Soit $\mathbb{K}$ un corps de caractéristique $\neq 2$ et E un $\mathbb{K}$-ev de dimension finie.

I. GÉNÉRALITÉS

1. Lien avec l'algèbre bilinéaire

Déf 1 : soit b une forme bilinéaire sur E. L'application $q_b : \begin{array}{l} E \to \mathbb{K} \\ x \mapsto b(x,x) \end{array}$ est appelée forme quadratique.

Remarque 2 : Une forme quadratique est un polynôme homogène de degré 2 en les coordonnées, dans toute base.

Ex 3 : $q_1(x,y) = 3x^2 + 6xy$, $q_2 = \det$ sur $M_2(\mathbb{R})$, $q_3(A) = \mathrm{Tr}(A^2)$ sur $M_n(\mathbb{K})$ sont des formes quadratiques.

Prop 4 : Soit q une forme quadratique sur E. Il existe une unique forme bilinéaire symétrique, notée b_q, telle que $q(x) = b_q(x,x)$, $\forall x \in E$. On l'appelle forme polaire associée à q.

Ex 5 : $b_1((x,y),(x',y')) = 3xx' + 3xy' + 3x'y$ est la forme polaire de q_1

Prop 6 : (Formule de polarisation) Soit q une forme quadratique sur E et b_q sa forme polaire. On a : $\forall (x,y) \in E^2$, $b(x,y) = \frac{q(x+y) - q(x) - q(y)}{2}$

Rem 6 : $Q(E)$, l'ensemble des formes quadratiques sur E, est un ev isomorphe à $S_2(E)$, l'ensemble des formes bilinéaires symétriques

2. Représentation matricielle

Déf 7 : On appelle matrice associée à q dans $B = (e_1, \dots, e_n)$ une base de E, la matrice $M_B(q) = (b(e_i, e_j))_{i,j}$, où b est la forme polaire de q.

Remarque 8 : $q \in Q(E) \mapsto M_B(q) \in S_n(\mathbb{K})$ est un isomorphisme. On en déduit : $\dim Q(E) = \frac{n(n+1)}{2}$

Rem 9 : Si $A = \mathrm{Mat}_B(q)$ et $X = \mathrm{Mat}_B(x)$ alors $q(x) = {}^tXAX$.

Ex 10 : $M_{B_c}(q_1) = \begin{pmatrix} 3 & 3 \\ 3 & 0 \end{pmatrix}$ où B_c désigne la base canonique de $\mathbb{K}^2$

Prop 11 : Soit B_1 et B_2 deux bases de E et $P = P_{B_1}^{B_2}$ alors $M_{B_2}(q) = {}^tP M_{B_1}(q) P$

Rem 12 : Les matrices représentant une forme quadratique q constituent une classe de congruence dans $S_n(\mathbb{K})$

3. Lien avec la dualité

Soit q une forme quadratique sur E et b sa forme polaire.

Déf 13 : On définit l'application $b_d : \begin{array}{l} E \to E^* \\ y \mapsto b(\cdot, y) \end{array}$

Rem 14 : On note B une base de E et B^* sa base duale alors $M_B(q) = M_{B,B^*}(b_d)$

Déf 15 : On définit le noyau de q par $\mathrm{Ker}\, q := \mathrm{Ker}(b_d)$ et le rang de q par $\mathrm{rg}(q) := \mathrm{rg}(b_d)$

Ex 16 : $q_4(x,y,z) = x^2 - 2y^2 + 3z^2 + 4xy + 6xz$, $\mathrm{Ker}\, q = \mathrm{Vect}((1,1,-1))$, $\mathrm{rg}(q) = 2$.

Déf 17 : On dit que q est non dégénérée si $\mathrm{Ker}(q) = \{0\}$. Dans le cas contraire, on dit que q est dégénérée.

Ex 18 : q_1 et q_3 sont non dégénérées mais q_4 est dégénérée.

Prop 19 : Si q est non dégénérée, b_d est un isomorphisme entre E et E^*

App 20 : définition du gradient et du produit vectoriel.

Déf 21 : Lorsque q est non dégénérée, on appelle déterminant de q tout déterminant d'une matrice de $S_n(\mathbb{K})$ représentant q. La classe d'équivalence des déterminants de q dans $\mathbb{K}^*/\mathbb{K}^{*2}$ est appelée le discriminant de q et noté $\det(q)$.

Ex 22 : un déterminant de q_1 est -9, donc $\det(q) = -1$.

Déf 23 : On appelle partie régulière de q, la forme quadratique non dégénérée $\bar{q}$ de forme polaire $\bar{b} : (\bar{x}, \bar{y}) \in E/\mathrm{Ker}\, q \times E/\mathrm{Ker}\, q \mapsto b(x,y)$. On appelle discriminant de q, le discriminant de $\bar{q}$.

II. ORTHOGONALITÉ ET ISOTROPIE

1. Orthogonalité

Déf 24 : Soient $x, y \in E$. On dit que x et y sont orthogonaux si $b(x,y) = 0$. Si $A, B \in \mathcal{P}(E)$, on dit que A et B sont orthogonales si $\forall (x,y) \in A \times B$, $b(x,y) = 0$.

Déf 25 : Soit $A \subset E$, on définit $A^\perp = \{x \in E, \forall a \in A, b(x,a) = 0\}$.

Prop 26 : Si $A \subset E$ est un sev alors $\dim A^\perp + \dim A \geq \dim E$. Si de plus q est non dégénérée alors $\dim A^\perp + \dim A = \dim E$

Rem 27 : On n'a pas nécessairement $A^\perp \oplus A = E$

Contre-exemple 28 : $q_5(x,y) = x^2 - y^2$ et $A = \mathrm{vect}((1,1))$.

2. Isotropie

Déf 28 : On définit le cône isotrope de q par $C(q) = \{x \in E, q(x)\}$.

- $x \in E$ est dit isotrope si $x \in C(q)$. Sinon, x est dit anisotrope.
- q est dit isotrope si $C(q) \neq \{0\}$. Sinon, q est dit anisotrope.

Remarque 29 : En général, $C(q)$ n'est pas un e.v. Cependant, $C(q)$ est stable par homothétie : c'est un cône.

Prop 30 : On a : $\mathrm{Ker}(q) \subset C(q)$.

Rem 31 : L'inclusion est stricte, en général. Si $q(x,y) = x^2 - y^2$ sur $\mathbb{K}^2$ alors $\mathrm{Ker}\, q = \{0\}$ et $(1,1) \in C(q)$.

Def 32 : Soit $A \subset E$ un sev. On dit que A est isotrope si $A \cap A^{\perp} \neq \{0\}$. Dans le cas contraire, A est dit anisotrope.

Def 33 : Soit $A \subset E$ un sev. On dit que A est totalement isotrope si $A \subset A^{\perp}$

Ex 34 : * $\mathrm{Ker}(q)$ est un sev totalement isotrope.
* Soit $x \in E \setminus \{0\}$. $F = \mathrm{vect}(x)$ est isotrope ssi x est isotrope ssi F est totalement isotrope.

Rem 35 : Un espace qui admet un vecteur isotrope n'est pas forcément isotrope. Si $q(x,y) = x^2 - y^2$, $\mathbb{R}^2$ est non isotrope mais $(1,1)$ est isotrope.

Prop 36 : Si F est totalement isotrope et q non dégénérée alors $\dim F \leq \frac{\dim E}{2}$

Prop 37 : Si $F \subset E$ est non isotrope alors $E = F \oplus F^{\perp}$.

3. Groupe orthogonal.

Def 38 : On appelle groupe orthogonal l'ensemble $O(q) = \{u \in GL(E),\ q \circ u = q\}$

Prop 39 : $O(q)$ est un sous groupe de $GL(E)$.

Ex 40 : Si $a \in E$ est anisotrope alors $s_a : x \mapsto x - 2\frac{b(a,x)}{q(a)} a \in O(q)$.

Ex 41 : Si E est euclidien, $O(E)$ désigne le groupe orthogonal de la norme euclidienne au carré.

Rem 42 : Pour le choix d'une base B de E, $O(q)$ s'identifie à $\{M \in GL_n(\mathbb{K}),\ {}^tMAM = A\}$ où $A = \mathrm{Mat}_B(q)$.

Prop 43 : Pour tout $u \in O(q)$, on a : $\det(u) = \pm 1$. On définit alors $SO(q) = \{u \in O(q),\ \det(u) = 1\}$.

Ex 44 : Si $a \notin C(q)$, $\det(s_a) = -1$.

Def 45 : On note $O(p,q) = \{M \in GL_n(\mathbb{R}),\ {}^tM I_{p,q} M = I_{p,q}\}$ où $I_{p,q} = \begin{pmatrix} I_p & 0 \\ 0 & -I_q \end{pmatrix}$

Prop 46 : On a : $O(p,q) \cong O(p) \times O(q) \times \mathbb{R}^{pq}$

III. CLASSIFICATION DES FORMES QUADRATIQUES

On cherche à classifier les couples (E,q) où q désigne une forme quadratique sur E. Pour cela, on dit que (E,q) est isomorphe à (E',q'), noté $(E,q) \simeq (E',q')$, s'il existe $u : E \to E'$ un isomorphisme tel que $q = q' \circ u$.
Cela revient à décrire les orbites sous l'action par congruence de $GL_n(\mathbb{K})$ sur $S_n(\mathbb{K})$.

Prop 47 : Si $(E,q) \simeq (E',q')$ alors $\mathrm{rg}(q) = \mathrm{rg}(q')$ et $\det(q) = \det(q')$

Prop 48 : Il y a une infinité de classes de congruences dans $S_n(\mathbb{Q})$

1. Réduction sous forme diagonale.

Def 49 : Une famille $(e_1, \dots, e_n)$ de E est dite q-orthogonale si $b(e_i, e_j) = 0\ \forall i \neq j$

Rem 50 : Soit B une base de E. B est orthogonale ssi $M_B(q)$ est diagonale.

Ex 51 : Pour $q(x) = \sum a_i x_i^2$, la base canonique est orthogonale.

THM 52 : Tout espace quadratique (E,q) admet une base orthogonale.

Prop 53 : Algorithme de Gauss

Soit $q(x) = \sum_{1 \leq i \leq n} a_i x_i^2 + \sum_{i<j} b_{i,j} x_i x_j$ une forme quadratique.

* Si $a_1 \neq 0$: alors $q(x) = a_1\left(x_1 + \frac{b_{1,2}}{2a_1} x_2 + \dots + \frac{b_{1,n}}{2a_1} x_n\right)^2 + q_1(x_2, \dots, x_n)$ et on applique l'algorithme à q_1
* Si $a_i = 0, \forall i \in [\![1,n]\!]$, et $b_{1,2} \neq 0$ alors : $q(x) = P_1(x)P_2(x) + q_3(x_3, \dots, x_n)$ où $P_1(x) = b_{1,2}\left(x_1 + \sum_{k=3}^{n} \frac{b_{2,k}}{b_{1,2}} x_k\right)$, $P_2(x) = x_2 + \sum_{k=3}^{n} \frac{b_{1,k}}{b_{1,2}} x_k$.

puis, on écrit $P_1 P_2 = \frac{1}{4}(P_1 + P_2)^2 - \frac{1}{4}(P_1 - P_2)^2$ et on applique l'algorithme à q_3.

* Si $q \neq 0$, on se ramène à un des deux cas précédents par permutation des coordonnées.

Ex 54 : $q_6(x) = x_1^2 + 4x_2^2 + 9x_3^2 + 2x_1x_2 + 6x_2x_3 = (x_1+x_2)^2 + 3(x_2+x_3)^2 + 6x_3^2$

2. Classification sur $\mathbb{C}$ et $\mathbb{R}$.

THM 55 : Toute forme quadratique complexe de dimension n et de rang r est représentée dans une base par la matrice $\begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} \in M_n(\mathbb{C})$.

Corollaire 56 : Deux formes quadratiques complexes de même dimension sont équivalentes ssi elles ont même rang.

THM 57 : Toute forme quadratique réelle est représentée dans une base par une matrice de la forme $\begin{pmatrix} I_p & & \\ & -I_q & \\ & & 0 \end{pmatrix}$ où (p,q) ne dépend pas du choix de base et est appelé signature de q.

Cor 58 : Deux formes quadratiques réelles de même dimension finie sont équivalentes ssi elles ont même signature.

Ex 59 : $q_6(x) = (x_1+x_2)^2 + 3(x_2+x_3)^2 + 6x_3^2$ est de signature $(3,0)$

Ex 60 : q_3 est de signature $\left(\frac{n(n+1)}{2}, \frac{(n-1)n}{2}\right)$.

Def 61 : Une forme quadratique réelle q est dite définie positive si $\forall x \in E \setminus \{0\}$, $q(x) > 0$

DEV Ellipsoïde de John-Lowner FGN Algèbre 3.

Rem 62 : Si q est définie positive alors sa signature est $(n,0)$

THM 63 : Soient q et φ deux formes quadratiques réelles avec φ définie positive. Il existe une base orthonormée pour φ et orthogonale pour q.

Déf 64 : Un ensemble de la forme $\mathcal{E} = \{x \in E, q(x) \leq 1\}$ avec q définie positive est appelé ellipsoïde.

Prop 65 : Soit $K \subset \mathbb{R}^n$ un compact d'intérieur non vide. Il existe un unique ellipsoïde contenant K et de volume minimal.

3. Classification sur les corps finis.

On suppose pour cette partie que $\mathbb{K}$ est un corps fini.

Prop 66 : $\mathrm{Card}(\mathbb{K}^*/(\mathbb{K}^*)^2) = 2$, on note $\mathbb{K}^*/(\mathbb{K}^*)^2 = \{1, \varepsilon\}$.

Prop 67 : Pour tout $a, b \in \mathbb{K}^*$, il existe $x, y \in \mathbb{K}$ tels que $ax^2 + by^2 = 1$.

Prop 68 : Toute forme quadratique non dégénérée est représentée dans une base par une matrice de la forme $\mathrm{diag}(1, \dots, 1, d)$ où $d \in \{1, \varepsilon\}$.

Cor 69 : Deux formes quadratiques de même dimension sont équivalentes ssi elles ont même rang et même discriminant.

DEV

App 70 : Soient p, q deux nombres premiers impairs. On a :
$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ où $\left(\frac{\cdot}{\cdot}\right)$ désigne le symbole de Legendre.

IV. APPLICATIONS.

1. Pour le calcul différentiel.

Prop 71 : Soit $f : U \subset \mathbb{R}^n \to \mathbb{R}^p$ deux fois différentiable. Alors pour tout $a \in U$, $d^2 f(a)$ est une forme bilinéaire symétrique.

Ex 72 : Soit q une forme quadratique réelle de forme polaire b, alors q est deux fois différentiable et $\forall a \in \mathbb{R}^n$, $d^2 q(a) = 2b$.

Rem 73 : La forme quadratique $x \mapsto d^2 f(a)(x,x)$ apparait dans la formule de Taylor à l'ordre 2.

Prop 74 : Soit $f : U \subset \mathbb{R}^n \to \mathbb{R}$ deux fois différentiables et $a \in U$:
* Si f admet un minimum local en a alors $x \mapsto d^2 f(a)(x,x)$ est positive.
* Si $x \mapsto d^2 f(a)(x,x)$ est une forme quadratique définie positive alors f admet en a un minimum local strict.

C-EX 75 : $f : x \mapsto x^3$ est telle que $f''(0) = 0$ mais 0 n'est pas un minimum local.

Prop 76 : Soit $f : U \subset \mathbb{R}^n \to \mathbb{R}$ convexe, où U est ouvert et convexe, et $a \in U$. On suppose f différentiable en a et $df(a) = 0$. Alors f admet un minimum global, sur U, en a.

Prop 77 : Avec les notations précédentes, on suppose f deux fois différentiable. Alors f est convexe sur U ssi $d^2 f$ est une forme quadratique positive en tout point de U.

App 78 : Soit $A \in \mathcal{S}_n^+(\mathbb{R})$. On pose : $\forall x \in \mathbb{R}^n$, $f(x) = \frac{1}{2}\langle Ax, x\rangle - \langle b, x\rangle$ où $b \in \mathbb{R}^n$. Résoudre $Ax = b$ est équivalent à rechercher les points critiques de f ce qui est équivalent à minimiser f car f est convexe.

2. Pour la classification des coniques.

Dans cette partie $E = \mathbb{R}^2$ et $\mathbb{K} = \mathbb{R}$.

Déf 79 : On appelle conique l'ensemble $\mathcal{C} = \{v \in \mathbb{R}^2, q(v) + \ell(v) = k\}$ où q est une forme quadratique non nulle, ℓ une forme linéaire sur $\mathbb{R}^2$ et $k \in \mathbb{R}$.

THM 80 : Soit $\mathcal{C}$ une conique définie par l'équation $q(v) + \ell(v) = k$. On suppose que $\mathcal{C}$ est non vide et non réduit à un point. Alors :
* Si la signature de q est $(2,0)$ alors $\mathcal{C}$ est une ellipse.
* Si la signature de q est $(1,1)$ alors $\mathcal{C}$ est une hyperbole qui, éventuellement, dégénère en deux droites non parallèles.
* Si la signature de q est $(1,0)$ alors $\mathcal{C}$ est une parabole qui dégénère en une droite ou en deux droites parallèles si la direction principale isotrope est contenue dans $\mathrm{Ker}\,\ell$.

* On ne suppose pas la symétrique dans ~~def~~ def 1

  ↳ c'est grave ?

* Que se passe-t-il en caractéristique ?.

* q non dégénérée, avec cône isotrope $\neq \{0\}$.

  Alors il existe une base de E ~~[illegible]~~ de vecteurs du cône isotrope.

pour $q = \begin{pmatrix} 1 & & \\ & 1 & \\ & & 1 \end{pmatrix}$ sur $\mathbb{C}^3$

$= \begin{pmatrix} 1 & & \\ & 1 & \\ & & -1 \end{pmatrix}$ sur $\mathbb{R}^3$

$= \begin{pmatrix} 1 & & \\ & 1 & \\ & & \varepsilon \end{pmatrix}$ sur $\mathbb{F}_q$,

quels sont les $F \subset E$ non isotropes

[F non isotrope ssi $q_{|F}$ non dégénéré]

quels sont les $x \in E$ non isotropes ?

[x non isotrope ssi $(\mathrm{Vect}\, x)^{\perp}$ non isotrope].

Références : * Clément de Seguins Pazzis, Invitation aux formes quadratiques. [caractéristique 2].

* Joseph Grifone, Algèbre linéaire
* D. Perrin, Cours d'algèbre.
* F. Rouvière, Petit guide de calcul différentiel.

LOI DE RÉCIPROCITÉ QUADRATIQUE

cf CALDERO-GERMONI (⚠ bcp de fautes...

Définition

Pour p nbre premier impair et a un élément de $\mathbb{F}_p$, on définit le symbole de Legendre de a par

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p^* \\ -1 & \text{si } a \text{ n'est pas un carré dans } \mathbb{F}_p^* \\ 0 & \text{si } a = 0 \end{cases}$$

⚠ Le définir sur $\mathbb{Z}$ via $\int$ et en déduire que sur $\mathbb{Z}/p\mathbb{Z}$, il vaut $a^{\frac{p-1}{2}}$.

Théorème

Soit p et q deux nbres premiers impairs distincts. Alors

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

preuve:

On va calculer de deux façons différentes le cardinal modulo p de la "sphère" définie sur $\mathbb{F}_q$:

$$X = \left\{ (x_1, \dots, x_p) \in \mathbb{F}_q^p \ , \ \sum_{i=1}^{p} x_i^2 = 1 \right\}.$$

1] On va faire agir le groupe cyclique $\mathbb{Z}/p\mathbb{Z}$ sur X

On fait agir $\mathbb{Z}/p\mathbb{Z}$ sur X par permutation circulaire.

$$\forall k \in \mathbb{Z}/p\mathbb{Z}, \ \forall x = (x_1, \dots, x_p) \in \mathbb{F}_q^p, \quad k \cdot (x_1, \dots, x_p) = (x_{1+k}, \dots, x_{p+k})$$

(avec les indices pris modulo p : $x_{i+p} = x_i \ \forall i$)

D'après la relation orbite-stabilisateur, on a $|\mathrm{Orb}(x)| = \frac{|\mathbb{Z}/p\mathbb{Z}|}{|\mathrm{Stab}(x)|}$

et en particulier, $|\mathrm{Stab}(x)| \mid |\mathbb{Z}/p\mathbb{Z}| = p$ donc comme p est premier, $|\mathrm{Stab}(x)| = 1$ ou $|\mathrm{Stab}(x)| = p$

- $|\mathrm{Stab}(x)| = 1$ ssi $|\mathrm{Orb}(x)| = p$
- $|\mathrm{Stab}(x)| = p$ ssi $\mathrm{Stab}(x) = \mathbb{Z}/p\mathbb{Z}$ (car $\mathrm{Stab}(x) \subset \mathbb{Z}/p\mathbb{Z}$)

ssi $x = (a, \dots, a)$ avec $a \in \mathbb{F}_q$

(⇒ évident ⇐ si $\exists i \neq j$ tq $x_i \neq x_j$ alors la permutation qui envoie x_i sur x_j n'est pas dans le stabilisateur)

ssi $pa^2 = 1$ car $\sum x_i^2 = 1$

Ainsi, comme en choisissant une famille de représentants, les orbites forment une partition de X, on a

$$\begin{aligned}
|X| &= \sum |\mathcal{O}(x)| \\
&= \sum_{x : |\mathrm{Stab}| = 1} \underbrace{|\mathcal{O}(x)|}_{p} + \sum_{x : |\mathrm{Stab}| \neq 1} \underbrace{|\mathcal{O}(x)|}_{=1} \\
&\equiv |\{x \,/\, |\mathrm{Stab}(x)| \neq 1\}| \quad [p] \\
&\equiv |\{a \in \mathbb{F}_q \,/\, pa^2 = 1\}| \quad [p] \\
&\equiv 1 + \left(\tfrac{p}{q}\right) \quad [p]
\end{aligned}$$

car $|\{a \in \mathbb{F}_q \,/\, pa^2 = 1\}| = \begin{cases} 2 & \text{si } p \text{ est un carré dans } \mathbb{F}_q^* \\ 0 & \text{si } p \text{ n'est pas un carré dans } \mathbb{F}_q^* \end{cases}$ (car $a^2 = p^{-1}$)
car q est impair ! (si $p = \alpha^2$ alors $\alpha^2 a^2 = 1$ admet comme solution $a = \alpha^{-1}$ et $a = -\alpha^{-1}$ qui sont bien 2 sol $\neq$ car on est en car $\neq 2$!)

2) On regarde X en terme de formes quadratiques.

On a $X = \{(x_1, \dots, x_p) \in \mathbb{F}_q^p : q(x_1, \dots, x_p) = 1\}$ avec $q(x_1, \dots, x_p) = \sum_{i=1}^{p} x_i^2$.
La matrice de la forme quadratique q dans la base canonique est I_p.

Posons $d = \frac{p-1}{2}$ et $a = (-1)^d$. On regarde la nouvelle forme quadratique
$\tilde{q}(x_1, \dots, x_p) = 2(x_1 x_2 + \dots + x_{p-2} x_{p-1}) + a x_p^2$ et l'ensemble $X' = \{(x_1, \dots, x_p) \in \mathbb{F}_q^p : \tilde{q}(x_1, \dots, x_p) = 1\}$
La matrice de $\tilde{q}$ dans la base canonique de $\mathbb{F}_q^p$ est

$$M = \begin{pmatrix} \begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} & & & \\ & \begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} & & \\ & & \ddots & \\ & & & \begin{smallmatrix} 0 & 1 \\ 1 & 0 \end{smallmatrix} & \\ & & & & a \end{pmatrix} \in \mathcal{M}_p(\mathbb{F}_q)$$

(car la forme bilinéaire associée est
$b((x_1, \dots, x_p), (\tilde{x}_1, \dots, \tilde{x}_p)) = x_1 \tilde{x}_2 + \tilde{x}_1 x_2 + \dots + x_{p-2} \tilde{x}_{p-1} + \tilde{x}_{p-2} x_{p-1} + a x_p \tilde{x}_p$)
(Rmq : pour ce faire, on a besoin de p impair car $M = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ (si $p = 2$) est de dét -1 ...)

Or la classification des formes quadratiques sur un corps fini donne :

> Soit $\mathbb{F}_q$ un corps fini de caractéristique $\neq$ de 2. Soit E un $\mathbb{F}_q$-ev de dim n. Soit $a \in \mathbb{F}_q^*$ qui ne soit pas un carré. Alors il y a deux classes d'équivalence de formes quadratiques non dégénérées sur E. Leur matrice dans une base adaptée est I_n ou $\mathrm{diag}(1, \dots, 1, a)$.

On dét $M = (-1)^{\frac{p-1}{2}} a = 1$ donc dans une base adaptée la matrice de $\tilde{q}$ est I_p. Donc $|X| = |X'|$ car $I_p = {}^tPMP$ pour un certain $P \in GL_p(\mathbb{F}_q)$
donc $x \mapsto Px$ est une bijection $X' \to X$

(*) c'est un hyperplan affine sur $\mathbb{F}_q^d$ qui est un $\mathbb{F}_q$-ev de dim d donc cet hyperplan est de dimension $d-1$ sur $\mathbb{F}_q$ donc contient q^{d-1} points.

Nous allons maintenant calculer $|X|'$

— si $(x_1, x_3, x_5, \dots, x_{p-2}) = 0$, l'équation devient $a x_p^2 = 1$ qui admet $1 + \left(\frac{a}{q}\right)$ solutions. Et il y a q^d possibilités pour $(x_2, \dots, x_{p-1})$ ($x_p \in \mathbb{F}_q$) (aucune contrainte pour eux) d'où $q^d \left(1 + \left(\frac{a}{q}\right)\right)$ possibilités en tout.

— si $(x_1, x_3, \dots, x_{p-2}) \neq 0$

• à $(x_1, \dots, x_{p-2})$ et x_p fixés l'équation devient celle d'un hyperplan affine ($l'\text{ens } \{(x_2, \dots, x_{p-1}) / 2x_1x_2 + \dots + x_{p-2}x_{p-1} = 0\}$ est bien un hyperplan car la forme linéaire $(x_2, \dots, x_{p-1}) \in \mathbb{F}_q^d \to 2x_1x_2 + \dots + x_{p-2}x_{p-1}$) est non nulle car $(x_1, \dots, x_{p-2}) \neq 0$) sur $\mathbb{F}_q^d$ (*) : q^{d-1} choix.

* il y a q choix pour x_p

• et $q^d - 1$ pour $(x_1, \dots, x_{p-2})$ (car $(x_1, \dots, x_{p-2}) \in \mathbb{F}_q^{d*}$)

Ce qui fait au final $q^d(q^d - 1)$ possibilités

Ainsi $|X|' = q^d(q^d - 1) + q^d\left(1 + \left(\frac{a}{q}\right)\right) = q^{2d} + q^d\left(\frac{a}{q}\right) = q^{p-1} + q^d\left(\frac{a}{q}\right)$

3] Conclusion [c'est juste mais faisons une présentation plus succincte]

On a donc

$$1 + \left(\frac{p}{q}\right) = q^{p-1} + q^d\left(\frac{a}{q}\right) \quad \text{mod } p$$

et donc en utilisant le petit thm de Fermat,

$$1 + \left(\frac{p}{q}\right) = 1 + q^d\left(\frac{a}{q}\right) \quad \text{mod } p$$

Or si $a \equiv b$ mod p avec $a, b \in [\![0, 2]\!]$ alors $a = b$ dans $\mathbb{Z}$. En effet, si $a - b = kp$ alors soit $k = 0$ soit $|a-b| \geq p \geq 3$ ↯. Or $\left(\frac{p}{q}\right)$ et $\left(\frac{q}{p}\right)$ valent $0, 1$ ou -1 et $q^d = q^{p-1/2}$ vaut 1 ou -1 donc on est bien dans ce cas là.

On a donc $1 + \left(\frac{p}{q}\right) = 1 + q^d\left(\frac{a}{q}\right)$ dans $\mathbb{Z}$ donc a fortiori dans $\mathbb{F}_q$. Or dans $\mathbb{F}_q$, on a $\left(\frac{a}{q}\right) = a^{q-1/2}$ donc on a

$$\left(\frac{p}{q}\right) = q^d a^{q-1/2} \quad \text{dans } \mathbb{F}_q$$
$$= q^d (-1)^{d\frac{q-1}{2}} \quad \text{dans } \mathbb{F}_q$$

Donc on fait l'égalité est dans $\mathbb{Z}$, donc sur $\mathbb{F}_p$. On sur

car à valeurs dans $[\![0 \dots 2]\!]$

$\mathbb{F}_p$. $\left(\frac{q}{p}\right) = q^{p-1/2}$ donc on a $\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{d\frac{q-1}{2}} = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ sur $\mathbb{F}_p$
et en fait,

$$\left(\frac{p}{q}\right) = \left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} \text{ sur } \mathbb{Z}$$

(car à valeurs dans [0, 2])

Retour sur la définition initiale

Soit p un nombre premier impair et $a \in \mathbb{F}_p^*$.

$$a^{\frac{p-1}{2}} = \begin{cases} 1 & \text{si } a \text{ est un carré dans } \mathbb{F}_p^* \\ -1 & \text{sinon.} \end{cases}$$

En effet, considérons les morphismes de groupe

$$\chi : \begin{array}{l} \mathbb{F}_p^* \to \mathbb{F}_p^* \\ x \mapsto x^2 \end{array}$$

$$\lambda : \begin{array}{l} \mathbb{F}_p^* \to \mathbb{F}_p^* \\ x \mapsto x^{p-1/2} \end{array}$$

D'après le thm de Lagrange $\chi \circ \lambda = \lambda \circ \chi = id$ donc $\lambda(a)^2 = 1$ donc $\lambda(a) = \pm 1$. Il s'agit alors de montrer que $\mathrm{Im}\,\chi = \mathrm{Ker}\,\lambda$.

. On a $\mathrm{Im}\,\chi \subset \mathrm{Ker}\,\lambda$ car $\lambda(\chi(a)) = a^{p-1} = 1$.

. On a $|\mathrm{Im}\,\chi| = |\mathbb{F}_p^*| / |\mathrm{Ker}\,\chi| = \frac{p-1}{2}$ ($|\mathrm{Ker}\,\chi| = 2$ car $-1 \neq 1$ car on est en caractéristique $p \neq 2$)

Et $|\mathrm{Ker}\,\lambda| \leq \frac{p-1}{2}$ car $\mathrm{Ker}\,\lambda \subset \{$racines de $x^{\frac{p-1}{2}} - 1$ sur $\mathbb{F}_p\}$
d'où le résultat

3] Conclusion

On a donc $q^{p-1} + q^d\left(\frac{a}{q}\right) = 1 + \left(\frac{p}{q}\right)$ $[p]$.

Or :

— $q^{d-1} \equiv 1$ $[p]$ par le petit thm de Fermat

vrai car q impair car $1 = -1$ sur $\mathbb{F}_2$ mais pas sur $\mathbb{Z}$

— $\left(\frac{a}{q}\right) = a^{p-1/2} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ sur $\mathbb{F}_q$ donc sur $\mathbb{Z}$ (car a sont tous les deux des entiers appartenant à $\{-1, 1\}$) donc sur $\mathbb{F}_p$.

— $\left(\frac{q}{p}\right) = q^{\frac{p-1}{2}} = q^d$ sur $\mathbb{F}_p$.

Donc on a $\left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \left(\frac{p}{q}\right)$ dans $\mathbb{F}_p$ donc dans $\mathbb{Z}$ par la même remarque. Et comme $\left(\frac{q}{p}\right)^2 = 1$, en multipliant par $\left(\frac{q}{p}\right)$ des 2 côtés, on a le résultat.