L'objectif des notes suivantes est de donner une idée de l'évolution du cours de *Master 1 intitulé Algèbre, Géométrie et Calculs*, délivré à l'Université de Montpellier et d'expliquer quelques compléments ; elles seront publiées sur

`https://webusers.imj-prg.fr/~joao-pedro.dos-santos/Enseignement.html`

après chaque cours. Ces notes ne se substituent pas à la présence [1], où les idées essentielles seront présentées.

Programme approximatif

Rappels sur les anneaux factoriels

1) Anneaux euclidiens, principaux et factoriels. Les lemmes de Gauss concernant l'irréductibilité dans $A[X]$ et $K[X]$ via la valuation de Gauss. L'hérédité "A factoriel $\Rightarrow$ $A[X]$ factoriel". Polynômes à deux variables irréductibles et quelques critères.
2) Courbes planes. Le Lemme de Study et les polynômes qui définissent une courbe plane.
3) Le résultant : Définition, calculs. Le résultant et les combinaisons linéaires.
4) Le résultant et le petit théorème de Bézout.
5) Le degré du résultant et directions asymptotiques.
6) Géométrie projective et le théorème de Bézout.

Références

[1] Gerd Fischer, *Plane algebraic curves*. Student Mathematical Library, American Mathematical Society, 2001. Vous pouvez la trouver dans la bibliothèque de l'Institut Alexander Grothendieck (FIS/14/CAE 844).

[2] F. K. Kirwan, *Complex algebraic curves*. London Mathematical Society Student Texts 23, Cambridge University Press, 1992. Disponible dans la bibliothèque de l'Institut Alexander Grothendieck (DKIR/14/6500).

1. "Car, à mon avis, ce qu'il y a de terrible, Phèdre, c'est la ressemblance qu'entretient l'écriture avec la peinture. De fait, les êtres qu'engendre la peinture se tiennent debout comme s'ils étaient vivants ; mais qu'on les interroge, ils restent figés dans une pose solennelle et gardent le silence. [...] Autre chose : quand, une fois pour toutes, il a été écrit, chaque discours va rouler de droite et de gauche et passe indifféremment auprès de ceux qui s'y connaissent, comme auprès de ceux dont ce n'est point l'affaire ; de plus, il ne sait pas quels sont ceux à qui il doit ou non s'adresser. Que par ailleurs s'élèvent à son sujet des voix discordantes et qu'il soit injustement injurié, il a toujours besoin du secours de son père ; car il n'est capable ni de se défendre ni de se tirer d'affaire tout seul." Socrate. *Phèdre*.

[3] E. Kunz, *Introduction to Plane Algebraic Curves*. Birkhüser Boston. Disponible dans la bibliothèque de l'Institut Alexander Grothendieck (DKIR/14/6500) ainsi que sur `https://scdi-montpellier.hosted.exlibrisgroup.com/primo-explore/login?vid=33UM_VU1`

[4] E. Brieskorn et H. Knörrer, *Plane algebraic curves*. Birkhäuser Verlag, 1986. Cette référence peut être trouvée dans le rayons de la Bibliothèque ainsi que sur `https://scdi-montpellier.hosted.exlibrisgroup.com/primo-explore/login?vid=33UM_VU1`

[5] P. Thuillier, *D'Archimède à Einstein* .D'Archimède à Einstein. Les faces cachées de l'invention scientifique, Fayard, 1988 ; Livre de poche, 1996.

[6] J. P. dos Santos, *Cours de Géométrie Différentielle*. `https://webusers.imj-prg.fr/~joao-pedro.dos-santos/Geometrie_differentielle_elementaire/Notes_de_cours.pdf`.

[7] M. W. Hirsch, *Differential Topology*. Graduate Texts in Mathematics, Springer.

[8] A. Seidenberg, *Elements of the theory of algebraic curves*

Cours 1

(17 Janvier 2022).

Notations générales :

1. Les anneaux sont toujours commutatifs et unitaires.
2. Sauf mention du contraire, A désigne toujours un anneau.
3. Étant donnés des éléments $x_1, \ldots, x_n$ de A, on désigne par $\langle x_1, \ldots, x_n \rangle$ l'idéal de $a_1 A + \cdots + a_n A$.
4. Si A est un anneau intègre, son corps de fractions sera noté $\mathrm{Fr}(A)$.
5. k désigne un corps.
6. Un vecteur avec entrées dans un anneau A est une matrice ayant une colonne. Le module des vecteurs de longueur n est noté A^n.

1 Rappels de la théorie des anneaux factoriels

La plupart des résultats suivants est vue dans un cours de troisième année en Algèbre, comme par exemple "Groupes et anneaux 2" qui a lieu au 6ème semestre.

On fera appel à plusieurs notions de la théorie des anneaux factoriels.

Définition 1. 1. On dit que un élément $x \in A$ *divise* un élément $z \in A$ s'il existe un $y \in A$ tel que $xy = z$. Dans ce cas, on écrira $x \mid z$.

2. Un élément $u \in A$ est *inversible* s'il divise 1. Il est clair que l'ensemble des éléments inversibles est, avec la multiplication de l'anneau, un groupe. Il sera désigné par $A^\times$.
3. Soit $x \in A$. Un élément $x' \in A$ est dit *associé* à x si $x' = ux$ avec $u \in A^\times$. On écrira $x \overset{\text{ass}}{\sim} y$ pour dire que x est associé à y et on remarquera que $\overset{\text{ass}}{\sim}$ est une relation d'équivalence.
4. Un élément $x \in A$ est *irréductible* s'il *n'est pas nul ou inversible* et si *chacun de ses diviseurs lui est associé.* [2]
5. Un élément $x \in A$ est dit *premier* s'il *n'est pas nul ou inversible* et satisfait la *version abstraite du Lemme d'Euclide* : Si un produit yz est divisible par x, alors ou bien x divise y, ou bien x divise z.

On notera que

2. Erratum, 25.01. Cette définition est incomplète et après "lui est associé" on doit rajouter "ou inversible". Quand A est un anneau intègre et $x \in A$ est irréductible, cette définition implique que si $x = yz$, alors soit $y \in A^\times$, soit $z \in A^\times$. Par contre, si $A = \mathbf{Z} \times \mathbf{Z}$, alors $x = (1, 0)$ est tel que $x = xx$, mais x n'est pas inversible.

Lemme 2. *Si A est intègre, alors tout premier est irréductible.*

Démonstration. Soit p premier et soit $p = fg$. Alors soit $p \mid f$, soit $p \mid g$. Si $p \mid f$, on écrit $pf_1 = f$. Donc $p = pf_1g$ et $f_1g = 1$ car $p(1 - f_1g) = 0$. Il suit que $1 - f_1g = 0$, parce que A est intègre et p est non-nul. Or, dans ce cas, f_1 et g sont inversibles. On déduit que $p \overset{\text{ass}}{\sim} f$. Si $p \mid g$, le même argument montre que $p \overset{\text{ass}}{\sim} g$ et f est inversible. Conclusion : Un diviseur de p lui est associé ou est inversible. □

Remarques 3. On remarquera que dans l'Arithmétique élémentaire, c'est-à-dire l'étude de l'anneau $\mathbf{Z}$, les premiers sont les irréductibles de la définition précédente.

Après ces définitions, les exemples suivants sont fondamentaux.

Exemple 4. Le Lemme d'Euclide dit que dans l'anneau $\mathbf{Z}$, les irréductibles coïncident avec les premiers. Par contre, soit $\theta = \mathrm{i}\sqrt{5}$ et soit A le sous-anneau $\{a+b\theta \,:\, a, b \in \mathbf{Z}\}$ de $\mathbf{C}$. L'élément 2 est irréductible (à vous !) mais il n'est pas premier. En effet, $6 = (1+\theta)(1-\theta)$ et 2 ne divise ni $1 + \theta$, ni $1 - \theta$.

Une des propriétés les plus souhaités d'un anneau est que le théorème fondamental de l'Arithmétique soit encore vrai : Chaque élément se décompose de façon unique comme produit d'éléments irréductibles. Voici la définition :

Définition 5. Un anneau A est factoriel s'il est *intègre* et si les propriétés suivantes sont vérifiées

F1. Pour chaque $f \in A$, il existe des éléments irréductibles $p_1, \ldots, p_m$, pas forcément distincts, tels que $f = p_1 \cdots p_m$.

F2. Si $p_1, \ldots, p_m$ et $q_1, \ldots, q_n$ sont irréductibles, pas forcément distincts, tels que $p_1 \cdots p_m = q_1 \cdots q_n$, alors $m = n$ et il existe $\sigma \in \mathcal{S}_m$ tel que $q_i \overset{\text{ass}}{\sim} p_{\sigma(i)}$.

Exemple 6. L'anneau $\mathbf{Z}$ est l'anneau factoriel par excellence. Ce fait est connu comme "le théorème fondamental de l'arithmétique".

Exemple 7 (**F1** fait défaut)**.** Soit $\mathcal{O}$ l'anneau des fonctions holomorphes sur tout le plan complexe. Soit $f : \mathbf{C} \to \mathbf{C}$ définie par $f(z) := \sin(\pi z)$. En écrivant $t_n(z) = z - n$ pour chaque $n \in \mathbf{Z}$, on voit que $t_n \mid f$ pour tout n. Ceci montre que f ne possède pas de décomposition en facteurs irréductibles.

Exemple 8 (**F2** fait défaut)**.** On peut prendre l'exemple de $\mathbf{Z}[\mathrm{i}\sqrt{5}]$ et décomposer 6 de deux façons différentes : $2 \cdot 3 = (1 - \mathrm{i}\sqrt{5})(1 + \mathrm{i}\sqrt{5})$.

À ce moment, le lecteur devra se rappeler de la preuve du fait que $\mathbf{Z}$ est factoriel. La vérification de **F1** est immédiate et employe la fait que $\mathbf{Z}$ est ordonné. La validité de **F2** est plus subtile et est conséquence des propositions suivantes :

P1 Division Euclidienne ⇒ Tout idéal est principal.

P2 Tout idéal est principal ⇒ Lemme d'Euclide.

P3 Lemme d'Euclide ⇒ l'unicité.

Il est ainsi important de pousser les propositions ci-dessus dans un contexte abstrait. La division euclidienne devient un axiome :

Définition 9 (Anneau euclidien)**.** Soit A intègre. Un jauge euclidien est une fonction $\varphi : A\backslash\{0\} \to \mathbf{N}$ ayant la propriété suivante :

DE. Pour chaque couple d'éléments $x \in A$ et $d \in A\backslash\{0\}$, il existe un[3] couple $q, r \in A$ tel que

$$x = dq + r \quad \text{et} \quad \text{si } r \neq 0, \text{ alors } \varphi(r) < \varphi(d).$$

Un anneau intègre avec un jauge euclidien est dit un anneau euclidien.

Exemple 10. Les exemples les plus importants d'anneaux euclidiens sont :

(a) L'anneau des entiers avec le jauge $|\bullet|$.

(b) L'anneau des polynômes en une variable $k[X]$ avec le jauge deg. (Ceci est normalement vu au cours d'Arithmétique de L2.)

(c) L'anneau des entiers de Gauss $\mathbf{Z}[\mathrm{i}]$ avec la norme $N(a+\mathrm{i}b) = a^2+b^2$. (Ce fait est moins célèbre que les autres, mais il a été traité aux TDs du cours "Groupes et anneaux" en L3.)

Ensuite on a **P1**.

Théorème 11. *Si A est Euclidien, alors tout idéal est principal.*

Démonstration. Il suffit de choisir l'élément non-nul de l'idéal en question ayant le plus petit jauge Euclidien et la division Euclidienne fait le reste. □

Maintenant, on donne un nom aux anneaux n'ayant que des idéaux principaux.

Définition 12. Un anneau A est principal si tout idéal est principal.

Maintenant le **P2** suit :

Théorème 13. *Soit A principal. Alors tout irréductible est premier.*

Démonstration. Soit $x \in A$ irréductible tel qeu $x \mid yz$. On suppose que $x \nmid y$ et on considère un générateru g de $\langle x, y\rangle$. Il suit que $g \mid x$. Dans ce cas, soit $g = ux$ avec $u \in A^\times$, soit $g \in A^\times$. Or, si $x = ug$, il suit que $x \mid y$, ce qui est exclu. Donc $g \in A^\times$ et on peut écirre $1 = ax + by$. Par conséquent, $z = axz + b \cdot yz$ et $x \mid z$. □

3. On ne demande pas l'unicité !

Finalement, **P3** :

Théorème 14. *Soit A un anneau intègre où tout irréductible est premier. Soient $p_1, \dots p_m$ et $q_1, \dots, q_n$ des irréductibles pas forcément distincts. Alors l'égalité*

$$p_1 \cdots p_m = q_1 \cdots q_n$$

implique que

(i) Les entiers m et n coïncident.

(ii) Il existe $\sigma \in \mathcal{S}_m$ telle que q_j et $p_{\sigma(j)}$ sont associés.

*En particulier, si A est intègre et **F1** est vraie, alors A est factoriel.*

Démonstration. On fait une récurrence sur $\min(m, n)$. Si $m = 1$, on a $p_1 = q_1 \cdots q_n$. Comme p_1 est premier, il doit diviser un certain q_j ; on suppose ainsi que $p_1 \mid q_1$. Dans ce cas, $p_1 \sim q_1$. Puisque A est intègre $\Rightarrow 1 = q_2 \cdots q_n$ et ceci contredit le fait que q_i soit irréductible. Donc $n = 1$. Le cas général est au lecteur.

La dernière affirmation est facile, puisque on a prouvé que la propriété **F2** est vraie. □

Remarques 15. Si A est intègre et principal, alors la propriété **F1** est vraie aussi. En effet, si ceci est faux, alors il existe $f \in A$ et des des éléments $\{d_n \in A : n \in \mathbf{N}\}$ tels que

(i) $d_n \mid \cdots \mid d_0 \mid f$ et

(ii) L'élément d_{n+1} n'est pas associé à d_n.

Or, ceci implique que

$$\langle f \rangle \subset \cdots \subset \langle d_i \rangle \subset \langle d_{i+1} \rangle \subset \cdots$$

et on est conduit à considérer l'idéal $I = \bigcup_i \langle d_i \rangle$. Soit g un générateur de I. Par définition, il existe un $m \in \mathbf{N}$ tel que $g \in \langle d_m \rangle$. On déduit que $d_m \mid d_{m+1}$. Puisque $d_{m+1} \mid d_m$, on voit que $d_m \overset{\text{ass}}{\sim} d_{m+1}$, en contradiction avec (ii).

2 La factorisation dans un anneau de polynômes

On suppose A factoriel ; on écrit $K = \mathrm{Fr}(A)$. On souhaite étudier les factorisation dans $A[X]$. L'idée principale ici est utiliser le contenu d'un polynôme. On fera ce chemin en empruntant la route ouverte par la valuation de Gauss.

Soit $\mathcal{P}$ un ensemble de premiers de A ayant la propriété suivante : Pour chaque irréductible π de A, il existe un *unique* élément $p \in \mathcal{P}$ associé à π. Avec cette convention, on voit que chaque élément de $A \backslash \{0\}$ s'écrit uniquement comme

$$u \cdot \prod_{p \in \mathcal{P}} p^{v_p}, \quad u \in A^\times, \quad v_p \in \mathbf{N}.$$

Pour chaque $p \in \mathcal{P}$, on peut ainsi introduire la fonction $v_p : A\backslash\{0\} \to \mathbf{N}$ qui à chaque élément associe l'exposant de p dans sa décomposition. Dit autrement :

$$v_p(f) = \max\{n \in \mathbf{N} \,:\, p^n \mid f\}.$$

Comme A est factoriel, il est immédiat de voir que

$$v_p(ab) = v_p(a) + v_p(b).$$

On prolonge v_p à $K\backslash\{0\} \to \mathbf{Z}$ en écrivant

$$v_p\left(\frac{a}{b}\right) = v_p(a) - v_p(b).$$

Il est utils de décréter $v_p(0) = \infty$, où $\infty \geqslant n$ pour chaque $n \in \mathbf{Z}$.

Exemple 16. (1) Soit $A = \mathbf{Z}$. Alors $v_2(3) = 1$, $v_2(1/36) = -2$.

(2) Soit $A = \mathbf{C}[X]$ et $p = X - 1$. Alors $v_p(X^2 - 1) = 1$ et $v_p(1/(X^3 - 1)) = -1$.

Le lecteur n'aura aucun souci à établir le résultat suivant.

Lemme 17. *Soit $a \in K - \{0\}$. Alors $a \in A$ si et seulment si $v_p(a) \geqslant 0$ pour tour $p \in \mathcal{P}$.*

Une autre propriété fondamentale de v_p est :

Lemme 18. *$a, b \in K$. Alors :*

(1) On a

$$v_p(a + b) \geqslant \min(v_p(a), v_p(b)).$$

(2) De plus, si $v_p(a) < v_p(b)$, alors $v_p(a + b) = \min(v_p(a), v_p(b))$.

Démonstration. On traite d'abord le cas $a, b \in A$.

(1) On suppose $v_p(a) \leqslant v_p(b)$. Or, $p^{v_p(a)} \mid a + b$ et donc $v_p(a) \leqslant v_p(a + b)$.

(2) Si $v_p(a) < v_p(b)$, alors $p^{v_p(a)+1} \nmid a + b$ car autrement, $a \equiv a + b \equiv 0 \mod p^{v_p(a)+1}$.

Le cas $a, b \in K$ se traite en écrivant $a = a_0/d$ et $b = b_0/d$. □

Cours 2

(24 janvier 2021).

Définition 19. Soit ∞ un symbole tel que $\infty \geqslant n$ pour chaque $n \in \mathbf{Z}$. Une fonction $v : K \to \mathbf{Z} \cup \{\infty\}$ satisfaisant

V0 $v(x) = \infty$ si et seulement si $x = 0$.

V1 $v(ab) = v(a) + v(b)$.

V2 $v(a + b) \geqslant \min(v(a), v(b))$

est appelée une valuation.

On prolonge v_p à $K[X]$.

Définition 20 (La valuation de Gauss)**.** Pour chaque $f = a_n X^n + \cdots + a0 \in A[X]$, on définit :

$$v_p\left(a_n X^n + \cdots a_0\right) = \min\{v_p(a_i)\}.$$

Exemple 21. $v_2(\frac{3}{4}X^3 + 2X^2 - \frac{1}{8}X + 1) = -3$.

Voici une propriété évidente de v_p.

Lemme 22. *Soit $f \in K[X]$. Alors pour tout $\lambda \in K$, on a $v_p(\lambda f) = v_p(\lambda) + v_p(f)$.*

Démonstration. Il suffit de voir que $\min\{v(\lambda) + v(a_i)\} = v(\lambda) + \min\{v(a_i)\}$. □

Ensuite, sa propriété la plus importante.

Théorème 23 ("Lemme de Gauss")**.** *Pour chaque couple de polynômes $f, g \in K[X]$, l'égalité*

$$v_p(fg) = v_p(f) + v_p(g)$$

est vraie.

Démonstration. J'écris v au lieu de v_p. On suppose que $v(f) = v(g) = 0$ pour commencer. On écrit $f = \sum_{i=0}^{\infty} a_i X^i$ et $g = \sum_{j=0}^{\infty} b_j X^j$, où $a_i = 0$, respectivement $b_j = 0$, sauf pour un nombre fini de valeurs de i, respectivement j. Comme pour i très grand, le coefficient a_i est nul, on voit que $v(a_i) > 0$ pour i très grand. Soit ainsi

$$m = \max\{i \,:\, v(a_i) = 0\}.$$

Dit autrement,

$$f = a_0 + \cdots + \underbrace{a_m}_{v=0} X^m + \underbrace{a_{m+1}}_{v>0} X^{m+1} + \cdots$$

De même, soit $n = \max\{i \in \mathbf{N} \,:\, v(b_i) = 0\}$. On écrit $fg = \sum_i c_i X^i$ et on note que

$$\begin{aligned} v(c_r) &= v(a_0 b_r + \cdots a_r b_0) \\ &\geqslant \min\{v(a_0 b_r), \ldots, v(a_r b_0)\} \\ &\geqslant 0. \end{aligned}$$

Ensuite, si $m, n > 0$, alors

$$c_{m+n} = \underbrace{a_0 b_{m+n} + a_1 b_{m+n-1} + \cdots + a_{m-1} b_{n+1}}_{v>0} + \underbrace{a_m b_n}_{v=0} + \underbrace{a_{m+1} b_{n-1} + \cdots + a_{m+n} b_0}_{v>0}.$$

Proposition 18-(2) $\Rightarrow v(c_{m+n}) = 0$. Donc, $\min\{v(c_i)\} = 0$. On remarquera que les cas $m = n = 0$ et $m = 0$ ou $n = 0$ ont été laissés de côté, mais le lecteur peut facilement les prouver avec la méthode précédente.

Finalement, on abandonne l'hypothèse $v(f) = v(g) = 0$. On écrit $f = p^{v(f)} \tilde{f}$ et $g = p^{v(g)} \tilde{g}$ avec $v(\tilde{f}) = v(\tilde{g}) = 0$. Il suit que $v(\tilde{f}\tilde{g}) = 0$. Or, $v(fg) = v(p^{v(f)+v(g)} \cdot \tilde{f}\tilde{g})$, et comme $v(p^r) = r + v(h)$, le cas général en découle. □

Il est utile d'introduire maintenant :

Définition 24. On appellera un $f \in K[X]$ p-primitif si $v_p(f) = 0$. Si f est p-primitif pour tout $p \in \mathcal{P}$, on dira que f est primitf.

Quelques remarques à propos des polynômes primitifs :

Lemme 25. *1. Si $f \in K[X]$ est primitif, alors $f \in A[X]$.*

2. Si $f \in A[X]$ est irréductible (et sont degré est > 0), alors f est primitif.

Corollaire 26 (Permanence de l'irréductibilité)**.** *Soit $f \in A[X]$ un polynôme irréductible de degré strictement positif. Alors il est aussi irréductible en $K[X]$.*

Démonstration. Comme f est irréductible, il doit être primitif (Lemme 25). Soit

$$\mathbf{Fact} = \left\{ (g,h) \in K[X] \times K[X] \,:\, \begin{array}{c} 0 < \deg g < \deg f \\ 0 < \deg h < \deg f \\ f = gh \end{array} \right\}$$

Pour $(g,h) \in \mathbf{Fact}$, soit $P(g,h) \subset \mathcal{P}$ l'ensemble fini de premiers tels que $\min\{v_p(g), v_p(h)\} < 0$. Si $\mathbf{Fact} \neq \varnothing$, on va construire $(\tilde{g}, \tilde{h}) \in \mathbf{Fact}$ tel que $P(\tilde{g}, \tilde{h}) = \varnothing$. Ceci produit une contradiction, car $v_p(\tilde{g}) \geqslant 0$ et $v_p(\tilde{h}) \geqslant 0$ implique $\tilde{g} \in A[X]$ et $\tilde{h} \in A[X]$.

Soit $p \in P(g,h)$. Comme $v_p(f) = 0$, on déduit que $v_p(g) = -v_p(h)$. On écrit $g = p^{v_p(g)} g_1$ et $h = p^{v_p(h)} h_1$ où $v_p(g_1) = v_p(h_1) = 0$. Il suit que $f = g_1 h_1$ et $v_p(g_1) = v_p(h_1) = 0$. On obtient $(g_1, h_1) \in \mathbf{Fact}$ tel que $|P(g_1, h_1)| < |P(h,g)|$. Par récurrence, on obtient $(\tilde{g}, \tilde{h}) \in \mathbf{Fact}$ tel que $P(\tilde{g}, \tilde{h}) = \varnothing$. □

Théorème 27. *["Théorème d'hérédité"] A factoriel $\Rightarrow$ $A[X]$ factoriel.*

Démonstration. On montre que tout irréductible est premier et on utilise Lemme 14 pour assurer que **F2** de la Définition 5 est vraie. Soit $f \in A[X]$ irréductible. Il est en particulier primitif et le Théorème 26 prouve que f est irréductible aussi en $K[X]$. On suppose $f \mid gh$ en $A[X]$. Alors $f \mid gh$ en $K[X]$. Comme f est premier en $K[X]$, on peut supposer que $f\varphi = g$ pour un certain $\varphi \in K[X]$. Or, mais $v_p(\varphi) = v_p(g)$ pour tout $p \in \mathcal{P}$ et $v_p(g) \geqslant 0$, ce qui implique que $\varphi \in A[X]$.

Pour terminer, on doit montrer **F1**. Ceci sera fait lors du prochain cours. □

Cours 3

(31 janvier 2021).

On termine la preuve du fait que $A[X]$ est factoriel : il reste vérifier que **F1** est vraie. Soit $f \in A[X]$; on doit trouver une décomposition de f en facteurs irréductibles. Si $\deg f = 0$, la factorialité de A suffit. On suppose ainsi $\deg f > 0$. Soit $\mathcal{P}_0 = \{p \in \mathcal{P} : v_p(f) > 0\}$; il s'agit d'un ensemble fini. On écrit

$$f = \prod_{p \in \mathcal{P}_0} p^{v_p(f)} \quad \cdot \quad f_1;$$

f_1 est primitif. Il suffit ainsi de traiter le cas f primitif. Or, si f est primitif et n'est pas irréductible, il suit que f possède un facteur de degré strictement inférieur et un argument par récurrence sur $\deg f$ est suffisant. La preuve du Théorème 27 est terminée.

Exemple 28. (1) Les anneaux de polynômes $k[X_1, \ldots, X_n]$ sont toujours factoriels.

(2) Les anneaux de la forme $\mathbf{Z}[X_1, \ldots, X_n]$ sont toujours factoriels.

On termine par quelques critères d'irréductibilité.

Définition 29. Soit A factoriel et p un irréductible de A. Un polynôme $f = a_d X^d + \cdots a_0$ de degré $d > 0$ est dit p-Eisenstein si $p \nmid a_d$, $p \mid a_i$ pour tout $i \in \{0, \ldots, d-1\}$, et $p^2 \nmid a_0$.

Théorème 30. *Soit A factoriel et p un irréductible de A. Alors tout polynôme primitif et p-Eisenstein est irréductible dans $A[X]$.*

Démonstration. Soit $f = a_d X^d + \cdots a_0$ un polynôme primitif et p-Eisenstein de degré $d > 0$. Soit $f = gh$ une factorisation de f avec $g, h \in A[X]$. f primitif $\Rightarrow 0 < \deg g < \deg f$. On écrit $g = \sum_{i=0}^{r} b_i X^i$ et $h = \sum_{i}^{s} c_i X^i$. Comme $p \mid a_0 = b_0 c_0$, on peut supposer que $p \mid b_0$ mais $p \nmid c_0$. Comme $p \nmid a_d$, on sait que $p \nmid b_r$ et $p \nmid c_s$. Soit $m = \min\{i : p \nmid b_i\}$. Clairement, $0 < m \leqslant r$ et

$$g = \underbrace{b_r}_{\not\equiv 0 \mod p} X^r + \cdots + \underbrace{b_m}_{\not\equiv 0} X^m + \underbrace{b_{m-1}}_{\equiv 0} X^{m-1} + \cdots + \underbrace{b_0}_{\equiv 0 \mod p}.$$

Par conséquent

$$a_m = \underbrace{b_0 c_m + b_1 c_{m-1} + \cdots + b_{m-1} c_1}_{\equiv 0 \mod p} + \underbrace{b_m c_0}_{\not\equiv 0 \mod p},$$

on déduit que $a_m \not\equiv 0 \mod p$. Puisque $m \leqslant r < d$, on arrive à une contradiction. □

Exemple 31. Soit $n \geqslant 1$ un entier. Alors $f = X^n + Y^n - 1 \in \mathbf{C}[X, Y]$ est irréductible. En effet, $p = Y - 1 \in \mathbf{C}[Y]$ est irréductible et f est p-Eisenstein et primitif en tant qu'élément de $(\mathbf{C}[Y])[X]$. De façon analogue, on montre que pour tout $\alpha \in \mathbf{C}^*$, le polynôme $f_\alpha = X^n - Y^n - \alpha$ est aussi irréductible.

L'autre critère utile d'irréductibilité est le suivant.

Théorème 32. *Soit $\varphi : A \to B$ un morphisme d'anneaux et soit $\varphi : A[X] \to B[X]$ le morphisme induit. Si $f \in A[X]$ est unitaire et $\varphi(f)$ est irréductible, alors f est irréductible.*

Démonstration. Exercice. □

Exemple 33. Soient $n \geqslant 1$ un entier. Alors le polynôme $X^n + Y^n + Z^n - 1 \in \mathbf{C}[X, Y, Z]$ est irréductible. En effet, soit $\varphi : \mathbf{C}[X, Y] \to \mathbf{C}[Y]$ défini par $\varphi(X) = 0$ et $\varphi(Y) = Y$. Son extension à $(\mathbf{C}[X, Y])[Z]$ envoye f en $Y^n + Z^n - 1 \in \mathbf{C}[Y, Z]$, qui est irréductible.

3 Géométrie : Courbes planes

On fixe k un corps. On souhaite étudier les polynômes à deux variables de façon géométrique.

Définition 34. Soit $f = \sum_{i,j} a_{ij} X^i Y^j$ un polynôme à deux variables. Son degré total est $\max\{i + j \,:\, a_{ij} \neq 0\}$.

On parlera souvent de de degré au lieu de degré total.

Pour chaque $f \in k[X, Y]$, on définit $\mathcal{Z}(f)$ comme étant l'ensemble des points $(x, y) \in k$ tels que $f(x, y) = 0$.

Définition 35. Une courbe algébrique plane, ou simplement une courbe plane, est un sous-ensemble de k^2 de la forme $\mathcal{Z}(f)$, où f est un polynôme de degré au moins 1. Une courbe plane est irréductible si elle a la forme $\mathcal{Z}(f)$ avec f irréductible.

Voici quelques exemples.

Exemple 36. (1) Une droite est une courbe de la forme $\mathcal{Z}(f)$ où $\deg f = 1$. Une quadrique, ou conique, est une courbe $\mathcal{Z}(f)$ où $\deg f = 2$. Une cubique est une courbe $\mathcal{Z}(f)$ où $\deg f = 3$. (Après on a des quartiques, quintiques, sextiques, etc)

(2) Soit $f = a_d X^d + \cdots + a_0$ avec $a_j \in k$ et $a_d \neq 0$. (C'est à dire, $f \in k[X]$.) Alors, $\mathcal{Z}(f)$ est la réunion des droites $\{x\} \times k$ où x parcourt les racines de f.

(3) Soit $k = \mathbf{R}$ et $f = X^2 + Y^2 + 1$. Il suit que $\mathcal{Z}(f) = \varnothing$!

(4) Soit $k = \mathbf{F}_2$ et $f = X^2 - X + Y^2 - Y$. Alors $\mathcal{Z}(f) = k^2$!

Un problème vient immédiatement. Il est possible d'avoir des quadriques qui sont aussi des quartiques, ou sextiques, etc. En effet, il suffit de noter que si $k = \mathbf{R}$, alors $\mathcal{Z}(X^2 + Y^2) = \mathcal{Z}(X^4 + Y^4) = \mathcal{Z}(X^6 + Y^6) = \{(0, 0)\}$! De plus, il est également possible

d'avoir des droites qui sont des cubiques, par exemple, si $k = \mathbf{C}$, alors $\mathcal{Z}(X) = \mathcal{Z}(X^3)$! De façon générale, on a, pour chaque $f \in k[X, Y]$, l'égalité $\mathcal{Z}(f) = \mathcal{Z}(f^m)$.

Pour éviter des courbes avec trop de points ou trop peu de points, on travaille à partir de maintenant avec k *algébriquement clos*[4], par exemple, $k = \mathbf{C}$. Pour chaque corps, il est possible de construire un corps le contenant qui soit algébriquement clos, mais ceci ne fait pas l'objet de ce cours. On remarquera ici que les corps finis ne sont pas algébriquement clos, par contre. La première conséquence intéressante est la suivante :

Lemme 37. *Soit $f \in k[X, Y]$ de degré strictement positif. Alors $\mathcal{Z}(f)$ est infini.*

Démonstration. On écrit $f = a_d(X)Y^d + \cdots + a_0(X)$ avec $a_d \neq 0$. Si $d = 0$, alors $f \in k[Y]$ et $\mathcal{Z}(f)$ est une réunion de droites et le résultat est prouvé. Sinon, $d > 0$. Soit $\mathcal{N} = \{x \in k \,:\, a_d(x) \neq 0\}$; il s'agit d'un ensemble infini. Soit $x \in \mathcal{N}$. Il suit que $f(x, Y) \in k[Y]$ est de degré $d > 0$ et donc possède une racine. Par conséquent, la première projection $\mathcal{Z}(f) \to k$ contient $\mathcal{N}$ dans son image et $\mathcal{Z}(f)$ est infini. □

4. Un corps est algébriquement clos quand tout polynôme de degré strictement positif possède une racine.

Cours 4

(7 février 2022).

Le résultat suivant permet de déterminer – de façon grossière – les abscisses et ordonnées des zéros communs de deux courbes.

Théorème 38. *Soit A factoriel. Soient $f, g \in A[X]$ n'ayant aucun facteur premier commun. Alors il existe $d \in A\backslash\{0\}$ ainsi que $a, b \in A[X]$ tels que*

$$af + bg = d.$$

Démonstration. Soit $K = \mathrm{Fr}(A)$. On montre que f et g n'ont pas de facteur irréductible commun dans $K[X]$. Pour cela, soit $\varphi \in K[X]$ un facteur premier de f et g ; on observe que $\deg \varphi > 0$. En éliminant les dénominateurs, on peut supposer que $\varphi \in A[X]$. En divisant par un $c \in A\backslash\{0\}$, on peut supposer que φ est, de plus, primitif. On écrit $\varphi f_1 = f$ et $\varphi g_1 = g$, où $f_1, g_1 \in K[X]$. Soit $p \in A$ un premier. Le lemme de Gauss dit que $v_p(f_1) = v_p(f)$ et $v_p(g_1) = v_p(g) \Rightarrow f_1, g_1 \in A[X]$ et φ divise f et g. Absurde.

Le fait que f et g soient premiers entre eux dans $K[X]$ implique l'existence de $a_1, b_1 \in K[X]$ tels que

$$1 = a_1 f + b_1 g.$$

Éliminant les dénominateurs, on arrive au résultat souhaité. □

Corollaire 39. *Soient f et g des polynômes de $k[X, Y]$. On suppose que f et g n'ont pas de facteur irréductible commun. Alors il existe un $d_1 \in k[X]\backslash\{0\}$, un $d_1 \in k[Y]\backslash\{0\}$, ainsi que $a_1, b_1, a_2, b_2 \in k[X, Y]$ tels que*

$$a_1 f + b_1 g = d_1 \quad \textit{et} \quad a_2 f + b_2 g = d_2.$$

Démonstration. On applique le lemme dans le cas $A = k[X]$ et $A = k[Y]$. □

Voici une conséquence importante.

Théorème 40. *Soient f et g deux polynômes premiers entre eux de $k[X, Y]$. Alors $\mathcal{Z}(f) \cap \mathcal{Z}(g)$ est fini.*

Démonstration. Dans la notation du corollaire précédent, on voit que si $(x, y) \in \mathcal{Z}(f) \cap \mathcal{Z}(g)$, alors $d_1(x) = d_2(y) = 0$. Comme d_1 et d_2 n'ont que un nombre fini de zéros, le résultat découle.

□

Exemple 41. Soient $f = X^2 - Y^2$ et $g = XY + X - Y - 1$ deux coniques. On souhaite déterminer $\mathcal{Z}(f) \cap \mathcal{Z}(g)$. On regarde f et g comme des éléments de $\mathbf{Q}(X)[Y]$ et on trouve une relation de Bézout. Ensuite on élimine les dénominateurs pour arriver à

$$f \cdot (X^3 - X^2 - X + 1) + g \cdot (X^2 - 1)(Y - 1) = (X^2 - 1)(X^3 - X^2 - X + 1).$$

Or, $X^3 - X^2 - X + 1 = (X^2 - 1)(X - 1)$, et donc $\mathcal{Z}(f) \cap \mathcal{Z}(g)$ est contenu dans $\mathcal{Z}(f) \cap \mathcal{Z}(X - 1) \cap \mathcal{Z}(X + 1)$. Les points d'intersection sont les quatre sommets du carré de longueur 2 centré à l'origine.

Théorème 42 (Lemme de Study)**.** *k algébriquement clos. Soient $p, f \in k[X, Y]$ des polynômes de degré* total *strictement positif avec p irréductible. Si $\mathcal{Z}(p) \subset \mathcal{Z}(f)$, alors $p \mid f$.*

Démonstration. Si $p \nmid f$, alors $|\mathcal{Z}(p) \cap \mathcal{Z}(f)| < \infty$ (Thm 40). Mais $\mathcal{Z}(p) \subset \mathcal{Z}(p) \cap \mathcal{Z}(f)$ et donc $\#\mathcal{Z}(p) < \infty$. Comme k alg. clos, $\mathcal{Z}(p)$ ne peut pas être fini (Lem 37). □

Soit maintenant $\mathcal{C}$ l'ensemble des polynômes de degré strictement positif sans facteur carré de $k[X, Y]$. Sur $\mathcal{C}$, on introduit la relation d'équivalence $f \sim g \iff f$ est un multiple non-constant de g (on a déjà rencontré cette relation d'équivalence : il s'agit simplement des éléments associés). On note que $f \sim g$, alors $\mathcal{Z}(f) = \mathcal{Z}(g)$.

Théorème 43. *k algébriquement clos. La fonction*

$$\mathcal{Z} : \mathcal{C}/\!\sim \longrightarrow \text{ Courbes planes}$$

est une bijection.

Démonstration. Soenit f et g sans facteur carré tels que $\mathcal{Z}(f) = \mathcal{Z}(g)$.Soit $p \mid f$ irréd. Alors $\mathcal{Z}(p) \subset \mathcal{Z}(f)$ et $\mathcal{Z}(p) \subset \mathcal{Z}(g) \Rightarrow p$ apparaît dans la décomposition en facteurs premiers de f et de g. Il suit que f et g ont les mêmes facteurs premiers et comme ils n'not pas de carré, on déduit que f et g différent par un inversible.

Ensuite, si $C = \mathcal{Z}(f)$ pour un certain $f = \prod_{i=1}^{n} p_i^{n_i}$, avec p_i des éléments irréductibles et $n_i > 0$, on déduit que $\mathcal{Z}(f) = \mathcal{Z}(\tilde{f})$, où $\tilde{f} = \prod_i p_i$. □

En vu tu théorème précédent, il est intéressant de définir une inverse à la fonction $\mathcal{Z}$. Pour cela, on introduit, pour C une courbe plane, l'idéal

$$\mathcal{I}(C) = \{g \in k[X, Y] \,:\, g \text{ s'annule sur } C\}.$$

Or, si f est sans facteur carré et $\mathcal{Z}(f) = C$, alors $f \in \mathcal{I}(C)$. Soit $g \in \mathcal{I}(C)$, de sorte que $\mathcal{Z}(g) \supset \mathcal{Z}(f)$. Soit p un facteur premier de $f \Rightarrow \mathcal{Z}(p) \subset \mathcal{Z}(f) \subset \mathcal{Z}(g) \Rightarrow p \mid g$ par le Lemme de Study. Il suit facilement que $f \mid g$. Ceci dit que $\mathcal{I}(C)$ est engendré par un élément sans facteur carré. Comme n'importe quel autre générateur de $\mathcal{I}(C)$ devra être associé à f, on déduit :

Corollaire 44. *La fonction*

$$C \longmapsto \textit{générateur de } \mathcal{I}(C)$$

est la bijection inverse à $\mathcal{Z}$ du Théorème 43.

Ceci permet la définition suivante :

Définition 45. Soit C une courbe plane. Son degré est le degré d'un générateur de $\mathcal{I}(C)$.

On étudiera quelques exemples de courbes et quelques propriétés caractéristiques de telles objets. Dans la suite, k est un corps algébriquement clos. Soit f un poly sans facteur carré de deg > 0 et $C = \mathcal{Z}(f)$. On écrit ∂_X et ∂_Y pour désigner les dérivées partielles de d'un polynôme par rapport à X ou Y.

Définition 46. Un point $P \in C$ est un point singulier ou une singularité de C si

$$\partial_X f(P) = \partial_Y f(P) = 0.$$

L'ensemble des points singuliers est noté $\mathrm{Sing}(C)$. Une courbe sans singularités est dite non-singulière.

Cours 5

(14 février 2022).

Soit $f \in k[X,Y]$ sans facteur carré et de degré total strictement positif et soit $C = \mathcal{Z}(f)$ la courbe associée. On se rappèle que $P \in C$ est dit singulier si $\partial_X f(P) = \partial_Y f(P) = 0$. Voici un exemple.

Exemple 47. Soit $f = X^2 + Y^2 - 1$. Pour que f puisse en effet définir une courbe, il faut que f ne posit pas divisible par un carré. Or, si la caractéristique de k est 2, alors $f = f_0^2$, où $f_0 = X + Y + 1$, et notre polynôme f n'est pas dans les conditions correctes et doit être exclu. Ceci étant, $\partial_X f = 2X$ et $\partial_Y f = 2Y$ et $\partial_X f(P) = \partial_Y f(P) = 0$ seulement quand $P = (0,0)$. Or, mais $(0,0) \notin C$. Donc $\mathrm{Sing}(C) = \varnothing$.

Théorème 48. $\#\mathrm{Sing}(C) < \infty$. [5]

Démonstration. On fera la preuve dans le cas où k est de caractéristique nulle. Il est aussi supposé que k est algébriquement clos, comme dans cet étude. (Cela n'est pas entièrement nécéssaire !) On écrit $f = f_1 \cdots f_r$ avec f_i premier. Si $C_i = \mathcal{Z}(f_i)$, alors $C = C_1 \cup \cdots \cup C_r$. Si $P \in C_i - \bigcup_{j \neq i} C_j \Rightarrow$

$$\partial_X f(P) = f_1(P) \cdots f_{i-1}(P) \cdot \partial_X f_i(P) \cdot f_{i+1}(P) \cdots f_r(P)$$

et

$$\partial_X(f)(P) = \underbrace{c}_{\in k^*} \partial_X(f_i)(P).$$

Donc $\partial_X(f)(P) = 0 \Leftrightarrow \partial_X(f_i)(P) = 0$. De même, $\partial_Y f(P) = 0 \Leftrightarrow \partial_Y f_i(P) = 0$.

Comme $\#\mathcal{Z}(f_i) \cap \mathcal{Z}(f_j) < \infty$, il suffit de montrer que $\#\mathrm{Sing}(\mathcal{Z}(f)) < \infty$ dans le cas où f est irréd.

On sait que soit $\#\mathcal{Z}(f) \cap \mathcal{Z}(\partial_X f) < \infty$, soit $f \mid \partial_X f$ (voir Thm 40). Si $f \mid \partial_X f$, alors $\partial_X f = 0$, étant donné que si $f = \sum_{i=0}^{d} a_i(Y)X^i$, alors $\partial_X f = \sum_{i=0}^{d-1} a_{i+1}(Y)X^i$. Dans ce cas, comme f est irréductible et k est algébriquement clos, on doit avoir $f = aY + b$ avec $a \neq 0$. Il suit que $\partial_Y f = a$. □

Remarques 49. Dans le reste de la séance, on a travaillé sur un exercice : Montrer que $X^3 + Y^3 - aXY \in \mathbf{C}[X,Y]$ est irréductible pour chaque $a \in \mathbf{C}$.

5. Dans le théorème , il est supposé que k est algébriquement clos. Ceci n'est pas l'hypothèse la plus faible, mais elle est quand même nécéssaire. Voici un exemple remarquable d'une (une version plus fine est due au grand géomètre O. Zariski). Soit k le corps $\mathbf{F}_p(t)$, où t est une *variable*. On introduit $f = Y^p - X^p - t$. Pour prouver que f est irréductible il faudra simplement observer que $\varphi = X^p + t \in k[X]$ n'est pas divisible par un carré et appliquer le critère d'Eisenstein. Or, on affirme que φ est, en fait, irréductible. Soit $A = \mathbf{F}_p[t]$; clairement $\mathrm{Frac}(A) = k$. Comme $\varphi \in A[X]$ est unitaire, le Lemme de Gauss assure que f est irréductible dans $k[X]$ s'il est irréductible dans $A[X]$. Mais une application immédiate du critère d'Eisenstein montre que φ est un polynôme t-Eisenstein, et donc Eisenstein. Par contre, $\partial_X f = \partial_Y f = 0$.

Cours 6

(21 février 2021).

On souhaite maintenant lier le concept de singularité avec le concept géométrique de multiplicité. Soit ainsi $f \in k[X,Y]$ sans facteur carré et $C = \mathcal{Z}(f)$. On suppose que l'origine $O \in C$ est un point singulier de C. On peut ainsi écrire

$$f = \sum_{i+j>1} c_{ij} X^i Y^j$$

puisque $f(O) = c_{00}$, $\partial_X f(O) = c_{10}$ et $\partial_Y f(O) = c_{01}$. Soit

$$D_\theta = \mathcal{Z}(Y - \theta X), \qquad \theta \in k;$$

c'est la droite de pente θ. Soit

$$\mathrm{eval}_{D_\theta} : k[X,Y] \longrightarrow k[X], \qquad \begin{array}{ccc} X & \longmapsto & X, \\ Y & \longmapsto & \theta X. \end{array}$$

Donc

$$\mathrm{eval}_{D_\theta}(f) = \sum_{i+j>1} c_{ij} \theta^i X^{i+j} = X^2 (\cdots)$$

Dit autrement, la multiplicité de $\mathrm{eval}_{D_\theta}(f)$ en 0 est toujours > 1. De même, soit D_∞ la droite (de pente "infinie") $D_\infty = \mathcal{Z}(X)$ et soit

$$\mathrm{eval}_{D_\infty} : k[X,Y] \longrightarrow k[X], \qquad \begin{array}{ccc} X & \longmapsto & 0 \\ Y & \longmapsto & X. \end{array}$$

de sorte que

$$\mathrm{eval}_{D_\infty}(f) = \sum_{j>1} c_{0j} X^j = X^2 \cdot (\cdots).$$

et la multiplicité du zéro 0 est > 1.

On définit, pour $\theta \in k \cup \{\infty\}$:

$$\langle C, D_\theta \rangle_O = \begin{array}{c} \text{multiplicité de "0"} \\ \text{en tant que zéro de } \mathrm{eval}_{D_\theta}(f), \end{array}$$

et on constante que $\langle C, D_\theta \rangle_O > 1$ si O est singularité.

On suppose maintenant que $O \in C$ n'est pas singularité. On a

$$\mathrm{eval}_{D_\theta}(f) = (c_{10} + \theta c_{01}) \cdot X + \sum_{i+j>1} c_{ij} X^{i+j}.$$

Si $c_{10} \neq 0 \Rightarrow \langle C, D_0 \rangle_O = 1$. Si $c_{01} \neq 0$ mais $c_{10} = 0$, $\langle C, D_1 \rangle_O = 1$.

Ceci suggère la définition suivante :

Définition 50 (La multiplicité)**.**

$$\mathrm{mult}_O(C) = \min_{\theta \in k \cup \{\infty\}} \langle C, D_\theta \rangle_O.$$

La discussion précédente montre :

Proposition 51. $O \in \mathrm{Sing}(C) \Leftrightarrow \mathrm{mult}_O(C) > 1$.

On donne encore une autre interprétation de la multiplicité.

Proposition 52. *On écrit*

$$f = f_m + \cdots$$

avec

$$f_d = \sum_{i+j=d} c_{ij} X^i Y^j$$

et $f_m \neq 0$. *Alors* $\mathrm{mult}_O(f) = m$.

Démonstration. On a

$$f(X, \theta X) = X^m \left(f_m(1, \theta) + f_{m+1}(1, \theta) X + \cdots \right).$$

Il suit que

$$\langle C, D_\theta \rangle_O = m \iff f_m(1, \theta) \neq 0.$$

Soit $\mathcal{T} \subset k$ l'ensemble des zéros du poly. $f_m(1, X)$. Il s'agit d'un ensemble fini. (Si $\#\mathcal{T} = \infty$ alors $f_m(1, X) = 0$ et en regardant les coefficients, il faudra que $f_m = 0$.) Donc,

$$\langle C, D_\theta \rangle_O = m, \qquad \text{si } \theta \notin \mathcal{T}.$$

et

$$\langle C, D_\theta \rangle_O > m, \qquad \text{si } \theta \in \mathcal{T}.$$

De même,

$$f(0, X) = X^m \left(f_m(0, 1) + f_{m+1}(0, 1) X + \cdots \right).$$

Il suit que

$$\langle C, D_\infty \rangle_O = m, \qquad \text{si } c_{0m} \neq 0$$

et

$$\langle C, D_\infty \rangle_O > m, \qquad \text{si } c_{0m} = 0.$$

Par conséquent, m est la multiplicité. □

Exemple 53. On prendra C comme étant la lemniscate $C = \mathcal{Z}(f)$, où $f = (X^2 + Y^2)^2 - (X^2 - Y^2)$. Il suit que $\mathrm{mult}_O(C) = 2$.

Il est clair que le fait de traiter seulement le cas de l'origine est contraignant. Il devient aussi important de comprendre les polynômes homogènes. On doit ainsi prendre le temps de développer deux thèmes annexes.

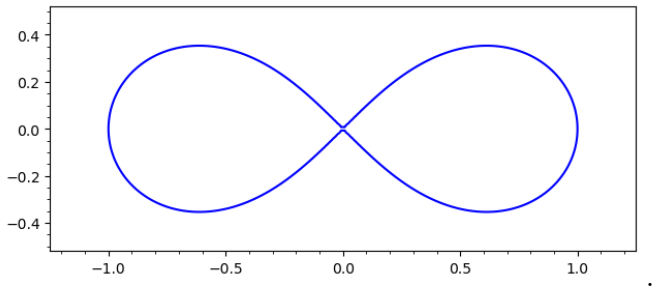

FIGURE 1 – La lemniscate

Les polynômes homogènes

On fixe un anneau A quelconque et un ensemble de variables $X_1, \ldots, X_n$. Soit $P = A[X_1, \ldots, X_n]$. Pour chaque $\boldsymbol{i} = (i_1, \ldots, i_n) \in \mathbf{N}^n$, on écrira

$$\boldsymbol{X}^{\boldsymbol{i}} := X_1^{i_1} \cdots X_n^{i_n}.$$

Par définition, $\deg \boldsymbol{X}^{\boldsymbol{i}}$ est $i_1 + \cdots + i_n$. On écrit aussi $|\boldsymbol{i}| = i_1 + \cdots + i_n$. On dira que $f \in P$ est homogène de degré d, s'il est de la forme

$$\sum_{d=|\boldsymbol{i}|} c_{\boldsymbol{i}} \boldsymbol{X}^{\boldsymbol{i}}.$$

Dit autrement, le A-sous-module de P engendré par les monômes de degré d est le A-sous-module des polynômes homogènes de degré d. L'utilité des homogènes a déjà apparu dans l'étude de la multiplicité. Ils feront encore un autre intervention lors de l'étude du resultant. Pour l'instant, on se contente de donner une caractérisation utile des polynômes homogènes.

Soit $f = \sum_{\boldsymbol{i}} c_{\boldsymbol{i}} \boldsymbol{X}^{\boldsymbol{i}}$. En écrivant $f_d = \sum_{|\boldsymbol{i}|=d} c_{\boldsymbol{i}} \boldsymbol{X}^{\boldsymbol{i}}$, on voit que

$$f_0 + \cdots + f_d,$$

où f_i est homogène de degré i. De plus, il est clair que cette écriture est *unique*.

Une façon intéressante de caractériser les polynômes homogènes est de regarder comment ils ses valeurs se comportent pour sur les "droites". En effet, si $f \in P$ est homogène de degré d alors $f(a\boldsymbol{X}) = a^d f(\boldsymbol{X})$ pour tout $a \in A$. La réciproque n'est pas toujours vraie si A est un anneau fini. Par contre, la technique suivante sert à contourner ce défaut. On considère P comme sous-anneau de $P[T]$. Soit $f \in P$, qui s'écrit comme

$$f = f_0 + \cdots + f_d, \quad f_i \text{ homogène de deg. } i.$$

On suppose que pour un certain m, on a $f(T\boldsymbol{X}) = T^m f(\boldsymbol{X})$. Donc,

$$\begin{aligned} f(T\boldsymbol{X}) &= f_0(\boldsymbol{X}) + T f_1(\boldsymbol{X}) + \cdots + T^d f_d(\boldsymbol{X}) \\ &= T^m f_0(\boldsymbol{X}) + T^m f_1(\boldsymbol{X}) + \cdots + T^m f_d(\boldsymbol{X}). \end{aligned}$$

Cette identité, étant valable sur $P[T]$ implique que $f_i(\boldsymbol{X}) = 0$ sauf quand $i = m$.

Proposition 54. *Un $f \in P$ est homogène de degré m si et seulement si $f(T\boldsymbol{X}) = T^m f(\boldsymbol{X})$ dans $P[T]$.*

Les affinités (ou transformations affines)

Définition 55. Une fonction $\alpha : k^2 \to k^2$ est une transformations affine, ou une affinité [6], si elle a la forme

$$\alpha(x, y) = (a_{11}x + a_{12}y + a_1, a_{21}x + a_{22}y + a_2),$$

ou, en notation vectorielle,

$$\alpha \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} a_1 \\ a_2 \end{pmatrix}.$$

Une affinité est inversible si la matrice en question est itou.

Proposition 56. *Soit α une transformation affine inversible et C une courbe plane. Alors $\alpha^{-1}(C)$ est aussi une courbe plane. Plus précisément, soit $\alpha^{\#} : k[X, Y] \to k[X, Y]$ le morphisme d'anneaux définit par*

$$\alpha^{\#}(X) = a_{11}X + a_{12}Y + a_1, \quad \alpha^{\#}(Y) = a_{21}X + a_{22}Y + a_2.$$

Alors $\alpha^{-1}(\mathcal{Z}(f)) = \mathcal{Z}(\alpha^{\#}(f))$.

Démonstration. On a

$$\begin{aligned}(x, y) \in \alpha^{-1}(C) &\Leftrightarrow f(\alpha(x, y)) = 0 \\ &\Leftrightarrow f(a_{11}x + a_{12}y + a_1, a_{21}x + a_{22}y + a_2) = 0 \\ &\Leftrightarrow \alpha^{\#} f(x, y) = 0.\end{aligned}$$

Ensuite, $\alpha^{\#}(f)$ est également un polynôme non-constant, car $\alpha^{\#}$ est un automorphisme de $k[X, Y]$. □

La multiplicité en général

On se donne une courbe plane $C = \mathcal{Z}(f)$, où f est un polynôme non-constant. On souhaite montrer :

6. En général, le terme affinité est employé pour désigner un type spécifique de transformation affine. Le lecteur fera attention à l'usage de ce terme dans d'autres contextes.

Proposition 57. *Soit $P \in C$. Soient α et β des affinités inversibles telles que $\alpha(O) = \beta(O) = P$. Alors*

$$\mathrm{mult}_O(\alpha^{-1}(C)) = \mathrm{mult}_O(\beta^{-1}(C)).$$

Démonstration. La preuve employe :

Lemme 58. *Soient $h \in k[X,Y]$ homogène de degré d et γ est une affinité inversible et linéaire. Alors $\gamma^{\#}(h)$ est homogène de degré d.*

Démonstration. Soit $\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ la matrice de γ. On note que

$$\begin{aligned}(\gamma^{\#}h)(TX,TY) &= h(a_{11}TX + a_{12}TY, a_{21}TX + a_{22}TY) \\ &= T^d h(a_{11}X + a_{12}Y\ ,\ a_{21}X + a_{22}Y) \\ &= T^d \gamma^{\#}(h).\end{aligned}$$

□

Soit $g = \alpha^{\#} f$: on sait que $\alpha^{-1}C = \mathcal{Z}(g)$. Si $m = \mathrm{mult}_O(\alpha^{-1}C)$, alors

$$g = \sum_{d \geqslant m} g_d$$

où g_d est homogène de degré d et $g_m \neq 0$. Soit $\gamma = \alpha^{-1}\beta : k^2 \to k^2$; il s'agit d'une affinité linéaire et inversible. On sait que $\gamma^{\#}g = \gamma^{\#}(g_m) + \gamma^{\#}(g_{m+1}) + \cdots$ où $\gamma^{\#}(g_d)$ est homogène de degré d et $\gamma^{\#}g_m \neq 0$. Ceci signifie que $m = \mathrm{mult}_O(\mathcal{Z}(\gamma^{\#}g))$. Or, $\mathcal{Z}(\gamma^{\#}g) = \gamma^{-1}(\alpha^{-1}C) = \beta^{-1}C$. □

On arrive en fin à la définition générale :

Définition 59. Soit $C = \mathcal{Z}(f)$ une courbe plane et $P \in C$. On définit $\mathrm{mult}_P(C)$ comme étant $\mathrm{mult}_O(\alpha^{-1}(C))$, où α est une affinité inversible telle que $\alpha(O) = P$.

Cours 7

(7 mars 2022).

4 Définition du résultant

On fixe un anneau A, deux entiers strictement positifs d et e, ainsi que deux polynômes $f = a_dX^d + \cdots + a_0$ et $g = b_eX^e + \cdots + b_0$ avec coefficients dans A. On ne suppose guère que a_d ou b_e est non-nul !

Définition 60. La matrice de Sylvester du couple f et g est la matrice $(d+e) \times (d+e)$ avec coefficients dans A :

$$\left(\begin{array}{cccccccccc} a_d & a_{d-1} & \cdots & a_0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & a_d & \cdots & \cdots & a_0 & 0 & \cdots & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & 0 & \cdots & 0 & a_d & \cdots & \cdots & a_0 \\ \hline b_e & b_{e-1} & \cdots & \cdots & \cdots & b_0 & 0 & \cdots & 0 \\ 0 & b_e & \cdots & \cdots & \cdots & \cdots & b_0 & \cdots & 0 \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & b_e & \cdots & b_0 \end{array}\right)$$

Le déterminant de $\mathrm{Syl}(f,g)$ est le résultant de f et g. Il sera noté par $\mathrm{res}(f,g)$. Dans le contexte où $A = k[Y_1, \ldots, Y_m]$, par exemple, on écrira $\mathrm{res}_X(f,g)$ pour dire qu'il s'agit de la variable X qu'il faudra "éliminer."

Remarques 61. Comme d et e sont fixés, $\mathrm{res}_X^{d,e}(f,g)$ serait une notation plus précise. Une conséquence de cette convention est : si $\deg f < d$ et $\deg g < e$, alors $\mathrm{res}_X^{d,e}(f,g) = 0$.

Exemple 62. 1/ Soient $f = XY - 1$ et, étant donnés $(a,b) \in k^2 - \{(0,0)\}$, $\ell = bY + aX$; l'ensemble algébrique $\mathcal{Z}(f)$ est une hyperbole et $\mathcal{Z}(\ell)$ une droite. Le résultant est un déterminant 2×2 :

$$R = \mathrm{res}_Y(f,\ell) = \begin{vmatrix} X & -1 \\ b & aX \end{vmatrix} = aX^2 + b$$

Il suit que $\deg_X(R) = 0$ si $a = 0$. Dit autrement, R est une contante si ℓ est l'axe des abscisses.

2/ On reprend l'exemple 41. On a $f = X^2 - Y^2$ et $g = XY + X - Y - 1$. Il suit que

$$\mathrm{res}_Y^{2,1}(f,g) = X^4 - 2X^3 + 2X - 1 = (X+1)(X-1)^3.$$

Les points de l'intersection sont sur les droites $\mathcal{Z}(X-1)$ et $\mathcal{Z}(X+1)$.

3/ Soient

$$f = X^2 - 2Y^2 + XY - 2X + 5Y$$
$$g = X^2 + XY + Y - X - 2.$$

Clairement

$$\begin{aligned}\mathrm{res}_Y^{2,1}(f,g) &= \begin{vmatrix} -2 & X+5 & X^2-2X \\ X+1 & X^2-X-2 & 0 \\ 0 & X+1 & X^2-X-2 \end{vmatrix} \\ &= -2X^4 - X^3 + 6X^2 + 7X + 2 \\ &= -(X-2)(2X+1)(X+1)^2.\end{aligned}$$

Le lecteur remarquera ici que le degré du resultant semble mystérieux et sans lien simple entre les degrés des polynômes qui le définissent. On commence doucement son étude :

Définition 63. Soit $f \in k[X,Y]$ non constant et sans facteur carré et C la courbe $\mathcal{Z}(f)$. Une droite $D = \mathcal{Z}(\ell)$, avec $\deg \ell = 1$, est dite une direction asymptotique de C si en écrivant

$$f = \underbrace{f_0}_{\text{hom. deg. } 0} + \cdots + \underbrace{f_d}_{\text{hom. deg } d}$$

avec $f_d \neq 0$, on a $\ell \mid f_d$.

Exercice 64. Soit $f \in \mathbf{Q}[X,Y]$ un polynôme de degré deux, qu'on écrira comme

$$a_{20}X^2 + a_{11}XY + a_{02}Y^2 + a_{10}X + a_{01}Y + a_{00}$$

et soit $\ell = rX + sY$ un polynôme de degré 1. Montrer que si $\deg(\mathrm{res}_Y(f,\ell)) < 2$, alors ℓ est direction asymptotique de f. (Ceci se fait de façon plus simple avec SAGE...)

Pour l'instant, on laisse cet étude en suspens et on passe aux propriétés basiques du résultant.

On désigne par $A[X]_{<n}$ le A-module libre des polynômes ayant degré au plus n. Clairement, $\{1, X, \ldots, X^{n-1}\}$ en est une base ordonnée. Soit

$$A[X]_{<e} \times A[X]_{<d} \xrightarrow{\mathcal{L}_{f,g}} A[X]_{<d+e}$$

$$(p,q) \longmapsto pf + qg.$$

Il est clair que

$$\mathcal{B} = \{(X^{e-1},0), \ldots, (X^0,0), (0,X^{d-1}), \ldots, (0,X^0)\}$$

est une base de $A[X]_{<e} \times A[X]_{<d}$. Il est aussi clair que

$$\mathcal{C} = \{X^{d+e-1}, \cdots, X, X^0\}$$

est une base ordonnée de $A[X]_{<d+e}$. Un calcul simple montre que la matrice

$$\mathrm{Mat}_{\mathcal{B},\mathcal{C}}(\mathcal{L}_{f,g}) : A^{d+e} \longrightarrow A^{d+e}$$

est

$$\mathrm{Syl}^{d,e}(f,g)^\top.$$

Dans la suite, on fera appel à quelques propriétés basiques des matrices carrés sur un anneau en général. L'étudiant peux toujours construire les preuves en remarquant que, si A est intègre avec corps de fractions K, alors $\mathrm{res}^{d,e}(f,g)$ est aussi le déterminant de l'application linéaire

$$\mathcal{L}_{f,g} : K[X]_{<e} \times K[X]_{<d} \longrightarrow K[X]_{<d+e}.$$

Proposition 65. *On suppose que A factoriel. Les conditions suivantes sont équivalentes :*

(1) Ou bien $a_d = b_e = 0$, ou bien il existe un couple

$$(p,q) \in A[X]_{<e} \times A[X]_{<d}$$

distinct de $(0,0)$ tel que $pf = qg$.

(2) Le résultant $\mathrm{res}(f,g)$ s'annule.

(3) Ou bien $a_d = b_e = 0$, ou bien f et g possèdent un facteur commun de degré strictement positif.

Démonstration. (1)⇒(2). Si $a_d = b_e = 0$, (2) est vraie. On suppose $a_d \neq 0$, par exemple. Soient p et q comme dans l'énoncé. Donc $\mathcal{L}_{f,g}(p,-q) = 0$ et le déterminant est nul par la règle de Cramer : en effet, si le déterminant n'était pas nul, le système linéaire sur $K := \mathrm{Fr}(A)$

$$\mathrm{Syl}^{d,e}(f,g)^\top \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_{d+e} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

ne peut que avoir $x_j = 0$ comme solution.

(2)⇒(3) On suppose que $a_d \neq 0$. Soit $K = \mathrm{Fr}(A)$. Le noyau de $\mathcal{L}_{f,g}$ est non-trivial. Donc, il existe un élément $(p,q) \in K[X]_{<e} \times K[X]_{<d}$, différent de $(0,0)$, tel que $\mathcal{L}_{f,g}(p,q) = 0$. Éliminant les dénominateurs, on peut trouver $(p,q) \in A[X]_{<e} \times A[X]_{<d}$ dans le noyau, c'est-à-dire, $pf = -qg$. On fait appel au fait que $A[X]$ est factoriel et écrit $f = c \cdot \pi_1^{\nu_1} \cdots \pi_r^{\nu_r}$, où $c \in A$ et chaque $\pi_i \in A[X]$ est irréductible de degré > 0. Or, si aucun π_i ne divise g,

il suit de $pf = -qg$ que $\pi_1^{\nu_1} \cdots \pi_r^{\nu_r} \mid q$, ce qui est impossible parce que $\deg \pi_1^{\nu_1} \cdots \pi_r^{\nu_r} = \deg f = d$, en contradiction avec $\deg q \leqslant d-1$.

(3)⇒(1) Si $\pi f_1 = f$ et $\pi g_1 = g$, alors $g_1 f = f_1 g$. Or, mais $\deg \pi \geqslant 1$ et donc $\deg f_1 < d$ ainsi que $\deg g_1 < e$.

□

Cours 8

(14/03/2022).

Le fait que la matrice de Sylvester est associée à $\mathcal{L}_{f,g}$ donne encore une conséquence intéressante, dans le cas où A est intègre.

Théorème 66. *On suppose A intègre et que* $\mathrm{res}(f,g) \neq 0$. *Alors, pour tout $h \in A[X]_{<d+e}$, l'élément* $\mathrm{res}(f,g) \cdot h$ *appartient à* $\mathrm{Im}(\mathcal{L}_{f,g})$.

Démonstration. Comme $\mathcal{L}_{f,g} : K[X]_{<e} \times K[X]_{<d} \to K[X]_{<d+e}$ est inversible, on peut écrire $h = \mathcal{L}_{f,g}(p,q)$, avec $(p,q) \in K[X]_{<e} \times K[X]_{<d}$. On sait que les coefficients de p et q sont, par Cramer, de la forme

$$\frac{\text{déterminant d'une matrice avec coefficients dans } A}{\mathrm{res}(f,g)}.$$

En effet, $h \in A[X]$. Donc,

$$(\mathrm{res}(f,g) \cdot p, \mathrm{res}(f,g) \cdot q) \in A[X]_{<e} \times A[X]_{<d}$$

et

$$\mathrm{res} \cdot h = \mathrm{res}(f,g)p \cdot f + \mathrm{res}(f,g)q \cdot g.$$

□

Corollaire 67. *On suppose que A est intègre. Alors il existe $(p,q) \in A[X]_{<e} \times A[X]_{<d}$ tel que*

$$pf + qg = \mathrm{res}(f,g).$$

(Le cas $\mathrm{res}(f,g) = 0$ *est également inclus.)*

Démonstration. Si $\mathrm{res}(f,g) \neq 0$, cela suit directement du Théorème précédent appliqué à $h = \mathrm{res}(p,q)$. Si $\mathrm{res}(f,g) = 0$, alors il exsite $(p,q) \in \mathrm{Ker}\,\mathcal{L}_{f,g} \backslash \{0\} \Rightarrow \mathrm{res}(f,g) = 0 = \mathcal{L}_{f,g}(p,q)$. □

Première application géométrique du resultant

On va recourir plusieurs fois à la propriété suivantes des resultants, laissée comme exercice.

Exercice 68. Soit $\varphi : A \to B$ un morphisme d'anneaux et soit $\varphi : A[X] \to B[X]$ le morphisme d'anneaux définit par $\sum a_i X^i \mapsto \sum \varphi(a_i) X^i$. Montrer que pour tout couple d'entiers strictement positifs d et e, et tout couple de polynômes f, g de $A[X]$, l'équation $\varphi(\mathrm{res}^{d,e}(f,g)) = \mathrm{res}^{d,e}(\varphi(f), \varphi(g))$ est vraie.

Soient f et g des éléments de $k[X,Y]$. En les considérant comme des polynômes en Y ayant coefficients en $k[X]$, on écrit

$$f = a_d(X)Y^d + \cdots + a_0(X) \quad \text{et} \quad g = b_e(X)Y^e + \cdots + b_0(X)$$

et on suppose que $d, e \geqslant 1$. Soit

$$R = \operatorname{res}_Y^{d,e}(f,g) \in k[X].$$

Maintenant, pour chaque $x \in k$, soit $\mathrm{ev}_x : k[X] \to k$ l'évaluation en x ; l'extension naturelle de ev_x à $k[X,Y]$ sera également désignée par ev_x (dit autrement, $\mathrm{ev}_x : h(X,Y) \mapsto h(x,Y)$). Par l'exercice 68, on a

$$\operatorname{res}^{d,e}(\mathrm{ev}_x(f), \mathrm{ev}_x(g)) = R(x).$$

Si $(x,y) \in \mathcal{Z}(f) \cap \mathcal{Z}(g)$, alors $\mathrm{ev}_x(f) \in k[Y]$ et $\mathrm{ev}_x(g) \in k[Y]$ auront y comme zéro commun, donc seront divisibles simultannéament par $Y - y$. Ceci entraine $R(x) = 0$.

On obtient :

Théorème 69. *Soient* $\mathrm{pr}_X : k^2 \to k$ *et* $\mathrm{pr}_Y : k^2 \to k$ *les projections sur la première et la deuxième coordonnée respectivement. Alors* $\mathrm{pr}_X(\mathcal{Z}(f) \cap \mathcal{Z}(g))$ *est contenu dans les zéros de* $\operatorname{res}_Y^{d,e}(f,g) \in k[X]$. *De même,* $\mathrm{pr}_Y(\mathcal{Z}(f) \cap \mathcal{Z}(g))$ *est contenu dans les racines de* $\operatorname{res}_X^{d,e}(f,g) \in k[Y]$. □

(Une autre façon d'arriver à ce résultat : On écrit $R(X) = p(X,Y)f(X,Y)+q(X,Y)g(X,Y)$ et on note que si $(x,y) \in \mathcal{Z}(f) \cap \mathcal{Z}(g)$, alors $R(x) = 0$.)

Ceci signifie que si on connait les zéros de R, alors on peut déterminer au moins les abscisses des zéros communs de f et g. Par contre, le nombre de zéros de R peut ne pas être si simple à comprendre.

Exemple 70. Soient $f = X^2 + y^2 - 2$ et $g = 2X^2 + Y^2 - 3$ et soient $C = \mathcal{Z}(f)$ (cercle de rayon 2) et $E = \mathcal{Z}(2x^2 + y^2 - 3)$ (une ellipse). On a

$$\operatorname{res}_Y^{2,2} = \begin{vmatrix} 1 & 0 & X^2-2 & 0 \\ 0 & 1 & 0 & X^2-2 \\ 1 & 0 & 2X^2-3 & 0 \\ 0 & 1 & 0 & 2X^2-3 \end{vmatrix} = X^4 - 2X^2 + 1 = (X^2-1)^2$$

et

$$\operatorname{res}_X^{2,2}(f,g) = Y^4 - 2Y^2 + 1 = (Y^2-1)^2.$$

On déduit que les points d'intersection appartiennent à $\{(1,1),(1,-1),(-1,1),(-1,-1)\}$. On vérifie qu'ils sont en fait tous les points d'intersection.

Le résultant de polynômes homogènes

Proposition 71. *Soit $A = k[U_1, \dots, U_m]$. Soient*

$$f = \underbrace{a_d}_{\text{hom. deg } 0} X^d + \cdots + \underbrace{a_0}_{\text{hom. deg } d} \quad \text{et} \quad g = \underbrace{b_e}_{\text{hom. deg } 0} X^e + \cdots + \underbrace{b_0}_{\text{hom. deg } e}$$

des polynômes de $A[X]$ tels que a_i soit homogène de degré $d-i$ et b_i soit homogène de degré $e-i$. Si $\operatorname{res}_X^{d,e}(f,g) \neq 0$, alors $\operatorname{res}_X^{d,e}(f,g)$ est homogène de degré de.

Démonstration. Soit $A' = A[T]$. On écrira $R = \operatorname{res}_X^{d,e}(f,g)$. Il suit que

$$R(T\boldsymbol{U}) = \begin{vmatrix} a_d & Ta_{d-1} & \cdots & T^d a_0 & 0 & 0 & \cdots & 0 \\ 0 & a_d & \cdots & \cdots & a_0 T^d & 0 & \cdots & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\ 0 & \cdots & 0 & \cdots & 0 & a_d & \cdots & T^d a_0 \\ b_e & Tb_{e-1} & \cdots & T^e b_0 & 0 & 0 & \cdots & 0 \\ 0 & b_e & \cdots & \cdots & T^e b_0 & 0 & \cdots & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\ 0 & \cdots & 0 & \cdots & 0 & b_e & \cdots & T^e b_0 \end{vmatrix}$$

On multiplie la première ligne par T, la deuxième par T^2, …, et la e-ème par T^e, ensuite la $(e+1)$-ème par T, la $(e+2)$-ème par T^2, etc, et la $(e+d)$-ème par T^d pour obtenir l'expression suivante

$$\begin{vmatrix} Ta_d & T^2 a_{d-1} & \cdots & T^{d+1} a_0 & 0 & 0 & \cdots & 0 \\ 0 & T^2 a_d & \cdots & \cdots & a_0 T^{d+2} & 0 & \cdots & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\ 0 & \cdots & 0 & \cdots & 0 & T^e a_d & \cdots & T^{d+e} a_0 \\ Tb_e & T^2 b_{e-1} & \cdots & T^{e+1} b_0 & 0 & 0 & \cdots & 0 \\ 0 & T^2 b_e & \cdots & \cdots & T^{e+2} b_0 & 0 & \cdots & \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \\ 0 & \cdots & 0 & \cdots & 0 & T^e b_e & \cdots & T^{e+d} b_0 \end{vmatrix} = \qquad (*)$$

$$= T^{1+\cdots+e+1+\cdots+d} R(T\boldsymbol{U}).$$

Attention, même is la graphie laisse entendre que $T^{d+1}a_0$ et $T^{e+1}b_0$ sont sur la même colonne, ceci et faux en général : T^{d+1} est sur la $(d+1)$-ème colonne tandis que $T^{e+1}b_e$ est sur la $(e+1)$-ème ! Comme le déterminant est multi-linéaire sur ses colonnes, en analysant le déterminant $(*)$, on voit que

$$T^{1+\cdots+e+1+\cdots+d} R(T\boldsymbol{U}) = T^{1+2+\cdots+d+e} R(\boldsymbol{U}).$$

Comme cette identité est vrai sur $A[T, \boldsymbol{U}]$, on déduit que

$$R(T\boldsymbol{U}) = \underbrace{T^{\frac{(d+e+1)(d+e)}{2} - \frac{(d+1)d}{2} - \frac{(e+1)e}{2}}}_{T^{de}} \cdot R(\boldsymbol{U}).$$

Ceci signifie que $R(\boldsymbol{U})$ est homogène. (Le lecteur devra refaire la preuve dans le cas $d = 2$ et $e = 3$ pour voir que malgré les complications graphiques, l'idée est très simple.) $\square$

Cours 9

(4/4/22).

Corollaire 72. *Soient $f, g \in k[X,Y]$ ayant respectivement degrés $d \geqslant 1$ et $e \geqslant 1$. Alors* $\deg \operatorname{res}_Y^{d,e}(f,g) \leqslant de$ *et si f et g n'ont pas de direction asymptotique commune, alors* $\deg \operatorname{res}_Y^{d,e}(f,g) = de$.

Démonstration. On écrit $f = f_d + \cdots + f_d$ et $g = f_0 + \cdots + g_e$ avec f_n et g_n homogènes de degré n. (On observe ici que $f_d \neq 0$ et $g_e \neq 0$.) On considère leur homogenisation :

$$\widetilde{f}(T,X,Y) = T^d f_0 + \cdots + T^0 f_d \qquad \text{et} \qquad \widetilde{g}(T,X,Y) = T^e g_0 + \cdots T^0 g_e;$$

$\widetilde{f}, \widetilde{g} \in k[T,X,Y]$ sont homogènes de degré d et e respectivement. On écrit maintenant

$$\widetilde{f} = a_d Y^d + \cdots + a_0 \qquad \text{et} \qquad \widetilde{g} = b_e Y^e + \cdots b_0;$$

où $a_i \in k[T,X]$ est homogène de degré $d-i$ et b_j est homogène de degré $e-j$. Avec cette notation, a_d et b_e sont des *constantes* qui ne peuvent pas être simultanément nuls ; en effet, $a_d = b_e = 0$ implique $X \mid f_d$ et $X \mid g_e$ (vérifier !), ce qui est exclu par l'hypothèse concernant les directions asymptotiques.

D'après Prp. 71,

$$\widetilde{R}(T,X) = \operatorname{res}_Y^{d,e}(\widetilde{f}, \widetilde{g})$$

est homogène de degré de. Ensuite, on note que

$$R(X) := \operatorname{res}_Y^{d,e}(f,g) = \widetilde{R}(1,X).$$

Puisque $\widetilde{R} \in k[T,X]$ est homogène de degré de, on peut l'écrire comme

$$\widetilde{R} = c_0 X^{de} + c_1 T X^{de-1} + \cdots + c_{de} T^{de},$$

et

$$R(X) = c_0 X^{de} + c_1 X^{de-1} + \cdots + c_{de}.$$

Alors $\deg R = de \Leftrightarrow c_0 \neq 0$. Or, mais $c_0 = \widetilde{R}(0,1)$. Donc $\deg R < de \Leftrightarrow \widetilde{R}(0,1) = 0$. Ceci implique que $\widetilde{f}(0,1,Y) = f_d(1,Y)$ et $\widetilde{g}(0,1,Y) = g_e(1,Y)$ ont une racine commune, c'est-à-dire, $f_d(1,\theta) = g_e(1,\theta) = 0 \Rightarrow \mathcal{Z}(f_d) \cap \mathcal{Z}(g_e) \supset \mathcal{Z}(\theta X - Y) \Rightarrow \mathcal{Z}(\theta X - Y)$ est une direction asymptotique. □

Remarques 73. Il est possible de montrer que si $\deg \operatorname{res}^{d,e}(f,g) < de$, alors f et g ont forcément une direction asymptotique commune.

Corollaire 74 (Le petit Théorème de Bézout)**.** *Soient f et g des éléments de $k[X,Y]$ ayant respectivement degrés $d > 0$ et $e > 0$. Soient C et D les courbes planes $\mathcal{Z}(f)$ et $\mathcal{Z}(g)$. Alors, si f et g sont premiers entre eux, il suit que $\#C \cap D \leqslant de$.*

Démonstration. L'idée est d'appliquer la Prp. 71 et le Thm 69. Il a deux obstacles. (P1) Il est possible que $\mathrm{res}_Y^{d,e}(f,g)$ soit nul et (P2) il est possible que deux points distincts de $C \cap D$ soient sur la même abscisse. La solution est de faire des "mouvements" avec C et D pour empêcher (P1) et (P2).

Pour chaque $\lambda \in k$, soit

$$t_\lambda : k^2 \longrightarrow k^2$$

l'affinité inversible $(x,y) \mapsto (x+\lambda y, y)$. Il s'agit d'une transvection : les droites horizontales restent inchangées, mais une translation est faite le long de chacune de ces droites. On écrit

$$C_\lambda = t_\lambda^{-1}(C) \quad \text{et} \quad D_\lambda = t_\lambda^{-1}(D).$$

On note que $C_\lambda = \mathcal{Z}(t_\lambda^\# f)$ et $D_\lambda = \mathcal{Z}(t_\lambda^\# g)$. Il suffit de montrer que $\#C_\lambda \cap D_\lambda \leqslant de$ pour un certain λ. Soit $C \cap D = \{P_i := (x_i, y_i) \,:\, i = 1, \ldots, r\}$. Si $i \neq j$ est un couple tel que $y_i \neq y_j$, on définit

$$\lambda_{ij} = \frac{x_i - x_j}{y_i - y_j}.$$

Il suit que si $\lambda \notin \{\lambda_{ij}\}$, alors

$$\mathrm{pr}_X : C_\lambda \cap D_\lambda \longrightarrow k$$

est *injective*. En effet, on a $C_\lambda \cap D_\lambda = \{(x_i - \lambda y_i, y_i)\}$, et si $x_i - \lambda y_i = x_j - \lambda y_j$, alors il faudra forcément que $i = j$. (Si $y_i = y_j$, alors $x_i = x_j$ et donc $i = j$. Si $y_i \neq y_j$, alors $\lambda(y_i - y_j) = x_i - x_j$, ce qui est impossible par construction de λ.) Ceci exclut P2.

On élimine maintenant le problème P1. Il s'agit d'une technique assez simple qui trouvera son utilité dans d'autres contextes, alors on l'écrira comme un exercice.

Exercice 75. Soit $h \in k[X_1, \ldots, X_n, Y]$ de degré $d > 0$. Si h_d désigne sa composante homogène de degré d, alors la coefficient de Y^d dans le polynôme

$$h(X_1 + \lambda_1 Y, \ldots, X_n + \lambda_n Y, Y)$$

est $h_d(\lambda_1, \ldots, \lambda_n, 1)$.

D'après ce résultat, on voit que si $f_d(\lambda, 1) \neq 0$, alors le coefficient de Y^d dans $t_\lambda^\# f$ est non-nul. Par conséquent, si $\mathrm{res}_Y^{d,e}(t_\lambda^\# f, t_\lambda^\# g) = 0$, on doit forcément conclure que $t_\lambda^\# f$ et $t_\lambda^\# g$ ne sont pas premiers entre eux (Proposition 65). Mais ceci est impossible car f et g le sont et $t_\lambda^\# : k[X,Y] \to k[X,Y]$ est un automorphisme. □

Le Petit Théorème de Bézout possède déjà plusieurs applications qui seront présentés comme exercices. Par contre, on souhaite comprendre le théorème de Bézout de façon plus générale. Il faut passer à la géométrie projective.

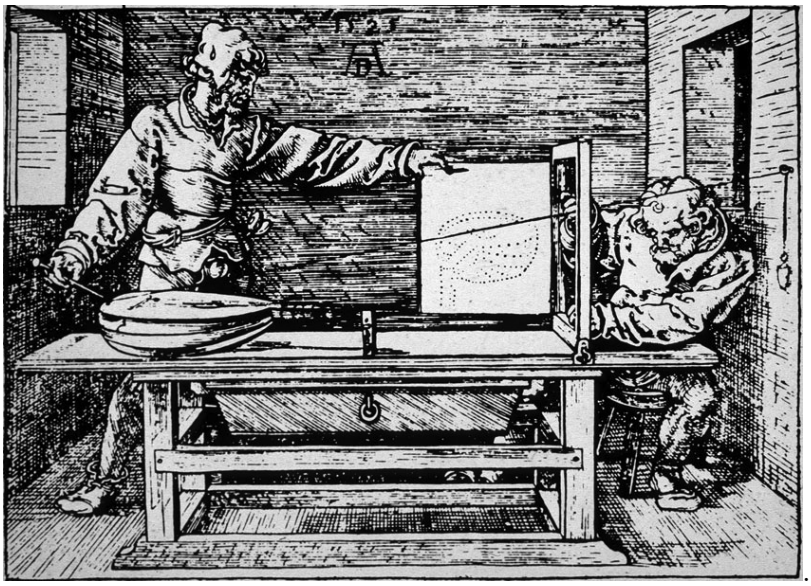

FIGURE 2 – A. Dürer, Dessin à la fin de Underweysung der Messung, Nürnberg 1525

Géométrie projective

On commence par l'exemple des droites $L = \mathcal{Z}(X)$ et $M = \mathcal{Z}(X-1)$. Clairement, $L \cap M = \varnothing$, mais en faisant le dessin, on se convaincra que L et M se rencontrent "à l'infini". D'où vient ce phénomène ? Soit $E = \mathbf{R}^3$ et plaçons L et M dans le plan $\Pi = \{1\} \times \mathbf{R}^2$. Soit S^2 la sphère de rayon 1 et centre à l'origine. Relions chaque point de Π à S^2 par la projection $\pi : p \mapsto \dfrac{p}{\|p\|}$. Les images de $\pi(L)$ et $\pi(M)$ deviennent des (morceaux de) méridiens. On pourrait alors dire que les "droites" $\pi(L)$ et $\pi(M)$ se rencontrent aux pôles. Mais, si au lieu de travailler avec S^2, on se concentre à l'espace des *droites vectorielles de* $\mathbf{R}^3$, on obtiendra que "M et L se rencontrent à l'axe des y".

Définition 76. L'ensemble des droites vectorielles de k^3 est l'espace projectif $\mathbf{P}^2$.

Il est traditionnel, étant donné in point $(t, x, y) \in k^3 \backslash \{0\}$, d'écrire

$$\boxed{(t : x : y) = \text{droite vectorielle de } k^3 \text{ passant par } (t, x, y).}$$

Il suit, par exemple, que $(t : x : y) = (\lambda t : \lambda x : \lambda y)$ pour $\lambda \in k^*$. Le point $(0 : 0 : 0)$ n'existe pas. Soit

$$\Pi \longrightarrow \mathbf{P}^2, \quad (1, x, y) \longmapsto (1 : x : y);$$

il s'agit clairement d'une fonction injective et on obtient une "copie" de k^2, en identifiant $k^2 = \Pi$, dans $\mathbf{P}^2$. Son image sera désignée par $(k^2)_0$. Avec cette idée, on commence à penser aux points du plan comme étant des droites. Voir la Figure 2.

Ceux qui souhaitent comprendre comment les peintres et architectes d'autrefois ont contribué aux mathématiques, peuvent lire le chapitre III de l'excellent livre de Pierre Thuiller [5].

Exercice 77. Montrer que $\mathbf{P}^2 \smallsetminus (k^2)_0 = \{D \in \mathbf{P}^2 \ : \ D \text{ parallèle à } \Pi\}$. L'ensemble

$$\Omega := \mathbf{P}^2 \smallsetminus (k^2)_0$$

est *la droite à l'infini*. Ses points sont les points *à l'infini*. Il est aussi commode de parler des points de $(k^2)_0$ comme étant des points *à distance finie*.

De même, les fonctions

$$\begin{aligned} k^2 &\longrightarrow \mathbf{P}^2 \qquad (t, y) \mapsto (t : 1 : y) \\ k^2 &\longrightarrow \mathbf{P}^2 \qquad (t, x) \mapsto (t : x : 1) \end{aligned}$$

sont des injections. Leurs images respectives seront notées par $(k^2)_1$ et $(k^2)_2$. Clairmenet,

$$\mathbf{P}^2 = (k^2)_0 \cup (k^2)_1 \cup (k^2)_2.$$

Exercice 78. Décrire les complémentaires $\mathbf{P}^2 \smallsetminus (k^2)_1$ et $\mathbf{P}^2 \smallsetminus (k^2)_2$ de façon géométrique comme à l'exercice 77.

Exercice 79. Soit $k = \mathbf{R}$ et munissons $\mathbf{P}^2$ de la topologie quotient suivante. Soit $\psi : S^2 \to \mathbf{P}^2$ la fonction qui à chaque $p \in S^2$ associe la droite $\mathbf{R}p$. On dira que $U \subset \mathbf{P}^2$ est ouvert si $\psi^{-1}(U)$ est ouvert de S^2.

1) Montrer que $\mathbf{P}^2$ est compact.
2) Montrer que la bijection naturelle $\mathbf{R}^2 \to (\mathbf{R}^2)_0$ est un homéomorphisme.
3) Montrer que Ω est homéomorphe au cercle unitaire S^1.
4) Montrer que $(\mathbf{R}^2)_0$ est dense dans $\mathbf{P}^2$.

La compacité de $\mathbf{P}^2$ est l'un de ses points remarquables. Il est possible, à l'aide de ψ, de donner à $\mathbf{P}^2$ la structure d'une variété différentielle de classe C^∞ et le fait que $\mathbf{P}^2$ soit plus naturellement construit de façon abstraite *et non dans un espace euclidien* $\mathbf{R}^N$ est une des bonnes raisons pour l'introduction des variétés différentielles abstraites. Voir le dernier chapitre de [6]. Il est néanmoins possible de voir $\mathbf{P}^2$ comme sous-variété de S^4, cf. l'exercice 16 de la page 29 dans [7].

La clôture projective

On souhaite maintenant passer de k^2 à $\mathbf{P}^2$ à l'aide de $(k^2)_0 = \Pi$. Soit $C = \mathcal{Z}(f)$, qu'on regarde comme un sous-ensemble de $k^2 = (k^2)_0$. En prenant toutes les droites qui relient l'origine à un point de C, on obtient un "cône" $\widehat{C} \subset k^3$: C'est un sous-ensemble contenant, pour chaque $p \in \widehat{C}$, la droite $k \cdot p$. (Il ne s'agit pas vraiment d'un cône, sauf dans le cas où C est un cercle.) Ensuite, on observe que chaque polynôme homogène $F \in k[T, X, Y] \smallsetminus k$ donne lieu à un "cône" $\{(t, x, y) \;\; F(t, x, y) = 0\}$.

On se concentre ainsi sur les polynômes homogènes. Or, si F est homogène, alors F s'annule sur $\Delta \in \mathbf{P}^2 \Leftrightarrow F$ s'annule sur un point de Δ distinct de l'origine. On dira ainsi que $F(\Delta) = 0$. Par contre, si $F(t, x, y) \neq 0$, alors il n'a aucune valeur numérique qui puisse être associée à $F(t : x : y)$!

Définition 80. Si $F \in k[T, X, Y]$ est homogène et non-constant, on écrira $\mathcal{Z}(F) = \{\Delta \in \mathbf{P}^2 \; : \; F(\Delta) = 0\}$. Une courbe plane *projective* est un sous-ensemble C de $\mathbf{P}^2$ de la forme $\mathcal{Z}(F)$, avec F non-constant. De plus, on dira que C est irréductible s'il est possible de prendre F irréductible. Une *droite projective* est une courbe projective $\mathcal{Z}(\ell)$ avec ℓ homogène de degré 1.

Remarques 81. Avec cette définition, Ω est la droite $\mathcal{Z}(T)$.

Définition 82. Soit $C = \mathcal{Z}(f)$ une courbe plane. On définit la *clôture projective* de C comme étant $\overline{C} = \overline{\mathcal{Z}}(f^{\sim})$. C'est la courbe projective associée à C.

Exercice 83. Soient $g = X^2 + Y^2 - 1$ et $\Gamma = \mathcal{Z}(g) \subset \mathbf{R}^2$. Quel est l'équation de $\overline{\Gamma} \cap (\mathbf{R}^2)_1$, et comment appeler cette courbe plane ? Interpretez ceci à l'aide du cône $\widehat{\Gamma} = \{(t, x, y) \in k^3 \; : \; \widetilde{g}(t, x, y) = 0\}$. (Voir la Figure 3)

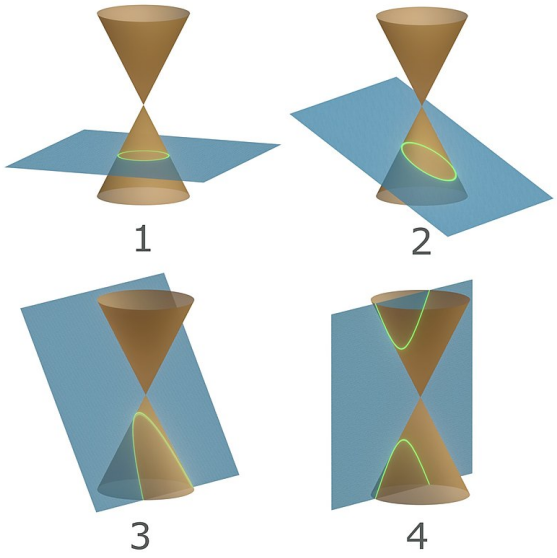

FIGURE 3 – Sections coniques

Cours 11 et 12

(20/04/22 et 24/04/22).

On souhaite maintenant démontrer le théorème de Bézout en toute généralité. L'idée est similaire à celle de la version faible ; on doit supposer que les points d'intersection sont dans une configuration agréable et appliquer ce qu'on sait sur le résultant.

Soit k algébriquement clos. Soit $F \in k[T, X, Y]$ homogène de degré $d > 0$, et soit $G \in k[T, X, Y]$ homogène de degré e. On suppose que F et G sont premiers entre eux et on désigne par C et D les courbes planes associées. Le fait que F et G sont premiers entre eux assure que l'ensemble $C \cap D$ est *fini*.

Soit

$$R = \mathrm{res}_Y^{d,e}(F, G) \in k[T, X].$$

En écrivant

$$F = \underbrace{F_0(T, X)}_{\text{hom. deg } 0} Y^d + \cdots + \underbrace{F_d(T, X)}_{\text{hom. deg } d} Y^0$$

et

$$G = \underbrace{G_0(T, X)}_{\text{hom. deg } 0} Y^e + \cdots + \underbrace{G_e(T, X)}_{\text{hom. deg } e} Y^0,$$

la propos. 71 assure que R est homogène de degré de.

Hypothèse 84. $Z = (0 : 0 : 1) \notin C \cap D$.

Avec cette hypothèse, on observe que *aucun* point de $C \cap D$ a la forme $(0:0:y)$; en effet, $(0:0:y) = Z$. Sans perte de généralité, on peut supposer $Z \notin C$. De plus, on voit que cette hypothèse n'est pas déraisonnable : l'ensemble $C \cap D$ est fini, on peut très bien fixer un point de la droite à l'infini Ω qui ne soit pas dans $C \cap D$.

On passe maintenant à une deuxième hypothèse. Soit $\mathbf{P}^1$ l'ensemble des droites vectorielles de k^2.

Hypothèse 85. La fonction

$$\pi : C \cap D \longrightarrow \mathbf{P}^1, \qquad (t:x:y) \longmapsto (t:x)$$

est injective.

Comment comprendre cette hypothèse géométriquement ? [7] Soit $\Omega' = \mathcal{Z}(Y)$. Clairement, $Z \notin \Omega'$. Pour chaque $P \in \mathbf{P}^2 \smallsetminus \{Z\}$, il existe une unique droite projective $\overline{ZP}$ contenant Z et Q. Comme on est dans $\mathbf{P}^2$, l'ensemble $\overline{ZP} \cap \Omega'$ et un singleton ! En fait, si $P = (t:x:y)$, il n'est pas difficile de voir que $\overline{ZP} \cap \Omega' = \{(t:x:0)\}$. L'hypothèse 85 en fait dit quelque chose de géométrique : pour $P, Q \in C \cap D$, les trois points Z, P, Q ne sont jamais colinéaires.

Dans un souci d'économie, on dira que les courbes satisfaisant les Hypothèses 84 et 85 sont en *bonne position*. On va maintenant démontrer le Théorème de Bézout dans ce contexte.

Comme $F(0,0,1) = F_0 \in k$, on voit que $F_0 \neq 0$. Donc, la Proposition 71 assure que $R \neq 0$, car on a supposé F et G premiers entre eux.

Comme k est alg. clos,

$$R = \lambda \prod_{j=1}^{m} \ell^{\mu_j},$$

où

— $\lambda \in k^*$,
— $\ell_j \in k[T, X]$ est homogène de degré 1,
— Si $i \neq j$, alors ℓ_i et ℓ_j ne sont pas proportionels.
— $\mu_j > 0$.

Soit $Q_j \in \mathbf{P}^1$ l'unique zéro de ℓ_j.

Lemme 86. *$\{Q_1, \ldots, Q_m\} = \mathrm{Im}(\pi)$ et $\pi : C \cap D \to \mathcal{Z}(R)$ est une bijection.*

Démonstration. Soit $Q_j = (t_j : x_j)$. Or, $R(t_j, x_j) = 0 \Rightarrow$

$$F(t_j, x_j, Y) \in k[Y] \quad \text{et} \quad G(t_j, x_j, Y) \in k[Y]$$

7. Les arguments qui suivent ont besoin d'une compréhension plus solide de la géométrie projective ; ceci a été travaillé dans une feuille d'exercices.

ont *au moins un* zéro commun, disons y_j. Donc $(t_j : x_j : y_j) \in C \cap D$. De plus, soit $P = (t : x : y) \in C \cap D$. (Rappel : $(t, x) \neq (0, 0)$.) Comme

$$F(t, x, Y) \in k[Y] \quad \text{et} \quad G(t, x, Y) \in k[Y]$$

s'annulent sur y, on déduit que $R(t, x) = 0$. □

Définition 87. Si C et D sont en bonne position, on définit la *multiplicité d'intersection* au point $P \in C \cap D$ comme étant la μ_j si $\pi(P) = Q_j$. Notation : $\langle C, D \rangle_P$.

Avec cette définition, le fait que $\deg R = de$ se traduit immédiatement dans :

Théorème 88 (Bézout)**.**

$$\sum_{P \in C \cap D} \langle C, D \rangle_P = de.$$

Il faut maintenant supprimer les hypothèses pour définir la multiplicité d'intersection. Comme pour le cas de la multiplicité d'intersection entre une courbe et une droite, on fera appel aux "transformations".

Définition 89. Soit $\alpha \in \mathrm{GL}_3(k)$. La transformation projective induite par α est la fonction $[\alpha] : \mathbf{P}^2 \to \mathbf{P}^2$ définie par $\Delta \mapsto \alpha(\Delta)$ pour chaque $\Delta \in \mathbf{P}^2$. Une fonction $\mathbf{P}^2 \to \mathbf{P}^2$ est une transformation projective si elle est de la forme $[\alpha]$ pour un certain $\alpha \in \mathrm{GL}_3(k)$. Le groupe des transformations projectives sera désigné par $\mathcal{P}$ dans la suite. [8]

Exercice 90 (L'analogue de la Prp. 56)**.** Soit $\alpha \in \mathrm{GL}_3(k)$. Montrer que $[\alpha]^{-1}(\mathcal{Z}(H)) = \mathcal{Z}(\alpha^{\#} H)$, où $\alpha^{\#} : k[T, X, Y] \to k[T, X, Y]$ est le morphisme défini par

$$\begin{pmatrix} \alpha^{\#} T \\ \alpha^{\#} X \\ \alpha^{\#} Y \end{pmatrix} = \alpha \begin{pmatrix} T \\ X \\ Y \end{pmatrix}.$$

Soient maintenant $\Delta = \mathcal{Z}(\Phi)$ et $\Gamma = \mathcal{Z}(\Psi)$ des courbes projectives telles que Φ et Ψ sont premiers entre eux. Pour chaque $P \in \Gamma \cap \Delta$, comment définir la multiplicité d'intersection $\langle \Gamma, \Delta \rangle_P$? L'idée est simple : on trouve une transformation projective τ telle que $[\tau]^{-1}(\Gamma)$ et $[\tau]^{-1}(\Gamma)$ soient en bonne position et pour chaque $P \in \Gamma \cap \Delta$, on décrète

$$\langle \Gamma, \Delta \rangle_P := \langle [\tau]^{-1}(\Gamma), [\tau]^{-1}(\Delta) \rangle_{[\tau]^{-1}(P)}.$$

Par contre, il est envisageable que le choix de τ fasse la définition contradictoire. On doit montrer le résultat suivant, qui est tiré de [8].

8. On démontre facilement que $\mathcal{P} \simeq \mathrm{GL}_3(k)/Z$, où Z sont les matrices scalaires. Le groupe $\mathrm{GL}_3(k)/Z$, noté par $\mathrm{PGL}_3(k)$, est le groupe linéaire général projectif.

Théorème 91. *On suppose que C et D sont en bonne position. Soit $\alpha \in \mathrm{GL}_3(k)$ telle que $[\alpha]^{-1}(C)$ et $[\alpha]^{-1}(D)$ sont aussi en bonne position. Alors pour chaque $P \in \mathbf{P}^2$, l'on a*

$$\langle C, D\rangle_P = \langle [\alpha]^{-1}(C), [\alpha]^{-1}(D)\rangle_{[\alpha]^{-1}(P)}$$

Démonstration. On introduit neuf variables $U, U', U'', V, \ldots, W''$. Soit

$$\mathcal{O} = k[U, U', U'', V, \ldots, W'']$$

et $K = \mathrm{Fr}(\mathcal{O})$. On considère $\mathbf{P}^2(K)$ l'ensemble des droites vectorielles de K^3 et on considère $\mathbf{P}^2$ comme étant contenu dans $\mathbf{P}^2(K)$. On fera quelques fois appel aux morphismes de évaluation

$$\mathrm{eval}_I : \mathcal{O} \longrightarrow k$$

définie par

$$\begin{pmatrix} U & U' & U'' \\ V & V' & V'' \\ W & W' & W'' \end{pmatrix} \longmapsto \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

et

$$\mathrm{eval}_\alpha : \mathcal{O} \longrightarrow k$$

définie par

$$\begin{pmatrix} U & U' & U'' \\ V & V' & V'' \\ W & W' & W'' \end{pmatrix} \longmapsto \alpha.$$

Soient C_K et D_K les courbes dans $\mathbf{P}^2(K)$ définies par F et G. Il n'est pas difficile de voir que l'inclusion $C_K \cap D_K \supset C \cap D$ est une égalité.

Maintenant on considère la transfo. proj. générique

$$A : \mathbf{P}^2(K) \longrightarrow \mathbf{P}^2(K)$$

$$\Delta \longmapsto \begin{pmatrix} U & U' & U'' \\ V & V' & V'' \\ W & W' & W'' \end{pmatrix}(\Delta)$$

Ensuite

$$A^{-1}(C_K) = \mathcal{Z}_K(A^{\#}F) \quad \text{et} \quad A^{-1}(D_K) = \mathcal{Z}_K(A^{\#}G).$$

On remarque que $A^{\#}F$ et $A^{\#}G$ sont des éléments de $\mathcal{O}[T, X, Y]$ et que $\mathrm{eval}_I(A^{\#}F) = F$ tandis que $\mathrm{eval}_\alpha(A^{\#}F) = \alpha^{\#}F$.

Les courbes $A^{-1}(C_K)$ et $A^{-1}(D_K)$ sont en bonne position. Par exemple, si $Z \in A^{-1}(C_K) \cap A^{-1}(D_K)$, on déduit que

$$F(A(0, 0, 1)) = G(A(0, 0, 1)) = 0.$$

Or, utilisant la spécialisation $\mathrm{eval}_I : \mathcal{O} \to k$, on obtiendra $F(0,0,1) = G(0,0,1) = 0$, ce qui est exclu. De plus,

$$A^{-1}(C_K) \cap A^{-1}(D_K) = A^{-1}(C \cap D).$$

On observe que si

$$\widetilde{A} = \begin{pmatrix} \widetilde{U} & \widetilde{U}' & \widetilde{U}'' \\ \widetilde{V} & \widetilde{V}' & \widetilde{V}'' \\ \widetilde{W} & \widetilde{W}' & \widetilde{W}'' \end{pmatrix}$$

est la matrice complémentaire [9] de A, alors

$$A^{-1}(C_K) \cap A^{-1}(D_K) = \widetilde{A}(C \cap D); \qquad (\dagger)$$

en effet, A^{-1} et $\widetilde{A}$ ont le même effet sur les droites de K^3. À ce moment, on note que $\widetilde{A} \in \mathrm{Mat}_3(\mathcal{O})$.

Soit $\overline{K}$ une extension algébriquement close de K. Il suit que

$$\begin{aligned} S &:= \underbrace{\mathrm{res}_Y^{d,e}(A^{\#}F, A^{\#}G)}_{\in \mathcal{O}[T,X]} \\ &= \Lambda \cdot \prod_{j=1}^{n} L_j^{\nu_j}, \end{aligned}$$

où

— $\Lambda \in \overline{K}^*$,
— $L_j \in \overline{K}[T,X]$ est homogène de degré 1,
— Si $i \neq j$, alors L_i et L_j ne sont pas proportionels.
— $\nu_j > 0$.

Le fait que les polynômes L_j soient dans $\overline{K}[T,X]$ peut être raffiné.

Comme avant, si $\pi : \mathbf{P}^2(\overline{K}) \smallsetminus \{Z\} \to \mathbf{P}^1(\overline{K})$ est la projection de centre Z, alors

$$\begin{aligned} \pi(A^{-1}(C_K \cap D_K)) &= \text{zéros de } S \text{ dans } \mathbf{P}^1(\overline{K}) \\ &= \text{zéros de } L_1, \ldots, L_n. \end{aligned}$$

Par contre, (†) dit que

$$\pi(A^{-1}(C_K \cap D_K)) = \pi(\widetilde{A}(C \cap D)).$$

Ceci implique que si

$$C \cap D = \{(t_j : x_j : y_j)\}_{j=1}^{m}$$

9. Je ne suis jamais certain de la terminologie Francophone pour cela. La matrice complémentaire est telle que $A\widetilde{A} = \det(A)\mathrm{I}$.

alors $\widetilde{A}(C \cap D)$ est s

$$\left\{(\widetilde{U}t_j + \widetilde{U}'x_j + \widetilde{U}''y_j \ : \ \widetilde{V}t_j + \widetilde{V}'x_j + \widetilde{V}''y_j \ : \ \widetilde{W}t_j + \widetilde{W}'x_j + \widetilde{W}''y_j)\right\}_{j=1}^{m}.$$

Donc

$$\begin{aligned} \begin{matrix}\text{zéros de} \\ L_1, \ldots, L_n\end{matrix} &= \pi(\widetilde{A}(C \cap D)) \\ &= \left\{(\widetilde{U}t_j + \widetilde{U}'x_j + \widetilde{U}''y_j \ : \ \widetilde{V}t_j + \widetilde{V}'x_j + \widetilde{V}''y_j)\right\}_{j=1}^{m} \end{aligned}$$

Or, ce dernier ensemble possède m éléments : si

$$(\widetilde{U}t_i + \widetilde{U}'x_i + \widetilde{U}''y_i \ : \ \widetilde{V}t_i + \widetilde{V}'x_i + \widetilde{V}''y_i) = (\widetilde{U}t_j + \widetilde{U}'x_j + \widetilde{U}''y_j \ : \ \widetilde{V}t_j + \widetilde{V}'x_j + \widetilde{V}''y_j)$$

alors par spécialisation

$$(t_i : x_i) = (t_j : x_j) \quad \Rightarrow \quad i = j.$$

On peut ainsi supposer que L_j s'annule sur le point

$$(\widetilde{U}t_j + \widetilde{U}'x_j + \widetilde{U}''y_j \ : \ \widetilde{V}t_j + \widetilde{V}'x_j + \widetilde{V}''y_j) \in \mathbf{P}^1(K).$$

Donc :

$$L_j = \Lambda_j \cdot \left[(\widetilde{V}t_j + \widetilde{V}'x_j + \widetilde{V}''y_j) \cdot T - (\widetilde{U}t_j + \widetilde{U}'x_j + \widetilde{U}''y_j) \cdot X\right]$$

avec $\Lambda_j \in \overline{K}^*$. On obtient

$$S = \Lambda \cdot \prod_{j=1}^{m} \Lambda_j^{\nu_j} \cdot \underbrace{\prod_{j=1}^{m} \left[(\widetilde{V}t_j + \widetilde{V}'x_j + \widetilde{V}''y_j) \cdot T - (\widetilde{U}t_j + \widetilde{U}'x_j + \widetilde{U}''y_j) \cdot X\right]^{\nu_j}}_{\in \mathcal{O}[T,X]}.$$

Il suit que le coefficient $\Lambda \cdot \prod_{j=1}^{m} \Lambda_j^{\nu_j}$ appartient à $\mathcal{O}$. On spécialise pour obtenir

$$\mathrm{eval}_I(S) = \mathrm{eval}_I\left(\Lambda \cdot \prod_{j=1}^{m} \Lambda_j^{\nu_j}\right) \cdot \prod_{j=1}^{m} [x_j \cdot T - t_j \cdot X]^{\nu_j}$$

En spécialisant via $\alpha = \begin{pmatrix} a & a' & a'' \\ b & b' & b'' \\ c & c' & c'' \end{pmatrix}$:

$$\mathrm{eval}_I(S) = \mathrm{eval}_\alpha\left(\Lambda \cdot \prod_{j=1}^{m} \Lambda_j^{\nu_j}\right) \cdot \prod_{j=1}^{m} \left[(\widetilde{b}t_j + \widetilde{b}'x_j + \widetilde{b}''y_j) \cdot T - (\widetilde{a}t_j + \widetilde{a}'x_j + \widetilde{a}''y_j) \cdot X\right]^{\nu_j},$$

où on a utilisé la même notation pour la matrice complémentaire. Or, il est clair que

$$\mathrm{eval}_I(S) = \mathrm{res}_Y^{d,e}(F, G)$$

et

$$\mathrm{eval}_\alpha(S) = \mathrm{res}_Y^{d,e}(\alpha^\# F, \alpha^\# G).$$

Ceci est suffisant pour montrer le théorème. □

Exemple 92. Soient C le cercle donné par $\mathcal{Z}_{\mathbf{C}}(f)$ où $f = X^2+Y^2-1$ et D le cercle donné par $\mathcal{Z}_{\mathbf{C}}(g)$ avec $g = (X-3)^2+Y^2-1$. Les courbes projectives associées sont $\overline{C} = \mathcal{Z}(\widetilde{f})$, où $\widetilde{f} = X^2+Y^2-T^2$, et $\overline{D} = \mathcal{Z}_{\mathbf{C}}(\widetilde{g})$ où $\widetilde{g} = X^2-6XT+9T^2+Y^2-T^2$. On observe que $(0:0:1) \notin \overline{C} \cup \overline{D}$. De plus,

$$\mathrm{res}_Y^{2,2}(f,g) = 9(2X-3)^2.$$

On déduit que sur $(\mathbf{C}^2)_0$, les courbes C et D se coupent sur $(3/2, \pm\mathrm{i}\sqrt{5}/2)$. Les points $\overline{C} \cap \overline{D} \cap \Omega$ sont les zéros de $X^2+Y^2 = 0$, donc $(0:1:\pm\mathrm{i})$. Il suit que

$$\overline{C} \cap \overline{D} = \{(1:3/2:\pm\mathrm{i}\sqrt{5}/2), (0:1:\pm\mathrm{i})\};$$

Comme $\sum_P \langle \overline{C}, \overline{D} \rangle_P = 4$, on voit que chaque point a multiplicité 1.