170 : Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications

Cadre : K corps de caractéristique différente de 2, E un K - espace vectoriel de dimension finie n.

I-Formes bilinéaires symétriques et formes quadratiques

1-Formes bilinéaires symétriques versus formes quadratiques

Définition 1. Une forme bilinéaire sur E est une application $f : E \times E \to K$ linéaire en ses deux variables. Un forme bilinéaire f est dite symétrique si pour tous $x, y \in E, f(x, y) = f(y, x)$

Exemple 2. Le produit scalaire est une forme bilinéaire.

Définition 3. Soit f une forme bilinéaire sur E. L'application $f_y : x \in E$ associe $f(x, y) \in K$ est une forme linéaire sur E (De même pour f_x).

Définition 4. Une application $q : E \to K$ est dite forme quadratique sur E s'il existe une forme bilinéaire symétrique $f : E \times E \to K$ telle que $f(x, x) = q(x)$.

Exemple 5.

- $E = \mathbb{R}^3$, $q(x) = 2x_1^2 - 3x_2^2 + 3x_3^2 + 2x_1x_2 - 3x_1x_3 + 5x_2x_3$ est une forme quadratique.
- L'application déterminant : $det : \mathcal{M}_2(\mathbb{R}) \to \mathbb{R}$ est une forme quadratique.
- $q : \mathcal{M}_n(\mathbb{R}) \to \mathbb{R}$, $A \mapsto Tr({}^tAA)$

Proposition 6. Réciproquement, si $q : E \to K$ une forme quadratique sur E, alors il existe une unique forme bilinéaire symétique $f : E \times E \to K$ telle que $f(x, x) = q(x)$ pour tout $x \in E$, f est donnée par : $f(x, y) = \frac{1}{2}(q(x + y) - q(x) - q(y))$. f est appelé forme polaire de q.

Exemple 7.

- $q_1 : \mathbb{R}^2 \to \mathbb{R}, \quad q_1(x_1, x_2) = x_1^2 + x_2^2 + x_1x_2$ admet pour forme polaire $f(x, y) = x_1y_1 + x_2y_2 + \frac{1}{2}x_1y_2 + \frac{1}{2}x_2y_1$
- $q_2 : \mathcal{M}_n(\mathbb{R}) \to \mathbb{R}, \quad A \mapsto Tr({}^tAA)$ admet pour forme polaire $f(A, B) = Tr({}^tAB)$

2-Expression matricielle

Définition 8. Soit f une forme bilinéaire sur E et (e_i) une base de E. On appelle matrice de f dans la base $B = (e_i)_i$ la matrice :

$$Mat_B(f) = \begin{pmatrix} f(e_1, e_1) & f(e_1, e_2) & \dots & f(e_1, e_n) \\ f(e_2, e_1) & f(e_2, e_2) & \dots & f(e_2, e_n) \\ \vdots & \vdots & \ddots & \vdots \\ f(e_n, e_1) & f(e_n, e_2) & \dots & f(e_n, e_n) \end{pmatrix}$$

Remarque 9. f forme bilinéaire symétrique $\Leftrightarrow$ La matrice de f (dans une base quelconque) est symétrique.

Définition 10. Soit f une forme bilinéaire sur E, x,$y \in E$, $\mathcal{B} = (e_i)_i$ une base de E et $A = Mat_{\mathcal{B}}(f)$, $X = Mat_{\mathcal{B}}(x)$, $Y = Mat_{\mathcal{B}}(y)$. On a : $f(x, y) = {}^tXAY$.

Remarque 11. On appelle matrice de q la matrice de sa forme polaire.

Exemple 12. Soit $q(x, y, z) = 3x^2 + y^2 + 2xy - 3xz$. Alors :

$$Mat(q) = \begin{pmatrix} 3 & 1 & -3/2 \\ 1 & 1 & 0 \\ -3/2 & 0 & 0 \end{pmatrix}$$

Remarque 13. L'application qui à f associe sa matrice dans une base fixée de E est un isomorphisme.

Définition 14. (matrices congruentes ou équivalentes) Deux matrices carrées A et B d'ordre n sont dites congruentes s'il existe $P \in \mathcal{GL}_n(\mathbb{R})$ telle que $A = {}^tPBP$.

Proposition 15. (Avec les notations précédentes) Deux matrices sont congruentes de rang $r \Leftrightarrow$ Elles représentent la même forme quadratique dans deux bases $\mathcal{B}$ et $\mathcal{B}'$ de E, P matrice de passage de $\mathcal{B}$ à $\mathcal{B}'$, $r = rg(q)$.

Définition 16. Soit f une forme bilinéaire sur E. On appelle rang de f le rang de la matrice qui représente f dans une base (quelconque) de E.

Remarque 17. f est dite non dégénérée $\Leftrightarrow$ son rang est maximal $\Leftrightarrow$ sa matrice associée est inversible.

Proposition 18. Soit $f : E \times E \to K$ Une forme bilinéaire, $j : E \to E^*$, $y \mapsto j(y) = f_y$, où $f_y : E \to K$, $x \mapsto f(x, y)$. On a :

- $j(y)(x) = f_y(x) := f(x, y)$
- f_y non dégénérée $\Leftrightarrow$ f_y est un isomorphisme

Exemple 19. Si f est un produit scalaire, alors f_y est un isomorphisme d'espaces vectoriels.

3-Rang et noyau d'une forme quadratique

Définition 20. On appelle noyau et on note $N(q)$ (respectivement rang, noté $rg(q)$) d'une forme quadratique q le noyau (respectivement le rang) de la forme polaire associée à q.

Proposition 21. Soit f la forme bilinéaire sur E associée à la forme quadratique q.

1. Le rang de q est le rang de l'application $j : E \to E^*$, $y \mapsto f(., y) = f_y$.
2. Le noyau de q est le noyau de l'application j, c'est-à-dire $N(q) := \{y \in E | f(x, y) = 0, \forall x \in E\}$

3. q est dite non dégénérée si j est injective, c'est-à-dire si $N(q) = \{0\}$, ou encore si $f(x,y) = 0, \forall x \in E \Rightarrow y = 0$.

Définition 22. Soit q une forme quadratique à valeurs réelles. q est dite positive si $q(x) \geq 0$ pour tout x.
q est dite définie positive si elle est positive et si $q(x) = 0 \Leftrightarrow x = 0$.

Proposition 23. Une forme quadratique définie est non dégénéréee.

Exemple 24. pour $x \in \mathbb{R}^3$, $q(x) = 4x_1^2 + 3x_2^2 + 5x_1x_2 - 3x_1x_3 + 8x_2x_3$ est non définie et non dégénérée.

Proposition 25. $\dim(E) = \dim(N(q)) + rg(q)$

II-Orthogonalité et isotropie

1-Orthogonalité

Soit q une forme quadratique et b sa forme polaire associée.

Définition 26.
- Deux vecteurs x et y sont dits orthogonaux selon q (ou selon b) si $b(x,y) = 0$.
- Soit $A \subset E$. On appelle orthogonal de A selon q (ou selon b) l'ensemble $A^\perp = \{y \in E | \forall x \in A, b(x,y) = 0\}$.
- Deux sous-ensembles A et B de E sont dit orthogonaux selon q (ou selon b) si $\forall x \in A$, $\forall y \in B$, $b(x,y) = 0$. On note alors $A \perp B$.

Proposition 27.

- $A^\perp$ est un sev de E.
- $\{0\}^\perp = E$
- $E^\perp = N(q)$
- $\forall A \subset E : N(q) \subset A^\perp$

Proposition 28. Soit F un sev de E alors

- $dim(E) = dim(F) + dim(F^\perp) - dim(F \cap N(q))$
- $F^{\perp\perp} = F + N(q)$

Remarque 29. En particulier si q est non dégénérée alors :

- $dim(E) = dim(F) + dim(F^\perp)$
- $F^{\perp\perp} = F$

Contre-exemple 30. $E = \mathbb{R}^2$, $q(x) = x_1^2 - x_2^2$. $F = Vect\begin{pmatrix}1\\1\end{pmatrix}$. Alors $F = F^\perp$. q est non dégénérée, mais $E \neq F \oplus F^\perp$.

2-Isotropie

Définition 31. Un vecteur $x \in E$ est dit isotrope pour q (ou pour b) si $b(x,x) = 0$ (autrement dit si $q(x) = 0$).

Définition 32. On appelle cône isotrope l'ensemble $\mathcal{I}(q) = \{x \in E | q(x) = 0\}$

Remarque 33. $\mathcal{I}(q)$ n'est pas un espace vectoriel mais un sous-ensemble de vecteurs $\mathcal{V}$, avec $\mathcal{V} = \{x \in \mathcal{V} | \forall \lambda \in K,\ \lambda x \in \mathcal{V}\}$.

Exemple 34.

- Si $E = \mathbb{R}^2$ et $q(x) = x_1^2 - x_2^2$, on a $\mathcal{I}(q) = \{(x_1,x_2) \in \mathbb{R}^2 | x_1 = \pm x_2\}$ (voir figure 1)
- Si $E = \mathbb{R}^3$ et $q(x) = x_1^2 + x_2^2 - x_3^2$, on a $\mathcal{I}(q) = \{(x_1,x_2,x_3) \in \mathbb{R}^3 | x_3 = \pm\sqrt{x_1^2 + x_2^2}\}$(voir figure 2)

Proposition 35. $N(q) \subset \mathcal{I}(q)$

Contre-exemple 36. Dans les exemples précédents, $N(q) \neq \{0\}$ donc on n'a pas l'inclusion réciproque.

Définition 37. Un sous-espace vectoriel F de E est dit isotrope si : $F \cap F^\perp \neq \{0\}$

Remarque 38. E admet des sous espaces isotropes $\Leftrightarrow \mathcal{I}(q) \neq \{0\}$

Proposition 39. Soit F un sous-espace vectoriel de E alors : $E = F \oplus F^\perp \Longleftrightarrow F$ est non isotrope (i.e. $F \cap F^\perp = \{0\}$).

Exemple 40. $q : \mathbb{R}^4 \to \mathbb{R}$, $q(x) = x_1^2 + 2x_1x_2 + 2x_1x_3 + 2x_1x_4 + 4x_2x_3 + 4x_3x_4$. Tout hyperplan d'équation $ax_1 + x_2 + bx_3 + x_4 = 0$ est isotrope.

Exemple 41. $q : \mathcal{M}_2(\mathbb{R}) \to \mathbb{R}$, $A \mapsto \det(A)$. $F = \{A \in \mathcal{M}_2(\mathbb{R} | Tr(A) = 0\}$
$F^\perp = \{A \in \mathcal{M}_2(\mathbb{R}) | A = \begin{pmatrix}a & 0\\0 & a\end{pmatrix}$, $a \in \mathbb{R}\}$. F est non isotrope et $\mathcal{M}_2(\mathbb{R}) = F \oplus F^\perp$.

3-Groupe orthogonal

Proposition 42. Soit q une forme quadratique non degénérée sur E et $f \in End(E)$. Soit f^* l'unique endomorphisme de E tel que $\forall (x,y) \in E^2$, $b(f(x),y) = b(x, f^*(y))$. Les propriétés suivantes sont équivalentes :

1. $q(f(x)) = q(x) \quad \forall x \in E$
2. $b(f(x), f(y)) = b(x,y) \quad \forall x, y \in E$
3. $f^* \circ f = I_d$ (ou de manière équivalente $f \circ f^* = I_d$).

Un tel endomorphisme est dit orthogonal relativement à q. On note
$O(q) = \{f \in End(E) | f \circ q = f\}$. $O(q)$ est un groupe, appelé groupe orthogonal de q.

Proposition 43. Soit $\mathcal{B}$ une base de E, $S = Mat_{\mathcal{B}}(q)$ et $A = Mat_{\mathcal{B}}(f)$, on a :
$f \in O(q) \Longleftrightarrow {}^tASA = A$

Exemple 44. Soit $q : \mathbb{R}^2 \to \mathbb{R}$ définie dans la base canonique par $q(x) = 2x_1x_2$. On a
$O(q) = \left\{\begin{pmatrix}a & 0\\0 & 1/a\end{pmatrix}, a \in \mathbb{R}\backslash\{0\}\right\} \cup \left\{\begin{pmatrix}0 & b\\1/b & 0\end{pmatrix}, b \in \mathbb{R}\backslash\{0\}\right\}$

4-Bases orthogonales et réduction simultanée

Définition 45. Une base $\mathcal{B} = \{e_i\}$ de E est dite orthogonale pour la forme bilinéaire symétrique b ou q-orthogonale si $\forall j \neq i$, $b(e_i, e_j) = 0$. Elle est dite orthonormale si $b(e_i, e_j) = \delta_{e_i,e_j}$.

Proposition 46. Soit $E \neq \{0\}$. Il existe $B = (e_1, ..e_n)$ base de E telle que $\forall x \in K^n$, si $x = \sum_{i=1}^n x_i e_i$, $\quad q(x) = \sum_{i=1}^r a_i x_i^2$, avec $a_i \in K$, et $r = rg(q)$. La base B est dite q-orthogonale.

Remarque 47. Chercher une base orthogonale revient donc à chercher une base dans laquelle la matrice de q est diagonale.

Théorème 48. (Méthode de Gauss) Pour toute forme quadratique q il existe $r = rg(q)$ formes linéaires indépendantes $l_1, .., l_r$ telles que $q(x) = \sum \lambda_i l_i(x)^2$, $\lambda_i \in K$.

Exemple 49. Si $E = \mathbb{R}^3$ et $q(x) = 5x_1x_2 + 6x_1x_3 + 3x_2x_3$ la méthode de Gauss nous donne $(q) = \frac{1}{20}(5x_1 + 5x_2 + 9x_3)^2 - \frac{1}{20}(5x_1 + 5x_2 - 3x_3)^2 - \frac{18}{5}x_3^2$.

Théorème 50. Soit $(E, <,>)$ un espace euclidien et q une forme quadratique sur E alors il existe des bases qui sont orthogonales pour $<,>$ et q.

Application 51. (Convexité logarithmique du déterminant) Soient A, B dans $S_n^{++}(\mathbb{R}) = \{\text{matrices symétriques définies positives}\}$ et α, $\beta \in \mathbb{R}$ tels que $\alpha + \beta = 1$. Alors $\det(\alpha A + \beta B) \geqslant (\det(A))^\alpha (\det(B))^\beta$.

Application 52. (Ellipsoïde de John Loewner) Soit K un compact non vide de $\mathbb{R}^n$. Alors il existe un unique ellipsoïde centré en 0 de volume minimal qui contient K.

III-Classification des formes quadratiques

Définition 53. Soient b et b' deux formes bilinéaires symétriques sur E. On dit que b et b' sont équivalentes s'il existe $u \in GL_n(E)$ tel que $\forall x, y \in E$, $b'(x, y) = b(u(x), u(y))$. Autrement dit si $\exists P \in \mathcal{GL}_n(\mathbb{K})$ telle que $Mat_{\mathcal{B}}(q') = {}^tP(Mat_{\mathcal{B}}(q'))P$

1-Sur un espace vectoriel complexe

Dans cette partie E designe un $\mathbb{C}$-ev de dimension n (E est donc isomorphe à $\mathbb{C}^n$ moyennant le choix d'une base), q forme quadratique sur E .

Théorème 54. Il existe une base $(e_i)_i$ de E telle que si $x = \sum x_i e_i$, $q(x) = x_1^2 + ... + x_r^2$ où $r = rg(q)$, c'est-à-dire : $Mat_{e_i}(q) = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix}$

Corollaire 55. Il existe une base q-orthonormée $\Leftrightarrow rg(q) = n \Leftrightarrow q$ est non dégénérée.

Proposition 56. Il existe une unique classe d'équivalence des formes quadratiques non dégénérées.

2-Sur un espace vectoriel réel

Dans cette partie E designe un $\mathbb{R}$-ev de dimension n (E est donc isomorphe à $\mathbb{R}^n$ moyennant le choix d'une base), q forme quadratique sur E .

Théorème 57. (Sylvester) Soit q une forme quadratique sur E. Il existe une base $(e_i)_i$ de E telle que si $x = \sum x_i e_i$ on a : $q(x) = x_1^2 + ... + x_p^2 - x_{p+1}^2 - ... - x_r^2$ où $r = rg(q)$ et p un entier qui ne dépend que de q (et non pas de la base). On a donc : , c'est-à-dire :
$Mat_{e_i}(q) = \begin{pmatrix} I_p & 0 & 0 \\ 0 & -I_{r-p} & 0 \\ 0 & 0 & 0 \end{pmatrix}$
Le couple $(p, r - p)$ noté $sgn(q)$ est appelé signature de q.

Remarque 58. On peut déterminer la signature d'une forme quadratique q à l'aide des valeurs propres de sa matrice associée A. Son rang est égal aux nombre de valeurs propres non nulles et $r - p$ est le nombre de valeurs propres de A strictement négatives.

Exemple 59. Sur $\mathcal{M}_2(\mathbb{R})$ le déterminant est une forme quadratique de signature $(2, 2)$.

Exemple 60. Sur $\mathbb{R}^3$, par la méthode de Gauss, on trouve que la signature de $q(x) = x_1^2 + 2x_2^2 + 15x_3^2 - 4x_1x_2 + 6x_1x_3 - 8x_2x_3$ est $(2, 1)$

Corollaire 61. Soit q une forme quadratique sur E alors :

- q definie positive (ie E euclidien) $\Longleftrightarrow sgn(q) = (n, 0) \Longleftrightarrow$ il existe des bases orthonormées.
- q définie négative $\Longleftrightarrow sgn(q) = (0, n)$
- q est non dégénérée (ie $N(q) = \{0\}$) $\Longleftrightarrow sgn(q) = (p, n - p)$

Proposition 62. Il y a $n + 1$ classes d'équivalence de formes quadratiques non dégénérées.

3-Sur un corps fini

Dans ce paragraphe $K = F_q$ est un corps fini de caractéristique différente de 2 et E est un K-espace vectoriel de dimension n.

Théorème 63. Soit $\alpha \in F_q^*$, $\alpha \notin F_q^{*2}$. Il y a deux classes d'équivalences de formes quadratiques non dégénérées sur E, de matrices,

$$q_1 = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{pmatrix} \text{ ou } q_2 = \begin{pmatrix} 1 & & & 0 \\ & \ddots & & \\ & & 1 & \\ 0 & & & \alpha \end{pmatrix}$$

Une forme quadratique q est de l'un ou l'autre type selon son déterminant modulo les carrés du corps de base.

Lemme 64. L'équation en x, y, $ax^2 + by^2 = 1$, avec $a, b \in F_q^*$, a des solutions dans F_q.

Application 65. (Loi de réciprocité quadratique) On définit le symbole de Legendre par pour tout $n \in F_p$ $(\frac{n}{p}) = \begin{cases} 1 \text{ si n est un carré modulo } p \\ 0 \text{ si p divise n} \\ -1 \text{ sinon} \end{cases}$

Soit p, q deux nombres premiers impairs alors :

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{(p-1)(q-1)/4}$$

IV-Applications

1-Recherche de minimum

Théorème 66. Soit $f : U \subset \mathbb{R}^n \to \mathbb{R}$ une fonction de classe $\mathcal{C}^2$ telle que $df_a = 0$ pour un $a \in U$ de sorte que $f(a+h) = f(a) + \frac{1}{2}q(h) + \circ(||h||^2)$, où q est la forme quadratique définie par $q(h) = \sum_i h_i^2 \frac{\partial^2 f}{\partial x_i^2}(a) + 2\sum_{i<j} h_i h_j \frac{\partial^2 f}{\partial x_i \partial x_j}(a)$ alors :

1. Si f admet un minimun (resp. maximum) relatif en a alors q est une forme quadratique positive (resp. négative).
2. Si q est une forme quadratique définie positive (resp. définie négative) alors f admet un minimum (resp. maximum) relatif en a.

Exemple 67. (en dimension 2) Soit $f : U \subset \mathbb{R}^2 \to \mathbb{R}$ de classe $\mathcal{C}^2$ telle que $df_a = 0$ pour $a \in U$. On note $r = \frac{\partial^2 f}{\partial x^2}(a)$, $s = \frac{\partial^2 f}{\partial x \partial y}(a)$ et $t = \frac{\partial^2 f}{\partial y^2}(a)$ alors :

- si $rt - s^2 > 0$ et $r > 0$, f admet un minimum relatif en a.
- si $rt - s^2 > 0$ et $r < 0$, f admet un maximum relatif en a.
- si $rt - s^2 < 0$, f n'admet pas d'extremum en a.
- si $rt - s^2 = 0$, on ne peut pas conclure.

2-Racines distinctes d'un polynôme

Application 68. (Comptage des racines d'un polynôme par les formes quadratiques.) Soit $P \in \mathbb{R}[X]$ de degré n et $a_1, ..., a_n$ les racines de P (dans $\mathbb{C}$) comptées avec multiplicité. Pour $i \in \mathbb{N}$, on note $s_i = \sum_{k=1}^n a_k^i$, la i-ème somme de Newton. Soit q la forme quadratique réelle définie sur $\mathbb{R}^n$ par :

$$q(x) = q(x_0, ..., x_{n-1}) = \sum_{0 \leq i,j \leq n-1} s_{i+j} x_i x_j$$

Notons (s, t) la signature de q, on a :

1. le nombre de racines complexes distinctes de P est $s + t = rg(q)$
2. le nombre de racines réelles distinctes de P est $s - t$

3-Classification des coniques

Définition 69. Soient q une forme quadratique non nulle et φ une forme linéaire sur l'espace euclidien $(\mathbb{R}^2, <,>)$. On appelle conique l'ensemble :
$\mathcal{C} = \{v \in \mathbb{R}^2 | q(v) + \varphi(v) = k\}$ où $k \in \mathbb{R}$.

Exemple 70. L'équation $x^2 + y^2 - 1 = 0$ décrit une conique constituée du cercle de centre 0 et de rayon 1.

Théorème 71. (voir figure 3) Soit $\mathcal{C}$ une conique définie comme précédemment. On suppose $\mathcal{C} \neq 0$ et non réduit à un point.

1. Si $sgn(q) = (2, 0)$: $\mathcal{C}$ est une ellipse.
2. Si $sgn(q) = (1, 1)$: $\mathcal{C}$ est une hyperbole qui eventuellement dégénère en deux droites non parallèles.
3. Si $sgn(q) = (1, 0)$: $\mathcal{C}$ est une parabole, qui dégénère en une droite, ou en deux droites parallèles si la direction principale isotrope est contenu dans $Ker(\varphi)$.

Proposition 72. Par cinq points distincts A, B, C, D et E d'un plan affine réel passe une conique. Elle est unique ssi 4 points quelconques parmis ces 5 sont non alignés. Elle est non dégénrée ssi 3 points quelconques parmis ces 5 sont non alignés.

Développements possibles

- Classification des formes quadratiques sur F_q.
- Comptage des racines d'un polynôme via les formes quadratiques.
- Loi de réciprocité quadratique.
- Ellipsoide de John Loewner.
- Lemme de Morse.
- Par 5 points distincts passe une connique

Références

- Grifone
- Gourdon
- Perrin

ANNEXES :

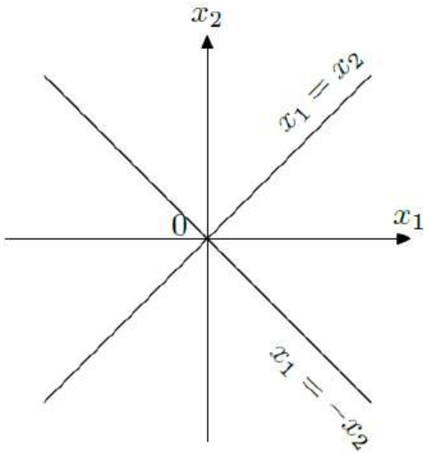

Figure 1

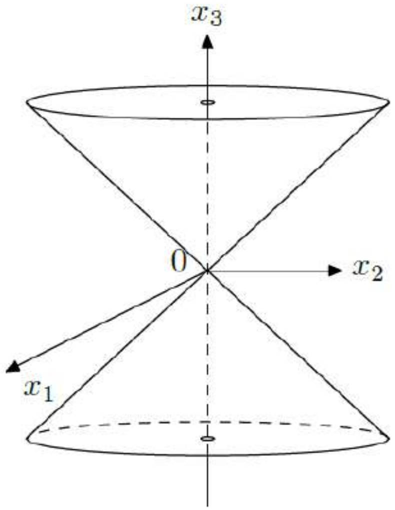

Figure 2

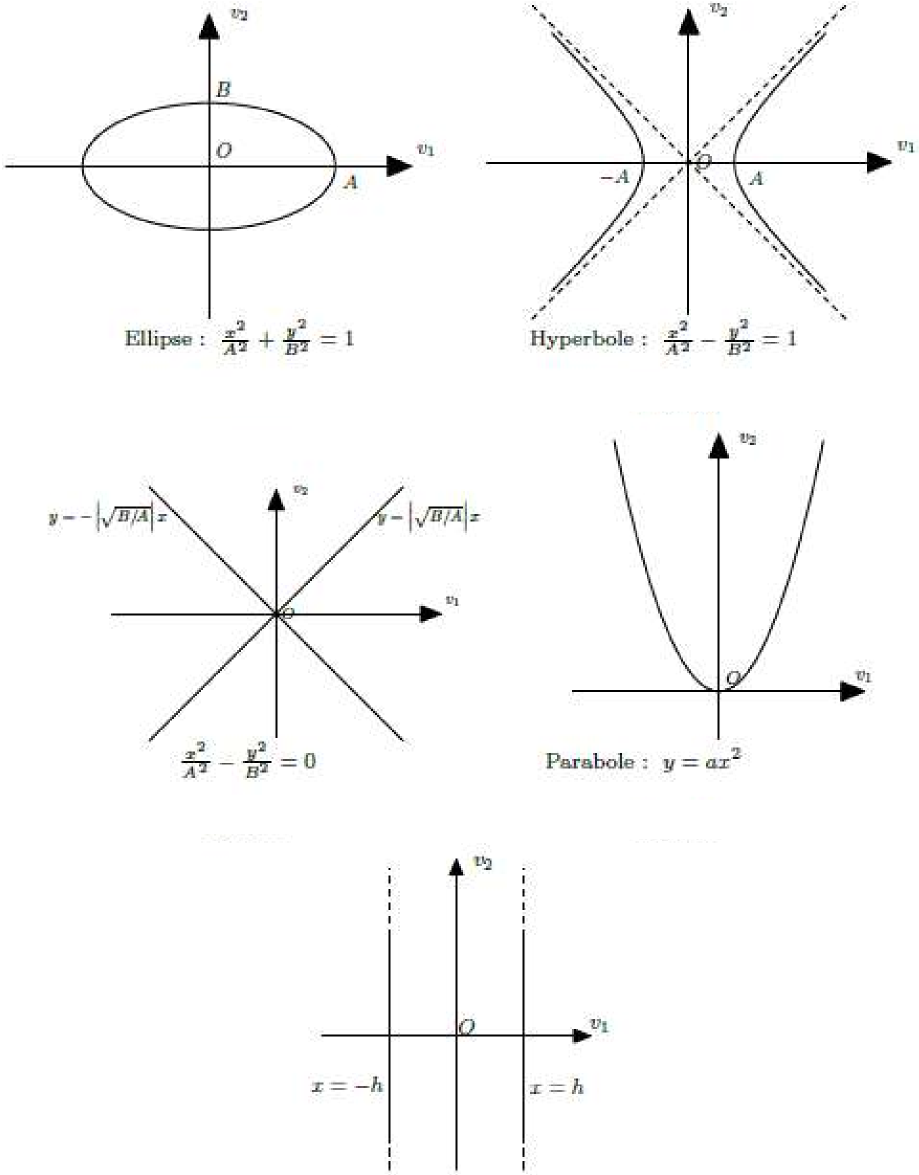

Figure 3