CHAPITRE 5

CONIQUES PROJECTIVES (ET AFFINES)

Les passages en petits caractères 23.8 et 23.12 n'ont pas été traités en cours et peuvent être omis.

21. Rappels sur les formes quadratiques

[1] Cette section, constituée de rappels de L2 ou L3, a été exposée rapidement en cours. Ses résultats sont considérés comme connus. Soit k un corps.

Définition 21.1. — Soient V, E deux k-espaces vectoriels. Une **application bilinéaire** de $V \times V$ dans E est une application $b : V \times V \to E$ qui est linéaire en chaque variable (l'autre variable étant fixée), i.e. pour $u, u', v, v' \in V$ et $\lambda, \mu, \lambda', \mu' \in k$, on a :

$$b(\lambda u + \lambda' u', v) = \lambda b(u, v) + \lambda' b(u', v) \qquad \text{et} \qquad b(u, \mu v + \mu' v') = \mu b(u, v) + \mu' b(u, v').$$

En appliquant successivement ces deux conditions on obtient que :

$$b(\lambda_1 u_1 + \lambda_2 u_2, \mu_1 v_1 + \mu_2 v_2) = \lambda_1\mu_1 b(u_1, v_1) + \lambda_1\mu_2 b(u_1, v_2) + \lambda_2\mu_1 b(u_2, v_1) + \lambda_2\mu_2 b(u_2, v_2).$$

Plus généralement, pour tout $n \in \mathbb{N}^*$ et $u_i, v_i \in V$ et $\lambda_i, \mu_i \in k$, on a :

$$b\Big(\sum_{i=1}^{n} \lambda_i u_i, \sum_{j=1}^{n} \mu_j v_j\Big) = \sum_{i=1}^{n} \lambda_i b\Big(u_i, \sum_{j=1}^{n} \mu_j v_j\Big) = \sum_{i,j=1}^{n} \lambda_i \mu_j \, b(u_i, v_j).$$

Exemple 21.2. — Soit $A = k[X_1, \dots, X_r]$ l'algèbre des polynômes sur k en r variables ; pour tout r-uplet $\mathbf{a} = (a_1, \dots, a_r) \in \mathbb{N}^r$ on note $X^{\mathbf{a}}$ le monôme $X_1^{a_1} \cdots X_r^{a_r}$. Alors la multiplication $m : A \times A \to A$ est définie par $X^{\mathbf{a}} \cdot X^{\mathbf{b}} = X^{\mathbf{a}+\mathbf{b}}$ et la condition que m soit k-bilinéaire. C'est-à-dire, pour $P = \sum_{\mathbf{a} \in \mathbb{N}^r} \alpha_{\mathbf{a}} X^{\mathbf{a}}$ et $Q = \sum_{\mathbf{b} \in \mathbb{N}^r} \beta_{\mathbf{b}} X^{\mathbf{b}}$ arbitraires, on a :

$$P \cdot Q = m(P, Q) = \sum_{\mathbf{a}, \mathbf{b} \in \mathbb{N}^r} \alpha_{\mathbf{a}} \beta_{\mathbf{b}} \, m(X^{\mathbf{a}}, X^{\mathbf{b}}) = \sum_{\mathbf{a}, \mathbf{b} \in \mathbb{N}^r} \alpha_{\mathbf{a}} \beta_{\mathbf{b}} \, X^{\mathbf{a}+\mathbf{b}}.$$

Dans la suite de cette section, on suppose $\boxed{\operatorname{car}(k) \neq 2.}$

Définitions 21.3. — Soit V un k-espace vectoriel.

(1) Une **forme bilinéaire** sur V est une application bilinéaire $\phi : V \times V \to k$.

(2) On dit que ϕ est **symétrique** si pour tout $x, y \in V$ on a $\boxed{\phi(x, y) = \phi(y, x).}$

---

[1] Version du 26/10/2016.

(3) Dans ce cas, on dit que l'application $Q : V \to k$, $x \mapsto Q(x) = \phi(x, x)$ est la **forme quadratique** définie par ϕ. Pour tout $\lambda \in k$ et $x, y \in V$, on a $Q(\lambda x) = \lambda^2 Q(x)$ et :

$$\begin{aligned} Q(x+y) &= \phi(x+y, x+y) = \phi(x,x) + \phi(x,y) + \phi(y,x) + \phi(y,y) \\ &= Q(x) + Q(y) + 2\phi(x,y). \end{aligned} \tag{$\dagger$}$$

Donc ϕ est déterminée par Q, i.e. :

$$\phi(x,y) = \frac{1}{2}\big(Q(x+y) - Q(x) - Q(y)\big) \tag{$*$}$$

et, si Q est donnée, on dit que ϕ est la **forme polaire** de Q.

(4) En remplaçant y par $-y$ dans la formule ($\dagger$), on obtient $Q(x-y) = Q(x) + Q(y) - 2\phi(x,y)$ d'où la formule également utile :

$$\phi(x,y) = \frac{1}{4}\big(Q(x+y) - Q(x-y)\big). \tag{$**$}$$

Remarque. — Pour vérifier qu'une application $\phi : V \times V \to k$ est une forme bilinéaire symétrique, il suffit de voir que $\phi(x,y) = \phi(y,x)$ et que ϕ est linéaire en la première variable, car ces deux conditions entraînent alors la linéarité en la deuxième variable.

Désormais, on suppose V de **dimension finie** n. Soit ϕ une forme bilinéaire symétrique (en abrégé : fbs) sur V et Q la forme quadratique associée.

Définition 21.4 **(Expression dans une base et rang).** — Soit $\mathscr{B} = (e_1, \dots, e_n)$ une base de V et soient $(x_1, \dots, x_n)$ les coordonnées correspondantes. Pour $i, j = 1, \dots, n$, posons $a_{ij} = \phi(e_i, e_j)$; comme ϕ est symétrique alors $a_{ji} = a_{ij}$.

(i) La matrice $A = (a_{ij})_{1 \le i,j \le n}$ est *symétrique* (i.e. ${}^tA = A$) ; elle est appelée la matrice de ϕ (ou de Q) dans la base $\mathscr{B}$ et notée $\mathrm{Mat}_{\mathscr{B}}(\phi)$ ou $\mathrm{Mat}_{\mathscr{B}}(Q)$.

(ii) Pour tout $x = \sum_{i=1}^n x_i e_i$ et $y = \sum_{j=1}^n y_j e_j$, notons ${}^tX = (x_1, \dots, x_n)$ et ${}^tY = (y_1, \dots, y_n)$, alors on a $\boxed{\phi(x,y) = \sum_{i,j=1}^n a_{ij}\, x_i y_j}$ et ceci est égal, d'une part, à

$$(x_1, \dots, x_n) A \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = {}^tXAY \tag{$\dagger$}$$

et, d'autre part, à :

$$\sum_{i=1}^n a_{ii}\, x_i y_i + \sum_{1 \le i < j \le n} a_{ij}\,(x_i y_j + x_j y_i). \tag{$\ddagger$}$$

(iii) Pour $y = x$, ($\ddagger$) donne $Q(x) = \sum_{i=1}^n a_{ii}\, x_i^2 + \sum_{1 \le i < j \le n} 2a_{ij}\, x_i x_j$ donc Q correspond dans la base $\mathscr{B}$ au polynôme $\sum_{i=1}^n a_{ii}\, X_i^2 + \sum_{1 \le i < j \le n} 2a_{ij}\, X_i X_j$ homogène de degré 2.

(iv) Réciproquement, si Q est donnée par $Q(X) = \sum_{i=1}^n c_i\, X_i^2 + \sum_{1 \le i < j \le n} c_{ij}\, X_i X_j$ alors sa forme polaire ϕ est donnée par $\phi(e_i, e_i) = c_i$ et, pour $i \neq j$, $\phi(e_i, e_j) = c'_{ij}$ où $c'_{ij} = c'_{ji} = (1/2)c_{ij}$. Donc

$$\mathrm{Mat}_{\mathscr{B}}(Q) = \begin{pmatrix} c_1 & c'_{12} & \cdots & \cdots & c'_{1n} \\ c'_{21} & c_2 & c'_{23} & \cdots & c'_{2n} \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ c'_{n-1,1} & \cdots & \ddots & c_{n-1} & c'_{n-1,n} \\ c'_{n1} & c'_{n2} & \cdots & c'_{n,n-1} & c_n \end{pmatrix}.$$

(v) Soit $\mathscr{C}$ une autre base de V et $P = \mathrm{Mat}_{\mathscr{B}}(\mathscr{C})$ la matrice de passage. Alors

$$(\star) \qquad \boxed{\mathrm{Mat}_{\mathscr{C}}(\phi) = {}^tPAP.}$$

(vi) On appelle **rang** de ϕ (ou de Q) le rang de la matrice A. D'après le point précédent, ceci ne dépend pas de la base choisie, car comme P (et donc ${}^tP$) est inversible, alors A et ${}^tPAP$ ont même rang.(2) On dit que Q (ou ϕ) est **non dégénérée** si elle est de rang $n = \dim(V)$, i.e. si sa matrice dans n'importe quelle base est inversible.

(vii) On appelle **noyau** de Q (ou de ϕ) et l'on note $N(Q)$ ou $N(\phi)$ le sev de V suivant :

$$N(\phi) = \{x \in V \mid \forall y \in V, \quad \phi(y, x) = 0\}.$$

Pour toute base $\mathscr{B}$ de V, on a $N(\phi) = \mathrm{Ker}(A)$; par conséquent, $N(\phi) = \{0\}$ ssi ϕ est non dégénérée.

Démonstration. — Seul les points (v) et (vii) nécessitent une démonstration. Donnons-en deux pour (v). Écrivons $\mathscr{C} = (f_1, \dots, f_n)$ et posons $B = \mathrm{Mat}_{\mathscr{C}}(\phi)$.

1ère démonstration. Écrivons $f_i = \sum_{r=1}^n p_{ri} e_r$ pour tout i. Alors

$$b_{ij} = \phi(f_i, f_j) = \sum_{r,s=1}^n p_{ri} p_{sj} \phi(e_r, e_s) = \sum_{r,s=1}^n p_{ri} p_{sj} a_{rs} = \sum_{r,s=1}^n ({}^tP)_{ir} a_{rs} p_{sj} = ({}^tPAP)_{ij}.$$

2ème démonstration. Soient $u, v \in V$ arbitraires, notons X, Y (resp. X', Y') leurs coordonnées dans la base $\mathscr{B}$ (resp. $\mathscr{C}$). D'après la formule de changement de coordonnées, on a $X = PX'$ et $Y = PY'$ donc

$$\phi(v, u) = {}^tYAX = {}^tY' \, ({}^tPAP) \, X'$$

et ceci entraîne que $b_{ij} = \phi(f_i, f_j)$ est le coefficient d'indice (i, j) de la matrice ${}^tPAP$ (car alors ${}^tY' = (0, \dots, 0, 1, 0, \dots, 0)$ avec le 1 à la i-ème place et de même pour X'), d'où $B = {}^tPAP$.

Prouvons maintenant (vii). Soit $x \in V$ et X le vecteur colonne de ses coordonnées dans la base $\mathscr{B}$. Alors $x \in N(\phi)$ ssi $\phi(y, x) = 0$ pour tout $y \in V$, i.e. ssi :

$$(*) \qquad \forall\, Y \in k^n, \qquad {}^tYAX = 0.$$

Or, notant U le vecteur colonne AX et $Y(i)$ le vecteur dont toutes les coordonnées sont nulles sauf la i-ème qui vaut 1, on voit que ${}^tY(i)U$ égale la i-ème coordonnée u_i de U. Par conséquent, la condition $(*)$ équivaut à la nullité de $U = AX$. Ceci montre que $N(\phi) = \mathrm{Ker}(A)$. □

Une propriété importante des formes quadratiques non dégénérées est qu'elles induisent un isomorphisme entre V et V^*, i.e. on a les résultats suivants.

***Définition 21.5* (importante).** — Soit ϕ une fbs sur V ; notons θ l'application linéaire $V \to V^*$, $x \mapsto \phi(-, x)$. C'est-à-dire :

(i) Pour tout $x \in V$, $\theta(x)$ est l'application $V \to k$, $y \mapsto \phi(y, x)$. La linéarité de ϕ en la première variable signifie que $y \mapsto \phi(y, x)$ est une forme linéaire sur V, donc on a bien $\theta(x) \in V^*$.

(2) On verra plus bas qu'on peut trouver une base $\mathscr{C}$ dans laquelle la matrice de ϕ est *diagonale* ; alors le rang est le nombre de coefficients diagonaux non nuls.

(ii) La linéarité de ϕ en la deuxième variable entraîne alors que θ est linéaire i.e. que $\theta(\lambda x + x') = \lambda\theta(x) + \theta(x')$ (égalité de formes linéaires) ; en effet, pour tout $y \in V$ on a :

$$\theta(\lambda x + x')(y) = \phi(y, \lambda x + x') = \lambda\phi(y, x) + \phi(y, x') = \lambda\theta(x)(y) + \theta(x')(y).$$

Proposition 21.6. — *Soient $\mathscr{B}$ une base de V, $\mathscr{B}^*$ la base duale de V^* et $A = \mathrm{Mat}_{\mathscr{B}}(\phi)$. Alors A est la matrice de θ dans les bases $\mathscr{B}$ (au départ) et $\mathscr{B}^*$ (et l'arrivée), notée* $\mathrm{Mat}_{\mathscr{B}^*,\mathscr{B}}(\theta)$.

Démonstration. — Écrivons $\mathscr{B} = (e_1, \dots, e_n)$ et $\mathscr{B}^* = (e_1^*, \dots, e_n^*)$. Pour tout $f \in V^*$, son écriture $f = \sum_{i=1}^n c_i e_i^*$ est donnée par $c_i = f(e_i)$. Pour $f = \theta(e_j)$ on a : $\theta(e_j)(e_i) = \phi(e_i, e_j) = a_{ij}$ et donc $\theta(e_j) = \sum_{i=1}^n a_{ij} e_i^*$. Ceci montre que $\mathrm{Mat}_{\mathscr{B}^*,\mathscr{B}}(\theta) = A$. □

Corollaire 21.7. — *ϕ (ou Q) est non dégénérée ssi θ est un isomorphisme $V \xrightarrow{\sim} V^*$. Dans le cas contraire, on dit que Q est* dégénérée *et son noyau $N(Q)$ égale* $\mathrm{Ker}(\theta)$.

***Définition 21.8* (Orthogonalité).** — Soit ϕ une fbs sur V.

(i) On dit que deux vecteurs $x, y \in V$ sont **orthogonaux** (pour ϕ) si $\phi(x, y) = 0$. Plus généralement, on dit que deux sous-ensembles X, Y de V sont orthogonaux si l'on a $\phi(x, y) = 0$ pour tout $x \in X$ et $y \in Y$. On notera $X \perp Y$ pour signifier que X et Y sont orthogonaux.

(ii) Pour tout sous-ensemble Y de V, son orthogonal (relativement à ϕ), noté $Y^\perp$, est :

$$(\star) \qquad \boxed{Y^\perp = \{x \in V \mid \phi(x, y) = 0, \quad \forall y \in Y\}.}$$

Remarquons au passage que $V^\perp = N(\phi)$.

(iii) $Y^\perp$ est un **sous-espace vectoriel** de V (même si Y n'en est pas un) ; de plus, on a les propriétés suivantes :

$$(\star\star) \qquad \boxed{Y \subset Z \Longrightarrow Z^\perp \subset Y^\perp} \qquad \text{et} \qquad \boxed{Y^\perp = \mathrm{Vect}(Y)^\perp}$$

en particulier, si Y est un sous-espace vectoriel F de V et si $(f_1, \dots, f_p)$ est une famille génératrice de F, alors

$$\boxed{F^\perp = \{f_1, \dots, f_p\}^\perp = \{x \in V \mid \phi(x, f_i) = 0, \quad \forall i = 1, \dots, p\}.}$$

Démonstration de (iii). — Soient $x, x' \in Y^\perp$ et $\lambda \in k$, alors on a, pour tout $y \in Y$, $\phi(\lambda x + x', y) = \lambda\phi(x, y) + \phi(x', y) = 0$, ce qui montre que $\lambda x + x' \in Y^\perp$. Donc $Y^\perp$ est un sous-espace vectoriel de V.

Il est immédiat que si $Y \subset Z$, alors $Z^\perp \subset Y^\perp$ car si $x \in Z^\perp$ alors x est orthogonal à tout élément de Z, donc x est *a fortiori* orthogonal à tout élément de Y (puisque $Y \subset Z$), donc $x \in Y^\perp$.

Comme $Y \subset \mathrm{Vect}(Y)$, ceci donne l'inclusion $\mathrm{Vect}(Y)^\perp \subset Y^\perp$. Montrons l'inclusion réciproque. Soit $x \in Y^\perp$ et soit v un élément arbitraire de $\mathrm{Vect}(Y)$; par définition, v s'écrit comme une combinaison linéaire finie $v = \lambda_1 y_1 + \cdots + \lambda_r y_r$, avec $y_i \in Y$ et $\lambda_i \in k$; alors on a

$$\phi(x, v) = \sum_{i=1}^r \lambda_i \underbrace{\phi(x, y_i)}_{=0} = 0$$

et donc $x \in \mathrm{Vect}(Y)^\perp$. Ceci montre que $Y^\perp \subset \mathrm{Vect}(Y)^\perp$, d'où l'égalité $\mathrm{Vect}(Y)^\perp = Y^\perp$. □

***Théorème 21.9* (Orthogonalité pour ϕ non dégénérée).** — *Soit ϕ une* fbs non dégénérée *sur V et soit F un sev de V.*

(i) *On a* $\boxed{\dim(F^\perp) = \dim(V) - \dim(F)}$ *et* $\boxed{F = (F^\perp)^\perp.}$

(ii) *Si* $F \cap F^\perp = \{0\}$, *alors* $\boxed{V = F \oplus F^\perp.}$

(iii) *En fait* (ii) *est vrai même sans supposer que* ϕ *soit non dégénérée.*

Démonstration. — (i) Si $x \in F$ alors pour tout $y \in F^\perp$ on a $\phi(x, y) = 0$ et donc $x \in (F^\perp)^\perp$. Ceci montre que $F \subset (F^\perp)^\perp$, sans supposer que ϕ soit non dégénérée.

Soit $\theta : V \to V^*$ l'application linéaire associée à ϕ. Alors $\theta(F)$ est un sev de V^* et l'on a

$$F^\perp = \big\{y \in V \mid \forall x \in V, \quad 0 = \phi(x, y) = \theta(x)(y)\big\} = \theta(F)^0,$$

où ^{0} désigne l'orthogonalité entre V et V^* (cf. 15.1). On a donc

$$(*) \qquad \dim(F^\perp) = \dim(V) - \dim \theta(F).$$

Supposons maintenant que ϕ soit non dégénérée. Alors θ est bijective donc $\theta(F)$ est de même dimension que F, et donc $(*)$ entraîne que $\dim(F^\perp) = \dim(V) - \dim(F)$.

On a de même $\dim(F^\perp)^\perp = \dim(V) - \dim(F^\perp) = \dim(F)$, et alors l'inclusion $F \subset (F^\perp)^\perp$ entraîne l'égalité $F = (F^\perp)^\perp$. Ceci prouve (i).

(ii) et (iii) : ne supposant plus que ϕ soit non dégénérée, on a toujours $\dim \theta(F) \le \dim(F)$ et donc $\dim(F^\perp) \ge \dim(V) - \dim(F)$.

Si l'on a $F \cap F^\perp = \{0\}$, alors F et $F^\perp$ sont en somme directe, et d'après ce qui précède on a :

$$\dim(F \oplus F^\perp) = \dim(F) + \dim(F^\perp) \ge \dim(V)$$

et ceci entraîne que $F \oplus F^\perp = V$ (et que $\dim(F^\perp) = \dim(V) - \dim(F)$). □

Remarque 21.10. — Attention ! Le lecteur peut penser au cas de $V = \mathbb{R}^n$ muni du produit scalaire euclidien $(x \mid y) = \sum_{i=1}^n x_i y_i$; dans ce cas, pour tout sev F de V on a $F \cap F^\perp = \{0\}$ car si $x \in F \cap F^\perp$ alors l'égalité $0 = (x \mid x) = \sum_{i=1}^n x_i^2$ entraîne que $x = 0$. Mais ceci est une particularité du cas euclidien et n'est pas vrai pour une fbs non dégénérée ϕ arbitraire. Par exemple, soit ϕ la fbs sur $\mathbb{R}^2$ définie par

$$\phi(u, v) = x_1 y_2 + x_2 y_1 \qquad \text{si } u = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix} \text{ et } v = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix};$$

sa matrice dans la base canonique $\mathscr{B} = (e_1, e_2)$ de $\mathbb{R}^2$ est $A = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, donc ϕ est non dégénérée. Cependant, on a $\phi(e_1, e_1) = 0 = \phi(e_2, e_2)$ donc chacune des droites $D_1 = \mathbb{R}e_1$ et $D_2 = \mathbb{R}e_2$ est égale à son propre orthogonal, i.e. $D_1^\perp = D_1$ et $D_2^\perp = D_2$.

***Définition 21.11* (Restriction à un sous-espace).** — Soit ϕ une fbs sur V et soit F un sev de V.

(i) On note ϕ_F la fbs sur F obtenue en restreignant ϕ à $F \times F$, i.e. $\phi_F(x, y) = \phi(x, y)$ pour tout $x, y \in F$; on l'appelle la *restriction* de ϕ à F.

(ii) On a $F \cap F^\perp = \{x \in F \mid \forall y \in F \quad \phi(x, y) = 0\} = N(\phi_F)$. Donc l'assertion (ii) du théorème 21.9 peut se récrire comme suit : « *si* ϕ_F *est non dégénérée, alors* $V = F \oplus F^\perp$ ».

Remarque 21.12. — Attention ! Même si ϕ est non dégénérée, ϕ_F ne l'est pas nécessairement. Par exemple, soit ϕ la forme polaire de la forme quadratique $Q(x_1 x_2) = x_1 x_2$ sur $\mathbb{R}^2$, elle est non dégénérée mais sa restriction à chaque droite isotrope $D_1 = \mathbb{R}e_1$ ou $D_2 = \mathbb{R}e_2$ est nulle, donc dégénérée.

***Définition 21.13* (Bases orthogonales).** — Soient Q une forme quadratique sur V et ϕ sa forme polaire. Soient $\mathscr{B} = (e_1, \dots, e_n)$ une base de V et $(x_1, \dots, x_n)$ les coordonnées correspondantes.

(i) On dit que $\mathscr{B}$ est une base **orthogonale** pour ϕ (ou pour Q) si l'on $\phi(e_i, e_j) = 0$ pour $i \neq j$, ce qui équivaut à dire que la matrice $A = \mathrm{Mat}_{\mathscr{B}}(\phi)$ est **diagonale**.

(ii) Ceci équivaut encore à dire que $Q(x_1, \dots, x_n) = c_1\, x_1^2 + \cdots + c_n\, x_n^2$, et dans ce cas $c_1, \dots, c_n$ sont les coefficients diagonaux de A.

***Théorème 21.14* (Existence de bases orthogonales).** — *Soit ϕ une fbs sur V.*

(i) *Il existe une base de V orthogonale pour ϕ.*

(ii) *Si $\mathscr{B} = (e_1, \dots, e_n)$ est une base de V orthogonale pour ϕ et si $(x_1, \dots, x_n)$ sont les coordonnées correspondantes, alors $Q(x_1, \dots, x_n) = c_1x_1^2 + \cdots + c_nx_n^2$ et le rang de ϕ est égal au nombre de c_i non nuls. En particulier, ϕ est non dégénérée ssi tous les c_i sont $\neq 0$.*

(iii) *Si Q est de rang $r < n$ on peut supposer, quitte à renuméroter les e_i, que $c_i = Q(e_i)$ est non nul pour $i = 1, \dots, r$ et nul pour $i > r$. Alors $N(Q)$ est le sev $\mathrm{Vect}(e_{r+1}, \dots, e_n)$, donné par les équations $x_i = 0$ pour $i = 1, \dots, r$.*

Démonstration. — (i) Procédons par récurrence sur $n = \dim(V)$. Il n'y a rien à montrer si $n = 0$ ou si $\phi = 0$. On peut donc supposer $n \geq 1$, le résultat établi pour $n - 1$ et $\phi \neq 0$. Alors la forme quadratique Q est non nulle (cf. 21.3 $(*)$), donc il existe $e_1 \in V$ tel que $Q(e_1) \neq 0$. Posons $F = ke_1$; comme $\phi(e_1, e_1) \neq 0$, alors $F \cap F^\perp = \{0\}$ et donc, d'après le théorème 21.9, on a $V = F \oplus F^\perp$.

Par hypothèse de récurrence, il existe une base $(e_2, \dots, e_n)$ de $F^\perp$ telle que $\phi(e_i, e_j) = 0$ pour $i \neq j$. Alors $(e_1, e_2, \dots, e_n)$ est une base de V orthogonale pour ϕ. Ceci prouve (i).

(ii) est clair, car le rang de ϕ est le rang de la matrice $A = \mathrm{Mat}_{\mathscr{B}}(\phi)$, qui est diagonale de coefficients diagonaux $c_1, \dots, c_n$.

Enfin, (iii) découle du point (vii) de 21.4. On peut aussi le redémontrer comme suit : Fixons un indice $i > r$; comme la base $\mathscr{B}$ est orthogonale et comme $\phi(e_i, e_i) = 0$, alors e_i est orthogonal à tous les éléments de $\mathscr{B}$ donc appartient à $N(Q)$. Ceci montre que $\mathrm{Vect}(e_{r+1}, \dots, e_n) \subset N(Q)$. Réciproquement, si un élément $v = \sum_{j=1}^n a_j e_j$ appartient à $N(Q)$ alors, pour $i = 1, \dots, r$, l'égalité $0 = \phi(e_i, v) = a_i c_i$ donne $a_i = 0$ (car $c_i \neq 0$), donc $v \in \mathrm{Vect}(e_{r+1}, \dots, e_n)$. $\square$

Le théorème 21.14 est valable pour tout corps k de caractéristique $\neq 2$. La possibilité d'effectuer des réductions supplémentaires dépend de propriétés « arithmétiques » de k, c.-à-d., de quels éléments de k sont des carrés. Lorsque $k = \mathbb{C}$ ou $\mathbb{R}$, on peut donner des versions plus précises.

***Théorème 21.15* (Formes quadratiques sur $\mathbb{C}$).** — *Soient k un corps algébriquement clos,*[3] *V un k-ev de dimension n et Q une forme quadratique sur V, de rang $r \leq n$. Il existe une base $\mathscr{B}$ de V telle que $\mathrm{Mat}_{\mathscr{B}}(Q)$ soit diagonale, avec les r premiers coefficients égaux à 1 et les autres nuls, i.e. dans les coordonnées correspondant à cette base on ait : $Q(x_1, \dots, x_n) = x_1^2 + \cdots + x_r^2$.*

---

[3] Il suffit en fait que tout élément de k possède une racine carrée dans k, cf. la démonstration.

Démonstration. — D'après le théorème 21.14, il existe une base $(f_1, \ldots, f_n)$ de V orthogonale pour Q. Pour tout i, posons $c_i = Q(f_i)$. Alors le rang r de Q est le nombre de c_i non nuls et, quitte à renuméroter les f_i, on peut supposer que $c_i \neq 0$ pour $i \leq r$ et $c_i = 0$ pour $i > r$. Comme k est algébriquement clos, chaque $c_i \neq 0$ possède dans k une racine carrée $\mu_i \neq 0$. Posons alors $e_i = \mu_i^{-1} f_i$ pour $i \leq r$, et $e_i = f_i$ pour $i > r$. Alors la base $\mathscr{B} = (e_1, \ldots, e_r, e_{r+1}, \ldots, e_n)$ est encore orthogonale, et vérifie $Q(e_i) = 1$ pour $i \leq r$ et $Q(e_i) = 0$ pour $i > r$. Ceci prouve le théorème. $\square$

***Théorème 21.16* (Théorème d'inertie de Sylvester).** — *Soient V un $\mathbb{R}$-espace vectoriel de dimension n, Q une forme quadratique sur V et ϕ sa forme polaire.*

(i) *Soit $\mathscr{B} = (e_1, \ldots, e_n)$ une base orthogonale pour ϕ et soit p (resp. q) le nombre d'indices i tels que $Q(e_i) > 0$ (resp. < 0). Alors p et q ne dépendent pas de la base orthogonale choisie.*

(ii) *Le couple (p, q) s'appelle la* **signature** *de Q (ou de ϕ); on a* $\operatorname{rang}(\phi) = p + q$.

(iii) *On peut choisir $\mathscr{B}$ de sorte que la matrice diagonale $D = \operatorname{Mat}_{\mathscr{B}}(\phi)$ ait pour termes diagonaux* $(1, \ldots, 1, -1, \ldots, -1, 0, \ldots, 0)$, *le nombre de* 1 *(resp.* -1*) étant p (resp. q).*

Démonstration. — Posons $r = \operatorname{rang}(\phi)$. Soient $\mathscr{B} = (e_1, \ldots, e_n)$ et $\mathscr{C} = (f_1, \ldots, f_n)$ deux bases de V orthogonales pour ϕ. Notons p (resp. p') le nombre d'indices i tels que $Q(e_i) > 0$ (resp. $Q(f_i) > 0$) et q (resp. q') le nombre d'indices i tels que $Q(e_i) < 0$ (resp. $Q(f_i) < 0$). Alors

$$r = p + q = p' + q'$$

et il s'agit de montrer que $q = q'$ et $p = p'$. Quitte à renuméroter les éléments de $\mathscr{B}$ et $\mathscr{C}$, on peut supposer que

$$(\star) \qquad \begin{cases} Q(e_i) > 0 & \text{pour } i = 1, \ldots, p \\ Q(e_i) < 0 & \text{pour } i = p+1, \ldots, p+q \\ Q(e_i) = 0 & \text{pour } i > p+q = r\,; \end{cases} \qquad \begin{cases} Q(f_i) > 0 & \text{pour } i = 1, \ldots, p' \\ Q(f_i) < 0 & \text{pour } i = p'+1, \ldots, p'+q' \\ Q(f_i) = 0 & \text{pour } i > p'+q' = r\,. \end{cases}$$

Notons P_+ le sous-espace de V engendré par les vecteurs e_i tels que $Q(e_i) \geq 0$. Ces vecteurs sont au nombre de $n - q$, donc $\dim P_+ = n - q$. Soit x un élément arbitraire de P_+, écrivons $x = \sum_{i \in I} x_i e_i$, avec $I = \{1, \ldots, p\} \cup \{r+1, \ldots, n\}$; alors, d'après $(\star)$, on obtient

$$(1) \qquad Q(x) = \sum_{i=1}^{p} x_i^2\, Q(e_i) \geq 0.$$

D'autre part, soit P'_- le sous-espace de V engendré par les vecteurs f_j tels que $Q(f_j) < 0$. Ces vecteurs sont au nombre de q', donc $\dim P'_- = q'$. Soit y un élément non nul de P'_-, on peut écrire $y = \sum_{j=p'+1}^{p'+q'} y_j f_j$, avec au moins l'un des y_j non nul (car $y \neq 0$). Alors, d'après $(\star)$ à nouveau, on obtient

$$(2) \qquad Q(y) = \sum_{j=p'+1}^{p'+q'} y_j^2\, Q(f_j) < 0.$$

Par conséquent, on a $P_+ \cap P'_- = \{0\}$ donc P_+ et P'_- sont en somme directe, d'où

$$n = \dim V \geq \dim P_+ + \dim P'_- = n - q + q'$$

d'où $q \geq q'$. Échangeant les rôles des bases $\mathscr{B}$ et $\mathscr{C}$, on obtient de même $q' \geq q$, d'où $q = q'$, puis $p = r - q = r - q' = p'$. Ceci prouve (i).

Prouvons (iii). Soit $\mathscr{B} = (e_1, \ldots, e_n)$ comme ci-dessus ; pour $i = 1, \ldots, p+q$, notons c_i la racine carrée de $|Q(e_i)|$ et remplaçons e_i par $c_i^{-1} e_i$; on obtient ainsi une base orthogonale ayant la propriété désirée. $\square$

22. Quadriques et coniques projectives, théorème de Pascal

Le but de cette section est d'étudier les quadriques projectives de $\mathbb{P}^n(k)$, c.-à-d. les sous-ensembles

$$\mathscr{V}(Q) = \{[x_0, \dots, x_n] \in \mathbb{P}^n(k) \mid Q(x_0, \dots, x_n) = 0\}$$

où Q est une forme quadratique sur k^{n+1}, i.e. un polynôme homogène de degré 2 :

$$Q(x) = \sum_{i=0}^{n} a_i x_i^2 + \sum_{0 \le i < j \le n} b_{ij} x_i x_j.$$

Remarquons tout de suite que, pour un point $p = [x]$ de $\mathbb{P}^n(k)$, le point x de k^{n+1} n'est défini qu'à homothétie près donc on ne peut pas parler de la *valeur* de Q en p, mais comme Q est un polynôme homogène de degré 2 alors $Q(\lambda x) = \lambda^2 Q(x)$ pour tout $\lambda \in k^\times$, donc le fait que $Q(x)$ soit nul ne dépend que de p, ce qui justifie la définition de $\mathscr{V}(Q)$. Lorsque $n = 2$, on dit « conique » au lieu de quadrique.

Même si l'on ne s'intéressera dans la suite qu'aux quadriques (et surtout aux coniques), nous donnons ci-dessous des définitions générales, en guise d'introduction à la géométrie algébrique.

***Définition 22.1* (Hypersurfaces de k^n).** — Soit $P \in k[X_1, \dots, X_n]$ un polynôme non constant.(4) On définit sa *variété des zéros* dans l'espace affine k^n, notée $\mathscr{V}(P)$,(5) par :

$$\mathscr{V}(P) = \{x = (x_1, \dots, x_n) \mid P(x) = 0\}$$

et l'on dit que c'est une hypersurface (algébrique) de k^n. En fait, quand on dit cela, on suppose implicitement que le corps k est algébriquement clos, par exemple $k = \mathbb{C}$, ou bien que k est considéré comme **sous-corps d'un corps algébriquement clos** $\overline{k}$, par exemple $k = \mathbb{R}$ et $\overline{k} = \mathbb{C}$.

En effet, lorsque k n'est pas algébriquement clos, il arrive que $\mathscr{V}(P)$ ne soit « pas intéressant », par exemple si $k = \mathbb{R}$, et si l'on pose $P_c = X^2 + Y^2 + c$ pour $c \in \mathbb{R}$, alors

$$\mathscr{V}(P_0) = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 0\}$$

se réduit au point $(0, 0)$, au lieu d'être une honnête « courbe algébrique » comme par exemple le cercle

$$\mathscr{V}(P_{-1}) = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$$

ou l'hyperbole

$$\{(x, y) \in \mathbb{R}^2 \mid xy = 1\} = \mathscr{V}(XY - 1)$$

ou la parabole

$$\{(x, y) \in \mathbb{R}^2 \mid y = x^2\} = \mathscr{V}(Y - X^2).$$

Pire encore, $\mathscr{V}_{\mathbb{R}}(P_1) = \{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = -1\}$ est vide. Toutefois, dans $\mathbb{C}$ on a $(x + iy)(x - iy) = x^2 + y^2$ donc dans $\mathbb{C}[X, Y]$ si l'on fait le changement de variables $X' = X + iY$ et $Y' = -X + iY$, alors $P_1 = 1 - X'Y'$ et donc

$$\mathscr{V}_{\mathbb{C}}(P_1) = \{(x', y') \in \mathbb{C}^2 \mid x'y' = 1\}$$

(4) On suppose P *non constant* car $\mathscr{V}(P) = k^n$ si $P = 0$, tandis que $\mathscr{V}(P) = \varnothing$ si P est une constante $\neq 0$.

(5) On note $\mathscr{V}$ pour « Variété » ; d'autres auteurs notent $\mathcal{Z}(P)$ pour « Zéros ».

est une « honnête » hyperbole, et le fait que $\mathscr{V}_{\mathbb{R}}(P_1) = \varnothing$ signifie simplement que cette hyperbole « complexe » n'a pas de « points réels ». On verra bien d'autres exemples de la sorte dans la suite.

Toutefois, nous ne voulons pas imposer à k d'être algébriquement clos, car précisément on veut pouvoir étudier des courbes algébriques dans $\mathbb{R}^2$ telles que cercles, ellipses, hyperboles et paraboles...

***Définition 22.2* (Polynômes homogènes).** — On dit qu'un polynôme non nul $P \in k[X_1, \dots, X_r]$ est *homogène* de degré d si tous les monômes qui le composent sont de même degré total d. Par exemple, si $r = 3$ un polynôme homogène de degré 1 est de la forme $a_1X_1 + a_2X_2 + a_3X_3$, et un polynôme homogène de degré 2 de la forme :

$$a_1X_1^2 + a_2X_2^2 + a_3X_3^2 + a_{1,2}X_1X_2 + a_{1,3}X_1X_3 + a_{2,3}X_2X_3.$$

Exercice 22.3. — Soit n un entier ≥ 2. Quelle est la dimension du k-espace vectoriel des polynômes en n variables sur k, homogènes de degré 2 ?

***Définition 22.4* (Hypersurfaces de $\mathbb{P}^n(k)$).** — Soit $P \in k[X_0, \dots, X_n]$ un polynôme en $(n+1)$ variables **homogène** de degré $d \geq 1$. On définit sa *variété des zéros* dans l'espace projectif $\mathbb{P}^n(k)$, encore notée $\mathscr{V}(P)$, par :

$$\mathscr{V}(P) = \{[x] = [x_0, x_1, \dots, x_n] \in \mathbb{P}^n(k) \mid P(x) = 0\}$$

et l'on dit que c'est une hypersurface (algébrique) de $\mathbb{P}^n(k)$. Remarquons d'abord que ceci est **bien défini** : en effet, si on remplace $x \in k^{n+1}$ par λx, avec $\lambda \in k^\times$, alors, comme P est homogène de degré d, on a $P(\lambda x) = \lambda^d P(x)$, donc la nullité ou non de $P(x)$ ne dépend que de $[x]$.[6] Par exemple, si P est homogène de degré 1, i.e. si $P = a_0X_0 + \cdots + a_nX_n$, alors $\mathscr{V}(P)$ est simplement l'hyperplan projectif $\mathbb{P}(\mathrm{Ker}(f))$, où f est la forme linéaire $f(x) = a_0x_0 + \cdots + a_nx_n$.

Comme dans le paragraphe précédent, quand on considère $\mathscr{V}(P)$ avec P homogène de degré $d > 1$, on suppose implicitement que le corps k est algébriquement clos, par exemple $k = \mathbb{C}$, ou bien que k est considéré comme sous-corps d'un corps algébriquement clos $\overline{k}$, par exemple $k = \mathbb{R}$ et $\overline{k} = \mathbb{C}$.

En effet, si $k = \mathbb{R}$ et si l'on note X, Y, Z au lieu de X_0, X_1, X_2 et qu'on considère le polynôme $P = X^2 + Y^2 + Z^2$ homogène de degré 2, alors

$$\mathscr{V}_{\mathbb{R}}(P) = \{[x, y, z] \in \mathbb{P}^2(\mathbb{R}) \mid x^2 + y^2 + z^2 = 0\} = \varnothing.$$

Par contre, dans $\mathbb{C}[X, Y, Z]$, on a $X^2 + Y^2 + Z^2 = (X + iY)(X - iY) + Z^2$ donc si l'on fait le changement de variable $X' = X + iY$ et $Y' = -X + iY$, alors

$$\mathscr{V}_{\mathbb{C}}(P) = \{[x', y', z] \in \mathbb{P}^2(\mathbb{C}) \mid x'y' = z^2\}$$

est une honnête courbe algébrique projective, appelée une conique projective (cf. ci-dessous).

Dans la suite de cette section, on suppose $\boxed{\mathrm{car}(k) \neq 2}$ et V désigne un k-ev de dimension $n+1$, d'où $\dim(\mathbb{P}(V)) = n$. Sauf mention du contraire, les formes quadratiques considérées seront supposées *non nulles*, i.e. dans la suite la phrase « Soit Q une forme quadratique sur V » signifie : « Soit Q une forme quadratique sur V, non nulle ».

[6] Par contre, on ne peut pas parler de la « valeur » de P au point $[x]$.

Définitions 22.5. — Soit Q une forme quadratique sur V, non nulle.

(i) Un vecteur $v \in V$ est dit **isotrope** (pour Q) si l'on a $Q(v) = 0$.

(ii) L'ensemble $C(Q) = \{v \in V \mid Q(v) = 0\}$ des vecteurs isotropes est appelé le **cône isotrope**. C'est un *cône*, au sens où il est stable par homothéties : si $v \in C(Q)$ et $\lambda \in k^\times$ alors $Q(\lambda v) = \lambda^2 Q(v) = 0$ donc $\lambda v \in C(Q)$.

(iii) L'image de $C(Q) - \{0\}$ dans $\mathbb{P}(V)$ est l'hypersurface de $\mathbb{P}(V)$ définie par le polynôme homogène Q, i.e. c'est :

$$\mathscr{V}(Q) = \{[v] \in \mathbb{P}(V) \mid Q(v) = 0\}.$$

On dit que $\mathscr{V}(Q)$ est la **quadrique projective** définie par Q, et lorsque $\dim \mathbb{P}(V) = 2$ on dit **conique** au lieu de quadrique.

Exemples 22.6. — (1) Si Q est la forme quadratique sur $\mathbb{R}^2$ définie par $Q(x_1, x_2) = x_1 x_2$, alors le cône isotrope est la réunion de la droite d'équation $x_1 = 0$ et de celle d'équation $x_2 = 0$, et la quadrique $\mathscr{V}(Q) \subset \mathbb{P}^1(\mathbb{R})$ est formée des deux points $[0, 1]$ et $[1, 0]$.

(2) Si Q est la forme quadratique sur $\mathbb{R}^3$ définie par $Q(x_1, x_2, x_3) = x_1^2 + x_2^2 - x_3^2$, alors le cône isotrope est le cône d'équation $x_1^2 + x_2^2 = x_3^2$: la section par chaque plan « horizontal » d'équation $x_3 = c$ donne le cercle de centre $(0, 0, c)$ et de rayon $r = |c|$. Son image $\mathscr{V}(Q)$ dans $\mathbb{P}^2(\mathbb{R})$ est formée du « cercle » $\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 = 1\}$ dans le plan affine $\mathscr{P} = \mathbb{P}^2(\mathbb{R})$ privé de la droite $\mathscr{D}_\infty$ d'équation $z = 0$; il lui manque les deux points d'intersection avec $\mathscr{D}_\infty$, qui sont les deux points $[1, i, 0]$ et $[1, -i, 0]$ de $\mathbb{P}^2(\mathbb{C})$.

Remarque. — Attention ! Il ne faut pas confondre le cône isotrope $C(Q) = \{x \in V \mid Q(x) = 0\}$ avec le sev $N(Q) = \{x \in V \mid \forall y \in V,\ \phi(x, y) = 0\}$. On a toujours $N(Q) \subset C(Q)$ mais l'inclusion est en général stricte : dans les deux exemples précédents Q est non dégénérée donc $N(Q) = \{0\}$, tandis que $C(Q)$ est un cône $\neq \{0\}$.

***Exemple 22.7* (important)**. — Décrivons tout d'abord les quadriques d'une droite projective $\mathbf{D} = \mathbb{P}(E)$, où $\dim(E) = 2$. Soit Q une forme quadratique sur E et soient $\mathscr{B} = (e_0, e_1)$ une base de E orthogonale pour Q et (x_0, x_1) les coordonnées correspondantes. Quitte à échanger e_0 et e_1 on peut supposer que $\lambda = Q(e_0)$ est $\neq 0$; alors en remplaçant Q par $\lambda^{-1} Q$ (ce qui ne change pas la quadrique) on se ramène au cas où $Q(e_0) = 1$, d'où $Q(x_0, x_1) = x_0^2 - \delta x_1^2$, pour un certain $\delta \in k$. Distinguons les cas suivants :

(i) $\delta = 0$, d'où $Q(x_0, x_1) = x_0^2$. Dans ce cas, $\mathscr{V}(Q)$ est formée d'un point « double », i.e. c'est le point $p = [0, 1]$ de $\mathbf{D}$ « compté deux fois ».

(ii) $\delta \neq 0$. Soit α une racine carrée de δ dans le corps algébriquement clos $\overline{k}$, alors $Q(x_0, x_1) = (x_0 - \alpha x_1)(x_0 + \alpha x_1)$. Donc $\mathscr{V}(Q)$ est formée des deux points distincts $[\alpha, 1]$ et $[-\alpha, 1]$. Ces deux points sont dans $\mathbb{P}(E)$ ssi $\alpha \in k$; sinon, notant k' l'extension quadratique $k[\alpha] = k[T]/(T^2 - \delta)$ de k, ils sont dans $\mathbb{P}^1(k')$.[7]

Revenons à un k-ev V de dimension $n + 1 \geq 3$ et décrivons l'intersection de la quadrique $\mathscr{V}(Q) \subset \mathbb{P}(V)$ et d'une droite projective $\mathbf{D} = \mathbb{P}(E)$, pour E un sev de V de dimension 2. Notons Q_E la restriction de Q à E et remarquons que $\mathbf{D} \cap \mathscr{V}(Q)$ est la variété des zéros $\mathscr{V}(Q_E) \subset \mathbf{D}$.

Lemme 22.8. — *On a l'une des trois alternatives suivantes :*

[7] Plus précisément, ils sont dans $\mathbb{P}(E_{k'})$, où $E_{k'}$ désigne le k'-espace vectoriel déduit de E par extension des scalaires de k à k', cf. 23.14.

a) *$Q_E = 0$ et $\mathbf{D} \subset \mathscr{V}(Q)$.*

b) *Q_E est non dégénérée. Alors $\mathbf{D} \cap \mathscr{V}(Q)$ est formée de deux points distincts $p \neq q$ (éventuellement à coordonnées dans une extension quadratique de k).*

c) *Q_E est de rang 1. Alors $\mathbf{D} \cap \mathscr{V}(Q)$ est formée d'un seul point p.*

Démonstration. — On a $Q_E = 0$ ssi $\mathscr{V}(Q_E) = \mathbf{D}$, et ceci équivaut à $\mathbf{D} \subset \mathscr{V}(Q)$. Supposons donc $Q_E \neq 0$. Soit (e_0, e_1) une base orthogonale de E. Comme dans l'exemple précédent, on se ramène au cas où $Q(e_0) = 1$ et l'on pose alors $Q(e_1) = -\delta$. Sous ces conditions, on a

$$\mathbf{D} \cap \mathscr{V}(Q) = \{[xe_0 + ye_1] \mid x^2 + \delta y^2 = 0\}$$

où $(x, y) \neq (0, 0)$.

Supposons Q_E non dégénérée, i.e. $\delta \neq 0$. Notons α une racine carrée de δ (éventuellement dans une extension quadratique k' de k). Alors $\mathbf{D} \cap \mathscr{V}(Q)$ est formée des deux points distincts $p = [\alpha e_0 + e_1]$ et $q = [-\alpha e_0 + e_1]$.

Enfin, supposons Q_E de rang 1, i.e. $\delta = 0$. Dans ce cas, $\mathbf{D} \cap \mathscr{V}(Q)$ est formée du « point double » $p = [e_1]$ (défini par l'équation $x^2 = 0$). □

Corollaire 22.9. — *Soit $\mathscr{C} = \mathscr{V}(Q)$ une quadrique de $\mathbb{P}(V)$. Si $\mathscr{C}$ contient trois points d'une droite $\mathbf{D}$ alors $\mathscr{C}$ contient $\mathbf{D}$.*

Démonstration. — Ceci découle de la proposition précédente. □

Avant d'énoncer le théorème sur la conique passant par cinq points donnés (22.12) et celui de Pascal (22.14), qui nous intéresseront principalement dans le cas non dégénéré, on a besoin d'énoncer quelques résultats qui nous permettront de traiter le cas dégénéré.

Proposition 22.10. — *Soit $\mathscr{C} = \mathscr{V}(Q)$ une conique d'un plan projectif $\mathbb{P}(V)$. Supposons que $\mathscr{C}$ contienne une droite $\mathbf{D}$.*

(i) *Alors $\mathscr{C}$ est dégénérée.*

(ii) *Plus précisément, si l'on choisit des coordonnées homogènes $[x, y, z]$ telles que $\mathbf{D}$ ait pour équation $Z = 0$, alors $Q = ZL(X, Y, Z)$ pour une certaine forme linéaire L.*

(iii) *Si L n'est pas multiple de Z, alors Q est de rang 2 et $\mathscr{C}$ est la réunion de $\mathbf{D}$ et de la droite $\mathbf{D}'$ d'équation $L = 0$. Sinon, $Q = \lambda Z^2$ est de rang 1 et dans ce cas on dit que $\mathscr{C}$ est la* « droite double » *$\mathbf{D}$.*

Démonstration. — Soit ϕ la forme polaire de Q. Écrivons $\mathbf{D} = \mathbb{P}(E)$, où E est un sev de V de dimension 2. Par hypothèse, la restriction de Q à E est nulle, donc pour tout $x, y \in E$ on a :

$$\phi(x, y) = \frac{1}{2}\big(Q(x + y) - Q(x) - Q(y)\big) = 0.$$

Soient (e_1, e_2) une base de E, complétons-la en une base $\mathscr{B} = (e_1, e_2, e_3)$ de V et notons (x, y, z) les coordonnées dans cette base. Alors $A = \mathrm{Mat}_{\mathscr{B}}(\phi)$ est de la forme suivante :

$$\begin{pmatrix} 0 & 0 & a \\ 0 & 0 & b \\ a & b & c \end{pmatrix}$$

où $a = \phi(e_1, e_3)$, $b = \phi(e_2, e_3)$ et $c = Q(e_3)$ ne sont pas tous nuls (car Q est supposée non nulle). Alors on a

$$Q(X, Y, Z) = cZ^2 + 2Z(aX + bY) = Z(2aX + 2bY + cZ),$$

ce qui donne (ii) avec $L(X,Y,Z) = (2aX + 2bY + cZ)$. De plus, on voit que A est de rang ≤ 2 (car ses colonnes 1 et 2 sont liées), d'où (i).

Enfin, on voit que A est de rang 1 ssi $a = 0 = b$, ce qui correspond au cas où L est multiple de Z. Le point (iii) en découle. □

Remarques 22.11. — (1) Réciproquement, la réunion de deux droites $\mathbf{D}$ et $\mathbf{D}'$ du plan projectif est une conique. En effet, soient L et L' les formes linéaires (uniques à homothétie près) définissant $\mathbf{D}$ et $\mathbf{D}'$ et soit $Q = LL'$. Alors, pour tout $[x,y,z] \in \mathbb{P}(V)$, on a $Q(x,y,z) = L(x,y,z)L'(x,y,z)$ et ceci est nul ssi l'un au moins de $L(x,y,z)$ et $L'(x,y,z)$ est nul : ceci montre que $\mathscr{V}(Q)$ est la réunion de $\mathbf{D}$ et $\mathbf{D}'$.

(2) Il résulte de la proposition que si $\mathscr{C}$ est une conique dégénérée (i.e. la réunion de deux droites ou une droite « double ») et si $p_1,\dots,p_5$ sont cinq points distincts de $\mathscr{C}$, alors au moins trois de ces points sont alignés.

Théorème 22.12. — *Soient $\mathbb{P}(V)$ un plan projectif et $p_1,\dots,p_5$ cinq points distincts de $\mathbb{P}(V)$, quatre d'entre eux n'étant jamais alignés. Alors il existe une unique conique $\mathscr{C}$ passant par ces cinq points.*

Démonstration. — Distinguons deux cas. (1) Supposons que trois points soient alignés sur une droite $\mathbf{D}$, par exemple p_1,p_2,p_3. Si une conique $\mathscr{C}$ contient les p_i alors, d'après 22.9 et 22.10, elle contient $\mathbf{D}$ donc elle est dégénérée et est la réunion de $\mathbf{D}$ et d'une seconde droite $\mathbf{D}'$. Alors, comme p_4 et p_5 ne sont pas sur $\mathbf{D}$ ils doivent être sur $\mathbf{D}'$ et donc $\mathbf{D}' = (p_4p_5)$. Ceci montre que, dans ce cas, $\mathbf{D} \cup \mathbf{D}'$ est l'unique conique contenant les p_i.

(2) Supposons maintenant que trois des p_i ne sont jamais alignés. Alors (p_1,p_3,p_5,p_2) [(8)] forment un repère projectif et dans ce repère ils ont pour coordonnées homogènes respectives : $[1,0,0]$, $[0,1,0]$, $[0,0,1]$, et $[1,1,1]$. De même, $p_4 = [a,b,c]$ avec a,b,c tous non nuls et deux à deux distincts (car si on avait, par exemple, $c = 0$ (resp. $a = b$) alors p_1,p_3,p_4 (resp. p_5,p_2,p_4) seraient alignés).

Soit $Q(X,Y,Z) = \alpha X^2 + \beta Y^2 + \gamma Z^2 + uYZ + vZX + wXY$ une forme quadratique arbitraire. Elle s'annule en p_1 (resp. p_3, resp. p_5) ssi $\alpha = 0$ (resp. $\beta = 0$, resp. $\gamma = 0$), et l'annulation en p_2 et p_4 équivaut aux deux équations linéaires en u,v,w suivantes :

$$u + v + w = 0 \qquad \text{et} \qquad bc\,u + ca\,v + ab\,w = 0.$$

On en déduit $w = -u - v$ puis $b(c-a)\,u + a(b-c)\,v = 0$, d'où $v = \dfrac{b}{a}\,\dfrac{c-a}{b-c}\,u$, puis

$$w = -u - v = \frac{-u}{a(b-c)}\Big(a(b-c) - b(a-c)\Big) = \frac{c}{a}\,\frac{a-b}{b-c}\,u.$$

Ceci détermine de façon unique Q, à homothétie près, i.e. en prenant $u = a(b-c)$ on obtient que

$$Q(X,Y,Z) = a(b-c)YZ + b(c-a)ZX + c(a-b)XY$$

est l'équation de l'unique conique qui passe par le repère standard $[1,0,0]$, $[0,1,0]$, $[0,0,1]$, $[1,1,1]$ et par le point $[a,b,c]$. (Celle-ci est non dégénérée d'après la remarque 22.11.) □

[(8)] Ce choix de numérotation est lié à la démonstration du théorème de Pascal 22.14 qui va suivre.

***Définition 22.13* (Côtés opposés d'un hexagone).** — Soient A, B, C, D, E, F six points d'un plan projectif, dont trois ne sont jamais alignés.(9) Pour chaque numérotation $p_1, \dots, p_6$ de ces points, appelons « *paires de côtés opposés* » (pour la numérotation donnée) les trois paires de droites

$$\big((p_1p_2), (p_4p_5)\big), \qquad \big((p_2p_3), (p_5p_6)\big), \qquad \big((p_3p_4), (p_6p_1)\big)$$

et notons P_1 (resp. P_2, resp. P_3) le point de concours de la 1ère paire (resp. de la 2ème, resp. 3ème). Ces trois points sont distincts. (Si on avait par exemple $P_1 = P_2$, ce point appartiendrait à $(p_1p_2) \cap (p_2p_3)$ et à $(p_4p_5) \cap (p_5p_6)$ donc devrait être égal à p_2 et à p_5, impossible car $p_2 \neq p_5$.)

Si $k = \mathbb{R}$ et si les points $p_1, \dots, p_6$ du plan affine $\mathscr{E} = \mathbb{R}^2$ forment *dans cet ordre* les sommets d'un hexagone convexe régulier (donc inscrit dans un cercle), alors la notion de « côtés opposés » a le sens habituel et les côtés opposés sont parallèles (et donc dans le plongement projectif $\widehat{\mathbb{P}}(\mathscr{E})$, les points P, Q, R appartiennent à la droite à l'infini). Mais dans la définition précédente, la numérotation des p_i est arbitraire, ce qui donne plus de configurations possibles.

Théorème 22.14. — *Soient A, B, C, D, E, F six points d'un plan projectif, dont trois ne sont jamais alignés.*

(i) **(Théorème de Pascal)** (10) *Si ces points appartiennent à une même conique $\mathscr{C}$ (nécessairement non dégénérée) alors, pour toute numérotation $p_1, \dots, p_6$, les points de concours des trois paires de côtés opposés sont alignés.*

(ii) *Réciproquement, si pour une numérotation $p_1, \dots, p_6$ les points de concours des trois paires de côtés opposés sont alignés, alors il existe une unique conique $\mathscr{C}$ passant par A, B, C, D, E, F.*

Démonstration. — Choisissons une numérotation $p_1, \dots, p_6$. Reprenant les notations de la démonstration précédente, on peut supposer que p_1, p_3, p_5, p_2, p_4 et p_6 ont pour coordonnées homogènes respectives :

$$[1,0,0], \quad [0,1,0], \quad [0,0,1], \quad [1,1,1], \quad [a,b,c] \quad \text{et} \quad [u,v,w],$$

avec a, b, c (resp. u, v, w) non nuls et deux à deux distincts. D'après le théorème précédent, l'unique conique $\mathscr{C}$ passant par $p_1, \dots, p_5$ est donnée par

$$Q(X,Y,Z) = a(b-c)YZ + b(c-a)ZX + c(a-b)XY,$$

et donc p_6 appartient à $\mathscr{C}$ ssi on a :

$$0 = Q(u,v,w) = a(b-c)vw + b(c-a)wu + c(a-b)uv.$$

Déterminons à quelle condition les points de concours des trois paires de côtés opposés sont alignés.

La droite (p_1p_2), resp. (p_4p_5), a pour équation $y = z$, resp. $bx = ay$, donc elles se coupent au point $P_1 = [a,b,b]$. De même, la droite (p_2p_3), resp. (p_5p_6), a pour équation $x = z$, resp. $vx = uy$, donc elles se coupent au point $P_2 = [u,v,u]$.

Enfin, la droite (p_3p_4), resp. (p_6p_1), a pour équation $cx = az$, resp. $wy = vz$, donc elles se coupent au point $P_3 = [aw, cv, cw]$.

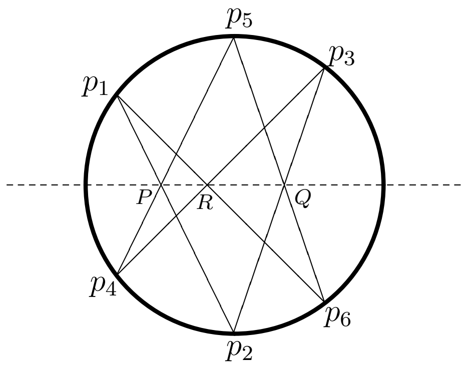
(9)En particulier, ces six points sont deux à deux distincts.

(10)Blaise Pascal, mathématicien et philosophe français (1623-1662), qui fut l'élève de Desargues.

Alors P_1, P_2, P_3 sont alignés ssi le déterminant $\begin{vmatrix} a & u & aw \\ b & v & cv \\ b & u & cw \end{vmatrix}$ est nul, or on voit qu'il vaut :

$$vw\, a(c-b) + wu\, b(a-c) + uv\, c(b-a) = -Q(u,v,w).$$

Ceci montre (ii), et aussi (i) puisque la numérotation $p_1, \dots, p_6$ a été choisie arbitrairement. □



22.15. Classification des coniques projectives réelles. — Il résulte du théorème d'inertie de Sylvester 21.16 qu'il n'y a, à homographie près, que cinq types de coniques réelles $\mathscr{C} = \mathscr{V}(Q) \subset \mathbb{P}^2(\mathbb{R})$. En effet, d'après le théorème de Sylvester, il existe une base $\mathscr{B}$ de $\mathbb{R}^3$ telle que, dans les coordonnées correspondantes, on ait $Q(X,Y,Z) = aX^2 + bY^2 + cZ^2$, avec a, b, c dans $\{-1, 0, 1\}$ et non tous nuls. Comme Q et $\pm Q$ définissent la même conique, on a les cinq alternatives suivantes :

(1) Q est de rang 1. Dans ce cas, on peut supposer que $Q = X^2$ et alors $\mathscr{C}$ est la droite double de $\mathbb{P}^2(\mathbb{R})$ d'équation $x^2 = 0$.

(2) Q est de rang 2. Dans cas cas, on peut supposer que $Q = X^2 \pm Y^2$ et l'on a les deux sous-cas :

2a) $Q = X^2 - Y^2 = (X - Y)(X + Y)$. Alors $\mathscr{C}$ est la réunion des deux droites projectives d'équations $x = y$ et $x = -y$.

2b) $Q = X^2 + Y^2$. Alors dans $\mathbb{P}^2(\mathbb{C})$, $\mathscr{C}_{\mathbb{C}}$ est la réunion des deux droites projectives d'équations $x = iy$ et $x = -iy$; elles se coupent au point $p = [0, 0, 1]$ qui est le seul point réel de $\mathscr{C}$.

(3) Q est de rang 3, i.e. non dégénérée. On peut alors supposer que $Q = X^2 + Y^2 \pm Z^2$ et l'on a les deux sous-cas :

3a) $Q = X^2 + Y^2 + Z^2$. Dans ce cas, $\mathscr{C}$ n'a pas de point réel.

3b) $Q = X^2 + Y^2 - Z^2$.

On voit donc qu'à homographie près, $Q = X^2 + Y^2 - Z^2$ est l'unique conique projective non dégénérée ayant des points réels. Remarquons que si on prend comme droite à l'infini $\mathscr{D}_\infty$ la droite d'équation $z = 0$ (resp. $y = 0$) alors dans le plan affine $\mathscr{E} = \mathbb{P}^2(\mathbb{R}) - \mathscr{D}_\infty$, identifié aux triplets de points $(x, y, 1)$ (resp. $(x, 1, z)$) de $\mathbb{R}^3$, on obtient l'ellipse (resp. l'hyperbole) d'équation $x^2 + y^2 = 1$ (resp. $x^2 - z^2 = 1$).

De plus, si l'on fait le changement de coordonnées $u = z + y$ et $v = z - y$ (de sorte que $z^2 - y^2 = uv$) et qu'on prend comme droite à l'infini $\mathscr{D}_\infty$ la droite d'équation $v = 0$ alors dans le plan affine $\mathscr{E} = \mathbb{P}^2(\mathbb{R}) - \mathscr{D}_\infty$, identifié aux triplets de points $(x, u, 1)$ de $\mathbb{R}^3$, on obtient la parabole d'équation $u = x^2$.

On voit donc qu'en passant aux coniques projectives, on fait disparaître la distinction entre les trois sortes de coniques affines réelles non dégénérées (ellipses, hyperboles, paraboles).

Terminons cette section en introduisant les notions de *plan hyperbolique* et de *sev totalement isotrope*. Soient V un k-ev de dimension $n \geq 2$, Q une forme quadratique sur V, ϕ sa forme polaire et $N(Q)$ son noyau.

Lemme 22.16. — *Soit E un sev de V et Q_E la restriction de Q à E.*

(i) *Alors Q_E est non dégénérée ssi $E \cap E^{\perp} = \{0\}$. Dans ce cas, on a :*

(ii) $V = E \oplus E^{\perp}$ *et* : (iii) $Q_{E^{\perp}}$ *est non dégénérée.*

Démonstration. — On a $N(Q_E) = \{x \in E \mid \forall y \in E, \quad \phi(x, y) = 0\} = E \cap E^{\perp}$ d'où (i). Alors (ii) découle de 21.9 (ii).

Prouvons (iii). Soit $\mathscr{B}_1$ (resp. $\mathscr{B}_2$) une base de E (resp. $E^{\perp}$) et A_1 (resp. A_2) la matrice de Q_E (resp. $Q_{E^{\perp}}$) dans cette base. Alors $\mathscr{B} = \mathscr{B}_1 \cup \mathscr{B}_2$ est une base de V et $\mathrm{Mat}_{\mathscr{B}}(Q)$ égale $A = \begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$, d'où $\mathrm{dét}(A) = \mathrm{dét}(A_1)\,\mathrm{dét}(A_2)$. Ceci est non nul (car Q est non dégénérée), d'où $\mathrm{dét}(A_2) \neq 0$ donc $Q_{E^{\perp}}$ est non dégénérée. □

Proposition 22.17. — *Soit $e_1 \in V$ un vecteur isotrope tel que $e_1 \notin N(Q)$. Alors :*

(i) *Il existe un vecteur isotrope e_2 tel que $\phi(e_1, e_2) = 1$.*

(ii) *Soient $E = \mathrm{Vect}(e_1, e_2)$ et Q_E la restriction de Q à E. Alors (e_1, e_2) est une base de E et $\mathrm{Mat}_{(e_1,e_2)}(Q_E) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ donc Q_E est non dégénérée.*

(iii) *Par conséquent, $V = E \oplus E^{\perp}$.*

Démonstration. — Comme $e_1 \notin N(Q)$ il existe $v \in V$ tel que $\lambda = \phi(e_1, v)$ soit $\neq 0$. Remplaçant v par $\lambda^{-1}v$, on se ramène au cas où $\phi(e_1, v) = 1$. Soit $c = Q(v)$. Si $c = 0$ on peut prendre $e_2 = v$. Sinon, comme

$$Q(v + \mu e_1) = Q(v) + 2\mu\phi(v, e_1) = c + 2\mu,$$

alors $e_2 = v - (c/2)e_1$ vérifie $Q(e_2) = 0$ et $\phi(e_2, e_1) = 1$. Alors e_2 n'est pas colinéaire à e_1, donc (e_1, e_2) forme une base du sev E et la matrice de Q_E est comme indiqué. Ceci montre que Q_E est non dégénérée. Ceci prouve (i) et (ii). Alors (iii) découle du lemme précédent. □

Définition 22.18. — Un sev E de dimension 2 de V est un **plan hyperbolique** s'il possède une base (e_1, e_2) comme ci-dessus. La proposition précédente démontre donc que tout vecteur isotrope $v \notin N(Q)$ appartient à au moins un plan hyperbolique.

Définition 22.19. — Un sev F de V est dit *totalement isotrope* si $Q_F = 0$, c.-à-d. si $\phi(x, y) = 0$ pour tout $x, y \in F$.

Lemme 22.20. — *Supposons Q* non dégénérée. *Alors, si F est un sev totalement isotrope de dimension p, on a $2p \leq n = \dim(V)$.*

Démonstration. — Soit $(f_1, \ldots, f_p)$ une base de F. Comme Q est non dégénérée, l'application $\theta : V \to V^*$ est un isomorphisme, donc la famille $\big(\theta(f_1), \ldots, \theta(f_p)\big)$ est libre. On peut donc la compléter en une base $\mathscr{C}$ de V^*. Soit $(g_1, \ldots, g_n)$ la base de V dont $\mathscr{C}$ est la base duale. Alors, pour $i, j = 1, \dots, p$ on a : $\phi(f_i, g_j) = \theta(f_i)(g_j) = \delta_{ij}$ (rappelons que $\delta_{ij} = 1$ si $i = j$ et $= 0$ sinon).

Il en résulte que F et $G = \mathrm{Vect}(g_1, \dots, g_p)$ sont en somme directe, car si on a une égalité $\sum_{j=1}^{p} x_j f_j = \sum_{j=1}^{p} y_j g_j$ alors en appliquant $\phi(f_i, -)$ on obtient $0 = y_i$ pour tout $i = 1, \dots, p$. Comme $\dim(G) = p$ (car les g_i sont linéairement indépendants), on en déduit que $2p = \dim(F \oplus G) \leq \dim(V)$. □

Exemple 22.21. — Si $n = 2p$ et si V est la somme directe orthogonale de p plans hyperboliques, i.e. si dans certaines coordonnées Q est donnée par

$$Q(X_1, \dots X_{2p}) = X_1 X_2 + \cdots + X_{2p-1} X_{2p}$$

alors le cône isotrope $C(Q)$ contient les deux sous-espaces de dimension p totalement isotropes $F_1 = \mathrm{Vect}(e_1, e_3, \dots, e_{2p-1})$ et $F_2 = \mathrm{Vect}(e_2, e_4, \dots e_{2p})$. Et donc la quadrique projective $\mathscr{V}(Q) = \{[x_1, \dots, x_{2p}] \in \mathbb{P}^{2p-1}(k) \mid Q(x) = 0\}$ contient les deux sous-espaces projectifs $\mathbb{P}(F_1)$ et $\mathbb{P}(F_2)$, chacun de dimension $p - 1$.

23. Hyperplans tangents à une hypersurface affine ou projective

Pour énoncer, dans la section suivante, le théorème de Brianchon, on doit introduire la définition suivante :

Définition 23.1. — Soient k un corps de caractéristique $\neq 2$, V un k-ev de dimension $n + 1 \geq 3$ et Q une forme quadratique *non dégénérée* sur V. Pour tout $v \neq 0$ dans V, on note $(kv)^\perp$ l'hyperplan de V orthogonal, pour la forme polaire ϕ de Q, à la droite kv.

(i) Pour tout point $p = [v]$ de la quadrique projective $\mathscr{V}(Q) \subset \mathbb{P}(V)$, *l'hyperplan* (projectif) *tangent* à $\mathscr{V}(Q)$ au point p est l'hyperplan projectif $\mathbb{P}((kv)^\perp)$.

(ii) De même, pour tout point $v \neq 0$ du cône isotrope $C(Q) \subset V$, *l'hyperplan* (affine) *tangent* à $C(Q)$ au point v est l'hyperplan $v + (kv)^\perp$, qui ici égale $(kv)^\perp$ car $v \in (kv)^\perp$ puisque $\phi(v, v) = Q(v) = 0$.

Ceci est un cas particulier de la définition d'hyperplan tangent en un point *lisse* (voir plus bas) d'une hypersurface affine ou projective, que nous donnons plus bas après quelques « rappels » sur les dérivées partielles et la différentielle d'un polynôme.

***Rappels 23.2* (Polynômes à plusieurs indéterminées)**. — Soient k un corps et $r \in \mathbb{N}^*$. L'anneau des polynômes en r variables (ou *indéterminées*), à coefficients dans k, noté $k[X_1, \dots, X_r]$, est le k-espace vectoriel (de dimension infinie) dont une base est donnée par les monômes

$$X^{\mathbf{a}} = X_1^{a_1} \cdots X_r^{a_r} \quad \text{pour } \mathbf{a} = (a_1, \dots, a_r) \in \mathbb{N}^r,$$

i.e. c'est l'ensemble de toutes les sommes **finies** $P = \sum_{\mathbf{a} \in \mathbb{N}^r} \alpha_{\mathbf{a}} X^{\mathbf{a}}$, où $\alpha_{\mathbf{a}} \in k$ et, par convention, les $\alpha_{\mathbf{a}}$ sont nuls sauf un nombre fini d'entre eux. La multiplication est l'application k-bilinéaire définie par $X^{\mathbf{a}} \cdot X^{\mathbf{b}} = X^{\mathbf{a}+\mathbf{b}}$ i.e.

$$X_1^{a_1} \cdots X_r^{a_r} \cdot X_1^{b_1} \cdots X_r^{b_r} = X_1^{a_1+b_1} \cdots X_r^{a_r+b_r}$$

c.-à-d., pour $P = \sum_{\mathbf{a}\in\mathbb{N}^r} \alpha_{\mathbf{a}} X^{\mathbf{a}}$ et $Q = \sum_{\mathbf{b}\in\mathbb{N}^r} \beta_{\mathbf{b}} X^{\mathbf{b}}$ arbitraires, on a :

$$P \cdot Q = \sum_{\mathbf{a},\mathbf{b}\in\mathbb{N}^r} \alpha_{\mathbf{a}}\beta_{\mathbf{b}} X^{\mathbf{a}+\mathbf{b}} = \sum_{\mathbf{c}\in\mathbb{N}^r} \left(\sum_{\substack{\mathbf{a},\mathbf{b}\in\mathbb{N}^r \\ \mathbf{a}+\mathbf{b}=\mathbf{c}}} \alpha_{\mathbf{a}}\beta_{\mathbf{b}} \right) X^{\mathbf{c}}.$$

Pour tout $\mathbf{a} \in \mathbb{N}^r$, on pose $|\mathbf{a}| = a_1 + \cdots + a_r$ et l'on dit que le monôme $X^{\mathbf{a}}$ est de degré total $|\mathbf{a}|$. Si $P = \sum_{\mathbf{a}\in\mathbb{N}^r} \alpha_{\mathbf{a}} X^{\mathbf{a}}$ est non nul, on appelle *degré* de P et l'on note $\deg(P)$ le plus grand des entiers $|\mathbf{a}|$ pour $\mathbf{a}$ tel que $\alpha_{\mathbf{a}} \neq 0$ (il n'y a qu'un nombre fini de tels $\mathbf{a}$).

Par exemple, le polynôme en 3 variables $P = XYZ + 3Y^2Z^2 + 27X^3Y + Y^4 + 11Y^2Z^3 \in \mathbb{Q}[X,Y,Z]$ est de degré 5.

La définition précédente reste valable en remplaçant k par n'importe quel anneau commutatif A. On obtient ainsi l'anneau $A[X_1,\dots,X_r]$ des polynômes en r variables à coefficients dans A.

Revenons à notre corps k et, pour tout $i = 1,\dots,r$, notons R_i l'anneau des polynômes sur k en les $(r-1)$ variables $X_1,\dots,\widehat{X_i},\dots,X_r$, où le $\widehat{\ }$ sur le X_i signifie que cette variable a été omise. On a alors :

$$(*) \qquad k[X_1,\dots,X_n] = k[X_1,\dots,\widehat{X_i},\dots,X_n][X_i] = R_i[X_i],$$

i.e. tout élément P de $k[X_1,\dots,X_n]$ s'écrit de façon unique comme une somme **finie** $P = \sum_{s\in\mathbb{N}} A_s X_i^s$, où les A_s sont dans R_i et sont nuls sauf un nombre fini d'entre eux. Si $P \neq 0$ et si d est le plus grand entier tel que $A_s \neq 0$, on dit que P est *de degré* d en X_i et l'on pose $\deg_{X_i}(P) = d$. Ceci est bien sûr inférieur ou égal au degré total $\deg(P)$ de P.

Ainsi, dans l'exemple précédent, on a :

$$\begin{aligned}
P &= (27X^3Y + Y^4) + (XY)\,Z + 3Y^2\,Z^2 + 11Y^2\,Z^3 && \in k[X,Y][Z] \quad \text{et } \deg_Z(P) = 3,\\
&= (XZ + 27X^3)\,Y + (3Z^2 + 11Z^3)\,Y^2 + Y^4 && \in k[X,Z][Y] \quad \text{et } \deg_Y(P) = 4,\\
&= (3Y^2Z^2 + 11Y^2Z^3 + Y^4) + (YZ)\,X + 27Y\,X^3 && \in k[Y,Z][X] \quad \text{et } \deg_X(P) = 3.
\end{aligned}$$

Définition 23.3 **(Dérivée d'un polynôme)**. — Soit A un anneau commutatif. On introduit une application $D : A[X] \to A[X]$, appelée la *dérivation*, en posant, pour tout $P = a_0 + a_1X + a_2X^2 + \cdots + a_dX^d$,

$$D(P) = P' = a_1 + 2a_2X + \cdots + da_dX^{d-1}.$$

Ce polynôme est appelé le *polynôme dérivé* de P. On le notera aussi $\partial_X P$.

Proposition 23.4. — *Pour tout $P, Q \in A[X]$ et $\lambda, \mu \in A$, on a :*

(i) *$D(\lambda P + \mu Q) = \lambda D(P) + \mu D(Q)$, i.e. la dérivation est A-linéaire ;*

(ii) *$(PQ)' = P'Q + PQ'$.*

(iii) *Par conséquent, pour tout $n \in \mathbb{N}^*$ on a $D(P^n) = nP^{n-1}P'$.*

Démonstration. — (i) est immédiat et laissé au lecteur. Pour prouver (ii) on observe que, pour Q fixé, les deux applications $P \mapsto D(PQ)$ et $P \mapsto D(P)Q + PD(Q)$ sont A-linéaires, donc pour montrer qu'elles coïncident il suffit de le faire lorsque P est un monôme X^p, c.-à-d. il suffit de montrer que $D(X^pQ) = D(X^p)Q + X^pD(Q)$ pour tout $Q \in A[X]$.

Mais à nouveau, X^p étant fixé, les deux applications $Q \mapsto D(X^pQ)$ et $Q \mapsto D(X^p)Q + X^pD(Q)$ sont A-linéaires, donc pour montrer qu'elles coïncident il suffit de le faire lorsque

Q est un monôme X^q. Bref, il suffit de vérifier que

$$D(X^pX^q) = D(X^p)X^q + X^pD(X^q).$$

Mais ceci est facile, car $X^pX^q = X^{p+q}$ donc le terme de gauche vaut $(p+q)X^{p+q-1}$, tandis que celui de droite vaut $pX^{p-1}X^q + qX^pX^{q-1} = (p+q)X^{p+q-1}$. Ceci prouve (ii). Alors (iii) s'en déduit facilement par récurrence sur n. $\square$

Définition 23.5 **(Dérivées partielles d'un polynôme à plusieurs variables)**
Revenons à notre corps k.[11] Pour tout $P \in k[X_1, \dots, X_r]$, on note $\partial_{X_i}P$, ou simplement $\partial_i P$, le polynôme dérivé de P considéré comme élément de $k[X_1, \dots, \widehat{X_i}, \dots, X_n][X_i]$, i.e. on « dérive P *par rapport à la variable* X_i » en considérant les autres variables comme des « constantes ».

Ainsi, en reprenant l'exemple $P = XYZ + 3Y^2Z^2 + 27X^3Y + Y^4 + 11Y^2Z^3$, on a :

$$\begin{aligned}
\partial_Z P &= XY + 6Y^2\,Z + 33Y^2\,Z^2,\\
\partial_Y P &= (XZ + 27X^3) + 2(3Z^2 + 11Z^3)\,Y + 4Y^3,\\
\partial_X P &= YZ + 81Y\,X^2.
\end{aligned}$$

Proposition 23.6 **(Formule d'Euler)**. — *Soit $P \in k[X_1, \dots, X_r]$ un polynôme non nul homogène de degré d. On a l'égalité :*

$$(\star) \qquad d \cdot P = X_1\partial_1 P + \cdots + X_r\partial_r P = \sum_{i=1}^{r} X_i\partial_i P.$$

Démonstration. — Comme chaque application $P \mapsto X_i\partial_i P$ est k-linéaire, le terme de droite est une fonction linéaire de P, ainsi bien sûr que le terme de gauche. Donc il suffit de démontrer la formule lorsque P est un monôme $X_1^{a_1} \cdots X_r^{a_r}$ de degré d, i.e. $a_1 + \cdots + a_r = d$. Dans ce cas, on voit que pour tout $i = 1, \dots, r$, on a

$$X_i\partial_i(X_1^{a_1} \cdots X_r^{a_r}) = a_i X_1^{a_1} \cdots X_r^{a_r}$$

et donc le terme de droite est égal à $(\sum_{i=1}^r a_i)X_1^{a_1} \cdots X_r^{a_r} = dX_1^{a_1} \cdots X_r^{a_r}$. Ceci prouve la proposition. $\square$

Définitions 23.7 **(Points lisses et hyperplans tangents)**
Soit $P \in k[X_1, \dots, X_n]$ non constant et soit $a = (a_1, \dots, a_n) \in k^n$.

(i) La **différentielle** de P en a, notée d_aP, est la forme linéaire sur k^n qui à tout $(x_1, \dots, x_n)$ associe le scalaire $(\partial_1 P)(a)\,x_1 + \cdots + (\partial_n P)(a)\,x_n$.[12]

(ii) Soit $a \in \mathscr{V}(P)$. On dit que a est un point**lisse** de $\mathscr{V}(P)$ si $d_aP \neq 0$, c.-à-d. si les dérivées partielles $\partial_i P$, pour $i = 1, \dots, n$, ne s'annulent pas toutes au point a. Dans le cas contraire, on dit que a est un point **singulier** de $\mathscr{V}(P)$.

(iii) Si a est un point *lisse* de $\mathscr{V}(P)$, **l'hyperplan tangent** à $\mathscr{V}(P)$ au point a, noté $T_a\mathscr{V}(P)$ est l'hyperplan affine de direction $\mathrm{Ker}(d_aP)$ passant par a, i.e. :

$$\begin{aligned}
T_a\mathscr{V}(P) &= \big\{x = a + u \mid u \in \mathrm{Ker}(d_aP)\big\} = \big\{x = (x_1, \dots, x_n) \mid u = x - a \in \mathrm{Ker}(d_aP)\big\}\\
&= \big\{x = (x_1, \dots, x_n) \mid \sum_{i=1}^{n} \partial_i P(a)(x_i - a_i) = 0\big\}.
\end{aligned}$$

[11] En fait, ce qui suit est valable pour n'importe quel anneau commutatif k.

[12] Dans la suite, on notera simplement $\partial_i P(a)$ au lieu de $(\partial_i P)(a)$.

La différentielle d_aP, la lissité d'un point et l'hyperplan tangent en un point lisse, « ne dépendent pas des coordonnées affines » sur k^n, i.e. on a la proposition suivante :

Proposition 23.8. — (i) *La forme linéaire $d_aP : k^n \to k$ ne dépend pas du choix des coordonnées. Plus précisément, pour tout système $(Y_1, \dots, Y_n)$ de coordonnées affines centrées en a, d_aP est la* partie linéaire *du polynôme $Q(Y_1, \dots, Y_n)$ défini par $Q(Y_1, \dots, Y_n) = P(Y_1 + a_1, \dots, Y_n + a_n)$.*

(ii) *Par conséquent, la notion de point lisse et la définition de l'hyperplan tangent ne dépendent pas du choix des coordonnées.*

Démonstration. — Traitons d'abord le cas d'une translation. Soit $F \in R[X]$, où R est un anneau commutatif, et soit $r \in R$. Faisons le changement de variable $Y = X - r$, i.e. $X = Y + r$. Alors $F(X) = F(a+Y)$ s'écrit comme un polynôme en Y, qu'on notera $Q(Y)$ et qui est déterminé par l'égalité $Q(Y) = F(a+Y)$. Montrons que :

$$(*) \qquad (\partial_Y Q)(Y) = (\partial_X P)(Y + a).$$

En écrivant $F = \sum_{i=0}^{d} \alpha_i X^i$, on se ramène à vérifier cette égalité lorsque F est un monôme X^p, auquel cas $Q(Y) = (Y + a)^p$. Alors, d'après la formule 23.3 (iii), on a $(\partial_Y Q)(Y) = p(Y + a)^{p-1} = (\partial_X F)(Y + a)$, ce qui prouve $(*)$.

Revenons à notre polynôme $P \in k[X_1, \dots, X_n]$ et faisons le changement de variables $Y_i = X_i - a_i$, de sorte que a est le point défini par $Y_i(a) = 0$ pour $i = 1, \dots, n$. On dit alors que le système de coordonnées affines $(Y_1, \dots, Y_n)$ est *centré* en a. Alors $P(X_1, \dots, X_n) = P(a_1 + Y_1, \dots, a_n + Y_n)$ s'écrit comme un polynôme en les Y_i, qu'on notera $Q(Y_1, \dots, Y_n)$ et qui est déterminé par l'égalité

$$Q(Y_1, \dots, Y_n) = P(a_1 + Y_1, \dots, a_n + Y_n).$$

Fixons un indice i et considérons le 1er (resp. 2ème) membre comme un polynôme en Y_i (resp. X_i) à coefficients dans l'anneau $R = k[Y_1, \dots, \widehat{Y_i}, \dots, Y_n]$. Alors, d'après $(*)$ on a

$$(\partial_{Y_i} Q)(Y_1, \dots, Y_n) = (\partial_{X_i} P)(a_1 + Y_1, \dots, a_n + Y_n)$$

et donc $(\partial_{Y_i} Q)(0) = (\partial_{X_i} P)(a)$ pour tout i. On voit donc que a est lisse dans les coordonnées X_i ssi il l'est dans les coordonnées Y_i, et dans ce cas en utilisant les coordonnées Y_i l'hyperplan tangent est défini par :

$$T_{y=0}\mathscr{V}(P) = \big\{y = (y_1, \dots, y_n) \mid \sum_{i=1}^{n} (\partial_{Y_i} Q)(0)\, y_i = 0\big\} = \big\{x = a + y \mid \sum_{i=1}^{n} (\partial_{X_i} P)(a)(x_i - a_i) = 0\big\}$$

et coïncide bien avec l'hyperplan tangent défini en utilisant les coordonnées X_i.

De plus, Q se décompose de façon unique comme la somme de ses « composantes homogènes » :

$$(\star) \qquad Q = Q_0 + Q_1 + Q_2 + \cdots + Q_d,$$

où $Q_0 = Q(0)$ (qui ici vaut 0), $d = \deg(Q)$ et pour $s = 1, \dots, d$, Q_s est le polynôme homogène de degré s obtenu en regroupant tous les monômes de degré s apparaissant dans Q.

Fixons une variable Y_i. Alors, pour tout $s = 1, \dots, d$, $\partial_{Y_i} Q_s$ est un polynôme homogène de degré $s - 1$, donc s'annule en 0 si $s \geq 2$ et est une constante c_i si $s = 1$; de plus compte tenu des annulations $(\partial_{Y_i} Q_s)(0) = 0$ pour $s \neq 1$, on a $c_i = (\partial_{Y_i} Q)(0)$. Alors, d'après la formule d'Euler, on a

$$Q_1 = \sum_{i=1}^{n} c_i Y_i = \sum_{i=1}^{n} (\partial_{Y_i} Q)(0) Y_i = d_{y=0} Q.$$

Montrons enfin que la décomposition $(\star)$ ne dépend que du point choisi comme « centre des coordonnées » (i.e. comme origine de l'espace affine $\mathscr{E} = k^n$), et non du choix des coordonnées elles-mêmes (i.e. du choix d'une base de l'espace vectoriel $E = k^n$).

Notons $\mathscr{B}$ la base canonique de k^n et soient $\mathscr{C}$ une autre base, $B = \mathrm{Mat}_{\mathscr{B}}(\mathscr{C})$ la matrice de passage, et $(Y'_1, \dots, Y'_n)$ les coordonnées dans la base $\mathscr{C}$. Alors on a la formule de changement de coordonnées

$$\begin{pmatrix} Y_1 \\ \vdots \\ Y_n \end{pmatrix} = B \begin{pmatrix} Y'_1 \\ \vdots \\ Y'_n \end{pmatrix}$$

c.-à-d. $Y_i = \sum_{j=1}^{r} b_{ij} Y'_j$ pour $i = 1, \dots, n$. Par conséquent, en notant $\widetilde{Q}_s$ le polynôme en les Y'_i défini par l'égalité $Q_s(Y_1, \dots, Y_n) = \widetilde{Q}_s(Y'_1, \dots, Y'_n)$ et en définissant de même $\widetilde{Q}$, on voit que chaque $\widetilde{Q}_s$ est un polynôme en les Y'_i homogène de degré s, et donc

$$\widetilde{Q} = \widetilde{Q}_0 + \widetilde{Q}_1 + \widetilde{Q}_2 + \cdots + \widetilde{Q}_d$$

est la décomposition de $\widetilde{Q}$ en composantes homogènes. Alors le même argument que précédemment montre que la forme linéaire $d_{y'=0}\widetilde{Q}(Y'_1, \dots, Y'_n)$ est égale à $\widetilde{Q}_1(Y'_1, \dots, Y'_n) = Q_1(Y_1, \dots, Y_n)$, donc à $d_{y=0}Q(Y_1, \dots, Y_n)$. Ceci achève la démonstration de la proposition. □

Exemple 23.9. — On suppose $\mathrm{car}(k) \neq 2$. Dans k^2, considérons l'hyperbole $\mathscr{C} = \mathscr{V}(P)$, où $P = X^2 - Y^2 - 1$. Soit p le point de $\mathscr{C}$ de coordonnées $(1, 0)$. On a $\partial_X P(p) = 2$ et $\partial_Y P(p) = 0$ donc p est un point lisse de $\mathscr{C}$ et la tangente à $\mathscr{C}$ en p a pour équation $2(x - 1) = 0$, c.-à-d. $2x = 2$ (i.e. $x = 1$).

Si l'on fait le changement de coordonnées $Z = X + Y$ et $U = X - Y$ (i.e. $X = (Z + U)/2$ et $Y = (Z - U)/2$), alors $P(X, Y) = ZU - 1 = Q(Z, U)$ et p a pour coordonnées $Z = 1 = U$. On a $\partial_Z Q(p) = 1 = \partial_U Q(p)$, et la tangente à $\mathscr{C}$ en p a pour équation $(z - 1) + (u - 1) = 0$, c.-à-d. $z + u = 2$. C'est bien la droite d'équation $2x = 2$ obtenue plus haut !

***Définition 23.10* (Hyperplans tangents à une hypersurface projective)**

Soit $P \in k[X_0, \dots, X_n]$ homogène de degré $d \geq 1$, soit $\mathscr{V}(P)$ sa variété des zéros dans $\mathbb{P}^n(k)$ et soit $a = [a_0, a_1, \dots, a_n] \in \mathscr{V}(P)$.

(i) On dit que a est un point **lisse** de $\mathscr{V}(P)$ si les dérivées partielles $\partial_i P$, pour $i = 0, \dots, n$, ne s'annulent pas toutes au point a. Dans le cas contraire, on dit que a est un point **singulier** de $\mathscr{V}(P)$.

(ii) Si a est un point lisse de $\mathscr{V}(P)$, **l'hyperplan tangent** à $\mathscr{V}(P)$ au point a, noté $T_a\mathscr{V}(P)$ est l'hyperplan de $\mathbb{P}^n(k)$ d'équation $\sum_{i=0}^{n} \partial_i P(a)\, x_i = 0$, i.e. :

$$T_a\mathscr{V}(P) = \big\{[x] = [x_0, x_1, \dots, x_n] \in \mathbb{P}^n(k) \mid \sum_{i=0}^{n} x_i\, \partial_i P(a) = 0\big\}.$$

Remarquons qu'il passe bien par le point a, car on a $\sum_{i=0}^{n} a_i\, \partial_i P(a) = d \cdot P(a) = 0$, d'après la formule d'Euler.

Le lien avec la définition dans le cas affine est donné par la proposition qui suit. Soit $a = [a_0, \dots, a_n] \in \mathscr{V}(P)$. Fixons un indice i_0 tel que $a_{i_0} \neq 0$. Pour alléger la notation, prenons $i_0 = 0$ i.e. plaçons-nous dans le cas où $a = [1, a_1, \dots, a_n]$ appartient à l'espace affine $\mathscr{E}$ complémentaire de l'hyperplan projectif $\mathbf{H}_\infty$ donné par l'équation $x_0 = 0$. Comme d'habitude, identifions $\mathscr{E}$ à l'hyperplan affine $\mathscr{H} = \{(1, x_1, \dots, x_n)\}$ de k^{n+1}, et identifions $\mathscr{H}$ à k^n via $(1, x_1, \dots, x_n) \leftrightarrow (x_1, \dots, x_n)$. Notons $f \in k[X_1, \dots, X_n]$ le polynôme défini par :

$$f(X_1, \dots, X_n) = P(1, X_1 \dots, X_n)$$

et notons $\widehat{a} = (a_1, \dots, a_n)$ le point de k^n correspondant à $a \in \mathscr{E}$. Alors, pour tout $i = 1, \dots, n$, on a $\partial_i f(X_1, \dots, X_n) = \partial_i P(1, X_1 \dots, X_n)$ et donc, en particulier, $\partial_i f(\widehat{a}) = \partial_i P(a)$.

Proposition 23.11. — *Avec les notations précédentes, on a :*

(i) *a est un point lisse de $\mathscr{V}(P)$ ssi $\widehat{a}$ est un point lisse de $\mathscr{V}(f)$. Dans ce cas, on a :*

(ii) $\boxed{T_a\mathscr{V}(P) \cap \mathscr{E} = T_{\widehat{a}}\mathscr{V}(f).}$

(iii) *Réciproquement, $T_a\mathscr{V}(P)$ est le « complété projectif » de $T_{\widehat{a}}\mathscr{V}(f)$, i.e. si ce dernier est défini par l'équation affine $c_0 + \sum_{i=1}^n c_i X_i = 0$ alors $T_a\mathscr{V}(P)$ est défini par l'équation homogène $c_0 X_0 + \sum_{i=1}^n c_i X_i = 0$.*

Démonstration. — (i) Si $\widehat{a}$ est un point lisse de $\mathscr{V}(f)$, il existe un indice $i \geq 1$ tel que $\partial_i f(\widehat{a}) = \partial_i P(a)$ soit non nul, donc a est un point lisse de $\mathscr{V}(P)$. Réciproquement, supposons que a soit un point lisse de $\mathscr{V}(P)$. Alors il existe au moins un indice $i \in \{0, \ldots, n\}$ tel que $\partial_i P(a)$ soit non nul. Si $i = 0$ était le seul indice ayant cette propriété on aurait, d'après la formule d'Euler,

$$0 = P(a) = \sum_{i=0}^{n} a_i \, \partial_i P(a) = 1 \cdot \partial_0 P(a) \neq 0,$$

ce qui est impossible. Donc il existe au moins un indice $i \geq 1$ tel que $\partial_i P(a) = \partial_i f(\widehat{a})$ soit non nul, donc $\widehat{a}$ est un point lisse de $\mathscr{V}(f)$. Ceci prouve (i).

Dans ce cas, $T_a\mathscr{V}(P) \cap \mathscr{E}$ s'identifie à l'ensemble des points $(x_1, \ldots, x_n)$ de k^n tels que

$$(\dagger) \qquad 0 = \partial_0 P(a) + \sum_{i=1}^{n} x_i \, \partial_i P(a) = \partial_0 P(a) + \sum_{i=1}^{n} x_i \, \partial_i f(\widehat{a}).$$

Or, d'après la formule d'Euler, on a $\partial_0 P(a) = -\sum_{i=1}^n a_i \, \partial_i P(a) = -\sum_{i=1}^n a_i \, \partial_i f(\widehat{a})$ et donc l'égalité (†) se récrit en :

$$0 = \sum_{i=1}^{n} (x_i - a_i) \, \partial_i f(\widehat{a})$$

ce qui est la définition de l'hyperplan tangent $T_{\widehat{a}}\mathscr{V}(f)$.

Réciproquement, si $T_{\widehat{a}}\mathscr{V}(f)$ est défini par l'équation affine $c_0 + \sum_{i=1}^n c_i X_i = 0$, celle-ci est unique à homothétie près i.e. il existe $\lambda \in k^*$ telle que $c_i = \lambda \partial_i P(a)$ pour $i = 0, \ldots, n$ et donc $T_a\mathscr{V}(P)$ est défini par l'équation homogène $c_0 X_0 + \sum_{i=1}^n c_i X_i = 0$. (13) □

Il résulte de la proposition précédente que la lissité d'un point de $\mathscr{V}(P)$ et l'hyperplan projectif tangent à $\mathscr{V}(P)$ en un point lisse, « ne dépendent pas des coordonnées homogènes » sur $\mathbb{P}(V)$, i.e. on a la proposition suivante. (14)

Corollaire 23.12. — *Soit $\mathbb{P}(V)$ un espace projectif de dimension n. Soient $[x_0, \ldots, x_n]$ un système de coordonnées homogènes, $P \in k[X_0, \ldots, X_n]$ un polynôme homogène de degré $d \geq 1$ et $\mathscr{V}$ l'hypersurface définie par P, i.e. :*

$$\mathscr{V} = \big\{[x_0, \ldots, x_n] \in \mathbb{P}(V) \mid P(x_0, \ldots, x_n) = 0\big\}.$$

Soit $[y_0, \ldots, y_n]$ un second système de coordonnées homogènes.

(i) *Il existe un polynôme Q homogène de degré d, unique à homothétie près, tel que $Q(y_0, \ldots, y_n) = P(x_0, \ldots, x_n)$ et l'on a*

$$\mathscr{V} = \big\{[y_0, \ldots, y_n] \in \mathbb{P}(V) \mid Q(y_0, \ldots, y_n) = 0\big\}.$$

(13) Ceci est un cas particulier de la correspondance bijective entre sous-espaces affines de $\mathscr{E} = \mathbb{P}^n(k) - \mathbf{H}_\infty$ et sous-espaces projectifs de $\mathbb{P}^n(k)$ non contenus dans $\mathbf{H}_\infty$, cf. Prop. 11.15.

(14) On pourrait démontrer directement l'indépendance des coordonnées dans le cas projectif, mais il est plus rapide d'utiliser le travail déjà fait dans le cas affine.

(ii) *Un point $p \in \mathscr{V}$ est lisse relativement aux coordonnées x_i ssi il l'est relativement aux coordonnées y_i et dans ce cas, notant respectivement a_i et b_i ses coordonnées, on a :*

$$\begin{aligned} T_p\mathscr{V} &= \big\{[x_0, \dots, x_n] \in \mathbb{P}(V) \mid \sum_{i=0}^{n} x_i\, \partial_{X_i} P(a_0, \dots, a_n) = 0\big\} \\ &= \big\{[y_0, \dots, y_n] \in \mathbb{P}(V) \mid \sum_{i=0}^{n} y_i\, \partial_{Y_i} Q(b_0, \dots, b_n) = 0\big\}. \end{aligned}$$

Démonstration. — Soient $\mathscr{B}$ et $\mathscr{C}$ les bases de k^{n+1} (uniques à homothétie près) correspondant aux coordonnées homogènes x_i et y_i. Notons a_{ij}, resp. a'_{ij}, les coefficients de la matrice $A = \mathrm{Mat}_{\mathscr{B}}(\mathscr{C})$, resp. $A^{-1} = \mathrm{Mat}_{\mathscr{C}}(\mathscr{B})$. Alors on a $x_i = \sum_{i=0}^{n} a_{ij}\, y_j$ pour tout $i = 0, \dots, n$. Faisons le changement de variables

$$\forall i = 0, \dots, n, \qquad X_i = \sum_{i=0}^{n} a_{ij}\, Y_j$$

(qui équivaut à $Y_i = \sum_{i=0}^{n} a'_{ij}\, X_j$ pour tout i). Alors il existe un unique polynôme $Q \in k[Y_0, \dots, Y_n]$ tel que $P(X_0, \dots, X_n) = Q(Y_0, \dots, Y_n)$, et Q est homogène de degré d.

Si l'on remplace les bases $\mathscr{B}$ et $\mathscr{C}$ par des bases homothétiques $\mu\mathscr{B}$ et $\nu\mathscr{C}$ alors A est changée en λA, où $\lambda = \mu^{-1}\nu$, et Q est changé en $\lambda^d Q$. L'assertion (i) en découle.

Le point (ii) découle de la proposition 23.11 combinée à l'indépendance des coordonnées dans le cas affine établie dans la proposition 23.8. □

On va maintenant décrire les points singuliers d'un cône quadratique $C(Q) \subset V$ et de la quadrique projective $\mathscr{V}(Q) \subset \mathbb{P}(V)$. Pour la suite de cette section, on suppose $\boxed{\mathrm{car}(k) \neq 2.}$

Soit V un k-ev de dimension n, Q une forme quadratique sur V de rang $r \geq 1$ et $N(Q)$ son noyau. Soit $\mathscr{B} = (e_1, \dots, e_n)$ une base de V orthogonale pour Q et soient $(x_1, \dots, x_n)$ les coordonnées correspondantes. Quitte à renuméroter les e_i, on peut supposer que $c_i = Q(e_i)$ est non nul pour $i = 1, \dots, r$ et nul pour $i > r$. Alors Q est donnée dans la base $\mathscr{B}$ par $Q(X) = c_1 X_1^2 + \cdots + c_r X_r^2$, d'où :

$$\partial_{X_i} Q = \begin{cases} 2c_i X_i & \text{si } i = 1, \dots, r, \\ 0 & \text{si } i > r. \end{cases}$$

Par conséquent, pour tous $v = \sum_{i=1}^{n} p_i e_i$ et $x = \sum_{i=1}^{n} x_i e_i$ dans V, on a

$$(\star) \qquad (d_v Q)(x) = \sum_{i=1}^{n} (\partial_{X_i} Q)(v) x_i = 2 \sum_{i=1}^{r} c_i p_i x_i = 2\phi(v, x)$$

ce qui montre que $d_v Q$ est la forme linéaire $2\phi(v, -)$. En particulier, le point $0 = (0, \dots, 0)$ est toujours un point singulier du cône isotrope $C(Q)$, mais *c'est le seul si Q est non dégénérée.* On a donc démontré la :

Proposition 23.13. — *Soient Q une forme quadratique sur V, ϕ sa forme polaire, $N(Q)$ son noyau, $C(Q)$ son cône isotrope et $\mathscr{V}(Q) \subset \mathbb{P}(V)$ la quadrique associée.*

(i) *Pour tout $v \in V$, la différentielle $d_v Q$ est la forme linéaire $2\phi(v, -)$. Par conséquent :*

(ii) *Si $v \neq 0$, alors v (resp. $[v]$) est un point singulier de $C(Q)$ (resp. de $\mathscr{V}(Q)$) ssi $v \in N(Q)$.*

(iii) *Si $v \in C(Q) - N(Q)$ alors $T_v C(Q) = (kv)^\perp$ et $T_{[v]}\mathscr{V}(Q) = \mathbb{P}\big((kv)^\perp\big)$.*

De plus, comme expliqué en 22.1, si le corps de base est $\mathbb{R}$ on peut être amené à considérer des points de $C(Q)$ ou $\mathscr{V}(Q)$ « à valeurs dans $\mathbb{C}$ ». Introduisons donc la notion d'extension du corps de base :

***Définition 23.14* (Extension des scalaires).** — Soient $k \subset K$ deux corps et V un k-espace vectoriel de dimension n. Si l'on choisit une base $\mathscr{B} = (e_1, \dots, e_n)$ de V, alors V s'identifie à k^n et l'on peut alors le plonger dans le K-espace vectoriel K^n.

Ce plongement ne dépend pas de la base $\mathscr{B}$ choisie. En effet, notons $e_1 \otimes 1, \dots, e_n \otimes 1$ les vecteurs de la base canonique de K^n, qu'on notera $\mathscr{B}_K$. Pour tout $v = \sum_{i=1}^n a_i e_i$ dans V, on pose :

$$v \otimes 1 \overset{\text{déf.}}{=\!=} \sum_{i=1}^n a_i e_i \otimes 1.$$

Si $\mathscr{C} = (f_1, \dots, f_n)$ est une autre base de V et si $P = (p_{ij})_{1 \le i,j \le n}$ est la matrice de passage alors la matrice exprimant $\mathscr{C}_K = (f_1 \otimes 1, \dots, f_n \otimes 1)$ dans la base $\mathscr{B}_K$ n'est autre que P, qui appartient à $\mathrm{GL}_n(k) \subset \mathrm{GL}_n(K)$ donc est inversible. Par conséquent, $\mathscr{C}_K$ est une autre base de K^n.

Ceci nous conduit à noter V_K le K-espace vectoriel ainsi défini. On dira que c'est le K-espace vectoriel déduit de V par extension des scalaires de k à K.(15)

Ceci nous sera utile dans la situation suivante. Reprenons les notations précédentes : Q une forme quadratique de rang $r \geq 1$ sur V, $\mathscr{B} = (e_1, \dots, e_n)$ une base de V telle que $Q(x) = \sum_{i=1}^r c_i x_i$ pour tout $x = \sum_{i=1}^n x_i e_i$, avec les $c_i \neq 0$, de sorte que $N(Q)$ est le sev donné par les équations $x_j = 0$ pour $j > r$. Pour tout corps K contenant k, Q se prolonge en une forme quadratique Q_K sur V_K, définie par

$$(*) \qquad Q_K(x_1 e_1 + \cdots + x_n e_n) = c_1 x_1^2 + \cdots + c_r x_r^2, \qquad \forall (x_1, \dots, x_n) \in K^n$$

et l'on pose

$$C_K(Q) = \{x_1 e_1 + \cdots + x_n e_n \in V_K \mid Q_K(x_1, \dots, x_n) = 0\}.$$
$$\mathscr{V}_K(Q) = \{[x_1 e_1 + \cdots + x_n e_n] \in \mathbb{P}(V_K) \mid Q_K(x_1, \dots, x_n) = 0\}.$$

D'après ce qui précède, $C_K(Q)$ et $\mathscr{V}_K(Q)$ ne dépendent que de V, Q et K, et pas du choix de la base $\mathscr{B}$.

De plus, $C_K(Q) \subset V_K$ et $\mathscr{V}_K(Q) \subset \mathbb{P}(V_K)$ sont, respectivement, le cône isotrope et la quadrique projective associés à la forme quadratique Q_K sur V_K. La formule $(*)$, combinée à la proposition précédente appliquée sur le corps K, montre alors que pour tout $v \neq 0$ dans V_K, v (resp. $[v]$) est un point singulier de $C_K(Q)$ (resp. $\mathscr{V}_K(Q)$) ssi $x_j(v) = 0$ pour $j > r$, i.e. ssi v appartient au sous-espace $N(Q)_K = N(Q_K)$ de V_K. En particulier, si Q est non dégénérée (i.e. si $r = n$), il en est de même de Q_K. On obtient donc la :

***Proposition 23.15*.** — *Soit K un corps contenant k.*

(i) *Si Q est non dégénérée, il en est de même de Q_K donc $C_K(Q) - \{0\}$ et $\mathscr{V}_K(Q)$ sont formés de points lisses.*

(ii) *Au contraire, si Q est dégénérée alors $C_k(Q)$ contient au moins un point singulier $v \neq 0$ et donc la quadrique projective $\mathscr{V}(Q) = \{[w] \in \mathbb{P}(V) \mid Q(w) = 0\}$ contient au moins le point singulier $[v]$.*

***Remarques 23.16*.** — Prenons par exemple $k = \mathbb{R}$ et $V = \mathbb{R}^3$.

a) Il se peut que la conique projective $\mathscr{V}(Q)$ soit vide, c'est par exemple le cas si $Q(X, Y, Z) = X^2 + Y^2 + Z^2$. D'après la proposition précédente, ceci entraîne que Q est non dégénérée et donc que tous les points de $\mathscr{V}_{\mathbb{C}}(Q)$ sont lisses.

(15) On peut définir V_K de façon canonique comme le produit tensoriel $V \otimes_k K$, sans avoir à choisir une base de V, cf. le cours 4M002.

b) Si Q est dégénérée, on a vu que $\mathscr{V}_{\mathbb{R}}(Q)$ contient au moins un point singulier ; il est possible que ce soit le seul point réel : si $Q(X,Y,Z) = X^2 + Y^2$ alors d'une part $N(Q)$ est la droite engendrée par $(0,0,1)$, et d'autre part le seul point réel de $\mathscr{V}(Q)$ est le point $p = [0,0,1]$ qui est singulier. En passant à $\mathbb{C}$, on a $Q(X,Y,Z) = (X - iY)(X + iY)$ donc $\mathscr{V}_{\mathbb{C}}(Q)$ est la réunion des droites d'équations $x = iy$ et $x = -iy$, qui se coupent au point réel $p = [0,0,1]$.

On peut maintenant revenir sur l'intersection d'une droite et d'une quadrique (lemme 23.17), en tenant compte des conditions de tangence :

Proposition 23.17. — *Soient Q une forme quadratique non nulle sur V et E un sev de V de dimension 2. Dans $\mathbb{P}(V)$, considérons l'intersection de $\mathscr{V}(Q)$ et de la droite projective $\mathbf{D} = \mathbb{P}(E)$. On a l'une des trois alternatives suivantes :*

a) *$Q_E = 0$ et $\mathbf{D} \subset \mathscr{V}(Q)$.*

b) *Q_E est non dégénérée. Alors $\mathbf{D} \cap \mathscr{V}(Q)$ est formée de deux points distincts $p \neq q$ (éventuellement à coordonnées dans une extension quadratique de k) qui sont des points lisses de $\mathscr{V}(Q)$. De plus, $\mathbf{D}$ n'est pas tangente à $\mathscr{V}(Q)$ en ces points.*

c) *Q_E est de rang 1. Alors $\mathbf{D} \cap \mathscr{V}(Q)$ est formée d'un seul point p (à coordonnées dans k) et si p est un point lisse de $\mathscr{V}(Q)$ alors $\mathbf{D}$ est contenue dans l'hyperplan tangent $T_p\mathscr{V}(Q)$.*

Démonstration. — On a $Q_E = 0$ ssi $\mathscr{V}(Q_E) = \mathbf{D}$, et ceci équivaut à $\mathbf{D} \subset \mathscr{V}(Q)$. Ceci règle l'alternative (a).

Supposons $Q_E \neq 0$. Soit (e_0, e_1) une base orthogonale de E, avec $Q(e_0) \neq 0$. Multipliant Q par $Q(e_0)^{-1}$ (ce qui ne change pas $\mathscr{V}(Q)$), on se ramène au cas où $Q(e_0) = 1$ et l'on pose alors $Q(e_1) = -\delta$.

Supposons Q_E non dégénérée, i.e. $\delta \neq 0$. Alors $E \cap E^{\perp} = \{0\}$, d'après le lemme 22.16, et donc $V = E \oplus E^{\perp}$. Soit alors $(e_2, \dots, e_n)$ une base orthogonale de $E^{\perp}$, alors $\mathscr{B} = (e_0, \dots, e_n)$ est une base orthogonale de V. Notons $(x_0, \dots, x_n)$ les coordonnées correspondantes. Alors

$$Q(X_0, \dots, X_n) = X_0^2 - \delta X_1^2 + \sum_{i=2}^{n} c_i X_i^2 \quad \text{et donc } \partial_{X_i} Q = \begin{cases} 2X_0 & \text{si } i = 0, \\ -2\delta X_1 & \text{si } i = 1, \\ 2c_i X_i & \text{si } i \geq 2. \end{cases}$$

Notons α une racine carrée de δ (éventuellement dans une extension quadratique de k). On voit alors que $\mathbf{D} \cap \mathscr{V}(Q)$ est formée des deux points $p = [\alpha, 1, 0, \dots, 0]$ et $q = [-\alpha, 1, 0, \dots, 0]$. De plus, $d_pQ = 2\alpha X_0 - 2\delta X_1$ est une forme linéaire non nulle, donc p est un point lisse de $\mathscr{V}(Q)$, et l'hyperplan tangent $T_p\mathscr{V}(Q)$ a pour équation $\alpha x_0 = \delta x_1$ donc coupe la droite $\mathbf{D}$ en le point $[\delta, \alpha, 0, \dots, 0]$, donc $\mathbf{D} \not\subset T_p\mathscr{V}(Q)$, i.e. $\mathbf{D}$ n'est pas tangente à $\mathscr{V}(Q)$ en p. Et de même pour q. Ceci règle le cas de l'alternative (b).

Supposons enfin Q_E de rang 1, i.e. $\delta = 0$. Dans ce cas, $\mathbf{D} \cap \mathscr{V}(Q)$ est formée de l'unique point $p = [e_1]$. D'après la proposition 23.13, $p = [e_1]$ est un point singulier de $\mathscr{V}(Q)$ ssi $e_1 \in N(Q)$, et sinon on a $T_p\mathscr{V}(Q) = \mathbb{P}\big((ke_1)^{\perp}\big)$. Comme e_0 et e_1 sont orthogonaux à e_1, on a bien $E \subset (ke_1)^{\perp}$ d'où $\mathbf{D} \subset T_p\mathscr{V}(Q)$. Ceci achève la démonstration de la proposition. $\square$

24. Polarité et théorème de Brianchon

Dans cette section, on suppose $\boxed{\mathrm{car}(k) \neq 2.}$ Soient V un k-ev de dimension $n+1 \geq 3$ et Q une forme quadratique *non dégénérée* sur V, de forme polaire ϕ. Alors l'isomorphisme $\theta : V \xrightarrow{\sim} V^*$ permet de « transporter » ϕ en une fbs non dégénérée ϕ^* sur V^*, définie par :

$$\forall f, g \in V^*, \quad \phi^*(f,g) = \phi\big(\theta^{-1}(f), \theta^{-1}(g)\big),$$

c.-à-d. $\phi^*\big(\theta(x), \theta(y)\big) = \phi(x,y)$ pour tout $x, y \in V$. (ϕ^* est bien non dégénérée, car si $\theta(x) \in N(\phi^*)$ alors pour tout $y \in V$ on a $0 = \phi^*\big(\theta(x), \theta(y)\big) = \phi(x,y)$, d'où $x = 0$.) On pose $Q^*(f) = \phi^*(f,f)$ pour tout $f \in V^*$, i.e. $Q^*(\theta(v)) = Q(v)$ pour tout $v \in V$.

Remarque 24.1. — Via l'identification canonique $V = V^{**}$ (qui identifie tout $x \in V$ à la forme linéaire $\varepsilon_x : f \mapsto f(x)$ sur V^*), l'isomorphisme $\theta^* : V^* \to V$ défini par ϕ^* n'est autre que θ^{-1}. En effet, pour tout $x, y \in V$ on a, par définition :

$$\theta^*\big(\theta(x)\big)(\theta(y)) = \phi^*\big(\theta(x), \theta(y)\big) = \phi(x,y) = \varepsilon_x(\theta(y)),$$

d'où $\theta^*(\theta(x)) = x$ et donc $\theta^* = \theta^{-1}$. Par conséquent, la fbs ϕ^{**} sur V définie par ϕ^* n'est autre que ϕ car, comme $(\theta^*)^{-1} = \theta$, alors pour tout $x, y \in V$ on a : $\phi^{**}(x,y) = \phi^*\big(\theta(x), \theta(y)\big) = \phi(x,y)$. Donc (V, Q) et (V^*, Q^*) jouent des rôles symétriques.

Lemme 24.2. — *Soient $\mathscr{B}$ une base de V, $\mathscr{B}^*$ la base duale de V^*. Notons $A = \mathrm{Mat}_{\mathscr{B}}(Q)$.*

(i) *On a* $\mathrm{Mat}_{\mathscr{B}^*}(Q^*) = A^{-1}$.

(ii) *Par conséquent, pour tout $\lambda \in k^\times$, on a $(\lambda Q)^* = \lambda^{-1} Q^*$.*

Démonstration. — Soient $x, y \in V$, notons X, Y les vecteurs colonnes de leurs coordonnées dans la base $\mathscr{B}$. Posons $A^* = \mathrm{Mat}_{\mathscr{B}^*}(Q^*)$. Comme $\phi^*(\theta(x), \theta(y)) = \phi(x,y)$ et comme A est aussi la matrice de θ dans les bases $\mathscr{B}$ et $\mathscr{B}^*$, on a :

$${}^tXAY = \phi(x,y) = \phi^*(\theta(x), \theta(y)) = {}^t(AX)A^*(AY) = {}^tX({}^tAA^*A)Y.$$

Il en résulte ${}^tAA^*A = A = {}^tA$ (car A est symétrique), d'où $A^*A = \mathrm{Id}$ et donc $A^* = A^{-1}$. Ceci prouve (i). Et (ii) en découle, car λQ a pour matrice λA, donc $(\lambda Q)^*$ a pour matrice $\lambda^{-1}A^{-1}$. □

***Définitions 24.3* (Pôles et polaires, polarité).** — (1) À tout hyperplan $\mathbb{P}(H)$ de $\mathbb{P}(V)$ on associe son *pôle*, qui est le point $p = \mathbb{P}(H^\perp)$.

(2) À tout point $p = [v]$ de $\mathbb{P}(V)$ on associe son *hyperplan polaire*, qui est l'hyperplan $\mathbb{P}\big((kv)^\perp\big)$.

(3) Plus généralement, à tout sous-espace projectif $\mathbb{P}(W)$ de dimension d on peut associer le sous-espace projectif $\mathbb{P}(W^\perp)$, qui est de dimension $n - d - 1$.

(4) On obtient ainsi des bijections réciproques entre points et hyperplans de $\mathbb{P}(V)$ et, plus généralement, entre sous-espaces projectifs de dimension d et $n-1-d$. Ces bijections *renversent les inclusions* et *échangent les notions d'intersection et de sous-espace engendré.*

Démonstration. — Le point (4) découle du fait que cette notion de « polarité » est obtenue en composant l'isomorphisme $\theta : V \xrightarrow{\sim} V^*$ avec la dualité projective entre $\mathbb{P}(V^*)$ et $\mathbb{P}(V)$ (cf. Prop. 15.6). □

Un point-clé de la notion de polarité est fourni par la proposition suivante.

Proposition 24.4. — *Soit $\mathscr{V}(Q) \subset \mathbb{P}(V)$ une quadrique non dégénérée, θ l'isomorphisme $V \xrightarrow{\sim} V^*$ qu'elle induit et Q^* la forme quadratique sur V^* définie par $Q^*(\theta(v)) = Q(v)$, pour tout $v \in V$. Alors :*

(i) *L'homographie* $\overline{\theta} : \mathbb{P}(V) \to \mathbb{P}(V^*)$, $[v] \mapsto [\theta(v)]$ *induit une bijection de* $\mathscr{V}(Q)$ *sur la quadrique* $\mathscr{V}(Q^*) \subset \mathbb{P}(V^*)$.

(ii) *Pour tout point* p *de* $\mathscr{V}(Q)$, *le point* $\overline{\theta}(p)$ *de* $\mathscr{V}(Q^*)$ *correspond à l'hyperplan tangent en* p *à* $\mathscr{V}(Q)$.

Démonstration. — (i) découle de la définition de Q^*. Prouvons (ii). Soit $p = [v]$ un point de $\mathscr{V}(Q)$. D'une part, le point $\overline{\theta}(p) = [\theta(v)]$ de $\mathscr{V}(Q^*) \subset \mathbb{P}(V^*)$ correspond, via la dualité entre $\mathbb{P}(V^*)$ et $\mathbb{P}(V)$, à l'hyperplan :

$$\mathbb{P}\big(\theta(v)^0\big) = \{[w] \in \mathbb{P}(V) \mid 0 = \theta(v)(w) = \phi(v,w)\} = \mathbb{P}\big((kv)^\perp\big).$$

D'autre part, d'après la Prop. 23.13, on a $T_p\mathscr{V}(Q) = \mathbb{P}\big((kv)^\perp\big)$, d'où la proposition. □

En particulier, si $\mathbb{P}(V)$ est un plan projectif, alors pour tout point p de la conique $\mathscr{V}(Q)$, la droite tangente à $\mathscr{V}(Q)$ en p correspond au point $\overline{\theta}(p)$ de la conique $\mathscr{V}(Q^*)$. On obtient alors l'énoncé dual du théorème de Pascal :

Théorème 24.5. — *Dans le plan projectif, soient* $\mathbf{D}_1, \dots, \mathbf{D}_6$ *six droites distinctes, dont trois ne sont jamais concourantes. Notons* p_{12} *le point de concours de* $\mathbf{D}_1$ *et* $\mathbf{D}_2$, *et définissons de même* p_{23}, p_{34}, *etc.*

(i) **(Théorème de Brianchon)** [16] *Si ces droites sont tangentes à une même conique non dégénérée* $\mathscr{C}$, *alors les trois droites* $(p_{12}p_{45})$, $(p_{23}p_{56})$ *et* $(p_{34}p_{61})$ *sont concourantes.* (*Et bien sûr ceci est vrai pour tout choix de numérotation des six droites, cf. figure plus bas*).

(ii) *Réciproquement, si ces trois droites sont concourantes, alors* $\mathbf{D}_1, \dots, \mathbf{D}_6$ *sont tangentes à une unique conique non dégénérée* $\mathscr{C}$.

Démonstration. — Soit $f_i \in V^*$ une équation (unique à homothétie près) de $\mathbf{D}_i$ et soit q_i le point $[f_i]$ de $\mathbb{P}(V^*)$. Alors trois des q_i ne sont jamais alignés. De plus, la droite (q_1q_2) (resp. (q_2q_3), etc.) est la duale du point p_{12} (resp. p_{34}, etc.).

Notons E, F, G les points de concours des « paires de côtés opposés » $\big((q_1q_2), (q_4, q_5)\big)$, etc. Comme on l'a vu dans la définition 22.13, ces trois points sont distincts. D'autre part, ils sont duaux des droites $(p_{12}p_{45})$, $(p_{23}p_{56})$ et $(p_{34}p_{56})$; celles-ci sont donc deux à deux distinctes.

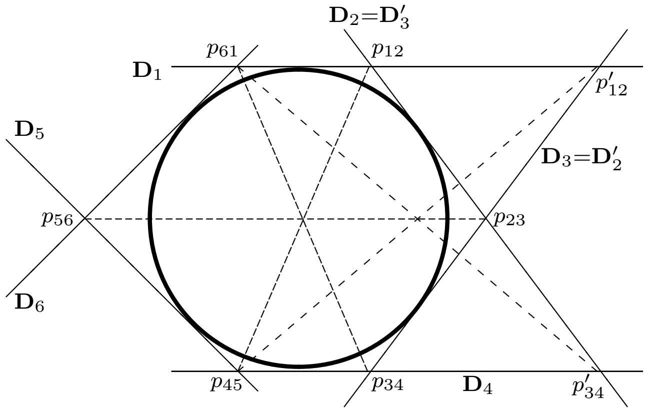
(i) Supposons que $\mathbf{D}_1, \dots, \mathbf{D}_6$ soient tangentes à une même conique non dégénérée $\mathscr{C} = \mathscr{V}(Q)$. Alors, d'après la proposition 24.4, les points $q_1, \dots, q_6$ de $\mathbb{P}(V^*)$ appartiennent à la conique non dégénérée $\mathscr{V}(Q^*)$ donc, d'après le théorème de Pascal appliqué dans $\mathbb{P}(V^*)$, les points E, F, G sont alignés et donc les trois droites de l'énoncé sont concourantes.

(ii) Réciproquement, supposons que ces trois droites soient concourantes. Alors les points E, F, G sont alignés et donc, d'après la réciproque du théorème de Pascal (appliquée dans $\mathbb{P}(V^*)$), il existe une forme quadratique non dégénérée Γ sur V^*, unique à homothétie près, telle que les points $q_1, \dots, q_6$ appartiennent à la conique $\mathscr{V}(\Gamma)$. D'après la remarque 24.1, il existe une unique forme quadratique non dégénérée Q sur V telle que $\Gamma = Q^*$, et alors les droites $\mathbf{D}_1, \dots, \mathbf{D}_6$ sont tangentes à $\mathscr{V}(Q)$ d'après la proposition 24.4. Ceci prouve (ii), à l'exception de l'assertion d'unicité de $\mathscr{C}$.

Mais si Q' est une forme quadratique non dégénérée telle que les $\mathbf{D}_i$ soient tangentes à $\mathscr{V}(Q')$, alors les q_i appartiennent à $\mathscr{V}(Q'^*)$ et donc il existe $\mu \in k^\times$ tel que $Q'^* = \mu\Gamma$, d'où $Q' = \mu^{-1}Q$ d'après le lemme 24.2. Ceci achève la démonstration du théorème. □

[16] Charles Julien Brianchon, mathématicien français (1783-1864), contemporain de Poncelet.

Dans la figure ci-dessous, on a représenté en pointillé les droites $(p_{12}p_{45})$, etc. et avec des tirets plus espacés les droites $(p'_{12}p_{45})$, etc. correspondant à une autre numérotation des droites, en l'occurrence $\mathbf{D}'_2 = \mathbf{D}_3$ et $\mathbf{D}'_3 = \mathbf{D}_2$ (la droite $(p_{23}p_{56})$ est la même dans les deux cas).

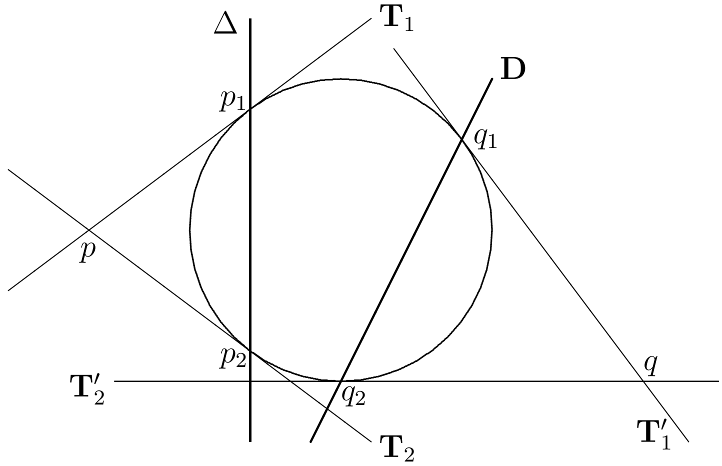


Terminons cette section avec la proposition suivante. Soit $\mathscr{C} = \mathscr{V}(Q)$ une conique non dégénérée du plan projectif $\mathbb{P}(V)$. Pour un point p de $\mathscr{C}$, on a vu que la droite polaire est la tangente à $\mathscr{C}$ en p. Et pour un point p n'appartenant pas à $\mathscr{C}$, sa droite polaire est décrite comme suit.

Proposition 24.6. — *Dans un plan projectif $\mathbb{P}(V)$, soient $\mathscr{C} = \mathscr{V}(Q)$ une conique non dégénérée, p un point de $\mathbb{P}(V)$ n'appartenant pas à $\mathscr{C}$ et $\mathbf{D}$ une droite non tangente à $\mathscr{C}$. Alors :*

(i) $\mathbf{D}$ *coupe $\mathscr{C}$ en deux points distincts q_1 et q_2 (éventuellement à coordonnées dans une extension quadratique de k). Soient $\mathbf{T}'_1$ et $\mathbf{T}'_2$ les tangentes à $\mathscr{C}$ en ces points. Alors le point de concours q de $\mathbf{T}'_1$ et $\mathbf{T}'_2$ est le pôle de la droite $\mathbf{D}$ relativement à la forme quadratique Q.*

(ii) *De même, par p il passe deux droites distinctes $\mathbf{T}_1$ et $\mathbf{T}_2$ tangentes à $\mathscr{C}$ (qui éventuellement sont des droites de $\mathbb{P}(V_{k'})$, où k' est une extension quadratique de k, et qui ont p pour unique point à coordonnées dans k). Notons p_1 et p_2 leurs points de contact avec $\mathscr{C}$; alors la droite $\Delta = (p_1p_2)$ est la polaire du point p relativement à la forme quadratique Q.*



Démonstration. — (ii) Posons $p = [u]$ et $E = (ku)^{\perp}$. Alors la droite polaire de p est la droite $\Delta = \mathbb{P}(E)$. Notons ϕ la forme polaire de Q.

Par hypothèse $Q(u) \neq 0$, donc $ku \cap E = \{0\}$ et donc $V = ku \oplus E$. Comme Q est non dégénérée, alors Q_E ne l'est pas non plus. Donc $\Delta \cap \mathscr{C}$ est formée de deux points distincts

$p_1 = [v_1]$ et $p_2 = [v_2]$ (éventuellement à coordonnées dans une extension quadratique k' de k). Alors on a $\Delta = (p_1p_2)$ et il reste à voir que chacune des droites $\mathbf{T}_i = (pp_i)$ est tangente à $\mathscr{C}$ en p_i. Or $\mathbf{T}_i = \mathbb{P}(E_i)$, où $E_i = ku \oplus kv_i$, et comme $\phi(u, v_i) = 0 = \phi(v_i, v_i)$ alors $E_i \subset (kv_i)^\perp$ et donc la droite $\mathbb{P}(E_i)$ est tangente à $\mathscr{C}$ en $p_i = [v_i]$, d'après la proposition 23.13 (ou 24.4).

Pour prouver (i), on peut utiliser que la polarité est involutive : soit q le pôle de $\mathbf{D}$, alors $\mathbf{D}$ est la polaire de q. Comme $\mathbf{D}$ n'est pas tangente à $\mathscr{C}$ alors $q \notin \mathscr{C}$, donc $\mathbf{D}$ est donnée à partir de q par la construction précédente, d'où (i).

On peut aussi raisonner directement, comme suit. On a $\mathbf{D} = \mathbb{P}(E)$, où E est un sev de V de dimension 2, alors le pôle de $\mathbf{D}$ est le point $q = \mathbb{P}(E^\perp)$.

Comme $\mathbf{D}$ n'est pas tangente à $\mathscr{C}$, alors Q_E est non dégénérée (cf. la démonstration de (i) : si $N(Q_E)$ contenait un vecteur $w \neq 0$, on aurait $E \subset (kw)^\perp$ et donc $\mathbf{D}$ serait tangente à $\mathscr{C}$ en $[w]$). Donc $\mathbf{D} \cap \mathscr{C}$ est formée de deux points distincts $q_1 = [v_1]$ et $q_2 = [v_2]$ (éventuellement à coordonnées dans une extension quadratique k' de k). Alors (v_1, v_2) est une base de E, donc la droite vectorielle $E^\perp$ est l'intersection des deux plans vectoriels $H_i = (kv_i)^\perp$, pour $i = 1, 2$, et donc le pôle q est l'intersection des deux droites projectives $\mathbf{T}'_i = \mathbb{P}(H_i)$, qui sont les tangentes à $\mathscr{C}$ en q_1 et q_2. □

25. Vers Bézout : intersection d'une conique avec une courbe de degré d

Dans cette section, on se place dans le plan projectif $\mathbb{P}^2(k)$. On suppose que k est contenu dans un corps algébriquement clos $\overline{k}$. (Par exemple $k = \mathbb{R} \subset \mathbb{C}$.)

Terminologie 25.1. — Pour tout polynôme non nul $F \in k[X, Y, Z]$ homogène de degré $d \geq 1$, la variété des zéros $\mathscr{V}(F) = \{[x, y, z] \in \mathbb{P}^2(k) \mid F(x, y, z) = 0\}$ est appelée la *courbe projective plane* définie par F.(17)

Comme déjà dit au §13.3, quand on considère une telle courbe, on s'autorise à considérer aussi les points de $\mathscr{V}(F)$ « à valeurs dans $\overline{k}$ », i.e. les points de

$$\mathscr{V}_{\overline{k}}(F) = \{[x, y, z] \in \mathbb{P}^2(\overline{k}) \mid F(x, y, z) = 0\}.$$

Lemme 25.2. — *Soit $P \in \overline{k}[X, Y]$ un polynôme homogène de degré $d \geq 1$. Alors :*

(i) *P se factorise en un produit de d facteurs linéaires (pas nécessairement distincts).*

(ii) *Par conséquent, la variété des zéros $\mathscr{V}_{\overline{k}}(P) \subset \mathbb{P}^2(\overline{k})$ est formée de d points « comptés avec multiplicités ».*

Démonstration. — (i) Écrivons $P = \sum_{i=0}^{d} a_i Y^i X^{d-i}$. Supposons d'abord, pour simplifier, que $a_0 \neq 0$. Remplaçant P par $a_0^{-1} P$, on se ramène au cas où $a_0 = 1$. Alors

$$\frac{1}{Y^d} P(X, Y) = \frac{1}{Y^d}\big(X^d + a_1 Y X^{d-1} + \cdots + a_{d-1} Y^{d-1} X + a_d Y^d\big) = \sum_{i=0}^{d} a_i T^{d-i}$$

où l'on a posé $T = \dfrac{X}{Y}$. Comme $\overline{k}$ est algébriquement clos, ce polynôme $Q(T)$, unitaire de degré d, se factorise en un produit de d termes du 1er degré $T - \alpha_i$ (non nécessairement distincts), pour $i = 1, \dots, d$. Ou bien, si l'on préfère, on peut noter $\beta_1, \dots, \beta_s$ les racines

(17) L'adjectif « plane » signifie « contenu dans un plan ». Il existe dans $\mathbb{P}^3(k)$ des courbes projectives (définies par deux équations homogènes $F(x, y, z, t) = 0 = G(x, y, z, t)$ qui ne sont contenues dans aucun sous-espace projectif $\mathbb{P}(W)$ de dimension 2, ni même « isomorphes » à une courbe projective plane.

distinctes de Q dans $\overline{k}$, chacune étant de multiplicité m_i (avec $m_1 + \cdots + m_s = d$). On a donc

$$\sum_{i=0}^{d} a_i T^{d-i} = \prod_{i=1}^{d}(T - \alpha_i) = \prod_{j=1}^{s}(T - \beta_j)^{m_j}.$$

En remultipliant ceci par Y^d, on obtient :

$$P(X,Y) = \prod_{i=1}^{d}(X - \alpha_i Y) = \prod_{j=1}^{s}(X - \beta_j Y)^{m_j}.$$

Ceci prouve (i) lorsque $a_0 \neq 0$. Dans le cas général, soit r le plus petit entier ≥ 0 tel que $a_r \neq 0$. À nouveau, remplaçant P par $a_r^{-1}P$, on se ramène au cas où $a_r = 1$. Alors $P(X,Y) = Y^r P_1(X,Y)$, où $P_1(X,Y)$ est un polynôme homogène de degré $d - r$ contenant le terme X^{d-r} (avec le coefficient 1). D'après ce qui précède, appliqué à P_1, on a une factorisation

$$P_1(X,Y) = \prod_{i=1}^{d-r}(X - \alpha_i Y) = \prod_{j=1}^{s}(X - \beta_j Y)^{m_j},$$

où dans le terme de droite la somme des m_j vaut $d - r$. Il en résulte que

$$(\star) \qquad P(X,Y) = Y^r \prod_{i=1}^{d-r}(X - \alpha_i Y) = Y^r \prod_{j=1}^{s}(X - \beta_j Y)^{m_j}.$$

Ceci achève la preuve de (i). L'assertion (ii) en découle, car $(\star)$ montre que $\mathscr{V}_{\overline{k}}(P)$ est formé du point $[1,0]$, compté r fois, et des points $[\beta_j, 1]$, chacun compté m_j fois. $\square$

Corollaire 25.3. — *Soit $F \in k[X,Y,Z]$ homogène de degré $d \geq 1$ et soit* $\mathbf{D}$ *une droite de $\mathbb{P}^2(k)$ dont l'équation $L(X,Y,Z)$* ne divise pas *F. Alors :*

(i) $\mathbf{D} \cap \mathscr{V}(F)$ *est formé d'au plus d points distincts.*

(ii) *Si l'on se place sur le corps $\overline{k}$, cette intersection est formée d'exactement d points, comptés avec multiplicités.*

Démonstration. — Écrivons $L(X,Y,Z) = aX + bY + cZ$ et supposons par exemple que $c \neq 0$. Remplaçant L par $c^{-1}L$, on se ramène au cas où $c = 1$. On peut alors faire la division euclidienne du polynôme $F \in k[X,Y][Z]$ par le polynôme L, unitaire en Z. On obtient :

$$F(X,Y,Z) = L \cdot Q(X,Y,Z) + R(X,Y),$$

où R est de degré 0 en Z, i.e. il ne dépend que de X et Y. C'est aussi le polynôme en X, Y obtenu en remplaçant Z par $-aX - bY$; en particulier il est nul ou bien homogène de degré d. L'hypothèse que L ne divise pas F signifie que $R \neq 0$. On voit alors qu'un point $[x,y,z]$ de $\mathbb{P}^2(k)$ appartient à $\mathbf{D} \cap \mathscr{V}(F)$ ssi le point $[x,y]$ de $\mathbb{P}^1(k)$ vérifie $R(x,y) = 0$ (et dans ce cas $z = -ax - by$). Comme R est un polynôme non nul homogène de degré d alors, d'après le lemme 25.2, $\mathscr{V}_{\overline{k}}(R)$ est formé d'exactement d points comptés avec multiplicité, donc au plus d points distincts, et *a fortiori* $\mathscr{V}_k(R)$ contient au plus d points distincts. Ceci prouve (ii) et (i). $\square$

Proposition 25.4. — *Soit $F \in k[X,Y,Z]$ homogène de degré $d \geq 2$ et soit $\mathscr{C} = \mathscr{V}(Q)$ une conique non dégénérée de $\mathbb{P}^2(k)$, telle que $\mathscr{V}_{\overline{k}}(Q)$* ne soit pas *contenue dans $\mathscr{V}_{\overline{k}}(F)$. Alors :*

(i) $\mathscr{C} \cap \mathscr{V}(F)$ *est formé d'au plus $2d$ points distincts.*

(ii) *Si l'on se place sur le corps $\overline{k}$, cette intersection est formée d'exactement $2d$ points, « comptés avec multiplicités ».*

Démonstration. — À nouveau, (i) est une conséquence immédiate de (ii), donc il suffit de démontrer (ii). Pour simplifier l'écriture, supposons donc k algébriquement clos. Notons ϕ la forme polaire de Q. Comme $\mathscr{C} = \mathscr{V}(Q)$ n'est pas contenue dans $\mathscr{V}(F)$, il existe un point $p = [v] \in \mathscr{C}$ n'appartenant pas à $\mathscr{V}(F)$.

Comme Q est non dégénérée alors, d'après la proposition 22.17, il existe un vecteur isotrope w tel que $\phi(v, w) = 1$ et alors V est la somme directe du plan hyperbolique $E = \mathrm{Vect}(v, w)$ et de la droite vectorielle $D = E^{\perp}$. Soit u un générateur de D, alors $\mathscr{B} = (u, v, w)$ est une base de V et

$$\mathrm{Mat}_{\mathscr{B}}(Q) = \begin{pmatrix} \lambda & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}$$

avec $\lambda \neq 0$. Remplaçant simultanément Q et w par $-\lambda^{-1}Q$ et $(-\lambda/2)w$, on se ramène au cas où

$$\mathrm{Mat}_{\mathscr{B}}(Q) = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 0 & 1/2 \\ 0 & 1/2 & 0 \end{pmatrix}.$$

Remplaçant alors X, Y, Z par les coordonnées dans la base $\mathscr{B}$, on se ramène au cas où

$$Q(X, Y, Z) = -X^2 + YZ.$$

Prenons comme droite à l'infini $\mathscr{D}_\infty$ la droite d'équation $z = 0$. Elle coupe $\mathscr{D}$ en l'unique point $p = [0, 1, 0]$ qui par hypothèse n'appartient pas à $\mathscr{V}(F)$.

L'intersection $\mathscr{V}(F) \cap \mathscr{C}$ est donc contenue dans l'intersection de $\mathscr{C}$ avec le plan affine $\mathbb{P}(V) - \mathscr{D}_\infty$, qui est la parabole

$$\mathscr{C}' = \big\{[x, y, 1] \in \mathbb{P}(V) \mid y = x^2\big\} = \big\{[x, x^2, 1] \in \mathbb{P}(V) \mid x \in k\big\}.$$

On a donc

$$\mathscr{V}(F) \cap \mathscr{C} = \mathscr{V}(F) \cap \mathscr{C}' = \{x \in k \mid F(x, x^2, 1) = 0\}.$$

Comme F ne s'annule pas en $p = [0, 1, 0]$ alors F contient le terme Y^d avec un coefficient non nul, et donc le polynôme $P(X) = F(X, X^2, 1)$ est de degré exactement $2d$. Soient $\beta_1, \dots, \beta_r$ ses racines distinctes dans k, chacune étant de multiplicité m_i, avec $m_1 + \cdots + m_r = 2d$. Alors $\mathscr{V}(F) \cap \mathscr{C}$ est formé des points $[\beta_j, \beta_j^2, 1]$, chacun « compté m_i fois ». □

Définitions 25.5. — (1) On « rappelle » que l'anneau $A = \overline{k}[X, Y, Z]$ est **factoriel**, i.e. que tout $P \in A$ s'écrit comme produit d'éléments irréductibles, ceci de façon *unique* à l'ordre des facteurs près (et à multiplication près par des éléments inversibles de A, i.e. des éléments de $\overline{k}^{\times}$).[18] De plus, on peut montrer que si P est **homogène** alors tous les facteurs irréductibles de P sont également homogènes.

(2) Si $P = P_1^{m_1} \cdots P_r^{m_r}$ est ainsi factorisé, les P_i étant des polynômes homogènes irréductibles tels que $P_i \neq \lambda P_j$ pour tout $i \neq j$ et $\lambda \in \overline{k}^{\times}$, alors la variété des zéros $\mathscr{V}_{\overline{k}}(P)$ est la réunion des $\mathscr{V}_{\overline{k}}(P_i)$ (chacune étant « comptée m_i fois »), et l'on dit que celles-ci sont les **composantes irréductibles** de $\mathscr{V}_{\overline{k}}(P)$.

[18] Ceci est vrai pour $k[X_1, \dots, X_n]$ pour tout corps k, voir par exemple le cours 4M002 ou un cours de L3 d'arithmétique.

(3) Conservons les notations de (2) et soit $Q \in \overline{k}[X,Y,Z]$ un autre polynôme homogène. On peut montrer (théorème des zéros de Hilbert) que $\mathscr{V}_{\overline{k}}(Q)$ contient $\mathscr{V}_{\overline{k}}(P_i)$ si et seulement si P_i divise Q.

(4) On dit que P et Q sont **sans facteur commun** s'ils n'ont pas de diviseurs communs autres que les éléments de $\overline{k}^{\times}$. D'après le point (3), ceci équivaut à dire qu'aucune composante irréductible de $\mathscr{V}_{\overline{k}}(P)$ n'est contenue dans $\mathscr{V}_{\overline{k}}(Q)$ et vice-versa. On dit alors que $\mathscr{V}_{\overline{k}}(P)$ et $\mathscr{V}_{\overline{k}}(Q)$ sont **sans composante commune**. Si Q est irréductible, ceci est le cas ssi Q ne divise pas P.

(5) Si $Q \in \overline{k}[X,Y,Z]$ est un polynôme homogène de degré 2, il est irréductible ssi ce n'est pas le produit de deux formes linéaires, i.e. ssi la forme quadratique Q est non dégénérée. Dans ce cas, on voit que la condition « $\mathscr{V}_{\overline{k}}(Q)$ n'est pas contenue dans $\mathscr{V}_{\overline{k}}(F)$ » utilisée dans la proposition 25.4 équivaut à dire que Q et F sont sans facteur commun.

On peut alors démontrer (mais ceci demande un peu de travail) le théorème suivant : [19]

***Théorème 25.6* (de Bézout).** — *Soient k un corps algébriquement clos et $F, G \in k[X,Y,Z]$ deux polynômes homogènes, de degrés p et q, sans facteur commun. Alors :*

(i) *$\mathscr{V}(F) \cap \mathscr{V}(G)$ est formé d'au plus pq points distincts.*

(ii) *Si l'on définit de façon appropriée la notion de* « multiplicité d'intersection en un point », *alors $\mathscr{V}(F) \cap \mathscr{V}(G)$ est formé d'exactement pq points, « comptés avec multiplicités ».*

Références pour le théorème de Bézout :

[Fu] W. Fulton, Algebraic curves (Benjamin, 1974), Chap. 5, §3 (disponible en ligne sur la page de l'auteur).
[Ku] E. Kunz, Introduction to plane algebraic curves (Birkhäuser, 2005), Chap. 5.
[ST] J. H. Silverman, J. Tate, Rational points on elliptic curves (Springer, 1992), App. §§3-4.

[19] Étienne Bézout, mathématicien français (1730-1783).