Géométrie algébrique élémentaire

Alexis TCHOUDJEM
Institut Camille Jordan
Université Claude Bernard Lyon I
Boulevard du Onze Novembre 1918
69622 Villeurbanne
FRANCE

Villeurbanne, le 7 mai 2014

Cours du mercredi 22 janvier 2014

Introduction

À l'origine de la géométrie algébriq ue est l'étude des solutions des systèmes d'équations polynomiales :

$$\begin{aligned}
&f_1(x_1, ..., x_n) = 0 \\
&\vdots \\
&f_r(x_1, ..., x_n) = 0
\end{aligned}$$

où les $f_i \in k[X_1, ..., X_n]$ et k est un corps. On note $V(f_1, ..., f_n)$ l'ensemble des solutions du système.

Si les f_i sont linéaires, on obtient un sous-ev et sa « taille »est donnée par sa dimension. En général, on n'a pas un sous-ev mais on peut quand même généraliser la notion de dimension. On utilisera pour cela un lien important entre la géométrie et l'algèbre :

Si $g \in (f_1, .., f_n)$, alors $V(g, f_1, ..., f_n) = V(f_1, ..., f_n)$. Donc $V(f_1, ..., f_n)$ ne dépend que de l'idéal I engendré par les f_i.

Peut-on retrouver I à partir de l'ensemble $V(f_1, ..., f_n)$?

Presque si le corps est algébriquement clos. Le théorème des zéros de Hilbert, que l'on démontrera bientôt, a pour conséquence :

si k est algébriquement clos, alors $\sqrt{I} := \{f \in k[X_1, ..., X_n] \ : \ ^{\exists}\, m > 0,\ f^m \in I\} = \{f \in k[X_1, ..., X_n] \ : \ f|_V = 0\}$. Et on peut définir la dimension à partir de l'algèbre quotient : $k[X_1, ..., X_n]/I$.

Cas où $r = 1,\ n = 2$.

Une *courbe algébrique plane* est un ensemble des points de $\mathbb{A}^2 = k^2$ (le plan affine) dont les coordonnées (x, y) vérifient une équation

$$f(x, y) = 0 \tag{1}$$

pour un certain polynôme $f \in k[X, Y]$. On considérera d'autres espaces ambiants que le plan affine. On appellera donc une telle courbe une courbe affine plane.

Le degré de l'équation (1) est le *degré* de la courbe ; une courbe de degré 2 est une *conique*, une courbe de degré 3 est une *cubique*, *etc.*

Exemples : $x^2 + y^2 = 1$, $y^2 = x^3$, $y^2 = x^3 + x^2$, $y^2 = x^3 - x$, $xy = 1$, $xy = 0$.

Comme l'anneau $k[X, Y]$ est factoriel, un polynôme f se factorise en

$$f = f_1^{k_1}...f_n^{k_n}$$

en produits de facteurs irréductibles deux à deux non proportionnels (de manière unique à un facteur constant non nul près).

La courbe X d'équation $f = 0$ est la réunion des courbes X_i d'équations $f_i = 0$. On dira qu'une courbe définie par un polynôme irréductible est une courbe irréductible. La décomposition $X = \cup_i X_i$ est la décomposition de X en composante irréductibles.

Si $k = \mathbb{R}$, le point $(0, 0)$ devrait être appelé une courbe car il est défini par l'équation $x^2 + y^2 = 0$ ou par $x^6 + y^6 = 0$. Une de ces équations est irréductible, l'autre est réductible. De telles ambiguïtés n'existent pas sur un corps algébriquement clos.

Lemme 0.0.1 *Soient k un corps quelconque, $f \in k[X, Y]$ un polynôme irréductible, $g \in k[X, Y]$ un polynôme quelconque non divisible par f. Alors le système d'équations*

$$f(x, y) = g(x, y) = 0$$

a un nombre fini de solutions.

Si k est un corps algébriquement clos, si $f \in k[X, Y]$ est non constant, alors l'équation $f(x, y) = 0$ a une infité de solutions. On en déduit, dans ce cas, grâce au lemme qu'un polynôme irréductible f est entièrement déterminé (à multiplication par une constante près) par la courbe d'équation $f(x, y) = 0$.

Le nombre de racines d'un polynôme dans k est égal au degré. Le célèbre théorème de Bezout généralise ce résultat en donnant le nombre de points d'intersection en fonction des degrés de f et g (si k est algébriquement clos) et en comptant les points à l'infini.

Si on considère le cas des coniques, on voit qu'il faut préciser certains détails notamment, tenir compte des points à l'infini.

0.1 Courbes rationnelles

Certaines courbes peuvent être paramétrées par des fonctions rationnelles.

Par exemple : $x^2 + y^2 = 1$, $y^2 = x^3 + x^2$.

On dit que ce sont des *courbes rationnelles.*

Exercice : la courbe $y^2 = x^3 - x$ n'est pas rationnelle.

0.2 Fonction Zeta

Soit $\mathbb{F}_q$ le corps de cardinal q. Soit X une courbe irréductible d'équation $f(x,y) = 0$ où $f \in \mathbb{F}_q[X,Y]$.

Pour tout n on note N_n le cardinal de $X(\mathbb{F}_{q^n})$. Pour tenir compte de tous les N_n, on considère la série $\sum_{n\geq 1} N_n \frac{t^n}{n}$.

Théorème 0.2.1 (Weil-Dwork) *La série* $\exp\left(\sum_n N_n \frac{t^n}{n}\right)$ *est une fonction rationnelle notée* $Z_X(t)$.

Exemples : Si $X = (x^2 + y^2 = 1)$, alors $Z_X(t) = (1-t)/(1-qt)$ si $q = -1 \bmod 4$, $(1+t)/(1-qt)$ si $q = 3 \bmod 4$.

Certains invariants connus de X se retrouvent dans Z_X. Par exemple le genre ...

Chapitre 1

Courbes affines

1.1 Ensembles algébriques affines

Soit k un corps quelconque (commutatif *quand même ! quand même ...)*
Si $n \geq 1$, on note $\mathbb{A}^n(k)$ ou $\mathbb{A}^n := k^n$.

1.1.1 Topologie de Zariski

Si $S \subseteq k[X_1, ..., X_n]$, on note $V(S) := \{x \in \mathbb{A}^n \ : \ \forall\, f \in S,\, f(x) = 0\}$
Remarque : $V(S) = V(\langle S \rangle)$.

Proposition 1.1.1 *Les ensembles de la forme $V(I)$, I idéal de $k[X]$ sont les fermés d'une topologie de $\mathbb{A}^n$: la topologie de Zariski .*

Démonstration : $\emptyset = V((1))$, $\mathbb{A}^n = V(0)$, $V(I) \cup V(J) = V(IJ)$, $\bigcap_i V(I_i) = V(\sum_i I_i)$. **Q.e.d.**

Les fermés de $\mathbb{A}^n$ pour la topologie de Zariski sont appelés des *ensembles algébriques affines* .

Ex. : les fermés de $\mathbb{A}^1$ sont les ensembles finis et $\mathbb{A}^1$; les fermés irréductibles de $\mathbb{A}^2$ sont les réunions finies de courbes algébriques planes irréductibles et de points.

1.1.2 Théorème des zéros de Hilbert

On dit qu'un morphisme d'anneaux $\phi : B \to A$ est *fini* si A est un $\phi(B)-$module de type fini *i.e.* si A est une $\phi(B)-$ algèbre de type fini et si tous les éléments de A sont entiers sur $\phi(B)$.

Théorème 1.1.2 (de normalisation de Nöther) *Soit A une $k-$algèbre de type fini. Il existe un entier $n \geq 0$ et un morphisme fini injectif $k[T_1, ..., T_n] \to A$.*

Démonstration : *Dans le cas où k est fini.* Soient $a_1, ..., a_r$ des générateurs de A. On raisonne par récurrence sur r. Si $0 \neq F \in k[X_1, ..., X_r]$ annule $(a_1, ..., a_r)$, alors soit F_d la composante homogène non nulle de plus haut degré ($=: d$) de F. Puisque k est infini, il existe $t_1, ..., t_r \in k$ non tous nuls tels que $F_d(t_1, ..., t_r) \neq 0$. Quitte à renuméroter les a_i, on peut supposer $t_r \neq 0$. Comme F_d est homogène, on peut supposer $t_r = 1$. Alors $F(a_1, ..., a_r) = \underbrace{F_d(t_1, ..., t_{r-1}, 1)}_{\neq 0} a_r^d +$ *termes de degré* $< d$ *en* a_r. Donc $A = k[a_1, ..., a_r]$ est entier sur $k[a_1, ..., a_{r-1}]$ et on peut appliquer l'hypothèse de récurrence à $k[a_1, ..., a_{r-1}]$. **Q.e.d.**

Si $x \in \mathbb{A}^n$, on note $\mathfrak{m}_x$ l'idéal $(X_1 - x_1, ..., X_n - x_n)$.
Exercice : $\mathfrak{m}_x = \ker(f \mapsto f(x))$ est un idéal maximal de $k[X_1, ..., X_n]$.
Si k est algébriquement clos, ils sont tous de cette forme :

Corollaire 1.1.2.1 *i) Soit A un corps qui est une* $k-$*algèbre de type fini. Alors A est une extension finie de k.*

ii) Si k est algébriquement clos, si $\mathfrak{m}$ *est un idéal maximal de* $k[X_1, ..., X_n]$*, il existe* $x \in k^n$ *tel que* $\mathfrak{m} = \mathfrak{m}_x$*.*

Démonstration : i) soit $k[T_1, ..., T_n] \to A$ un morphisme fini injectif. Alors A corps $\Leftrightarrow k[T_1, ..., T_n]$ corps. Donc $n = 0$.

ii) on a $A/\mathfrak{m} = k$ d'après *i)* et on pose $x := (x_1, ..., x_n)$ où $x_i := X_i \bmod \mathfrak{m}$. **Q.e.d.**

Théorème 1.1.3 (des zéros de Hilbert) *Soit A une* $k-$*algèbre de type fini. Alors A est un anneau de Jacobson* i.e. *: pour tout idéal premier* $\mathfrak{p} \leq A$*, on a :*

$$\mathfrak{p} = \bigcap_{\substack{\mathfrak{m} \geq \mathfrak{p} \\ \mathfrak{m} \text{ maximal}}} \mathfrak{m} \ .$$

Démonstration : En quotientant par $\mathfrak{p}$, il suffit de montrer que si A est intègre, $\bigcap \mathfrak{m} = 0$ lorsque $\mathfrak{m}$ décrit les idéaux maximaux de A. Par l'absurde : soit $0 \neq x \in \bigcap \mathfrak{m}$. L'algèbre $A[x^{-1}]$ est de type fini sur k. Soit $\mathfrak{n}$ un idéal maximal de $A[x^{-1}]$. Le corps $A[x^{-1}]/\mathfrak{n}$ est une extension finie de k d'après le corollaire. Donc $k \leq A/\mathfrak{n} \cap A \leq A[x^{-1}]/\mathfrak{n} \Rightarrow A/\mathfrak{n} \cap A$ est une $k-$algèbre intègre de dimension finie donc un corps †. Donc $\mathfrak{n} \cap A$ est un idéal maximal de A donc contient x. Mais alors $x \in \mathfrak{n}$ ce qui est impossible acr x est inversible dans $A[x^{-1}]$. **Q.e.d.**

†. Soit B une $k-$algèbre intègre de dimension finie comme $k-$espace vectoriel, soit $0 \neq b \in B$, la multiplication par $b : y \mapsto by$ est injective donc surjective ! donc b a un inverse.

Cours du mercredi 29 janvier 2014

1.1.3 Correspondance entre idéaux radicaux et ensembles algébriques affines

Définition 1 *Soit I un idéal d'un anneau A. On pose* $\sqrt{I} := \{x \in A : \exists\, n > 0,\, x^n \in I\}$.

Exemple : $\sqrt{(x^2, y)} = (x, y)$ dans $k[x, y]$.

Remarque : $\sqrt{\sqrt{I}} = \sqrt{I}$.

On dit que I est un idéal *radical* si $\sqrt{I} = I$. Les idéaux premiers sont radicaux

Proposition 1.1.4

$$\sqrt{I} = \bigcap_{\substack{\mathfrak{p} \geq I \\ \mathfrak{p}\text{ premier}}} \mathfrak{p}\ .$$

On en déduit :

Proposition 1.1.5 *Si A est une $k-$algèbre de type fini, alors pour tout I idéal de A, on a :*

$$\sqrt{I} = \bigcap_{\substack{\mathfrak{m} \geq I \\ \mathfrak{m}\text{ maximal}}} \mathfrak{m}\ .$$

Si $Z \subseteq \mathbb{A}^n(k)$, on pose $I(Z) := \{f \in k[T_1, ..., T_n] \ :\ f|_Z = 0\}$.

Par exemple, $I(\emptyset) = (1)$ et $I(\mathbb{A}^n) = 0$.

Les idéaux $I(Z)$ sont toujours radicaux !

Exercice : Si $Z \subseteq \mathbb{A}^n$, alors $\overline{Z} = V(I(Z))$. En particulier, si Z est fermé, $Z = V(I(Z))$.

Deux idéaux peuvent avoir le même ensemble de zéros : on a toujours $V(I) = V(\sqrt{I})$.

Supposons k algébriquement clos.

On a : $I(Z) = \bigcap_{x \in Z} \mathfrak{m}_x$.

Proposition 1.1.6 *Si $I \leq k[T_1, ..., T_n]$, alors $I(V(I)) = \sqrt{I}$*

≪ *Les points sont des idéaux maximaux !* ≫

Corollaire 1.1.6.1 *Les applications :*

$$\{\ \textit{idéaux radicaux de } k[T]\} \longleftrightarrow \{\textit{fermés algébriques de } \mathbb{A}^n\}$$

$$I \longmapsto V(I)$$

$$I(Z) \longleftarrow\!\shortmid\ Z$$

sont des bijections réciproques. Les restrictions donnent des bijections réciproques :

$$\{ \text{ idéaux maximaux de } k[T]\} \longleftrightarrow \{\text{points de } \mathbb{A}^n\}$$

Par cette bijection, les idéaux premiers correspondent aux *fermés irréductibles.*

Exercice : si $Z \subseteq \mathbb{A}^n$ est un fermé algébrique, les points de Z sont en bijection avec les idéaux maximaux de $k[T_1, ..., T_n]$ qui contiennent $I(Z)$.

1.1.4 Espaces topologiques irréductibles

Définition 2 *Un espace topologique non vide X est irréductible si X n'est pas réunion de deux fermés propres. Un fermé de X est irréductible s'il est irréductible pour la topologie induite.*

Remarque : Cela revient à dire que deux ouverts non vides s'intersectent ou que tous les ouverts non vides sont denses.

Exemples :

a) Sur $\mathbb{R}$, muni de la topologie usuelle, seuls les points sont irréductibles.

Proposition 1.1.7 *i) Soit $f : X \to Y$ une application continue. Si $Z \subseteq X$ est irréductible, alors $f(Z)$ aussi.*

ii) Si $Y \subseteq Z \subseteq \overline{Y} \subseteq X$, alors Y irréductible $\Leftrightarrow$ Z irréductible.

Définition 3 *Un sous-espace irréductible maximal de X est une composante irréductible de X.*

Remarque : par le lemme de Zorn, toute partie irréductible de X est contenue dans une composante irréductible. De plus les composantes irréductibles sont fermées.

Proposition 1.1.8 *Soit $Z \subseteq \mathbb{A}^n(k)$ un fermé. Alors Z irréductible $\Leftrightarrow$ $I(Z)$ idéal premier.*

En particulier, $\mathbb{A}^n$ est irréductible.

Exercice : les fermés irréductibles de $\mathbb{A}^2$ sont les points, $\mathbb{A}^2$ et les $V(f)$ où $f \in k[X, Y]$ est un polynôme irréductible.

Exercice : Soit $f \in k[X, Y]$. On note $f = f_1^{a_1}...f_n^{a_n}$ la décomposition en facteurs irréductibles de f où les f_i sont deux à deux premiers entre eux. Alors, $I(V(f)) = (f_1...f_n)$ et les $V(f_i)$ sont les composantes irréductibles de $V(f)$.

1.1.5 Espaces nœthériens

Définition 4 *Un espace topologique X est nœthérien si toute suite décroissante de fermés est stationnaire.*

Lemme 1.1.9 *Soit X un espace topologique nœthérien. Alors :*

(i) tout sous-espace de X est nœthérien ;

(ii) tout ouvert de X est quasi-compact ;

(iii) Tout fermé de X a un nombre fini de composantes irréductibles.

Tout fermé de X est donc une union finie de composantes irréductibles.

Proposition 1.1.10 *L'espace $\mathbb{A}^n(k)$ est nœthérien.*

Corollaire 1.1.10.1 *Si I est un idéal radical de $k[T]$, alors I est l'intersection d'un nombre fini d'idéaux premiers qui ne se contiennent pas deux à deux. L'ensemble de ces idéaux premiers est déterminé par I.*

1.2 Dimension

Soit V un fermé algébrique affine de $\mathbb{A}^n$. On note $k[V] := \{f|_V \ : \ f \in k[T_1, ..., T_n]\}$.

Remarque : $k[V] \simeq k[T_1, ..., T_n]/I(V)$ est de type fini réduite.

Proposition 1.2.1 *Si I est un idéal de $k[V]$, on note $V_V(I) := \{x \in V \ : \ \forall\, f \in I, f(x) = 0\}$ et si $Z \subseteq V$, on note $I_V(Z) := \{f \in k[V] \ : \ \forall\, z \in Z,\, f(z) = 0\}$. On a :*

$$I_v(V_V(I)) = \sqrt{I}$$

pour tout idéal I de $k[V]$.

Démonstration : On utilise la bijection $J \mapsto J \bmod I(V)$ entre les idéaux de $k[T_1, ..., T_n]$ contenant $I(V)$ et les idéaux de $k[V]$. **Q.e.d.**

Définition 5

$$\dim V := \partial_k k[V]$$

$:= \max\{r \ : \ ^{\exists}\, , x_1, ..., x_r \in k[V]$ *algébriquement indépendants sur* $k\}$.

Voici quelques propriétés :

Proposition 1.2.2 $\dim V = 0 \Leftrightarrow V$ *fini. Dans ce cas* $|V| = \dim_k k[V]$.

Démonstration : si $\dim V = 0$, alors $k[V]$ est de dimension finie sur k (tous les x_i, générateurs de $k[V]$ sont lagébriques sur k). Si $\mathfrak{m}_1, ..., \mathfrak{m}_n$ sont des idéaux maximaux deux à deux distincts de $k[V]$, alors $\dim_k k[V] \geq \dim_k k[V]/\mathfrak{m}_1 \cap ... \cap \mathfrak{m}_n = \sum_i \dim k[V]/\mathfrak{m}_i = n$. Donc il y a un nombre fini d'idéaux maximaux de $k[V]$: $\mathfrak{m}_1, ..., \mathfrak{m}_n$. Comme $k[V]$ est réduite, $k[V] \simeq \oplus_i k[V]/\mathfrak{m}_i$ est de dimension n sur k. **Q.e.d.**

Proposition 1.2.3 *i)* $V_1 \leq V_2 \Rightarrow \dim V_1 \leq \dim V_2$ *;*

ii) si $F \leq V$, V *irréductible,* $\dim F = \dim V \Rightarrow F = V$ *;*

iii) si $V = V_1 \cup ... \cup V_r$ *est la décomposition de* V *en composantes irréductibles, alors* $\dim V = \max \dim V_i$.

1.2.1 Degré de transcendance

Soit $k \leq K$ une extension de corps quelconque. si $x_1, ..., x_n \in K$ sont algébriquement indépendants sur k et si K est algébrique sur $k(x_1, ..., x_n)$, on dit que $\{x_1, ..., x_n\}$ est une base de transcendance de K sur k.

Proposition 1.2.4 *i) Les bases de transcendance ont toutes le même cardinal : c'est le degré de transcendance de* K/k *;*

ii) (théorème de la base incomplète) : si K *est algébrique sur* $k(a_1, ..., a_n)$, *si* $a_1, ..., a_m$ *sont algébriquement indépendants sur* k, $m \leq n$, *alors il existe* $1 \leq i_1 < ... < i_p \leq n$ *tels que* $a_1, ..., a_m, a_{i_1}, ..., a_{i_p}$ *forment une base de transcendance de* K/k.

Exemple : $\mathrm{degtr}(k(X_1, ..., X_n)/k) = n$.

Proposition 1.2.5 *Soit* $f \in k[T_1, ..., T_n]$ *non constant. Toutes les composantes irréductibles de* $H_f := V(f)$ *sont de dimension* $n - 1$.

Démonstration : Il suffit de traiter le cas où f est irréductible. Supposons par exemple que la variable T_n apparaît dans f. Notons $t_i := T_i \bmod (f)$. Si $P \in k[T_1, ..., T_{n-1}]$, alors $P(t_1, ..., t_{n-1}) = 0$ dans $k[T_1, ..., T_n]/(f) = k[t_1, ..., t_n] \Rightarrow f|P$ dans $k[T_1, ..., T_n] \Rightarrow P = 0$ car $\deg_{T_n} f > 0$. Donc $t_1, ..., t_{n-1}$ sont algébriquement indépendants. Donc $t_1, ..., t_{n-1}$ ou $t_1, ..., t_n$ est une base de transcendance de $\mathrm{Frac} k[t_1, ..., t_n]$ sur k. Comme $f(t_1, ..., t_n) = 0$, c'est $t_1, ..., t_{n-1}$ qui est une base de transcendance. **Q.e.d.**

Proposition 1.2.6 *Si* V *est un fermé algébrique irréductible de* $\mathbb{A}^n$, *alors* $\dim V = \mathrm{degtr} k(V)/k$ *où* $k(V) := \mathrm{Frac} k[V]$.

En particulier si V est un sous-espace linéaire de k^n, on retrouve la dimension usuelle.

Cours du mercredi 5 février 2014

1.2.2 Autre façon de définir la dimension

Soit I un idéal de $k[T_1,...,T_n]$. On pose $H_I(s) := \dim k[T_1,...,T_n]_{\leq s}/I_{\leq s}$.
Exemple : $H_0(s) = \binom{s+n}{n}$.

Proposition 1.2.7 *Pour s assez grand, $H_I(s)$ est un polynôme en s.*

Pour un $n-$uplet $\alpha = (\alpha_1,...,\alpha_n)$, on notera $|\alpha| := \alpha_1 + ... + \alpha_n$.

Démonstration : Soit $\leq$ un ordre total sur les monômes tel que si $|a| < |b|$, $T^a < T^b$. On note $TD(f)$ le terme dominant d'un polynôme $f \in k[T_1,...,T_n]$ pour cet ordre et $TD(I)$ l'idéal engendré par les $TD(f)$, $f \in I$. Alors $H_I(s) = H_{TD(I)}(s)$ car les classes $T^\gamma \bmod I$ (respectivement $\bmod TD(I)$), où $|\gamma| \leq s$ et $T^\gamma \notin TD(I)$, forment une base de $k[T_.1,...,T_n]_{\leq s}/I_{\leq s}$ (respectivement de $k[T_1,...,T_n]_{\leq s}/TD(I)_{\leq s}$). Or si on pose $A := k[T_1,...,T_n]$, si I, J sont des idéaux homogènes, on a une suite exacte de $k-$espaces vectoriels qui préserve les degrés :

$$0 \to A/I \cap J \to A/I \oplus A/J \to A/I + J \to 0$$

$$x \mapsto x \bmod I \oplus x \bmod J,\ x \oplus y \mapsto x - y\ .$$

On montre ensuite que $H_{TD(I)}(s)$ est un polynôme en raisonnant par récurrence sur le nombre minimal de monômes générateurs de $TD(I)$. On utilise pour cela, par exemple que si $I = \langle T^{\gamma_1},...,T^{\gamma_r}\rangle$ et si $J = \langle T^\gamma\rangle$, alors $I \cap J = \langle g_1,...,g_r\rangle$ où $g_i = \text{ppcm}(T^{\gamma_i}, T^\gamma)$. **Q.e.d.**

Proposition 1.2.8 *Si $A = k[T_1,...,T_n]/I$ est une $k-$algèbre de type fini, si $k[X_1,...,X_r] \to A$ est un morphisme injectif fini, alors* $\deg H_I(s) = r = \partial_k(A)$.

Démonstration : Notons $f_1,...,f_r$ les images respectives de $X_1,...,X_r$. Soit $d := \max\{\deg f_i\ :\ 1 \leq i \leq r\}$. Alors $H_I(sd) \geq \dim k[X_1,...,X_r]_{\leq s} = \binom{s+r}{r}$. Donc $\deg H_I(s) \geq r$. Soit $B := k[f_1,...,f_r]$. Le $B-$module A est de type fini donc $A = Bb_1 + ...Bb_N$ pour certains $b_i \in A$. On peut supposer, quitte à les ajouter, que parmi les b_i, il ya les $a_i := T_i \bmod I$. De plus $b_ib_j = \sum_{k=1}^N b_{i,j}^k b_k$ pour certains $b_{i,j}^k \in B$. Si on note $q := \max\{b_{i,j}^k\}$, alors on a facilement par récirrence que $a_1^{\alpha_1}...a_n^{\alpha_n} \in B_{\leq|\alpha|d}b_1 + ... + B_{\leq|\alpha|d}b_N$. Donc $\dim A_{\leq s} \leq N \dim B_{\leq sd} = N\binom{sd+r}{r} = N\frac{(sd+1)...(sd+r)}{r!}$. D'où $\deg H_I(s) \leq r$. **Q.e.d.**

Exercice : Si $\dim V = d$, $V \leq \mathbb{A}^n$, il existe E un sous-espace de k^n de dimension d, un morphisme linéaire : $f : \mathbb{A}^n \to E$ tel que $f|_V : V \to E$ est surjectif de fibres finies *(indication : utiliser le théorème de normalisation de Nöther).*

Exemple : $A = k[X,Y]/(XY-1)$. $H_I(s) = \binom{s+2}{s} - \binom{s}{s-2} = 2s+1$. Posons $x := X \bmod XY-1$, $y := Y \bmod XY-1$. Alors $x, -y$ sont solutions de l'équation $T^2-(x-y)T-1 = (T-x)(T+y) \in k[x-y][T]$; donc A est entier sur $k[x-y]$ et $x-y$ est algébriquement indépendant sur k. Et $\mathbb{A}^2 \to \mathbb{A}^1$, $(x,y) \mapsto x-y$ est surjective de fibres de cardinal 1 ou 2.

1.2.3 Définition des courbes algébriques affines

Définition 6 *Soit $C \subseteq \mathbb{A}^n$ un fermé algébrique irréductible de dimension 1. On dit que C est une courbe algébrique affine irréductible. Si $f \in k[X,Y]$ est un polyn ôme non constant, on dit que $V(f)$ est une courbe algébrique plane.*

Conséquence : Les fermés propres des courbes irréductibles : points.

Exemple : $V(y^2-xy-x^2y+x^3)$ est une courbe algébrique plane, $\{(t^3,t^4,t^5) : t \in \mathbb{A}^1\} = \{(x,y,z) \in \mathbb{A}^3 : x^3 = yz, y^2 = xz, z^2 = x^2y\}$ est une courbe algébrique irréductible.

Exercice : l'idéal $I(C)$ de la courbe $C := \{(t^3,t^4,t^5) : t \in \mathbb{A}^1\}$ ne peut être engendré par moins de 3 éléments ! néanmoins, la courbe C peut être définie par deux équations dans $\mathbb{A}^3$!

indication : $I(C)$ est engendré par x^3-yz, y^2-xz, z^2-x^2y car $k[x,y,z]/(x^3-yz, y^2-xz, z^2-x^2y) = k[\overline{x}] + k[\overline{x}]\overline{y} + k[\overline{x}]\overline{z}$ donc $k[x,y,z]/(x^3-yz, y^2-xz, z^2-x^2y) \to k[t^3,t^4,t^5]$ est un iso. Et $C = V(g, f_2)$ où $g := \frac{f_2^3+z^3f_1}{y}$ (on a : $y \notin I(C) \Rightarrow g \in I(C)$)).

1.3 Applications régulières, isomorphismes

Soit $f : U \to \mathbb{A}^1$ une fonction définie sur un ouvert U d'un fermé algébrique X de $\mathbb{A}^n$. On dit que f est *régulière* en $x \in U$ s'il existe un ouvert $x \in V \subseteq U$, $a, b \in k[X]$ tels que $\forall\, y \in V$, $b(y) \neq 0$ et $f(y) = a(y)/b(y)$.

Notation : $\mathcal{O}_X(U)$ est l'algèbre des fonctions régulières sur l'ouvert U de X.

Voici une conséquence du théorème des zéros de Hilbert :

Proposition 1.3.1 *Soit $X \subseteq \mathbb{A}^n$ un fermé algébrique.*

i) $\mathcal{O}_X(X) = k[X]$;

ii) si $f \in k[X]$ est non nulle, alors $k[X_f] = k[X][f^{-1}]$ (où $X_f := \{x \in X : f(x) \neq 0\}$ et $k[X][f^{-1}]$ est l'algèbre des fonctions sur X_f engendrée par $k[X]$ et la fonction $t \mapsto 1/f(t)$).

Contre-exemple : si $k = \mathbb{C}$, $\mathbb{A}^1 \to \mathbb{A}^1$, $x \mapsto e^x$ n'est pas régulière.

Exercice : $k[\mathbb{A}^2 \setminus \{0\}] = k[\mathbb{A}^2]$.

Plus généralement, on dit que $F : U \to \mathbb{A}^n$, $x \mapsto (f_1(x), ..., f_n(x))$ est régulière si tous les $f_i : U \to \mathbb{A}^1$ le sont.

Définition 7 *Si $X \subseteq \mathbb{A}^m$ et $Y \subseteq \mathbb{A}^n$, si $U \subseteq X$ et $V \subseteq Y$ sont des ouverts, un morphisme $f : U \to V$ est une application telle que $f : U \to \mathbb{A}^n$ est régulière. Un isomorphisme $f : U \to V$ est un morphisme bijectif dont l'application réciproque $f^{-1} : V \to U$ est aussi un morphisme.*

Remarque importante : si $U = \cup_a U_a$ est un recouvrement ouvert, si $\forall\, a, f|_{U_a} : U_a \to \mathbb{A}^n$ est régulière, alors f est régulière.

Exemple : $\mathbb{A}^1 \setminus \{0\} \to V(XY - 1)$, $t \mapsto (t, t^{-1})$ est un isomorphisme.

Contre-exemple : $\mathbb{A}^1 \to V(Y^2 - X^3)$, $t \mapsto (t^3, t^2)$ est un morphisme bijectif qui n'est pas un isomorphisme.

Exercice : déterminer l'image de $f : \mathbb{A}^2 \to \mathbb{A}^2$, $(x, y) \mapsto (x, xy)$. Est-elle ouverte ? dense ? fermée ?

Remarque : Si $f : U \to V$, $g : V \to W$ sont des morphismes entre ouverts de fermés algébriques, alors $g \circ f : U \to W$ est aussi un morphisme.

Notation : soit $F : X \to Y$ un morphisme entre fermés algébriques. On note $F^* : k[Y] \to k[X]$, $h \mapsto h \circ F$ le morphisme d'algèbres associé.

Proposition 1.3.2 *(i) $F \mapsto F^*$ est une bijection entre les morphismes de variétés $X \to Y$ et les morphismes d'algèbres $k[Y] \to k[X]$;*

(ii) L'application F est un isomorphisme si et seulement si $F^* : k[Y] \to k[X]$ est un isomorphisme de $k-$algèbres.

Démonstration :

i) On suppose que Y est un fermé de $\mathbb{A}^N$. Voici la réciproque : si $\phi : k[Y] \to k[X]$ est un morphisme de $k-$algèbres, on pose $F_\phi := (f_1, ..., f_N)$ où les f_i sont les images par ϕ des fonctions coordonnées $T_i|_Y$, $1 \leq i \leq N$.

ii) il suffit de vérifier que $(F \circ G)^* = G^* \circ F^*$.

Q.e.d.

Exemple : $\{(t^2, t^3, t^5) \ : \ t \in k\} = V(z - xy, y^2 - x^3) \simeq V(y^2 - x^3) \subseteq \mathbb{A}^2$ est une courbe plane mais $\{(t^3, t^4, t^5) \ : \ t \in k\} = V(x^3 - yz, y^2 - xz, z^2 - x^2y)$ n'est pas isomorphe à une courbe plane.

Exercice : on suppose k de caractéristique $\neq 2$. Montrer que $f : \mathbb{A}^1 \to X := V(Y^2 - X^2 - X^3)$, $t \mapsto (t^2 - 1, t(t^2 - 1))$ induit un isomorphisme $f^* : k[X] \simeq A$ où A est la sous-algèbre de $k[t]$ formé des g tels que $g(1) = g(-1)$.

Proposition 1.3.3 *soient U, V des ouverts de fermés algébriques affines. Soit $F : U \to V$ un morphisme. Alors F est continue et pour tout ouvert W de V, tout $f \in \mathscr{O}_V(W)$, $f \circ F \in \mathscr{O}_U(F^{-1}W)$.*

Réciproquement, si $F : U \to V$ est une application continue telle que :

$$\forall\, f \in \mathscr{O}_V(W),\ f \circ F \in \mathscr{O}_U(F^{-1}W)$$

alors F est un morphisme.

Définition 8 (pôles d'une fonction rationnelle) *Soit X un fermé algébrique irréductible. Soit $f \in k(X)$. On dit que f est régulière en $x \in X$ s'il existe $a, b \in k[X]$ tels que $b(x) \neq 0$ et $f = a/b$ (dans $k(X)$). Dans ce cas, on pose $f(x) := a(x)/b(x)$ (c'est indépendant du couple (a, b) choisi. Sinon, on dit que x est un pôle de f.*

Exercice : Soit $X = V(x^2 + y^2 - 1)$. Alors $f := (1 + x)/y \in k(X)$ a pour pôle unique $(1, 0)$ *(indication : $f = y/(1 - x)$ est régulière en $(-1, 0)$.*

1.4 Courbes rationnelles

Définition 9 (Résultant) *Soient* $P := a_pX^p + ... + a_0, Q := b_qX^q + ... + b_0 \in A[X]$ *où* A *est un anneau.*

$$\textit{Soit } \mathrm{Rés}_{p,q}(P,Q) := \begin{vmatrix} a_p & ... & a_0 & & \\ & & & & \\ b_q & ... & b_0 & & \\ & & & & \end{vmatrix} \in A$$

(q lignes avec les coefficients de P *et p lignes avec ceux de* Q *: c'est un déterminant* $p+q \times p+q$*). C'est le résultant de* P *et* Q*.*

Remarques : si $a_p = b_q = 0$, alors $\mathrm{Rés}_{p,q} = 0$; si $\phi : A \to B$ est un morphisme d'anneaux, alors $\phi(\mathrm{Rés}_{p,q}(P,Q)) = \mathrm{Rés}_{p,q}(P^\phi, Q^\phi)$; $\mathrm{Rés}_{p,q}(P,Q) = a_p^q b_o^p + (-1)^{(q-1)p} a_0^q b_q^p +$ des termes de degrés $< p$ en b_0 et $< q$ en a_0 (car, par exemple, la diagonale est $(\underbrace{a_p, ..., a_p}_{q}, \underbrace{b_0, ..., b_0}_{p})$).

Proposition 1.4.1 *Soit* k *un corps algébriquement clos, soient* P, Q *de degrés* $\leq p, q$*. Alors :*

$$\mathrm{Rés}_{p,q}(P,Q) = 0 \Leftrightarrow$$

$$P, Q \textit{ ont une racine commune dans } k \textit{ ou } \deg P < p, \deg Q < q \ .$$

Démonstration : Le résultant est le déterminant de la matrice de :

$$k[X]_{\leq q-1} \oplus k[X]_{\leq p-1} \longrightarrow k[X]_{\leq p+q-1}$$

$$U \oplus V \longmapsto PU + QV$$

dans les bases $(X^{q-1}, ..., 1, X^{p-1}, ..., 1)$ et $(X^{p+q-1}, ..., 1)$. **Q.e.d.**

Théorème 1.4.2 *Soient* $F, G \in k(t)$*. On suppose que* F *ou* G *est non constante. Alors il existe une unique courbe affine plane irréductible* C *qui contient l'image de :*

$$t \mapsto (F(t), G(t))$$

de plus, « le paramétrage évite au plus un point de C *»*

Démonstration : Si $F = A/B$, $G = C/D$, on considère : $\mathrm{Rés}(A - XB, C - YD) \in k[X,Y]$. **Q.e.d.**

Exemple : $F(t) = (1-t^2)/(1+t^2)$, $G(t) = 2t/(1+t^2)$, $R(X,Y) = \mathrm{Rés}_{2,2}(1 - t^2 - X(1+t^2), 2t - Y(1+t^2) = 4(X^2 + Y^2 - 1)$, donc $C = V(x^2 + y^2 - 1)$ Seul le point $(-1,0)$ exclu du paramétrage.

Définition 10 *On dit qu'une courbe C affine plane irréductible est rationnelle s'il existe F, G tels que F ou G est non constante et telle que l'image de :*

$$t \mapsto (F(t), G(t))$$

est contenue dans C.

Exemples : les droites et les graphes de fonctions rationnelles, les coniques

Théorème 1.4.3 *Soit C une courbe affine plane irréductible. Sont équivalentes :*

(i) C est rationnelle ;

(ii) il existe $f \in k(C)$ telle que $k(C) = k(f)$;

(iii) le corps $k(C)$ est $k-$isomorphe à $k(t)$.

De plus, il existe dans ce cas un isomorphisme : $\mathbb{A}^1 \setminus S \to C \setminus T$ pour des parties finies S de $\mathbb{A}^1$ et T de C.

Pour démontrer ce théorème, on utilise le :

Théorème 1.4.4 (Lüroth) *(Pour cet énoncé, k n'est pas forcément algébriquement clos) Soit $k \leq K \leq k(T)$ un corps tel que $k \neq K$. Alors il existe $x \in k(T)$ tel que $K = k(x)$.*

Lemme 1.4.5 *Soit $f/g \in k(T)$ une fraction irréductible non constante. Alors $[k(T) : k(f/g)] = \max\{\deg f, \deg g\}$.*

Démonstration : Considérons $F := g(X)f/g - f(X) \in k(f/g)[X]$. Le polynôme F est de degré $d := \max\{\deg f, \deg g\}$, annule t et F est irréductible dans $k(X)[f/g]$ donc dans $k[X, f/g]$ donc dans $k(f/g)[X]$.

Q.e.d.

Remarque : si k est algébriquement clos, le nombre $\max\{\deg f, \deg g\}$ est le cardinal maximal des fibres de l'application $\mathbb{A}^1 - - - > \mathbb{A}^1$, $t \mapsto f(t)/g(t)$.

Démonstration du théorème de Lüroth : Soit $f(X) = X^d + a_1 X^{d-1} + ... + a_d \in K[X]$ le polynôme minimal de t sur K. Soit i tel que $a_i \notin k$. On a $a_i = p/q$ où $p, q \in k[t]$ sont premiers entre eux. Soit $c(t) \in k[t]$ le ppcm des dénominateurs des coefficients de f écrits sous forme de fractions irréductibles $\in k(t)$. Soit $c(t) =: F(X,t) \in k[t, X]$. Posons $R(X,t) := q(X)p(t) - q(t)p(X)$. On a $f|R/q(t)$ dans $K[X]$. Donc dans $k(t)[X]$ aussi. Donc $F|R$ dans $k(t)[X]$. Puisque $R \in k[t][X]$ est de contenu 1, $F|R$ dans $k[t, X]$. Mais alors $\max\{\deg p, \deg q\} \leq \deg_t F \leq \deg_t R = \max\{\deg p, \deg q\}$. Donc $a(X)F = R$ pour un certain $a \in k[X]$. Comme le contenu de R dans $k[X][t]$ est 1, a est une constante. D'où $\deg_X F = \max\{\deg p, \deg q\}$. Or, $k(p/q) \leq K \leq k(t)$, et :

$$[k(t) : K] = \deg_X f = \max\{\deg p, \deg q\} = [k(t) : k(p/q)] \ .$$

Donc $k(p/q) = K$. **Q.e.d.**

Démonstration : Si $k(C) \simeq k(t)$, on note x, y les fonctions coordonnées sur C. Soient $f(t), g(t) \in k(t)$ les images de x et y dans $k(t)$. Soit $r \in k(C)$ l'antécédent de t.

Alors on a deux isomorphismes réciproques l'un de l'autre :

$$\begin{tikzcd} \mathbb{A}^1 \setminus S \arrow[r, "\sim"] & C \setminus T \\ t \arrow[r, mapsto] & (f(t), g(t)) \\ r(x,y) & (x,y) \arrow[l, mapsto] \end{tikzcd}$$

où $S = \{t \in \mathbb{A}^1 : t$ est un pôle de f ou de g ou $(f(t), g(t))$ est un pôle de $r\}$ et $T = \{(x,y) \in C : (x,y)$ est un pôle de $r\}$. **Q.e.d.**

Exemple : $\mathbb{A}^1 \setminus \{\pm i\} \simeq V(x^2 + y^2 - 1) \setminus \{(1,0)\}$, $t \mapsto ((1-t^2)/(1+t^2), 2t/(1+t^2))$, $y \mapsto y/(1+x)$.

Exercice :

a) les courbes $x^n + y^n = 1$, $n \geq 3$ ne sont pas rationnelles,

b) $y^2 = x^3 - x$ n'est pas rationnelle,

c) $y^2 = x^3 - x^2$ est rationnelle.

Cours du mercredi 19 février 2014

1.5 Singularités

1.5.1 Multiplicité

Soit $C \subseteq \mathbb{A}^2$ une courbe affine plane. Soit F un générateur de $I(C)$. Soit $(x_0, y_0) \in C$. On a :

$$F = F_d + F_{d+1} + ...$$

où $d \geq 1$ et les F_k sont des polynômes homogènes en $X - x_0, Y - y_0$:

$$F_k = \sum_{\substack{i,j \geq 0 \\ i+j=k}} a_{i,j} (X - x_0)^i (Y - y_0)^j$$

pour certains $a_{i,j} \in k$ et où $F_d \neq 0$. On dit que d est la *multiplicité* de C en $P := (x_0, y_0) =: m_P(C)$.

On dit que P est *lisse* si $m_P(C) = 1$, singulier si $m_P(C) \geq 2$. Autrement dit, le point P est lisse si et seulement si $\partial_X F(P)$ ou $\partial_Y F(P) \neq 0$.

Le polynôme F_d se factorise en $F_d = L_1 ... L_d$ où les L_j sont des formes linéaires (en $X - x_0, Y - y_0$). Les droites d'équations $L_j = 0$ sont les tangentes de C en P. Si toutes les tangentes sont distinctes, on dit que P est un point (double, triple, ...) *ordinaire*.

Exemple : $(0,0)$ *est un point double ordinaire pour la courbe d'équation* $y^2 = x^3 + x^2$ *et un point double non ordinaire pour* $y^2 = x^3$.

Remarque : La définition ne dépend pas du générateur choisi.

Définition 11 *Soit* $C \subseteq \mathbb{A}^2$ *une courbe affine plane. Si tous les points sont lisses, on dit que* C *est lisse.*

Exemples : les droites affines, les graphes de polynômes, le cercle et toutes les coniques irréductibles sont lisses mais $V(xy)$ n'est pas lisse.

Remarque : Si $0 \neq F \in I(C)$, alors $I(C) = (F) \Leftrightarrow F$ sans facteur carré et $C = V(F)$. Et, F sans facteur carré $\Leftrightarrow$ pgcd$(F, \partial_X F, \partial_Y F) = 1$.

1.5.2 Anneaux des fonctions régulières au voisinage d'un point

Définition 12 *Soit* X *un fermé d'une variété algébrique (ou simplement un ouvert d'un fermé algébrique. Si* $x \in X$*, on note* $\mathscr{O}_{X,x}$ *la* $k-$*algèbre :*

$$\{(f, U) \ : \ U \text{ est un voisinage ouvert de } x \text{ et } f \in \mathscr{O}_X(U)\} / \sim$$

où $(f, U) \sim (g, V)$ *s'il existe un voisinage ouvert* W *de* x *tel que* $W \subseteq U \cap V$ *et* $f|_W = g|_W$*. On note* $\mathfrak{m}_{X,x} := \{f \in \mathscr{O}_{X,x} \ : \ f(x) = 0\}$

Proposition 1.5.1 *L'anneau* $\mathscr{O}_{X,x}$ *est local d'idéal maximal* $\mathfrak{m}_{X,x}$ *et* $\mathscr{O}_{X,x}/\mathfrak{m}_{X,x} \simeq k$.

Exercice : vérifier que $\mathscr{O}_{X,x} \simeq k[X]_{M_x}$ où M_x est l'idéal maximal de $k[X]$ qui s'annule en x. Rappelons que $k[X]_{M_x} = \{a/b \ : \ a, b \in k[X], \ b \notin M_x\}$ où $a/b = a'/b'$ s'il existe $c \notin M_x$ tel que $c(b'a - ab') = 0$.

1.5.3 Caractérisation intrinsèque de la lissité

Lemme 1.5.2 *Soit* C *une courbe affine. Soit* $P \in C$*. Notons* M_P *l'idéal maximal de* $k[C]$ *définissant* P*. Alors pour tout* $n \geq 0$, $M_P^n / M_P^{n+1} \simeq \mathfrak{m}_{C,P}^n / \mathfrak{m}_{C,P}^{n+1}$.

Remarque : si F est un générateur de $I(C)$, si $P = (0,0)$, alors $M_P^n / M_P^{n+1} \simeq M^n + (F) / M^{n+1} + (F)$ où $M := (X, Y) \leq k[X, Y]$.

Exercice : vérifier que pour tout $n \geq m_P(C)$, $m_P(C) = \dim_k \mathfrak{m}_{C,P}^n / \mathfrak{m}_{C,P}^{n+1}$ et que pour tout $0 \leq n < m_P(C)$, $\dim_k \mathfrak{m}_{C,P}^n / \mathfrak{m}_{C,P}^{n+1} = n + 1$.

Proposition 1.5.3 *Soit* C *une courbe affine plane irréductible. Soit* $P \in C$*. Sont équivalentes :*

(i) C *est lisse en* P *;*

(ii) $\dim_k M_P/M_P^2 = 1$ *;*

(iii) $\dim_k \mathfrak{m}_{C,P}/\mathfrak{m}_{C,P}^2 = 1$.

Démonstration : $ii \Rightarrow i$: Soit f un générateur de $I(C)$, si C n'est pas lisse en $P = (0,0)$, alors $f \in (X,Y) \leq k[X,Y]$. Mais alors, $M_P/M_P^2 \simeq (X,Y)/(X,Y)^2$ qui est de dimension 2 *absurdo !* **Q.e.d.**

Soit C une courbe affine irréductible. Soit $x \in C$.

Lemme 1.5.4 *Soit* I *un idéal premier non nul de* $\mathscr{O}_{C,x}$*. Alors* $I = \mathfrak{m}_x$*.*

Démonstration : Soit I un idéal premier non nul de $k[C]$, alors $k[C]/I = k[V_C(I)]$ est une $k-$algèbre de dimension finie intègre donc c'est un corps et I est maximal ! **Q.e.d.**

Lemme 1.5.5 *Tout idéal non nul de* $\mathscr{O}_{C,x}$ *contient une puissance de* $\mathfrak{m}_x$*.*

Proposition 1.5.6 *Supposons que la courbe* C *est plane mais non forcément irréductible. Soit* $P \in C$*. Alors* P *est lisse* $\Leftrightarrow$ $\mathfrak{m}_{C,P}$ *est un idéal principal de l'anneau* $\mathscr{O}_{C,P}$

Démonstration : Soit $t \in \mathfrak{m} \setminus \mathfrak{m}^2$ où $\mathfrak{m} := \mathfrak{m}_{C,P}$. Alors, $t \bmod \mathfrak{m}^2$ engendre $\mathfrak{m}/\mathfrak{m}^2$. Donc $\mathfrak{m}.\mathfrak{m}/(t) = \mathfrak{m}/(t)$ d'où, par le lemme de Nakayama : $\mathfrak{m}/(t) = 0$ *i.e.* $\mathfrak{m} = (t)$. **Q.e.d.**

Remarque : en général, même si P est lisse, M_P n'est pas principal : par ex. : $V(y^2 - x^3 + x)$ *(exo).*

Lemme 1.5.7 *Soit* $P \in C$*. Tout idéal propre non nul de* $\mathscr{O}_{C,P}$ *contient un idéal de la forme* $\mathfrak{m}_{C,P}^n$*,* $n \geq 1$*.*

Théorème 1.5.8 *Soit* C *une courbe affine plane. Soit* $P \in C$*. Sont équivalentes :*

(i) P *est lisse ;*

(ii) l'anneau $\mathscr{O}_{C,P}$ *est principal ;*

(iii) l'anneau $\mathscr{O}_{C,P}$ *est intégralement clos.*

Démonstration :

(i) $\Rightarrow$ (ii) : on sait déjà que $\mathfrak{m} := \mathfrak{m}_{C,P}$ est principal. Soit t un générateur. Soit $a \in \bigcap_{n>0} \mathfrak{m}^n = \bigcap_{n>0}(t^n) = 0$. La suite d'idéaux $[t^n : a] := \{x \in A : t^n x \in (a)\}$ est croissante donc stationnaire :

$$\exists\, N > 0, \forall\, n \geq N,\ [t^n : a] = [t^{n+1} : a] =: I\ .$$

Mais alors : $It^{n+1} = [t^{n+1} : a]t^{n+1} = (a) = [t^n : a]t^{n+1} = (a)t = [t^n : a]t^n t$. Donc $(a) = (a)t \Rightarrow a = 0$.

Donc si $f, g \in \mathscr{O}_{C,p}$ sont non nuls, il existe m, n tels que $f \in (t^n) \setminus (t^{n+1})$ et $g \in (t^m) \setminus (t^{m+1})$. On a : $f = t^n u$, $g = t^m v$ avec u, v inversibles et donc $fg = 0 \Rightarrow t^{m+n}uv = 0 \Rightarrow t^{m+n} = 0 \Rightarrow t = 0 \Rightarrow f$ ou $g = 0$ absurde !

Soit I un idéal non nul de $\mathscr{O}_{C,p}$. Il existe n tel que $I \leq (t^n)$ et $I \not\leq (t^{n+1})$. Soit $x \in I \setminus (t^{n+1})$. On a $x = t^n u$ pour un u inversible. Donc $t^n \in I$ et $I = (t^n)$. (iii) $\Rightarrow$ (i) : il suffit de montrer que $\mathfrak{m}_P$ est principal. Soit $0 \neq f \in \mathfrak{m}$. Soit n tel que $\mathfrak{m}^n \leq (f)$ et $\mathfrak{m}^{n-1} \not\leq (f)$. Soit $g \in \mathfrak{m}^{n-1} \setminus (f)$. Alors $g/f \in k(C)$ et $g/f\mathfrak{m} \leq \mathscr{O}_{C,P}$. Si $g/f\mathfrak{m} \leq \mathfrak{m}$, alors l'« astuce du déterminant »permet de trouver un polynôme unitaire à coefficients dans $\mathscr{O}_{C,P}$ qui annule g/f $\Rightarrow g/f \in \mathscr{O}_{C,P}$ absurde ! Donc $g/f\mathfrak{m} = \mathscr{O}_{C,P} \Rightarrow \mathfrak{m} = (g/f)$. **Q.e.d.**

Remarque : si C est une courbe plane quelconque, si P est un point lisse de C, alors il existe une unique composante irréductible C_1 de C qui passe par P. On a alors $\mathscr{O}_{C,P} \simeq \mathscr{O}_{C_1,P}$.

Corollaire 1.5.8.1 *Soit C une courbe affine plane irréductible. La courbe C est lisse si et seulement si $k[C]$ est intégralement clos.*

COURS DU MERCREDI 26 FÉVRIER

Lemme 1.5.9 (Artin-Rees) *Soit A un anneau nœthérien. Soient I, I' deux idéaux de A. Il existe n_0 tel que :*

$$\forall\, n \geq n_0,\ I^n \cap I' = I^{n-n_0}(I^{n_0} \cap I') \ .$$

Démonstration : Soient $a_1, ..., a_r$ des générateurs de l'idéal I. Soit J l'idéal engendré par les polynômes homogènes F de $A[T_1, ..., T_r]$ tels que $F(a) \in I'$. Soient $F_1, ..., F_m \in A[T_1, ..., T_r]$ des polynômes homogènes qui engendrent J. Soient $d_i := \deg F_i$ et $n_0 ge \max\{d_i\}$. Si$n \geq n_0$ etsi $x \in I \cap I'$, alors il existe $F \in A[T_1, ..., T_r]$ homogène de degré n tel que $F(a) \in I'$. On a $F = P_1 + ... + P_N F_N$ pour certains P_i que l'on peut supposer homogènes de degrés respectifs $n - d_i$. Alors :

$$x = P_1(a)F_1(a) + ... + P_N F_N(a)$$

et pour chaque i, $P_i(a)F_i(a) \in I^{n-d_i}(I^{d_i} \cap I') = I^{n-n_0}(I^{n_0-d_i}(I^{d_i} \cap I')) \leq I^{n-n_0}(I^{n_0} \cap I')$. **Q.e.d.**

Théorème 1.5.10 (d'intersection de Krull) *Soit A un anneau nœthérien local d'idéal maximal $\mathfrak{m}$. On a :*

$$\bigcap_{n>0} \mathfrak{m} = 0 \ .$$

Démonstration : Soit $I' := \bigcap_{n>0} \mathfrak{m} = 0$. Il existe n_0 tel que :

$$\mathfrak{m}^{n_0+1} \cap I' = \mathfrak{m}(\mathfrak{m}^{n_0} \cap I')$$

$$\Leftrightarrow I' = \mathfrak{m} I' \ .$$

Il existe donc $x \in 1+\mathfrak{m}$ tel que $xI' = 0$ mais $x \in A^\times$ donc $I' = 0$. **Q.e.d.**

1.5.3.1 Cas général

Soit X un fermé algébrique. On note $T_xX := (\mathfrak{m}_x/\mathfrak{m}_x^2)^*$ où $\mathfrak{m}_x$ est l'idéal maximal de l'anneau local $\mathscr{O}_{X,x}$.

Proposition 1.5.11 *La restriction à* $\mathfrak{m}_x$ *induit un isomorphisme de* $k-$*espaces vectoriels :*

$$\mathrm{Der}_{k_x}(\mathscr{O}_{X,x}, k_x) \to T_xX$$

où $\mathrm{Der}_{k_x}(\mathscr{O}_{X,x}, k_x)$ *est l'espace des formes linéaires* $\delta : \mathscr{O}_{X,x} \to k$ *telles que* $\forall\, f, g,\ \delta(fg) = f(x)\delta(g) + g(x)\delta(f)$.

Soient X un fermé de $\mathbb{A}$ et $I(X) =: (f_1, ..., f_r)$. On pose $J := \left(\frac{\partial f_i}{\partial X_j}\right)_{\substack{1\le i\le r\\ 1\le j\le r}}$. Alors on a un isomorphisme :

$$\begin{aligned} \ker J &\longrightarrow \mathrm{Der}_{k_x}(\mathscr{O}_{X,x}, k_x) \quad . \\ v &\longmapsto (h \mapsto \textstyle\sum_j v_j \partial_{X_j} h) \\ (\delta(X_j))_{1\le j\le n} &\longleftarrow\!\shortmid\ \delta \end{aligned}$$

D'où :

Proposition 1.5.12 $\dim T_xX = n - \mathrm{rg}(J(x))$.

Définition 13 *On dit qu'une courbe algébrique affine* C *est lisse en un point* $x \in C$ *si* $\dim T_xC = 1$ i.e. *si* C *est un fermé de* $\mathbb{A}^n$, C *est lisse en* x *si* $\mathrm{rang}(J(x) = n-1$.

Exercice : quels sont les points singuliers de la courbe $C = \{(t^3, t^4, t^5) : t \in \mathbb{A}^1\}$?

Proposition 1.5.13 *Une courbe* C *est lisse en* $x \in C \Leftrightarrow \mathscr{O}_{C,x}$ *intégralement clos* $\Leftrightarrow \mathscr{O}_{C,x}$ *principal.*

1.5.4 Désingularisation

On dira qu'une courbe C est lisse si $k[C]$ est intégralement clos.

Proposition 1.5.14 *Soit C une courbe affine irréductible. Il existe une courbe lisse C' et un morphisme fini $\pi : C' \to C$ qui induit un isomorphisme : $\pi^{-1}C_{\text{rég}} \to C$.*

Démonstration : Soit C' tel que $k[C'] \simeq \widetilde{k[C]}$ la fermeture intégrale de $k[C]$ dans $k(C)$. **Q.e.d.**
Exemple de désingularisation : $\mathbb{A}^1 \to V(y^2 - x^3)$, $t \mapsto (t^2, t^3)$.

Exercice : trouver une désingularisation de $y^2 = x^3 - x^4$.

On dit que deux fermés algébriques X, X' sont *birationnels* s'il existe un ouvert $U \subseteq X$, un ouvert $U' \subseteq X'$ (non vides) et un isomorphisme $\phi : U \simeq U'$.

Exercice. X, X' sont birationnels si et seulement si $k(X) \simeq k(X')$.

Proposition 1.5.15 *Toute courbe algébrique plane irréductible est birationnelle à une courbe algébrique plane dont les éventuelles singularités sont des points ordianires.*

Proposition 1.5.16 *Toute courbe algébrique irréductible est birationnelle à une (et une seule à isomorphisme près) courbe projective lisse.*

1.6 Anneaux de valuation discrète

1.6.1 Valuations

Une *valuation discrète* sur un corps K est une application $v : K \to \mathbb{Z} \cup \{\infty\}$ telle que :

(i) $\forall\, x \in K,\ v(x) = \infty \Leftrightarrow x = 0$;

(ii) $v|_{K^\times} : K^\times \to \mathbb{Z}$ est un morphisme de groupes surjectif ;

(iii) $\forall\, x, y \in K,\ v(x + y) \geq \min\{v(x), v(y)\}$.

Exemples : $\mathbb{Q}, v_p$ avec p premier ; $k(T)$ et l'ordre d'annulation en t_0, $k((t))$ et la valuation usuelle des séries, $k(t)$ et $v_\infty(f/g) := \deg g - \deg f$.

Remarque : l'ensemble $\mathscr{O}_v := v^{-1}(\mathbb{N} \cup \{\infty\})$ est un sous-anneau intègre de K et K est son corps des fractions. C'est l'anneau de valuation de (K, v).

Un *anneau de valuation discrète* est un anneau intègre A tel qu'il existe une valuation v sur le corps K des fractions de Atel que $A = \mathscr{O}_v$.

Proposition 1.6.1 (Propriétés) *Soit v une valuation discrète sur un corps K. L'anneau $\mathscr{O}_v$ vérifie :*

(i) $\mathcal{O}_v^\times = v^{-1}(1)$;

(ii) $\mathscr{O}_v$ *est local d'idéal maximal* $\mathfrak{m} := v^{-1}(\{1, ..., \infty\})$;

(iii) $\mathfrak{m}$ *est principal et* $\mathfrak{m} = t \Leftrightarrow v(t) = 1$;

(iv) $\forall\, n \geq 1$, $\mathfrak{m}^n = v^{-1}(\{n, ..., \infty\})$;

(v) *l'anneau* $\mathscr{O}_v$ *est principal et ses idéaux sont les* $\mathfrak{m}^n$, $n \geq 0$.

On dit que $k := A/\mathfrak{m}$ *est le corps résiduel de* $\mathscr{O}_v$. *Un générateur de* $\mathfrak{m}$ *est une uniformisante de* $\mathscr{O}_v$.

Remarque : $t \in \mathscr{O}_v$ *est une uniformisante si et seulement si* $t \in \mathfrak{m} \setminus \mathfrak{m}^2$.

Exercices :

1) *si* v *est une valuation sur un corps* K *et si* $x, y \in K$, *alors* $v(x) \neq v(y) \Rightarrow v(x+y) = \min\{v(x), v(y)\}$.
2) $\mathscr{O}_v$ *est un sous-anneau maximal de* K.
3) *Un anneau principal, local qui n'est pas un corps est un anneau de valuation discrète.*

1.6.2 Ordre d'annulation

Soit C une courbe. Soit $P \in C$ un point lisse *au sens où* $\mathscr{O}_{C,p}$ *est principal.* Si $f \in \mathscr{O}_{C,P}$, on note :

$$\mathrm{ord}_P(f) := \sup\{n \geq 0 \ :\ f \in \mathfrak{m}^n\}$$

où $\mathfrak{m} = \mathfrak{m}_{C,P}$; c'est l'ordre d'annulation en P.

Remarque : si $f \in \mathfrak{m}^n \setminus \mathfrak{m}^{n+1}$, alors $\mathrm{ord}_P(f) = n$.

Théorème 1.6.2 *Si* P *est un point lisse, alors on peut prolonger* ord_P *à* $k(C)$ *en posant :* $\mathrm{ord}_P(f/g) := \mathrm{ord}_P f - \mathrm{ord}_P g$. *On obtient ainsi une valuation discrète sur* $k(C)$ *dont l'anneau des valuations est* $\mathscr{O}_{C,P}$.

Exemples :

a) si $C = \mathbb{A}^1$, si $x_0 \in k$ et si $f \in k(C) = k(t)$, alors $\mathrm{ord}_{x_0} f$ est la multiplicité de x_0 comme zéro de f (ou $-$l'ordre de x_0 comme pôle de f). L'élément $(t - x_0)$ est une uniformisante.
b) Si $C = (y^2 = x^3 - x)$, si $P = (0,0)$, alors $\mathrm{ord}_P x = 2$ et $\mathrm{ord}_P y = 1$: donc y est une uniformisante.
c) Si $C = (y^2 + y = x^3 + x)$, si $P = (0,0)$, alors $\mathrm{ord}_P x = 1$ et $\mathrm{ord}_P y = 1$: donc x, y sont des une uniformisantes.

Exercice : Montrer que pour une courbe plane C et pour un point lisse $P = (x_0, y_0) \in C$, si f est un générateur de $I(C)$, si $\partial_X f(P) \neq 0$, alors $y - y_0$ est une uniformisante *(indication : dans* $\mathscr{O}_{C,P}$, *on a* $\mathfrak{m}_{C,P} = (x - x_0, y - y_0)$ *et* $\partial_X f(P)(x - x_0) + \partial_Y f(P)(y - y_0) = 0 \bmod \mathfrak{m}_{C,P}^2$ *donc* $\mathfrak{m}_{C,P}/\mathfrak{m}_{C,P}^2$ *est engendré par* $y - y_0$ *...).*

COURS DU MERCREDI 12 MARS 2014

1.6.3 Développements limités

Soit C une courbe et P un point lisse de C. Soit t une uniformisante pour $\mathscr{O}_{C,P}$.

Notation : si $f, g \in k(C)$, si $n \geq 0$, on écrit $f = g + O(t^n)$ si $f - g \in \mathfrak{m}^n$.

Théorème 1.6.3 *Soit $0 \neq f \in k(C)$. Si $n_0 := \mathrm{ord}_P f$, alors il existe une unique série de Laurent $\sum_{n \geq n_0} a_n t^n \in k((t))$ telle que :*

$$f = \sum_{n=n_0}^{r} a_n t^n + O(t^{r+1})$$

pour tout $r \geq 0$. En associant 0 à 0, on obtient un morphisme de corps $k(C) \to k((t))$.

La série $\sum_{n \geq n_0} a_n t^n$ est le développement limité de f en P relativement à t.

Exercice : Soit $C = (y^2 = x^3 - 1)$. En $P = (1, 0)$ et pour l'uniformisante $t = y$, le développement limité de x ne contient que des puissances paires de y.

Chapitre 2

Courbes projectives

2.1 Un peu de géométrie projective

2.1.1 L'espace projectif

Soit V un $k-$espace vectoriel. On pose $\mathbb{P}(V) := V \setminus \{0\}/\sim$ où $x \sim y$ si $y = \lambda x$ pour un certain $\lambda \in k^\times$.

Si $V = k^{n+1}$, on note $\mathbb{P}^n(k) := \mathbb{P}(k^{n+1})$.

Notation : $\pi : V \setminus \{0\} \to \mathbb{P}(V)$, $v \mapsto [v]$ est la surjection canonique.

Remarque : on peut identifier $\mathbb{P}(V)$ à l'ensemble des droites vectorielles de V. Si $W \leq V$, on dit que $\pi(W \setminus \{0\})$ est un sous-espace projectif de dimension $\dim W - 1$.

Exercice : Si P_1, P_2 sont des sous-espaces projectifs de $\mathbb{P}^n$ de dimension n_1, n_2 avec $n_1 + n_2 \geq n$, alors $P_1 \cap P_2 \neq \emptyset$. En particulier, deux droites projectives se rencontrent toujours.

2.1.2 Cartes affines

Soit $n \geq 1$. Pour tout i, soit $U_i := \{[x_0 : ... : x_n] \in \mathbb{P}^n \ : \ x_i \neq 0\}$.

L'application $j_0 : \mathbb{A}^n \to U_0 \subseteq \mathbb{P}^n$, $(x_1, ..., x_n) \mapsto [1 : x_1 ... : x_n]$ est bijective.

Complétion projective : soit $D \subseteq \mathbb{A}^n$ une droite affine. Il existe une unique droite projective $\overline{D}$ dans $\mathbb{P}^n$ telle que $j_0^{-1}\overline{D} = D$.

Par exemple si $n = 2$, si D est la droite d'équation :

$$(x, y) \in \mathbb{A}^2 \ : \ ax + by + c = 0$$

$\overline{D}$ est la droite projective d'équation :

$$[x : y : z] \in \mathbb{P}^2 \ : \ ax + by + cz = 0 \ .$$

On a dans ce cas : $\overline{D} = j_0(D) \cup \{\infty_D\}$ où $\infty_D := [-b : a : 0]$.

On dit qu'on a ajouté à D un point *à l'infini* : ∞_D.

Exercice : deux droites affines $d_1, d_2 \subseteq \mathbb{A}^2$ sont parallèles si et seulement si $\infty_{d_1} = \infty_{d_2}$.

Rappel : si k est un corps, $\mathbb{P}^n(k) := k^{n+1} \setminus \{0\}/\sim$ où $x \sim y$ si $\exists\, \lambda \in k^\times$, $x = \lambda y$.

Notation : $\pi : k^{n+1} \setminus \{0\} \to \mathbb{P}^n(k)$, $x \mapsto [x] := x \bmod \sim$.

Une *carte affine de* $\mathbb{P}^n$ est la donnée de H un hyperplan de k^{n+1} et d'une application bijective de la forme :

$$k^n \to \mathbb{P}^n \setminus \pi(H \setminus \{0\})$$
$$v \mapsto [e_0 + \phi(v)]$$

où $e_0 \notin H$ et $\phi : k^n \simeq H$ est un isomorphisme linéaire. Pour une carte affine fixée, on appelle points à l'infini les points de $\pi(H \setminus \{0\})$.

Exemples : soit $C := \{[x : y : z] \in \mathbb{P}^2(\mathbb{R}) \,:\, x^2 + y^2 = z^2\}$. Pour la carte affine $i_1 : \mathbb{R}^2 \to \mathbb{P}^2(\mathbb{R})$, $(x, y) \mapsto [x : y : 1]$, vérifier que $i_1^{-1}C$ est un cercle et que C n'a pas de point à l'infini. Pour la carte affine $i_2 : \mathbb{R}^2 \to \mathbb{P}^2(\mathbb{R})$, $(x, y) \mapsto [1 : x : y]$, vérifier que $i_2^{-1}C$ est une hyperbole avec deux points à l'infini.

Exercice : trouver une carte affine $i : \mathbb{R}^2 \to \mathbb{P}^2(\mathbb{R})$ telle que $i^{-1}C$ est une parabole. Pour l'exemple trouvé, déterminer l'unique point à l'infini.

2.2 Fermés de l'espace projectif

Soient $P_i \in k[X_0, ..., X_n]$ des polynômes homogènes. L'ensemble :

$$V(P_i \,:\, i) := \{[x] \in \mathbb{P}^n \,:\, \forall\, i,\, P_i(x) = 0\}$$

est bien défini. De plus $V(P_i \,:\, i) = V(I)$ où I est l'idéal de $k[X_0, ..., X_n]$ engendré par les P_i.

Dorénavant, on suppose k algébriquement clos.

2.2.1 Idéaux homogènes

Proposition 2.2.1 *Soit I un idéal de $k[X_0, ..., X_n]$. Sont équivalentes :*

(i) *pour tout $P \in I$, tout $t \in k^\times$, $P(tX_0, ..., tX_n) \in I$;*

(ii) *pour tout $P \in I$, les composantes homogènes de P sont dans I ;*

(iii) *l'idéal I est engendré par des polynômes homogènes ;*

(iv) *l'idéal I est engendré par un nombre fini de polynômes homogènes ;*

(v) *on a : $I = \oplus_d I \cap k[X_0, ..., X_n]_d$.*

Un tel idéal est dit *homogène*.

Remarque : tout idéal homogène strict est contenu dans $(X_0, ..., X_n)$.

Un *fermé* de $\mathbb{P}^n$ est un ensemble de la forme :

$$V(I) := \{[x] \in \mathbb{P}^n \,:\, \forall\, P \in I,\, P(x) = 0\}\ .$$

Proposition 2.2.2 *Les $V(I)$ sont les fermés d'une topologie sur $\mathbb{P}^n$.*

Soit $\pi : \mathbb{A}^{n+1} \setminus \{0\} \to \mathbb{P}^n$ la surjection canonique.

Proposition 2.2.3 *Un $F \subseteq \mathbb{P}^n$ est fermé si et seulement si $\pi^{-1}F \cup \{0\}$ est fermé dans $\mathbb{A}^{n+1}$.*

Exercice : on note U_i les ouverts $(x_i \neq 0)$ et $j_i : \mathbb{A}^n \to U_i$, $(x_0, ..., \hat{x_i}, ...x_n) \mapsto [x_0 : ... : 1 : ... : x_n]$. Vérifier que les U_i recouvrent $\mathbb{P}^n$ et que $F \subseteq \mathbb{P}^n$ est fermé si et seulement si pour tout i, $j_i^{-1}F$ est fermé dans $\mathbb{A}^n$.

Si A est un fermé de $\mathbb{A}^{n+1}$, on note $\widetilde{I}(A)$ l'idéal correspondant dans $k[X_0, ..., X_n]$. Si I est un idéal homogène de $k[X_0, ..., X_n]$, on note $\widetilde{V}(I)$ le fermé correspondant dans $\mathbb{A}^{n+1}$.

Exercice : $V(I) = \pi(\widetilde{V}(I) \setminus \{0\})$.

Notation : si A est un fermé de $\mathbb{P}^n$, alors $I(A) := \widetilde{I}(\pi^{-1}A \cup \{0\})$.

Proposition 2.2.4 *L'idéal $I(A)$ est un idéal homogène strict de $k[X_0, ..., X_n]$.*

Exercice : soit $p := [p_0 : ... : p_n] \in \mathbb{P}^n$. Alors $I(\{p\}) = (p_iX_j - p_jX_i : 0 \leq i, j \leq n) = (X_j - p_j/p_0X_0 : j > 0)$ si $p_0 \neq 0$.

Proposition 2.2.5 *Si F est un fermé de $\mathbb{P}^n$, alors $V(I(F)) = F$.*

2.2.2 Théorème des zéros

Théorème 2.2.6 (version projective du théorème des zéros) *Si I est un idéal homogène strict de $k[X_0, ..., X_n]$, alors $I(V(I)) = \sqrt{I}$.*

Corollaire 2.2.6.1 *Soit I un idéal homogène de $k[X_0, ..., X_n]$. Alors :*

$$V(I) = \emptyset \Leftrightarrow \sqrt{I} \supseteq (X_0, ..., X_n)$$
$$\Leftrightarrow \forall\, i,\ ^{\exists}\, d \geq 1,\ X_i^d \in I$$
$$\Leftrightarrow\ ^{\exists}\, N \geq 1,\ I \text{ contient tous les monômes de degré } N$$
$$\Leftrightarrow\ ^{\exists}\, N \geq 1,\ \oplus_{d \geq N} k[X_0, ..., X_n]_d \subseteq I\ .$$

2.3 Propriétés topologiques

Tout fermé de $\mathbb{P}^n$ est un espace topologique nœthérien, on a donc comme dans le cas affine une décomposition en fermés irréductibles et une notion de composantes irréductibles.

Exercice : si F est un fermé de $\mathbb{P}^n$, alors F est irréductible $\Leftrightarrow I(F)$ est premier.

Exercice : soit F un fermé non vide de $\mathbb{P}^n$. Alors F est irréductible $\Leftrightarrow I(F)$ est premier $\Leftrightarrow \pi^{-1}F \cup \{0\}$ est un fermé irréductible de $\mathbb{A}^{n+1}$.

Exercice : l'application $\mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^{mn+m+n}$, $([x], [y]) \mapsto [x_iy_j]_{\substack{0 \leq i \leq m \\ 0 \leq j \leq n}}$, est une bijection sur son image, le fermé $V((X_{i,j}X_{k,l} - X_{il}X_{k,j})_{\substack{0 \leq i,k \leq m \\ 0 \leq j,l \leq n}})$.

2.4 Le théorème fondamental de l'élimination projective

On dira que $F \subseteq \mathbb{P}^m \times \mathbb{A}^n$ est un fermé si F est défini par des polynômes $P_i(x, y)$ homogènes en les x_i.
Remarque : $F \subseteq \mathbb{P}^m \times \mathbb{A}^n$ est fermé $\Leftrightarrow (\pi \times \mathrm{Id})^{-1} F \cup \{0\} \times \mathbb{A}^n \subseteq \mathbb{A}^{m+1} \times \mathbb{A}^n$ est fermé $\Leftrightarrow \forall\, i,\ j_i \times \mathrm{Id}^{-1} F$ est fermé dans $\mathbb{A}^m \times \mathbb{A}^n$.

Théorème 2.4.1 *Si $F \subseteq \mathbb{P}^m \times \mathbb{A}^n$ est fermé, alors $pr_2(F)$ est un fermé de $\mathbb{A}^n$.*

Contre-exemple : $pr_2(V(xy - 1))$ n'est pas un fermé de $\mathbb{A}^1$.

2.5 Produits d'espaces projectifs

On dira qu'une partie $F \subseteq \mathbb{P}^{m_1} \times ... \times \mathbb{P}^{m_r}$ est fermée si elle définie par des équations polynômiales $F_i(x^{(1)}, ..., x^{(r)})$ homogènes en les $x^{(i)}$.

Exercice : il existe bien une topologie sur $\mathbb{P}^{m_1} \times ... \times \mathbb{P}^{m_r}$ dont les parties de la forme ci-dessus sont les fermés. *Attention, ce n'est pas la topologie produit !*

2.6 Morphismes

Soient $X \subseteq \mathbb{P}^m$, $Y \subseteq \mathbb{P}^n$ des fermés projectifs. Soient $U \subseteq X$, $V \subseteq Y$ des ouverts.

Définition 14 *Une application $f : U \to V$ est régulière en $x \in U$ s'il existe un voisinage ouvert U_x de x et des fonctions polynomiales homogènes $f_0, ..., f_n \in k[T_0 : ... : T_m]$ de même degré tels que : $\forall\, t \in U_x$, $^\exists\, i$, $f_i(t) \neq 0$ et $f(t) = [f_0(t) : ... : f_n(t)]$. Si f est régulière sur U, on dit que f est un morphisme*

Exemple : l'application $\mathbb{P}^1 \to V(Y^2 - XZ) \subseteq \mathbb{P}^2$, $[u : v] \mapsto [u^2 : uv : v^2]$ est un isomorphisme mais la réciproque n'est pas définie par une seule formule.

Exercice : la composée de deux morphismes est un morphisme.

Corollaire 2.6.0.1 (du théorème d'élimination) *Soit $f : \mathbb{P}^m \to \mathbb{P}^n$ une application régulière, alors $f(F)$ est fermé dans $\mathbb{P}^n$, pour tout fermé F de $\mathbb{P}^m$.*

Notation : si U est un ouvert de X un fermé de $\mathbb{P}^n$, on note $\mathscr{O}_X(U)$ la $k-$algèbre des fonctions régulières $f : U \to \mathbb{A}^1$.

Exercice : $\mathscr{O}_X(X) = k$.

Exercice : Une application $f : U \to V$ est régulière si et seulement si f est continue et si pour tout ouvert W de V, pour tout $g \in \mathscr{O}_Y(W)$, $g \circ f \in \mathscr{O}_X(f^{-1}W))$.

Exercice : généraliser la notion de morphismes aux applications $f : U \to V$ où U et V sont des ouverts de fermés de produits d'espaces projectifs et vérifier que :

$$\mathbb{P}^m \times \mathbb{P}^n \to \mathbb{P}^{mn+m+n}$$

$$([x_i]_i, [y_j]_j) \mapsto [x_i y_j]_{i,j}$$

est un isomorphisme sur son image qui est fermée.

Exercice : l'application $\pi : \mathbb{A}^{n+1} \setminus \{0\} \to ¶^n$ est un morphisme.

2.7 Définition des courbes projectives planes

Une *hypersurface projective* est un fermé de $\mathbb{P}^n$ défini par une équation $H = V(P)$ où P est un polynôme homogène de degré ≥ 1. Si $\deg P = 1$, c'est un *hyperplan*, si $\deg P = 2$, c'est une *quadrique* (ou *conique* si $n = 2$), si $\deg P = 3$, c'est une *cubique*, *etc*

Le *degré de l'hypersurface* H est le degré de P un générateur de $I(H)$.

Une *courbe projective plane* est une hypersurface de $\mathbb{P}^2$ de la forme $V(P)$ où $P \in k[X_0, X_1, X_2]$ est un polynôme homogène de degré ≥ 1.

Exercice : si P est irréductible, la courbe est irréductible.

Exercice : les fermés propres d'une courbe irréductible sont finis.

Lemme 2.7.1 *Soit $F \in k[X, Y, Z]$ un polynôme homogène non nul. Si $F = F_1F_2$, alors F_1, F_2 sont aussi homogènes.*

Lemme 2.7.2 *Si C est une courbe projective plane, alors $I(C)$ est un idéal principal engendré par un polynôme homogène.*

Proposition 2.7.3 *Une courbe C est irréductible $\Leftrightarrow$ $I(C)$ est premier.*

Proposition 2.7.4 *Un fermé propre non vide de $\mathbb{P}^2$ est une réunion finie de courbes irréductibles et de points.*

Exercice : plus généralement, on a l'équivalence : un fermé $F \subseteq \mathbb{P}^n$ est irréductible $\Leftrightarrow I(F)$ est premier $\Leftrightarrow \pi^{-1}F \cup \{0\}$ est irréductible dans $\mathbb{A}^{n+1}$.

Une *courbe projective irréductible* est un fermé C de $\mathbb{P}^n$, pour un certain n tel que $A(C) := k[X_0, ..., X_n]/I(C)$ est intègre de degré de transcendance 2.

Attention ! les éléments de $A(C)$ sont seulement des fonctions sur $\pi^{-1}C \subseteq \mathbb{A}^{n+1} \setminus \{0\}$.

Problème ouvert : une courbe de $\mathbb{P}^3$ peut-elle être définie par deux polynômes homogènes ?

Exercice : les idéaux homogènes irréductibles et propres de $k[X, Y, Z]$ sont :

$$0,\ (F),\ \text{où } F \text{ est homogène irréductible},\ I(\{[x_0 : y_0 : z_0]\}) \text{ pour un } [x_0 : y_0 : z_0] \in \mathbb{P}^2.$$

indication : si F, G sont homogènes premiers entre eux dans $k[X, Y, Z]$, alors ils le sont aussi dans $k(X, Y)[Z]$ et on peut trouver $A, B \in k[X, Y, Z]$ homogènes tels que $0 \neq AF + BG \in k[X, Y]$.

En déduire les fermés irréductibles de $\mathbb{P}^2$.

2.7.1 Dimension

Si $F \subseteq \mathbb{P}^n$ est un fermé non vide , on pose $\dim F := \dim \pi^{-1}F \cup \{0\} - 1 = \partial_k k[X_0, ..., X_m]/I(F) - 1$.

Proposition 2.7.5 *Soit F un fermé irréductible de $\mathbb{P}^n$. Si $F_1 \subseteq F$ est un fermé strict, alors $\dim F_1 < \dim F$.*

2.8 Lien courbes affine / projectives

On identifie $\mathbb{A}^m$ et l'ouvert $U_0 := \{[1 : x_1 : ... : x_m] \in \mathbb{P}^m\}$. Si $P_1, ..., P_n \in k[X_0, ..., X_m]$ sont des polynômes homogènes, alors $V(P_1, ..., P_n) \cap \mathbb{A}^m = V(\widetilde{P_i})$ où $\widetilde{P_i} = P_i(1, X_1, ..., X_m)$.

Si $P \in k[X_0, ..., X_m]$ est homogène de degré d, $\widetilde{P}$ est de degré $\leq d$ avec égalité si et seulement si X_0 ne divise pas P. On dit que $\widetilde{P}$ est le *déshomogénéisé* de P.

Remarque : Si F est un fermé (irréductible) de $\mathbb{P}^m$, alors $F \cap \mathbb{A}^m$ est un fermé irréductible de $\mathbb{A}^n$.

Si $F \in k[X_1, ..., X_m]$, on note $\overline{F} := X_0^d F(X_1/X_0, ..., X_m/X_0)$, où $d = \deg F$. C'est *l'homogénéisé* de F.

On identifie $\mathbb{A}^2$ et l'ouvert $(z \neq 0) = \{[x : y : 1] \ : \ x, y \in k\}$.

Si $F \in k[X, Y]$ est de degré d, on pose $\overline{F} := Z^d F(X/Z, Y/Z)$, c'est l'*homogénéisé* de F.

Exemple : l'homogénéisé de $y^2 - x(x-1)(x-\lambda)$ est $y^2 z - x(x-z)(x-\lambda z)$.

Proposition 2.8.1 *a) si F est de degré d, alors $\overline{F}$ est homogène de degré d ;*

b) $\overline{FG} = \overline{F}\,\overline{G}$;

c) si H est homogène premier à X_0, alors $H = \overline{\widetilde{H}}$.

Soit $Z \subseteq \mathbb{A}^m$ un fermé algébrique. Soit $I := I(Z)$. On pose $\overline{I} := (\overline{F} \ : \ F \in I)$ et $Z^* := V_{\mathbb{P}^m}(\overline{I})$.

Exemple : si $I = (Y - X^2, Z - X^3)$, alors $(\overline{Y - X^2}, \overline{Z - X^3}) \subsetneq \overline{I}$ car $ZW - XY \in \overline{I} \setminus (\overline{Y - X^2}, \overline{Z - X^3})$.

Proposition 2.8.2 *Z^* est l'adhérence de Z dans $\mathbb{P}^m$. De plus, si $Z = Z_1 \cup ... \cup Z_l$ est la décomposition de Z en composantes irréductibles, alors $Z^* = Z_1^* \cup ... \cup Z_l^*$ est la décomposition de Z^* en composantes irréductibles.*

Proposition 2.8.3 *Si $C = V(F)$ est une courbe affine plane, alors $V(\overline{F}) = \overline{C}$.*

On dit que $\overline{Z}$ est la complétion projective de Z.

Remarque : $\overline{C}$ ne dépend que de C (non de F).

On dit que les points de $\overline{Z} \setminus Z$ sont les points à l'infini. Ce sont les points de $\overline{Z} \cap H_\infty$ où $H_\infty = (x_0 = 0)$.

Lemme 2.8.4 *Si C est une courbe projective affine plane de degré d, alors C a au plus d points à l'infini et au moins* 1.

Exercice : quels sont les points à l'infini de $x^2 + y^2 = 1$.

Théorème 2.8.5 *L'application $C \mapsto \overline{C}$ est une bijection entre les courbes algébriques de $\mathbb{A}^2$ et les courbes projectives planes ne contenant pas la droite à l'infini $z = 0$. Cette bijection préserve l'irréductibilité. La réciproque est donnée par $\mathbf{C} \mapsto \mathbf{C} \cap \mathbb{A}^2$.*

Exercice : $Z \mapsto \overline{Z}$ est une bijection entre les fermés algébriques de $\mathbb{A}^m$ et les fermés de $\mathbb{P}^m$ qui n'ont aucune composante irréductible contenue dans H_∞. De plus cette bijection préserve l'irréductibilité et la dimension.

Corollaire 2.8.5.1 *Les fermés de $\mathbb{P}^2$ sont $\mathbb{P}^2$, les unions finies de courbes irréductibles et de points et $\emptyset$.*

2.8.1 Courbes projectivement équivalentes

On dit que deux courbes projectives $C_1, C_2 \subseteq \mathbb{P}^2$ sont projectivement équivalentes s'il existe $g \in \mathrm{GL}_3(k)$ tel que $gC_1 = C_2$.

Remarque : l'action de GL_{n+1} sur $\mathbb{P}^n$ préserve les fermés.

Exercice : trouver deux courbes affines planes non isomorphes dont les complétions projectives sont projectivement équivalentes. $(x^2 + y^2 = 1) \not\simeq (y = x^2)$.

Exercice : trouver deux courbes affines planes isomorphes dont les complétions projectives ne sont pas isomorphes. $(y = x^2) \simeq (y = x^3)$.

Exercice : si $C = V(F)$, alors $I(\overline{C}) = I(\overline{F})$.

Cours du mercredi 2 avril 2014

2.9 Points lisses et fonctions rationnelles

Soit $C \subseteq \mathbb{P}^2$ une courbe algébrique plane. Soit H un générateur de $I(C) \leq k[X, Y, Z]$.

On dit que $P \in C$ est *lisse* si $(\partial_X H, \partial_Y H, \partial_Z H)(P) \neq (0, 0, 0)$. On dit que P est *singulier* sinon.

Remarque : cette définition ne dépend pas du générateur choisi ni des coordonnées homogènes choisies pour P.

Proposition 2.9.1 *Si C est une courbe projective plane de degré d et si la caractéristique de k ne divise pas d, alors $C^{\mathrm{sing}} = V(\partial_X H, \partial_Y H, \partial_Z H)$.*

Démonstration : On utilise l'identité d'Euler :

$$X\partial_X H + Y\partial_Y H + Z\partial_Z H = dH$$

pour tout $H \in k[X, Y, Z]_d$. **Q.e.d.**

Si $P \in C$, une courbe projective plane, est lisse, la *tangente* à C en P est la droite (projective) d'équation :

$$\partial_X H(P)X + \partial_Y H(P)Y + \partial_Z H(P)Z = 0$$

où $(H) = I(C) \leq k[X,Y,Z]$.

Proposition 2.9.2 *Soient $C \subseteq \mathbb{A}^2$ une courbe et $\overline{C} \subseteq \mathbb{P}^2$ sa complétion projective. Si $P \in C$, alors P est un point lisse de C si et seulement si P est un point lisse de $\overline{C}$.*

Exemple : La courbe d'équation $y^2 = f(x)$, où $f \in k[X]$ est unitaire de degré $d \geq 3$ et *n'est pas un carré*, a pour complétion projective $\overline{C}$. L'unique point à l'infini de $\overline{C}$ est lisse si $d = 3$ et singulier si $d > 3$.

Exercice : $T_P\overline{C}$ est la complétion projective de T_PC.

Germes de fonctions au voisinage d'un point

Soit C une courbe projective ou un ouvert d'une courbe. Soit $P \in C$. Soient U, V des voisinages ouverts de P dans C. Si $f \in \mathscr{O}_C(U)$, $g \in \mathscr{O}_C(V)$, on note $f \sim g$ s'il existe un voisinage ouvert W de P dans $U \cap V$ tel que $f|_W = g|_W$.

L'anneau des germes de fonctions régulières au voisinage de P est l'anneau :

$$\mathscr{O}_{C,P} := \{(f,U) \ : \ P \in U \text{ ouvert } \subseteq C, \ f \in \mathscr{O}_C(U)\}/\sim \quad .$$

Proposition 2.9.3 *L'anneau $\mathscr{O}_{C,P}$ est local d'idéal maximal $\mathfrak{m}_{C,P}$, idéal des germes f qui s'annulent en P.*

Remarque : $\mathfrak{m}_{C,P}$ est le noyeau du morphisme surjectif $\mathscr{O}_{C,P} \to k$, $(f,U) \bmod \sim \mapsto f(P)$.

Remarque : si V est un voisinage ouvert de P, alors la restriction à V induit un isomorphisme :

$$\mathscr{O}_{C,P} \simeq \mathscr{O}_{C\cap U,P} \quad .$$

Exercice : on a

$$\mathscr{O}_{C,P} = \left(k[\widehat{C}]_{M_P}\right)_0 := \{a/b : a, b \text{ sont homogènes de même degré dans } k[\widehat{C}] \text{ et } b(P) \neq 0\} \, ,$$

les éléments homogènes de degré 0 du localisé en M_P l'idéal homogène des fonctions dans $k[\widehat{C}]$ qui s'annulent en P (en n'importe lequel de ses représentants dans $\widehat{C}$.

On en déduit grâce au cas affine :

Proposition 2.9.4 *Soit C une courbe projective plane. Si $P \in C$, alors sont équivalentes :*

i) *P est lisse ;*

ii) $\dim_k \mathfrak{m}_{C,P}/\mathfrak{m}_{C,P}^2 = 1$ *;*

iii) *$\mathcal{O}_{C,P}$ est principal ;*

iv) *$\mathcal{O}_{C,P}$ est intégralement clos ;*

v) *$\mathcal{O}_{C,P}$ est un anneau de valuation discrète.*

On peut donc définir l'ordre d'annulation en $P \in C$ si P est lisse et on dispose de la notion de développement limité en un point lisse.

Définition 15 *Une courbe projective est lisse en P si* $\dim_k \mathfrak{m}_{C,P}/\mathfrak{m}_{C,P}^2 = 1$.

2.10 Coniques

Proposition 2.10.1 *Soit $H \in k[X, Y, Z]$ homogène de degré 2 irréductible. Alors $V(H)$ est une courbe projective lisse.*

Démonstration : Soit P un point singulier. Supposons par exemple que $P = [0 : 0 : 1]$. Alors

$$H = aX^2 + bY^2 + cZ^2 + dXY + eYZ + fXZ$$

on a forcément $c = e = f$ si $H(P) = \partial_X H(P) = \partial_Y H(P) = 0$. Donc H est homogène de degré 2 en X, Y donc réductible *absurde !*. **Q.e.d.**

Théorème 2.10.2 *Toute conique projective irréductible est projectivement équivalente à la conique d'équation $yz = x^2$* i.e. *si $C \subseteq \mathbb{P}^2$ est une conique irréductible, il existe $g \in \mathrm{GL}_3(k)$ tel que $g(C) = V(YZ - X^2)$.*

C'est évident en caractéristique $\neq 2$ car toutes les formes quadratiques non dégénérées sont équivalentes. Nous allons donner une démonstration qui marche en toute caractéristique.

Lemme 2.10.3 *Le groupe* GL_3 *agit transitivement sur les triplets de points non alignés de $\mathbb{P}^2$.*

Lemme 2.10.4 *Soit C une conique projective irréductible. Pour tout $P \in C$, $T_P C \cap C = \{P\}$.*

Démonstration : On peut supposer $P = [0 : 0 : 1]$. Mais alors H est de la forme

$$H = aX^2 + bY^2 + cZ^2 + dXY + (eY + fX)Z$$

et la tangente a pour équation $eY + fX = 0$. S'il y a un point d'intersection autre que P, alors $eY + fX | aX^2 + bY^2 + cZ^2 + dXY$ dans $k[X, Y]$ donc divise H : absurde! **Q.e.d.**

Exercice : soit C une conique projective irréductible. En caractéristique 2, il existe $Q \in \mathbb{P}^2$ tel que toutes les tangentes de C passent par Q.

Exercice : En caractéristique $\neq 2$, si $P \notin C$, une conique irréductible, alors il existe 2 tangentes à C qui passent par P.

Démonstration du théorème : soit $P_1 \neq P_2 \in C$. Soit P_3 tel que $T_{P_1}C \cap T_{P_2}C = \{P_3\}$. Il existe $g \in \mathrm{GL}_3(k)$ tel que $g(P_1), g(P_2), g(P_3) = [0:0:1], [0:1:0], [1:0:0]$. On peut donc supposer que $P_1, P_2, P_3 = [0:0:1], [0:1:0], [1:0:0]$. Alors $H = aX^2 + dYZ + eXZ + fXY$. La droite $T_{P_1}C$ a pour équation : $dY + eX = 0$. La droite $T_{P_2}C$ a pour équation : $dZ + fX = 0$. Comme ces équations s'annulent en P_3, on a : $e = f = 0$. Donc $H = aX^2 + dYZ$ avec $a, d \neq 0$ car H irréductible. On a alors $g(C) = V(X^2 - YZ)$ pour un $g = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & \mu & 0 \\ 0 & 0 & \nu \end{pmatrix} \in \mathrm{GL}_3(k)$ bien choisi.

Q.e.d.

Théorème 2.10.5 *Toute conique projective irréductible est isomorphe à* $\mathbb{P}^1$.

Démonstration : Il suffit de vérifier que $V(X^2 - YZ) \simeq \mathbb{P}^1$. C'est bine le cas! **Q.e.d.**

Corollaire 2.10.5.1 *Si C est une conique, alors $\mathbb{P}^2 \setminus C$ est une variété affine.*

Démonstration : Soit $\phi : \mathbb{P}^2 \to \mathbb{P}^5$, $[x:y:z] \mapsto [x^2 : y^2 : z^2 : yz : xz : xy]$. C'est un iso sur son image et si $C = V(x^2 - yz)$, $\phi(\mathbb{P}^2 \setminus C) = \phi(\mathbb{P}^2) \cap \mathbb{P}^5 \setminus V(x_0 - x_3)$. **Q.e.d.**

2.11 Fonctions rationnelles

Soit C un fermé *irréductible* de $\mathbb{P}^n$. On note $\widehat{C} := \pi^{-1}C \cup \{0\} \subseteq \mathbb{A}^{n+1}$ le cône au-dessus de C. On a $k[\widehat{C}] = k[X_0, ..., X_m]/I(C)$.

Pour tout $d \geq 0$, on note $k[\widehat{C}]_d := k[X_0, ..., X_n]_d / I(C) \cap k[X_0, ..., X_n]_d$.

Exercice : en utilisant que l'idéal $I(C)$ est homogène, vérifier que $k[\widehat{C}] = \oplus_{d \geq 0} k[\widehat{C}]_d$.

Définition 16 *On note* $k(C) := k(\widehat{C})_0 := \{f/g \ : \ ^{\exists}\, d \geq 0,\ f, g \in k[\widehat{C}]_d\}$. *C'est un corps : le corps des fonctions rationnelles sur* C.

Exemple : $k(\mathbb{P}^1) = k(t)$ où $t = y/x$.

Remarque : pour toute fermé projectif irréductible, X, $\dim X = \mathrm{degtr}_k(k(X))$.

Proposition 2.11.1 *Si* U_i *est une carte affine* $(x_i \neq 0)$ *de* $\mathbb{P}^n$ *telle que* $U_i \cap C \neq \emptyset$, *alors l'application :*

$$k[C \cap U_i] \to k(C),\ f \mapsto f \circ \pi$$

induit un $k-$*isomorphisme de corps :* $k(C \cap U_i) = \mathrm{Frac}k[C \cap U_i] \simeq k(C)$.

Concrètement, si $U_i = (x \neq 0)$, alors $f \circ \pi(x, y, z) = f(1 : y/x : z/x)$.

Exemple : soit $C = V(Y^2Z - X^3 - Z^3)$. C'est une courbe irréductible. On a :

$$k(C) = k(x, y) = k(s, t) = k(u, v)$$

où $x = X/Z, y = Y/Z$; $s = X/Y, t = Z/Y$; $u = Y/X, v = Z/X$. On a les relations suivantes :

$$y^2 = x^3 + 1,\ t = s^3 + t^3,\ u^2v = 1 + v^3\ ;\ s = x/y, t = 1/y,\ u = y/x, v = 1/x$$

dans $k(C)$.

Définition 17 *Soient* $f \in k(C)$ *et* $P \in C$. *On dit que* f *est régulière en* P *s'il existe* $p, q \in k[\widehat{C}]$ *de même degré tels que* $q(P) \neq 0$ *et* $f = p/q$. *Dans ce cas, on pose* $f(P) := p(P)/q(P)$

Exercice : vérfier que $f(P)$ est bien défini *i.e.* si $f = p/q = p'/q'$ dans $k(C)$ comme dans la définition, alors $p(P)/q(P) = p'(P)/q'(P)$ dans k.

On obtient un morphisme injectif :

$$\mathscr{O}_{C,P} \to k(C),\ (f, U) \mapsto f$$

et $\mathrm{Frac}(\mathscr{O}_{C,P}) = k(C)$. L'image du morphisme ci-dessus est exactement la sous-algèbre des fonctions rationnelles régulières en P.

Exercice : pour tout ouvert U de C, $\mathscr{O}_C(U) := \bigcap_{P \in U} \mathscr{O}_{C,P}$ (intersection dans $k(C)$).

Exercice : $\bigcap_{P \in C} \mathscr{O}_{C,P} = k$.

Exercice : $k(C) = \mathrm{Frac}\mathscr{O}_C(U) = \mathrm{Frac}\mathscr{O}_{C,P}$ pour tout ouvert non vide de C et tout $P \in C$.

2.12 Applications (bi)rationnelles

Exemple : Soient $C = V(H)$, $C' = V(H')$ deux courbes projectives planes irréductibles. Soit un triplet $F_0, F_1, F_2 \in k[\widehat{C}]$ de même degré tel que $H'(F_0, F_1, F_2) = 0$. Alors si U est l'ouvert des $[x] \in C$ tels que $^\exists\, i$, $F_i(x) \neq 0$, $U \to C'$, $x \mapsto [F_0(x) : F_1(x) : F_2(x)]$ est un morphisme. Soit un triplet $(f_0, f_1, f_2) \in k(C)^3$ tel que $H'(f_0, f_1, f_2) = 0$. Soit U l'ouvert des $P \in C$ tels que f_i est régulière en P, $i = 0, 1, 2$, et pour un certain i, $f_i(P) \neq 0$. Alors $U \to C'$, $P \mapsto [f_0(P) : f_1(P) : f_2(P)]$ est un morphisme (*exo : vérifier que U est bien un ouvert non vide de C*).

Cours du mercredi 9 avril 2014

Rappel : si X est une variété projective irréductible, on note $\widehat{X} := \pi^{-1}X \cup \{0\}$ et $k(X) := k(\widehat{X})_0$. Si $f \in k(X)$, on dit que f est régulière en $P \in X$ s'il existe $a, b \in k[\widehat{X}]$ homogènes de même degré tels que $f = a/b$ et $b(P) \neq 0$ On note $\mathrm{Dom}(f) := \{P \in X \ : \ f \text{ est régulière en } P\}$. C'est un ouvert non vide de de X.

Valeurs d'une fonction rationnelle : si $f \in k(X)$ et si $P \in \mathrm{Dom}(f)$, on pose $f(P) = a(P)/b(P)$ si $f = a/b$ avec $a, b \in k[\widehat{X}]$ de même degré et $b(P) \neq 0$.

Exercice : l'application $f : \mathrm{Dom}(f) \to \mathbb{A}^1$, $P \mapsto f(P)$ est un morphisme.

Soit $P \in X$. Soit A le sous-anneau des fonctions $f \in k(X)$ régulières en P. L'application :

$$A \to \mathscr{O}_{X,P}\,,\ f \mapsto (f, \mathrm{Dom}(f)) \bmod \sim$$

est un isomorphisme d'anneaux (la réciproque est définie ainsi : soit $f : U \to \mathbb{A}^1$ un morphisme où U est un ouvert contenant P ; quitte à prendre un plus petit ouvert, on peut supposer qu'il existe $a, b \in k[\widehat{X}]$ homogènes de même degré tels que $\forall\, x \in U$, $b(x) \neq 0$ et $\forall\, x \in U$, $f(x) = a(x)/b(x)$; alors on associe à f la fraction a/b ; si $(f, U) \sim (g, V)$, alors la fraction associée à g est la même (dans $k(X)$)). Donc $\mathrm{Frac}(\mathscr{O}_{X,P}) \simeq k(X)$

Soient X, X' des variétés quasiprojectives irréductibles (*i.e.* des ouverts de fermés d'espaces projectifs).

Une application *rationnelle* $f : X - -- > X'$ est un morphisme $f : U \to X'$ où U est un ouvert non vide de X.

On dit que deux applications rationnelles $f, g : X - -- > X'$ sont équivalentes si elles coïncident sur un ouvert non vide.

Exercice : c'est bien une relation d'équivalence !

2.12.1 Description à équivalence près des applications rationnelles

Exercice :

a) une application rationnelle $f : X - -- > \mathbb{P}^n$ où X est un fermé irréductible de $\mathbb{P}^m$ est équivalente à une application rationnelle de la forme $[F_0 : ... : F_n]$ pour certains $F_i \in k[\widehat{X}]$ homogènes de même degré, non tous nuls et aussi à une application rationnelle de la forme $[f_0 : ... : f_n]$ où les $f_i \in k(X)$ ne sont pas tous nuls.

b) Deux applications rationnelles $[F_0 : ... : F_n]$ et $[G_0 : ... : G_n]$ sont équivalentes si et seulement si pour tous i, j, $F_iG_j = F_jG_i$ dans $k[\widehat{X}]$.

c) Si $f = [f_0 : ... : f_n] : X \to \mathbb{P}^n$ est une application rationnelle avec $f_i \in k(C)$, pour tout i, alors $f \sim [hf_0 : ... : hf_n]$ pour tout $0 \neq h \in k(C)$.

Soit $f : X - -- > \mathbb{P}^n$ un morphisme. Si $P \in X$, on dira que f est régulière en P s'il existe un voisinage ouvert V de P dans X, un morphisme $g : V \to \mathbb{P}^n$ tel que $f \sim g$. Dans ce cas, on peut sans ambiguïté définir f comme une fonction sur V *exo !*.

2.12.2 Applications birationnelles

Une application rationnelle $f : X - -- > X'$ est *dominante* s'il existe un ouvert U où f est un morphisme tel que $f(U)$ est dense dans X'.

Exercice : c'est indépendant de l'ouvert U choisi *i.e.* si $f : U \to X'$ est un morphisme tel que $\overline{f(U)} = X'$, si $\emptyset \neq V \subseteq U$, alors $\overline{f(V)} = X'$.

Propriétés :

a) si $\varphi_1, \varphi_2 : C - -- > \mathbb{P}^n$, où C est une courbe irréductible, coïncident sur une partie infinie de C, alors $\varphi_1 = \varphi_2$;

b) si $\varphi : X - -- > Y$ est dominante, où X, Y sont des fermés projectifs, alors on peut définir $\varphi^* : k(Y) \to k(X)$, $h \mapsto h \circ \varphi$; on obtient une bijection :

$$\left\{ \text{ Applications rationnelles dominantes : } X - -- > Y \right\}$$

$$\stackrel{*}{\to}$$

$$\left\{ k-\text{morphismes de corps } k(Y) \to k(X) \right\} ;$$

c) $(\varphi_1 \circ \varphi_2)^* = \varphi_2^* \circ \varphi_1^*$.

Remarque : si Y est une courbe irréductible, $f : X - -- > Y$ est dominante si et seulement si f est non constante.

2.12.3 Application birationnelles

Une application *birationnelle* $f : X - -- > X'$ est un isomorphisme $f : U \overset{\simeq}{\rightarrow} V$ où U est un ouvert de X et V un ouvert de X'. Dans ce cas, on dit que X, X' sont birationnellement équivalentes.

Exemple : toute variété est birationnellement équivalente à tous ses ouverts non vides.

Proposition 2.12.1 *Si X, X' sont des fermés projectifs irréductibles, alors X, X' sont birationnelles si et seulement si $k(X) \simeq k(X')$.*

Exercice : $\mathrm{Aut}\mathbb{P}^1 = \mathrm{PGL}_2$ *indication : déterminer d'abord les $k-$automorphismes du corps $k(\mathbb{P}^1) \simeq k(t)$.*

Définition 18 *Une courbe rationelle est une courbe birationnelle à $\mathbb{P}^1$.*

Corollaire 2.12.1.1 *Une courbe projective irréductible C est rationnelle si et seulement s'il existe une application rationnelle $f : \mathbb{P}^1 - -- > C$ non constante.*

Démonstration : Cela résulte du théorème de Lüroth. **Q.e.d.**

Exercice : Montrer que pour toute courbe irrréductible C, il existe toujours une application rationnelle $f : C - -- > \mathbb{P}^1$ non constante.

2.13 Prolongement des applications rationnelles sur les courbes lisses

Exercice : soit $f : \mathbb{P}^1 - -- > \mathbb{P}^n$ une appplication rationnelle, montrer que f se prolonge en un morphisme $\mathbb{P}^1 \to \mathbb{P}^n$ (*indication : soient $f_0, ..., f_n \in k[X, Y]$ des polynômes homogènes de même degré tels que $f = [f_0 : ... : f_n]$ sur un ouvert non vide de $\mathbb{P}^1$. Quitte à diviser par leur* pgcd*, on peut supposer que les f_i sont premiers entre eux. Alors ils n'ont aucun zéro commun !*)

Exemple : l'application rationnelle $\mathbb{P}^1 - -- > \mathbb{P}^2$, $[x : y] \mapsto [1 : y/x : y^2/x^2]$ se prolonge à $\mathbb{P}^1$.

Si X est une courbe projective lisse irréductible, alors c'est pareil !

Proposition 2.13.1 *Soit C une courbe projective irréductible. Soit $f : C - -- > \mathbb{P}^n$ une application rationnelle. Alors si P est un point lisse de P, f est régulière en P (*i.e. *il existe un ouvert U contenant P tel que $f : U \to \mathbb{P}^n$ est un morphisme). En particulier, si C est lisse f est un morphisme sur C.*

Démonstration : Il existe $f_0, ..., f_n \in k(C)$, un ouvert non vide U de C tels que pour tout $P \in U$, f_i est régulière en P, il existe i tel que $f_i(P) \neq 0$ et $f(P) = [f_0(P) : ... : f_n(P)]$. Soit $P \in C$ (non forcément dans

U). Soit t une uniformisante de $\mathscr{O}_{C,P}$ (il en existe vu que C est lisse en P). Soit $m := \min_{i=0}^{n}\{\mathrm{ord}_P(f_i)\}$. Alors $g := [t^{-m}f_0 : ... : t^{-m}f_n]$ est régulière sur un voisinage ouvert de P et est équivalente à f. **Q.e.d.**

Corollaire 2.13.1.1 *Une courbe projective rationnelle lisse est isomorphe à* $\mathbb{P}^1$.

Exercice : montrer que $y^2 = x^3 - x$ n'est pas rationnelle en utilisant qu'elle est lisse et que $(x, y) \mapsto (x, -y)$ est un automorphisme avec 4 points fixes.

Théorème 2.13.2 *Toute courbe projective est birationnellement équivalente à une courbe plane.*

Démonstration : Soit X une courbe fermée dans un $\mathbb{P}^n$. Alors le corps des fractions rationnelles $k(X)$ est de degré de transcendance 1 sur k. Donc il existe $x \in k(X)$ tel que l'extension $k(X)/k(x)$ est algébrique séparable. Donc il existe $y \in k(X)$ telle que $k(X) = k(x, y)$. Soit R un polynôme dans $k[X, Y]$ de degré minimal qui annule x, y. Soit C la courbe projective plane $V(\overline{R}(X, Y, Z)) \subseteq \mathbb{P}^2$. Alors $k(C) \simeq \mathrm{Frac}(k[X, Y]/(R)) \simeq k(X)$ où $d := \deg R$ et $\overline{R}(X, Y, Z) = Z^d R(X/Z, Y/Z)$. **Q.e.d.**

Théorème 2.13.3 *Toute courbe irréductible est birationnelle à une courbe projective lisse, unique à isomorphisme près (mais non nécessairement plane).*

Démonstration : *Unicité :* soit $\varphi : C_1 - -- > C_2$ un isomorphisme birationnelle entre courbes lisses. Alors φ est un isomorphisme. **Q.e.d.**

Soit un triplet $(f_0, f_1, f_2) \in k(C)^3 \setminus \{(0, 0, 0\}$ tel que $H'(f_0, f_1, f_2) = 0$. Soit U l'ouvert des $P \in C$ tels que $\forall\, i$, $f_i \in \mathscr{O}_{C,P}$ et $^\exists\, i$, $f_i(P) \neq 0$. L'application $U \to C'$, $P \mapsto [f_0(P) : f_1(P) : f_2(P)]$ est un morphisme.

Exercice : si $C, C' = V(H')$ sont des courbes projectives planes irréductibles, si un triplet $(f_0, f_1, f_2) \in k(C)^3 \setminus \{(0, 0, 0\}$ est tel que $H'(f_0, f_1, f_2) = 0$, on note $(f_0 : f_1 : f_2)$ l'application rationnelle correspondante. Toutes les applications rationnelles $C - -- > C'$ sont de cette forme.

Proposition 2.13.4 *Soit* $\phi = (f_0 : f_1 : f_2)$ *une application rationnelle. Il existe* S *une partie finie de* C *telle que* $P \mapsto (f_0(P) : f_1(P) : f_2(P))$ *est une vraie application* $C \setminus S \to C'$.

Soit $f : X - -- > Y$ une application rationnelle, le *domaine de* f est la réunion des ouverts U_a de X tel qu'il existe un morphisme $f_a : U_a \to Y$ dans la classe de f.

Exercice : si $f : X - -- > Y$ est une application rationnelle, si U_a est un ouvert tel qu'il existe un morphisme $f_a : U_a \to Y$ dans la classe de f, on pose $f(P) := f_a(P)$ si $P \in U_a$. C'est indépendant de l'ouvert U_a choisi. L'application $f : \mathrm{Dom}(f) \to Y$ est un morphisme.

Proposition 2.13.5 *Le domaine de définition de $\phi = (f_0 : f_1 : f_2)$ est l'ouvert des $P \in C$ tel qu'il existe $h \in k(C)^\times$ vérifiant :*

(i) $\forall\, i$, *hf_i est régulière en P,*

(ii) $^\exists\, i$, $hf_i(P) \neq 0$.

Si P est dans le domaine de ϕ, on peut définir $\phi(P)$ sans ambiguïté.

Si le domaine de ϕ est C, on dit que ϕ est un morphisme.

Exemple : soient $C = (y^2 = xz)$, $C' = \mathbb{P}^1$. L'application rationnelle $(1 : y/x) : C - -- > \mathbb{P}^1$ est un morphisme mais on ne peut pas trouver $f_0, f_1 \in k(C)$ telles que $(f_0 : f_1) = (1 : y/x)$ et $\forall\, P \in C$, $f_0(P)$ ou $f_1(P) \neq 0$.

Exercice : montrer que $(1 : y/x) : C \to \mathbb{P}^1$ est un isomorphisme en donnant sa réciproque.

Cours du mercredi 16 avril 2014

2.14 Multiplicité d'un point sur une courbe

Soit $F \in k[X, Y, Z]$ un polynôme homogène sans facteur carré non constant. Soit $P = (x_0 : y_0 : z_0)$ un point de la courbe $C := (F = 0)$. On dira que P est de *multiplicité* d si en X, Y, Z, la composante homogène non nulle de $F(x_0 + X, y_0 + Y, z_0 + Z)$ de plus petit degré est de degré d.

Supposons que F ne contient pas la droite $(z = 0)$ et que $P = (x_0, y_0, 1)$ est sur la courbe défini par F de multiplicité d. Alors (x_0, y_0) est de multiplicité d sur la courbe affine $(F(X, Y, 1) = 0) = C \cap (z \neq 0)$.

On en déduit :

Proposition 2.14.1 *Soit C une courbe plane projective. Soit F un générateur de $I(C)$. Alors si $P \in C$, $m_P(C) \geq 1$. De plus, P est lisse si et seulement si sa multiplicité est* 1.

Exemple : si $n \geq 3$, la courbe $y^2 = x^n$ a un seul point à l'infini. Ce point est de multiplicité $n - 2$.

Proposition 2.14.2 *Une courbe de degré d, irréductible avec un point de multiplicité $d - 1$ est rationnelle.*

Démonstration : On peut supposer que $d \geq 3$. On peut supposer que C est une courbe de degré d dans $\mathbb{P}^2$ telle que $C \cap (z \neq 0) \neq \emptyset$. Alors si $(F) = I(C)$, on a :

$$F(x, y, 1) = F_{d-1}(x, y) + F_d(x, y)$$

où F_i sont homogènes de degré i. Comme $F(x, y, 1) \in k[x, y]$ est irréductible, $F_{d-1}, F_d \neq 0$ et donc $F_{d-1}(1, t), F_d(1, t) \neq 0$ dans $k[t]$.

On résout $F(x, tx, 1) = 0 \Leftrightarrow x = 0$ ou $F_{d-1}(1, t) + xF_d(1, t) = 0$.

On obtient une application rationnelle non constante :

$$\mathbb{A}^1 - -- > C\ ,\ t \mapsto [-F_{d-1}(1, t) : -tF_{d-1}(1, t) : F_d(1, t)]\ .$$

Q.e.d.

En particulier, toute cubique irréductible admettant un point singulier est rationnelle.

Exercice : soit C une cubique irréductible avec un point singulier. Si ce point est de *rebroussement*, alors C est projectivement équivalente à $y^2 = x^3$; si ce point est double ordinaire, alors C est projectivement équivalente à $xy = x^3 + y^3$.

Exercice : une cubique avec 3 points singuliers est la réunion de 3 droites : par ex. : $x^3 + y^3 + z^3 = 3xyz$.

Proposition 2.14.3 *Toute quartique projective irréductible admettant* 3 *points singuliers est rationnelle.*

Démonstration : Soit $H = \sum_{\substack{i,jk \geq 0 \\ i+j+k=4}} a_{i,jk} X^i Y^j Z^k$ irréductible homogène de degré 4. On peut supposer que les 3 points singuliers sont $[1 : 0 : 0], [0 : 1 : 0], [0 : 0 : 1]$. Donc : pas de terme en X^4, Y^4, Z^4. On peut supposer que les multiplicités en ces points sont 2 : donc $H = aX^2Y^2 + bX^2Z^2 + cY^2Z^2 + dXYZ^2 + eXZY^2 + fYZX^2$. On considère :

$$\phi : \mathbb{P}^2 - -- > \mathbb{P}^2,\ [x : y : z] \mapsto [x^{-1} : y^{-1} : z^{-1}]\ .$$

qui envoie $V(H)$ sur une conique. **Q.e.d.**

Exercice : soit C une quartique avec 4 points singuliers. Alors C est la réunion de 2 coniques.

2.15 Théorème de Bézout

2.15.1 Multiplicité d'intersection dans le cas affine

On commence par le cas affine.

Soit $P \in \mathbb{A}^2$. On note $\mathscr{O}_P = \mathscr{O}_{\mathbb{A}^2,P}$.

Si $f, g \in \mathscr{O}_P$, on pose $I_P(f, g) := \dim_k \mathscr{O}_P/(f, g)$.

Proposition 2.15.1 *i)* $I_P(f,g) < \infty$ *si et seulement si* f,g *sont sans facteurs communs dans* $\mathscr{O}_P$.

ii) $I_P(f,gh) = I_P(f,g) + I_P(f,h)$ *si* f,g,h *sont deux à deux sans facteurs communs dans* $\mathscr{O}_P$.

iii) $I_P(f,g) \geq mult_P(f)mult_P(g)$ *avec égalité si les premières composantes homogènes non nulles du développement de Taylor de* f,g *au voisinage de* P *sont premières entre elles (on note* $mult_P(f)$ *le degré de la première composante homogène non nulle du développement de Taylor de* f *au voisinage de* P*).*

iv) $I_P(f,g) > 0 \Rightarrow f(P) = g(P) = 0$.

Démonstration : Du premier point : on peut supposer $f,g \in k[X,Y]$. Soit h leur pgcd. Comme f,g sont premiers entre eux dans $\mathscr{O}_P$, $h \notin \mathfrak{m}_P$ est inversible et dans $\mathscr{O}_P$, $(f,g) = (f/h, g/h)$ on peut donc supposer f,g premiers entre eux dans $k[X,Y]$. Mais alors, $V(f,g) \subseteq \mathbb{A}^2$ est fini. Notons $Q_1,...,Q_N$ les points de $V(f,g) \setminus \{P\}$. On a :

$$V(f,g) = V(M_P M_{Q_1}...M_{Q_N})$$

donc d'après le théorème des zéros, $\sqrt{(f,g)} = M_P M_{Q_1}...M_{Q_N}$. Soit $N > 0$ tel que $(M_P M_{Q_1}...M_Q)^N \leq (f,g)$. Comme $M_{Q_i}\mathscr{O}_P = \mathscr{O}_P$, on a :

$$(M_P M_{Q_1}...M_Q)^N \mathscr{O}_P = M_P^N \mathscr{O}_P = \mathfrak{m}_P^N \leq (f,g)\mathscr{O}_P$$

d'où un morphisme surjectif :

$$\mathscr{O}_P/\mathfrak{m}_P^N \to \mathscr{O}_P/(f,g)$$

et $I_P(f,g) \leq \dim_k \mathscr{O}_P/\mathfrak{m}_P^N = \sum_{i=0}^{N-1} \dim_k \mathfrak{m}_P^i/\mathfrak{m}_P^{i+1} = \sum_{i=0}^{N-1} \dim_k (X,Y)^i/(X,Y)^{i+1} = N(N+1)/2 < \infty$.

Démontrons l'inégalité $mult_P(f,g) \geq mult_P(f)mult_P(g)$ *:* on peut supposer $P = (0,0)$. On note $m := \mathrm{mult}_P(f)$, $n := \mathrm{mult}_P(g)$ et $M := (x,y)$.

On a $\dim_k \mathscr{O}_P/(f,g) \geq \dim_k \mathscr{O}_P/(f,g) + M^{m+n}$. Or on a une suite exacte :

$$\begin{array}{ccccccc}
\mathscr{O}_P/M^n \oplus \mathscr{O}_P/M^m & \longrightarrow & \mathscr{O}_P/M^{m+n} & \longrightarrow & \mathscr{O}_P/(f,g) + M^{m+n} & \longrightarrow & 0 \\
A \oplus B & \longmapsto & Af + Bg & & & & \\
 & & C & \longmapsto & C \bmod (f,g) + M^{m+n} & &
\end{array}$$

donc $\dim_k \mathscr{O}_P/(f,g) \geq \dim_k \mathscr{O}_P/(f,g) + M^{m+n} \geq \dim_k \mathscr{O}/M^{m+n} - \dim_k \mathscr{O}_P/M^m - \dim_k \mathscr{O}_P/M^n = \binom{m+n+1}{m+n-1} - \binom{m+1}{m-1} - \binom{n+1}{n-1} = mn.$ **Q.e.d.**

Exemple : $I_{(0,0)}(y-x^2, y-ax) = 1$ si $a \neq 0$, 2 si $a = 0$.

Exercice : Calculer $I_P(f,g)$ où $P=(0,0)$, $f=(x^2+y^2)^2+3x^2y-y^3$, $g=(x^2+y^2)^3-4x^2y^2$.

Soient C, C' deux courbes affines sans composante commune. Si $P \in \mathbb{A}^2$, on note :

$$I_P(C,C') := I_P(f,f')$$

où $I(C)=(f), I(C')=(f')$.

Exercice : on suppose que P est un point lisse de C. Soit f un générateur de $I(C)$ et soit f' un générateur de $I(C')$. Montrer que $I_p(C,C') = \mathrm{ord}_{P\in C}(f'|_C)$. (*indication : vérifier que* $\mathscr{O}_P/(f,g) \simeq \mathcal{O}_{C,P}/(g|_C)$).

Exercice : Soit $C = V(f)$ une courbe plane avec f sans facteur carré. Montrer que si $D = (y = ax+b)$ est une droite qui n'est pas contenu dans C, si $P = (x_0, y_0) \in C \cap D$, alors $I_P(C,D)$ est la multiplicité de la racine x_0 dans $f(x, ax+b)$. Montrer que pour toute droite D, $I_P(C,D) \geq \mathrm{mult}_P(C)$ avec égalité pour toutes les droites excepté un nombre fini d'entre elles.

En déduire que si D est une droite qui rencontre C en $P_1, ..., P_n$ et si :

$$\sum_i \mathrm{mult}_{P_i}(C) > \deg f$$

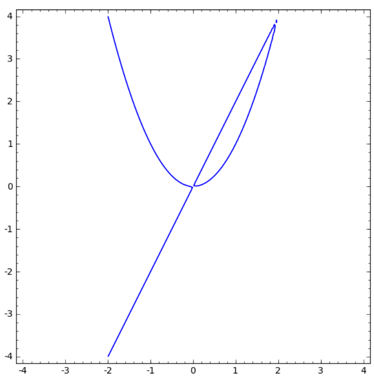
alors D est une composante de f.

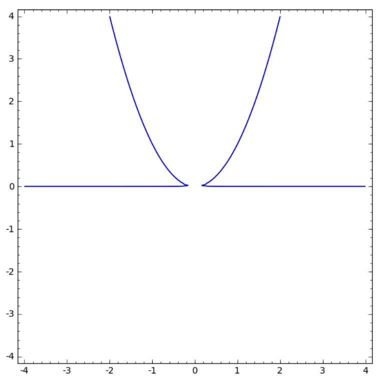
2.15.2 Intersection transverse

Soient C, C' deux courbes affines planes. Soit $P \in C \cap C'$. On dit que C et C' s'intersectent transversalement en P si P est un point lisse de C et de C' et si $T_PC \neq T_PC'$.

Exemple : en $(0,0)$, $y = x^2$ et $y = ax$ s'intersectent transversalement si et seulement si $a \neq 0$.

Proposition 2.15.2 *Soit $P \in C \cap C'$. On a :*
C, C' s'intersectent transversalement $\Leftrightarrow$ $I_P(C,C') = 1$.





Démonstration : $\Rightarrow$: supposons $P = (0,0)$. Comme les parties homogènes de degré 1 de f, g sont linéairement indépendantes, il existe $a, b \in k$, $c, d \in k$ tels que $r := af + bg = X \bmod (X,Y)^2$, $s := cf + dg = Y \bmod (X,Y)^2$. Mais alors, $(X,Y)/(X,Y)^2$ est engendré par r, s. Donc (X,Y) aussi (par Nakayama !). Donc $\mathscr{O}_P/(f,g)$ est l'image de $\mathscr{O}_P/(r,s) \simeq \mathscr{O}_{(0,0)}/(X,Y) \simeq k$. Et la multiplicité est 1.

$\Leftarrow$: On écrit $f = f_1 + ...$, $g = g_1 + ...$ où f_1, g_1 sont homogènes de degré 1 non nuls si $I_P(f,g) = 1$ avec $P = (0,0)$. Si $f_1 = \lambda g_1$, alors $(f,g) = (f - \lambda g, g) = (f_2 - \lambda g_2 + ..., g_1 + ...)$. Donc $I_P(f,g) = I_P(f - \lambda g, g) \geq 2$ contradiction.

Q.e.d.

Lemme 2.15.3 *Si $f, g \in k[X,Y]$ sont premiers entre eux, alors* $\dim_k k[X,Y]/(f,g) < \infty$ *et on a :*

$$\dim_k k[X,Y]/(f,g) = \sum_{P \in \mathbb{A}^2} I_P(f,g) \ .$$

Démonstration :

si $a \in k[X,Y]$, on notera pour tout P a_P l'image de a dans $\mathscr{O}_P/(f,g)$.

Vérifions que l'application :

$$k[X,Y]/(f,g) \to \oplus_{P \in \mathbb{A}^2} \mathscr{O}_P/(f,g) \, , \ a \mapsto \oplus_{P \in \mathbb{A}^2} a_P$$

est un isomorphisme. *Injectivité :* si $a \in k[X,Y]$ est tel que $\forall P \in \mathbb{A}^2, a_P \in (f,g)\mathscr{O}_P$, alors soit J l'idéal $\{h \in k[X,Y] \ : \ ha \in (f,g)\}$. Si $J \overset{<}{\neq} k[X,Y]$, alors J est dans un idéal maximal M_P de $k[X,Y]$, $P \in \mathbb{A}^2$. Mais il existe $h \notin M_P$ tel que $ha \in (f,g)$*i.e.* $h \in J$ d'où la contradiction. Donc $a \in (f,g)$.

Surjectivité : soient $P_1, ..., P_N \in \mathbb{A}^2$ tels que $\{P_1, ..., P_N\} = V(f,g)$. On a $\oplus_{P \in \mathbb{A}^2} \mathscr{O}_P/(f,g) = \oplus_{i=1}^N \mathscr{O}_{P_i}/(f,g)$. Il suffit de montrer que $0 \oplus ... \oplus 1 \oplus ... \oplus 0$ avec 1 en $i$ième position est atteint. Soit $h \in k[X,Y]$ tel que $h(P_i) \neq 0$ et $h(P_j) = 0$ si $j \neq i$. Il existe N tel que $M_{P_j}^N \leq (f,g)\mathscr{O}_{P_j}$ pour tout j. Alors quitte à considérer h^N, on peut supposer que $h_{P_j} = 0 \bmod (f,g)$ pour tout $j \neq i$. Comme $(M_{P_i}^N, h) = (1)$, il existe $a \in k[X,Y]$ tel que $ah = 1 \bmod (f,g)$ dans $k[X,Y]$. Alors ah a pour image $0 \oplus ... \oplus 1 \oplus ... \oplus 0$ dans $\oplus_{P \in \mathbb{A}^2} \mathscr{O}_P/(f,g)$.

Q.e.d.

2.15.3 Multiplicité d'intersection dans le cas projectif

Soient $C, C' \subseteq \mathbb{P}^2$ deux courbes projectives planes sans composante commune de degrés d, d' respectivement. Si $P \in \mathbb{P}^2$, on note $I_P(C,C') := \dim_k \mathscr{O}_{\mathbb{P}^2,P}/(I_{C,P} + I_{C',P})$ où $I_{C,P}$ est l'idéal de $\mathscr{O}_{\mathbb{P}^2,P}$ engendré par F où F est un générateur de $I(C)$:

$I_{C,P} := \{a/b : a, b \in k[X,Y,Z]$ homogènes de même degré, $b(P) \neq 0$, $a \in (F)\}$.

Exercice : si P est de la forme $[x : y : 1]$, alors $I_P(C, C') = m_{(x,y)}(C \cap \mathbb{A}^2, C' \cap \mathbb{A}^2) = I_{(x,y)}(f, g)$ où $f(X, Y) := F(X, Y, 1)$ et $g(X, Y) := G(X, Y, 1)$.

Théorème 2.15.4 (Bézout) *Soient $C, C' \subseteq \mathbb{P}^2$ deux courbes projectives planes sans composante commune de degrés d, d' respectivement. On a l'égalité :*

$$\sum_{P \in \mathbb{P}^2} I_P(C, C') = dd' \ .$$

Démonstration : L'ensemble $C \cap C'$ est fini donc il existe H une forme linéaire sur k^3 telle que $\forall\, P \in C \cap C'$, $H(P) \neq 0$. Quitte à faire un changement linéaire de coordonnées, on peut supposer que $H = Z$. Mais alors :

$$\sum_{P \in \mathbb{P}^2} I_P(C, C') = \sum_{P \in \mathbb{A}^2} I_P(f, f') = \dim_k k[X, Y]/(f, f')$$

où $f := F(X, Y, 1)$, $f' := F'(X, Y, 1)$ avec $(F) = I(C)$, $(F') = I(C')$, $F, F' \in k[X, Y, Z]$ homogènes de degrés d, d'. Remarquons que F, F' sont premiers avec Z donc f, f' sont de degrés d, d' et premiers entre eux. Vérifions que dans ce cas $\dim_k k[X, Y]/(f, f') = dd'$.

Si $n \geq 0$, on pose $k[X, Y]_{\leq n} :=$ l'espace des polynômes de degrés $\leq n$ et $(f, f')_{\leq n} := (f, f') \cap k[X, Y]_{\leq n}$.

Si $n \geq d + d'$, on a une suite exacte courte :

$$\begin{array}{ccccccccc} 0 & \longrightarrow & k[X,Y]_{\leq n-d-d'} & \xrightarrow{j} & k[X,Y]_{\leq n-d} \oplus k[X,Y]_{\leq n-d'} & \xrightarrow{p} & (f,f')_{\leq n} & \longrightarrow & 0 \\ & & A & \longmapsto & Af' \oplus -Af & & & & \\ & & & & B \oplus C & \longmapsto & Bf + Cf' & & \end{array}$$

i.e. j est injective, p est surjective et $\operatorname{im} j = \ker p$.

On en déduit que $\dim_k (f, f')_{\leq n} = \binom{n-d+2}{n-d} + \binom{n-d'+2}{n-d'} - \binom{n-d-d'+2}{n-d-d'}$. Donc :

$$\dim_k k[X, Y]_{\leq n}/(f, f')_{\leq n} = \binom{n+2}{n} - \binom{n-d+2}{n-d} - \binom{n-d'+2}{n-d'} + \binom{n-d-d'+2}{n-d-d'}$$
$$= dd'$$

pour tout $n \geq d, d'$. Donc :

$$\dim_k k[X, Y]/(f, f') = dd' \ .$$

Q.e.d.

2.15.4 Conséquences de Bézout

2.15.4.1 Équations des cubiques planes

Section non traitée en cours ...

Soit C une courbe projective plane irréductible. On dit que $P \in C$ est un *point d'inflexion* de C si $I_P(T_PC, C) \geq 3$.

Soit F un générateur de $I(C)$ dans $k[X_1, X_2, X_3]$. On note $H_F := \det(\partial_{X_iX_j}F)_{1\leq i,j\leq 3}$. *Exercice :* si $\deg F = n$, alors $\deg H_F = 3(n-2)$.

Proposition 2.15.5 (car $(k) = 0$**)** *On suppose que C est de degré ≥ 3. Le point $P \in C$ est d'inflexion ou singulier si et seulement si $H_F(P) = 0$.*

Démonstration : Quitte à faire un changement linéaire de coordonnées, on peut supposer que $P = [0:0:1]$ et que $T_PC = (y = 0)$. Alors $F(X,Y,1) =: f(X,Y) = Y + aX^2 + bXY + cY^2 + dX^3 + eX^2Y + ...$ Or, $\mathrm{mult}_P(F, H_F) = \mathrm{mult}_0(f, g)$ où $g = \partial_y f^2 \partial_{xx} f + \partial_x f^2 \partial_{yy} f - 2\partial_x f \partial_y f \partial_{xy} f$ et $g = 2a + 6dx + (8ac - 2b^2 + 2e)y + ...$ **Q.e.d.**

Proposition 2.15.6 (car $(k) = 0$**)** *Soit C une courbe projective plane irréductible de degré 3. Alors, C est projectivement équivalente à $Y^2Z = X^3$, $Y^2Z = X^2(X+Z)$ ou $Y^2Z = X(X-Z)(X-\lambda Z)$, $\lambda \in k$, $\lambda \neq 0, 1$.*

Démonstration : D'après Bézout C a 9 points d'inflexions. On peut supposer que l'un d'eux est $P = [0:1:0]$. Quitte à faire un changement linéaire de variables, on peut aussi supposer que $T_PC = (z = 0)$. **Q.e.d.**

2.15.4.2 Le théorème de Chasles pour les cubiques

Théorème 2.15.7 *Soit $C \subseteq \mathbb{P}^2$ une cubique irréductible. Soient $P_1, ..., P_8$ 8 points distincts de C. Il existe un 9ième point de C P_9 tel que :*

– ou bien $P_9 \notin \{P_1, ..., P_8\}$ et toute cubique Y qui passe par $P_1, ..., P_8$ passe aussi par P_9 ;

– ou bien $P_9 \in \{P_1, ..., P_8\}$ et toute cubique Y qui passe par $P_1, ..., P_8$ vérifie : $\mathrm{mult}_{P_9}(Y, C) \geq 2$.

Démonstration : Le théorème est vrai mais on ne fera la démonstration que pour le cas où P_1, P_2, P_3 sont sur deux droites distinctes et (P_1P_2), (P_2P_3) ne rencontrent pas $\{P_4, ..., P_8\}$.

Soit $S_3 := k[X,Y,Z]_3$. On a $\dim_k S_3 = 10$. Chaque P_i définit un hyperplan de S_3 : $\{F \in S_3 : F(P_i) = 0\}$. On a donc :

$$\dim_k\{F \in S_3 : \forall\, 1 \leq i \leq 8,\ F(P_i) = 0\} \geq 2\ .$$

S'il y a égalité, soient $F_1, F_2 \in S_3$ une base de $\{F \in S_3 \ : \ \forall\, 1 \leq i \leq 8,\, F(P_i) = 0\}$. On peut choisir pour F_1 l'équation de C donc on peut supposer que F_1, F_2 sont sans composante commune. Soit P_9 le 9ème poihnt d'intersection de $(F_1 = 0)$ et $(F_2 = 0)$. Si Y est une cubique qui passe par $P_1, ..., P_8$, alors $F = \lambda F_1 + \mu F_2$, donc $\mathrm{mult}_{P_9}(F_1, F) \geq \mathrm{mult}_{P_9}(F_1, F_2)$.

Supposons donc maintenant que $\dim_k\{F \in S_3 \ : \ \forall\, 1 \leq i \leq 8,\, F(P_i) = 0\} > 2$. Soient x, y deux points distincts dans $(P_1P_2) \setminus X$. Notons L une équation de (P_1P_2). On peut trouver une cubique Y d'équation $G = 0$ qui passe par $x, y, P_1, ..., P_8$ car $\dim_k\{F \in S_3 \ : \ F(x) = F(y) = 0, \forall\, 1 \leq i \leq 8,\, F(P_i) = 0\} \geq 1$. Mais alors $(L = 0) \cap (G = 0)$ contient ≥ 4 points. Par Bézout, $L|G$. Soit $B := G/L$. Le polynôme B est l'équation d'une conique C qui passe par $P_3, ..., P_8$. On trouve de même une conique $C' \neq C$ d'équation B' qui passe par $P_2, P_4, ..., P_8$. Mais alors $C \cap C'$ contient au moins 5 points. Par Bézout, il existe L'' une équation linéaire qui définit une composante commune de C et C'. On a :$B = L"L_1$, $B' = L"L_2$ pour certaines équations linéaires L_1, L_2. On en déduit qu'une des droites $(L" = 0)$, $(L_1 = 0)$ ou $(L_2 = 0)$ contient 4 points parmi $\{P_2, ..., P_8\}$ (en effet, si $L"(P_2) = 0$, alors ou bien $(L" = 0)$ contient 3 points de $\{P_3, , ..., P_8\}$ et donc au moins 4 avec P_2 ou bien $(L_2 = 0)$ contient au moins 4 points de $\{P_3, , ..., P_8\}$. De même si $L"(P_3) = 0$. Si $L"(P_2)$ et $L"(P_3) \neq 0$, quitte à renuméroter, on peut supposer que $L"$ s'annule en P_4, P_5, P_6 (si l'annulation a lieu en moins de 3 points, L_1 s'annule en au moins 4 points). Mais alors si $L_1 \neq L_2$, L_1 et L_2 ont au plus un point en commun donc $L"(P_7)$ ou $L"(P_8) = 0$. Si $L_1 = L_2$, c'est facile). Absurde car C est une cubique irréductible ! **Q.e.d.**

Corollaire 2.15.7.1 (Loi de groupes sur une cubique) *Soit $X \subseteq \mathbb{P}^2$ une cubique irréductible lisse. Soit $e \in X$. Si $x, y \in X$, on note xy le troisième point d'intersection de la droite (xy) avec X. On note $x \oplus y$ le troisième point d'intersection de la droite $e(xy)$ avec X. L'application $X \times X \to X$, $(x, y) \mapsto x \oplus y$ est une loi de groupes commutative de neutre e.*

Remarque : si $x = y$, on remplace (xy) par la tangente à X en x. *Exercice* : $X \times X \to x$, $(x, y) \mapsto x \oplus y$ est un morphisme.

Démonstration : Le seul point délicat est l'associativité. Soient x, y, z 3 points distincts de X. On considère les 8 points $e, x, y, xy, zy, x \oplus y, y \oplus z$. ils sont sur 3 cubiques :

$$X,\ \langle x, y\rangle \cup \langle yz, y \oplus z\rangle \cup \langle z, x \oplus y\rangle,\ \langle y, z\rangle \cup \langle xy, x \oplus y\rangle \cup \langle x, y \oplus z\rangle\ .$$

On suppose que $e, x, y, xy, zy, x \oplus y, y \oplus z$ sont deux à deux distincts.

D'après le théorème de Chasles, $(x \oplus y)z = x(y \oplus z) \Rightarrow (x \oplus y) \oplus z = x \oplus (y \oplus z)$.

Pour le cas général, l'ensemble des x, y, z tels que $e, x, y, xy, zy, x \oplus y, y \oplus z$ sont deux à deux distincts est un ouvert non vide de $X \times X \times X$. De plus,

$\{(x,y,z)\in X\times X\times X\ :\ (x\oplus y)\oplus z = x\oplus(y\oplus z)\}$ est fermé dans $X\times X\times X$ c'est donc tout ! **Q.e.d.**

2.16 Diviseurs

Soit X une courbe projective lisse.

Définition 19 *On note* $\mathrm{Div}X$ *le groupe abélien libre ayant pour base les points de* X*. Un diviseur est un élément de* $\mathrm{Div}X$

Un diviseur de X est donc une somme formelle

$$D := \sum_{x\in X} n_x x$$

où $\forall\, x \in X$, $n_x \in \mathbb{Z}$ et $n_x = 0$ sauf pour un nombre fini de $x \in X$. On notera $n_x(D)$ le coefficient devant x de D. Le *degré* de D est l'entier $\deg D := \sum_x n_x(D)$. Un diviseur est *positif* si tous ses coefficients $n_x(D) \geq 0$. On notera $D' \geq D$ si $D' - D$ est positif.

2.16.1 Diviseurs principaux

Soit $f \in k(X)$. On pose $\mathrm{ord}_P(f) := \infty$ si $f = 0$.

Lemme 2.16.1 *Si* $f \neq 0$*, alors il n'y a qu'un nombre fini de* $x \in X$ *tel que* $\mathrm{ord}_x(f) \neq 0$.

Démonstration : Soit $U := \mathrm{Dom}(f)\cap\mathrm{Dom}(f^{-1})$. C'est un ouvert non vide et si $x \in X \setminus U$, qui est fini, $\mathrm{ord}_x f \geq 0$ et $\mathrm{ord}_x(f^{-1}) = -\mathrm{ord}_x f \geq 0 \Rightarrow \mathrm{ord}_x f = 0$. **Q.e.d.**

On peut donc définir si $f \in k(X) \setminus \{0\}$, $\mathrm{div} f := \sum_{x\in X} \mathrm{ord}_x(f)x$.

On dit qu'un tel diviseur est *principal*.

On a un morphisme de groupes :

$$\mathrm{div} :\ k(X)^\times \to \mathrm{Div}X\ \ .$$

On dit que $D, D' \in \mathrm{Div}X$ sont équivalents, on le note $D \sim D'$, si $D - D' \in \mathrm{div}(k(X)^\times)$.

On note $\mathrm{Cl}X := \mathrm{Div}X/\mathrm{div}(k(X)^\times)$.

Si $D \in \mathrm{Div}X$, on pose :

$$D_+ := \sum_{\substack{x\\ n_x(D)>0}} n_x(D)x\ ,\ D_- := \sum_{\substack{x\\ n_x(D)<0}} -n_x(D)x\ \ .$$

Les diviseurs D_+, D_- sont positifs et $D = D_+ - D_-$.

Zéros et pôles

Si $f \in k(X)^\times$, on pose $\mathrm{div}(f)_0 := (\mathrm{div} f)_+$ et $\mathrm{div}(f)_\infty := (\mathrm{div} f)_-$. Ce sont le *diviseur des zéros* et le *diviseur des pôles* de f.

2.16.2 les espaces $L(D)$

Soit $D \in \mathrm{Div}X$. On note :

$$L(D) := \{f \in k(X) \ : \ \forall\, x \in X,\, \mathrm{ord}_x f + n_x(D) \geq 0\} \ .$$

Proposition 2.16.2 *(i) $L(D)$ est un sous-$k-$espace vectoriel de dimension finie de $k(X)$;*

(ii) $L(0) = k$;

(iii) si $D' \leq D$, alors $L(D') \leq L(D)$;

(iv) $\forall\, f \in k(X)^\times$, $L(D) \simeq L(D + \mathrm{div} f)$, $h \mapsto hf$.

Démonstration : (i) : il suffit de traiter le cas où $D \geq 0$; dans ce cas, on choisit pour tout $x \in X$ une uniformisante t_x de $\mathscr{O}_{X,x}$; l'application linéaire $L(D) \to \oplus_x \mathscr{O}_{X,x}/\mathfrak{m}_x^{n_x(D)}$, $h \mapsto \oplus_x t_x^{n_x(D)} h \mod \mathfrak{m}_x^{n_x(D)}$ a pour noyau les $h \in k(X)$ tels que $\mathrm{ord}_x h \geq 0$ pour tout x *i.e.* k. De plus, l'espace d'arrivée est de dimension finie !

Q.e.d.

2.16.3 Théorème de Riemann-Roch : énoncé

Théorème 2.16.3 *Il existe une unique classe de diviseurs $K_X \in \mathrm{Cl}X$ telle que :*

$$\dim_k L(D) = \deg D + \dim_k L(K_X - D) + 1 - g$$

pour tout diviseur $D \in \mathrm{Div}X$, où $g := \dim_k L(K_X)$ est appelé le genre de X.

Démonstration unicité :

On a forcément $g = \max\{\deg D - l(D) + 1 \ : \ D \in \mathrm{Div}X\}$. Donc si K' convient aussi, on a : $l(K - K') = l(K' - K) = 1$. Soit $f \in L(K - K')$. Soit $f' \in L(K' - K)$. Alors $\forall\, x \in X$, $\mathrm{ord}_x f \geq n_x(K') - n_x(K)$, $\mathrm{ord}_x f' \geq n_x(K) - n_x(K') \Rightarrow \forall x$, $\mathrm{ord}_x(ff') \geq 0 \Rightarrow ff' = c \in k^\times$ par exemple, $ff' = 1$. Mais alors $K' = K + \mathrm{div} f$. **Q.e.d.**

Voici quelques conséquences directes du théorème de Riemann-Roch :

Corollaire 2.16.3.1 $\deg(K_X) = 2g - 2$.

Corollaire 2.16.3.2 $\forall\, D \in \mathrm{Div}X$, $\deg D > 2g - 2 \Rightarrow l(D) = \deg D + 1 - g$

Corollaire 2.16.3.3 $g(X) = 0 \Leftrightarrow X \simeq \mathbb{P}^1$.

Démonstration : $\Rightarrow$: soit $x \in X$. On a $\dim l(x) = 2$. Donc il existe $f \in K$ non constante telle que $f \in L(x)$. Forcément, $\mathrm{ord}_x f = -1$. Donc $\mathrm{div}_\infty f = x$ et $[K : k(f)] = 1$ *i.e.* $K = k(f)$ donc $f : X \to \mathbb{P}^1$ induit un isomorphisme birationnel donc un isomorphisme : $f : X \simeq \mathbb{P}^1$. **Q.e.d.**

Corollaire 2.16.3.4 *Soit $X \subseteq \mathbb{P}^2$ une courbe projective plane lisse et irréductible de degré d. Alors $g(X) = \frac{(d-1)(d-2)}{2}$.*

Démonstration : Soit F un générateur de $I(X)$. Soit D une droite qui rencontre X en d points distincts. On peut supposer que cette droite est la droite à l'infini $X_0 = 0$. Soient $D = x_1 + ... + x_d$ où les x_i sont les points de $D \cap X$. Alors $L(mD) = k[X_1, X_2]_{\leq m}/(f)$ où $f(X_1, X_2) = F(1, X_1, X_2)$ est de degré d. Mais alors, on trouve :

$$\begin{aligned} l(mD) &= \frac{(m+1)(m+2)}{2} - \frac{(m-d+1)(m-d+2)}{2} \\ &= md + 1 - g \\ \Rightarrow g &= \frac{(d-1)(d-2)}{2} \ . \end{aligned}$$

Q.e.d.

2.17 Démonstration du théorème de Riemann-Roch

2.17.1

Lemme 2.17.1 *Soit k un corps algébriquement clos. Soit A une $k-$algèbre intègre de type fini de corps des fractions K. Soit L/K une extension finie de corps. Alors l'ensemble des éléments de L entiers sur A est un anneau qui est un $A-$module de type fini.*

Démonstration : On commence par le cas où $L = K$. D'après le lemme de normalisation de Nœther, il existe $x_1, ..., x_r \in A$, algébriquement indépendants sur k tels que A est entier sur $k[x_1, ..., x_r]$. On peut même choisir les x_i tels que $K/k(x_1, ..., x_r)$ soit une extension séparable ((*exo*)).Soit $\omega_1, ..., \omega_N$ une base de K comme $k(x_1, ..., x_r)-$espace vectoriel. On peut choisir les ω_i entiers sur $k[x_1, ..., x_r]$. Soit B l'anneau des éléments de K entiers sur $k[x_1, ..., x_r]$. L'application :

$$K \to k(x_1, ..., x_r)^N, \ u \mapsto (\mathrm{Tr}_{K/k(x_1,...,x_r)}(u\omega_i))_{i=1}^N$$

envoie B dans $k[x_1, ..., x_r]^N$. C'est une application injective car $\forall\, i\ \mathrm{Tr} u\omega_i = 0 \Rightarrow \forall\, x \in K$, $\mathrm{Tr} ux = 0 \Rightarrow \forall\, x \in K$, $\mathrm{Tr} x = 0$ absurde car $K/k(x_1, ..., x_r)$ est séparable. Donc B est un $k[x_1, ..., x_r]-$ module de type fini en tant que sous-$k[x_1, ..., x_r]-$module d'un $k[x_1, ..., x_r]-$ module de type fini. Si $K \overset{<}{\neq} L$, notons encore B l'anneau des éléments de L entiers sur A ; soient $y_1, ..., y_d \in L$ entiers sur A qui forment une base de L comme $K-$espace vectoriel. Alors B est un $A[y_1, ..., y_d]-$module de type fini d'après le cas précédent. Donc B est un $A-$module de type fini. **Q.e.d.**

Lemme 2.17.2 *Soit $t \in k(X)$ un élément non nul. Soit R_t l'anneau des éléments de $k(X)$ entiers sur $k[t]$. Alors il existe un ouvert affine U de X tel que $k[U] = R_t$.*

Démonstration : L'anneau R_t est de type fini sur k d'après le lemme précédent. Il existe donc une variété affine $\Omega \leq \mathbb{A}^N$ et un isomorphisme $\phi : R_t \overset{\simeq}{\rightarrow} k[\Omega]$. Forcément, Ω est une courbe affine irréductible et lisse (car $k[\Omega] = R_t$ est intégralement clos. Comme $k(\Omega) \simeq \mathrm{Frac}(R_t) = k(X)$, il existe un isomorphisme birationnel $f : \overline{\Omega}^{\mathbb{P}^N} --- > X$ tel que $f^* = \phi$. Il existe donc $U \subseteq \Omega$ et $V \subseteq X$ des ouverts affines non vides tels que $f : U \simeq V$. Comme Ω est lisse, f se prolonge à Ω ; comme X est lisse f^{-1} se prolonge à X. On en déduit que $f(\Omega)$ est un ouvert affine de X et que $k[f(\Omega)] = (f^{-1})^* k[\Omega] = R_t$. **Q.e.d.**

2.17.2 Degré des diviseurs principaux

Théorème 2.17.3 *Soit $K := k(X)$. Pour tout $x \in K \setminus k$, on a :*

$$[K : k(x)] = \sum_{P \in X} \max\{\mathrm{ord}_P(x), 0\} \ .$$

Démonstration : Soit U un ouvert affine de X tel que $R_x = k[U]$. L'anneau R_x est de Dedekind donc :

$$xR_x = \prod_{P \in U} M_P^{n_x(P)} \ .$$

on vérifie facilement que $n_x(P) = \mathrm{ord}_P(x)$. De plus si $P \in X$, $\mathrm{ord}_P(x) \geq 0 \Rightarrow P \in U$. En effet, soit un tel P. Alors $\mathrm{ord}_P x \geq 0 \Rightarrow x \in \mathscr{O}_P \Rightarrow k[x] \leq O_P \Rightarrow R_x \leq O_P$ car O_P est intégralement clos. Si $\mathfrak{m}_P \cap R_x = 0$, alors $k[x] \setminus 0 \leq O_P^\times \Rightarrow k(x) \leq O_P \Rightarrow K \leq O_P$ car $K/k(x)$ est entier. C'est absurde car $\mathrm{ord}_P : K \to \mathbb{Z}$ ne serait plus surjective. Donc il existe $Q \in U$ tel que $M_Q = \mathfrak{m}_P \cap R_x$. Forcément $Q = P$. En effet, écrivons $Q = [q_0 : ... : q_N]$, $P = [p_0 : ... : p_N]$. Choisissons h une forme linéaire sur $\mathbb{A}^{N+1}$ telle que $h(P) \neq 0$, $h(Q) \neq 0$. Alors pour tous i, j, $X_i q_j - X_j q_i / h^2 \in k(U)$ s'annule en Q. Donc $X_i q_j - X_j q_i / h^2 = a/b$ avec $a \in M_Q$ et $0 \neq b \in k[U]$ et donc $a(P) = 0$ et $p_i q_j = p_j q_i$ pour tous i, j *i.e.* $P = Q$. En particulier, $P \notin U \Rightarrow \mathrm{ord}_P(x) < 0$.

Comme $k[x]$ est principal, R_x est un $k[x]-$module libre de rang fini (c'est de type fini et sans torsion). Comme $\mathrm{Frac} R_x = K$, le rang est $n := [K : k(x)]$.

Donc $R_x / xR_x \simeq k[x]^n / xk[x]^n \simeq k^n$. D'après le théorème des restes chinois :

$$R_x / \prod_{p \in U} M_P^{n_p} \simeq \prod_{P \in U} k[U]/M_P^{n_p}$$

et $k[U]/M_P^{n_p}$ est de dimension n_p (*exo*). **Q.e.d.**

Il y a autant de zéros que de pôles, comptés avec multiplicité :

Corollaire 2.17.3.1 *Si $x \in K \setminus k$, alors* $\deg(\mathrm{div}_0(x)) = \deg(\mathrm{div}_\infty(x)) = [K : k(x)]$. *En particulier,* $\deg(\mathrm{div} x) = 0$.

2.17.3 Les adèles et l'inégalité de Riemann

Nous allons montrer que $l(D) \geq \deg D - g + 1$ pour une certaine constante g qui dépend de K.

Définition 20 (anneau des adèles) *On pose $\mathbb{A}_K$ le produit restreint de K par rapport aux points P de X et aux anneaux O_P :*

$$\mathbb{A}_K := \{(x_P)_{P \in X} : \forall P,\ x_P \in K \text{ et } x_P \in O_P \textit{ sauf au plus pour un nombre fini de } P \in X\}.$$

On a un plongement diagonal de K dans $\mathbb{A}_K$: $x \mapsto (x, x, ...)$. Si D est un diviseur de X, on pose $\mathbb{A}_K(D) := \{(x_P) \ : \ \forall\, P,\ \mathrm{ord}_P(x) + n_D \geq 0\}$.

Lemme 2.17.4 *Soient* $D := \sum_P n_P P$, $E := \sum_P n'_P P$ *deux diviseurs. On a :*

(i) *si* $D \leq E$, *alors* $\mathbb{A}_K(D) \leq \mathbb{A}_K(E)$ *;*

(ii) $\mathbb{A}_K(\min\{D, E\}) = \mathbb{A}_K(D) \cap \mathbb{A}_K(E)$ *;*

(iii) $\mathbb{A}_K(\max\{D, E\}) = \mathbb{A}_K(D) + \mathbb{A}_K(E)$ *;*

(iv) $K \cap \mathbb{A}_K(D) = L(D)$.

Lemme 2.17.5 *Si* $D \leq E$ *sont des diviseurs, alors* $\dim_k \mathbb{A}_K(E)/\mathbb{A}_K(D) = \deg E - \deg D$.

Démonstration : Par récurrence sur $\deg E - \deg D$. Si $\deg E - \deg D = 0$, alors $D \leq E \Rightarrow D = E$ et c'est évident !

Si $\deg E - \deg D = 1$, alors $E = D + P$ où $P \in X$. Soit t une uniformisante de O_P. L'application :

$$A_K(D) \to O_P/\mathfrak{m}_P, \ \ (x_Q) \mapsto t^{n_D+1} x_P \bmod \mathfrak{m}_P$$

est surjective de noyau $A_K(D)$.

Si $\deg E - \deg D > 1$, alors il existe un diviseur E' tel que $D \leq E' \leq E$ et $\deg E - \deg E' = 1$. On a :

$$\begin{aligned}\dim_k \mathbb{A}_K(E)/\mathbb{A}_K(D) &= \dim_k \mathbb{A}_K(E)/\mathbb{A}_K(E') + \dim_k \mathbb{A}_K(E')/\mathbb{A}_K(D) \\ &= \deg E - \deg E' + \deg E' - \deg D \ .\end{aligned}$$

Q.e.d.

Lemme 2.17.6 *Si* $D \leq E$, *alors* $\dim_k \mathbb{A}_K(E) + K/\mathbb{A}_K(D) + K = (\deg E - l(E)) - (\deg D - l(D))$.

Démonstration : L'application $\mathbb{A}_K(E) \to \frac{\mathbb{A}_K(E)+K}{\mathbb{A}_K(D)+K}$ est surjective de noyau $\mathbb{A}_K(E) \cap (\mathbb{A}_K(D) + K) = \mathbb{A}_K(D) + L(E)$.

Or $\dim_k \frac{\mathbb{A}_K(E)}{\mathbb{A}_K(D)+L(E)} = \dim_k \frac{\mathbb{A}_K(E)/\mathbb{A}_K(D)}{\mathbb{A}_K(D)+L(E)/\mathbb{A}_K(D)}$ et $\frac{\mathbb{A}_K(D)+L(E)}{\mathbb{A}_K(D)} \simeq \frac{L(E)}{\mathbb{A}_K(D) \cap L(E)}$.

Mais $\mathbb{A}_K(D) \cap L(E) = \mathbb{A}_K(D) \cap K \cap L(E) = L(D) \cap L(E) = L(D)$ ...

Q.e.d.

Si D est un diviseur, on pose $r(D) := \deg D - l(D)$.

Lemme 2.17.7 *Si* $D \leq E$, *alors* $r(D) \leq r(E)$ *et si* $f \in K^\times$, $r(D + \mathrm{div} f) = r(D)$.

Théorème 2.17.8 *La fonction* $r(D)$ *est majorée lorsque* D *décrit les diviseurs de* X.

Démonstration : Soit $x \in K\setminus k$. On a $\deg(\mathrm{div}_\infty(x)) = [K : k(x)] =: n$. Si $y \in R_x$, alors on a : $\mathrm{ord}_P x \geq 0 \Rightarrow x \in O_P \Rightarrow k[x] \leq O_P \Rightarrow y$ entier sur $O_P \Rightarrow y \in O_P$ car O_P est intégralement clos. De manière équivalente : $\mathrm{ord}_P y < 0 \Rightarrow \mathrm{ord}_P x < 0$. Donc $\mathrm{supp}(\mathrm{div}_\infty y) \subseteq \mathrm{supp}(\mathrm{div}_\infty x)$. Il existe donc $k > 0$ tel que $\mathrm{div}_\infty y \leq k\mathrm{div}_\infty x i.e.\ k\mathrm{div}_\infty x + \mathrm{div} y \geq \mathrm{div}_0 y \geq 0$. Donc pour tout $y \in R_x$, $y \in L(k\mathrm{div}_\infty x)$ pour un certain $k > 0$. Soit $y_1, ..., y_n$ une base de $K/k(x)$. On choisit les y_j dans R_x. Pour tout i, $y_i \in L(k_i\mathrm{div}_\infty x)$ pour un certain $k_i > 0$. Soit $k := \max\{k_i\}$. Pour tout i, $y_i \in L(k\mathrm{div}_\infty(x))$. Comme x est transcendant sur k, les éléments $x^i y_j$, $0 \leq i \leq m-k$, $1 \leq j \leq n$, sont dans $L(m\mathrm{div}_\infty x)$ et sont $k-$linéairement indépendants sur k. Donc $l(m\mathrm{div}_\infty x) \geq n(m-k+1)$. Donc :

$$r(m\mathrm{div}_\infty x) = \deg(m\mathrm{div}_\infty x) - l(m\mathrm{div}_\infty x) \leq (mn) - n(m-k+1) = nk - n \ .$$

La suite croissante $r(m\mathrm{div}_\infty x)$ est donc majorée donc stationnaire. Notons $g-1$ la limite. Soit D un diviseur de X, nous allons voir que $r(D) \leq g-1$.

On a $-D = D_1 + D_2$ où $\mathrm{supp}D_1 \cap \mathrm{supp}\mathrm{div}_\infty x = \emptyset$ et $\mathrm{supp}D_2 \subseteq \mathrm{supp}\mathrm{div}_\infty x$. Soit $P \in X$ tel que $n_P(D_1) < 0$. On a $k[x] \leq O_P$ et $\mathfrak{m}_P \cap k[x] = (\pi_P) \neq 0$ pour un certain $\pi_P \in k[x]$. Soit m_P tel que $\mathrm{ord}_P(\pi_P^{m_P}) + n_P(D_1) \geq 0$. De plus, comme $k[x] \leq R_x$, $\mathrm{supp}(\mathrm{div}_\infty \pi_P) \subseteq \mathrm{supp}(\mathrm{div}_\infty x)$ et donc $\mathrm{supp}(\mathrm{div}_\infty \pi_P) \cap \mathrm{supp}D_1 = \emptyset$. Soit $f := \prod_{P\,:\,n_P(D_1)<0} \pi_P^{m_P}$ où les $m_P \geq 0$ sont choisis pour que $\mathrm{ord}_P(\pi_P^{m_P}) + n_P(D_1) \geq 0$. Donc les éventuels coefficients < 0 de $\mathrm{div} f + D_1$ sont dans l'ensemble des pôles de x. Comme $\mathrm{supp}D_2 \subseteq \mathrm{supp}\mathrm{div}_\infty x$, $\mathrm{div} f - D = \mathrm{div} f + D_1 + D_2$ a des coefficients < 0 seulement (éventuellement) dans l'ensemble des pôles de x. Donc pour m assez grand, $\mathrm{div} f - D + m\mathrm{div}_\infty x \geq 0$. Donc

$$\mathrm{div} f + m\mathrm{div}_\infty x \geq D$$

$$\Rightarrow r(\mathrm{div} f + m\mathrm{div}_\infty x) \geq r(D)$$

$$\Rightarrow r(m\mathrm{div}_\infty x) \geq r(D)$$

$$\Rightarrow g - 1 \geq r(D) \ .$$

Q.e.d.

Définition 21 *On pose $g := 1+\max\{\deg D - l(D)\}$ où D décrit les diviseurs de X. C'est le genre de X.*

Remarque : on a $g = 1+\max_{m\in\mathbb{Z}}\{\deg(m\mathrm{div}_\infty x) - l(m\mathrm{div}_\infty x)\}$ pour tout $x \in K \setminus k$.

Exercice : retrouver que $g = 0$ si $X = \mathbb{P}^1$.

Corollaire 2.17.8.1 *Pour tout diviseur D de X, on a :*

$$l(D) \geq \deg D + 1 - g \ .$$

Corollaire 2.17.8.2 *Pour tout diviseur D,* $\dim_k \mathbb{A}_K/\mathbb{A}_K(D)+K<\infty$.

Démonstration : On sait que si $D'\geq D$, $r(D')-r(D)=\dim_k \mathbb{A}_K(D')+K/\mathbb{A}_K(D)+K$. Or $r(D')$ est majoré donc comme $\mathbb{A}_K=\cup_{D'}\mathbb{A}_K(D')$, $\dim_k \mathbb{A}_K/\mathbb{A}_K(D)+K\leq \sup\{r(D')\ :\ D'\}-r(D)$. **Q.e.d.**
On pose pour tout diviseur D, $H(D):=\mathbb{A}_K/\mathbb{A}_K(D)+K$. On a donc $r(D)=g-1-\dim_k H(D)$. Donc $g=\dim_k H(0)$.

Pour démontrer le théorème de Riemann-Roch il suffit donc de démontrer que $\dim_k H(D)=l(K_X-D)$ pour un certain diviseur K_X.

2.17.4 Fin de la démonstration du théorème de Riemann-Roch

Une *forme différentielle ω sur K* est une forme linéaire sur $\mathbb{A}_K$ qui s'annule sur le sous-espace $\mathbb{A}_K(D)+K$ pour un certain diviseur D de X. On peut donc identifier une forme différentielle avec un élément de $H(D)^*$.

Soit $\Omega(X)$ l'ensemble des formes différentielles de K. Si $f\in K$ et $\omega\in\Omega(X)$, on pose $f\omega(\xi):=\omega(f\xi)$ si $\xi\in\mathbb{A}_K$. L'ensemble $\Omega(X)$ devient ainsi un $K-$espace vectoriel.

Remarque : si $\omega\in H(D)^*$, $f\omega\in H(D-\mathrm{div} f)^*$.

Proposition 2.17.9 $\dim_K \Omega(X)=1$.

Lemme 2.17.10 *Soit $0\neq\omega\in\Omega(X)$, il existe un diviseur maximal (pour $\leq$) tel que $\omega\in H(D)^*$.*

Démonstration : Remarquons que si $\omega\in H(D_1)^*\bigcap H(D_2)^*$, alors $\omega\in H(\max\{D_1,D_2\})^*$. Il suffit donc de montrer que les degrés des diviseurs D tels que $\omega\in H(D)^*$ sont majorés. Soit D un tel diviseur. Si D' est un diviseur et si $f\in L(D')$, on a $\mathbb{A}_K(D-D')\leq\mathbb{A}_K(D+\mathrm{div} f)$. Soient $f_1,...,f_n$ une $k-$base de $L(D')$, on a $f_1\omega,...,f_n\omega$ qui s'annulent sur $\mathbb{A}_K(D-D')\leq\mathbb{A}_K(D+\mathrm{div} f_i)$ $(\forall\, i)$ et qui sont $k-$linéairement indépendants. Donc $\dim_k H(D-D')\geq l(D')$. D'où :

$$g-1-\deg(D-D')+l(D-D')\geq l(D')$$

$$\Leftrightarrow \deg D\leq g-1+r(D')+l(D-D')\leq 2g-2+l(D-D')=2g-2$$

si on choisit $D'>D$ tel que $L(D-D')=0$. **Q.e.d.**

Démonstration de la proposition : Raisonnons par l'absurde. Soient $\omega,\omega'\in\Omega(X)$ $K-$linéairement indépendants. Soit $(a_1,...,a_n)$ une base de $L(D')$. Alors $a_1\omega,...,a_n\omega,a_1\omega',...,a_n\omega'$ sont $k-$linéairements indépendantes dans $H(D-D')^*$ si on choisit D tel que $\omega,\omega'\in H(D)^*$. Donc $\dim_k H(D-D')\geq 2n=2l(D')$. On en déduit que :

$$g-1-\deg D+\deg D'+l(D-D')\geq 2l(D')$$

$$\Rightarrow g - 1 + 2(\deg D' - l(D')) \geq \deg D + \deg D'$$

$$\Rightarrow 3g - 3 \geq \deg D' + \deg D$$

pour tout $D' > D$ *absurde* si on choisit D' assez grand.

Q.e.d.

Soit $0 \neq \omega \in \Omega(X)$, on choisit D maximal tel que $\omega \in H(D)^*$. On note $D =: \mathrm{div}\omega$, c'est le diviseur de ω.

Corollaire 2.17.10.1 *Soient* $0 \neq \omega, \omega' \in \Omega(X)$*, alors :* $\mathrm{div}\omega \sim \mathrm{div}\omega'$

Démonstration : Soit $f \in K$ tel que $f\omega = \omega'$. Alors $\omega \in H(D)^* \Rightarrow f\omega = \omega' \in H(D + \mathrm{div}f)^*$. Donc $\mathrm{div}\omega' = \mathrm{div}f\omega = \mathrm{div}\omega + \mathrm{div}f$. **Q.e.d.**

Démonstration du théorème de Riemann-Roch : Il reste à montrer que pour tout diviseur D, $\dim_k H(D) = l(K_X - D)$ ou encore :

$$\dim_k H(K_X - D) = l(D) \ .$$

Soit $\omega \in \Omega(X)$ tel que $\mathrm{div}\omega = K_X$. Si $f \in L(D)$, alors $f\omega \in H(K_X + \mathrm{div}f)^* \leq H(K_X - D)^*$. D'où une application linéaire $c : L(D) \to H(K_X - D)^*$. Réciproquement, si $\lambda \in H(K_X - D)^*$, soit $K' := \mathrm{div}\lambda$. Alors $\lambda = g\omega$ pour une $g \in K$. On a : $\omega = g^{-1}\lambda \Rightarrow \omega \in H(K_X - D - \mathrm{div}g)^* \Rightarrow K_X - D - \mathrm{div}g \leq K_X$ par maximalité de K_X. Donc $\mathrm{div}g + D \geq 0$ *i.e.* $g \in L(D)$. L'application $H(K_X - D)^* \to L(D)$ obtenue, $\lambda \mapsto g$ est l'inverse c^{-1}. Donc $\dim_k H(K_X - D)^* = l(D)$.

Q.e.d.

2.17.5 Lien avec les différentielles usuelles

On note I le noyau du morphisme $k(X) \otimes_k k(X) \to k(X)$, $a \otimes b \mapsto ab$. On pose $\Omega^1 := I/I^2$. Si $f \in k(X)$, on pose $df := f \otimes 1 - 1 \otimes f \bmod I^2$. L'application $d : k(X) \to \Omega^1$ induit un isomorphisme :

$$\mathrm{Hom}_{k(X)}(\Omega^1, k(X)) \simeq \mathrm{Der}_k(k(X), k(X)) \ .$$

Si $P \in X$, si $\omega \in \Omega_1$, alors soit t une uniformisante de X en P. On a $\omega = f dt$ pour un $f \in k(X)$. On pose $\mathrm{Rés}_P(\omega) := c_{-1}$, coefficient de f devant t^{-1} dans $k((t)) \supseteq k(X)$. Ce nombre est indépendant de l'uniformisante choisie.

Si $\xi \in \mathbb{A}_K$, on pose $\langle \omega, \xi \rangle := \sum_{P \in X} \mathrm{Rés}_P(\xi_P \omega)$. On obtient ainsi un élément de Ω. L'application $\Omega^1 \to \Omega$, $\omega \mapsto \langle \omega, \cdot \rangle$ est un isomorphisme (*cf.* J.-P Serre, *Groupes algébriques et corps de classes*, II §8).

2.17.6 Application

Théorème 2.17.11 *Soit X une courbe projective irréductible lisse de genre 1. Alors X est isomorphe à une cubique plane lisse $c \subseteq \mathbb{P}^2$.*

Démonstration : D'après le théorème de riemann-roch, si $\deg D > 0$, on a $l(D) = \deg D$. En particulier, si $x \in X$, il existe $f \in L(2x)$ non constant et $g \in L(3x) \setminus L(2x)$. Alors $1, f, f^2, f^3, g, g^2, fg \in L(6x)$ sont $k-$linéairement indépendants :

$$a_0 + a_1 f + a_2 f^2 + a_3 f^3 + a_4 g + a_5 fg + a_6 g^2 = 0$$

pour des a_i non tous nuls. On vérifie que $\forall\, i,\ a_i \neq 0$, que $k(f,g) = k(X)$ donc $X \setminus \{x\} \to \mathbb{A}^2$, $x \mapsto (f(x), g(x))$ est un isomorphisme birationnel. Comme X n'est pas rationnelle, l'image est bien une cubique lisse de $\mathbb{P}^2$.

Q.e.d.

Index

algébrique (ensemble), 7

birationnels, 24

composante irréductible, 10
courbe rationelle, 41

degré, 51
degré d'une hypersurface, 32
degré de transcendance, 12
diviseur principal, 51
domaine de définition d'une application rationnelle, 43

fini (morphisme d'anneaux), 7

homogénéisé d'un polynôme, 33
hypersurface projective, 32

inflexion, 49
irréductible, 10

Jacobson (anneau de), 8

multiplicité, 19, 43

nœthérien (espace topologique), 11

régulier(ère), 14
radical (idéal), 9
radical d'un idéal, 9
rationnelle, 18

Zariski (topologie de), 7