Loi de réciprocité quadratique

Julie Parreaux

2018-2019

Référence du développement : H2G2 [3, p.182]

Leçons où on présente le développement : 120 (Anneaux $\mathbb{Z}/n\mathbb{Z}$) ; 121 (Nombres premiers) ; 123 (Corps finis) ; 126 (Équation en arithmétique) ; 170 (Formes quadratiques).

1 Introduction

La loi de réciprocité quadratique nous permet de caractériser les carrés dans $\mathbb{F}_q$. Savoir si un nombre est un carré modulo q est un problème difficile puisque la moitié des éléments de $\mathbb{F}_q$ sont des carrés. En effet, la méthode naïve consiste à tester tous les éléments afin de savoir s'ils sont ou non un carré. La loi de réciprocité quadratique nous donne un procédé calculatoire pour savoir si un nombre est un carré modulo q.

2 La loi de réciprocité quadratique via les formes quadratiques

On commence par donnée une définition importante : on définit le symbole de Legendre.

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

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

Schéma du développement (leçons 123 et 126)

1. Montrer le lemme.
   (a) Montrer que a est un carré modulo q si et seulement si a^{-1} en est un.
   (b) Montrer que a est un carré modulo q si et seulement si $aX^2 - 1 \in \mathbb{F}_q[X]$ possède deux racines distinctes.
   (c) Dénombrer l'ensemble $\left|\{x \in \mathbb{F}_q, ax^2 = 1\}\right|$ en fonction de si a est ou non un carré dans $\mathbb{F}_q$.
2. Montrer à l'aide d'action de groupe que $|X| = 1 + \left(\frac{p}{q}\right)[p]$.
3. Montrer à l'aide de forme quadratique que $|X| = q^d\left(q^d + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right)$.
   (a) Dire que les deux formes quadratiques sont équivalentes.
   (b) Dénombrer les éléments de X'.
   (c) En déduire le cardinal de X.
4. Conclure sur le cardinal de X.

Schéma du développement (leçons 120, 121 et 170)

1. Énoncer le lemme.
2. Montrer à l'aide d'action de groupe que $|X| = 1 + \left(\frac{p}{q}\right)[p]$.
3. Montrer à l'aide de forme quadratique que $|X| = q^d\left(q^d + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right)$.
   (a) Montrer que les deux formes quadratiques sont équivalentes.
   (b) Dénombrer les éléments de X'.
   (c) En déduire le cardinal de X.
4. Conclure sur le cardinal de X.

On donne maintenant un lemme qui va nous être utile tout au long de la démonstration (on n'est pas obliger de le démontrer à l'oral mais le faire pour les leçons 123 et 126).

Lemme 1. *Soit a un entier non nul et q un nombre premier impaire. Alors,*

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

Démonstration. Soit a un entier non nul et q un nombre premier impaire.

Étape a : a est un carré modulo q si et seulement si a^{-1} en est un

$$\begin{array}{rcll} a = x^2[q] & \Leftrightarrow & a^{-1} = x^2\left(a^{-1}\right)^2[q] & \text{(multiplication par } \left(a^{-1}\right)^2[q]) \\ & \Leftrightarrow & a^{-1} = y^2[q] & \text{(où } y = xa^{-1}) \end{array}$$

Étape b : a est un carré modulo q si et seulement si $aX^2 - 1 \in \mathbb{F}_q[X]$ possède deux racines distinctes
On raisonne dans $\mathbb{F}_q$. (Supposons que x est inversible.)

$$\begin{array}{rcll} a = x^2[q] & \Leftrightarrow & a\left(x^{-1}\right)^2 = 1[q] & \text{(multiplication par } \left(x^{-1}\right)^2[q]) \\ & \Leftrightarrow & a\left(x^{-1}\right)^2 - 1 = 0[q] & \text{(par soustraction de 1)} \\ & \Leftrightarrow & x^{-1} \text{ est une racine de } aX^2 - 1 & \text{(par définition)} \\ & \Leftrightarrow & aX^2 - 1 \text{ a deux racines distinctes} & \text{(car } x \text{ est inversible si et seulement si } x \neq 0) \end{array}$$

Étape c : Dénombrons l'ensemble $\left|\{x \in \mathbb{F}_q, ax^2 = 1\}\right|$ en fonction de si a est ou non un carré dans $\mathbb{F}_q$
On peut distingué deux cas.

— Si a n'est pas un carré modulo q, alors par ce qu'on vient de dire $\left|\{x \in \mathbb{F}_q, ax^2 = 1\}\right| = 0 = 1 - 1 = 1 + \left(\frac{a}{q}\right)$ (symbole de Legendre vaut -1 car a est non nul par hypothèse).

— Si a est un carré modulo q, alors par ce qu'on vient de dire $\left|\{x \in \mathbb{F}_q, ax^2 = 1\}\right| = 2 = 1 + 1 = 1 + \left(\frac{a}{q}\right)$ (symbole de Legendre vaut 1).

□

Théorème. *Soient p, q premiers impairs distincts. Alors*

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

Démonstration. L'idée de cette preuve qui est intéressante car elle va dénombrer de deux manières différentes un certain ensemble X. On pose $X = \{(x_1, \ldots, x_p) \in \mathbb{F}_q | x_1 + \cdots + x_p = 1\}$.

Étape 1 : montrons à l'aide d'action de groupe que $|X| = 1 + \left(\frac{p}{q}\right)\ [p]$. (On raisonne sur $\mathbb{F}_q$.) On fait agir $\mathbb{Z}_{/p\mathbb{Z}}$ sur $\mathbb{F}_q^p$ par permutation des coordonnées :

$$\forall k \in \mathbb{Z}_{/p\mathbb{Z}}, \forall x = (x_1, \dots, x_p) \in \mathbb{F}_q^p, k.x = \left(x_{1+k \mod p}, \dots, x_{p+k \mod p}\right)$$

Comme l'action permute les coordonnées (la somme de leurs carrés reste 1), X est stable sous l'action de $\mathbb{Z}_{/p\mathbb{Z}}$, étudions les orbites des éléments de X par cette actions.

— L'orbite de $(x, \dots, x) \in F_q^p$ où $x \in \mathbb{F}_q$ est triviale, c'est le singleton $\{(x, \dots, x)\}$ (l'ensemble des éléments atteignable depuis x est x par permutation de ces coordonnées) et toutes les orbites triviales sont de cette forme (une orbite triviale est une orbite telle que $\{y \in X, k.x = y\} = \{x\}$ et dans ce cas la, comme on agit par permutation des coordonnées, x est telle que on l'a définie). On en déduit qu'il y a autant d'orbites triviales que d'éléments $x \in \mathbb{F}_q$ tel que $px^2 = 1$. Par le lemme 1, on a que $\left|\{x \in \mathbb{F}_q, ax^2 = 1\}\right| = 1 + \left(\frac{a}{q}\right)$. (De plus, leur stabilisateur est $\mathbb{Z}_{/p\mathbb{Z}}$, en effet, comme pour tout élément $k \in \mathbb{Z}_{/p\mathbb{Z}}, k. = x$, cela conclut.)

— Les orbites non triviales sont alors des orbites dont le stabilisateur est trivial. En effet,

$$\begin{aligned} \mathrm{Stab}(x) &= \{n \in \mathbb{Z}_{/p\mathbb{Z}} | n.x = \left(x_{1+n \mod p}, \dots, x_{p+n \mod p}\right)\} \\ &= \{n \in \mathbb{Z}_{/p\mathbb{Z}} | \forall i x_i = x_{i+n \mod p}\} \\ &= \{1\} \text{ (car } \exists i \neq j, x_i \neq x_j) \end{aligned}$$

Comme $|\mathrm{Orb}(x)|\,|\mathrm{Stab}(x)| = \left|\mathbb{Z}_{/p\mathbb{Z}}\right|$, on en déduit que $|\mathrm{Orb}(x)| = 1$. Par la formule des classes, on a $|X| = \left|\{x \in \mathbb{F}_q | px^2 = 1\}\right| + kp \mod p$ où k est le nombre d'orbites non triviales. On a alors $|X| = 1 + \left(\frac{p}{q}\right) \mod p$.

Étape 2 : montrons à l'aide de forme quadratique que $|X| = q^d\left(q^d + (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\right)$. On pose $q_1(x_1, \dots, x_p) = x_1 + \dots + x_p$ et $q_2(z_1, \dots, z_q, y_1, \dots, y_d, t) = 2(y_1 z_1 + \dots z_d y_d) + at^2$ deux formes quadratiques avec $d = \frac{p-1}{2}$ et $a = (-1)^q$.

Étape a : montrons que ces deux formes quadratiques sont équivalentes. Considérons les matrices de ces formes quadratiques :

$$I_p = \begin{bmatrix} 1 & & 0 \\ & \ddots & \\ 0 & & 1 \end{bmatrix} \quad \text{et} \quad A = \begin{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} & & & \\ & \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} & & \\ & & \ddots & \\ & & & a \end{bmatrix}$$

Les matrices I_p et A sont congruentes. En effet, $\mathrm{rg}(I_p) = p = \mathrm{rg}(A)$ et $\det(I_p) = 1 = \underbrace{(-1)^{\frac{p-1}{2}}}_{\text{développement par les lignes}} \underbrace{(-1)^{\frac{p-1}{2}}}_{a} = \det(A)$, donc elles ont même discriminant.Le théorème de classification des formes quadratiques sur $\mathbb{F}_q$ s'applique. On en déduit que les formes quadratiques q_1 et q_2 sont équivalentes. Ainsi le cardinal de X est égal au cardinal de $X' = \{(x_1, \dots, x_d, z_1, \dots, z_d, t)\,|q_2(x_1, \dots, x_d, z_1, \dots, z_d, t) = 1\}$.

Étape b : dénombrons les éléments de X'**.** Soit $(x_1, \dots, x_d, z_1, \dots, z_d, t) \in X'$. On distingue alors deux cas :

— Si $y_1 = y_d = 0$ alors $at^2 = 1$.
  — On a q possibilités pour chaque z_i (car $z_i \in \mathbb{F}_q$).
  — On a $1 + \left(\frac{a}{q}\right)$ possibilité (lemme 1).

On en conclut qu'on a $q\left(1+\left(\frac{a}{q}\right)\right)$.

— Il existe y_i tel que $y_i \neq 0$.
  — Une fois les z_i et t sont fixés, il reste à choisir les x_i qui forment un hyperplan affine de $\mathbb{F}_q^d$. On a alors q^{d-1} possibilités.
  — Pour fixé les z_i, on a alors $q^d - 1$ possibilités.
  — Pour fixé t, on a q possibilités.

On en déduit qu'on a $\left(q^d-1\right) qq^{d-1} = \left(q^d-1\right) q^d$.

Étape c : En déduire le cardinal de X. Des calculs précédent, on a :

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

Étape 3 : Conclure sur le cardinal définitif de X. On a :

$$\begin{aligned} 1+\left(\frac{p}{q}\right) &= \left(\frac{q}{p}\right)\left(\left(\frac{p}{q}\right) + (-1)^{\frac{q-1}{2}\frac{p-1}{2}}\right)\ [p] \\ 1+\left(\frac{p}{q}\right) &= \left(\frac{q}{p}\right)(-1)^{\frac{q-1}{2}\frac{p-1}{2}} + 1\ [p] \qquad \left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = 1 \\ \left(\frac{p}{q}\right) &= \left(\frac{q}{p}\right)(-1)^{\frac{q-1}{2}\frac{p-1}{2}}\ [p] \end{aligned}$$

Les termes considérés étant dans $\{1,-1\}$ l'égalité reste vraie dans $\mathbb{Z}$, on en conclut :

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

□

3 Compléments autours du dénombrement dans des corps finis

Applications à cette loi

Proposition. 3 *est un carré modulo p si et seulement si $p \equiv -1[12]$.*

Application. Les nombres de Merssenne.

Corps finis

La notion de corps finis est une notions importantes dès que l'on fait des mathématiques à l'aide d'un ordinateur. Cependant, elle n'est pas simple à définir et à manipuler.

Quelques propriétés des corps finis On donne ici quelques propriétés de structures sur ces corps finis.

Théorème ([7, p.74])**.** *Soit K un corps fini. Alors $K^\times$ est cyclique.*

Démonstration. On utilise la formule suivante : $n = \sum_{d|n}\varphi(d)$. On considère le sous-groupe engendré par un élément d'ordre $d|q-1$: le nombre d'élément d'ordre d est 0 ou $\varphi(d)$. On conclut par la formule. □

Application. Soit $p \in \mathbb{N}^*$ un nombre premier, $(\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}$. En effet, $\mathbb{Z}/p\mathbb{Z}$ est un corps donc $(\mathbb{Z}/p\mathbb{Z})^\times$ est un groupe cyclique. Il est donc isomorphe à un $\mathbb{Z}/n\mathbb{Z}$. Comme $|\,(\mathbb{Z}/p\mathbb{Z})^\times\,| = p-1$; on conclut.

On définit la notion de caractéristique pour un anneaux [5, p.30]. Dans le cas d'un corps, un morphisme de corps lié à cette caractérisation est alors facilement exploitable.

Définition. Soit A un anneau unitaire et $f : \mathbb{Z} \to A$ un morphisme d'anneau tel que $n \mapsto n1$. Si f est injectif, on dit que A est de caractéristique nulle. Sinon, soit $c > 0$ tel que $\ker f = c\mathbb{Z}$. On dit alors que la caractéristique de A est c.

Proposition. *La caractéristique d'un anneau unitaire intègre est* 0 *ou un nombre premier.*

Démonstration. Par l'absurde en contredisant la minimalité de la caractéristique. □

Proposition. *Soit K un corps commutatif de caractéristique $p > 0$. Alors $f : K \to K$ définie par $x \mapsto x^p$ est un morphisme de corps.*

Étude des carrés dans $\mathbb{F}_q$

Nous allons rappeler quelques notions autours des carrés dans un corps finis et du symbole de Legendre [4, p.119]. On est ainsi souvent amené à étudier les carrées de $(\mathbb{Z}/n\mathbb{Z})^*$.

Définition (Carré modulo n)**.** Soit a et n deux entiers premiers entre eux. S'il existe un entier b tel que $a \equiv b^2[n]$, on dit que a est un résidu quadratique de n ou un carré modulo n. Sinon, on dit que a est un résidu non quadratique.

Définition (Symbole de Legendre)**.** Soit n un nombre premier impair. Le symbole de Legendre pour $a \in \mathbb{Z}$ est :

$$\left(\frac{a}{p}\right) = \begin{cases} 0 & \text{, si } a \equiv 0[p] \\ 1 & \text{, si } a \text{ est un résidu quadratique de } p \\ -1 & \text{, si } a \text{ n'est pas un résidu quadratique de } p \end{cases}$$

Proposition. *Si p est un nombre premier et $\left(\mathbb{F}_p^*\right)^2$ l'ensemble des éléments de $\mathbb{F}_p^*$ qui sont des carrés, on a :*

1. *si $p = 2$, $\mathbb{F}_2^* = (\mathbb{F}_2^*)^2$.*
2. *si $p > 2$, l'application de $\mathbb{F}_p^*$ dans $\mathbb{F}_p^*$ définie par $x \mapsto x^{(p-1)/2}$ est un morphisme de groupes dont le noyau est $\left(\mathbb{F}_p^*\right)^2$, sous-groupe cyclique d'ordre $\frac{p-1}{2}$ et dont l'image est $\{-1, 1\}$.*

Démonstration.

1. Trivial car $\mathbb{F}_2^*$ est réduit à l'élément neutre.
2. L'application est un endomorphisme de groupe multiplicatif par commutativité. D'autre part, le groupe $\mathbb{F}_p^*$ est cyclique d'ordre $p-1$, on peut choisir un élément générateur g.
   Soit x un élément du noyau de ce morphisme, il existe k un entier tel que $x = g^k$. Comme $x^{(p-1)/2} = 1$, on a $g^{k(p-1)/2} = 1$, soit $(p-1)|k(p-1)/2$ et $2|k$. Posons $l = \frac{k}{2}$, on a $x = \left(g^l\right)^2$, donc x est un carré. La réciproque est immédiate.
   L'égalité $x = \left(g^l\right)^2$ démontre que le noyau est engendré par g^2. Donc comme g est un générateur ses éléments sont d'ordre $\frac{p-1}{2}$. En passant à l'image, les éléments du noyau sont racines de $X^2 - 1$ soit sont dans $\{-1, 1\}$.

□

Corollaire. *Dans $\mathbb{F}_p^*$, un élément x est un carré si et seulement si l'ordre de x divise $\frac{p-1}{2}$ et il y a autant de carré que de non carré.*

Démonstration. La condition $^{(p-1)/2} = 1$ caractérise les éléments de l'unique sous-groupe d'ordre $\frac{p-1}{2}$ de $\mathbb{F}_p^*$. L'ordre de $\mathbb{F}_p^*$, il reste $\frac{p-1}{2}$ éléments qui ne sont pas des carrés. □

Corollaire. *Si p est un nombre premier impair, a et b des entiers, on a :*

1. $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2}[p]$.
2. $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
3. *Si $a \equiv b[p]$, alors* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

Démonstration.

1. Si $a \equiv 0[p]$, on est ok. Si a est un résidu quadratique de p, il existe x tel que $a \equiv x^2[p]$, d'où $a^{(p-1)/2} \equiv 1[p]$. On traite le dernier cas de manière analogue.
2. On applique le résultat précédent.
3. Découle de la définition.

□

Application. Trouver des carrés revient en la résolution d'équations diophantienne du second degré.

Théorème (Loi de réciprocité quadratique)**.** *Soient p et q sont deux nombres premiers impaires et distincts, alors*

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

Remarque. La loi de réciprocité quadratique est vrai même si p et q ne sont pas premier. On utilise le symbole de Jacobi.

Définition (Symbole de Jacobi)**.** Si n est un entier naturel impair tel que $n = \prod_i p_i^{\alpha_i}$ sa factorisation primaire et a un entier, le symbole de Jacobi $\left(\frac{a}{n}\right)$ est défini par : $\left(\frac{a}{n}\right) = \prod_i \left(\frac{a}{p_i}\right)^{\alpha_i}$.

Théorème (Critère d'Euler)**.** *Soit p un nombre premier impaire et a un entier premier avec p, alors* $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}[p]$

Démonstration. Voir corollaire ci-dessus. □

Remarque. On peut utiliser ces résidus quadratique pour d'autres tests de primalité : Lucas-Lehmer qui utilise les nombres de Mercènes.

Théorème de classification des formes quadratiques

Nous allons maintenant nous intéresser aux actions par congruence sur les espaces de matrices [3, p.250]. Le but est de donner une classification "simple" de deux matrices congruentes afin de classifier les formes quadratiques.

Définition. $GL_n(K)$ agit par congruence sur les matrices symétrique $\mathcal{S}_n(K)$ via l'application $\varphi : GL_n(K) \times \mathcal{S}_n(K)$ définie par $(P, A) \mapsto P.A = PA^tP$.

Définition. Deux matrices symétriques sont dites congruentes si elles appartiennent à la même orbite pour l'action de congruence.

Théorème (Classification sur des corps classiques)**.**

1. *Si $K = \mathbb{C}$, deux matrices sont dans la même orbite si et seulement si elles ont même rang.*
2. *Si $K = \mathbb{R}$, deux matrices sont dans la même orbite si et seulement si elles ont même rang et ont la même signature.*
3. *Si $K = \mathbb{F}_q$, deux matrices inversibles sont dans la même orbites si et seulement si elles ont le même discriminant.*

Démonstration.

1. Si rg$A \neq 0$ alors A est congruente à une matrice diagonale. On a alors l'existence d'une base orthogonale qui donne la forme normale de l'orbite. On utilise alors m'invariance du rang pour conclure.
2. Analogue au cas complexe, sauf que la forme normal possède en plus un bloc pour $-Id$. On applique la formule de Grassmann puis l'invariance du rang et de la signature.
3. A est inversible donc non-dégénérée. On choisi un non-carré et en orthogonalisant, on voit que la forme normale est une matrice diagonale dont les valeur sont 1 ou ce non-carré (uniquement deux classe dans K car d'indice 2). Par orthogonalisation, on obtient une matrice diagonale de 1 sauf pour la dernière valeur. Via le discriminant, on est capable de choisir cette valeur.

□

Actions de groupes

Les actions de groupes [2, p.195] sont des notions importantes car elles permettent d'agir sur un ensemble. Elles ont plusieurs applications notamment en géométrie (c'est la base de la géométrie) ou en dénombrement si le groupe est fini (via les formules sur les cardinaux).

Remarque. Il y a deux monde : celui des groupes et des objets sur lesquels ils agissent. La translation dans le monde des objets (par application de l'action) se traduit par la conjugaison dans les groupes.

Définition (Action de groupes)**.** Une action de groupe d'un groupe G sur un ensemble X est une application $f : G \times X \to X$ telle que $\forall x \in X, f(e, x) = x$ et $\forall g_1, g_2 \in G, \forall x \in X, f(g_1.g_2, x) = f(g_1, f(g_2, x))$.

Une action de groupe de G sur X peut être également la donné d'un morphisme de G dans $\mathfrak{S}_{|X|}$.

Définition (Action fidèle [1, p.174])**.** Soit G un groupe agissant sur E. On dit que G agit fidèlement sur E si pour tout $g \in G$, $gx = x$ pour tout $x \in E$ implique $g = 1_G$ (le neutre). Autrement dit si le morphisme de l'action est injectif.

Exemple (Actions de groupes). Donnons quelques exemples classiques d'actions de groupes.

— G opère sur G par translation à gauche.
— G opère sur $\mathcal{P}(G)$ par translation à gauche.
— G opère sur G par conjugaison.
— G opère sur $\mathcal{P}(G)$ par conjugaison.

Définition (Stabilisateur)**.** On définit le stabilisateur de l'action, pour tout élément $x \in X$, comme $\text{Stab}(x) = \{g \in G, f(g,x) = x\}$.

Remarque. Le stabilisateur d'un élément x de X est vu comme l'ensemble des éléments (de G) qui stabilise, "laisse fixe" x lors de l'application de f. On vérifie facilement que $\text{Stab}(x)$ est un sous-groupe de G.

Définition (Action libre [3, p.16])**.** Une action de G sur X est libre si tous les stabilisateurs des points de X sont triviaux.

Proposition ([3, p.15])**.** *Soit G un groupe opérant sur un ensemble X et $x \in X$. Alors,* $\text{Stab}(g.x) = g\text{Stab}(x)g^{-1}$.

Démonstration. $\left(g\text{Stab}(x)g^{-1}\right).(g.x)$(Action du groupe $\left(g\text{Stab}(x)g^{-1}\right)$ sur l'image) $= \left(g\text{Stab}(x)\right).x$ (calcul des actions) $= g.x$ (stabilisateur). On en déduit l'inclusion $\subseteq$. En remplaçant x par $g.x$ et g par g^{-1}, on obtient par le même procédé, l'inclusion inverse. □

Proposition ([8, p.31])**.** *Soit $\varphi : G \to \mathfrak{S}(X)$ une action de G sur l'ensemble X. Alors,* $\ker(\varphi) = \bigcap_{x \in X} \text{Stab}(x)$.

Démonstration. Si $g \in \ker(\varphi)$, $g.x = \varphi(g)(x) = e.x = x$ et $g \in \bigcap_{x \in X} \text{Stab}(x)$. Inversement, $g.x = \varphi(g)(x) = x$ et $g \in \ker(\varphi)$. □

Remarque. On justifie ainsi la définition d'action fidèle et notamment l'injectivité du morphisme.

Proposition ([8, p.42])**.** *Si $m \leq n$, alors si $\mathfrak{S}_n$ agit sur $\mathfrak{S}_m$ alors* $\mathfrak{S}_m \simeq \bigcap_{p \in \{m+1,\dots,n\}} \text{Stab}(p)$.

Lemme ([1, p.172])**.** *Soit G opérant sur un ensemble E. La relation sur E définie par $x \sim y$ s'il existe $g \in G$ tel que $y = g.x$ est une relation d'équivalence.*

Démonstration. **Reflexive** On prend $g = 1_G$
Symétrique On multiplie par g^{-1}
Transitive On utilise les propriétés de calcul
□

Définition (Orbite)**.** L'orbite de l'action, pour tout élément $x \in X$, comme : $\text{Orb}(x) = \{y \in X | \exists g \in G, f(g,x) = y\}$.

Remarque. Une orbite est une classe d'équivalence sur la relation d'équivalence définie précédemment. Une orbite d'un élément x de X comme l'ensemble des éléments (de X) atteignable à partir de x en appliquant f à un g.

Exemple (Exemples sur ces notions). Quelques exemples sur les notions d'orbites et de stabilisateurs.

— G opère sur G par translation à gauche.
  — $\text{Stab}(x) = \{e\}$
  — $\text{Orb}(x) = G$ (ici $X = G$)

Définition (Action transitive [1, p.172])**.** On dit que G agit transitivement sur E si pour tous $x, x' \in E$, il existe $g \in G$ tel que $x' = gx$.

Lemme ([1, p.172])**.** *Soit G agissant sur E. Alors les propriétés suivantes sont équivalentes :*

1. *G agit transitivement sur E*
2. *$\forall x \in E, \text{Orb}(x) = E$*
3. *$\exists x_0 \in E$ tel que $\text{Orb}(x_0) = E$*
4. *E n'admet qu'une seule orbite : E*

Démonstration. **Montrons** $1 \Rightarrow 2$ $\text{Orb}(x) \subseteq E$: définition. $\text{Orb}(x) \supseteq E$: si $x' \in E$, $\exists g$ tel que $x' = g.x$, alors $x' \in \text{Orb}(x)$.

Montrons $2 \Rightarrow 3$ Évident

Montrons $3 \Rightarrow 4$ Par la relation d'équivalence : les classes forment une partition.

Montrons $4 \Rightarrow 1$ Soient $x, x' \in E$, alors x, x' sont dans la même orbite. Donc, il existe g tel que $x' = gx$.
□

Définition (Points fixes)**.** Nous définition les points fixes d'un élément g de G comme l'ensemble des éléments (de X) qui sont stabilisés par g. De manière plus formelle on définit l'orbite comme $\text{Fix}(g) = \{x \in X, f(g,x) = x\}$.

Lemme ([1, p.172])**.** *Soit G agissant sur E. Alors les propriétés suivantes sont équivalentes :*

1. *x est un point fixe sous l'action de G*
2. $\text{Orb}(x) = \{x\}$
3. $|\text{Orb}(x)| = 1$
4. $\text{Stab}(x) = G$

Démonstration. **Montrons** $1 \Rightarrow 2$ Définition orbite et point fixe.

Montrons $2 \Rightarrow 3$ Évident

Montrons $3 \Rightarrow 4$ $\text{Stab}(x) \subseteq G$: ok ; $\text{Stab}(x) \supseteq G$: comme $|\text{Orb}(x)| = 1$, $\forall g, g.x = x$. Donc $\forall g, g \in \text{Stab}(x)$.

Montrons $4 \Rightarrow 1$ Définition orbite et point fixe. □

Lemme. *Soit G un groupe et X un ensemble sur lequel G agit. Pour tout élément $x \in X$, on a la relation suivante :* $|\text{Stab}(x)|\,|\text{Orb}(x)| = |G|$

Démonstration. On prouve cette relation à l'aide d'une bijection entre Orb et G/Stab.
Soit $x \in X$. On pose

$$\begin{array}{rccc} \varphi_x : & G/\text{Stab} & \to & \text{Orb} \\ & g & \mapsto & f(g,x) \end{array}$$

Cette application est bien définie car Stab est un sous-groupe de G donc le quotient est bien un groupe. (Attention : ce n'est pas un morphisme car Orb est un sous-ensemble de X.) De plus, elle est surjective par définition de l'orbite.

Elle est injective. En effet, si $g_1, g_2 \in G$ tels que $f(g_1,x) = f(g_2,x)$. On a alors, en composant par g_1^{-1}, $f(g_1^{-1}, f(g_1,x)) = f(g_1^{-1}, f(g_2,x))$. Par les propriétés sur f, on a $f(g_1^{-1}g_1, x) = f(g_1^{-1}g_2, x)$. Or, comme $f(e,x) = x$, on a $f(g_1^{-1}g_2, x) = f(g_1^{-1}g_1, x) = f(e,x) = x$.

On a donc bien une bijection entre ces deux ensembles finis et on conclut en passant aux cardinaux. □

Lemme. *Soit G un groupe et X un ensemble sur lequel G agit. On a la relation suivante* $\sum_{g\in G} |\text{Fix}(g)| = \sum_{x\in X} |\text{Stab}(x)|$

Démonstration. On pose un ensemble $S = \{(g,x) \in G \times X | f(g,x) = x\}$. On pose ensuite l'application S définie telle que :

$$\begin{array}{rccc} S : & G \times X & \to & \{0,1\} \\ & g,x & \mapsto & \begin{cases} 1 & \text{si } (g,x) \in S \\ 0 & \text{sinon} \end{cases} \end{array}$$

Comme $\text{Stab}(x)$ et $\text{Fix}(g)$ forment des partitions respectivement de X et de G, on a $S(.,x) = \mathbb{1}_{\text{Stab}(x)}$ et $S(g,.) = \mathbb{1}_{\text{Fix}(g)}$. On a alors $|S| = \sum_{g\in G} |\text{Fix}(g)| = \sum_{x\in X} |\text{Stab}(x)|$. D'où le résultat. □

Théorème (Formule du Burnside)**.** *Soit G un groupe et X un ensemble sur lequel G agit. Le nombre d'orbite de l'action est* $t = \frac{1}{|G|} \sum_{g\in G} |Fix(g)|$

Démonstration. On va alors montrer que $t\,|G| = \sum_{g\in G} |Fix(g)|$. On remarque que $X = \sqcup_{i=1}^{t} \text{Orb}(x_i)$ où x_i est un représentant d'un des orbites. Comme on a $\sum_{g\in G} |\text{Fix}(g)| = \sum_{x\in X} |\text{Stab}(x)|$ (lemme 3) $= \sum_{i=1}^{t} |\text{Orb}(x_i)| \frac{|G|}{|\text{Orb}(x_i)|}$ (lemme 3) $= t\,|G|$ (G indépendant somme). D'où le résultat. □

Remarque. On voit apparaître une version de la formule des classes.

Actions associées à l'action d'un groupe et invariants [6, p.47]

Proposition. *Soit G un groupe opérant sur un ensemble E, $p \in \mathbb{N}*$, alors G opère de façon naturelle sur $E^p = E_\times \cdots \times$ par $g(x_1, \ldots, g_p) = (gx_1, \ldots gx_p)$.*
G opère aussi sur $\mathcal{P}(E)$, l'ensemble des sous-ensembles de E par l'action : si $A \in \mathcal{P}(E)$, $gA = \{ga, a \in A\}$.

De plus, si G opère sur E et F, il opère sur l'ensemble des fonctions de E dans F.

Définition. Soit G un groupe opérant sur E. Un élément $x \in E$ est dit invariant quand : $\forall g \in G, gx = x$.

Si on se donne un espace homogène (G, E), un ensemble K et qu'on fait opérer G sur K de manière triviale, on cherche le plus petit entier p et une (ou plusieurs) fonction invariante $f : E^p \to K$. Cette recherche est la recherche d'invariant pour notre action de groupe et dans ce cas précis pour la géométrie que l'on considère.

Cette recherche d'invariant permet la classification des figures. Si on se donne une géométrie par un espace homogène (G, E). On considère l'espace des orbites $\mathcal{P}(E)/G$ (définit par l'action de G sur $\mathcal{P}(E)$) et on cherche suffisamment d'invariant sur chaque orbite pour les caractériser (puisqu'une figure en géométrie correspond à une orbite de cette action).

Références

[1] G. Berhuy. *Algèbre : le grand combat*. Calvage & Mounet, 2018.

[2] J. Calais. *Éléments de la théorie des groupes*. puf, 1984.

[3] P. Caldero and J. Germoni. *Histoires hédonistes de groupes et de géométries, tome 1*. Calvage et Mounet, 2013.

[4] S. Al Fakir. *Algèbre et théorie des nombres*. ellipse, 2003.

[5] X. Gourdon. *Algèbre*. Les maths en tête. Ellipses, 2009.

[6] G. Laville. *Géométrie pour le capes et l'agrégation*. ellipse, 1998.

[7] D. Perrrin. *Cours d'algèbre*. Ellipse, 1996.

[8] F. Ulmer. *Théorie des groupes*. ellipses, 2012.