Partie III
Plan projectif et courbes planes

Résumé. Cette partie définira de plusieurs façons le plan projectif sur un corps. Ensuite, l'intersection de droites et de courbes du plan projectif sera analysée pour aboutir au théorème de Bezout.

III.1 Le plan projectif $\mathbb{P}_2$

Définition 27. Soit un corps K. Le *plan projectif* $\mathbb{P}_2(K)$ est l'ensemble des points $P = (a, b, c) \neq (0, 0, 0) \in K^3$ de sorte que deux points $P = (a, b, c)$ et $P' = (a', b', c')$ sont considérés comme étant des points équivalents s'il existe $t \in K^*$ tel que $(a, b, c) = t(a', b', c')$. Les nombres a, b et c sont appelés les *coordonnées homogènes* du point P.

Plus généralement, nous définissons le *n-espace projectif* $\mathbb{P}_n(K)$ comme l'ensemble des classes d'équivalence des $(n+1)$-uples suivants :

$$\mathbb{P}_n(K) = \frac{\{(a_0, a_1, \ldots, a_n) \in K^{n+1} \mid a_0, a_1, \ldots, a_n \text{ non tous nuls}\}}{\sim},$$

où $(a_0, a_1, \ldots, a_n) \sim (a'_0, a'_1, \ldots, a'_n)$ s'il existe $t \in K^*$ tel que

$$(a_0, a_1, \ldots, a_n) = t(a'_0, a'_1, \ldots, a'_n).$$

Définition 28. Soit un corps K. Le degré d'un terme d'un polynôme p de l'anneau $K[X_1, \ldots, X_n]$ est la somme des exposants des variables X_i apparaissant dans ce terme. Le *degré du polynôme* p est le plus grand degré de ses termes.

Exemple 15. Le polynôme $p(X, Y, Z) = 3X^3Y + 4X^2Y^2Z - YZ^2$ est un polynôme de degré 5.

Définition 29. Soit un corps K. Un polynôme $p \in K[X_1, \ldots, X_n]$ est un polynôme *homogène* de degré d si chacun de ses termes est de degré d. De plus, p est dit *irréductible* s'il ne peut pas s'écrire comme le produit non trivial de deux polynômes de $K[X_1, \ldots, X_n]$.

Notation. Si p est un polynôme homogène de degré d défini sur un corps K et à n variables, alors nous écrirons $p \in K[X_1, \ldots, X_n]_d$.

Proposition 30. *Soient un corps K et un polynôme non nul $p(X_1, \ldots, X_n)$ à coefficients dans K. Alors, p est est un polynôme homogène de degré $d > 0$ si et seulement si, pour une variable auxiliaire t,*

$$p(tX_1, \ldots, tX_n) = t^d p(X_1, \ldots, X_n). \tag{III.1}$$

Preuve. La condition nécessaire est évidente. Démontrons la condition suffisante. Écrivons p comme une somme de polynômes homogènes non nuls de degré d_i :

$$p = p_{d_1} + p_{d_2} + \cdots + p_{d_k}, \quad d_1 < d_2 < \cdots < d_k.$$

La relation (III.1) implique que

$$t^{d_1} p_{d_1} + t^{d_2} p_{d_2} + \cdots + t^{d_k} p_{d_k} = t^d p = t^d p_{d_1} + t^d p_{d_2} + \cdots + t^d p_{d_k},$$

et donc, $t^{d_i} = t^d$ pour tout i. Par conséquent, $k = 1$ car $d_1 < d_2 < \cdots < d_k$, et $p = p_{d_1} = p_d$. □

Corollaire 31 (Formule d'Euler). *Si $F \in K[X_1, \ldots, X_n]_d$ est un polynôme homogène de degré d défini sur un corps K, alors*

$$\sum_{i=1}^{n} X_i \frac{\partial F}{\partial X_i} = d \cdot F.$$

Preuve. La proposition 30 donne $F(tX_1, \ldots, tX_n) = t^d F(X_1, \ldots, X_n)$. En dérivant par rapport à t, il vient que

$$\sum_{i=1}^{n} X_i \frac{\partial F}{\partial X_i}(tX_1, \ldots, tX_n) = d t^{d-1} F(X_1, \ldots, X_n).$$

Si nous prenons $t = 1$ dans la relation précédente, nous obtenons la thèse. □

Remarque. La dérivée d'un polynôme se définit de manière purement algébrique. Si $p(X) = \sum_{k=0}^{n} a_k X^k$ est un polynôme de l'anneau $K[X]$, alors

$$\left(\sum_{k=0}^{n} a_k X^k \right)' = \sum_{k=1}^{n} a_k k X^{k-1}.$$

Définition 32. Soit un corps K. Une *courbe* C de $\mathbb{P}_2(K)$ est l'ensemble des points qui satisfait à

$$p(X, Y, Z) = 0,$$

où $p \in K[X, Y, Z]_d$ est un polynôme homogène de degré $d \geq 1$. Si $d = 1$, alors C est appelée une droite ; si $d = 2$, une conique ; si $d = 3$, une cubique, etc... Le nombre d est appelé le *degré* de la courbe.

Le plan usuel (x, y) sur un corps K, encore appelé *plan affine* et noté $\mathbb{A}_2(K)$, est l'ensemble des point $(x, y) \in K^2$. Si nous introduisons les coordonnés X, Y, Z telles que $x = X/Z$ et $y = Y/Z$, alors à tout point (x, y) de $\mathbb{A}_2(K)$ correspond le point (X, Y, Z) de $\mathbb{P}_2(K)$. Réciproquement, si $Z \neq 0$, alors à tout point (X, Y, Z) de $\mathbb{P}_2(K)$ correspond le point (x, y) de $\mathbb{A}_2(K)$. Voyons à présent ce qui se passe quand $Z = 0$. Considérons, dans $\mathbb{A}_2(K)$, deux droites parallèles $L : ax+by+c = 0$ et $L' : a'x+b'y+c = 0$ où $a' = ta$ et $b' = tb$. En coordonnées homogènes, c.-à-d. dans $\mathbb{P}_2(K)$, ces droites s'écrivent $L : aX + bY + cZ = 0$ et $L' : a'X + b'Y + c'Z = 0$. L'intersection de ces droites a lieu en un point pour lequel $Z = 0$. Un tel point est appelé *point à l'infini*. Cela permet de donner une nouvelle définition de $\mathbb{P}_2(K)$:

$$\mathbb{P}_2(K) = \mathbb{A}_2(K) \cup \{\text{l'ensemble des directions dans } \mathbb{A}_2(K)\}.$$

Nous voyons donc que l'introduction des coordonnées homogènes n'oblige plus à faire la distinction entre droites parallèles ou non : deux droites distinctes s'intersectent en un point unique comme le montre la proposition 34.

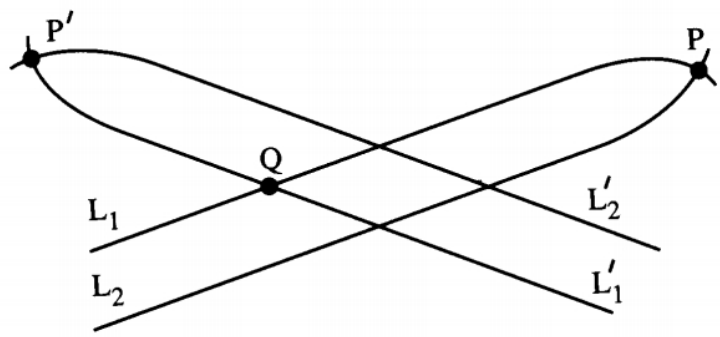

Figure 1: Intersection de droites parallèles.

Lemme 33 (Théorème du rang). *Soient V un espace vectoriel de dimension finie, W un espace vectoriel quelconque et $T : V \to W$ une application linéaire. Alors,*

$$\dim \operatorname{Ker} T + \dim \operatorname{Im} T = \dim V.$$

Preuve. Dans la suite, nous avons uniquement besoin du cas où W est de dimension finie ; nous allons donc uniquement démontrer le lemme avec cette hypothèse supplémentaire. Soient $\{v_1, \ldots, v_p\}$ et $\{w_1, \ldots, w_q\}$ des bases respectives de $\operatorname{Ker} T$ et de $\operatorname{Im} T$.
(i) Par définition de $\operatorname{Im} T$, $\exists y_i \in V$ tel que $T(y_i) = w_i$. Montrons que les

vecteurs $y_1, \ldots, y_q$ sont linéairement indépendants. Par l'absurde, si $\alpha_1 y_1 + \cdots + \alpha_q y_q = 0$, alors

$$T\left(\sum_{i=1}^{q} \alpha_i y_i\right) = \sum_{i=1}^{q} \alpha_i T(y_i) = \sum_{i=1}^{q} \alpha_i w_i = T(0) = 0.$$

Par conséquent, $w_1, \ldots, w_q$ sont linéairement dépendants et ne forment pas une base.
(ii) Montrons que $\{v_1, \ldots, v_p, y_1, \ldots, y_q\}$ est une base de V. L'indépendance linéaire de $v_1, \ldots, v_p, y_1, \ldots, y_q$ se démontre de la même façon que pour $y_1, \ldots, y_q$. Il reste à démontrer le caractère générateur de $v_1, \ldots, v_p, y_1, \ldots, y_q$, i.e. $\forall x \in V, \exists \alpha_i, \beta_i$ tels que $x = \sum_{i=1}^{p} \alpha_i v_1 + \sum_{i=1}^{q} \beta_i y_i$. Or, étant donné que $\{w_1, \ldots, w_q\}$ est une base de $\operatorname{Im} T$,

$$T(x) = \sum_{i=1}^{q} \beta_i w_i = \sum_{i=1}^{q} \beta_i T(y_i) = T\left(\sum_{i=1}^{q} \beta_i y_i\right),$$

et donc $x - \sum_{i=1}^{q} \beta_i y_i \in \operatorname{Ker} T$ et est une combinaison linéaire de $v_1, \ldots, v_p$; ce qui signifie que x est une combinaison linéaire de $v_1, \ldots, v_p, y_1, \ldots, y_q$. □

Proposition 34. *Soient un corps K et deux droites distinctes*

$$L : aX + bY + cZ = 0 \quad \textit{et} \quad L' : a'X + b'Y + c'Z = 0$$

de $\mathbb{P}_2(K)$. Alors L et L' ont un unique point d'intersection. De plus, deux points distincts de $\mathbb{P}_2(K)$ définissent une et une seule droite.

Preuve. (i) Considérons l'application linéaire

$$T : \mathbb{P}_2(K) \to \mathbb{P}_2(K), \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} \mapsto \begin{pmatrix} a & b & c \\ a' & b' & c' \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix},$$

alors, comme L et L' sont distinctes, le rang de la matrice des coefficients vaut 2, et donc le noyau est de dimension $(3 - 2) = 1$.
(ii) Soient $P_1 = (a_1, b_1, c_1)$ et $P_2 = (a_2, b_2, c_2)$ deux points distincts de L et l'application linéaire

$$T : \mathbb{P}_2(K) \to \mathbb{P}_2(K), \begin{pmatrix} a \\ b \\ c \end{pmatrix} \mapsto \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix}.$$

Comme P_1 et P_2 sont distincts, la matrice des coordonnées des points est de rang 2, et donc le noyau est de dimension 1. □

Revenons à la définition de $\mathbb{P}_2(K)$. Toute droite de $\mathbb{A}_2(K)$ est parallèle à une droite passant par l'origine de la forme $L : ax = by$. Cependant, si $(a', b') = (ta, tb)$, alors la droite $L' : a'x = b'y$ est la même droite que L. Par conséquent, l'ensemble des directions de $\mathbb{A}_2(K)$ est donné par les points (a, b) de la droite projective $\mathbb{P}_1(K)$. Nous avons alors

$$\mathbb{P}_2(K) = \mathbb{A}_2(K) \cup \mathbb{P}_1(K).$$

III.2 Intersections et théorème de Bezout

III.2.1 Intersection d'une droite et d'une courbe

Étudions l'intersection d'une droite L et d'une courbe C de degré d dans $\mathbb{P}_2$ définies sur un corps K. Dans un premier temps, nous allons supposer que K est un corps de caractéristique nulle[†] ou de caractéristique $p > d$. Fixons les notations :

$$C : F(X, Y, Z) = 0.$$

Nous savons que deux points distincts définissent une droite. Soient $P_1 = (a_1, b_1, c_1)$ et $P_2 = (a_2, b_2, c_2)$ deux points distincts de la droite L, alors L peut se paramétriser sous la forme

$$L : \begin{cases} X = sa_1 + ta_2 \\ Y = sb_1 + tb_2 \\ Z = sc_1 + tc_2 \end{cases}.$$

Les points d'intersection de la droite et de la courbe sont donc donnés par

$$F(sa_1 + ta_2, sb_1 + tb_2, sc_1 + tc_2) = 0. \tag{III.2}$$

Le point d'intersection P_1 correspond à $s = 1$ et $t = 0$. Considérons cette fonction comme une fonction de t et notons-la $f(t)$. Le développement en série de Mac-Laurin donne

$$f(t) = f(0) + \frac{f'(0)}{1!}t + \frac{f''(o)}{2!}t^2 + \cdots + \frac{f^{(d)}}{d!}t^d.$$

Définition 35. Nous dirons que L intersecte C en P_1 avec un *ordre* m si $f^{(m)}(0) \neq 0$ et si $f^{(l)}(0) = 0$ pour $l < m$.

Notation. Si P est un point d'intersection d'ordre m entre une droite L et une courbe C, alors nous notons $I(P, L, C) = m$. Par convention, si $P \notin L \cap C$, alors $I(P, L, C) = 0$.

[†]Cela signifie que K est infini.

Supposons que P_1 soit un point d'ordre $m \geq 2$. Cela signifie que $f'(0) = 0$ et donc, par (III.2), que

$$\left.\frac{\partial F}{\partial X}\right|_{P_1} a_2 + \left.\frac{\partial F}{\partial Y}\right|_{P_1} b_2 + \left.\frac{\partial F}{\partial Z}\right|_{P_1} c_2 = 0. \tag{III.3}$$

Définition 36. Un point P d'une courbe $C : F(X, Y, Z) = 0$ est dit *singulier* si

$$\left.\frac{\partial F}{\partial X}\right|_{P} = \left.\frac{\partial F}{\partial Y}\right|_{P} = \left.\frac{\partial F}{\partial Z}\right|_{P} = 0;$$

sinon P est dit *non singulier* ou *simple*. De plus, la courbe C est appelée *courbe non singulière* si tous ses points sont simples.

Supposons que P_1 soit un point non singulier. La relation (III.3) implique que le point $P_2 = (a_2, b_2, c_2)$ appartient à la droite

$$\left.\frac{\partial F}{\partial X}\right|_{P_1} X + \left.\frac{\partial F}{\partial Y}\right|_{P_1} Y + \left.\frac{\partial F}{\partial Z}\right|_{P_1} Z = 0. \tag{III.4}$$

Par le corollaire 31, le point $P_1 = (a_1, b_1, c_1)$ appartient également à cette droite. La relation (III.4) définit la *tangente* à la courbe C au point (simple) P_1.

Si K est un corps de caractéristique $p \leq d$, alors la formule de Mac-Laurin n'est plus applicable. En gardant les mêmes notations que ci-dessus, nous pouvons écrire f comme un polynôme en T, i.e.

$$f(t) = k_0 + k_1 t + \cdots + k_d t^d.$$

La seule différence avec ce qui précède est que nous ne pouvons plus exprimer les coefficients k_i sous la forme $\frac{f^{(i)}(0)}{i!}$. Nous dirons que le point P_1 est un *point d'ordre* m si $k_m \neq 0$ et si $k_l = 0$ pour $l < m$; les autres définitions restant les mêmes.

Lemme 37. *Soient un point P, une droite L et deux courbes C_1 et C_2. Alors*

$$I(P, L, C_1 C_2) = I(P, L, C_1) + I(P, L, C_2).$$

Preuve. Trivial. □

Lemme 38. *Soient un point P, une droite L et deux courbes C_1 et C_2. Si C_1 et C_2 ont le même degré et si $C_1 + C_2 \neq 0$, alors*

$$I(P, L, C_1 + C_2) \geq \min\{I(P, L, C_1), I(P, L, C_2)\}.$$

Preuve. Trivial. □

Proposition 39. *Si $F(X,1,0)$ est un polynôme en X et si $L : Z = 0$ est la droite à l'infini, alors $I((r,1,0), L, F)$ est égal à la multiplicité de r comme racine de $F(X,1,0)$.*

Preuve. Soit la transformation linéaire

$$T : \mathbb{P}_2 \to \mathbb{P}_2, \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} \mapsto \begin{pmatrix} X' \\ Y' \\ Z' \end{pmatrix} = \begin{pmatrix} 1 & -r & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix},$$

qui envoie le point $(r,1,0)$ en $(0,0,1)$ et dont l'inverse est donnée par

$$T^{-1} : \mathbb{P}_2 \to \mathbb{P}_2, \begin{pmatrix} X \\ Y \\ Z \end{pmatrix} \mapsto \begin{pmatrix} X' \\ Y' \\ Z' \end{pmatrix} = \begin{pmatrix} 1 & 0 & r \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix} \begin{pmatrix} X \\ Y \\ Z \end{pmatrix}.$$

Notons

$$\begin{aligned} f(X,Y) &= F(T^{-1}(X,Y,1)) = F(X+r,1,Y), \\ l(X,Y) &= L(T^{-1}(X,Y,1)) = Y. \end{aligned}$$

Donc, $l(X,Y)$ est de la forme $bX - aY$ avec $b = 0$ et $a = -1$ que nous pouvons paramétriser par $\phi(t) = \begin{pmatrix} at \\ bt \end{pmatrix} = \begin{pmatrix} -t \\ 0 \end{pmatrix}$ et

$$f(\phi(t)) = f(-t,0) = F(-t+r,1,0).$$

$I((r,1,0), L, F)$ est alors donné par l'ordre de la racine de $f(\phi(t))$ en $t = 0$, soit encore par l'ordre de la racine de $F(-t+r,1,0)$ en $t = 0$, ce qui est égal à la multiplicité de r comme racine de $F(X,1,0)$. □

III.2.2 Théorème de Bezout

Le théorème de Bezout apparaît sous plusieurs formes en géométrie algébrique. Nous allons uniquement présenter une version faible de ce théorème.

Définition 40. Soit un corps K. Le *résultant*, noté $R(f,g)$, de deux polynômes f et $g \in K[X]$ est le déterminant

$$R(f,g) = \left|\begin{array}{c} \left.\begin{array}{cccccccccc} a_n & a_{n-1} & \dots & \dots & a_1 & a_0 & 0 & \dots & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_2 & a_1 & a_0 & 0 & \dots & 0 \\ 0 & 0 & \ddots & \ddots & & \ddots & \ddots & \ddots & & 0 \\ \dots & & & & & & & & & \end{array}\right\} m \text{ lignes} \\ \left.\begin{array}{cccccccccc} b_m & b_{m-1} & \dots & \dots & b_1 & b_0 & 0 & \dots & \dots & 0 \\ 0 & b_m & b_{m-1} & \dots & b_2 & b_1 & b_0 & 0 & \dots & 0 \\ 0 & 0 & \ddots & \ddots & & \ddots & \ddots & \ddots & & 0 \\ \dots & & & & & & & & & \end{array}\right\} n \text{ lignes} \end{array}\right| ,$$

si

$$f(X) = \sum_{i=0}^{n} a_i X^i \quad \text{et} \quad g(X) = \sum_{i=0}^{m} b_i X^i.$$

Lemme 41. *Soit un corps K. Deux polynômes f et $g \in K[X]$ ont un facteur non constant en commun si et seulement si il existe des polynômes non nuls ϕ et $\psi \in K[X]$ de degré respectivement strictement inférieur à celui de f et à celui de g tels que $\psi f = \phi g$.*

Preuve. ($\Rightarrow$) Si f et g ont un facteur commun h, alors $f = h\phi$, $g = h\psi$ et $\psi f = \phi g$.
($\Leftarrow$) Si $\psi f = \phi g$, alors tout facteur irréductible de g divise soit ψ, soit f. Or, comme le degré de ϕ est strictement inférieur à celui de g, au moins un des facteurs irréductibles de g divise f. □

Théorème 42. *Soit un corps K. Deux polynômes f et $g \in K[X]$ donnés par*

$$f(X) = \sum_{i=0}^{n} a_i X^i \quad et \quad g(X) = \sum_{i=0}^{m} b_i X^i$$

ont un facteur non constant en commun si et seulement si

$$R(f,g) = \begin{vmatrix} a_n & a_{n-1} & \dots & \dots & a_1 & a_0 & 0 & \dots & \dots & 0 \\ 0 & a_n & a_{n-1} & \dots & a_2 & a_1 & a_0 & 0 & \dots & 0 \\ 0 & 0 & \ddots & \ddots & & \ddots & \ddots & \ddots & & 0 \\ \dots & & & & & & & & & \\ b_m & b_{m-1} & \dots & \dots & b_1 & b_0 & 0 & \dots & \dots & 0 \\ 0 & b_m & b_{m-1} & \dots & b_2 & b_1 & b_0 & 0 & \dots & 0 \\ 0 & 0 & \ddots & \ddots & & \ddots & \ddots & \ddots & & 0 \\ \dots & & & & & & & & & \end{vmatrix} = 0.$$

Preuve. ($\Rightarrow$) Par le lemme précédent, $\exists \phi$ et $\psi \in K[X]$ tels que $\psi f = \phi g$ où

$$\phi(X) = \sum_{i=0}^{n-1} \alpha_i X^i \quad \text{et} \quad \psi(X) = \sum_{i=0}^{m-1} \beta_i X^i$$

avec au moins un $\alpha_i \neq 0$ et un $\beta_i \neq 0$. Il s'ensuit que

$$\begin{array}{lll}
a_0\beta_0 & = b_0\alpha_0, & \\
a_1\beta_0 + a_0\beta_1 & = b_1\alpha_0 + b_0\alpha_1, & \\
a_2\beta_0 + a_1\beta_1 + a_0\beta_2 & = b_2\alpha_0 + b_1\alpha_1 + b_0\alpha_2\ , & \\
\vdots & \vdots & \\
a_n\beta_{m-1} = & & b_m\alpha_{n-1}.
\end{array}$$

Si nous considérons ce système comme un système homogène de $m+n$ équations à $m+n$ variables, nous avons une solution non triviale

$$(\beta_0, \ldots, \beta_{m-1}, \alpha_0, \ldots, \alpha_{n-1}).$$

Le déterminant du système est donc nul et par conséquent $R(f,g) = 0$.
($\Leftarrow$) Si $R(f,g) = 0$, alors il existe un α_i ou un β_i différent de 0. Si $\alpha_i \neq 0$, alors $\phi \neq 0$, et $\psi f = \phi g$ avec $\phi \neq 0$ et donc $\psi \neq 0$. □

Lemme 43. *Soit un corps K. Si F et $G \in K[X,Y,Z]$ sont deux courbes de degré respectif n et m vues comme des polynômes en l'unique variable Z à coefficients dans l'anneau $K[X,Y]$, alors le résultant de F et de G par rapport à Z, noté $R(X,Y)$, est soit nul, soit un polynôme homogène de degré mn.*

Preuve. Soient

$$\begin{aligned}
F(X,Y,Z) &= A_0(X,Y)Z^n + A_1(X,Y)Z^{n-1} + \cdots + A_n(X,Y), \\
G(X,Y,Z) &= B_0(X,Y)Z^m + B_1(X,Y)Z^{m-1} + \cdots + B_m(X,Y),
\end{aligned}$$

où $A_i(X,Y)$ et $B_i(X,Y)$ sont des polynômes homogènes de degré i. Alors,

$$R(tX,tY) = \begin{vmatrix}
A_0 & tA_1 & \ldots & t^nA_n & 0 & \ldots & 0 \\
0 & A_0 & tA_1 & \ldots & t^nA_n & & 0 \\
\vdots & & \ddots & \ddots & & \ddots & \vdots \\
0 & 0 & 0 & A_0 & tA_1(X,Y) & \ldots & t^nA_n \\
B_0 & tB_1 & \ldots & t^mB_m & 0 & \ldots & 0 \\
0 & B_0 & tB_1 & \ldots & t^mB_m & & 0 \\
\vdots & & \ddots & \ddots & & \ddots & \vdots \\
0 & 0 & 0 & B_0 & tB_1 & \ldots & t^mB_m
\end{vmatrix}.$$

Si nous multiplions la $i^{\text{ième}}$ ligne par t^{i-1} et la $(m+j)^{\text{ième}}$ ligne par t^{j-1}, nous obtenons

$$\begin{aligned} t^{\alpha}R(tX,tY) &= \begin{vmatrix} A_0 & tA_1 & \dots & t^nA_n & 0 & \dots & 0 \\ 0 & tA_0 & t^2A_1 & \dots & t^{n+1}A_n & & 0 \\ \vdots & & \ddots & \ddots & & \ddots & \vdots \\ 0 & 0 & 0 & t^{m-1}A_0 & t^mA_1(X,Y) & \dots & t^{n+m-1}A_n \\ B_0 & tB_1 & \dots & t^mB_m & 0 & \dots & 0 \\ 0 & tB_0 & t^2B_1 & \dots & t^{m+1}B_m & & 0 \\ \vdots & & \ddots & \ddots & & \ddots & \vdots \\ 0 & 0 & 0 & t^{n-1}B_0 & t^nB_1 & \dots & t^{m+n-1}B_m \end{vmatrix} \\ &= t^{\beta}R(X,Y), \end{aligned}$$

où la deuxième égalité est obtenue en mettant t^i en évidence dans la $(i+1)^{\text{ième}}$ colonne. Nous avons donc

$$\alpha = (1+2+\cdots+(m-1)) + (1+2+\cdots+(n-1)) = \frac{(m-1)m}{2} + \frac{(n-1)n}{2}$$

et

$$\beta = 1+2+\cdots+(m+n-1) = \frac{(m+n-1)(m+n)}{2}.$$

Comme $\beta - \alpha = mn$, $R(tX,tY) = t^{mn}R(X,Y)$, et donc, par la proposition 30, $R(X,Y)$ est soit un polynôme de degré mn, soit un polynôme nul. □

Théorème 44 (Théorème faible de Bezout). *Soit un corps infini K. Si $F \in K[X,Y,Z]_m$ et $G \in K[X,Y,Z]_n$ sont deux courbes ayant plus de mn points communs, alors F et G ont un facteur non constant en commun.*

Preuve. Les courbes F et G ont au moins $mn+1$ points en commun ; joignons chaque paire de points par une droite. Comme le nombre de droites est fini et que K est infini, il existe un point P qui n'appartient à aucune de ces droites, ni à F, ni à G. Choisissons un système de coordonnées homogènes tel que $P = (0,0,1)$. Nous pouvons considérer F et G comme des polynômes en Z :

$$\begin{aligned} F(X,Y,Z) &= A_0(X,Y)Z^m + A_1(X,Y)Z^{m-1} + \cdots + A_m(X,Y), \\ G(X,Y,Z) &= B_0(X,Y)Z^n + B_1(X,Y)Z^{n-1} + \cdots + B_n(X,Y), \end{aligned}$$

où $A_i(X,Y)$ et $B_i(X,Y)$ sont des polynômes homogènes de degré i. Par le lemme 43, le résultant de F et de G par rapport à Z, i.e. $R(X,Y)$, est soit un polynôme nul, soit un polynôme de degré mn. Notons (a,b,c) un des

$mn + 1$ points d'intersection. Ce point appartient à $F \cap G$, ce qui signifie que $F(a, b, Z)$ et $G(a, b, Z)$ ont une racine commune c. Par conséquent, $R(a, b) = 0$. Comme aucun des couples (a, b) correspondant aux $mn + 1$ points d'intersection ne sont proportionnels (car ils ne sont pas colinéaires à $P = (0, 0, 1)$), $R(X, Y)$ ne peut pas être de degré mn. Il vient donc que $R(X, Y) = 0$ et, par le théorème 42, F et G ont un facteur non constant en commun. □

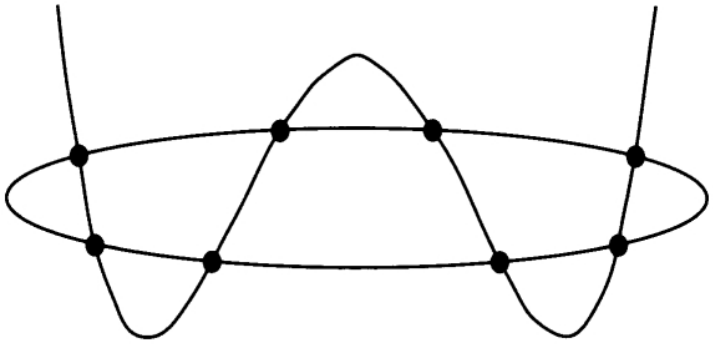

Figure 2: Intersection d'une courbe de degré 4 et d'une courbe de degré 2.

Corollaire 45. *Soit un corps infini K. Si $C \in K[X, Y.Z]_d$ est une courbe et si L est une droite telle que $\sum_{P \in L} I(P, L, C) > d$, alors L divise C.*

Preuve. Par l'absurde, supposons que L ne divise pas C. Par le théorème 44, nous savons que C et L ont un nombre fini de points communs et, par conséquent, $\sum_{P \in L}(I, L, C)$ est fini. Montrons que $\sum_{P \in L} I(P, L, C) \leq d$. Par une transformation projective, nous pouvons supposer que L est la droite à l'infini $Z = 0$. En faisant éventuellement une translation sur la variable Y, nous pouvons également supposer que tous les points d'intersection ont une coordonnée en Y non nulle. Notons $P_i = (r_i, 1, 0)$ les points d'intersection de $C(X, 1, 0)$ avec $L : Z = 0$. Comme K est infini, il existe $(r, 1, 0)$ qui n'appartient pas à $C \cap L$ et donc, $C(X, 1, 0)$ est un polynôme non nul. Ce polynôme a donc au plus d racines comptées avec leur mutiplicité. Par conséquent, par la proposition 39, $\sum_{P \in L} I(P, L, C) \leq d$, ce qui est contraire à l'hypothèse. □

À retenir.

▶ Soit un corps K. Le *n-espace projectif* $\mathbb{P}_n(K)$ est l'ensemble des classes d'équivalence des $(n+1)$-uples

$$\mathbb{P}(K) = \frac{\{(a_0, a_1, \ldots, a_n) \mid a_0, a_1, \ldots, a_n \text{ non tous nuls}\}}{\sim},$$

où $(a_0, a_1, \ldots, a_n) \sim (a'_0, a'_1, \ldots, a'_n)$ si

$$(a_0, a_1, \ldots, a_n) = t(a_0, a_1, \ldots, a_n)$$

avec $t \in K\backslash\{0\}$. Si $n = 2$, alors $\mathbb{P}_2(K)$ est le *plan projectif*.

▶ Une *courbe* de $\mathbb{P}_2(K)$ est un polynôme homogène de degré $d \geq 1$ de l'anneau $K[X, Y, Z]$. Si $d = 1$, alors c'est une droite; si $d = 2$, une conique; si $d = 3$, une cubique.

▶ Un point P d'une courbe $C : F(X, Y, Z) = 0$ est un *point singulier* si

$$\left.\frac{\partial F}{\partial X}\right|_P = \left.\frac{\partial F}{\partial Y}\right|_P = \left.\frac{\partial F}{\partial Z}\right|_P = 0.$$

Une courbe dont tous les points sont non singuliers est une *courbe non singulière*.

▶ Une courbe est *irréductible* si elle ne peut pas s'écrire comme le produit non trivial de deux polynômes.