Leçon 101: Groupe opérant sur un ensemble. Exemples et applications.

Trinome E: DAVIET Samuel, GIAT Florent, TARDIEU-ROUILLY Claire

References: ROMBALDI, PERRIN, H2G2 (tome 1), CVA.

I Définitions et premières propriétés

Def 1: On dit que le groupe G opère à gauche sur l'ensemble E si on a une application : $G\times E \to E$ $(g,x)\mapsto g.x$ telle que :

$\forall x\in E,\ 1.x = x$

$\forall (g,g',x)\in G^2\times E$ $g.(g'.x) = (gg').x$

Une telle application est aussi appelée action à gauche de G sur E.

Théorème 2: Soit $S(E)$ le groupe des permutations de E. Pour tout $g\in G$, l'application $\varphi(g): E\to E$ est alors une bijection de E sur E, c'est-à-dire $\varphi(g)\in S(E)$. φ est un morphisme de groupe de $(G,.)$ dans $(S(E),\circ)$. Le noyau de ce morphisme φ est le noyau de l'action à gauche de G sur E. Réciproquement, un tel morphisme φ définit une action à gauche de G sur E avec $g.x = \varphi(g)(x)$.

Déf 3: Soit G un groupe opérant sur un ensemble non vide E. $\forall x\in E$, le sous-ensemble : $G.x = \{g.x \mid g\in G\}$ de E est appelé orbite de x sous l'action de G.

Prop 4: La relation $x \sim y$ si et seulement si il existe $g\in G$ tel que $y = g.x$ est une relation d'équivalence sur E et la classe de $x\in E$ pour cette relation est l'orbite de x. Il en résulte que les orbites forment une partition de E.

Def 5: On dit que l'action de G sur E est transitive (resp. simplement transitive) si : $\forall (x,y)\in E^2\ \exists g\in G \mid y = g.x$ (resp. $\forall (x,y)\in E^2,\ \exists ! g\in G \mid y = g.x$).

Dans le cas d'une action transitive ou simplement transitive, il y a une seule orbite.

Def 6: On dit que l'action de G sur E est fidèle si le morphisme de groupes : $\varphi: g\in G \mapsto (\varphi(g): x\mapsto g.x)\in S(E)$ est injectif, ce qui signifie que : $(g\in G, \forall x\in E, g.x = x) \Leftrightarrow (g = 1)$.

Def 7: Soit G un groupe opérant sur un ensemble non vide E. $\forall x\in X$, le sous-ensemble : $G_x = \{g\in G \mid g.x = x\}$ de G est le stabilisateur de x sous l'action de G.

Remarque 8: Les stabilisateurs G_x sont des sous-groupes de G.

Théorème 9: Soit G un groupe agissant sur un ensemble X et soit A un élément de X. On note G_A le stabilisateur de A et $\pi: G\to G/G_A$ la projection canonique et π_A l'application $G\to G.A$, $g\mapsto g.A$. Alors il existe une unique application $\bar{\pi}_A : G/G_A \to G.A$ qui rend commutatif le diagramme :

$$\begin{array}{ccc} G & \xrightarrow{\pi_A} & G.A \\ {\scriptstyle\pi}\downarrow & \nearrow{\scriptstyle\bar{\pi}_A} & \\ G/G_A & & \end{array}$$

L'application $\bar{\pi}_A$ est bijective.

Def 10: Soit G un groupe opérant sur un ensemble E. $\forall g\in G$ le sous-ensemble : $Fix_g := \{x\in E, g.x = x\}$ de E est le fixateur de g sous l'action de G.

Théorème 11: (Formule des classes)

Soit $(G,.)$ un groupe opérant sur un ensemble E. $\forall x\in E$ l'application : $\varphi_x : G/G_x \to G.x$ $\bar{g} = gG_x \mapsto g.x$ est bien définie et bijective.

Dans le cas où G est fini on a : $card(G.x) = [G : G_x] = \frac{card(G)}{card(G_x)}$

Remarque 12: (Équation des classes)

Soit $(G,.)$ un groupe fini opérant sur un ensemble E. En notant $G.x_1,\dots,G.x_r$ toutes les orbites deux à deux distinctes, on a $card(E) = \sum_{i=1}^{r} card(G.x_i) = \sum_{i=1}^{r} \frac{card(G)}{card(G_{x_i})}$

Théorème 13: (Formule de Burnside)

Soit G un groupe fini agissant sur un ensemble fini X. Soit X/G l'ensemble des orbites pour cette action. Alors $|X/G| = \frac{1}{|G|}\sum_{g\in G} |X^g|$ où $X^g = \{x\in X,\ g.x = x\}$ le fixateur de g.

Application 14: On considère le groupe symétrique S_n agissant de façon naturelle sur l'ensemble $A = \{1,\dots,n\}$. On considère la variable aléatoire sur S_n qui associe à $\sigma\in S_n$ son nombre d'invariant X^σ. Quelle est la moyenne et la variance de cette variable ?

Application 15: Si G est un groupe fini d'ordre p^α opérant sur un ensemble fini E de cardinal n, alors l'action admet forcément des points fixes.

II Utilisations des actions de groupes au sein des groupes

Def 16: G agit sur lui-même par translation à gauche :

$(g,h)\in G\times G \to g.h = gh$.

Théorème 17: (Cayley)

L'action de G sur lui-même par translation à gauche est fidèle et G est isomorphe à un sous-groupe de $S(G)$.

Def 18: Un groupe G agit sur lui-même par conjugaison :

$(g,h)\in G\times G \to g.h = ghg^{-1}$

Le morphisme de groupe correspondant de $(G,.)$ dans $(S(G),\circ)$ est noté :

$Int(g) : G\to G$, $h\mapsto ghg^{-1}$. L'image de ce morphisme est le groupe $Int(G)$ des automorphismes intérieurs de G.

Def 19: Le centre (ou commutateur) $Z(G)$ d'un groupe G est la partie de G formée des éléments de G qui commutent à tous les autres éléments de G soit $Z(G) = \{h\in G, \forall g\in G, gh = hg\}$.

Prop 20: $Z(G)$ est le fixateur de G pour l'action de conjugaison.

Def/Prop 21: Soit G un groupe et H un sous groupe de G alors $N(H) = \{g \in G \mid gHg^{-1} = H\}$ est le normalisateur de H et $N(H)$ est le stabilisateur de H pour l'action par conjugaison de G sur l'ensemble de ses sous-groupes.

Def 22: Si $p \geq 2$ est un nombre premier, tout groupe de cardinal p^{α}, où α est un entier naturel non nul, $(G,.)$ est un p-groupe.

Theoreme 23: Pour tout nombre premier p, le centre d'un p-groupe n'est pas réduit à $\{1\}$.

Def 24: Soit G un groupe fini de cardinal n et p un diviseur premier de n. Si $n = p^{\alpha}m$ avec $p \nmid m$ on appelle p-sous-groupe de Sylow de G un sous groupe de G de cardinal p^{α}.

Theoreme 25: (Sylow)
Soit G un groupe fini et p un diviseur premier de $|G|$, alors G contient au moins un p-sous groupe de Sylow.

Lemme 26: Soit G un groupe avec $|G| = n = p^{\alpha}m$, avec $p \nmid m$ et soit H un sous-groupe de G. Soit S un p-Sylow de G. Alors il existe $a \in G$ tel que $aSa^{-1} \cap H$ soit un p-Sylow de H.

Theoreme 27: (Sylow)
Soit G un groupe de cardinal $|G| = p^{\alpha}m$ avec $p \nmid m$ et p premier
1) Si H est un sous groupe de G qui est un p-groupe, il existe un p-Sylow S avec $H \subset S$.
2) Les p-Sylow sont tous conjugués (et donc leur nombre k divise n)
3) On a $k \equiv 1$ mod(p) (donc k divise m)
On notera que l'assertion $k \mid n$ resulte du fait que les p-Sylow forment une orbite sous G.

Dev 2 Application 28: Tout groupe simple d'ordre 60 est isomorphe à A_5

III Actions sur les matrices

Exemple 29: On fait agir $Gl_n(\mathbb{R})$ sur l'ensemble X des sous-espaces vectoriels de $\mathbb{R}^n$ de dimension m : $\varphi: Gl_n \times X \to X$
$(G,F) \mapsto G.F = G(F)$

L'action est transitive et pour la forme normale $F = \langle e_1, \dots, e_m \rangle$ où $\mathcal{E}$ est la base canonique de $\mathbb{R}^n$, le stabilisateur est isomorphe à $Gl_m \times Gl_{n-m} \times \mathbb{R}^{m(n-m)}$.

Def 30: Soit $\mathbb{K}$ un corps. On appelle action de Steinitz l'action qui fait agir $G = Gl_m(\mathbb{K}) \times Gl_n(\mathbb{K})$ sur $M_{m,n}(\mathbb{K})$
$\varphi: G \times M_{m,n}(\mathbb{K}) \to M_{m,n}(\mathbb{K})$
$((P,Q),A) \mapsto (P,Q).A = PAQ^{-1}$

Theoreme 31: (du rang)
Soit $\mathbb{K}$ un corps, m et n deux entiers et soient A et B deux matrices $m \times n$ à coefficients dans $\mathbb{K}$. Alors A et B sont équivalentes si et seulement si elles ont le même rang : $rg\,A = rg\,B$.

Theoreme 32: (du rang - autre formulation)
Deux matrices A et B de $M_{m,n}(\mathbb{K})$ ont la même orbite sous l'action de Steinitz si et seulement si elles ont le même rang : $G.A = G.B \Leftrightarrow rg\,A = rg\,B$.

Prop 33: Soit $\mathbb{K}$ un corps fini, m et n deux entiers et soit $G = Gl_m(\mathbb{K}) \times Gl_n(\mathbb{K})$ et $A \in M_{m,n}(\mathbb{K})$. Alors $|G.A| = \dfrac{|Gl_m(\mathbb{K}) \times Gl_n(\mathbb{K})|}{|G_A|}$

Prop 34: On choisit pour forme normale des orbites pour l'action de Steinitz $J_{r,m,n} = \begin{pmatrix} I_r & 0 \\ 0 & 0 \end{pmatrix} \in M_{m,n}(\mathbb{K})$. Son stabilisateur est le sous groupe de G décrit par :
$$\begin{pmatrix} Gl_r(\mathbb{K}) & M_{r,m-r}(\mathbb{K}) \\ 0 & Gl_{m-r}(\mathbb{K}) \end{pmatrix} \times \begin{pmatrix} Gl_r(\mathbb{K}) & 0 \\ M_{n-r,r}(\mathbb{K}) & Gl_{n-r}(\mathbb{K}) \end{pmatrix}$$

2/3

Prop 35: Soit $\mathbb{K}$ le corps des réels ou des complexes. Soient m et n deux entiers. Pour r entier satisfaisant $0 \leq r \leq \min(m,n)$ on note O_r l'orbite des matrices $m \times n$ de rang r à coefficient dans $\mathbb{K}$. Alors l'adhérence $\overline{O_r}$ de l'orbite est donné par : $\overline{O_r} = \bigcup_{0 \leq k \leq r} O_k$.

Corollaire 36: L'unique orbite fermée est l'orbite de la matrice nulle dite "minimale" $O_0 = \{0\}$.

Def 37: Soit $\mathbb{K}$ un corps et soit n un entier naturel. L'action de congruence est l'action de $GL_n(\mathbb{K})$ sur $S_n(\mathbb{K})$, l'espace des matrices symétriques $n \times n$ définie par : $\forall g \in GL_n(\mathbb{K})$, $\forall A \in S_n(\mathbb{K})$ $g.A = gA\,{}^tg$.
On dit que deux matrices symétriques A et A' de $S_n(\mathbb{K})$ sont congruentes si elles appartiennent à la même orbite pour l'action de congruence.

Prop 38: Soit $\mathbb{K}$ un corps quelconque et q une forme quadratique sur E un espace de dimension finie. Alors E admet une base orthogonale pour q. Dit autrement il existe une base dans laquelle la matrice de q est diagonale.

Théorème 39: (classification des formes quadratiques)

1) Si $\mathbb{K} = \mathbb{C}$ deux matrices $A, A' \in S_n(\mathbb{C})$ sont dans la même orbite si et seulement si elles ont même rang : $Orb(A) = Orb(A') \Leftrightarrow rg\,A = rg\,A'$

2) Si $\mathbb{K} = \mathbb{R}$ deux matrices $A, A' \in S_n(\mathbb{R})$ sont dans la même orbite si et seulement si elles ont la même signature : $Orb(A) = Orb(A') \Leftrightarrow sgn(A) = sgn(A')$

3) Si $\mathbb{K} = \mathbb{F}_q$ est un corps fini de cardinal impair, deux matrices inversibles $A, A' \in S_n(\mathbb{F}_q)$ sont dans la même orbite si et seulement si elles ont le même discriminant : $Orb(A) = Orb(A') \Leftrightarrow \delta(A) = \delta(A')$.

IV Applications

Def 40: Pour p nombre premier impair et a un élément de $\mathbb{F}_p$ on définit le symbol de Legendre de a par $\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}}$
$= \begin{cases} 1 \text{ si } a \text{ est un carré dans } \mathbb{F}_p^* \\ -1 \text{ si } a \text{ n'est pas un carré dans } \mathbb{F}_p^* \\ 0 \text{ si } a = 0. \end{cases}$

Théorème 41: (loi complémentaire)
Soit p un nombre premier impair. Alors :
$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$

Théorème 42: (loi de réciprocité quadratique)
Soit p et q deux nombres premiers impairs distincts. Alors :
$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

Dev

Prop 43: On a les isomorphismes exceptionnels suivants :

1) $GL_2(\mathbb{F}_2) \simeq S_3$

2) $PGL_2(\mathbb{F}_3) \simeq S_4$

n°3

NH_2G_2 p.304. $\boxed{\text{Loi de réciprocité quadratique}}$ Leçon : 101,

<u>Théorème</u> : Soient p et q deux nbres 1[er] impairs distincts.
Alors $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$.

On va calculer de 2 manières différentes $|X|$ où
$$X = \{(x_1,\dots x_p) \in \mathbb{F}_q^p \;/\; \sum_{i=1}^{p} x_i^2 = 1\}.$$

Mais pour commencer, on va montrer un Lemme :

<u>Lemme</u> : Pour $a \in \mathbb{F}_q^*$, le nbre de solut° ds $\mathbb{F}_q$ de $ax^2 = 1$ est $\left(\frac{a}{q}\right)+1$ solutions.

En effet, : * Si a est un carré : $\exists \alpha \in \mathbb{F}_q \;/\; \alpha^2 = a$.
$\Rightarrow x = \alpha^{\pm 1}$ est solution.

(et il n'y en a pas d'autre car on est ds un corps ($\Rightarrow$ anneau intègre) donc un poly. d'ordre 2 a max. 2 racines).

Donc 2 solut°. et $\left(\frac{a}{q}\right)+1 = 1+1 = 2$.

* Si a pas carré on a : $ax^2 = 1 \Rightarrow x^2 = a^{-1}$.
$\Rightarrow a = (x^{-1})^2$ absurde. Donc 0 solut°
et $\left(\frac{a}{q}\right)+1 = -1+1 = 0$.

<u>Rq</u> : On peut faire le lemme : pour $a \in \mathbb{F}_q$, nbre de sol. de $x^2 = a$
c'est tjrs $\left(\frac{a}{q}\right)+1$ mais il faut pour pour le cas $a=0$: $\left(\frac{0}{q}\right) = 0$ et on a bien 1 solut° à $x^2 = 0$.

<u>1[er] calcul de $|X|$</u> :

On fait agir $\mathbb{Z}/p\mathbb{Z}$ sur X : $k.(x_1,\dots x_p) = (x_{1+k},\dots x_{p+k})$ avec les indices vus mod. p.

C'est bien une act° car :
* bien déf : On a tjrs que $\sum_{i=1}^{p} x_i^2 = 1$ donc on a bien $\forall k \in \mathbb{Z}/p\mathbb{Z} : k.x \in X$.
* $0.x = x$
* $k.(k'.x) = (k+k').x$.

et on rappelle la formule des classes : $\forall x \in X : |O_x| = \frac{|G|}{|G_x|} = \frac{|\mathbb{Z}/p\mathbb{Z}|}{|G_x|}$.

On sait que les orbites partitionnent X
Or G_x est un ss-gpe de $\mathbb{Z}/p\mathbb{Z}$ donc par Lagrange $|G_x| \mid p$
$\Rightarrow |G_x| = 1$ ou p $\Rightarrow G_x = \mathbb{Z}/p\mathbb{Z}$ ou $\{0\}$.

Donc on a : $|X| = \sum_{O \in X/\mathbb{Z}/p\mathbb{Z}} |O| = \sum_{O \in X/\mathbb{Z}/p\mathbb{Z}} \frac{|\mathbb{Z}/p\mathbb{Z}|}{|G_x|}$ par la formule des classes. (x représentant de chaque orbite.
$$= \sum_{G_x = \mathbb{Z}/p\mathbb{Z}} \frac{p}{p} + \sum_{G_x = \{0\}} p$$
$$= \sum_{G_x = \mathbb{Z}/p\mathbb{Z}} 1 + \sum_{G_x = \{0\}} p. \quad (*)$$

Quand a-t-on $G_x = \mathbb{Z}/p\mathbb{Z}$?

On a $G_x = \mathbb{Z}/p\mathbb{Z} \Leftrightarrow x = (x_1,\dots x_p) = 1.(x_1,\dots x_p) = (x_2, x_3,\dots x_p, x_1)$.
$= 2.(x_1,\dots x_p) = (x_3, x_4,\dots x_1, x_2)$
$= \dots$
$= (p-1).(x_1,\dots x_p)$.

$\Leftrightarrow x = (x_1,\dots x_1) \;/\; p x_1^2 = 1$. qui a par le lemme : $\left(\frac{p}{q}\right)+1$ solut° ds $\mathbb{F}_q$.

Ainsi, il y a $\left(\frac{p}{q}\right)+1$ $x_1 \in \mathbb{F}_q \;/\; G_x = \mathbb{Z}/p\mathbb{Z}$.

Ainsi, par $(*)$ $|X| = \sum_{G_x = \mathbb{Z}/p\mathbb{Z}} 1 \mod p \Rightarrow \boxed{|X| = \left(\frac{p}{q}\right)+1 \mod p.}$

2ème calcul de $|X|$:

On veut calculer le nbre de pts de $\mathbb{F}_q^p$ / $\overset{\text{forme quadratique}}{Q(x)} = x_1^2+\dots+x_p^2$ vaut 1.

Pour commencer, si on note $\underline{e}$ la base canonique de $\mathbb{F}_q^p$, on a :

$$Mat_{\underline{e}}(Q) = \begin{pmatrix}1 & & 0\\ & \ddots & \\ 0 & & 1\end{pmatrix}_{p\times p} \overset{\text{congrue}}{\sim} \begin{pmatrix} \begin{pmatrix}0&1\\1&0\end{pmatrix} & & & 0\\ & \ddots & & \\ & & \begin{pmatrix}0&1\\1&0\end{pmatrix} & \\ 0 & & & (-1)^{\frac{p-1}{2}}\end{pmatrix}_{p\times p} = Mat_{\mathcal{B}}(Q)$$ pour une certaine base $\mathcal{B}$ de $\mathbb{F}_q^p$.

Ces 2 matrices st bien congrues car $A \equiv B$ avec $A, B \in \mathcal{S}_n(\mathbb{F}_q)$, A, B inversibles
$\Leftrightarrow disc(A) = disc(B)$.

Or ici : $disc\left(\begin{pmatrix}1&0\\0&1\end{pmatrix}\right) = 1$ et $disc\left(\begin{pmatrix}\begin{pmatrix}0&1\\1&0\end{pmatrix} & & 0\\ & \begin{pmatrix}0&1\\1&0\end{pmatrix} & \\ 0 & & (-1)^{\frac{p-1}{2}}\end{pmatrix}\right) = \underbrace{(-1)\times\dots(-1)}_{\frac{p-1}{2}\text{ fois}}\times(-1)^{\frac{p-1}{2}}$ par le det. par bloc

$= (-1)^{p-1} = 1$ car p impair.

On écrit alors Q dans notre nouvelle base $\mathcal{B}$ et on note $\hat{x} = (\hat{x}_1, \hat{y}_1, \dots \hat{x}_{\frac{p-1}{2}}, \hat{y}_{\frac{p-1}{2}}, \hat{z}_p)$ ds la base $\mathcal{B}$:

$$Q(\hat{x}) = 2\hat{x}_1\hat{y}_1 + \dots + 2\hat{x}_{\frac{p-1}{2}}\hat{y}_{\frac{p-1}{2}} + (-1)^{\frac{p-1}{2}}\hat{z}_p$$

On cherche donc le nbre de pts de $\mathbb{F}_q^p$ / $2\hat{x}_1\hat{y}_1 + \dots + 2\hat{x}_{\frac{p-1}{2}}\hat{y}_{\frac{p-1}{2}} + (-1)^{\frac{p-1}{2}}\hat{z}_p^2 = 1$.

2 cas : (i) $(\hat{y}_1, \dots \hat{y}_{\frac{p-1}{2}}) \in \mathbb{F}_q^{\frac{p-1}{2}} \setminus \{(0,\dots 0)\}$ fixé.

On a alors : ok $\leftarrow \underbrace{(q^{\frac{p-1}{2}}-1)}_{\hat{y}}\ \underbrace{q^{\frac{p-1}{2}-1}}_{\hat{x}}\ \underbrace{q}_{\hat{z}_p}$ choix de $x \in \mathbb{F}_q^p$. $\rightarrow \hat{z}_p \in \mathbb{F}_q$.

↳ on peut exprimer un $\hat{x}_i$ en f° des autres, ex si $\hat{y}_1 \neq 0$: $\hat{x}_1 = \frac{1}{2}\left(1 - 2\hat{x}_2\hat{y}_2 - \dots - (-1)^{\frac{p-1}{2}}\hat{z}_p^2\right)\hat{y}_1^{-1}$ (par cas 2 donc ok)

Donc on a $\frac{p-1}{2}-1$ degré de liberté.

(ii) $(\hat{y}_1, \dots \hat{y}_{\frac{p-1}{2}}) = (0, \dots 0)$.

On a alors : ok $\leftarrow \underbrace{1}_{\hat{y}} \times \underbrace{q^{\frac{p-1}{2}}}_{\hat{x}} \times \underbrace{\left(\left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)+1\right)}_{\hat{z}_p}$ $\rightarrow$ par le lemme vu qu'on ait ramené à l'équation : $(-1)^{\frac{p-1}{2}}\hat{z}_p^2 = 1$

plus de contraintes sur $\hat{x}$

Au total on a donc : $q^{\frac{p-1}{2}}\left(q^{\frac{p-1}{2}}-1\right) + q^{\frac{p-1}{2}}\left(\left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)+1\right)$.

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

car par def : $\left(\frac{q}{p}\right) = q^{\frac{p-1}{2}}$ et $\left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$

et comme $|\mathbb{F}_p^*| = p-1$ on a $\forall x \in \mathbb{F}_p^*$: $x^{p-1} = 1$.

Donc en particulier : $q^{p-1} = 1$ mod p.

Conclusion : On a : $\left(\frac{p}{q}\right)\cancel{+1} = |X| = \cancel{1+}\left(\frac{q}{p}\right)(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ mod p.

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

$\Rightarrow \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ mod p car $\left(\frac{q}{p}\right) = \pm 1$. (donc on peut bien le passer de l'autre côté).

$\Rightarrow \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ ds $\mathbb{Z}$ car on sait que $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = \pm 1$ ds $\mathbb{Z}$

de m̂ que $(-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \pm 1$ ds $\mathbb{Z}$.

Précision : prenons par ex : $\overline{x}^p = \overline{y}^p$ et je sais que ds $\mathbb{Z}$: $\begin{vmatrix} x = \pm 1 \\ y = \pm 1.\end{vmatrix}$

$\overline{x}^p = \overline{y}^p \Rightarrow x + kp = y + \tilde{k}p$ ds $\mathbb{Z}$ — car ds $\mathbb{Z}$ je sais que $x = \pm 1$, $y = \pm 1$ donc $k = \tilde{k} = 0$.

$\Rightarrow x = y$ ds $\mathbb{Z}$

cf Algèbre p. 131. 3.6.1. $\boxed{\text{Formule de Burnside et première application}}$ Leçon : 101, 104, 105.
(validé par Caldero).

__Énoncé__ : G groupe fini agit sur X ensemble finit.
Soit X/G l'ensemble des orbites pour cette action.

1. Formule des classes : Pour $x \in X$: $|\mathcal{O}_x| = \dfrac{|G|}{|G_x|}$ où $G_x = \{g \in G \,/\, g.x = x\}$ le stabilisateur de x.

2. Formule de Burnside : $|X/G| = \dfrac{1}{|G|} \sum_{g \in G} |X^g|$ où $X^g = \{x \in X \,/\, g.x = x\}$, $g \in G$ fixé.

3. Application : On considère le groupe symétrique $\mathfrak{S}_n$ agissant naturellement sur l'ensemble $X = \{1, \dots n\}$.
On considère la v.a. Y sur $\mathfrak{S}_n$ qui associe à $\sigma \in \mathfrak{S}_n$ son nbre d'invariants X^σ.
Calculer $\mathbb{E}[Y]$ et $\mathrm{Var}[Y]$.

---

① Soit $x \in X$ fixé. On considère l'application $\varphi : \begin{array}{l} G \to \mathcal{O}_x \\ g \mapsto g.x \end{array}$

On a φ bien définie car G agit sur X et φ surj car par def de $\mathcal{O}_x$: $\mathcal{O}_x = \mathrm{Im}\,\varphi$.

Par passage au quotient :
$$\begin{tikzcd} G \arrow[r, two heads, "\varphi"] \arrow[d] & \mathcal{O}_x \\ G/G_x \arrow[ur, "\bar{\varphi}"'] & \end{tikzcd}$$
on obtient $G/G_x \simeq \mathcal{O}_x$.

(on peut car $G_x \subset \mathrm{Ker}\,\varphi$; ici $\hat{m}$ $G_x = \mathrm{Ker}\,\varphi$)

↳ Surj. : ok car φ surj.

↳ Inj : Soit $g, g' \in G/G_x$ / $g.x = g'.x$
$\Rightarrow (g'^{-1}g).x = x \Rightarrow g'^{-1}g \in G_x \Rightarrow g'^{-1}g = e$ dans G/G_x (quotienter c'est tuer)
$\Rightarrow g = g'$.

__cl__ : $|\mathcal{O}_x| = \left|\dfrac{G}{G_x}\right| = \dfrac{|G|}{|G_x|}$.

② On pose $R = \{(g, x) \in G \times X \,/\, g.x = x\}$. On va calculer $|R|$ de 2 manières $\neq$.

Pour cela on introduit $\pi_1 : \begin{array}{l} R \to G \\ (g,x) \mapsto g \end{array}$ et $\pi_2 : \begin{array}{l} R \to X \\ (x,g) \mapsto x \end{array}$.

- Soit $g \in G$.
On a : $|\pi_1^{-1}(g)| = |\{x \in X \,/\, g.x = x\}| = |X^g|$ par déf. de X^g.
($|\pi_1^{-1}(g)| = |\{(g,x), x \in X / g.x = x\}|$)
Donc $|R| = \sum_{g \in G} |X^g|$. ↜ on compte le nbre de couples $(g,x) / g.x = x$. Comme g change à chaque fois ds la somme et que l'on comptabilise $\neq$ les x / $g.x = x$ (càd $x \in \pi_1^{-1}(g)$) on a bien pas de doublons

- De $\hat{m}$ pour $x \in X$:
On a : $|\pi_2^{-1}(x)| = |\{g \in G / g.x = x\}| = |G_x|$ par def de G_x.
($= |\{(g,x), g \in G / g.x = x\}|$)
Donc $|R| = \sum_{x \in X} |G_x|$.
$= |G| \sum_{x \in X} \dfrac{1}{|\mathcal{O}_x|}$ par la Formule des classes.
$= |G| \sum_{\mathcal{O} \in X/G} \sum_{x \in \mathcal{O}} \dfrac{1}{|\mathcal{O}|} = |G| \sum_{\mathcal{O} \in X/G} \dfrac{|\mathcal{O}|}{|\mathcal{O}|} = |G|\,|X/G|$.

__cl__ : $|X/G| = \dfrac{1}{|G|} \sum_{g \in G} |X^g|$.

③ * Calcul de $\mathbb{E}[Y]$.

On a $\mathbb{E}[Y] = \frac{1}{|\mathfrak{S}_n|} \sum_{\sigma \in \mathfrak{S}_n} |X^\sigma| = \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} |X^\sigma| = |X/\mathfrak{S}_n|$. par la formule de Burnside.

Or l'action naturelle de $\mathfrak{S}_n$ sur X ($((\sigma, i) \in \mathfrak{S}_n \times X \mapsto \sigma(i))$) est transitive.

En effet, pour un $i \in X$ fixé : $\forall j \in X, \exists \sigma \in \mathfrak{S}_n / \sigma(i) = j$. $\Rightarrow O_i = X$.

(et m̂ : $\forall 1 \leqslant i, j \leqslant n$, $\exists \sigma \in \mathfrak{S}_n / \sigma(i) = \sigma(j)$).

Ainsi $|X/\mathfrak{S}_n| = 1$ et $\mathbb{E}[Y] = 1$.

* Calcul de $\mathrm{Var}(Y) = \mathbb{E}[Y^2] - \mathbb{E}[Y]^2$.

On a $\mathbb{E}[Y^2] = \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} |X^\sigma|^2$ ← pour chaque σ on compte son nbre de pts fixes $|X^\sigma|$ et on met au carré puis on divise par $|\mathfrak{S}_n|$

On va donc regarder l'action de $\mathfrak{S}_n$ sur $X \times X$: $g.(x, x') = (g.x, g.x')$.

Cette action possède 2 orbites :

(i) les (x, x), $x \in X$ qui est bien une orbite par ce qui précède. ($\forall 1 \leqslant i, j \leqslant n \; \exists \sigma \in \mathfrak{S}_n / \sigma(i) = j$ $\Rightarrow \sigma.(i,i) = (j,j)$)

(ii) les (x, x'), $x, x' \in X$, $x \neq x'$.
c'est bien une orbite car $\forall$ couple $(i, i'), (j, j') \in X \times X$, $\exists \sigma \in \mathfrak{S}_n / \begin{cases} \sigma(i) = i' \\ \sigma(j) = j' \end{cases}$
$i \neq j$ et $i' \neq j'$

On a donc bien 2 orbites. (on a déjà recouvert tt les élém^ts de $X \times X$) (on ne peut pas envoyer (i,i) sur (i', j') $i' \neq j'$ avec un m̂ σ)

Par Burnside on a donc :
$$2 = |X \times X/\mathfrak{S}_n| = \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} |(X \times X)^\sigma|$$
$$= \frac{1}{n!} \sum_{\sigma \in \mathfrak{S}_n} |X^\sigma|^2$$
$$= \mathbb{E}[Y^2].$$

← car $(X \times X)^\sigma = X^\sigma \times X^\sigma$

(fixer (i, j) revient à fixer i et à fixer j
$\sigma.(i,j) = (i,j)$
$\Leftrightarrow (\sigma(i), \sigma(j)) = (i,j)$)

ccl : $\mathrm{Var}\, Y = 2 - 1^2 = 1$.

Classificat° des groupes simples d'ordre 60.
On admettra que le groupe alterné $\mathcal{A}_5$ est simple, d'ordre 60.
On veut montrer que tout groupe simple d'ordre 60 est isomorphe à $\mathcal{A}_5$.

① Si φ est un morphisme d'un groupe G vers un gpe H alors φ envoie le sous-groupe dérivé $D(G)$ dans $D(H)$.

. $D(G)$ est engendré par les commutateurs $[g,h] = ghg^{-1}h^{-1}$ où $g,h \in G$.
Puisque φ est un morphisme de groupes on a:
$\varphi([g,h]) = \varphi(g)\varphi(h)\varphi(g)^{-1}\varphi(h)^{-1} = [\varphi(g),\varphi(h)]$, $\varphi(g),\varphi(h) \in H$
Ainsi φ envoie $D(G)$ dans $D(H)$.

② Soit G un groupe simple d'ordre 60. G possède 6 5-Sylow.

. $|G| = 60 = 5 \times 3 \times 2^2$ D'après les théorèmes de Sylow on sait que N_5, le nombre de 5-Sylow de G vérifie:

$$\begin{cases} \to N_5 \mid 3\times 2^2 \\ \to N_5 \equiv 1 \ [5] \end{cases} \quad \text{donc } N_5 = 1 \text{ ou } N_5 = 6$$

Puisque G est simple $N_5 \neq 1$ car sinon le seul 5-Sylow de G serait alors normal dans G, ainsi $N_5 = 6$.

③ Il existe un morphisme injectif de G dans S_6.

. Puisque G possède 6 5-Sylow, on a une action de G sur ces 6 5-Sylow ce qui fournit un morphisme de G dans S_6:
On note $H_1, H_2, \dots H_6$ ces 6 5-Sylow. G agit par conjugaison sur $X = \{H_1, \dots, H_6\}$ et donc le morphisme cherché noté φ est définit de la façon suivante:

$$\varphi : \begin{array}{ccl} G & \longrightarrow & S(X) \simeq S_6 \\ & & x \longmapsto x \\ g & \longmapsto & H_i \longmapsto gH_ig^{-1} \end{array}$$

Ce morphisme φ est injective car $\ker(\varphi)$ est normal dans G donc le noyau est soit trivial soit G tout entier. Si $\ker\varphi = G$ alors $g.H_i = H_i$ $\forall g \in G$ donc $gH_ig^{-1} = H_i$ $\forall g \in G$ ce qui contredit le théorème de Sylow assurant la transitivité de l'action de G sur ses 6 5-Sylow. D'où $\ker\varphi = \{e\}$.

④ φ s'injecte dans $\mathcal{A}_6$

- D'après ① φ envoie $D(G)$ dans $D(S_6)$.

→ $D(G)$ étant un sous groupe distingué de G ($g[k,h]g^{-1} = [gkg^{-1}, ghg^{-1}]$)
On a $D(G) = G$ ou $D(G) = \{e\}$. ~~Puisque~~ Si $D(G) = \{e\}$
Alors $\forall g, h \in G$ $[g,h] = e$ donc G serait abélien
Or un groupe abélien est simple ssi il est d'ordre premier car tout élément non trivial engendre G, en particulier G est alors cyclique et simple donc d'ordre premier. D'où $D(G) = G$.

→ $D(S_6) \subset \mathcal{A}_6$ puisque $\varepsilon(ghg^{-1}h^{-1}) = \varepsilon(g)\varepsilon(h)\varepsilon(g)^{-1}\varepsilon(h)^{-1} = 1$
où ε est le morphisme signature.

φ est donc un morphisme injectif qui envoie G dans $\mathcal{A}_6$. On peut donc assimiler G à un sous-groupe de $\mathcal{A}_6$.

⑤ En faisant agir $\mathcal{A}_6$ sur $\mathcal{A}_6/G$, On montre que G s'injecte dans S_5 puis dans $\mathcal{A}_5$.

- On sait qu'un groupe K agit sur ~~les sous-groupes~~ K/H (où H est un sous-groupe de K), l'ensemble des classes à gauche modulo H, de la façon suivante :

$$K \times K/H \longrightarrow K/H$$
$$(k, k'H) \longmapsto k.k'H = (kk').H \,,\quad k, k' \in K$$

Cette action est transitive car $k''k'^{-1}$ envoie $k'H$ sur $k''H$ pour tout $k', k'' \in K$.

. On applique ce résultat au groupe $\mathcal{A}_6$ qui agit donc sur $\mathcal{A}_6/G$ de cardinal 6. Il existe alors un morphisme φ de $\mathcal{A}_6$ dans $S(\mathcal{A}_6/G) \simeq \mathfrak{S}_6$, et ce morphisme est injectif car $\mathcal{A}_6$ est simple et l'action de $\mathcal{A}_6$ sur $\mathcal{A}_6/G$ est transitive (si le morphisme était trivial, alors toute orbite serait singletonne).

On dispose donc d'un morphisme φ injectif de $\mathcal{A}_6$ dans S_6, et pour tout $g \in G$ on a $\varphi(g)(\bar{e} = eG = G) = geG = G = \bar{e}$.
Ainsi φ stabilise un élément : la classe $\bar{e}$ du neutre, or le stabilisateur d'un élément ds S_n (pour l'action naturelle) est isomorphe à S_{n-1}. φ envoie donc G injectivement dans S_5, et toujours d'après ① φ envoie $D(G) = G$ vers $D(\mathfrak{S}_5) \subset \mathcal{A}_5$.
Par cardinalité de G et $\mathcal{A}_5$, on en déduit $G \simeq \mathcal{A}_5$.