150

Exemples d'actions de groupe sur les espaces de matrices.

Soit $\mathbb{K}$ un corps et soient $m, n \in \mathbb{N}^*$.

I) Action de Steinitz

1) Définitions et invariants

Déf. 1 : Notons G le groupe $GL_m(\mathbb{K}) \times GL_n(\mathbb{K})$. L'action de Steinitz désigne l'action :

$$G \times M_{m,n}(\mathbb{K}) \to M_{m,n}(\mathbb{K})$$
$$((P,Q),A) \mapsto PAQ^{-1}$$

Déf. 2 : Deux matrices sont dites équivalentes ssi elles sont dans la même orbite pour cette action.

Motiv. 3 : Deux matrices sont équivalentes ssi elles codent la même application linéaire dans deux paires de bases différentes.

Déf. 4 : Soit $r \leq \min(m,n)$. On note $I_r = \begin{pmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 0 \end{pmatrix}$ la matrice comportant r 1 sur sa diagonale.

Th. 5 (Théorème du rang) : Deux matrices sont équivalentes ssi elles ont le même rang, ssi elles sont équivalentes à I_r où r est le rang d'une des matrices.

Déf. 6 : I_r est la forme normale (ou le représentant naturel) de l'orbite des matrices de rang r.

Corollaire 7 : L'action de Steinitz possède $\min(n,m)+1$ orbites.

App. 8 : Soit $A \in M_{m,n}(\mathbb{K})$. Alors, $rg(A) = rg({}^tA)$.

Prop. 9 : Le pivot de Gauss permet de transformer une matrice de rang r par une succession d'opérations élémentaires sur les lignes et les colonnes en I_r.

Rem. 10 : Le rang est invariant par extension de corps.

Prop. 11 : $Stab_{I_r} = \left\{ \begin{pmatrix} A & B \\ 0 & D \end{pmatrix}, \begin{pmatrix} A & 0 \\ C' & D' \end{pmatrix} \;;\; A \in GL_r(\mathbb{K}), B \in M_{r,n-r}(\mathbb{K}), C' \in M_{m-r,r}(\mathbb{K}), D \in GL_{n-r}(\mathbb{K}), D' \in GL_{m-r}(\mathbb{K}) \right\}$

Ainsi, si $\mathbb{K} = \mathbb{F}_q$, $|Stab_{I_r}| = |GL_r(\mathbb{F}_q)| \times |GL_{n-r}(\mathbb{F}_q)| \times |GL_{m-r}(\mathbb{F}_q)| \times |M_{r,n-r}(\mathbb{F}_q)| \times |M_{m-r,r}(\mathbb{F}_q)|$

Cor. 12 : Si $\mathbb{K} = \mathbb{F}_q$, $|O_r| = \dfrac{|M_{m,n}(\mathbb{F}_q)|}{|Stab_{I_r}|} = \dfrac{\prod_{i=0}^{m-1}(q^n - q^i)}{\prod_{i=0}^{r-1}(q^r - q^i)\prod_{i=0}^{m-r-1}(q^{n-r}-q^i)} = \prod_{i=0}^{r-1}(q^n - q^i)\prod_{i=0}^{m-r-1}(q^{n-r}-q^i)\,q^{-a_{m,n,r}}$

où $a_{m,n,r} = \frac{1}{2}\left((m-r)(m-r-1) + (n-r)(n-r-1)\right)$

2) Topologie

Ici, $\mathbb{K} = \mathbb{R}$ ou $\mathbb{C}$.

Prop. 13 : $\overline{O_r} = \bigcup_{0 \leq k \leq r} O_k$. Le rang est semi-continu inférieurement.

Cor. 14 : O_0 est l'unique orbite fermée.

Prop. 15 : $GL_n(\mathbb{K})$ est un ouvert dense de $M_n(\mathbb{K})$.

Prop. 16 : $O_n(\mathbb{R})$ est connexe par arcs.

App. 17 : $O_n(\mathbb{C})$ est connexe par arcs.

II - Action par conjugaison.

1) Définitions et invariants partiels

Déf. 18 : L'action par conjugaison désigne l'action

$$GL_n(\mathbb{K}) \times M_n(\mathbb{K}), \quad (P,A) \mapsto PAP^{-1}$$

Déf 19 : Deux matrices sont dites semblables si elles sont dans la même orbite pour cette action.

Motiv. 20 : Deux matrices sont semblables ssi elles codent la même application linéaire dans deux bases différentes.

Prop. 21 : Le déterminant, la trace, le rang et les polynômes caractéristiques et minimaux sont des invariants partiels.

Rem. 22 : les matrices $\begin{pmatrix} 0&1&0&0 \\ 0&0&0&0 \\ 0&0&0&1 \\ 0&0&0&0 \end{pmatrix}$ et $\begin{pmatrix} 0&1&0&0 \\ 0&0&0&0 \\ 0&0&0&0 \\ 0&0&1&0 \end{pmatrix}$ ont le même polynôme caractéristique X^4

et le même polynôme minimal X^2 mais ne sont pas semblables

Rem. 23 : L'orbite d'une matrice n'est jamais ouverte

Prop. 24 : Deux matrices de $M_n(\mathbb{R})$ sont semblables sur $\mathbb{R}$ si elles sont semblables sur $\mathbb{C}$.

2) Action par conjugaison sur les matrices diagonalisables.

Déf. 25 : $D_n(\mathbb{K})$ désigne l'ensemble des matrices diagonalisables de $M_n(\mathbb{K})$

Prop. 26 : $GL_n(\mathbb{K})$ agit bien par conjugaison sur $D_n(\mathbb{K})$.

Th. 27 : $\frac{D_n(\mathbb{K})}{GL_n(\mathbb{K})}$ est en bijection avec $\frac{\mathbb{K}^n}{S_n}$; chaque orbite est associée au spectre (avec multiplicité) de l'un de ses représentants.

Prop. 28 : Le polynôme caractéristique est un invariant total.

Rem. 29 : Le polynôme minimal ne l'est pas.

Prop. 30 : A diagonalisable $\Leftrightarrow O_A$ est fermée.

Prop. 31 : Si $A \in M_n(\mathbb{R})$, $O_{GL_n(\mathbb{R}),A} \cap M_n(\mathbb{R}) = O_{A,\mathbb{R}}$.

3) Action par conjugaison sur les matrices nilpotentes.

Déf. 32 : $\mathcal{N}_n(\mathbb{K})$ désigne l'ensemble des matrices nilpotentes de $M_n(\mathbb{K})$.

Prop. 33 (Lemme des noyaux itérés) : Soit $A \in \mathcal{N}_n(\mathbb{K})$ et notons $k_i = \dim(\ker A^i)$.
Alors, $\forall i \in [\![1, n]\!]$, $0 \leq k_{i+1} - k_i \leq k_i - k_{i-1}$.

Rem. 34 : Pour tout entier i, la dimension du noyau de A^i ne dépend que de l'orbite de A pour la conjugaison.

Déf. 35 : Pour toute orbite $\mathcal{O}$, on appelle partition associée à $\mathcal{O}$ la partition des $k_i - k_{i-1}$, $i \in \mathbb{N}^*$, où A est un élément quelconque de $\mathcal{O}$

Déf. 36 : On appelle diagramme de Young associé à $\mathcal{O}$ le diagramme de Young de la partition associée à $\mathcal{O}$ et on le note $Y(\mathcal{O})$.

Déf. 37 : Soit $p \in \mathbb{N}^*$. On appelle bloc de Jordan de taille p la matrice $\begin{pmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{pmatrix} \in M_p(\mathbb{K})$. On appelle réduite de Jordan toute matrice diagonale par blocs dont les blocs diagonaux sont des blocs de Jordan de taille décroissante

Prop. 38 : Soit $A \in \mathcal{N}_n(\mathbb{K})$. Il existe une réduite de Jordan semblable à A.

Th. 39 : Le diagramme de Young est un invariant total.

Cor 40 : Le nombre d'orbites est égal au nombre de partitions de n.

Prop. 41 : $\mathrm{Stab}_{S_n}(\sigma) = \{P^{-1}\Sigma_\sigma P, P \in GL_n(\mathbb{C})\}$.

Déf. 42 : Soient Y et Y' deux diagrammes de Young de taille n associés aux partitions λ et λ'. On dit que $Y \leq Y'$ si : $\lambda_1 \leq \lambda'_1$, $\lambda_1 + \lambda_2 \leq \lambda'_1 + \lambda'_2$, ... $\lambda_1 + \dots + \lambda_n = \lambda'_1 + \dots + \lambda'_n$.

Th. 43 : Soit $A \in \mathcal{N}_n(\mathbb{C})$. $\overline{O_A} = \bigcup_{Y(B) \leq Y(A)} O_B$.

4) Cas général et application au calcul différentiel

Th. 44 : Soit $A = D + N$ et $A' = D' + N'$ les décompositions de Dunford de deux matrices complexes. Si A est semblable à A', alors D est semblable à D' et N est semblable à N'.
Réciproquement, si D est semblable à D' et si, pour toute valeur propre λ de A, on a $Y(N, \lambda) = Y(N', \lambda)$, alors A est semblable à A' (où N_λ désigne la restriction de N au sous-espace caractéristique de λ).

Déf. 45 : On note par $SO_3(\mathbb{C})$ l'ensemble des matrices $P \in M_3(\mathbb{C})$ de déterminant 1 telles que $P^t P = I$.

Th. 46 : On a l'isomorphisme suivant :
$PSL_2(\mathbb{C}) \simeq SO_3(\mathbb{C})$] Dév. 1

III - Action par congruence

On suppose que $\mathrm{car}(K) \neq 2$ pour le reste de la leçon.

1) Matrices congruentes et invariants

Déf. 47 : L'action par congruence désigne l'action

$$GL_n(K) \times \mathcal{M}_n(K) \to \mathcal{S}_n(K), \quad (P, A) \mapsto PA^tP$$

Déf. 48 : Deux matrices symétriques sont dites congruentes si elles appartiennent à la même orbite pour cette action.

Motiv. 49 : Deux matrices symétriques sont congruentes si elles représentent la même forme bilinéaire dans deux bases différentes.

Prop. 50 : Toute matrice symétrique est congruente à une matrice diagonale. On peut l'obtenir grâce à la réduction de Gauss.

Rem. 51 : Elle n'est pas unique même à permutation près :

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \equiv \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$$

Th. 52 : Deux matrices symétriques complexes sont congruentes ssi elles ont le même rang.

Déf. 53 : Soit q une forme quadratique réelle. On définit $p'(q)$ par $p(q) := \max\{\dim F, F \text{ s.e.v. de } E, q_{|F} \text{ est définie positive}\}$.

On appelle signature de q le couple $(p(q), t(q))$ où $t(q) = p(-q)$.

Th. 54 (Loi d'inertie de Sylvester) : Soient $A, A' \in \mathcal{S}_n(\mathbb{R})$. Alors A et A' sont congruentes ssi A et A' ont la même signature, ssi elles sont congruentes à $\begin{pmatrix} I_p & & \\ & -I_t & \\ & & 0 \end{pmatrix}$ où (p,t) est la signature de l'une des matrices.

Prop. 55 : $GL_n(\mathbb{R}) \cap (GL_n(\mathbb{C}) \cdot J_n) = \bigcup_{p+q=n} GL_n(\mathbb{R}) \cdot I_{p,q}$.

2) Action par congruence sur les corps finis.

Th. 56 : Soient $A, A' \in \mathcal{S}_n(\mathbb{F}_q) \cap GL_n(\mathbb{F}_q)$. Alors A et A' sont congruentes si elles ont le même discriminant.

Prop. 57 : Soit $a \in \mathbb{F}_q^*$. $a^{\frac{q-1}{2}} = \begin{cases} 1 \text{ si } a \text{ est un carré de } \mathbb{F}_q^* \\ -1 \text{ sinon.} \end{cases}$

De plus, il y a $\frac{q-1}{2}$ carrés dans $\mathbb{F}_q$ et $\frac{q-1}{2}$ non carrés.

Prop. 58 : L'équation $ax^2 + by^2 = 1$ où $a, b \neq 0$ admet au moins une solution dans $\mathbb{F}_q \times \mathbb{F}_q$.

Th. 59 : L'action sur $GL_n(\mathbb{F}_q) \cap \mathcal{S}_n(\mathbb{F}_q)$ possède deux orbites ; $\begin{pmatrix} 1 & & \\ & \ddots & \\ & & 1 \end{pmatrix}$ et $\begin{pmatrix} 1 & & \\ & \ddots & \\ & & \eta \end{pmatrix}$ sont les formes normales, où η est un non carré de $\mathbb{F}_q$.

Prop. 60 (loi de réciprocité quadratique) : Soient p et q deux nombres premiers impairs distincts. Alors, $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ [DV. 2]

où $\left(\frac{p}{q}\right) = p^{\frac{q-1}{2}}$ est le symbole de Legendre

Prop. 61 : Soit L une extension de degré impair de $\mathbb{F}_q$ et soient $A, B \in \mathcal{S}_n(\mathbb{F}_q)$. Alors, A et B sont congruentes sur $\mathbb{F}_q$ si elles sont congruentes sur L.

Un isomorphisme entre les groupes de Lie $PSL_2(\mathbb{C})$ et $SO_3(\mathbb{C})$ (NH2G2, tome 2)

On commence par le lemme suivant :

Lemme 1 (voir exercice B.3 dans NH2G2, tome 1). *Le sous-groupe $SO_n(\mathbb{C})$ est la composante connexe du neutre dans $O_n(\mathbb{C})$*

Démonstration. Nous allons en fait montrer, à l'aide de la décomposition polaire, que $O_n(\mathbb{C}) \cong O_n(\mathbb{R}) \times \mathbb{R}^{n(n-1)/2}$. Soit $M \in O_n(\mathbb{C})$ et $M = UH$ sa décomposition polaire, avec U unitaire et H hermitienne définie positive. Il vient

$$I_n = {}^t MM = {}^t H {}^t UUH = \overline{HU^{-1}}UH$$

Donc $\overline{UH^{-1}} = UH$. Par unicité de la décomposition polaire, on a $\overline{U} = U$ et $\overline{H^{-1}} = H$. Ainsi $U \in O_n(\mathbb{R})$ et en écrivant $H = exp(B)$, avec B hermitienne (l'exponentielle réalise un homéomorphisme de $\mathcal{H}_n$ vers $\mathcal{H}_n^{++}$), il vient

$$exp(\overline{B}) = \overline{exp(B)} = exp(B)^{-1} = exp(-B)$$

donc $\overline{B} = -B$. Ainsi on vérifie que H s'écrit de manière unique sous la forme $exp(iA)$, où A est une matrice antisymétrique réelle.
Récirpoquement, il reste à vérifier que toute matrice de la forme $Uexp(iA)$, $(U, A) \in O_n(\mathbb{R}) \times A_n(\mathbb{R})$ est bien dans $O_n(\mathbb{C})$:

$${}^t(Uexp(iA)) = {}^t exp(iA) {}^t U = exp(i {}^t A)U^{-1} = exp(-iA)U^{-1} = (Uexp(iA))^{-1}$$

Comme $A_n(\mathbb{R})$ est homéomorphe à $\mathbb{R}^{n(n-1)/2}$, le résultat $O_n(\mathbb{C}) \cong O_n(\mathbb{R}) \times \mathbb{R}^{n(n-1)/2}$ est une conséquence de l'homéomorphisme de la décomposition polaire. Cela prouve que la composante connexe du neutre de $O_n(\mathbb{C})$ est homéomorphe à $SO_n(\mathbb{R}) \times \mathbb{R}^{n(n-1)/2}$, car $\mathbb{R}^{n(n-1)/2}$ est connexe et la composante connexe du neutre dans $O_n(\mathbb{R})$ est le sous-groupe $SO_n(\mathbb{R})$.
Remarquons enfin que $det(M) = det(U)det(H) = det(U)$, car l'égalité $\overline{H^{-1}} = H$ implique que $|det(H)| = 1$, donc $det(H) = 1$ (H est hermitienne définie positive donc de déterminant réel positif).
Ainsi, $SO_n(\mathbb{R}) \times \mathbb{R}^{n(n-1)/2} \cong SO_n(\mathbb{C})$, ce qui termine la preuve du lemme.

□

Passons maintenant à la preuve du théorème.
Le groupe de Lie $SL_2(\mathbb{C})$ agit par conjuguaison sur son espace tangent en l'identité $\mathfrak{sl}_2(\mathbb{C}) = \{H \in M_2(\mathbb{C}) \quad : \quad Tr(H) = 0\}$, définissant ainsi le morphisme suivant :

$$\begin{array}{rccc} \phi & : & SL_2(\mathbb{C}) & \to & GL(\mathfrak{sl}_2(\mathbb{C})) \\ & & P & \mapsto & X \mapsto PXP^{-1} \end{array}$$

Le déterminant étant invariant par l'action de conjuguaison, on a $det(\phi(P)(X)) = det(X)$ pour tout $(X, P) \in \mathfrak{sl}_2(\mathbb{C}) \times SL_2(\mathbb{C})$.
L'ensemble $\mathfrak{sl}_2(\mathbb{C})$ est un espace vectoriel de dimension 3. En effet une matrice complexe de trace nulle s'écrit sous la forme $X = \begin{pmatrix} a & b \\ c & -a \end{pmatrix}$, avec $a, b, c \in \mathbb{C}$. On peut donc identifier $\mathfrak{sl}_2(\mathbb{C})$ à $\mathbb{C}^3$ via l'isomorphisme (qui est aussi un difféomorphisme) $f : \mathfrak{sl}_2(\mathbb{C}) \to \mathbb{C}^3, X \mapsto (a, b, c)$.
On remarque ensuite que $det(X) = -bc - a^2 = (\frac{b-c}{2})^2 - (\frac{b+c}{2})^2 - a^2$, donc le déterminant est

identifié via f à une forme quadratique sur $\mathbb{C}^3$ (la forme quadratique $q = det \circ f^{-1}$) de rang 3. On peut ainsi identifier l'image de ϕ à un sous ensemble de $O(q)$ (cela grâce à l'isomorphisme $\begin{array}{ccc} GL(\mathfrak{sl}_2(\mathbb{C})) & \to & GL(\mathbb{C}^3) \\ g & \mapsto & f \circ g \circ f^{-1} \end{array}$), lui même identifiable à $O_3(\mathbb{C})$ car deux formes quadratiques complexes de même rang sont congruentes (plus précisément, en notant A la matrice symétrique associée à q, on a $rg(A) = 3$ donc il existe $g \in GL_3(\mathbb{C})$ tel que $A = g^t g$. Il s'ensuit donc $O(q) = Stab(A) = Stab(g^t g) = gStab(I_3)g^{-1} = gO_3(\mathbb{C})g^{-1}$).
On écrit donc $\phi(SL_2(\mathbb{C})) \subset O_3(\mathbb{C})$. De plus, comme ϕ est continue et $SL_2(\mathbb{C})$ est connexe, l'image de ϕ est connexe. Comme $I_3 \in \phi(SL_2(\mathbb{C}))$, il vient finalement grâce au lemme que $\phi(SL_2(\mathbb{C})) \subset O_3(\mathbb{C})_0 = SO_3(\mathbb{C})$.

— Montrons qu'on a en fait $\phi(SL_2(\mathbb{C})) = SO_3(\mathbb{C})$.

On remarque tout d'abord que ϕ est la restriction de l'application $\begin{array}{ccccc} \overline{\phi} & : & GL_2(\mathbb{C}) & \to & GL(\mathfrak{sl}_2(\mathbb{C})) \\ & & P & \mapsto & X \mapsto PXP^{-1} \end{array}$
définie sur l'ouvert $GL_2(\mathbb{C})$ et composée de fractions rationnelles, donc de classe C^1. Ainsi ϕ est bien un morphisme de sous-variétés tel que $d\phi(I) = d\overline{\phi}(I)|_{\mathfrak{sl}_2(\mathbb{C})}$.
Soit $H \in M_2(\mathbb{C})$ de norme suffisamment petite, on a $\overline{\phi}(I+H) = X \mapsto (I+H)X(I+H)^{-1}$.
Or $(I+H)X(I+H)^{-1} = X + HX - XH + o(||H||)$, donc $\overline{\phi}(I+H) = \overline{\phi}(I) + d\overline{\phi}(I).H + o(||H||)$ où $d\overline{\phi}(I).H = X \mapsto HX - XH$. On en déduit que

$$\begin{array}{ccccc} d\phi(I) & : & \mathfrak{sl}_2(\mathbb{C}) & \to & \mathfrak{so}_3(\mathbb{C}) \subset M_3(\mathbb{C}) \cong End(\mathfrak{sl}_2(\mathbb{C})) \\ & & H & \mapsto & X \mapsto HX - XH \end{array}$$

Avec $\mathfrak{so}_3(\mathbb{C}) = o_3(\mathbb{C}) = \{M \in M_3(\mathbb{C}) | M + {}^t M = 0\}$ est l'espace vectoriel de dimension 3 des matrices antisymétriques, où l'égalité des espaces tangents provient du fait que $so_3(\mathbb{C})$ est un ouvert de $o_3(\mathbb{C})$ contenant l'identité.
L'application linéaire $d\phi(I)$ est injective car

$$\begin{aligned} ker(d\phi(I)) &= \{H \in \mathfrak{sl}_2(\mathbb{C}) | HX = XH \quad \forall X \in \mathfrak{sl}_2(\mathbb{C})\} \\ &= \{H \in M_2(C) | tr(H) = 0, H = \lambda I_2\} = \{0\} \end{aligned}$$

Ainsi $d\phi(I)$ est injective entre deux espaces vectoriels de même dimension, donc $d\phi(I)$ est inversible.
Par un corolaire immédiat du théorème d'inversion locale, $\phi(SL_2(\mathbb{C}))$ contient donc un voisinage ouvert non-vide de I_3. Par le principe de translation, $\phi(SL_2(\mathbb{C}))$ est un sous-groupe non-vide ouvert, donc également fermé de $SO_3(\mathbb{C})$. Par connexité, on a bien $\phi(SL_2(\mathbb{C})) = SO_3(\mathbb{C})$.

— Il reste à déterminer le noyau de ϕ. Or P est dans le noyau si et seulement si $XP = PX$ pour tout $X \in \mathfrak{sl}_2(\mathbb{C})$. Cela implique comme précédemment que X est une homotéthie λI_2, et comme $det(X) = 1$ il vient $X = I_2$ ou $X = -I_2$.
Ainsi $PSL_2(\mathbb{C}) = SL_2(\mathbb{C})/\{I_2, -I_2\} \cong SO_3(\mathbb{C})$

Loi de réciprocité quadratique (NH2G2 Tome 1)

Soit p un nombre premier impaire, $\mathbb{F}_p$ le corps à p éléments, et a $\in \mathbb{F}_p$.
On définit le symbole de legendre de a dans $\mathbb{F}_p$ comme suit :

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

Nous allons tout d'abord noter le lemme suivant, très facile à montrer :

Lemme : soit $a \in \mathbb{F}_p^*$. On a :

$$| \{x \in \mathbb{F}_p \ , \ ax^2 = 1\} | = 1 + \left(\frac{a}{p}\right).$$

Passons maintenant au théorème.

Théorème : Loi de réciprocité quadratique
Soit p et q deux nombres premiers impairs distincts. Alors :

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

Démonstration :
Posons l'ensemble suivant :

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

Nous allons calculer le cardinal de cet ensemble de 2 manières différentes.
Faisons agir $\mathbb{Z}/p\mathbb{Z}$ sur X :

$$\begin{array}{ccc} \mathbb{Z}/p\mathbb{Z} \times X & \to & X \\ (k, (x_1, ..., x_p)) & \mapsto & (x_{1+k}, ..., x_{p+k}) \end{array}$$

où les indices sont vus modulo p : $x_{l+p} = x_l \ \forall l$
et écrivons :

$$|X| = \sum |\mathcal{O}_x| = \sum \frac{|\mathbb{Z}/p\mathbb{Z}|}{|Stab_x|}$$

où la première somme est une somme de cardinaux d'orbites distinctes.
Remarquons ensuite que $Stab_x$ est un sous-groupe de $\mathbb{Z}/p\mathbb{Z}$, donc par Lagrange, puisque p

est premier, $Stab_x = \{0\}$ ou $Stab_x = \mathbb{Z}/p\mathbb{Z}$.

Notre formule devient :

$$\begin{aligned} |X| &= \sum_{Stab_x=\{0\}} \frac{|\mathbb{Z}/p\mathbb{Z}|}{|\{0\}|} + \sum_{Stab_x=\mathbb{Z}/p\mathbb{Z}} \frac{|\mathbb{Z}/p\mathbb{Z}|}{|\mathbb{Z}/p\mathbb{Z}|} \\ &= \sum_{Stab_x=\{0\}} p + \sum_{Stab_x=\mathbb{Z}/p\mathbb{Z}} 1 \end{aligned}$$

Comptons maintenant le nombre d'éléments de X tel que $Stab_x = \mathbb{Z}/p\mathbb{Z}$.
Un tel élément vérifie $(x_1, ..., x_p) = (x_{1+k}, ..., x_{p+k})\ \forall k \in \mathbb{Z}/p\mathbb{Z}$. Il est alors aisé de vérifier que tous les x_i sont égaux et que donc notre élément s'écrit, par exemple, $(x_1, ..., x_1)$. Par définition de l'ensemble X, $px_1^2 = 1$. Le nombre d'élément de X vérifiant $Stab_x = \mathbb{Z}/p\mathbb{Z}$ est donc le nombre de solutions de l'équation $px^2 = 1$, c'est donc $1+\left(\frac{p}{q}\right)$ par le lemme.

Nous avons donc montré :

$$|X| = 1 + \left(\frac{p}{q}\right) \ mod\, p \tag{1}$$

Passons à la deuxième façon de calculer $|X|$.
Pour simplifier les notations, écrivons $d = \frac{p-1}{2}$ et $a = (-1)^d$.
Posons à présent la matrice suivante :

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

On remarque que $det(A) = (-1)^{\frac{p-1}{2}} a = 1 = det(I_p)$. Puisque A et I_p sont symétriques et de même déterminant (donc de même discriminant), elles sont congruentes par l'invariance totale du discriminant dans $\mathbb{F}_q$.
Soit donc $P \in GL_p(\mathbb{F}_q)$ tel que $A = {}^tPI_pP = {}^tPP$.

Nous avons une bijection entre $X = \{u \in \mathbb{F}_q^p\,,\ {}^t uu = 1\}$ et $X' = \{u \in \mathbb{F}_q^p\,,\ {}^t(Pu)Pu = 1\}$ (puisque $u \mapsto Pu$ est une bijection). De plus,

$$\begin{aligned} X' &= \{u \in \mathbb{F}_q^p\,,\ {}^t uAu = 1\} \\ &= \{(y_1, z_1, y_2, z_2, ..., y_d, z_d, t) \in \mathbb{F}_q^p\,,\ 2(y_1z_1 + ... + y_dz_d) + at^2 = 1\}. \end{aligned}$$

Comptons le nombre d'éléments de X' :

Cas 1 : $y_1 = ... = y_d = 0$.
Dans ce cas, nous pouvons choisir les z_i librement dans $\mathbb{F}_q$, ce qui donne q^d possibilités, puis il faut choisir t dans $\mathbb{F}_q$ tel que $at^2 = 1$: il y a $1+\left(\frac{a}{q}\right)$ possibilités d'après le lemme. Nous avons donc en tout $q^d(1 + \left(\frac{a}{q}\right))$ éléments.

Cas 2 : $\exists\, y_i \neq 0$.
Nous choisissons librement les y_i dans $\mathbb{F}_q$ en excluant $(0, ..., 0)$: $q^d - 1$ possibilités. Le choix de t dans $\mathbb{F}_q$ donne q possibilités. Il reste à choisir les z_i dans $\mathbb{F}_q$ vérifiant l'équation $2(y_1z_1 + ... + y_dz_d) + at^2 = 1$: il y a q^{d-1} possibilités, puisqu'après avoir choisi les $d-1$ premiers, le dernier est entièrement déterminé par l'équation. En tout, $(q^d-1)qq^{d-1} = (q^d-1)q^d$ éléments.

En sommant les deux cas possibles, on obtient :

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

Les équations (1) et (2) fournissent l'égalité suivante :

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

On remarque ensuite que $q^d = q^{\frac{p-1}{2}} = \left(\frac{q}{p}\right)$ et que $\left(\frac{a}{q}\right) = a^{\frac{q-1}{2}} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.
En remplaçant et en développant l'équation, on obtient :

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

et donc :

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

puisque $\left(\frac{q}{p}\right)\left(\frac{q}{p}\right) = 1$.

Enfin, les deux membres de l'égalité sont égaux à ± 1, donc par l'absurde, s'ils étaient différents, on obtiendrait $2 = 0\ mod\ p$, ce qui est impossible puisque p est strictement supérieur à 2.
L'égalité est donc vraie sur $\mathbb{Z}$, ce qui conclut la preuve.

□