_1, \dots, t_n) = \mathrm{Frac}(k[t_1, \dots, t_n])$

$k(\mathbb{P}^n) = k(\underbrace{\tau_1, \dots, \tau_n}_{n \text{ indéterminées, pas } n+1})$ où $\tau_i = t_i / t_0$

$= \left\{ \frac{f}{g} \text{ avec } f, g \in k[t_0, \dots, t_n] \right.$
$\left.$ homogènes du même degré $\right\}$

N_B: Si X est projective, les seules fonctions régulières sont les fonctions localement constantes.
En revanche, il y a en général beaucoup d'autres fonctions rationnelles, par exemple
$\frac{f}{g}$ si $f, g \in k[t_0, \dots, t_n]$ homogènes de même degré définit une fonction rationnelle sur $\mathbb{P}^n$, régulière sur $\{g \neq 0\}$.

Dimension d'une variété algébrique:
Si X est une variété algébrique irréductible, disons sur le alg't clos, on définit sa dimension ("de Krull"), notée $\dim(X)$, comme
$$\max\{\dim(Y) : Y \text{ fermé irréductible de } X \text{ avec } Y \neq X\} + 1$$
avec la convention que $\dim(\emptyset) = -1$

Ex: $\dim \mathbb{A}^1 = \max\{\dim(\{x\}), \dim(\emptyset)\} + 1 = 1$
↳ $\dim\{x\} = \max\{\dim(\emptyset)\} + 1 = 0$

Plus généralement, $\dim \mathbb{A}^n = n$

Thm (Hauptidealsatz de Krull, "théorème de l'idéal principal"):
si X est une variété algébrique et f une fonction régulière sur X, et si f n'est ni zéro ni inversible (dans $\mathcal{O}(X)$ ↳ anneau des fonctions régulières sur X) alors le fermé de Zariski $Z(f) := \{f = 0\}$ est de dimension $\dim(X) - 1$.

NB: si X n'est pas irréductible, il existe une façon unique d'écrire $X = \bigcup_{i=1}^{m} X_i$ avec X_i fermé dans X, irréductible et $X_i \not\subseteq X_j$ si $i \neq j$: ces X_i s'appellent les composants irréductibles de X et on pose alors $\dim(X) := \max(\dim(X_i))$

Prop: Si U est un ouvert dense de X alors $\dim U = \dim X$
(rédaction, si U est ouvert $\neq \emptyset$ de X irréductible).

Prop: Si X est irréductible, $\dim(X)$ est le degré de transcendance de $k(X)$ (corps des fonctions rationnelles sur X)

[Si $k \subseteq K$ sont deux corps, on dit que $x_1, \dots, x_m \in K$ sont algébriquement indépendants sur k lorsque le seul polynôme $f \in k[t_1, \dots, t_m]$ tel que $f(x_1, \dots, x_m) = 0$ est le polynôme nul.

On a alors un isomorphisme

$$\begin{array}{ccc} k(t_1, \dots, t_m) & \longrightarrow & k(x_1, \dots, x_m) \subseteq K \\ g/h & \longmapsto & \dfrac{g(x_1, \dots, x_m)}{h(x_1, \dots, x_m)} \end{array}$$

- $k(t_1, \dots, t_m)$: fractions rationnelles en m indéterminées
- $k(x_1, \dots, x_m)$: sous-corps engendré par $x_1, \dots, x_m$ et k dans K

Par une famille $(x_i)_{i \in I}$ infinie, "algébriquement indépendant" signifie que toute sous-famille finie l'est.

Prop : Si $k \subseteq K$ sont deux corps, il existe $(x_i)_{i \in I}$ une famille algébriquement indépendante maximale, c'est-à-dire que $k(x_i) \subseteq K$ est algébrique

(sous-corps engendré par (k) et les (x_i))

On l'appelle base de transcendance de K sur k.

Les bases de transcendance ont toutes le même cardinal, appelé degré de transcendance de K sur k]

Ex : on a vu que $\mathbb{A}^n$ (ou $\mathbb{P}^n$) a pour corps des fonctions rationnelles $k(t_1, \dots, t_n)$ ("transcendant pur" = corps des fractions rationnelles) donc son degré de transcendance est n et on retrouve

$$\dim(\mathbb{A}^n) = n \quad (\text{et } \dim(\mathbb{P}^n) = n)$$

- Dimension via la "fonction de Hilbert-Samuel" :

Si I est un idéal homogène de $k[t_0, \dots, t_n]$, on a $Z(I)$

on appelle fonction de Hilbert-Samuel de I la fonction $\mathbb{N} \to \mathbb{N}$ qui à $\ell \in \mathbb{N}$ associe $\dim_k k[t_0, \dots, t_d]^{[\ell]} / I^{[\ell]} = \dfrac{(d+\ell)!}{d!\,\ell!} - \dim I^{[\ell]}$

à $I^{[\ell]} = \{$polynômes homogènes de degré ℓ dans $I\}$

(k-espace vectoriel en tant que)

Cette fonction coïncide avec un polynôme en ℓ pour ℓ grand.

Ce polynôme s'appelle polynôme de Hilbert-Samuel de I (ou $Z(I)$).

2021-04-07

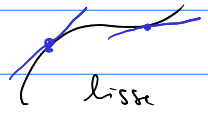
Son degré coïncide avec $\dim Z(I)$.

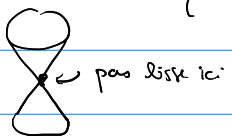
En particulier pour $I=0$, le facteur de H-S vaut

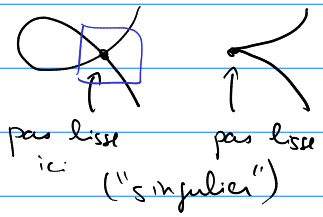
$$\frac{(d+\ell)!}{d!\,\ell!} = \frac{1}{d!}(\ell+d)(\ell+d-1)\cdots(\ell+1) = \text{polynôme de degré } d \text{ en } \ell$$

au voisinage de n'importe quel $\dim \mathbb{P}^d = d$.

Espaces tangents et lissité :







Si $X = Z(I)$ est une variété algébrique affine $\subseteq \mathbb{A}^n$ (le k algébriquement clos dos)

avec $I \subseteq k[t_1,\dots,t_n]$ idéal radical $= (f_1,\dots,f_r)$

et $x \in X(k)$ un point de X, on appelle espace tangent à X en x l'espace vectoriel noyau de la matrice $r \times n$

$$\left.\frac{\partial f_i}{\partial t_j}\right|_{\text{évalué en } x} \qquad \begin{pmatrix} i = \text{indice de la ligne} \\ j = \text{indice de la colonne} \end{pmatrix}$$

$$\begin{pmatrix} \frac{\partial f_1}{\partial t_1} & \cdots & \frac{\partial f_1}{\partial t_n} \\ \vdots & & \vdots \\ \frac{\partial f_r}{\partial t_1} & \cdots & \frac{\partial f_r}{\partial t_n} \end{pmatrix} \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$$

Intuitivement : $f_i(x + \varepsilon\vec{v}) = \cancel{f_i(x)} + \varepsilon\left(\sum_{j=1}^{n} \frac{\partial f_i}{\partial t_j} v_j\right) + O(\varepsilon^2)$

$\uparrow$ car $x \in X(k)$; $\uparrow$ s'annule pour un vecteur tangent

On le note $T_x X$ et sa dimension comme k-e.v. $\dim_k T_x X$

Thm : on a $\dim T_x X \geq \dim X$ si x est un point d'une variété algébrique affine X irréductible. Lorsqu'il y a égalité, on dit que x est un point {régulier / lisse} de X ou que X est lisse en x. Dans le cas contraire, on dit "singulier".

Si X est lisse en tout point, on dit juste "lisse".

Si X est une variété algébrique quasi-affine, on dit que $x \in X(k)$ est lisse lorsqu'il l'est sur $Z(I)$ où $X = Z(I) \cap V$ (fermé (équations), ouvert (inéquations))

Idem espace tangent.

Pour X une variété quasiprojective, on définit l'espace tangent à $x \in X(k)$ ou la notion de lissité en considérant une carte affine de l'espace projectif.

Prop: si X est projective, disons $X = Z(I)$ où $I = (f_1, \dots, f_r)$ idéal homogène radical engendré par $f_1, \dots, f_r$ homogènes, on a X lisse ssi les $\frac{\partial f_i}{\partial t_j}$ (toutes les dérivées de tous les polynômes) engendrent un idéal inclevant (= contient tous les t_j^n pour un certain n)

= les $\frac{\partial f_i}{\partial t_j}$ n'ont pas de zéro commun (k alg. clos) des $\mathbb{P}^n$

Ex: $\{x^2 + y^2 - z^2\} \subset \mathbb{P}^2_{(x:y:z)}$ est lisse car $\frac{\partial f}{\partial x} = 2x$, $\frac{\partial f}{\partial y} = 2y$, $\frac{\partial f}{\partial z} = 2z$ n'ont pas de zéro commun dans $\mathbb{P}^2$ (char $k \neq 2$)

Déf: une "courbe" (projective lisse) est une variété algébrique C irréductible projective lisse de dimension 1.

↳ ses fermés de Zariski sont les ensembles finis et la courbe tout entière.

Son corps des fonctions rationnelles $k(C)$ est de degré de transcendance 1 sur k.

Rappel : une "fonction rationnelle" sur C (une courbe) a été définie comme une fonction régulière sur un ouvert (toujours dense) de C.

Dans le cas d'une courbe, on peut lui attribuer la valeur "∞" là où elle n'est pas régulière, et on obtient alors un morphisme $C \to \mathbb{P}^1$.

{ Attention : ceci est spécifique à la dimension 1.
Penser à $\frac{x}{y}$ sur $\mathbb{A}^2$, pas régulière sur $\{y=0\}$
Ceci ne définit pas un morphisme $\mathbb{A}^2 \to \mathbb{P}^1$ $(x,y) \mapsto (y:x)$ }

Autrement dit, sur une courbe on peut identifier "fonction rationnelle" avec "morphisme vers $\mathbb{P}^1$".

Déf : si $k \subsetneq K$ sont deux corps, une valuation (discrète) sur K au-dessus de k est une fonction $v : K^\times \to \mathbb{Z}$ (où $K^\times = \{f \in K : f \neq 0\}$, qu'on étend à K en posant $v(0) = +\infty$) qui vérifie les propriétés suivantes :

- $v(f) = 0$ si $f \in k^\times$
- $v(f+g) \geq \min(v(f), v(g))$ (ceci implique qu'il y a égalité si $v(f) \neq v(g)$)
- $v(fg) = v(f) + v(g)$
- il existe au moins un $f \in K^\times$ tel que $v(f) = 1$

Dans ces conditions, $R := \{f \in K : v(f) \geq 0\}$ (incluant 0) est un sous-anneau de K, et $\mathfrak{m} := \{f \in k : v(f) > 0\}$ est un idéal de R, qui est d'ailleurs maximal.

On dit que R est l'anneau de la valuation v et que $\kappa := R/\mathfrak{m}$ est le "corps résiduel" de v.

Exemples de valuations : sur $K = k(t)$, on a les suivants :

- $v_\infty : k(t) \to \mathbb{Z} \cup \{+\infty\}$ $\quad \frac{f}{g} \mapsto \deg g - \deg f$ $\quad (0 \mapsto +\infty)$

- Les valuations définies par :

$v_0 : k(t) \to \mathbb{Z} \cup \{+\infty\}$ $\quad \frac{f}{g} \mapsto v_0(f) - v_0(g)$ $\quad (0 \mapsto +\infty)$

où $v_0(f) = r$ si $f \in k[t]$ s'écrit $a_r t^r + \dots + a_n t^n$ avec $a_r \neq 0$ (ordre croissant $r \leq n$)

(multiplicité de la racine 0 de f)

$-t$	$v_0(-t) = 1$
$t+t^2$	$v_0(t+t^2) = 1$
t^2	$v_0(t^2) = 2$

et plus généralement, si $a \in k$, $v_a(f) = v_0(f(t+a))$ (translation de f par $-a$)

En fait, si k est alg. clos, car $h \in k(t)^\times$ peut s'écrire

$$\prod_{b \in k} (t-b)^{r_b} \quad \text{à } r_b \in \mathbb{Z}, \text{ tous nuls sauf un nombre fini}$$

On a alors $r_b = v_b(h)$ (défini ci-dessus).

On peut montrer que (pour k algébriquement clos) les v_a ($a \in k$) et v_∞ sont exactement toutes les valuations de $k(t)$ au-dessus de k.

De façon générale,

Prop : si C est une courbe sur k algébriquement clos, toutes les valuations sur le corps $k(C)$ (des fonctions rationnelles sur k) au-dessus de k sont de la forme $\mathrm{ord}_x : k(C) \to \mathbb{Z} \cup \{+\infty\}$ où ord_x est l'unique valuation telle que

$$\begin{cases} \mathrm{ord}_x(f) \geq 0 & \Leftrightarrow f \text{ est régulière en } x \\ \mathrm{ord}_x(f) > 0 & \Leftrightarrow f \text{ s'annule en } x \end{cases}$$

On dira que $\mathrm{ord}_x(f)$ est l'ordre d'annulation de f en x (ou "ordre du zéro" de f en x)

On dit que f a un zéro d'ordre $k>0$ en x lorsque $\mathrm{ord}_x(f) = k$

et un pôle d'ordre $k>0$ lorsque $\mathrm{ord}_x(f) = -k$.

On dit que f est inversible en x lorsque $\mathrm{ord}_x(f) = 0$ (ni zéro ni pôle)

On dit que f est une uniformisante en x lorsque $\mathrm{ord}_x(f) = 1$ (zéro d'ordre exactement 1).

Le corps résiduel $\kappa_x = R_x/\mathfrak{m}_x$

où $R_x = \{f \in k(C) : \mathrm{ord}_x(f) \geq 0\}$

$\mathfrak{m}_x = \{f \in k(C) : \mathrm{ord}_x(f) > 0\}$

vaut simplement k (isomorphisme $f \bmod \mathfrak{m}_x \mapsto f(x)$).

On cherche maintenant à étudier toutes les valeurs $\mathrm{ord}_x(f)$ simultanément.

($k = k^{alg}$)

Déf: si C est une courbe, une fonction $D : C(k) \to \mathbb{Z}$ qui ne prend qu'un nombre fini de valeurs $\neq 0$ s'appellera un diviseur sur C.

Si $x \in C(k)$, on notera $[x]$ le diviseur $x \mapsto 1$, $y \mapsto 0$ si $y \neq x$

Un diviseur $x \mapsto n_x$ est donc de la forme

$$\sum_{x \in C} n_x [x]$$

Prop: si $f \in k(C)^\times$, alors la fonction $x \mapsto \mathrm{ord}_x(f)$ définit un diviseur sur C, c'est-à-dire qu'elle vaut 0 sauf en un nombre fini de points.

(I.e. une fonction rationnelle sur C n'a qu'un nombre fini de zéros et de pôles)

Ce diviseur se note $\mathrm{div}(f)$ et s'appelle "principal".

La propriété $v(fg) = v(f) + v(g)$ donne : $\mathrm{div}(fg) = \mathrm{div}(f) + \mathrm{div}(g)$

$v(1) = 0$ $\mathrm{div}(1) = 0$

Si on note $\mathrm{Div}(C)$ le groupe (abélien pour l'addition) des diviseurs sur C, et $\mathrm{Princ}(C) = \{\mathrm{div}(f) : f \in k(C)^\times\}$ les diviseurs dits "principaux", on vient de voir que $\mathrm{Princ}(C)$ est un sous-groupe de $\mathrm{Div}(C)$.

Le quotient $\mathrm{Div}(C)/\mathrm{Princ}(C) =: \mathrm{Pic}(C)$ s'appelle <u>groupe de Picard</u> de C.

Déf: Si D est un diviseur sur C, disons $\sum_{x \in C} n_x [x]$ son <u>degré</u> est $\deg(D) := \sum_{x \in C} n_x$.

Notamment, $\deg(\mathrm{div}(f)) = \sum_{x \in C} \mathrm{ord}_x(f)$.

Prop: Si $f \in k(C)^\times$ est une fonction rationnelle sur une courbe C, alors on a $\deg(\mathrm{div}(f)) = 0$ c'est-à-dire $\sum_{x \in C} \mathrm{ord}_x(f) = 0$.

Si on note $\mathrm{Div}^0(C) := \ker(\deg) = \{D \in \mathrm{Div}(C) : \deg(D) = 0\}$ alors $\mathrm{Princ}(C) \subseteq \mathrm{Div}^0(C)$.

On peut donc noter $\mathrm{Pic}^0(C) = \mathrm{Div}^0(C)/\mathrm{Princ}(C)$ "groupe de Picard de degré 0"

On a $\deg : \mathrm{Pic}(C) \to \mathbb{Z}$ morphisme défini par $D \pmod{\mathrm{Princ}(C)} \mapsto \deg(D)$.

Notation: on écrit $D \sim D'$ (pour $D, D' \in \mathrm{Div}(C)$) lorsque $D' - D \in \mathrm{Princ}(C)$ ("est un diviseur principal"). On dit qu'ils sont "linéairement équivalents".

Déf: Un diviseur $D = \sum_{x \in C} n_x [x]$ tel que $n_x \geq 0$ est dit "effectif". On note $D \geq 0$.

Prop: Si $f \in k(C)^\times$ est telle que $\mathrm{div}(f) \geq 0$ (i.e. f est régulière partout, i.e. n'a pas de pôle) alors f est <u>constante</u> ($f \in k^\times$) et réciproquement $\mathrm{div}(f) = 0$.

Déf: Si D est un diviseur sur C (une courbe), $D = \sum_{x \in C} n_x [x]$ on définit

$$\mathcal{L}(D) := \{ f \in k(C) : (\forall x \in C) \ \mathrm{ord}_x(f) \geq -n_x \}$$
$$= \{ f \in k(C) : f = 0 \text{ ou bien } \mathrm{div}(f) + D \geq 0 \}$$

Par exemple, $\mathcal{L}(0) = \{ f \in k(C) : (\forall x) \ \mathrm{ord}_x(f) \geq 0 \}$
$= \{ f$ n'ayant pas de pôle $\}$
$= k$ (cf. ci-dessus)

$\mathcal{L}([z]) = \{ f \in k(C) :$ f n'ayant pas de pôle sauf au pire un pôle d'ordre 1 en $z \}$

$\mathcal{L}(-[z]) = \{ f \in k(C) :$ f n'a aucun pôle et s'annule en $z \} = 0$

Prop: $\mathcal{L}(D)$ est un k-espace vectoriel de dimension finie.
Cette dimension se note $\ell(D)$.
On vient de voir que $\ell(0) = 1$ et $\ell(-[z]) = 0$.

Plus généralement:

Prop: ① si $\deg(D) < 0$ alors $\ell(D) = 0$.
② si $\deg(D) = 0$ et $\ell(D) \neq 0$ alors $\ell(D) = 1$ et $D \sim 0$ (signifie $D \in \mathrm{Prin}(C)$)

Dém: Si $\ell(D) \neq 0$ il existe $f \in \mathcal{L}(D)$ non nulle,
alors $D' := D + \mathrm{div}(f) \geq 0$.

$\deg D' = \deg D + \deg \mathrm{div}(f)$

① On ne peut pas avoir $D' \geq 0$ et $\deg(D') < 0$.

② Si $D' \geq 0$ et $\deg(D') = 0$ alors $D' = 0$
et $D = -\mathrm{div}(f) = \mathrm{div}\left(\frac{1}{f}\right) \sim 0$ ∎

Théorème (Riemann-Roch): Si C est une courbe, il existe un diviseur K (unique modulo $\sim$) appelé "diviseur canonique" de C et un entier $g \geq 0$ appelé "genre" de C tels que pour tout diviseur D on ait

$$\ell(D) - \ell(K-D) = \deg D + 1 - g \qquad (*)$$

Corollaire:
- $\ell(K) = g$
- $\deg(K) = 2g-2$
- Si $\deg(D) > 2g-2$ alors $\ell(D) = \deg D + 1 - g$.

Déb:
- $(*)$ appliquée à $D=0$ donne:
$$\ell(0) - \ell(K) = \deg 0 + 1 - g$$
$$1 - \ell(K) = 1 - g \quad \text{donc} \quad \ell(K) = g$$
- $(*)$ appliquée à $D=K$ donne:
$$\ell(K) - \ell(0) = \deg K + 1 - g$$
$$g - 1 = \deg K + 1 - g$$
donc $\deg K = 2g-2$
- Si $\deg D > 2g-2$ alors $\deg K - D < 0$ donc $\ell(K-D) = 0$ (prop précédente)
$(*)$ donne alors $\ell(D) - \ell(K-D) = \deg D + 1 - g$. □

Description du diviseur canonique.

Prop: Si C est une courbe, il existe un $k(C)$-espace vectoriel de dimension 1 noté Ω^1_C et appelé "espace des formes différentielles méromorphes sur C" et une application $d : k(C) \to \Omega^1_C$ k-linéaire vérifiant:
- $dc = 0$ si $c \in k$
- $d(fg) = f\,dg + g\,df$ si $f, g \in k(C)$
- si $\mathrm{ord}_x(t) = 1$ pour au moins un x alors $dt \neq 0$.

Ces conditions caractérisent Ω^1_C et d à isomorphisme près.

"Ω^1_C est un $k(C)$-e.v. de dimension 1"

signifie que $\frac{\omega}{\omega'} \in k(C)$ a un sens si $\omega' \in \Omega^1_C$, $\omega' \neq 0$.

Notamment, $\frac{df}{dt}$ a un sens si $dt \neq 0$

$f, t \in k(C)$

Prop: C une courbe, $x \in C$ et t une uniformisante en x ($\hookrightarrow \mathrm{ord}_x(t) = 1$)

Alors :

- $\mathrm{ord}_x\left(\frac{df}{dt}\right) = \mathrm{ord}_x(f) - 1$ si $\mathrm{ord}_x(f) \neq 0$ dans k (= pas multiple de la caractéristique)
- $\mathrm{ord}_x\left(\frac{df}{dt}\right) \geq 0$ si $\mathrm{ord}_x(f) \geq 0$

Déf: si $\omega \in \Omega^1_C$, $\omega \neq 0$, on peut définir

$\mathrm{ord}_x(\omega) := \mathrm{ord}_x\left(\frac{\omega}{dt}\right)$ où t est une uniformisante en x

(ne dépend pas du choix de t)

⚠ t dépend de x.

Le diviseur $\mathrm{div}(\omega) := \sum_{x \in C} \mathrm{ord}_x(\omega) \cdot [x]$

s'appelle le diviseur de la différentielle ω.

Si ω' est un autre élément de Ω^1_C ($\omega' \neq 0$)

alors on peut écrire $\omega' = \omega \cdot f$ avec $f \in k(C)^\times$

$\mathrm{div}(\omega') = \mathrm{div}(\omega) + \underbrace{\mathrm{div}(f)}_{\hookrightarrow \text{principal}}$

donc $\mathrm{div}(\omega') \sim \mathrm{div}(\omega)$

définit une classe bien définie de $\mathrm{Pic}(C)$

C'est exactement la classe "canonique" qui apparaît dans Riemann-Roch. ($K = \mathrm{div}(\omega)$ pour un $\omega \neq 0$ quelconque de Ω^1_C).

On peut la calculer au moyen de la proposition précédente.