Concours Agrégation, Mathématiques générales

Leçon 70- Formes quadratiques sur un espace vectoriel de dimension finie. Orthogonalité, isotropie. Applications.

Commentaires du jury 2015 : Il faut tout d'abord noter que l'intitulé implique implicitement que le candidat ne doit pas se contenter de travailler sur $\mathbb{R}$. Il faut savoir que les formes quadratiques existent sur le corps des complexes et sur les corps finis et il faut savoir les classifier. On ne doit pas oublier l'interprétation géométrique des notions introduites (lien entre coniques, formes quadratiques, cônes isotropes) ou les aspects élémentaires (par exemple le discriminant de l'équation $ax^2 + bx + c$ et la signature de la forme quadratique $ax^2+bxy+cy^2$). On ne peut se limiter à des considérations élémentaires d'algèbre linéaire. Les formes quadratiques ne sont pas toutes non dégénérées (la notion de quotient est utile pour s'y ramener). L'algorithme de Gauss doit être énoncé et pouvoir être pratiqué sur une forme quadratique de lien avec la signature doit être clairement énoncé. Malheureusement la notion d'isotropie est mal maîtrisée par les candidats, y compris les meilleurs d'entre eux. Le cône isotrope est un aspect important de cette leçon, qu'il faut rattacher à la géométrie différentielle. Il est important d'illustrer cette leçon d'exemples naturels.
Commentaires du jury 2016 : Il faut tout d'abord noter que l'intitulé implique implicitement que le candidat ne doit pas se contenter de travailler sur R. Le candidat pourra parler de la classification des formes quadratiques sur le corps des complexes et sur les corps finis. L'algorithme de Gauss doit être énoncé et pouvoir être pratiqué sur une forme quadratique simple. Les notions d'isotropie et de cône isotrope sont un aspect important de cette leçon. On pourra rattacher cette notion à la géométrie différentielle.

Bibliographie

[F. M. 1] Fresnel J., Matignon M. *Algèbre et Géométrie* (Hermann 2011)
[F. M. 1'] Errata, https ://www.math.u-bordeaux.fr/∼mmatigno/Errata-Alg-Géom.pdf
[F. M. 2] Fresnel J., Matignon M. *Algèbre et Géométrie-81 thèmes pour l'agrégation* (ellipses 2017)
[F. M. 2']Compléments et errata, https ://www.math.u-bordeaux.fr/∼mmatigno/Errata-FM2.pdf
[Fr. A] Fresnel J. *Algèbre des matrices* (Hermann 2011)
[Fr. B-C-D] Fresnel J. *Espaces quadratiques, euclidiens, hermitiens* (Hermann 1999)
[Fr. MMG] Fresnel J. *Méthodes modernes en géométrie* (Hermann 1996, 2010)
et
[A. F. B] Arnaudies J.M., Fraysse H. *Cours de mathématiques Algèbre bilinéaire* (Dunod 1987)

Développements conseillés :

(1) Algorithme de Gauss et existence de bases orthogonales, [Fr. B-C-D] p. 18.

(2) Décomposition en hyperbolique + définie d'un espace quadratique non dégénéré+ indice, [F. M. 1] n° 39 p. 93-96 (voir fichier [F. M. 1]-93-96.pdf)

(3) Classification des formes quadratiques sur les corps finis, [Fr. B-C-D], p. 46

(4) Loi de réciprocité quadratique, [F. M. 1] n°87 la preuve de V.A. Lebesgue p. 248.

(5) Groupe fini dont le groupe dérivé n'est pas l'ensemble des commutateurs, [F. M. 1] n° 80 p 197.

Exercice 1 Sur les combinaisons linéaires de carrés de formes linéaires, [F. M. 1] n°46 p. 106.

Soit E un K-espace vectoriel de dimension finie. Soient $\ell_1, \ell_2, ...\ell_p \in E^\star$, p formes linéaires et $\lambda_1, \lambda_2, ..., \lambda_p$, p éléments de $K - \{0\}$. Soit q la forme quadratique sur E définie par :

$$q(x) := \sum_{i=1}^{p} \lambda_i \ell_i(x)^2.$$

Soit r le rang de q. On se propose de majorer r.

(1) Déterminer la forme bilinéaire symétrique f associée à q (on pourra traiter d'abord le cas $p = 1$).

Preuve. Soit $f(x,y) := \sum_{i=1}^{p} \lambda_i \ell_i(x)\ell_i(y)$, *c'est une forme bilinéaire symétrique et* $f(x,x) = q(x)$.///

(2) On suppose ici que $dim(K\ell_1 + K\ell_2 + ...K\ell_p) = p$. Montrer que $E^\perp = (K\ell_1 + K\ell_2 + ... + K\ell_p)^\circ$ où " $\circ$ " désigne l'orthogonalité pour la dualité. En déduire que $r = p$.

Preuve. On a $E^\perp = \{y \in E \mid \forall x \in E,\ f(x,y) = 0\}$ *c'est à dire que* $\sum_{i=1}^{p} \lambda_i \ell_i(y)\ell_i = 0_{E^\star}$ *et puisque les formes* $\ell_i,\ 1 \leq i \leq p$ *sont linéairement indépendantes il suit que* $\lambda_i \ell_i(y) = 0$ *et donc* $\ell_i(y) = 0$ *pour* $1 \leq i \leq p$. *La réciproque étant évidente il suit que* $E^\perp = (K\ell_1 + K\ell_2 + ... + K\ell_p)^\circ$.///

(3) On suppose maintenant que $(\ell_1, \ell_2, ...\ell_p)$ est une famille quelconque. Montrer que : $E^\perp \supset (K\ell_1 + K\ell_2 + ...K\ell_p)^\circ$. En déduire que $r \leq dim(K\ell_1 + K\ell_2 + ... + K\ell_p)$.

Preuve. L'inclusion $E^\perp \supset (K\ell_1 + K\ell_2 + ...K\ell_p)^\circ$ *est immédiate ainsi* $\dim E - r = \dim E^\perp \geq \dim(K\ell_1 + K\ell_2 + ... + K\ell_p)^\circ = \dim E - \dim(K\ell_1 + K\ell_2 + ... + K\ell_p)$.///

(4) Montrer que $r = p$ si et seulement si $\ell_1, ..., \ell_p$ sont K-linéairement indépendantes.

Preuve. Puisque $\dim(K\ell_1 + K\ell_2 + ... + K\ell_p) \leq p$ *on a l'égalité* $r = p$ *ssi* $\dim(K\ell_1 + K\ell_2 + ... + K\ell_p) = p$ *i.e. ssi* $\ell_1, ..., \ell_p$ *sont* K*-linéairement indépendantes.*///

(5) Pour $p \geq 1$, trouver un exemple avec $r < dim(K\ell_1 + K\ell_2 + ...K\ell_p)$.

Preuve. Soit $q := \ell_1^2 - \ell_2^2$ *avec* $\ell_1 = \ell_2 \neq 0$. *Alors* $q = 0$ *et* $dim(K\ell_1 + K\ell_2) = 1$.///

Exercice 2 Restriction à un sous-espace d'une forme quadratique (rang, indice, signature), [F. M. 1] $n°43$ p. 100.

(1) Soit K un corps de caractéristique $\neq 2$ et (E, f) un K-espace quadratique de dimension finie et F un sous-espace vectoriel de E et f' la restriction à $F \times F$ de la la forme f.

(a) Montrer que $\operatorname{rg} f' \leq \operatorname{rg} f$ où rg. désigne le rang de la forme bilinéaire symétrique.

Preuve.Le rang de f *est le rang de la matrice de* f *dans une base quelconque de* E. *Soit* $B_F := (e_i)_{1 \leq i \leq t}$ *une base de* F *que l'on complète en une base* $B_E := (e_i)_{1 \leq i \leq n}$ *de* E. *Soit* $M(f, B_E)$ *resp.* $M(f', B_F)$ *La matrice de* f *resp.* f' *dans la base* B_E *resp.* B_F. *Par construction* $M(f', B_F)$ *est la matrice principale d'ordre* t *de* $M(f, B_E)$ *et son rang interprété comme le nombre maximal de vecteurs colonnes indépendants est inférieur ou égal au rang de la matrice extraite de* $M(f, B_E)$ *en enlevant les* $n - t + 1$ *dernières colonnes et ce rang est lui-même inférieur ou égal au rang* $M(f, B_E)$.///

(b) On suppose que (E, f) et (F, f') sont non dégénérés. Montrer que $\nu f' \leq \nu f$ où ν. désigne l'indice de la forme bilinéaire symétrique.

Preuve.Puisque (F, f') *est non dégénéré* $\nu f'$ *est égal à la dimension d'un Sous-Espace Totalement Isotrope Maximal. Un tel SETIM est en particulier un SETI pour* (E, f) *et donc de dimension inférieure ou égale à la dimension d'un SETIM de* (E, f).///

(2) Désormais $K = \mathbb{R}$ et (p, q) désigne la signature de f.

(a) Soit F_1, F_2 deux sous-espaces vectoriels de E avec $E = F_1 \overset{\perp}{\bigoplus} F_2$ et $(p_i, q_i),\ i = 1, 2$ la signature de la restriction de la forme bilinéaire symétrique à $F_i \times F_i$. Montrer que $(p, q) = (p_1 + p_2, q_1 + q_2)$.

Preuve.Puisque la signature de f *se lit sur la matrice de* f *dans une BO, on considère* $(e_i, 1 \leq i \leq t)$ *une BO pour* $(F_1, f_{F_1 \times F_1})$ *et* $(e_i, t + 1 \leq i \leq n)$ *une BO pour* $(F_2, f_{F_2 \times F_2})$. *Le nombre de termes* > 0 *sur la diagonale est* $p_1 + p_2$ *et c'est* p *par la loi d'inertie de Sylvester. Idem Le nombre de termes* < 0 *sur la diagonale est* $q_1 + q_2$ *et c'est* q.///

(b) Soit F un sous-espace vectoriel de E et (p', q') la signature de la restriction de la forme bilinéaire symétrique à $F \times F$.

(i) Montrer que F contient un sous-espace vectoriel D de signature $(p', 0)$.

Preuve.Soit f' la restriction de la forme bilinéaire symétrique f à $F \times F$. Par définition de la signature il existe une BO $(e_i, 1 \leq i \leq t)$ de (F, f') avec $p' = \{i \mid f'(e_i, e_i) > 0$, $q' = \{i \mid f'(e_i, e_i) < 0\}$. Ainsi $D :=< e_i >$ avec $f'(e_i, e_i) > 0$ est un sous-espace de F qui est défini positif pour f et de dimension p'.///

(ii) Montrer que $D \cap D^{\perp} = \{0\}$.

Preuve.Par construction l'espace quadratique $(D, f_{|D \times D})$ est défini (positif) et donc non dégénéré ; il suit que $D \cap D^{\perp} = \{0\}$.///

(iii) En déduire que $p' \leq p$.

Preuve.On a donc la décomposition $E = F_1 \bigoplus^{\perp} F_2$ avec $F_1 := D$ et $F_2 := D^{\perp}$. Le résultat suit alors de 2.a).///

(iv) Montrer que $q' \leq q$.

Preuve.Même preuve que précédement en considérant $D' :=< e_i >$ avec $f'(e_i, e_i) < 0$. Alors $(D', f_{|D' \times D'})$ est défini (négatif) et donc non dégénéré et de signature $(0, q')$.///

Exercice 3 Soit $M_2(\mathbb{R})$, l'espace vectoriel des matrices carrées à coefficients réels et $\mathcal{B}$ la base canonique $(E_{i,j})$ où les coefficients de $E_{i,j}$ sont nuls sauf celui à la position (i, j) qui vaut 1. On considère l'application $q : M_2(\mathbb{R}) \to \mathbb{R}$ définie par $q(M) = \det M$.

(1) Montrer que q est une forme quadratique (on pourra exprimer q dans la base $\mathcal{B} = (E_{1,1}, E_{2,2}, E_{1,2}, E_{2,1})$).

Preuve. Si $M = X_{1,1}E_{1,1} + X_{2,2}E_{2,2} + X_{1,2}E_{1,2} + X_{2,1}E_{2,1}$ alors $q(M) = X_{1,1}X_{2,2} - X_{1,2}X_{2,1}$ est une fonction polynôme homogène de degré 2 en les coordonnées de M dans la base $\mathcal{B}$. ///

(2) Ecrire la matrice de la forme bilinéaire associée dans la base $\mathcal{B}$.

Preuve. Si $M' := X'_{1,1}E_{1,1} + X'_{2,2}E_{2,2} + X'_{1,2}E_{1,2} + X'_{2,1}E_{2,1}$ alors $f(M, M') := \frac{1}{2}(X_{1,1}X'_{2,2} + X'_{1,1}X_{2,2}) - \frac{1}{2}(X_{1,2}X'_{2,1} + X'_{1,2}X_{2,1})$ est une forme bilinéaire symétrique et $f(M, M) = q(M)$. Alors $Mat(f, \mathcal{B}) := \begin{bmatrix} 0 & \frac{1}{2} & 0 & 0 \\ \frac{1}{2} & 0 & 0 & 0 \\ 0 & 0 & 0 & -\frac{1}{2} \\ 0 & 0 & -\frac{1}{2} & 0 \end{bmatrix} \in M_4(\mathbb{R})$ *. ///*

(3) Quelle est la signature de q ?

Preuve. L'espace quadratique est par construction somme directe orthogonale des plans hyperboliques $(P = \mathbb{R}E_{1,1} + \mathbb{R}E_{2,2}, q_{|P})$ et $(P' = \mathbb{R}E_{1,2} + \mathbb{R}E_{2,1}, q_{|P'})$ c'est un espace hyperbolique donc de signature $(2, 2)$. ///

(4) Quelle est l'indice de q ?

Preuve. On a $2\nu f = 4$ et donc $\nu f = 2$. ///

(5) Soit H un hyperplan de $M_2(\mathbb{R})$, déduire de ce qui précède qu'il existe $M \in H$ avec M inversible.

Preuve. Supposons qu'au contraire H ne rencontre pas les matrices inversibles ainsi $\forall M \in H$ on a $\det M = 0$ et donc $(H, q_{|H})$ est un SETI et donc $3 = \dim H \leq \nu f = 2$ ce qui est absurde.

Remarque. *La même démonstration vaut pour $M_2(K)$ avec K un corps de caractéristique $\neq 2$. Plus généralement on montre en utilisant la réalisation des formes linéaires sur $M_n(K)$ à l'aide de la trace qu'un hyperplan de $M_n(K)$ rencontre les inversibles. ///*

Exercice 4 Le groupe orthogonal des plans hyperbolique et euclidien, d'un plan non dégénéré, [Fr. B-C-D] p. 30-31.

Exercice 5 Cône isotrope, [F. M. 1] $n°137$ Question 1 p. 394.

Exercice 6 Le discriminant d'une forme quadratique, [F. M. 1] $n°51$ p. 128.

Exercice 7 Espace vectoriel de matrices nilpotentes, [Fr. B-C-D] ex. 16.16 p. 56. Pour un traitement avec la dualité voir [Fr. A] p. 163.

Soit K un corps commutatif de caractéristique différente de 2. Soit N un sous-espace vectoriel de $M_n(K)$ constitué de matrices nilpotentes. Soit $f : M_n(K) \times M_n(K) \to K$ définie par $f(A, B) = \operatorname{Tr} AB$.

(1) Montrer brièvement que f est une forme bilinéaire symétrique.

Preuve. Cela découle de la bilinéarité du produit matriciel et de la linéarité de la trace.///

(2) On note $E_{i,j} \in M_n(K)$ avec un 1 en position i, j et des zéros ailleurs. Calculer $f(E_{i,j}, E_{i',j'})$.

Preuve. On a $E_{i,j}E_{i',j'} = \delta_{j,i'}E_{i,j'}$ *et donc* $f(E_{i,j}, E_{i',j'}) = \delta_{j,i'}\delta_{i,j'}$*.///*

(3) Montrer que f est non dégénérée.

Preuve. Soit $A = \sum_{i,j} a_{i,j}E_{i,j} \in M_n(K)^\perp$*. Alors* $0 = f(A, E_{i',j'}) = \sum_{i,j} a_{i,j}\delta_{j,i'}\delta_{i,j'} = a_{j',i'}$ *et ce pour tout* (i', j') *; ainsi* $A = 0$*.///*

(4) Pour $1 \leq i < j \leq n$ on note $P_{i,j} := KE_{i,j} \bigoplus KE_{j,i}$ et $H := \sum_{1\leq i<j\leq n} P_{i,j}$. Montrer que $P_{i,j}$ est un plan hyperbolique et que $H := \sum_{1\leq i<j\leq n} P_{i,j}$ est un espace hyperbolique pour les restrictions respectives de f.

Preuve. Le résultat suit des égalités $f(E_{i,j}, E_{i,j}) = 0$ *pour* $i \neq j$ *et* $f(E_{i,j}, E_{j,i}) = 1$*. La famille* $E_{i,j}, E_{j,i}$ *est donc une base hyperbolique de* $P_{i,j}$*. De plus les plans* $P_{i,j}$ *sont en somme directe orthogonale.///*

(5) Montrer que $\forall N \in N$ on a $\operatorname{Tr} N^2 = 0$ et en déduire que $\forall N, N' \in N$ on a $\operatorname{Tr} NN' = 0$.

Preuve. On remarque que $N + N' \in N$ *et donc* $N + N'$ *est nilpotente et par suite* $(N + N')^2$ *aussi. Puisque la trace d'une matrice nilpotente est nulle il suit que* $2f(N, N') = f(N + N', N + N') - f(N, N) - f(N', N') = 0$*. D'où le résultat puisque car.*$(K) \neq 2$*.///*

(6) En déduire que $\dim N \leq \frac{n^2}{2}$.

Preuve. La question précédente montre que N *est un SETI de l'espace quadratique non dégénéré* $(M_n(\mathbb{R}), f)$ *et donc* $\dim N \leq$ *l'indice de* $f \leq \frac{n^2}{2}$*.///*

(7) En remarquant que $Id \in N^\perp$ montrer que $\dim N \leq \frac{n^2-1}{2}$.

Preuve. On a donc $N \subset N^\perp$ *et* $N \neq N^\perp$ *donc* $\dim N \leq -1 + \dim M_n(K) - \dim N$*.///*

(8) On suppose que $K = \mathbb{R}$. Quelle est la signature de la restriction de f à $D := \bigoplus_{1\leq i\leq n} \mathbb{R}E_{i,i}$? En déduire que $\dim N \leq \frac{n^2-n}{2}$.

Preuve. Puisque $f(E_{i,i}, E_{j,j}) = \delta_{i,j}$ *il suit que* $(E_{i,i}, 1 \leq i \leq n)$ *est une base orthonormale et donc* (D, f) *est euclidien donc de signature* $(n, 0)$*. Puisque* $D = H^\perp$*, il suit que l'indice de* f *est* $\frac{n^2-n}{2}$ *d'où l'inégalité* $\dim N \leq \frac{n^2-n}{2}$*.///*

(9) Exhiber un espace N de dimension $\frac{n^2-n}{2}$.

Preuve. Le sous-espace des matrices triangulaires supérieure avec diagonale nulle convient.///

(10) On note ${}_n(\mathbb{R})$ le sous-espace vectoriel de $M_n(\mathbb{R})$ des matrices symétriques. Montrer que ${}_n(\mathbb{R}) \cap N = \{0\}$. Retrouver ainsi le fait que $\dim N \leq \frac{n^2-n}{2}$.

Preuve. Puisqu'une matrice symétrique réelle est diagonalisable, il suit que ${}_n(\mathbb{R}) \cap N = \{0\}$*. Ainsi* $\dim_n(\mathbb{R}) + \dim N \leq n^2$ *et* $\dim_n(\mathbb{R}) = \frac{n^2-n}{2} + n$*.///*

Exercice 8 Base orthogonale simultanée pour 2 formes bilinéaires symétriques, [A. F. B] p. 115 et [Fr. B-C-D] ex. 10.29 p.150.

Soit K un corps de caractéristique $\neq 2$, E un K espace vectoriel de dimension n. Soit $B := (e_i)_i$ une base de E et f_1, f_2 deux formes bilinéaires symétriques sur E. Soit S_i la matrice de f_i dans la base B. On suppose que f_1 est non dégénérée.

(1) On suppose qu'il existe $B' = (e'_i)$ une base simultanément orthogonale pour f_1, f_2. Montrer que S_1 est inversible et que $S_1^{-1}S_2$ est diagonalisable.

Preuve. Soit $\theta : E \to E^\star$ définie par $\theta(x)(y) = f_1(x,y)$, alors la matrice S_1 est aussi la matrice de l'application linéaire θ de la base B dans la base duale de B. On a $\operatorname{Ker}\theta = E^\perp$ et puisque par définition f_1 est non dégénérée lorsque $E^\perp = \{0\}$, il suit que c'est équivalent au fait que S_1 est inversible. Si P est la matrice de l'identité de la base B' dans la base B alors ${}^tPS_1P =: D_1$ resp. ${}^tPS_2P =: D_2$ est la matrice de f_1 resp. f_2 dans la base B' et puisque c'est une BO pour f_1 et f_2 il suit que D_1, D_2 sont diagonales et $D_1^{-1}D_2 = P^{-1}S_1^{-1}S_2P$ est diagonale. ///

(2) On suppose $D = S_1^{-1}S_2$ diagonalisable. On écrit $E = \bigoplus_{1\leq i\leq s} E_i$ où $E_i = \ker(\tilde{D} - \lambda_i)$ parcourt les sous-espaces propres de l'endomorphisme $\tilde{D}$ induit par D.

(a) Soit $x_i \in E_i$ et $x_j \in E_j$. Montrer que $f_2(x_i, x_j) = \lambda_j f_1(x_i, x_j)$.

Preuve. On écrit $[X_i]$ pour la colonne des coordonnées de x_i dans la base B. Ainsi pour $k = 1, 2$, $f_k(x_i, x_j) = {}^t[X_i]S_k[X_j]$. Par hypothèse $S_1^{-1}S_2[X_j] = \lambda_j[X_j]$ et donc $S_2[X_j] = \lambda_j S_1[X_j]$, alors $f_2(x_i, x_j) = \lambda_j\, {}^t[X_i]S_1[X_j] = \lambda_j f_1(x_i, x_j)$. ///

(b) En déduire que pour $i \neq j$ on a $f_1(x_i, x_j) = f_2(x_i, x_j) = 0$.

Preuve. De même on a $f_2(x_i, x_j) = \lambda_i f_1(x_i, x_j)$ et ainsi $(\lambda_i - \lambda_j)f_1(x_i, x_j) = 0$ et donc si $i \neq j$ on a $f_1(x_i, x_j) = f_2(x_i, x_j) = 0$. ///

(c) Montrer l'existence d'une base simultanément orthogonale pour f_1, f_2.

Preuve. On considère $B'_i = (e'_{i,j}, j \in I_i)$ une BO de E_i pour f_1, alors a) montre que B'_i est une BO de E_i pour f_2. Soit B' la concaténation des famille $B'i$, c'est une BO pour f_1 et f_2 par b). ///

(3) On suppose que (E, f_1) est euclidien.

(a) Montrer qu'il existe $u \in \operatorname{End} E$ avec $f_2(x,y) = f_1(u(x), y) = f_1(x, u(y))$.

Preuve. C'est du cours. L'application linéaire $E \to E^\star$ définie par $x \to f_{1,x}$ où $f_{1,x}(y) = f_1(x,y)$ est bijective. Puisque $f_{2,x} \in E^\star$, il existe un unique $u(x) \in E$ avec $f_2(x,y) = f_1(u(x), y)$. L'unicité de $u(x)$ montre que $u \in \operatorname{End} E$. Enfin $f_2(y,x) = f_1(u(y), x) = f_1(x, u(y))$. ///

(b) Quelle est la matrice de u dans la base B ? Déduire que $S_1^{-1}S_2$ est diagonalisable.

Preuve. On a $f_2(x,y) = {}^t[X]S_2[Y] = {}^t[X][\,{}^tu]_B S_1[Y]$. Ainsi $S_2 = [\,{}^tu]_B S_1$ et donc $S_1^{-1}S_2 = [\,{}^tu]_B$. Par le théorème spectral l'endomorphisme symétrique u est diagonalisable dans un BON de (E, f_1). Remarquons que cette base est une BO simultanée pour f_1 et f_2 ce qui illustre dans ce cas l'équivalence montrée en (1) et (2). ///

Exercice 9 Les groupes $O_{p,q}(\mathbb{R})$, [F. M. 2] p. 105.

Exercice 10 Sous-groupes finis de $GL_n(\mathbb{R})$, [Fr. B-C-D] ex. 10.43 p. 165. et application aux sous-groupes finis de $SO_2(\mathbb{R})$ et de $SL_2(\mathbb{Z})$

Soit Φ une forme bilinéaire symétrique d'un $\mathbb{R}$-espace vectoriel E de dimension n. On note $O(\Phi) := \{u \in GL(E) \mid \forall (x,y) \in E \times E,\ \Phi(u(x), u(y)) = \Phi(x,y)\}$, le groupe orthogonal pour Φ. Soient $u \in GL(E)$ et Φ' la forme bilinéaire symétrique $\Phi \circ u$ (i.e. $\Phi'(x,y) := \Phi(u(x), u(y))$).

(1) Montrer que $O(\Phi') = u^{-1}O(\Phi)u$.

Preuve. On a $O(\Phi') := \{v \in GL(E) \mid \Phi' \circ v = \Phi'\} = \{v \in GL(E) \mid \Phi \circ u \circ v = \Phi \circ u\} =$
$= \{v \in GL(E) \mid \Phi \circ u \circ v \circ u^{-1} = \Phi\} = \{v \in GL(E) \mid u \circ v \circ u^{-1} \in O(\Phi)\} = u^{-1}O(\Phi)u$. ///

(2) Soient Ψ et Ψ' deux formes bilinéaires symétriques sur E de même signature. Montrer qu'il existe $u \in GL(E)$ avec $\Psi' = \Psi \circ u$.

Preuve. Ainsi si (p, q) *est la signature de* Ψ, *il existe une base* $\mathcal{B} = (e_i)$ *orthogonale pour* Ψ *avec* $\Psi(e_i) = 1$ *pour* $i \in I$, $\Psi(e_i) = -1$ *pour* $i \in J$, $\Psi(e_i) = 0$, *pour* $i \notin I \cup J$ *où* $I = p$ *et* $J = q$ *et puisque* Ψ' *a la même signature il existe donc de même une base* $\mathcal{B}' = (e'_i)$ *orthogonale pour* Ψ' *avec* $\Psi(e'_i) = 1$ *pour* $i \in I$, $\Psi(e'_i) = -1$ *pour* $i \in J$, $\Psi(e'_i) = 0$, *pour* $i \notin I \cup J$. *Soit* $u \in \mathrm{GL}(E)$ *avec* $u(e_i) = e'_i$ *pour tout* i. *Par construction les deux formes bilinéaires* Ψ' *et* $\Psi \circ u$ *coïncident sur la base* e_i *; ainsi* $\Psi' = \Psi \circ u$. ///

(3) Soit Φ une forme bilinéaire symétrique définie positive sur E et $G \subset GL(E)$ un sous-groupe fini. Soit $\Phi'(x, y) := \sum_{g \in G} \Phi(g(x), g(y))$ pour $x, y \in E$.

(a) Montrer que Φ' est une forme bilinéaire symétrique définie positive sur E et que $G \subset O(\Phi')$.

Preuve. Puique $\Phi'(x, x) = \sum_{g \in G} \Phi(g(x), g(x)) \geq 0$ *et que* $\Phi'(x, x) = 0$ *implique* $\Phi(x, x) = 0$ *il suit que* Φ' *est une forme bilinéaire symétrique définie positive sur* E. *De plus si* $g' \in G$ *alors* $\Phi'(g'(x), g'(y)) = \sum_{g \in G} \Phi(g(g'(x)), g(g'(y)))$ *et puisque* $g \in G \to gg' \in G$ *est une bijection il suit que* $\Phi' \circ g' = \Phi'$ *et donc* $g' \in O(\Phi')$. ///

(b) En déduire que $G \subset u^{-1}O(\Phi)u$ où $u \in GL(E)$.

Preuve. C'est alors une conséquence de (1). ///

(4) Soit $G \subset GL_n(\mathbb{R})$ un sous-groupe fini. Montrer qu'il existe $P \in GL_n(\mathbb{R})$ avec $G \subset P^{-1}O_n(\mathbb{R})P$.

Preuve. Soit Φ *le produit scalaire canonique sur* $\mathbb{R}^n$ *i.e. la base canonique* $\mathcal{B}$ *est une BON pour* Φ, *alors* $O_n(\mathbb{R})$ *est le sous-groupe de* $\mathrm{GL}_n(\mathbb{R})$ *des* $Mat(v \in O(\Phi), \mathcal{B})$ *et avec les notations précédentes* $\hat{G} \subset u^{-1}O(\Phi)u =$ *où* $\hat{g}$ *est l'endomorphisme induit par* $g \in G$ *et* $u \in GL(E)$ *et donc si* $P := Mat(u, \mathcal{B})$ *alors* $G \subset P^{-1}O_n(\mathbb{R})P$. ///

(5) Soit $G \subset SO_2(\mathbb{R})$ un sous-groupe d'ordre n. Montrer que $G =< R(\frac{2\pi}{n}) >$ où

$$R(\theta) := \begin{bmatrix} cos\theta & -sin\theta \\ sin\theta & cos\theta \end{bmatrix} \text{ pour } \theta \in \mathbb{R}.$$

Preuve. Soit $g \in G$ *alors* $g = R(\theta)$ *et* $g^n = R(n\theta) = Id$. *Il suit que* $R(\theta) \in < R(\frac{2\pi}{n}) >$. *Ainsi* $G \subset < R(\frac{2\pi}{n}) >$ *et avec les cardinaux on a égalité.* ///

(6) Soit $G \subset SL_2(\mathbb{Z})$ un sous-groupe d'ordre n.

(a) Montrer que G est cyclique.

Preuve. En effet puisque $SL_2(\mathbb{Z}) \subset SL_2(\mathbb{R}) \subset GL_2(\mathbb{R})$, *il suit de (4) qu'il existe* $P \in GL_2(\mathbb{R})$ *avec* $G \subset P^{-1}O_2(\mathbb{R})P$ *et puisque* $\det g = 1$ *si* $g \in G$ *on a que* $G \subset P^{-1}SO_2(\mathbb{R})P$ *; ainsi* $G =< P^{-1}R(\frac{2\pi}{n})P >$ *est cyclique d'ordre* n. ///

(b) Montrer que $n \in \{1, 2, 3, 4, 6\}$.

Preuve. On traduit le fait que $P^{-1}R(\frac{2\pi}{n})P \in SL_2(\mathbb{Z})$. *En particulier* $\chi_{R(\frac{2\pi}{n})} = X^2 - 2cos\frac{2\pi}{n}X + 1 \in \mathbb{Z}[X]$ *et donc* $2cos\frac{2\pi}{n} \in \{0, \pm 1, \pm 2\}$ *et donc* $n \in \{1, 2, 3, 4, 6\}$. ///

(c) Exhiber un sous-groupe de $SL_2(\mathbb{Z})$ d'ordre 4 (resp. 6).

Preuve. Il suffit de considérer le groupe engendré par la matrice compagne $C(n)$ *de la matrice compagnon du polynôme* $\chi_{R(\frac{2\pi}{n})}$ *pour* $n \in \{4, 6\}$ *i.e.* $X^2 + 1$ *resp.* $X^2 - X + 1$. *Alors* $C(4)^2 = -Id$ *et donc l'ordre de* $C(4)$ *est* 4 *et* $C(6)^3 = -Id$ *et donc l'ordre de* $C(6)$ *est* 6. ///

(d) Exhiber une infinité de sous-groupes de $SL_2(\mathbb{Z})$ d'ordre 6.

Preuve. Soit $P_m := \begin{bmatrix} 1 & m \\ 0 & 1 \end{bmatrix} \in SL_2(\mathbb{Z})$. *Alors* $P_m^{-1}C(6)P_m = \begin{bmatrix} -m & -1-m(m+1) \\ 1 & m+1 \end{bmatrix}$ *et parmi les groupes* $< \begin{bmatrix} -m & -1-m(m+1) \\ 1 & m+1 \end{bmatrix} >$ *il y en a une infinité puisque l'ensemble des matrices* $\begin{bmatrix} -m & -1-m(m+1) \\ 1 & m+1 \end{bmatrix}$ *est infini. ///*

Exercice 11 Classification des coniques sur un corps fini, [F. M. 1] $n°129$ p. 373, [Fr. MMG] p. 323.
Classification des quadriques affines, [Fr. MMG] p. 300.
Points rationnels sur une conique sur un corps fini, [F. M. 1] $n°131$ question 6 p. 377.
Soit $p > 2$ un nombre premier et $q := p^n$. On note $F(X,Y) := X^2 + Y^2 + 1 \in \mathbb{F}_q[X,Y]$.

(1) (a) Montrer que -1 est un carré dans $\mathbb{F}_q$ ssi $q = 1 \mod 4$.
   (b) Déterminer les couples (p,n) pour lesquels $q = 1 \mod 4$.

(2) Montrer que $\{1 + \mathbb{F}_q^2\} \cap \{-\mathbb{F}_q^2\} \neq \emptyset$. En déduire qu'il existe $(x_0, y_0) \in \mathbb{F}_q \times \mathbb{F}_q$ avec $F(x_0, y_0) = 0$.

(3) On suppose que $q \neq 1 \mod 4$, montrer que $y_0 \neq 0$ et en posant $X = x_0 + X'$ et $Y = y_0 + Y'$ montrer que le nombre de solutions dans $\mathbb{F}_q \times \mathbb{F}_q$ de $F(x,y) = 0$ vaut $q + 1$.

(4) On suppose que $q = 1 \mod 4$, montrer que l'on peut prendre $y_0 = 0$ et en posant $X = x_0 + X'$ et $Y = y_0 + Y'$ montrer que le nombre de solutions dans $\mathbb{F}_q \times \mathbb{F}_q$ de $F(x,y) = 0$ vaut $q - 1$.

Exercice 12 Groupe fini dont le groupe dérivé n'est pas l'ensemble des commutateurs, [F. M. 1] $n°80$ p 197.
Soient k un corps commutatif, car.$k \neq 2$, $A := k[X_1, X_2, X_3, X_4, X_5]$. Alors $A = \bigoplus_{d \geq 0} H_d$, où H_d est le k-espace vectoriel réunion de $\{0\}$ et de l'ensemble des polynômes homogènes de degré d. Soit $\mathcal{M}$ l'idéal de A engendré par $X_i,\ 1 \leq i \leq 5$. On rappelle que si $\mathcal{A}$ et $\mathcal{B}$ sont deux idéaux de A on note $\mathcal{AB}$ l'idéal engendré par les produits ab avec $a \in \mathcal{A}$ et $b \in \mathcal{B}$. Pour $n \in \mathbb{N}^\star$, on note A_n, la k-algèbre $\frac{A}{\mathcal{M}^n}$ et x_i désigne l'image de X_i dans A_n.

(1) Le k-espace vectoriel A_n
   (a) Montrer que $\mathcal{M}$ est un idéal maximal de A et que $\mathcal{M} = \bigoplus_{d \geq 1} H_d$
   (b) Montrer que $\mathcal{M}^2 = \bigoplus_{d \geq 2} H_d$, en déduire que A_2 est un k-espace vectoriel de dimension $1 + 5$ dont une base est $1, x_i, 1 \leq i \leq 5$
   (c) Montrer que $\mathcal{M}^3 = \bigoplus_{d \geq 3} H_d$, en déduire que A_3 est un k-espace vectoriel de dimension $1 + 5 + \frac{5(5+1)}{2}$. dont une base est $1, x_i, 1 \leq i \leq 5, x_i x_j, 1 \leq i \leq j \leq 5$.

(2) L'algèbre A_3. On note $\overline{\mathcal{M}}$ l'image de $\mathcal{M}$ dans A_3.
   (a) Montrer que $\overline{\mathcal{M}}^2$ est le sous-k-espace vectoriel de A_3 suivant $\bigoplus_{1 \leq i \leq j \leq 5} k x_i x_j$.
   (b) Soit $h_1 := \bigoplus_{1 \leq i \leq 5} k x_i$. Montrer que $\overline{\mathcal{M}} = h_1 \bigoplus \overline{\mathcal{M}}^2$.
   (c) On suppose que $q := x_1x_2 + x_3x_4 + x_5^2 \in \overline{\mathcal{M}}^2$ s'écrit aussi $uv + u'v'$ avec $u, v, u', v' \in \overline{\mathcal{M}}$. En écrivant les éléments $a \in \overline{\mathcal{M}}$ sous la forme $h_1(a) + h_2(a)$ avec $h_1(a) \in h_1$ et $h_2(a) \in \overline{\mathcal{M}}^2$, montrer que $q = h_1(u)h_1(v) + h_1(u')h_1(v')$.
   (d) Déduire de ce qui précède qu'il existe $U, V, U', V' \in H_1$ avec $X_1X_2 + X_3X_4 + X_5^2 = UV + U'V'$.
   (e) Quel est le rang de la forme quadratique sur k^5 définie par $X_1X_2 + X_3X_4 + X_5^2$?
   (f) Majorer le rang de la forme quadratique sur k^5 définie par $UV + U'V'$ où $U, V, U', V' \in H_1$?
   (g) Déduire de ce qui précède que l'ensemble $\{ab + a'b' \mid a, a', b, b' \in \overline{\mathcal{M}}\} \neq \overline{\mathcal{M}}^2$.

(3) Application à l'étude de l'ensemble des commutateurs d'un groupe.

Soit $G := \{ \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix} \in \mathrm{GL}_3(A_3) \mid a, b \in \overline{\mathcal{M}}, c \in \overline{\mathcal{M}}^2 \}$. On admet que si $M = \begin{bmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{bmatrix}, M' = \begin{bmatrix} 1 & a' & c' \\ 0 & 1 & b' \\ 0 & 0 & 1 \end{bmatrix}$ sont deux éléments de $\mathrm{GL}_3(A_3)$ le commutateur $MM'M^{-1}M'^{-1} = \begin{bmatrix} 1 & 0 & ab' - a'b \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$.

(a) Montrer que G est un sous-groupe de $\mathrm{GL}_3(A_3)$.

(b) Montrer que le groupe dérivé de G est distinct de l'ensemble des commutateurs de G.

(c) Calculer le cardinal de G lorsque $k = \mathbb{F}_p$.