4. Courbes planes

Sauf mention du contraire, le corps k désigne un corps algébriquement clos.

4.1. **Le théorème de Bezout.** Commençons par l'étude d'un cas particulier. Soit $F \in k[X,Y]$ un polynôme de degré $d > 0$. Soit $D \subset \mathbb{A}^2_k$ une droite affine. On désire étudier l'intersection des parties $V(F)$ et D. Quitte à effectuer un changement de coordonnées, on peut supposer que $D = V(Y)$. On a donc

$$V(F) \cap D = \{(x,0),\, F(x,0) = 0\}$$

Il y a deux possibilités, soit Y divise F et $D \subset V(F)$, soit le polynôme $F(X,0)$ est non nul et a un nombre fini de zéros $x_1, \ldots, x_r$. On a alors

$$F(X,0) = \prod_{i=1}^{r} (X - x_i)^{m_i}$$

et m_i mérite bien le nom de *multiplicité d'intersection* de la droite D avec la courbe $V(F)$ au point $(x_i, 0)$. Il faut remarquer que la somme des multiplicités d'intersections $\sum_{i=1}^{r} m_i$ est égale au degré du polynôme $F(X,0)$ qui est inférieure à d, mais peut parfois être strictement inférieur !

Les multiplicités manquantes sont évidemment à rechercher à l'infini. On identifie désormais le plan affine $\mathbb{A}^2_k$ à une partie du plan projectif $\mathbb{P}^2_k$ via le plongement $(x,y) \mapsto (x : y : 1)$. Considérons le polynôme $F^* \in k[X,Y,Z]$, qui est homogène de degré d, de sorte que la clôture projective de $V(F)$ dans $\mathbb{P}^2_k$ est $V_p(F^*)$. De même la clôture projective de D dans $\mathbb{P}^2_k$ est la droite projective $V_p(Y)$. Calculons alors l'intersection de $V_p(F^*)$ et $V_p(Y)$ à l'infini :

$$V_p(F) \cap V_p(Y) \cap V_p(Z) \subset \{(1:0:0)\}$$

Comme Y ne divise pas F, il ne divise pas non plus F^*. On en conclut que le polynôme $G(X,Z) := F^*(X,0,Z)$ est homogène de degré d. Le point $(1:0:0)$ est dans l'intersection $V_p(F) \cap V_p(Y)$ si et seulement si $G(1,0) = 0$, c'est-à-dire si et seulement si le monôme X^d n'apparaît pas dans F_d. Écrivons $G(X,Z) = Z^m H(X,Z)$ où $H(1,0) \neq 0$. Ainsi $(1:0:0) \in V_p(F) \cap V_p(Y)$ si et seulement si $m \geqslant 1$. L'entier m mérite le nom de multiplicité d'intersection des courbes $V_p(F)$ et $V_p(Y)$ au point $(1:0:0)$. Comme le degré du polynôme $F(X,0,1)$ est exactement le degré du polynôme H, on a bien

$$m + \sum_{i=1}^{r} m_i = m + \deg H = d = \deg F$$

En tenant compte de tous les points de l'espace projectif et de leur multiplicité, l'intersection d'une droite avec une courbe « de degré d » est bien égale à d. C'est cette situation que généralise le théorème de Bezout.

Définition 4.1. *Une courbe algébrique plane est une variété projective de la forme $V_p(F) \subset \mathbb{P}^2_k$ où $F \in k[X,Y,Z]$ est un polynôme homogène de degré $d > 0$.*

Soit $C = V_p(F)$ une courbe algébrique plane. Le Nullstellensatz fort implique que $I_p(C) = \sqrt{(F)}$. Soient $F_1, \dots, F_r$ les diviseurs irréductibles de F. Ce sont des polynômes homogènes et on a $\sqrt{(F)} = (F_1 \cdots F_r)$. Ainsi il existe un unique, à multiplication près par un élément de $k^\times$ polynôme homogène G homogène sans facteur carré tel que $I_p(C) = (G)$.

Définition 4.2. *Si C est une courbe algébrique plane, le* degré *de C est par définition le degré d'un polynôme homogène F tel que $I_p(C) = (F)$.*

Si $I_p(C) = (F)$, la courbe C est irréductible si et seulement si le polynôme F est irréductible.

Théorème 4.3 (Théorème de Bezout)**.** *Soient C_1 et C_2 deux courbes algébriques planes n'ayant aucune composante irréductible en commun. L'intersection de C_1 et C_2 est un ensemble fini et on a l'égalité*

$$\sum_{P \in C_1 \cap C_2} m(P; C_1, C_2) = \deg(C_1) \deg(C_2)$$

Une des principales difficultés est ici de définir correctement les multiplicités $m(P; C_1, C_2)$. Décomposons la démonstration de ce résultat en plusieurs étapes.

4.2. **Interlude sur les k-algèbre finies.** Une k-algèbre finie est une k-algèbre de dimension finie. Exceptionnellement, nous n'aurons pas besoin de supposer k algébriquement clos dans cette partie.

Proposition 4.4. *Soit A une k-algèbre finie. Alors A a un nombre fini d'idéaux maximaux. Notons les $\mathfrak{m}_1, \dots, \mathfrak{m}_r$. Pour tout $1 \leqslant i \leqslant r$, il existe un unique entier $e_i \geqslant 1$ tel que $\mathfrak{m}_i^{e_i} = \mathfrak{m}_i^{e_i+1}$ et $\mathfrak{m}_i^{e_i-1} \neq \mathfrak{m}_i^{e_i}$. L'isomorphisme naturel de A vers $\bigoplus_{i=1}^r A/\mathfrak{m}_i^{e_i}$ est un isomorphisme.*

4.3. **Multiplicités d'intersection et preuve du théorème de Bezout.**

Proposition 4.5. *Soient F_1 et F_2 deux polynômes non nul de $k[X, Y]$, premiers entre eux, alors $V(F_1) \cap V(F_2)$ est un ensemble fini.*

Démonstration. Il suffit de prouver que $(F_1, F_2) \cap k[X] \neq 0$. Supposons en effet que ce fait prouvé. Par symétrie on a également $(F_1, F_2) \cap k[Y] \neq 0$. Il existe alors deux polynômes non nuls à une variable tels que $(G(X), H(Y)) \subset k[X, Y]$. Alors $k[X, Y]/(G(X), H(Y))$ est un k-espace vectoriel de dimension finie, car engendré par la famille finie $(X^i Y^j)_{0 \leqslant i \leqslant \deg G - 1, 0 \leqslant j \leqslant \deg H - 1}$, c'est donc aussi le cas de $k[X, Y]/(F_1, F_2)$. Comme les points de $V(F_1) \cap V(F_2) = V(F_1, F_2)$ sont en bijection avec les idéaux maximaux de $k[X, Y]/(F_1, F_2)$, on en conclut que $V(F_1) \cap V(F_2)$ est fini.

Il reste à prouver que $(F_1, F_2) \cap k[X] \neq 0$. Supposons que $F_1 \notin k[X]$ et $F_2 \notin k[X]$ sinon il n'y a rien à faire. En particulier les polynômes F_1 et F_2 ne sont pas inversibles dans $k(X)[Y]$ et son premiers entre eux dans $k(X)[Y]$. De sorte que $(F_1)+(F_2) = k(X)[Y]$. Il existe donc $\frac{A_1}{B_1}$ et $\frac{A_2}{B_2}$ dans $k(X)$ tels que $1 = \frac{A_1}{B_1}F_1 + \frac{1_2}{B_2}F_2$ et donc $B_1(X)B_2(X) = A_1B_2F_1 + A_2B_1F_2 \in (F_1, F_2)$. □

Corollaire 4.6. *Soient F_1 et F_2 deux polynômes homogènes premiers entre eux de $k[X, Y, Z]$. L'ensemble $V_p(F_1) \cap V_p(F_2)$ est fini.*

Démonstration. Commençons par vérifier que si H est un hyperplan de $\mathbb{P}^2_k$, l'ensemble $V_p(F_1) \cap V_p(F_2) \cap (\mathbb{P}^2_k \setminus H)$ est fini. On peut se ramener au cas où H est l'hyperplan à l'infini du plongement de $\mathbb{A}^2_k$ dans $\mathbb{P}^2_k$. Il suffit de traiter le cas où $V_p(F_1) \not\subset H$ et $V_p(F_2) \not\subset H$ de sorte que les polynômes $F_{1,*}$ et $F_{2,*}$ de $k[X, Y]$ ne sont pas inversibles. Ils sont premiers entre eux dans $k[X, Y]$, on peut donc appliquer la proposition qui nous assure que l'ensemble

$$V_p(F_1) \cap V_p(F_2) \cap \mathbb{A}^2_k = V(F_{1,*}) \cap V(F_{2,*})$$

est fini.

On remarque qu'il existe trois hyperplans $H_0, \ldots, H_2$ de $\mathbb{P}^2_k$ tels que $H_0 \cap H_1 \cap H_2 = \emptyset$ (prendre par exemple les hyperplans $V_p(X_i)$)). Alors

$$V_p(F_1) \cap V_p(F_2) = \bigcup_{i=0}^{2} (V_p(F_1) \cap V_p(F_2) \cap (\mathbb{P}^2_k \setminus H_i))$$

est fini. □

Comme l'ensemble $V_p(F_1) \cap V_p(F_2)$ est fini, on peut trouver un hyperplan de $\mathbb{P}^2_k$ tel que $V_(F_1) \cap V_p(F_2) \cap H = \emptyset$. Quitte à faire un changement de repère projectif, on peut supposer que l'hyperplan H est l'hyperplan à l'infini du plongement de $\mathbb{A}^2_k$ dans $\mathbb{P}^2_k$ et donc que les courbes $C_1 := V_p(F_1)$ et $C_2 := V_p(F_2)$ ne s'intersectent pas à l'infini.

On suppose désormais que F_1 et F_2 sont sans facteur carré de sorte que $I_p(C_1) = (F_1)$ et $I_p(C_2) = (F_2)$.

L'algèbre $A := k[X, Y]/(F_{1,*}, F_{2,*})$ est une k-algèbre fini et ses idéaux maximaux sont en bijection naturelle avec les points de $C_1 \cap C_2$.

Définition 4.7. *Soit $P \in C_1 \cap C_2$ et $\mathfrak{m}_P$ l'idéal maximal de A correspondant. On définit alors l'entier $m(P; C_1, C_2)$ comme étant la dimension de $A/\mathfrak{m}^e$ où e est un entier tel que $\mathfrak{m}^e = \mathfrak{m}^{e+1}$ (voir la proposition 4.4).*

On admet que cette définition ne dépend que de C_1, C_2 et P et non du choix de l'hyperplan H.

Étant donné la proposition 4.4, le théorème de Bezout est alors une conséquence immédiate du résultat suivant.

Proposition 4.8. *Soient F_1 et F_2 deux éléments non inversibles et premiers entre eux de $k[X,Y]$. On alors*

$$\dim_k k[X,Y]/(F_1,F_2) \leqslant \deg F_1 \deg F_2$$

De plus cette inégalité est une égalité lorsque les adhérences de Zariski projectives de $V(F_2)$ et $V(F_2)$ ne s'intersectent pas à l'infini.

4.4. **Quelques remarques.** Les considérations de la partie précédentes peuvent se généraliser comme suit. On aimerait pouvoir définir la multiplicité d'intersection de deux courbes $V_p(F)$ et $V_p(G)$ même lorsque F et G ont des facteurs carrés. On aimerait cependant *garder trace* de ces puissances. Le bon cadre pour traiter ce genre de question est la théorie des schémas. Notre approche du théorème de Bezout nous permet cependant de traiter quelques cas particuliers.

Soient F et G deux polynômes homogènes premiers entre eux de $k[X,Y,Z]$. Comme $V_p(F)\cap V_p(G)$ est fini, il existe un hyperplan H n'intersectant pas $V_p(F)\cap V_p(G)$. Envoyons cet hyperplan à l'infini et posons $A = k[X,Y]/(F_*,G_*)$. On définit la *multiplicité d'intersection* de F et G en un point P de $V_p(F)\cap V_p(G)$ en posant

$$m(P;F,G) = \dim_k A/\mathfrak{m}_P^{e_P}$$

où e_P est encore un entier tel que $\mathfrak{m}_P^{e_P} = \mathfrak{m}_P^{e_P+1}$.

On admet encore que $m(P;F,G)$ ne dépend pas du choix de H. Cette multiplicité vérifie les propriétés suivantes

— $m(P;F,G_1G_2) = m(P;F,G_1) + m(P;F,G_2)$;
— $m(P;F,G) = m(P;G,F)$;
— $m(P;F,G) = m(P;F,G+aF)$ pour tout $a \in k$.

Proposition 4.9. *Soit C une courbe algébrique plane irréductible. Les fermés algébriques de C sont C ainsi que les parties finies de C.*

Démonstration. Soit $S \subsetneq C$ une partie algébrique de C. Alors par définition $S = V_p(I)$ pour un idéal homogène I. Il existe donc des polynômes homogènes $F_1,\dots,F_r$ tels que $I = (F_1,\dots,F_r)$ et donc que $S = V_p(F_1)\cap\cdots V_p(F_r)$. Comme $S \subsetneq C$, il existe i tel que $C \not\subset V_p(F_i)$. Or le théorème de Bezout implique que $C\cap V_p(F_i)$ est fini, donc S est fini. □

4.5. **Courbes lisses.**

Définition 4.10. *Soit C une courbe algébrique plane. Soit $P \in C$ et soit F tel que $I_p(C) = (F)$. On dit que la courbe C est* lisse *au point P si le vecteur $\left(\frac{\partial F}{\partial X}(P), \frac{\partial F}{\partial Y}(P), \frac{\partial F}{\partial Z}(P)\right)$ est non nul. Un point de C qui n'est pas lisse est dit* singulier*. Si P est un point lisse de C, la* tangente *à C en P est la droite projective, notée T_pC, d'équation*

$$\frac{\partial F}{\partial X}(P)X + \frac{\partial F}{\partial Y}(P)Y + \frac{\partial F}{\partial Z}(P)Z = 0$$

Remarque 4.11. La lissité de C au point P ne dépend pas du repère projectif choisi. Cela peut se voir en remarquant que le point P est lisse si et seulement si la différentielle dF_P est une application linéaire non nulle. La droite T_pC est alors $\mathbb{P}(\ker dF_P)$.

Proposition 4.12. *Soit C une courbe algébrique plane et soit P un point lisse de C. La tangente à C en P est l'unique droite projective L vérifiant*

$$m(P; C, L) \geqslant 2$$

Démonstration. Quitte à changer de repère projectif, on peut supposer que $L = V(Y)$ et $P = (0 : 0 : 1)$. La multiplicité $m(P; C, L)$ est le plus grand entier $m \geqslant 0$ tel que $X^m | F(X, 0, 1)$. Ainsi F peut s'écrire

$$F(X, Y, Z) = X^m G(X, Z) + Y H(X, Y, Z)$$

où G et H sont homogènes avec $G(1, 0) \neq 0$. On a bien $\frac{\partial F}{\partial X}(P) = 0$ si et seulement si $m \geqslant 2$ et L est l'unique droite projective passant par P dont l'équation est de la forme $aY + bZ = 0$. □

Si C est une courbe algébrique plane, on note C^{sing} l'ensemble de ses points singuliers.

Proposition 4.13. *Soit C une courbe algébrique plane irréductible. L'ensemble C^{sing} est une partie finie de C.*

Démonstration. Soit F tel que $I)(C) = (F)$. Par définition, on a

$$C^{sing} = V_p(F) \cap V_p\left(\frac{\partial F}{\partial X}\right) \cap V_p\left(\frac{\partial F}{\partial Y}\right) \cap V_p\left(\frac{\partial F}{\partial Z}\right)$$

Ainsi C^{sing} est une partie algébrique de C. Si elle n'est pas finie, on a $C^{sing} = C$. Dans ce cas on a $V_p(F) \subset V_p\left(\frac{\partial F}{\partial X}\right)$ et on en déduit que F divise $\frac{\partial F}{\partial X}$. En comparant le degré en X de ces deux polynômes, on en déduit $\frac{\partial F}{\partial X} = 0$. De même on a

$$\frac{\partial F}{\partial X} = \frac{\partial F}{\partial Y} = \frac{\partial F}{\partial Z} = 0$$

Ceci implique soit que F est une constante, ce qui contredit la définition d'une courbe algébrique plane, soit que le corps k est de caractéristique p, pour un nombre premier p, et qu'il existe un polynôme G tel que $F(X, Y, Z) = G(X^p, Y^p, Z^p)$. Si

$$G = \sum_{i,j,k} a_{i,j,k} X^i Y^j Z^k,$$

comme le corps k est algébriquement clos, il existe des éléments $b_{i,j,k} \in k$ tels que $a_{i,j,k} = b_{i,j,k}^p$ et finalement

$$F(X, Y, Z) = \left(\sum_{i,j,k} b_{i,j,k} X^i Y^j Z^k\right)^p$$

Ceci contredit l'irréductibilité de F. On a donc bien C^{sing} fini. □

Définition 4.14. *Une courbe algébrique irréductible de degré* 2 *est appelée* conique*, une courbe algébrique irréductible de degré* 3 *est appelée* cubique*.*

4.6. **Courbes elliptiques.**

Définition 4.15. *Une* courbe elliptique *est une cubique plane lisse.*

Soit E une courbe elliptique. Fixons O un point de E. Soient P et Q deux points de E. Le théorème de Bezout implique qu'il existe un unique droite projective L et un unique point R de E tels que

$$E \cdot L = P + Q + R$$

En effet, si P et Q sont distincts, la droite L est l'unique droite projective contenant P et Q. Si $P = Q$, la droite L est la tangente à E au point P. On note $P * Q$ le point R. Il existe alors une unique droite projective L' et un unique point $S \in E$ tels que

$$E \cdot L' = 0 + (P * Q) + S$$

On note $P +_0 Q$ le point S. Autrement dit $P +_0 Q$ est le point $(0 * (P * Q))$. On a ainsi défini une loi de composition interne sur E.

Théorème 4.16. *La loi de composition* $+_0$ *fait du couple* $(E, +_0)$ *un groupe abélien d'élément neutre* 0*.*

Remarque 4.17. La loi $+_0$ dépend vraiment du point 0 puisque c'est son élément neutre. Cependant, dans la plupart des cas, on note simplement $+$ la loi de groupe sur E.

Démonstration. La loi $+_0$ est clairement commutative. Vérifions que le point 0 est un élément neutre. Par définition, si $P \in E$, il existe une droite L et une droite L' telles que

$$E \cdot L = 0 + P + (0 * P) \quad E \cdot L' = 0 + (0 * P) + (0 +_0 P)$$

Ainsi $L = L'$ et $0 +_0 P = P$.

Si $P \in E$, vérifions qu'il existe $Q \in E$ tel que $P +_0 Q = 0$. Soit L la droite projective tangente à E en 0. On a alors

$$E \cdot L = 20 + (0 * 0)$$

On remarque au passage que l'on a $(0 * (0 * 0)) = 0$. Soit L' l'unique droite passant par P et $0 * 0$ (la tangente en P s'il se trouve que $P = 0 * 0$) et soit Q le troisième point d'intersection de L' avec E, on a alors

$$E \cdot L' = P + Q + (0 * 0)$$

On en déduit que $(P * Q) = (0 * 0)$ donc

$$P +_0 Q = (0 * (0 * 0)) = 0$$

L'associativité de la loi $+_0$ est la propriété la plus difficile à démontrer. La démonstration sera vue au prochain cours. □

Théorème 4.18. *Supposons que le corps k est de caractéristique différente de 2 et 3. Soit E une courbe elliptique. Quitte à faire un changement de repère projectif, il existe $(a, b) \in k^2$ tels que $4a^3 + 27b^2 \neq 0$ et*

$$E = V_p(Y^2Z - X^3 - aXZ^2 - bZ^3)$$

Démonstration. Comme E est de degré 3, la courbe E possède au moins un point d'inflexion P (voir les exercices). Choisissons l'axe $Z = 0$ tel que la droite $Z = 0$ soit tangente à E en P. D'après le théorème de Bezout, la droite $Z = 0$ coupe alors E uniquement en P. Ceci implique que l'équation de E est de la forme

$$F = X^3 + ZG(X, Y, Z)$$

où G est un polynôme homogène de degré 2. Ainsi E pour équation

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6$$

Le changement de variable $Y \mapsto Y - \frac{1}{2}(a_2X - a_3Z)$ permet d'éliminer a_1 et a_3. Ensuite le changement de variable $X \mapsto X - \frac{1}{3}a_2Z$ permet d'éliminer a_2. □