EXERCICES SUR LE THÉORÈME DE BEZOUT

Soit k un corps algébriquement clos. Étant donné un polynôme irréductible $f \in k[x,y]$ non nul et de degré strictement positif, la courbe affine associée est le lieu des zéros de f,

$$C = \{(x,y) \in k^2 : f(x,y) = 0\}.$$

Si f n'est pas irréductible, l'ensemble C ne prend pas en compte les multiplicités des facteurs irréductibles de f (*e.g.* $x^2 = 0$ si et seulement si $x = 0$). Pour garder trace de cela, on dira qu'une courbe plane affine est un polynôme en deux variables non nul et de degré strictement positif.

De manière analogue,une *courbe projective plane* est la donnée d'un polynôme homogène $f \in k[x_0, x_1, x_2]$ non nul de degré strictement positif, et son lieu des zéros est

$$C = \{[x_0 : x_1 : x_2] \in \mathbb{P}^2(k) : f(x_0, x_1, x_2) = 0\}.$$

Le but de cette feuille d'exercices est de montrer le théorème de Bezout : deux courbes planes *projectives* respectivement de degrés d, e n'ayant pas de composantes en commun (*i.e.* les polynômes qui les définissent ne partagent pas de facteurs irréductibles) se rencontrent exactement en de points, en tenant compte de la multiplicité.

La nécessité de considérer des courbes projectives et non pas affines se voit déjà pour des droites parallèles dans le plan : comme les peintres du XVème siècle l'avaient compris, deux droites parallèles se rencontrent à l'infini.

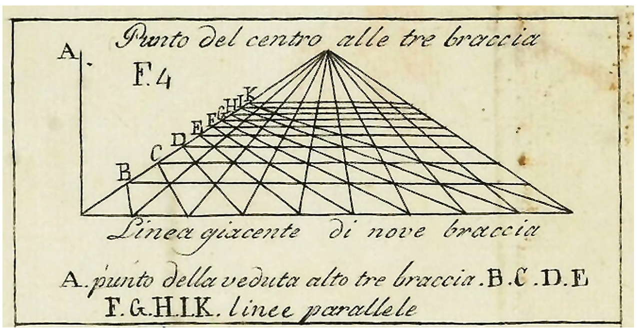

Figure 1. Leon Battista Alberti, *De pictura*, 1435

1. Rappels d'algèbre commutative

1.1. **Localisation.** Soit A un anneau. Une *partie multiplicative* de A est un sous-ensemble S contenant le produit 1 et stable par multiplication.

Definition 1.1. La *localisation* de A en un partie multiplicative S, notée $S^{-1}A$, est l'ensemble $A \times S$ modulo la relation d'équivalence suivante :

$$(a,s) \sim (a',s') \iff \text{il existe } t \in S \text{ tel que } t(as' - a's) = 0.$$

Si S ne contient pas de diviseur de zéro (*e.g.* si A est intègre et $0 \notin S$), la condition précédente est équivalente à $as' - a's = 0$. Dans ce cas on peut penser au couple (a,s) comme à la fraction $\frac{a}{s}$.

L'ensemble $S^{-1}A$ est muni des lois d'addition et multiplication suivantes, qui font de $S^{-1}A$ une A-algèbre :

$$(a,s)+(a',s')=(as'+a's,ss'),\qquad (a,s)\cdot(a',s')=(aa',ss').$$

Exercise 1.2. Soient A un anneau et S une partie multiplicative. Montrer les faits suivants :

(1) Tout élément de S est inversible dans $S^{-1}A$. Que se passe-t-il si $0\in A$?
(2) Soit $\varphi\colon A\to B$ un homomorphisme d'anneaux tel que l'image dans B de tout élément de S est inversible. Alors φ s'étend d'une manière et une seule à un homomorphisme de A-algèbres $S^{-1}A\to B$.
(3) Soit $\mathfrak{p}$ un idéal premier de A. Le sous-ensemble $S=A\setminus\mathfrak{p}$ est une partie multiplicative de A et $\mathfrak{p}S^{-1}A$ est l'unique idéal maximal de $S^{-1}A$. Un élément $f\in A$ est inversible dans $S^{-1}A$ si et seulement si $f\notin\mathfrak{p}$.

Definition 1.3. Pour un idéal premier $\mathfrak{p}$ d'un anneau A on désigne par $A_{\mathfrak{p}}$ la localisation $(A-\mathfrak{p})^{-1}A$.

Pour $f\in A$ et $S=\{f^n : n\in\mathbb{N}\}$ le localisé $S^{-1}A$ est noté A_f.

1.2. **Germes de fonctions régulières.** Soit k un corps algébriquement clos et $k[x_1,\dots,x_n]$ l'algèbre des polynômes en n-variables à coefficients dans k.

Definition 1.4. Étant donné $a=(a_1,\dots,a_n)\in k^n$, on considère l'idéal maximal $\mathfrak{m}_a=(x_1-a_1,\dots,x_n-a_n)$ et on pose

$$\mathcal{O}_{\mathbb{A}^n,a}:=k[x_1,\dots,x_n]_{\mathfrak{m}_a}.$$

Le cas de l'espace projectif est différent. Pour un polynôme homogène non nul $f\in k[x_0,\dots,x_n]$ on pose

$$k[x_0,\dots,x_n]_{(f)}=\left\{\frac{g}{f^r} : g\in k[x_0,\dots,x_n]\text{ homogène}, \deg(g)=r\deg(f)\right\}.$$

Il s'agit de l'anneau formé par les éléments de degré 0 de $k[x_0,\dots,x_n]_f$.

Definition 1.5. Pour un point $a=[a_0:\cdots:a_n]\in\mathbb{P}^n(k)$ on considère l'idéal maximal homogène $\mathfrak{m}_a$ de $k[x_0,\dots,x_n]$ engendré par les éléments $a_jx_i-a_ix_j$ pour $i,j=1,\dots,n$. On pose

$$\mathcal{O}_{\mathbb{P}^n,a}=\varinjlim_{f\notin\mathfrak{m}_a} k[x_0,\dots,x_n]_{(f)},$$

la relation d'ordre sur les éléments n'appartenant pas à l'idéal $\mathfrak{m}_a$ étant celle de divisibilité.

Si a_0 est non nul, on peut identifier $k[x_0,\dots,x_n]_{(x_0)}$ avec l'anneau des polynômes $k[\frac{x_1}{x_0},\dots,\frac{x_n}{x_0}]$ en les variables $\frac{x_i}{x_0}$. L'idéal de $k[\frac{x_1}{x_0},\dots,\frac{x_n}{x_0}]$ engendré par $\mathfrak{m}_a$ est l'idéal qui correspond au point $a^\flat=(\frac{a_1}{a_0},\dots,\frac{a_n}{a_0})\in k^n$. L'application naturelle $\mathcal{O}_{\mathbb{P}^n,a}\to\mathcal{O}_{\mathbb{A}^n,a^\flat}$ est un isomorphisme. Dans la suite on identifiera ces deux anneaux sans faire référence à l'isomorphisme qui précède.

1.3. **Anneaux artiniens.** Un anneau A est dit *artinien* si toute chaine déscendante d'idéaux est stationnaire.

Exercise 1.6. Montrer les faits suivants :

(1) Un anneau artinien A n'a qu'un nombre fini d'idéaux maximaux.
(2) Dans un anneau noethérien et artinien tout idéal premier est maximal.
(3) Un anneau noethérien A est artinien si et seulement s'il n'a qu'un nombre fini d'idéaux maximaux et il le produit des localisés de A à ses idéaux maximaux.

2. Le théorème de Bezout

2.1. **Nombres d'intersection.** Soient $f, g \in k[x, y]$ de polynômes non nuls et $p \in k^2$. On note C et D respectivement les lieux des zéros de f et g.

Definition 2.1. On dit que f et g se *rencontrent proprement* en p si f et g n'ont pas de facteur commun qui passe par p. On dit que f, g se rencontrent *rencontrent transversalement* si p est un point lisse de f et g et les tangentes sont distinctes.

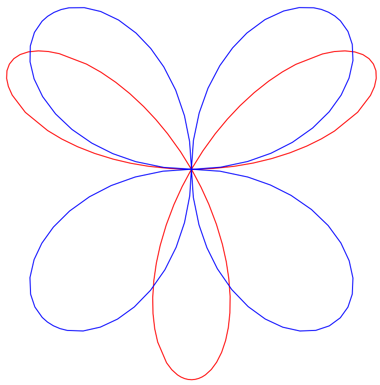

Figure 2. Intersection du *trifolium* et du *quadrifolium*.

Exercise 2.2. Supposons que f, g n'aient pas de facteurs commun. Montrer les faits suivants :

(1) f et g n'ont pas de facteurs commun en $k(x)[y]$.
(2) Il existe $d \in k[x]$ et $a, b \in k[x, y]$ tel que $af + bg = d$.
(3) $C \cap D$ est un ensemble fini. (Indication : répéter le raisonnement de (2) pour y).
(4) La k-algèbre $A := k[x, y]/(f, g)$ est noétherienne et artinienne.
(5) Le localisé de A en $\mathfrak{m}_p$ est de dimension finie sur k.

Definition 2.3. Supposons que f et g se rencontrent proprement en p. La *emultiplicité d'intersection* de f et g en p est

$$i_p(f, g) := \dim_k(\mathcal{O}_{\mathbb{A}^2,p}/(f, g)).$$

Exercise 2.4. Montrer les propriétés suivantes du nombres d'intersection :

(1) $i_p(f, g) = 0$ si et seulement si p n'appartient pas à $C \cap D$.
(2) Le nombre d'intersection est additif : si $f = \prod f_i^{r_i}$ et $g = \prod g_j^{s_j}$,
$$i_p(f, g) = \sum_{i,j} r_i s_j i_p(f_i, g_j).$$
En particulier $i_p(f, g)$ ne dépend que des composantes de f et g qui passent par p.
(3) Pour tout $a \in k[x, y]$, $i_p(f, g) = i_p(f, g + af)$.
(4) $i_p(f, g) \geqslant \operatorname{mult}_p(f) \operatorname{mult}_p(g)$ avec égalité si et seulement si f et g n'ont pas de droites tangentes en commun en p.

Exercise 2.5. Calculer la multiplicité d'intersection en l'origine $(0, 0)$ du *trifolium* et du *quadrifolium*, respectivement d'équations (voir Figure 2)

$$(x^2 + y^2)^3 - 4x^2y^2 = 0, \qquad (x^2 + y^2)^2 + 3x^2y - y^3 = 0.$$

2.2. **Énoncé et preuve du théorème de Bézout.** On se propose de démontrer le théorème suivant.

Theorem 2.6. *Soient $f, g \in k[x_0, x_1, x_2]$ des polynômes homogènes non nuls respectivement de degrés m, n strictement positifs. Supposons que f et g n'aient pas de facteurs en commun. Alors*

$$\sum_{p \in \mathbb{P}^2(k)} i_p(f, g) = mn.$$

On note C, D les lieux des zéros de f et g respectivement.

Exercise 2.7. Démontrer que le théorème de Bézout quand C est une droite.

Exercise 2.8. Montrer qu'il existe une droite de $\mathbb{P}^2$ qui ne rencontre pas $C \cap D$.

Quitte à faire un changement linéaire de coordonnées, on suppose que la droite d'équation $x_0 = 0$ ne rencontre pas $C \cap D$. On pose

$$\begin{aligned} f^\flat(x, y) &= f(1, x, y), & A &= k[x_0, x_1, x_2]/(f, g), \\ g^\flat(x, y) &= g(1, x, y), & A^\flat &= k[x, y]/(f^\flat, g^\flat), \\ & & R &= k[x_0, x_1, x_2]. \end{aligned}$$

Soit A_d l'image dans A de l'espace vectoriel des polynômes homogènes de degré d.

Exercise 2.9. Le but de cet exercice est de montrer que $\dim_k A_d = mn$ pour $d \geqslant m + n$. On considère la suite de R-modules,

$$(\star) \qquad 0 \longrightarrow R \xrightarrow{\psi} R \times R \xrightarrow{\varphi} R \xrightarrow{\pi} A \longrightarrow 0,$$

où $\psi(h) = (gh, -fh)$, $\varphi(a, b) = af + bg$ et π est la projection canonique. Prouver les faits suivants :

(1) La suite $(\star)$ est exacte et elle induit, pour tout $d \geqslant m + n$, une suite exacte
$$0 \longrightarrow R_{d-m-n} \xrightarrow{\psi} R_{d-m} \times R_{d-n} \xrightarrow{\varphi} R_d \xrightarrow{\pi} A_d \longrightarrow 0.$$
(2) $\dim_k R_d = \binom{d+2}{2}$.
(3) Conclure que $\dim_k A_d = mn$ pour $d \geqslant m + n$.

Exercise 2.10. On montre que l'application $\beta \colon A \to A$ définie par $\beta(h) = x_0 h$ est injective. Soient $a, b \in k[x_0, x_1, x_2]$ tels que $x_0 h = af + bg$. Montrer les faits suivants :

(1) Il existe $c \in k[x_1, x_2]$ tel que
$$b(0, x_1, x_2) = f(0, x_1, x_2)c(x_1, x_2), \qquad a(0, x_1, x_2) = -g(0, x_1, x_2)c(x_1, x_2).$$
(2) Il existe $a', b' \in k[x_0, x_1, x_2]$ tels que $a + cg = x_0 a'$ et $b - cf = x_0 b'$.
(3) Conclure que β est injective.

On fixe $d \geqslant m + n$ et une base $a_1, \ldots, a_{mn}$ de A_d. On pose $a_i^\flat(x, y) = a_i(1, x, y)$ pour $i = 1, \ldots, mn$.

Exercise 2.11. Le but de l'exercice est montrer que l'image de $a_1^\flat, \ldots, a_{mn}^\flat$ dans $A^\flat$ est une base de $A^\flat$ comme k-espace vectoriel.

(1) Montrer que, pour tout $r \geqslant 0$, les éléments de $x_0^r a_1, \ldots, x_0^r a_{mn}$ forment une base de A_{d+r}.
(2) Soit $h \in k[x, y]$. Montrer qu'il existe $\lambda_1, \ldots, \lambda_{mn} \in k$, $b, c \in k[x, y]$ tel que
$$h = \sum_{i=1}^{mn} \lambda_i a_i^\flat + bf + cg.$$

Soient $\mu_1, \dots, \mu_{mn} \in k$ tels que $\mu_1 a_1^\flat + \cdots + \mu_{mn} a_{mn}^\flat = 0$.

(3) Montrer qu'il existe des entiers positifs r, s, t et $b, c \in k[x_0, x_1, x_2]$ homogènes tels que
$$x_0^r \sum_{i=1}^{mn} \mu_i a_i = x_0^s bf + x_0^t cg.$$

(4) Conclure que les μ_i sont tous nuls.

3. Le théorème fondamental de Max Noether

Definition 3.1. Un 0-*cycle* sur $\mathbb{P}^2$ est une somme formelle
$$Z = \sum_{p \in \mathbb{P}^2(k)} m_p[p],$$
où m_p est un entier appelée la multiplicité de Z en p et noté $\mathrm{mult}_p(Z)$, et telle qu'il n'existe qu'un nombre fini de points p tels que m_p est non nul.

Étant donné un 0-cycle Z son *degré* est $\sum \mathrm{mult}_p(Z)$ et on dit qu'il est positif si $\mathrm{mult}_p(Z) \geqslant 0$ pour tout p. On dit qu'un 0-cycle Z est plus grand qu'un 0-cycle Z' si le 0-cycle $Z - Z'$ est positif.

Soient $f, g \in k[x_0, x_1, x_2]$ des polynômes homogènes non nuls de degrés strictement positif. On suppose que f, g n'aient pas de facteurs communs. Le *cycle d'intersection* de f est g est le 0-cycle
$$(f \cdot g) = \sum_{p \in \mathbb{P}^2(k)} i_p(f, g)[p].$$
D'après le théorème de Bézout on sait que son degré est $\deg(f)\deg(g)$.

Le but de cette partie est de montrer le théorème suivant :

Theorem 3.2. *Soient $f, g, h \in k[x_0, x_1, x_2]$ des polynômes homogènes non nul. On suppose que f et g n'aient pas de facteurs en commun. Alors les deux conditions suivantes sont équivalentes :*

(1) il existe $a, b \in k[x_0, x_1, x_2]$ homogènes tels que $h = af + bg$;

(2) pour tout point $p \in \mathbb{P}^2(k)$, la condition suivante est satisfaite :

(N_p) *l'image du polynôme h dans $\mathcal{O}_{\mathbb{P}^2,p}$ appartient à l'idéal engendré par f et g.*

Soient C, D les courbes projectives planes respectivement associées aux polynômes f et g. On remarque que la deuxième condition est vide lorsque le point p n'appartient pas à $C \cap D$. L'implication (1) $\Rightarrow$ (2) est triviale, donc on s'intéresse à montrer la réciproque.

Exercise 3.3. Montrer les faits suivants :

(1) On peut supposer que la droite d'équation $x_0 = 0$ ne rencontre pas $C \cap D$.

On définit $f^\flat(x, y) := f(1, x, y)$ et de manière analogue $g^\flat$ et $h^\flat$.

(2) Montrer que $h^\flat$ appartient à $k[x, y]/(f^\flat, g^\flat)$.

(3) Conclure. (Indication : utiliser l'exercice 2.10).

Exercise 3.4. Montrer que la condition (N_p) est satisfaite dans les cas suivants :

(1) f et g se rencontrent transversalement en p et $h(p) = 0$.

(2) p est un point lisse de f et $i_p(f, h) \geqslant i_p(f, g)$.

Exercise 3.5. Soient $f, g, h \in k[x_0, x_1, x_2]$ des polynômes homogènes de degré 3.

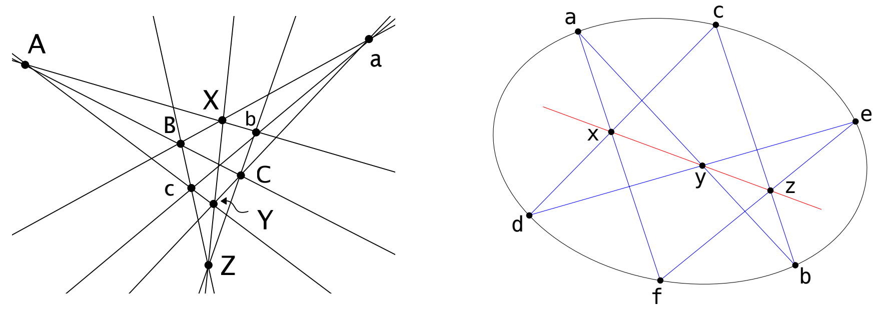

FIGURE 3. L'hexagone de Pappus à gauche et l'*Hexagrammum Mysticum* de Pascal à droite

(1) Supposons $(f \cdot g) = p_1 + \cdots + p_9$ où les points p_i sont des points lisses de f (mais pas forcément distincts) et $(f \cdot h) = p_1 + \cdots + p_8 + q$ pour un certain $q \in \mathbb{P}^2(k)$. Alors $q = p_9$. (Indication : on considérera une droite passant par p_9 qui ne contient pas q).

(2) En déduire le théorème de Pappus et l'existence de l'*Hexagrammum Mysticum* de Pascal (voir Figure 3).

4. Loi de groupe sur une cubique lisse

Soit $f \in k[x_0, x_1, x_2]$ un polynôme homogène de degré 3 irréductible tel que la courbe associée $C = \{[x_0 : x_1 : x_2] \in \mathbb{P}^2(k) : f(x_0, x_1, x_2) = 0\}$ soit lisse. On fixe un point $o \in C$.

Definition 4.1. Soient $p, q \in C$. On définit

$$p * q := (C \cdot L) - p - q,$$

où L est la droite passant par p et q si $p \neq q$, et L est la droite tangente à C en p si $p = q$. On pose aussi $\bar{p} = p * o$.

Exercise 4.2. Montrer que l'application $C \times C \to C$, $(p, q) \mapsto \overline{p * q}$ définit une loi de groupe commutative sur C. (Indication : pour l'associativité on utilisera l'exercice 3.4.)

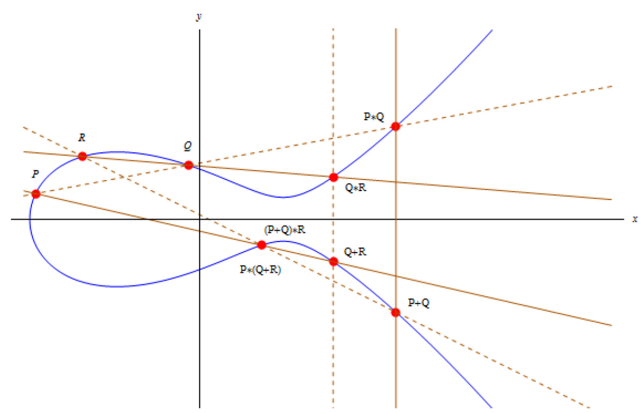

FIGURE 4. Associativité de la loi de groupe sur une courbe elliptique