

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 présence¹, 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*. Birkhäuser 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 et 2

(20 Janvier 2023).

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, \dots, x_n de A , on désigne par $\langle x_1, \dots, x_n \rangle$ l'idéal de $a_1A + \dots + a_nA$.
4. Si A est un anneau intègre, son corps de fractions sera noté $\text{Fr}(A)$.
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 *invertible* s'il divise 1. Il est clair que l'ensemble des éléments invertibles 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 $x \stackrel{\text{ass}}{\sim} y$ pour dire que x est associé à y et on remarquera que $\stackrel{\text{ass}}{\sim}$ est une relation d'équivalence.
 4. Un élément $x \in A$ est *irréductible* s'il n'est pas nul ou invertible et si chacun de ses diviseurs lui est associé ou est invertible.
 5. Un élément $x \in A$ est dit *premier* s'il n'est pas nul ou invertible 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

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 $p \stackrel{\text{ass}}{\sim} f$. Si $p \mid g$, le même argument montre que $p \stackrel{\text{ass}}{\sim} g$ et f est inversible. Conclusion : Un diviseur de p lui est associé ou est inversible. \square

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 $\theta = i\sqrt{5}$ 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, \dots, p_m , pas forcément distincts, tels que $f = p_1 \cdots p_m$.

F2. Si p_1, \dots, p_m et q_1, \dots, 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 $q_i \stackrel{\text{ass}}{\sim} p_{\sigma(i)}$.

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 $f : \mathbf{C} \rightarrow \mathbf{C}$ 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 $\mathbf{Z}[i\sqrt{5}]$ et décomposer 6 de deux façons différentes : $2 \cdot 3 = (1 - i\sqrt{5})(1 + i\sqrt{5})$.

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 emploie la fait que \mathbf{Z} est ordonné. La validité de **F2** est plus subtile et est conséquence des propositions suivantes :

P1 Division Euclidienne \Rightarrow Tout idéal est principal.

P2 Tout idéal est principal \Rightarrow Lemme d'Euclide.

P3 Lemme d'Euclide \Rightarrow 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 $\varphi : A \setminus \{0\} \rightarrow \mathbf{N}$ ayant la propriété suivante :

DE. Pour chaque couple d'éléments $x \in A$ et $d \in A \setminus \{0\}$, il existe un² 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 $\mathbf{Z}[i]$ avec la norme $N(a+ib) = a^2+b^2$. (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. \square

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 que $x \mid yz$. On suppose que $x \nmid y$ et on considère un générateur 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 écrire $1 = ax + by$. Par conséquent, $z = axz + b \cdot yz$ et $x \mid z$. \square

2. 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 est³ 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. \square

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 $d_m \stackrel{\text{ass}}{\sim} d_{m+1}$, en contradiction avec (ii).

2 La factorisation dans un anneau de polynômes

On suppose A factoriel et on écrit $K = \text{Fr}(A)$. On souhaite étudier les factorisation dans $A[X]$. L'idée principale ici est utiliser ce qui est connu sous le nom de *contenu* d'un polynôme. Par contre, cette notion est une confluence d'objets plus profonds : les *valuations*.

3. Correction : Il faudrait rajouter "de plus" ici.

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 $A \setminus \{0\}$ 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 $v_p : A \setminus \{0\} \rightarrow \mathbf{N}$, que voici

$$v_p(f) = \begin{array}{l} \text{exposant de } p \\ \text{dans sa factorisation de } f \end{array} = \max\{n \in \mathbf{N} : p^n \mid f\}.$$

Comme A est factoriel, il est immédiat de voir que

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

On prolonge v_p à $K \setminus \{0\} \rightarrow \mathbf{Z}$ en écrivant

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

Il est utile de décrire $v_p(0) = \infty$, où $\infty \geq n$ 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 seulement si $v_p(a) \geq 0$ pour tout $p \in \mathcal{P}$.

Une autre propriété fondamentale de v_p est :

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

(1) On a

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

(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 $v_p(a) \leq v_p(b)$. Or, $p^{v_p(a)} \mid a + b$ et donc $v_p(a) \leq v_p(a + b)$.

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

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

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

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

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

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

est appelée une valuation.

On prolonge v_p à $K[X]$.

Définition 20 (La valuation de Gauss). Pour chaque $f = a_n X^n + \dots + a_0 \in A[X]$, on définit :

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

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. Dit autrement, v_p est une valuation.

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,

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

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

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

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. \square

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 *primitif*.

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 son degré est > 0), alors f est primitif.

Corollaire 26 (Permanence de l'irréductibilité). Soit $f \in A[X]$ irréductible tel que $\deg f > 0$. Alors il est aussi irréductible en $K[X]$.

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

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

Pour $(g, h) \in \mathbf{Fact}$, soit

$$P(g, h) = \{p \in \mathcal{P} : \min\{v_p(g), v_p(h)\} < 0\}.$$

Il s'agit d'un ensemble fini. Si $\mathbf{Fact} \neq \emptyset$, on va construire $(\tilde{g}, \tilde{h}) \in \mathbf{Fact}$ tel que $P(\tilde{g}, \tilde{h}) = \emptyset$. Ceci produit une contradiction, car $v_p(\tilde{g}) \geq 0$ et $v_p(\tilde{h}) \geq 0$ 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 $|P(g_1, h_1)| < |P(g, h)|$. Par récurrence, on obtient $(\tilde{g}, \tilde{h}) \in \mathbf{Fact}$ tel que $P(\tilde{g}, \tilde{h}) = \emptyset$. \square

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 $v_p(g) \geq 0$, ce qui implique que $\varphi \in A[X]$.

Il reste à 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

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

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. \square

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

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

On termine par quelques critères d'irréductibilité.

Définition 29. Soit A factoriel et p un irréductible de A . Un polynôme $f = a_d X^d + \dots + a_0$ de degré $d > 0$ est dit p -Eisenstein si $p \nmid a_d$, $p \mid a_i$ pour tout $i \in \{0, \dots, d-1\}$, 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 en $A[X]$. En particulier, si $K = \text{Fr}(A)$, alors f est aussi irréductible en $K[X]$.

Démonstration. Soit $f = a_d X^d + \dots + a_0$ 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 $h = \sum_{i=0}^s c_i X^i$. 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, $0 < m \leq r$ et

$$g = \underbrace{b_r}_{\neq 0 \pmod p} X^r + \dots + \underbrace{b_m}_{\neq 0} X^m + \underbrace{b_{m-1}}_{\equiv 0} X^{m-1} + \dots + \underbrace{b_0}_{\equiv 0 \pmod p}.$$

Par conséquent

$$a_m = \underbrace{b_0 c_m + b_1 c_{m-1} + \dots + b_{m-1} c_1}_{\equiv 0 \pmod p} + \underbrace{b_m c_0}_{\neq 0 \pmod p},$$

on déduit que $a_m \not\equiv 0 \pmod{p}$. Puisque $m \leq r < d$, on arrive à une contradiction.

La dernière affirmation suit immédiatement de la permanence de l'irréductibilité (Corollaire 26). □

Cours 3

(27/1/23).

Exemple 31. Soit $n \geq 1$ 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 $\varphi : A \rightarrow B$ un morphisme d'anneaux et soit $\varphi : A[X] \rightarrow B[X]$ le morphisme induit. Si $f \in A[X]$ est unitaire et $\varphi(f)$ est irréductible, alors f est irréductible.

Démonstration. Exercice. □

Exemple 33. Soient $n \geq 1$ un entier. Alors le polynôme $X^n + Y^n + Z^n - 1 \in \mathbf{C}[X, Y, Z]$ est irréductible. En effet, soit $\varphi : \mathbf{C}[X, Y] \rightarrow \mathbf{C}[Y]$ défini par $\varphi(X) = 0$ et $\varphi(Y) = Y$. Son extension à $(\mathbf{C}[X, Y])[Z]$ envoie 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 *degré* au lieu de degré total.

Définition 35 (L'ensemble des zéros). Pour chaque $f \in k[X, Y]$, on définit $\mathcal{Z}(f)$ comme étant l'ensemble des points $(x, y) \in k^2$ tels que $f(x, y) = 0$.

Définition 36. 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 37. (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 $\mathcal{Z}(f) = \emptyset$!
- (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 clos⁴, 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 38. *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 $f \in k[X]$ 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 $\mathcal{Z}(f) \rightarrow k$ contient \mathcal{N} dans son image et $\mathcal{Z}(f)$ est infini. \square

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

Théorème 39. *Soit A factoriel. Soient $f, g \in A[X]$ n'ayant aucun facteur irréductible commun. Alors il existe $d \in A \setminus \{0\}$ ainsi que $a, b \in A[X]$ tels que*

$$af + bg = d.$$

Démonstration. Soit $K = \text{Fr}(A)$. 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 $c \in A \setminus \{0\}$, 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.

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

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

$$1 = a_1f + b_1g.$$

Éliminant les dénominateurs, on arrive au résultat souhaité. □

Corollaire 40. *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 $d_1 \in k[X] \setminus \{0\}$, un $d_2 \in k[Y] \setminus \{0\}$, ainsi que $a_1, b_1, a_2, b_2 \in k[X, Y]$ tels que*

$$a_1f + b_1g = d_1 \quad \text{et} \quad a_2f + b_2g = d_2.$$

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

Voici une conséquence importante.

Théorème 41. *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 40, 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. □

Cours 4

(3/2/23).

Exemple 42. 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.

Le Théorème 39 (ou le Corollaire 40) permet aussi d'obtenir plusieurs informations sur les idéaux *maximaux* de $k[X, Y]$.

Théorème 43 (Nullstellensatz). (1) Soit $P \in k^2$. Alors l'idéal $\mathfrak{m}_P = \{g \in k[X, Y] : g(P) = 0\}$ est maximal. De plus, si $P = (x, y)$, alors $\mathfrak{m}_P = (X - x, Y - y)$.

(2) Soient $P, Q \in k^2$. Si $\mathfrak{m}_P = \mathfrak{m}_Q$, alors $P = Q$.

(3) On suppose que k est algébriquement clos. Soit $\mathfrak{m} \subset k[X, Y]$ un idéal maximal. Alors il existe un $P \in k^2$ tel que $\mathfrak{m} = \mathfrak{m}_P$. Par conséquent, la fonction

$$P \longmapsto \mathfrak{m}_P$$

établit une bijection entre k^2 et les idéaux maximaux de $k[X, Y]$.

Démonstration. (1) et (2). Exercices pour le lecteur.

(3) Soit $\mathfrak{m} \subset k[X, Y]$ un idéal maximal et soit $h \in \mathfrak{m} \setminus \{0\}$. On le décompose en facteurs premiers : $h = f_1 \cdots f_r$. Comme \mathfrak{m} est maximal, en particulier premier, il suit qu'un des facteurs de f_i doit appartenir à \mathfrak{m} . Pour simplifier la notation, on suppose désormais que h est irréductible.

On montre maintenant que $\mathfrak{m} \neq (h)$ en montrant que l'égalité, qui est supposée désormais, mène à une contradiction. Soit $P \in \mathcal{Z}(h)$. Il suit que pour chaque $h \in \mathfrak{m}$, l'on a $h(P) = 0$ et donc $\mathfrak{m} \subset \mathfrak{m}_P \Rightarrow \mathfrak{m} = \mathfrak{m}_P$. Or, il suit que h s'annule seulement sur un point, ce qui est faux (Lemma 38). Donc il existe $g \in \mathfrak{m} \setminus (h)$. Comme $h \nmid g$, on sait que h et g sont premiers entre eux. Par conséquent, on peut écrire

$$\underbrace{d(X)}_{\neq 0} = \alpha(X, Y)f(X, Y) + \beta(X, Y)g(X, Y),$$

$$\underbrace{e(Y)}_{\neq 0} = \gamma(X, Y)f(X, Y) + \delta(X, Y)g(X, Y).$$

Mais ceci implique que $d(X), e(Y) \in \mathfrak{m}$. Or, si $\deg d = 0$ (ou $\deg e = 0$), alors $d \in k^*$ (ou $e \in k^*$) et $\mathfrak{m} = (1)$, ce qui est exclu. Donc d et e sont non-constants. On déduit que un facteur $X - x$ de d , respectivement et un facteur $Y - y$ de e , appartient à \mathfrak{m} . Donc $\mathfrak{m} \supset \mathfrak{m}_{(x,y)} \Rightarrow \mathfrak{m} = \mathfrak{m}_{(x,y)}$. \square

Théorème 44 (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 41). 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 (Lemme 38). \square

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 45. *k algébriquement clos. La fonction*

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

est une bijection.

Démonstration. Soient f et g sans facteur carré tels que $\mathcal{Z}(f) = \mathcal{Z}(g)$. Soit $p \mid f$ irréductible. 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'ont pas de carré, on déduit que f et g diffèrent 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 $\tilde{f} = \prod_i p_i$. \square

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 46. *La fonction*

$$C \longmapsto \text{générateur de } \mathcal{I}_C$$

est la bijection inverse à la fonction \mathcal{Z} définie dans le Théorème 45.

Ceci permet la définition suivante :

Définition 47. Soit C une courbe plane. Son *degré* est le degré d'un générateur de \mathcal{I}_C .

Exercice 48. Un idéal $I \subset k[X, Y]$ est *radical* si la propriété suivantes est vérifiée pour chaque $f \in k[X, Y]$: si $f^r \in I$ pour un certain $r > 0$, alors $f \in I$. Montrer qu'un idéal principal (f) de $k[X, Y]$ est radical si et seulement si f n'a pas de facteur carré.

Exercice 49. Soit \mathfrak{p} un idéal premier qui n'est pas maximal. Montrer que $\mathfrak{p} = (f)$, avec f irréductible. Indication : Suivre la preuve du Théorème 43.

4 Propriétés caractéristiques des courbes planes

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 polynôme 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 50. 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 $\text{Sing}(C)$. Une courbe sans singularités est dite non-singulière.

Exemple 51. Soit $f = X^2 + Y^2 - 1$. Pour que f puisse en effet définir une courbe, il faut que f ne soit 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 $\text{Sing}(C) = \emptyset$.

Exemple 52. Soit $f = Y^2 - X^3 - X^2$. Alors $\text{Sing}(C) = (0, 0)$.

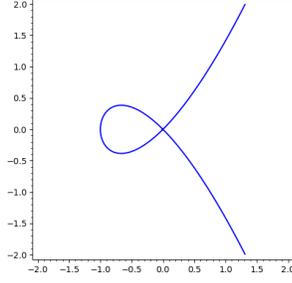


FIGURE 1 – La courbe $Y^2 = X^3 + X$

Théorème 53. $\#\text{Sing}(C) < \infty$.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 nécessaire!) 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 $\#\text{Sing}(\mathcal{Z}(f)) < \infty$ dans le cas où f est irréductible.

On sait que soit $\#\mathcal{Z}(f) \cap \mathcal{Z}(\partial_X f) < \infty$, soit $f \mid \partial_X f$ (voir Théorème 41). Si $f \mid \partial_X f$, alors $\partial_X f = 0$, étant donné que le degré de f , comme polynôme en X , est strictement supérieur au degré de $\partial_X f$, en tant que polynôme en X . Dans ce cas, $f \in k[Y]$, et comme f est irréductible et k est algébriquement clos, on doit avoir $f = aY + b$ avec $a \neq 0$. Il suit que $\partial_Y f = a \neq 0$. \square

Remarques 54. Dans la preuve du Théorème 53, on a imposé la condition que k était de caractéristique nulle et algébriquement clos. On suppose ici que k n'est ni de caractéristique

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 utilisée. 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 $\text{Frac}(A) = k$. 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, $\partial_X f = \partial_Y f = 0$.

nulle, ni algébriquement clos. Soit ainsi $p \geq 0$ la caractéristique de k . Si $\partial_X f = 0$, alors

$$f = \sum_{i=0}^d a_i(Y) X^{pi}.$$

(Si $p = 0$, ceci signifie simplement que $f \in k[Y]$.) Dans ce cas, on doit essayer de montrer que $\#\mathcal{Z}(\partial_Y f) \cap \mathcal{Z}(f) < \infty$. Si ceci n'est pas le cas, alors $f \mid \partial_Y f$ et on déduit à nouveau que $f = \sum_{j=0}^e b_j(X) Y^{pj}$. Dit autrement, $f \in k[X^p, Y] \cap k[X, Y^p] \Rightarrow$ si α_{ij} est le coefficient de $X^i Y^j$, alors $\alpha_{ij} = 0$ sauf si $i \equiv 0 \pmod p$ et $j \equiv 0 \pmod p$. Soit maintenant K une extension de k possédant des éléments β_{ij} tels que $\alpha_{ij} = \beta_{ij}^p$ pour chaque couple i, j . On obtient ainsi un $F \in K[X, Y]$ tel que $F^p = f$.

Cours 5

(10/02/23).

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 $\partial_Y f(O) = c_{01}$. Pour $\theta \in k$, soit

$$D_\theta = \mathcal{Z}(Y - \theta X)$$

la droite de pente θ . Soit

$$\text{eval}_{D_\theta} : k[X, Y] \longrightarrow k[X], \quad \begin{array}{l} X \longmapsto X, \\ Y \longmapsto \theta X \end{array}$$

le morphisme “d'évaluation” sur D_θ . Donc

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

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

$$\text{eval}_{D_\infty} : k[X, Y] \longrightarrow k[X], \quad \begin{array}{l} X \longmapsto 0 \\ Y \longmapsto X. \end{array}$$

On déduit

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

et la multiplicité de 0 est > 1 .

Définition 55 (Multiplicité d'intersection). Pour $\theta \in k \cup \{\infty\}$, on définit la multiplicité d'intersection entre C et D_θ comme étant

$$\langle C, D_\theta \rangle_O = \begin{array}{l} \text{multiplicité de “0”} \\ \text{en tant que zéro de } \text{eval}_{D_\theta}(f). \end{array}$$

Les arguments précédents ont établi la première affirmation de la proposition suivante.

Proposition 56. *Si O est une singularité, alors $\langle C, D_\theta \rangle_O > 1$ pour un certain $\theta \in k \cup \{\infty\}$. Réciproquement, si O n'est pas une singularité, alors il existe un $\theta \in k \cup \{\infty\}$ tel que $\langle C, D_\theta \rangle_O = 1$.*

Démonstration. Il nous manque la vérification de la dernière affirmation. On a

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

Si $\partial_X f(O) = c_{10} \neq 0 \Rightarrow \langle C, D_0 \rangle_O = 1$. Si $c_{10} = 0$ mais $\partial_Y f(O) = c_{01} \neq 0$, alors $\langle C, D_1 \rangle_O = 1$.

□

Ceci suggère la définition suivante :

Définition 57 (La multiplicité). La multiplicité du point $O \in C$ est l'entier

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

Une interprétation entièrement algébrique de la multiplicité suit.

Proposition 58. *On écrit*

$$f = f_m + \dots$$

avec

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

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

Démonstration. Soit $\theta \in k$. La propriété fondamentale d'un polynôme f_d est son homogénéité : $f_d(X, \theta X) = X^d f_d(1, \theta)$ et $f_d(0, X) = X^d f_d(0, 1)$. On a

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

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 polynôme $f_m(1, X)$. 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,

$$\langle C, D_\theta \rangle_O = \begin{cases} m, & \text{si } \theta \notin \mathcal{T}, \\ > m, & \text{si } \theta \in \mathcal{T}. \end{cases}$$

De même,

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

Il suit que

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

et

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

Par conséquent, m est la multiplicité.

□

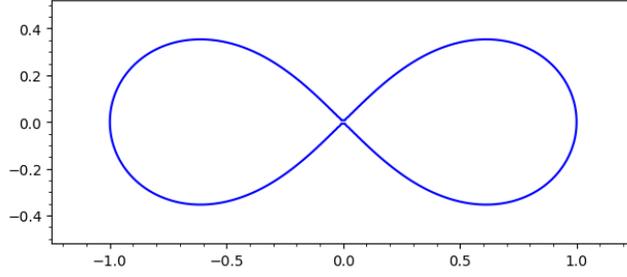


FIGURE 2 – La Lemniscate

Exemple 59. 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 $\text{mult}_O(C) = 2$.

Un point d’interprétation géométrique est important ici. Même si la courbe C est singulière au point O , il est possible d’avoir, en géométrie algébrique, une notion “d’espace tangent”.

Définition 60. Le cône tangent de C au point O est la courbe $f_m = 0$, où $m = \langle C, D_\theta \rangle_O$.

Le nom “cône” est contre-intuitif ici car d’habitude on pense aux cônes comme étant de dimension deux. Ceci peut être pallié en se rappelant qu’un cône n’est rien d’autre qu’une certaine réunion de droites qui passent par un point.

Exemple 61. Si C n’est pas singulière au point O , alors

$$\partial_X f(O)X + \partial_Y f(O)Y = \begin{pmatrix} \partial_X f(O) & \partial_Y f(O) \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix}$$

et le cône tangent $D = \mathcal{Z}(\partial_X f(O)X + \partial_Y f(O)Y)$ est la droite tangente. Le cône tangent à la Lemniscate est la réunion de droites $\mathcal{Z}(X^2 - Y^2) = \mathcal{Z}(X - Y) \cup \mathcal{Z}(X + Y)$.

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.

Les polynômes homogènes

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

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

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

$$\sum_{d=|\mathbf{i}|} c_i \mathbf{X}^i.$$

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 une autre intervention lors de l'étude du résultant. Pour l'instant, on se contente de donner une caractérisation utile des polynômes homogènes.

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

$$f_0 + \dots + f_d,$$

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 se comportent pour sur les "droites". En effet, si $f \in P$ est homogène de degré d alors $f(a\mathbf{X}) = a^d f(\mathbf{X})$ 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

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

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

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

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

Proposition 62. *Un $f \in P$ est homogène de degré m si et seulement si $f(T\mathbf{X}) = T^m f(\mathbf{X})$ dans $P[T]$.*

Cours 6

(17/2/23).

Les affinités (ou transformations affines)

Définition 63. Une fonction $\varphi : k^2 \rightarrow k^2$ est une transformations affine, ou une affinité⁶, si elle a la forme

$$\varphi(x, y) = (\alpha x + \beta y + \rho, \gamma x + \delta y + \sigma),$$

ou, en notation vectorielle,

$$\alpha \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \cdot \begin{pmatrix} x \\ y \end{pmatrix} + \begin{pmatrix} \rho \\ \sigma \end{pmatrix}.$$

Une affinité est inversible si la matrice en question l'est aussi.

Proposition 64. Soit φ une transformation affine inversible et C une courbe plane. Alors $\varphi^{-1}(C)$ est aussi une courbe plane. Plus précisément, soit $\varphi^\# : k[X, Y] \rightarrow k[X, Y]$ le morphisme d'anneaux définit par

$$\varphi^\#(X) = \alpha X + \beta Y + \rho, \quad \varphi^\#(Y) = \gamma X + \delta Y + \sigma.$$

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

Démonstration. On a

$$\begin{aligned} (x, y) \in \varphi^{-1}(C) &\Leftrightarrow f(\varphi(x, y)) = 0 \\ &\Leftrightarrow f(\alpha x + \beta y + \rho, \gamma x + \delta y + \sigma) = 0 \\ &\Leftrightarrow \varphi^\# f(x, y) = 0. \end{aligned}$$

Ensuite, $\varphi^\#(f)$ est également un polynôme non-constant, car $\varphi^\#$ 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 :

Proposition 65. Soit $P \in C$. Soient φ et ψ des affinités inversibles telles que $\varphi(O) = \psi(O) = P$. Alors

$$\text{mult}_O(\varphi^{-1}(C)) = \text{mult}_O(\psi^{-1}(C)).$$

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.

Démonstration. La preuve emploie :

Lemme 66. Soient $h \in k[X, Y]$ homogène de degré d et φ est une affinité inversible et linéaire. Alors $\varphi^\#(h)$ est homogène de degré d .

Démonstration. Soit $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ la matrice de φ . On note que

$$\begin{aligned} (\varphi^\#h)(TX, TY) &= h(\alpha TX + \beta TY, \gamma TX + \delta TY) \\ &= T^d h(\alpha X + \beta Y, \gamma X + \delta Y) \\ &= T^d \varphi^\#(h). \end{aligned}$$

□

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

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

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

On arrive en fin à la définition générale :

Définition 67. Soit $C = \mathcal{Z}(f)$ une courbe plane et $P \in C$. On définit $\text{mult}_P(C)$ comme étant $\text{mult}_O(\varphi^{-1}(C))$, où φ est une affinité inversible telle que $\varphi(O) = P$.

5 Définition du résultant

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

Définition 68. La matrice de Sylvester du couple f et g est la matrice $(d+e) \times (d+e)$

avec coefficients dans A :

$$\begin{pmatrix} a_d & a_{d-1} & \cdots & a_0 & 0 & 0 & \cdots & 0 & 0 \\ 0 & a_d & \cdots & \cdots & a_0 & 0 & \cdots & \cdots & 0 \\ \cdots & \cdots \\ 0 & \cdots & 0 & \cdots & 0 & a_d & \cdots & \cdots & a_0 \\ \hline b_e & b_{e-1} & \cdots & \cdots & \cdots & b_0 & 0 & \cdots & 0 \\ 0 & b_e & \cdots & \cdots & \cdots & \cdots & b_0 & \cdots & 0 \\ \cdots & \cdots \\ 0 & \cdots & \cdots & \cdots & \cdots & 0 & b_e & \cdots & b_0 \end{pmatrix}$$

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

Remarques 69. Comme d et e sont fixés, $\text{res}_X^{d,e}(f, g)$ serait une notation plus précise. Une conséquence de cette convention est : si $\deg f < d$ et $\deg g < e$, alors $\text{res}_X^{d,e}(f, g) = 0$.

Exemple 70. (1) Soient $a, b \in (a, b) \in k^2 - \{(0, 0)\}$, $\ell = bY + aX$ et $f = XY - 1$; $\mathcal{Z}(f)$ est une hyperbole et $\mathcal{Z}(\ell)$ une droite. Le résultant est un déterminant 2×2 :

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

Il suit que $\deg_X(R) = 0$ si $a = 0$. Dit autrement, R est une constante si ℓ est l'axe des abscisses. Cet exemple peut-être compris par la géométrie "à l'infini" ; il sera revu plus tard.

(2) On reprend l'exemple 42. On a $f = X^2 - Y^2$ et $g = XY + X - Y - 1$. Il suit que

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

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

(3) Soient

$$\begin{aligned} f &= X^2 - 2Y^2 + XY - 2X + 5Y \\ g &= X^2 + XY + Y - X - 2. \end{aligned}$$

Clairement

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

Le lecteur remarquera, en vue du Exemple précédent, que le degré du résultant semble mystérieux et sans lien simple entre les degrés des polynômes qui le définissent. On commence doucement son étude :

Définition 71. 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 72. 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 $\deg(\text{res}_Y(f, \ell)) < 2$, 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, $\{1, X, \dots, X^{n-1}\}$ en est une base ordonnée. Soit

$$\begin{aligned} A[X]_{<e} \times A[X]_{<d} &\xrightarrow{\mathcal{L}_{f,g}} A[X]_{<d+e} \\ (p, q) &\longmapsto pf + qg. \end{aligned}$$

Il est clair que

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

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

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

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

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

est

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

Dans la suite, on fera appel à quelques propriétés basiques des matrices carrés sur un anneau en général. L'étudiant peut toujours construire les preuves en remarquant que, si A est intègre avec corps de fractions K , alors $\text{res}^{d,e}(f, g)$ 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 73. *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 $\text{res}(f, g)$ 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) \Rightarrow (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 $K := \text{Fr}(A)$

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

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

(2) \Rightarrow (3) On suppose que $a_d \neq 0$. Soit $K = \text{Fr}(A)$. 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 $\deg q \leq d - 1$.

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

□

Cours 7

(24/2/23).

Nous avons fait notre premier devoir surveillé.

Cours 8

(10/3/23).

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

Théorème 74. *On suppose A intègre et que $\text{res}(f, g) \neq 0$. Alors, pour tout $h \in A[X]_{<d+e}$, l'élément $\text{res}(f, g) \cdot h$ appartient à $\text{Im}(\mathcal{L}_{f,g})$.*

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

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

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

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

et

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

□

Corollaire 75. *On suppose que A est intègre. Alors il existe $(p, q) \in A[X]_{<e} \times A[X]_{<d}$ tel que*

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

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

Démonstration. Si $\text{res}(f, g) \neq 0$, cela suit directement du Théorème précédent appliqué à $h = 1$. Si $\text{res}(f, g) = 0$, alors il existe $(p, q) \in \text{Ker } \mathcal{L}_{f,g} \setminus \{0\} \Rightarrow \text{res}(f, g) = 0 = \mathcal{L}_{f,g}(p, q)$. □

Première application géométrique du résultant

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

Exercice 76. Soit $\varphi : A \rightarrow B$ un morphisme d'anneaux et soit $\varphi : A[X] \rightarrow B[X]$ le morphisme d'anneaux défini 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 $\varphi(\text{res}^{d,e}(f, g)) = \text{res}^{d,e}(\varphi(f), \varphi(g))$ 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

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

où $d, e \geq 1$. (Même si $a_d = 0$ ou $b_e = 0$.) Soit

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

Maintenant, pour chaque $x \in k$, soit $\text{ev}_x : k[X] \rightarrow k$ l'évaluation en x ; l'extension naturelle $\text{ev}_x : k[X, Y] \rightarrow k[Y]$ sera également désignée par ev_x (dit autrement, $\text{ev}_x : h(X, Y) \mapsto h(x, Y)$). Par l'exercice 76, on a

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

(Ici, la définition du résultant avec des indices d et e fixés se montre utile.) Si $(x, y) \in \mathcal{Z}(f) \cap \mathcal{Z}(g)$, alors $\text{ev}_x(f) \in k[Y]$ et $\text{ev}_x(g) \in k[Y]$ auront y comme zéro commun, donc seront divisibles simultanément par $Y - y$. Ceci entraîne $R(x) = 0$.

On obtient :

Théorème 77. Soient $\text{pr}_X : k^2 \rightarrow k$ et $\text{pr}_Y : k^2 \rightarrow k$ les projections sur la première et la deuxième coordonnée respectivement. Alors $\text{pr}_X(\mathcal{Z}(f) \cap \mathcal{Z}(g))$ est contenu dans les zéros de $\text{res}_Y^{d,e}(f, g) \in k[X]$. De même, $\text{pr}_Y(\mathcal{Z}(f) \cap \mathcal{Z}(g))$ est contenu dans les racines de $\text{res}_X^{d,e}(f, g) \in k[Y]$. \square

Une autre façon d'arriver à ce résultat est la suivante. On écrit

$$R(X) = p(X, Y)f(X, Y) + q(X, Y)g(X, Y)$$

à l'aide du Théorème 74 et on observe que si $(x, y) \in \mathcal{Z}(f) \cap \mathcal{Z}(g)$, alors $R(x) = 0$.

Ceci signifie que si on connaît 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 78. 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

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

et

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

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 79. Soit $A = k[U_1, \dots, U_m]$. Soient

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

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 $\text{res}_X^{d,e}(f, g) \neq 0$, alors $\text{res}_X^{d,e}(f, g)$ est homogène de degré de . (Même si $\text{res}(f, g) = 0$, on peut dire qu'il est homogène de degré de . Par contre, ceci peut facilement conduire à des erreurs de raisonnement!)

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

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

On multiplie la première ligne par T , la deuxième par T^2 , \dots , 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

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

$$= T^{1+\dots+e+1+\dots+d} R(TU).$$

Attention, même si la graphie laisse croire que $T^{d+1} a_0$ et $T^{e+1} b_0$ sont sur la même colonne, ceci est 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

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

Comme cette identité est vraie dans $A[T, \mathbf{U}]$, on déduit que

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

Ceci signifie que $R(\mathbf{U})$ 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

Corollaire 80. *On suppose k algébriquement clos. Soient $f, g \in k[X, Y]$ ayant respectivement des degrés $d \geq 1$ et $e \geq 1$. Alors $\deg \operatorname{res}_Y^{d,e}(f, g) \leq de$ 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 $f = \sum_{i=0}^d f_i$ et $g = \sum_{i=0}^e g_i$ avec f_i et g_i homogènes de degré i . (On observe ici que $f_d \neq 0$ et $g_e \neq 0$.) On considère leur homogénéisation :

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

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

D'après Prp. 79,

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

est homogène de degré de ou nul. Grâce à l'exercice 76, on note que

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

Pour simplifier, on écrit $R(X) = \tilde{R}(1, X)$. Puisque $\tilde{R} \in k[T, X]$ est homogène de degré de , on peut l'écrire comme

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

d'où

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

Alors $\deg R < de \Leftrightarrow c_0 = 0$. Or, mais $c_0 = \tilde{R}(0, 1)$ et $\deg R < de \Leftrightarrow \tilde{R}(0, 1) = 0$. Une autre application de l'exercice 74 montre que

$$\tilde{R}(0, 1) = \operatorname{res}_Y^{d,e}(\tilde{f}(0, 1, Y), \tilde{g}(0, 1, Y)).$$

Or, mais

$$\tilde{f}(0, 1, Y) = f_d(1, Y) \quad \text{et} \quad \tilde{g}(0, 1, Y) = g_e(1, Y).$$

Donc $\deg R < de \Leftrightarrow \operatorname{res}_Y^{d,e}(f_d(1, Y), g_e(1, Y)) = 0$. On écrit maintenant

$$f_d(X, Y) = \sum_{i=0}^d a_i X^{d-i} Y^i \quad \text{et} \quad g_e(X, Y) = \sum_{i=0}^e b_i X^{e-i} Y^i.$$

D'après la Proposition 73, si $\text{res}_Y^{d,e}(f_d(1, Y), g_e(1, Y)) = 0$, alors ou bien $a_d = b_e = 0$, ou bien $f_d(1, Y)$ et $g_e(1, Y)$ possèdent une racine commune. Mais $a_d = b_e = 0$ implique que $X \mid f_d$ et $X \mid g_e$, ce qui est exclu. Ensuite, si $f_d(1, \theta) = g_e(1, \theta)$, alors $\theta X - Y \mid f_d$ et $\theta X - Y \mid g_e$, ce qui est également exclu. \square

Remarques 81. La preuve précédente permet aussi de montrer que si $\deg \text{res}^{d,e}(f, g) < de$, alors f et g ont forcément une direction asymptotique commune.

Cours 9

(17/3/23).

Corollaire 82 (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 $\#C \cap D \leq de$.

Démonstration. L'idée est d'appliquer la Proposition 79 et le Théorème 77. Il a deux obstacles.

O1. Il est possible que $\text{res}_Y^{d,e}(f, g) = 0$;

O2. 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 (O1) et (O2).

Pour chaque $\lambda \in k$, soit

$$t_\lambda : k^2 \longrightarrow k^2 \\ (x, y) \longmapsto (x + \lambda y, y).$$

Il s'agit d'une transvection : les droites horizontales restent inchangées, mais une translation est faite le long de chacune de ces droites. On observe que $t_\lambda^{-1} = t_{-\lambda}$. 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 $\#C_\lambda \cap D_\lambda \leq de$ pour un certain λ , ce que sera fait en montrant que pour un certain $\lambda \in k$, les obstacles O1 et O2 sont éliminés.

Élimination de O1. Il s'agit d'une technique assez simple qui trouvera son utilité dans d'autres contextes, alors on l'écrira comme un exercice.

Exercice 83. Soit $h \in k[X_1, \dots, X_n, Y]$ de degré $d > 0$. Si h_d désigne sa composante homogène de degré d , alors la coefficient de Y^d dans le polynôme

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

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

Soit λ tel que $f_d(\lambda, 1) \neq 0$. L'exercice montre que le coefficient de Y^d dans $t_\lambda^\# f$ est non-nul. Si $\text{res}_Y^{d,e}(t_\lambda^\# f, t_\lambda^\# g) = 0$, l'implication (2) \Rightarrow (3) de la Proposition 73 montre que $t_\lambda^\# f$ et $t_\lambda^\# g$ ne sont pas premiers entre eux. Mais ceci est impossible car f et g le sont et $t_\lambda^\# : k[X, Y] \rightarrow k[X, Y]$ est un automorphisme.

Élimination de O2. Soit $C \cap D = \{P_i := (x_i, y_i) : i = 1, \dots, r\}$. 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

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

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 O2. \square

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.

Cours 10

(24/3/23).

Géométrie projective

On commence par l'exemple des droites $L = \mathcal{Z}(X)$ et $M = \mathcal{Z}(X - 1)$. Clairement, $L \cap M = \emptyset$, 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 $\{1\} \times \mathbf{R}^2$. Soit \mathbf{S}^2 la sphère de rayon 1 et centre à l'origine. Relions chaque point de $\{1\} \times \mathbf{R}^2$ à \mathbf{S}^2 par la projection $\pi : p \mapsto \frac{p}{\|p\|}$. 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 \mathbf{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 84. L'ensemble des droites vectorielles de k^3 est l'espace projectif \mathbf{P}^2 .

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

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

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

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

il s'agit clairement d'une fonction injective et on obtient une "copie" de k^2 , en identifiant $k^2 = \{1\} \times k^2$, dans \mathbf{P}^2 . Son image sera désignée par

$$(k^2)_T = \{(t : x : y) \in \mathbf{P}^2 : t \neq 0\}.$$

Avec cette idée, on commence à penser aux points du plan comme étant des droites. Voir la Figure 3.

Remarques 85. 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].

La vérification de la proposition suivante est facile et omise.

Proposition 86. 1) *Le complémentaire de $(k^2)_T$ dans \mathbf{P}^2 est $\{D \in \mathbf{P}^2 : D \text{ parallèle à } \{1\} \times \mathbf{R}^2\}$.*

2) *Les fonctions*

$$\begin{aligned} \varphi_T : k^2 &\longrightarrow \mathbf{P}^2 & (x, y) &\longmapsto (1 : x : y) \\ \varphi_X : k^2 &\longrightarrow \mathbf{P}^2 & (t, y) &\longmapsto (t : 1 : y) \\ \varphi_Y : k^2 &\longrightarrow \mathbf{P}^2 & (t, x) &\longmapsto (t : x : 1) \end{aligned}$$

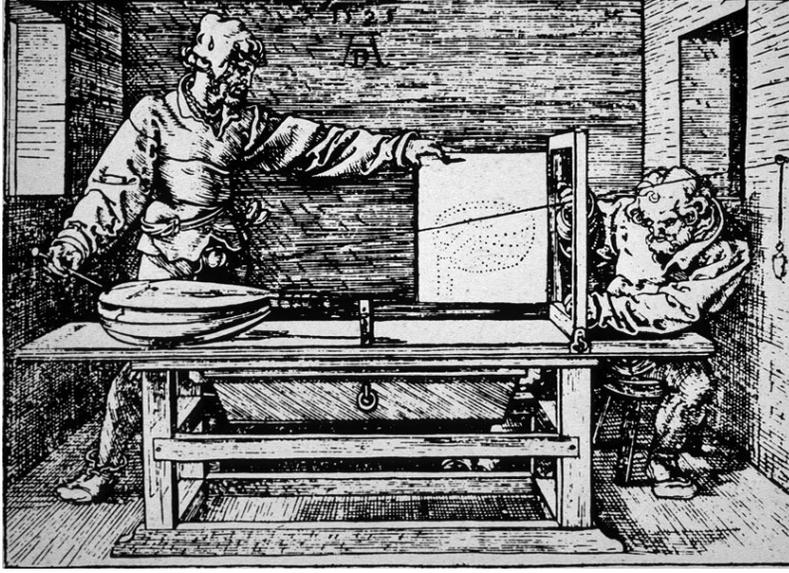


FIGURE 3 – A. Dürer, Dessin à la fin de *Unterweysung der Messung*, Nürnberg 1525

sont des injections. Si leurs images respectives sont notées par $(k^2)_T$, $(k^2)_X$ et $(k^2)_Y$, alors

$$\mathbf{P}^2 = (k^2)_T \cup (k^2)_X \cup (k^2)_Y.$$

□

Définition 87. L'ensemble

$$\begin{aligned} \Omega &:= \mathbf{P}^2 \setminus (k^2)_T \\ &= \{D \in \mathbf{P}^2 : D \text{ parallèle à } \{1\} \times \mathbf{R}^2\} \end{aligned}$$

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

Le cas où k est \mathbf{R} (ou \mathbf{C}) est assez intéressant.

Proposition 88. Soit $k = \mathbf{R}$ et $\mathbf{S}^2 \subset \mathbf{R}^3$ la sphère unitaire. Munissons \mathbf{P}^2 de la topologie suivante.⁷ Soit $\Psi : \mathbf{S}^2 \rightarrow \mathbf{P}^2$ la fonction qui à chaque $p \in \mathbf{S}^2$ associe la droite $\mathbf{R}p$. On dira que $U \subset \mathbf{P}^2$ est ouvert si $\Psi^{-1}(U)$ est ouvert de \mathbf{S}^2 .

- (1) \mathbf{P}^2 est compact et Ψ est localement un homéomorphisme.
- (2) Les sous-ensembles $(\mathbf{R}^2)_T$, $(\mathbf{R}^2)_X$ et $(\mathbf{R}^2)_Y$ sont ouverts et denses.
- (3) Pour chaque $\star = T, X, Y$, la bijection (décrite dans la Prp 86) $\varphi_\star : \mathbf{R}^2 \rightarrow (\mathbf{R}^2)_\star$ est un homéomorphisme.

⁷ Il s'agit de la topologie *quotient*. Sa propriété fondamentale est la suivante : Si M est un espace topologique et $f : \mathbf{P}^2 \rightarrow M$ une fonction, alors f est continue $\iff f\Psi$ est continue.

(4) Le sous-espace topologique Ω est homéomorphe au cercle unitaire \mathbf{S}^1 .

Démonstration. (1) Par construction, Ψ est surjective et continue. Donc \mathbf{P}^2 est compact car \mathbf{S}^2 l'est. Soit $\alpha : \mathbf{S}^2 \rightarrow \mathbf{S}^2$ la multiplication par -1 . De plus, si $U \subset \mathbf{S}^2$ est un ouvert tel que $U \cap \alpha U = \emptyset$, alors $\Psi|_U$ est une bijection. On vérifie que $\Psi^{-1}(\Psi(U)) = U \cup \alpha U$, qui est ouvert. Donc $\Psi|_U$ est une application ouverte et par conséquent un homéomorphisme sur l'ouvert $\Psi(U)$.

(2) On traite seulement le cas $(\mathbf{R}^2)_T$. Clairement, $\Psi^{-1}[(\mathbf{R}^2)_T]$ est $\mathbf{S}^2 \setminus \{0\} \times \mathbf{R}^2$. Par définition de la topologie, $(\mathbf{R}^2)_T$ est ouvert. Soit maintenant $F \subset \mathbf{P}^2$ fermé contenant $(\mathbf{R}^2)_T$. Donc $\Psi^{-1}F$ est un fermé contenant $\mathbf{S}^2 \setminus \{0\} \times \mathbf{R}^2$. Il suit que $\Psi^{-1}F = \mathbf{S}^2$ et donc $\Psi(\Psi^{-1}F) = \mathbf{P}^2$.

(3) On se concentre sur le cas de $\varphi_T : \mathbf{R}^2 \rightarrow (\mathbf{R}^2)_T$ et on écrit $\varphi_T^{-1} = \varphi'$. Soit

$$\mathbf{S}_T^2 := \Psi^{-1}(\mathbf{R}_T^2) = \mathbf{S}^2 \setminus \{0\} \times \mathbf{R}^2.$$

On considère le diagramme suivant :

$$\begin{array}{ccccc} \mathbf{S}_T^2 & \xrightarrow{\Psi} & \mathbf{R}_T^2 & \xrightarrow{\varphi'} & \mathbf{R}^2 \\ & \searrow & & \nearrow & \\ & & & & (t,x,y) \mapsto (x/t,y/t) \end{array}$$

Il n'est pas difficile de se convaincre que $\varphi'\Psi : \mathbf{S}_T^2 \rightarrow \mathbf{R}^2$ est continue, ouverte et surjective.

Continuité de φ' . Si $U \subset \mathbf{R}^2$ est ouvert, alors $\Psi^{-1}\varphi'^{-1}(U) = (\varphi'\Psi)^{-1}(U)$ est ouvert $\Rightarrow \varphi'^{-1}(U)$ est ouvert.

φ' est ouverte. Si $U \subset \mathbf{R}_T^2$ est ouvert, alors $(\varphi'\Psi|_{\mathbf{S}_T^2})^{-1}(\varphi'(U)) = \Psi^{-1}(U)$ est ouvert. Comme $\varphi'\Psi|_{\mathbf{S}_T^2}$ est ouverte et surjective, il suit que

$$\varphi'(U) = (\varphi'\Psi|_{\mathbf{S}_T^2})((\varphi'\Psi|_{\mathbf{S}_T^2})^{-1}(\varphi'(U)))$$

est ouvert.

(4) On laisse simplement une indication : Le cercle \mathbf{S}^1 est homéomorphe à \mathbf{R}/\mathbf{Z} , où l'on a donné à ce dernier ensemble la topologie quotient. \square

Remarques 89. Si $n \geq 1$ est un entier, on définit l'espace projectif de dimension n , \mathbf{P}^n , comme étant l'ensemble des droites vectorielles de k^{n+1} . Tous les résultats précédents peuvent se traduire dans ce contexte. Dans la suite, on n'aura besoin que de \mathbf{P}^2 et \mathbf{P}^1 .

La compacité de \mathbf{P}^2 est l'un de ses points remarquables. Elle permet de donner une interprétation géométrique de la notion de droite asymptotique.

Corollaire 90. *On maintient les hypothèses de la proposition. Soit $C \subset \mathbf{R}^2$ une courbe algébrique. Soit $(p_n) \subset C$ une suite telle que $\lim_n \|p_n\| = +\infty$.*

- 1) Soit $q_n := \varphi_T(p_n) \in (\mathbf{R}^2)_T$. Il existe une suite extraite $(q_{n_j})_{j \in \mathbf{N}}$ convergeant vers un $\omega \in \Omega$.
- 2) Si $\omega = (0 : \alpha : \beta)$, alors la droite $L \subset (\mathbf{R}^2)_T$ définie par $\mathcal{Z}(\alpha Y - \beta X)$ est une direction asymptotique.

Démonstration. (1) C'est une conséquence de la compacité que (q_n) possède une suite extraite convergente. Pour simplifier la notation, on suppose que $\lim_n q_n = \omega$ et on montre que $\omega \in \Omega$. Or, si $\omega \notin \Omega$, alors $\omega \in (\mathbf{R}^2)_T$. Comme $\varphi_T : \mathbf{R}^2 \rightarrow (\mathbf{R}^2)_T$ est homéomorphisme, (p_n) tend vers $\varphi_T^{-1}(\omega)$. Mais ceci est impossible.

(2) Pour simplifier la notation, on suppose que (q_n) converge vers ω et que $\omega \in (\mathbf{R}^2)_X$. Donc, $\omega = (0 : 1 : b)$. Comme $(\mathbf{R}^2)_X$ est ouvert, on peut supposer que $(q_n) \subset (\mathbf{R}^2)_X$. Comme $q_n \in (\mathbf{R}^2)_T$ également, l'on a $q_n = (a_n : 1 : b_n)$ et $a_n \neq 0$. De plus, $\lim a_n = 0$ et $\lim b_n = b$.

On écrit $f = \sum_0^d f_i$ avec f_i homogène de degré i , $d > 0$ et $f_d \neq 0$. Or, $q_n = \varphi_T(a_n^{-1}, b_n a_n^{-1})$ et donc

$$\begin{aligned} 0 &= a_n^d f(a_n^{-1}, a_n^{-1} b_n) \\ &= \sum_i a_n^{d-i} f_i(1 : b_n). \end{aligned}$$

Passant à la limite, $0 = f_d(1, b)$, et $Y - bX \mid f_d$. □

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].

Cours 11

(31/3/23).

La clôture projective

On souhaite maintenant passer de k^2 à \mathbf{P}^2 à l'aide de $(k^2)_T = \{1\} \times k^2$. Soit $C = \mathcal{Z}(f)$, qu'on regarde comme un sous-ensemble de $k^2 = (k^2)_T$. 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 $F \in k[T, X, Y] \setminus k$ donne lieu à un "cône" $\{(t, x, y) \mid F(t, x, y) = 0\}$.

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

Pour bien saisir les propriétés des objets projectifs, on doit faire appel à la notion de cône. Soit $S \subset \mathbf{P}^2$ un sous-ensemble. On introduit son cône

$$\begin{aligned} \widehat{S} &= \{P \in k^3 : \text{il existe } \Delta \in S \text{ telle que } P \in \Delta\} \\ &= \end{aligned}$$

Lemme 93. (1) Soient $P, Q \in \mathbf{P}^2$ des points distincts. Il existe une unique droite projective D les contenant.

(2) Soient L et M des droites projectives. Alors $L \cap M$ est un singleton.

Démonstration. (1) Soit $\Pi \subset k^3$ le sous-espace engendré par les droites P et Q : il s'agit d'un plan. Soit $\ell \in k[T, X, Y]$ homogène de degré 1 tels que $\Pi = \{(t, x, y) \in k^3 : \ell(t, x, y) = 0\}$. Il est clair que $\mathcal{Z}(\ell) \subset \mathbf{P}^2$ est une droite qui passe par P et Q . De plus, si $m \in k[T, X, Y]$ est homogène de degré 1 et m s'annule sur les droites P et Q , il est clair que $\Pi = \{(t, x, y) \in k^3 : m(t, x, y) = 0\}$ et il existe une constante $\lambda \in k^*$ telle que $\lambda \ell = m \Rightarrow \mathcal{Z}(\ell) = \mathcal{Z}(m)$.

(2) Il est clair que \widehat{L} et \widehat{M} se coupent le long d'une droite D , qui donne le point $L \cap M$. □

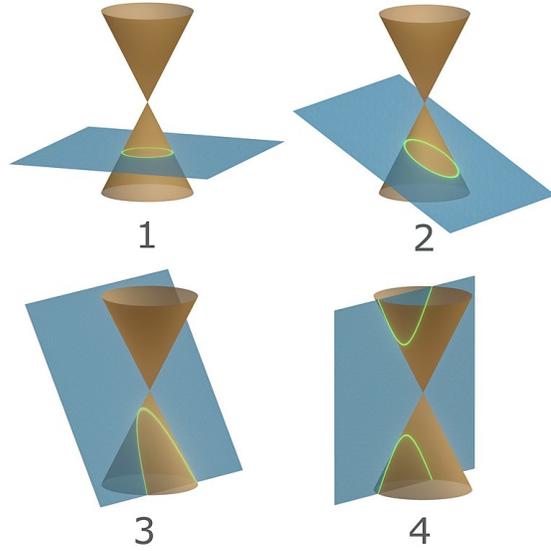


FIGURE 4 – Sections coniques

À chaque courbe plane on peut maintenant associer une courbe projective à l'aide de l'homogénéisation.

Définition 94 (Homogénéisation et clôture). 1) Soit $f \in k[X, Y]$ de degré $d \geq 1$. Si $f = \sum_{i=0}^d f_i$ avec f_i homogène de degré i , on définit son homogénéisation comme étant

$$f^\sim(T, X, Y) = f_d T^0 + f_{d-1} T^1 + \cdots + f_0 T^d.$$

2) 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 .

3) Les points de $\overline{C} \cap \Omega$ sont les points à l'infini.

Exemple 95. Soient $g = X^2 + Y^2 - 1$ et $C = \mathcal{Z}(g) \subset \mathbf{R}^2$ le cercle unitaire. Donc $\tilde{g} = X^2 + Y^2 - T^2$ et $\overline{C} = \mathcal{Z}(X^2 + Y^2 - T^2)$. Maintenant,

$$\varphi_X^{-1}(\overline{C} \cap (\mathbf{R}^2)_X) = \{(t, y) \in \mathbf{R}^2 : (t - y)(t + y) = 1;\}$$

il s'agit d'une hyperbole. Ceci se voit à l'aide du cône $\widehat{C} = \{(t, x, y) \in \mathbf{R}^3 : \tilde{g}(t, x, y) = 0\}$. (Voir la Figure 4)

Exercice 96. Soit C une courbe plane. Alors $\#\overline{C} \cap \Omega < \infty$.

Cours 12

(14/4/23).

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.

Courbes en bone position, multiplicité d'intersection et le théorème de Bézout

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 *projectives* associées. Le fait que F et G sont premiers entre eux assure que l'ensemble $C \cap D$ est *fini*.

Soit

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

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. 79 assure que R est homogène de degré de .

Hypothèse 97. $Z = (0 : 0 : 1) \notin C \cap D$.

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 98. La fonction

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

est injective.

Comment comprendre cette hypothèse géométriquement ?⁸ Soit $\Omega' = \mathcal{Z}(Y)$. Clairement, $Z \notin \Omega'$. Pour chaque $P \in \mathbf{P}^2 \setminus \{Z\}$, soit \overline{ZP} l'unique droite projective passant par Z et P . Comme on est dans \mathbf{P}^2 , l'ensemble $\overline{ZP} \cap \Omega'$ est 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 98 en fait dit quelque chose de géométrique : pour $P, P' \in C \cap D$ distincts, les trois points Z, P, P' ne sont jamais *colinéaires*. De façon encore plus géométrique, puisque

$$\overline{PP'} = \{Q \in \mathbf{P}^2 : Q \subset P + P'\},$$

on voit que la condition que Z, P, P' ne soient pas projectivement colinéaires est que les droites Z, P, P' ne soient pas *coplanaires*. La fonction π est en fait la *projection à partir du point Z*.

Dans un souci d'économie, on dira que les courbes satisfaisant les Hypothèses 97 et 98 sont en *bonne position*. On va maintenant démontrer le Théorème de Bézout dans ce contexte. D'abord, un exemple :

Exemple 99. On suppose que $C \cap D \subset (k^2)_T$, c'est-à-dire, que chaque $P \in C \cap D$ s'écrit comme $P = (1 : x : y)$. Alors C et D sont en bonne position si et seulement si il n'y a aucun couple de points de $C \cap D$ sur une même droite *verticale*. Par exemple, si $F = X^2 + Y^2 - T^2$ et $G = X$, alors C et D ne sont pas en bonne position car $C \cap D = \{(1 : 0 : \pm 1)\}$.

Comme $F(0, 0, 1) = F_0 \in k$, on voit que $F_0 \neq 0$. Donc, la Proposition 79 assure que $R \neq 0$, car l'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 proportionnels.
- $\mu_j > 0$.

Soit $Q_j = (t_j : x_j) \in \mathbf{P}^1$ l'unique zéro de ℓ_j .

Lemme 100. $\{Q_1, \dots, Q_m\} = \text{Im}(\pi)$ et $\pi : C \cap D \rightarrow \mathcal{Z}(R)$ est une bijection.

Démonstration. Si $R(t_j, x_j) = 0 \Rightarrow$

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

8. 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 . (On se rappelle que $F_0 \in k^*$.) Donc $(t_j : x_j : y_j) \in C \cap D$ et $Q_j = \pi(t_j : x_j : y_j)$. Réciproquement, soit $P = (t : x : y) \in C \cap D$; on se rappelle que $(t, x) \neq (0, 0)$. 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 101. 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 102 (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".

Le théorème de Bézout pour des courbes générales

On se donne $F, G \in k[T, X, Y]$ et $C, D \subset \mathbf{P}^2$ comme avant, mais on se garde de supposer que C et D sont en bonne position. On souhaite ainsi définir la multiplicité d'intersection. L'idée est de déranger les courbes C et D pour qu'elles soient en bonne position. Pour cela, on a besoin de la :

Définition 103. Soit $\alpha \in \text{GL}_3(k)$. La transformation projective induite par α est la fonction $\mathbf{P}^2 \rightarrow \mathbf{P}^2$ définie par $L \mapsto \alpha(L)$ pour chaque $L \in \mathbf{P}^2$. Une fonction $\mathbf{P}^2 \rightarrow \mathbf{P}^2$ est une transformation projective si elle est de cette forme. Le groupe des transformations projectives sera désigné par \mathcal{P} dans la suite.⁹

Exercice 104 (L'analogie de la Prp. 64). Soit $\alpha = \begin{pmatrix} a & a' & a'' \\ b & b' & b'' \\ c & c' & c'' \end{pmatrix} \in \text{GL}_3(k)$. Montrer que

$\alpha^{-1}(\mathcal{Z}(H)) = \mathcal{Z}(\alpha^\# H)$, où $\alpha^\# : k[T, X, Y] \rightarrow k[T, X, Y]$ est le morphisme défini par

$$\begin{aligned} T &\longmapsto aT + a'X + a''Y \\ X &\longmapsto bT + b'X + b''Y \\ Y &\longmapsto cT + c'X + c''Y \end{aligned} .$$

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

Si, pour un certain $\alpha \in \text{GL}_3(k)$ les courbes $\alpha^{-1}(C)$ et $\alpha^{-1}(D)$ sont en bonne position, alors on pourra définir la multiplicité d'intersection. Le résultat suivant va dans cette direction.

Proposition 105. *Il existe un $\alpha \in \text{GL}_3(k)$ tel que $\alpha^{-1}C$ et $\alpha^{-1}D$ soient en bonne position.*

L'idée de la preuve consiste à regarder α comme "prenant tous les valeurs possibles." On introduit neuf variables $U, U', U'', V, \dots, W''$. Soient

$$\mathcal{O} = k[U, U', U'', V, \dots, W''] \quad \text{et} \quad K = \text{Fr}(\mathcal{O}).$$

On considère \mathbf{P}_K^2 l'ensemble des droites vectorielles de K^3 et on considère \mathbf{P}^2 comme étant contenu dans \mathbf{P}_K^2 .

Soient C_K et D_K les courbes dans \mathbf{P}_K^2 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 en fait une *égalité* :

$$C_K \cap D_K = C \cap D.$$

Soit

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

Il s'agit d'une matrice avec coefficients dans \mathcal{O} . Il n'est pas difficile de voir que $\det(A) \neq 0$ et que A est inversible comme matrice 3×3 ayant coefficients dans K . Il s'agit de la matrice *générique*. De plus, à partir de A on obtient une transformation projective

$$A : \mathbf{P}_K^2 \longrightarrow \mathbf{P}_K^2.$$

Avec ces notations, la preuve est plus simple. Elle servira également pour traiter le théorème central de cette partie, le Théorème ??.

Démonstration de la Prp 105. On fait appel à l'affirmation suivante.

Affirmation. $A^{-1}(C_K)$ et $A^{-1}(D_K)$ sont en bonne position.

Le point Z n'appartient pas à $A^{-1}(C_K) \cap A^{-1}(D_K)$. Autrement, $A^\#F$ et $A^\#G$ s'annulent sur Z . Mais

$$A^\#F(Z) = F(U'', V'', W'') \quad \text{et} \quad A^\#G(Z) = G(U'', V'', W'').$$

De cet argument on déduit la chose suivante. Si $\alpha = \begin{pmatrix} a & a' & a'' \\ b & b' & b'' \\ c & c' & c'' \end{pmatrix} \in \text{GL}_3(k)$ est tel que

$$F(a'', b'', c'') \neq 0 \Rightarrow \alpha^\#F(Z) \neq 0.$$

Soient P et Q des points de $C_K \cap D_K$. Soient $(p, p', p'') \in P \setminus \{0\}$ et $(q, q', q'') \in Q \setminus \{0\}$. Alors Z , $A^{-1}(P)$ et $A^{-1}(Q)$ sont colinéaires si et seulement si

$$\begin{vmatrix} p' & p'' \\ q' & q'' \end{vmatrix} U'' - \begin{vmatrix} p & p'' \\ q & q'' \end{vmatrix} V'' + \begin{vmatrix} p & p' \\ q & q' \end{vmatrix} W'' = 0.$$

Les points Z , $A^{-1}(P)$ et $A^{-1}(Q)$ sont colinéaires si et seulement si les points $A(Z)$, P et Q sont colinéaires, ce qui a lieu si et seulement si $A(Z) = (U'' : V'' : W'')$, P et Q sont contenues dans un même plan de K^3 . Ceci à lieu si et seulement si

$$\begin{aligned} 0 &= \begin{vmatrix} U'' & V'' & W'' \\ p & p' & p'' \\ q & q' & q'' \end{vmatrix} \\ &= \begin{vmatrix} p' & p'' \\ q' & q'' \end{vmatrix} U'' - \begin{vmatrix} p & p'' \\ q & q'' \end{vmatrix} V'' + \begin{vmatrix} p & p' \\ q & q' \end{vmatrix} W''. \end{aligned}$$

On observe que comme $P \neq Q$, alors au moins l'un parmi les coefficients du polynôme linéaire en U'' , V'' , W'' ci-dessus est non-nul.

En conclusion, si $P_1, \dots, P_m \in \mathbf{P}^2$ sont les points d'intersection, si $(p_i, p'_i, p''_i) \in P_i \setminus \{0\}$ et si

$$L_{i,j}(U'', V'', W'') := \begin{vmatrix} U'' & V'' & W'' \\ p_i & p'_i & p''_i \\ p_j & p'_j & p''_j \end{vmatrix}$$

alors, étant donnée $\alpha = \begin{pmatrix} a & a' & a'' \\ b & b' & b'' \\ c & c' & c'' \end{pmatrix} \in \text{GL}_3(k)$, une condition nécessaire et suffisante pour que $\alpha^{-1}(C)$ et $\alpha^{-1}(D)$ soient en bonne position est que

$$F(a'', b'', c'') \cdot \prod_{i \neq j} L_{i,j}(a'', b'', c'') \neq 0.$$

On déduit qu'un tel α existe. □