Structures quotients - Actions de groupes

Table des matières

I Structures quotients

1) Relations d'équivalence, passage au quotient

Soit E un ensemble quelconque et $\mathcal{R}$ une **relation d'équivalence** sur E, c'est-à-dire une relation binaire (formellement, une partie de $E \times E$, et on note $x\mathcal{R}y$ pour signifier qu'un couple (x, y) est en relation) qui vérifie les propriétés suivantes :

- Réflexivité : $\forall x \in E,\ x\mathcal{R}x$;
- Symétrie : $\forall (x, y) \in E^2,\ (x\mathcal{R}y \implies y\mathcal{R}x)$;
- Transitivité : $\forall (x, y, z) \in E^3,\ (x\mathcal{R}y \text{ et } y\mathcal{R}z) \implies (x\mathcal{R}z)$.

Notation
Pour tout $x \in E$, on notera $cl(x)$ la **classe d'équivalence** de x pour la relation $\mathcal{R}$, définie par

$$cl(x) = \{y \in E,\ x\mathcal{R}y\}.$$

On parle aussi de "classe d'équivalence modulo $\mathcal{R}$".

Proposition 1 (Partition en classes d'équivalence)
Les classes d'équivalence modulo $\mathcal{R}$ forment une partition de E : elles sont non vides, disjointes ou confondues, et recouvrent tout E.

Preuve
Pour tout $x \in E$, on a $x \in cl(x)$ (par réflexivité), donc $cl(x) \neq \emptyset$.
Soient x, y dans E tels que $cl(x) \cap cl(y) \neq \emptyset$. Cela signifie qu'il existe $z \in cl(x) \cap cl(y)$, c'est-à-dire $x\mathcal{R}z$ et $y\mathcal{R}z$, donc par symétrie et transitivité $x\mathcal{R}y$.
On a alors $cl(x) = cl(y)$ car pour tout $t \in E$:

$$t \in cl(x) \iff x\mathcal{R}t \underset{\text{car } x\mathcal{R}y}{\iff} y\mathcal{R}t \iff t \in cl(y).$$

Donc les classes modulo $\mathcal{R}$ sont soit disjointes, soit confondues. Enfin, la réunion des classes forme E tout entier, car tout $x \in E$ est dans une (unique) classe : $cl(x)$.

Définition 2 (Ensemble quotient)
L'ensemble quotient $E/\mathcal{R}$ est l'ensemble des classes modulo $\mathcal{R}$:

$$E/\mathcal{R} = \{cl(x),\ x \in E\}.$$

Théorème 3 (Théorème de factorisation)
Soit $f : E \to F$ une application quelconque entre deux ensembles, et $\mathcal{R}$ une relation d'équivalence sur E.

(i) Si f est constante sur les classes d'équivalence modulo $\mathcal{R}$ (i.e. $x\mathcal{R}y \implies f(x) = f(y)$), alors il existe une application $\overline{f} : E/\mathcal{R} \to F$ telle que $f = \overline{f} \circ \pi$, où $\pi : \begin{cases} E & \longrightarrow & E/\mathcal{R} \\ x & \longmapsto & cl(x) \end{cases}$ est la surjection canonique. On a alors $Im(\overline{f}) = Im(f)$.

(ii) Si on a de plus ($x\mathcal{R}y \iff f(x) = f(y)$), alors $\overline{f}$ est injective, donc elle définit une bijection entre $E/\mathcal{R}$ et $Im(f)$.

Vocabulaire
On dit que $\overline{f}$ est obtenue par **passage au quotient** de f. Cette nouvelle application agit sur les classes modulo $\mathcal{R}$ et pas directement sur les éléments de E. Ainsi pour tout $x \in E$, on a

$$f(x) = (\overline{f} \circ \pi)(x) = \overline{f}(cl(x)).$$

Preuve

(i) Remarquons d'abord que $\pi : \left\{ \begin{array}{ccc} E & \longrightarrow & E/\mathcal{R} \\ x & \longmapsto & cl(x) \end{array} \right.$ est bien définie et surjective, car tout élément $\eta \in E/\mathcal{R}$ est non vide, donc est la classe modulo $\mathcal{R}$ d'au moins un élément $x \in E$.
Ensuite, le fait que f soit constante sur chaque classe $\eta \in E/\mathcal{R}$ entraîne que la valeur $f(x)$ ne dépend pas de x lui-même, mais seulement de la classe à laquelle appartient x, donc $cl(x)$. On peut donc poser, pour toute classe $\eta \in E/\mathcal{R}$:

$$\overline{f}(\eta) = f(x),$$

où x est n'importe quel élément de η, ce qui définit bien une application $\overline{f} : E/\mathcal{R} \to F$.
Avec cette application, on a bien $f = \overline{f} \circ \pi$, car pour tout $x \in E$:

$$\overline{f}(\pi(x)) = \overline{f}(cl(x)) = f(x).$$

Enfin, $Im(\overline{f}) = \{\overline{f}(\eta),\ \eta \in E/\mathcal{R}\} = \{f(x),\ x \in E\} = Im(f)$.

(ii) Supposons la propriété $(x\mathcal{R}y \iff f(x) = f(y))$. Pour tout $\eta, \xi \in E/\mathcal{R}$, il existe $x, y \in E$ tels que $\eta = cl(x)$ et $\xi = cl(y)$, donc

$$\overline{f}(\eta) = \overline{f}(\xi) \iff f(x) = f(y) \iff x\mathcal{R}y \iff cl(x) = cl(y) \iff \eta = \xi,$$

ce qui montre que $\overline{f}$ est injective.

2) Relation d'équivalence modulo un sous-groupe

Proposition 4 (Relations d'équivalence modulo un sous-groupe)
Soit $(G, \cdot)$ un groupe et H un sous-groupe de G.

(i) La relation $\mathcal{R}$ définie sur G par

$$\forall (x, y) \in G^2, \qquad x\mathcal{R}y \iff x^{-1}y \in H$$

est une relation d'équivalence.
Pour tout $x \in G$, la classe de x modulo $\mathcal{R}$ est

$$cl_{\mathcal{R}}(x) = xH = \{xh,\ h \in H\}.$$

On l'appelle **classe à gauche modulo H**.

(ii) La relation $\mathcal{R}'$ définie sur G par

$$\forall (x, y) \in G^2, \qquad x\mathcal{R}'y \iff xy^{-1} \in H$$

est une relation d'équivalence.
Pour tout $x \in G$, la classe de x modulo $\mathcal{R}'$ est

$$cl_{\mathcal{R}'}(x) = Hx = \{hx,\ h \in H\}.$$

On l'appelle **classe à droite modulo H**.

Preuve

(i) Soit $(x, y, z) \in G^3$. On a $x^{-1}x = e \in H$, donc $x\mathcal{R}x$.
Si $x\mathcal{R}y$, on a $x^{-1}y \in H$, donc $y^{-1}x = (x^{-1}y)^{-1} \in H$, c'est-à-dire $y\mathcal{R}x$.
Si $x\mathcal{R}y$ et $y \in \mathcal{R}z$, alors $x^{-1}y$ et $y^{-1}z$ sont dans H, donc $x^{-1}z = (x^{-1}y)(y^{-1}z) \in H$, c'est-à-dire $x\mathcal{R}z$.
Enfin, on a

$$y \in cl_{\mathcal{R}}(x) \iff x\mathcal{R}y \iff \exists h \in H,\ x^{-1}y = h \iff \exists h \in H,\ y = xh \iff y \in xH,$$

donc $cl_{\mathcal{R}}(x) = xH$.

(ii) Similaire.

ATTENTION !
Si G est non commutatif, on a $xH \neq Hx$ en général.

Exemple
Dans le groupe symétrique $G = S_3$, si on considère le sous-groupe $H = \langle (1\ 2) \rangle = \{Id, (1\ 2)\}$, alors en notant $x = (1\ 2\ 3)$, on a

$$xH = \{(1\ 2\ 3), (1\ 3)\} \neq Hx = \{(1\ 2\ 3), (2\ 3)\}.$$

Le théorème suivant est une application importante des classes à gauche/à droite modulo un sous-groupe :

Théorème 5 (Théorème de Lagrange)
Soit G un groupe fini et H un sous-groupe de G. Alors, $Card(H)$ divise $Card(G)$.

Preuve
Puisque la relation $\mathcal{R}$ précédemment définie est une relation d'équivalence sur G, les classes à gauche modulo H partitionnent G. Mais G étant fini, ces classes sont en nombre fini, disons $k \in \mathbb{N}^*$.

En notant $x_1, \cdots, x_k$ des représentants respectifs de chaque classe, on a donc $G = \bigcup_{i=1}^{k} x_i H$ (réunion disjointe), d'où $Card(G) = \sum_{i=1}^{k} Card(x_i H)$.

Or, chaque classe xH est clairement en bijection avec H, via l'application $\left\{ \begin{array}{ccc} H & \longrightarrow & xH \\ h & \longmapsto & xh \end{array} \right.$, d'inverse $\left\{ \begin{array}{ccc} xH & \longrightarrow & H \\ y & \longmapsto & x^{-1}y \end{array} \right.$. Donc $Card(xH) = Card(H)$ pour tout $x \in G$, et on déduit

$$Card(G) = \sum_{i=1}^{k} Card(H) = k Card(H),$$

avec $k = Card(G/\mathcal{R}) \in \mathbb{N}^*$, d'où $Card(H)$ divise $Card(G)$.

Corollaire 6 (Ordre des éléments d'un groupe fini)
Si G est un groupe fini, alors $\forall x \in G$, $x^{Card(G)} = e$.

Preuve
Soit $x \in G$. En appliquant le théorème de Lagrange au sous-groupe engendré $H = \langle x \rangle$ (qui est fini car G est fini), on obtient que $ord(x) = Card(H)$ divise $Card(G)$, et donc $x^{Card(G)} = e$.

Remarque
Dans la preuve du théorème de Lagrange, on a mis en évidence que toutes les classes à gauche xH ont même cardinal que H, et c'est également vrai pour les classes à droite Hx (mêmes arguments). Il y a donc **autant de classes à gauche que de classes à droite**, *puisqu'elles partionnent toutes deux l'ensemble G.*

Définition 7 (Indice d'un sous-groupe)
Soit G un groupe fini et H un sous-groupe de G. On appelle **indice de H dans G** *le nombre de classes à gauche (ou à droite) modulo H. On le note*

$$[G : H] = Card(G/H),$$

où G/H désigne un des deux ensembles quotients $G/\mathcal{R}$ ou $G/\mathcal{R}'$.

3) Sous-groupes distingués, automorphismes intérieurs

G désigne un groupe.

Définition 8 (Sous-groupe distingué)
On dit qu'un sous-groupe $H \subset G$ est **distingué dans G** *(ou* **normal dans G***) lorsque*

$$\forall g \in G, \quad gH = Hg$$

(i.e. lorsque les classes à gauche et à droite modulo H coïncident).

Notation
On notera $H \lhd G$ pour exprimer que H est un sous-groupe distingué dans G.

Proposition 9 (Caractérisation par la conjugaison)
Soit H un sous-groupe de G. Alors :

$$H \lhd G \iff \forall g \in G,\ gHg^{-1} \subset H,$$

où $gHg^{-1} = \{ghg^{-1},\ h \in H\}$.
En d'autres termes, H est distingué dans G si, et seulement si H est stable par conjugaison.

Preuve
Si $H \lhd G$, alors pour tout $g \in G$ et $h \in H$, on a $gh \in gH = Hg$, donc il existe $h' \in H$ tel que $gh = h'g$. D'où $ghg^{-1} = h' \in H$.
Réciproquement, si H est stable par conjugaison, alors pour tout $g \in G$ et $h \in H$, $gh = (ghg^{-1})g \in Hg$, donc $gH \subset Hg$, et $hg = g(g^{-1}hg) \in gH$, donc $Hg \subset gH$, et finalement $gH = Hg$, donc $H \lhd G$.

Remarque

- $H \lhd G \iff \forall g \in G,\ \varphi_g(H) \subset H$, *où* $\varphi_g : \left\{ \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & gxg^{-1} \end{array} \right.$ *est appelé* **automorphisme intérieur** *de G associé à g.*
  Ainsi, H est distingué dans G si, et seulement si H est stable par tous les automorphismes intérieurs de G.
- *On a $(\forall g \in G,\ \varphi_g(H) \subset H) \iff (\forall g \in G,\ \varphi_g(H) = H)$.*
  En effet, si on a $(\forall g \in G,\ \varphi_g(H) \subset H)$, alors pour tout $g \in G$, on a $\varphi_{g^{-1}}(H) \subset H$ (puisque $g^{-1} \in G$), c'est-à-dire $(\varphi_g)^{-1}(H) \subset H$, ce qui entraîne $H \subset \varphi_g(H)$.

Exemple

- Si G est commutatif, alors tout sous-groupe H est évidemment distingué dans G.
- Le centre d'un groupe G, noté $Z(G) = \{x \in G,\ \forall g \in G,\ gx = xg\}$ est toujours un sous-groupe distingué de G.
  En effet, pour tout $g \in G$ et $x \in Z(G)$, on a $gxg^{-1} = (gx)g^{-1} = (xg)g^{-1} = x \in Z(G)$.
- Si $f : G \to G'$ est un morphisme de groupes, alors le noyau $Ker(f)$ est toujours un sous-groupe distingué de G.
  En effet, pour tout $g \in G$ et $x \in Ker(f)$, on a $gxg^{-1} \in Ker(f)$ car

$$f(gxg^{-1}) = f(g)\underbrace{f(x)}_{=e'}f(g^{-1}) = f(g)f(g^{-1}) = f(gg^{-1}) = f(e) = e'.$$

4) Groupes quotients

Notation
Si $H \lhd G$, alors pour tout $x \in G$, on notera

$$\overline{x} = xH = Hx$$

la classe à gauche **et** à droite de x modulo H.

Le théorème suivant justifie l'intérêt de la notion de sous-groupe distingué :

Théorème 10 (Structure de groupe quotient)
Soit G un groupe et $H \lhd G$. Alors, l'ensemble quotient G/H (des classes à gauche **et** *à droite) est un groupe pour la loi de composition interne définie par :*

$$\cdot : \left\{ \begin{array}{ccc} G/H \times G/H & \longrightarrow & G/H \\ (\overline{x}, \overline{y}) & \longmapsto & \overline{x} \cdot \overline{y} = \overline{xy} \end{array} \right. .$$

L'élément neutre de ce groupe est $\overline{e} = H$.
De plus, l'application $\pi : \left\{ \begin{array}{ccc} G & \longrightarrow & G/H \\ x & \longmapsto & \overline{x} \end{array} \right.$ est alors un morphisme de groupes surjectif, appelé **surjection canonique modulo H**.

Preuve
Le point délicat est de vérifier que la loi de composition interne annoncée est bien définie, c'est-à-dire de s'assurer que $\overline{xy}$ ne dépend pas des représentants choisis dans $\overline{x}$ et $\overline{y}$.
Soit donc x, x', y, y' dans G tels que $\overline{x} = \overline{x'}$ et $\overline{y} = \overline{y'}$. On a $x^{-1}x'$ et $y^{-1}y'$ dans H, donc

$$(xy)^{-1}(x'y') = y^{-1}x^{-1}x'y' = \underbrace{\big(y^{-1}(x^{-1}x')y\big)}_{\in H \text{ car } H \lhd G} \underbrace{\big(y^{-1}y'\big)}_{\in H} \in H,$$

donc $(xy)\mathcal{R}(x'y')$, c'est-à-dire $\overline{xy} = \overline{x'y'}$. La loi de composition interne sur G/H est donc bien définie.
Ensuite, il est facile de vérifier que cette loi est associative, que $\overline{e}$ est neutre, et que pour tout $x \in G$, $\overline{x^{-1}}$ est le symétrique de $\overline{x}$.
Enfin, π est un morphisme de groupes car

$$\forall (x, y) \in G^2, \quad \pi(xy) = \overline{xy} = \overline{x} \cdot \overline{y} = \pi(x)\pi(y).$$

ATTENTION !
Si H est un sous-groupe de G quelconque, alors G/H ne peut pas être muni d'une structure de groupe en général, car le produit de deux classes n'est pas bien défini (sa valeur peut dépendre des représentants choisis).

Exemple

- Si $G = (\mathbb{Z}, +)$ et $H = n\mathbb{Z}$ avec $n \in \mathbb{N}$ (rappelons que tous les sous-groupes de $\mathbb{Z}$ sont de cette forme), alors $H \lhd G$ (puisque G est commutatif), donc l'ensemble quotient $G/H = \mathbb{Z}/n\mathbb{Z}$ possède une structure de groupe additif :

  $$+ : \left\{ \begin{array}{ccc} \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} & \longrightarrow & \mathbb{Z}/n\mathbb{Z} \\ (\overline{x}, \overline{y}) & \longmapsto & \overline{x} + \overline{y} = \overline{x + y} \end{array} \right. .$$

  Ici, les classes sont définies par

  $$\forall x \in \mathbb{Z}, \qquad \overline{x} = x + H = H + x = x + n\mathbb{Z}.$$

- Pour tout morphisme de groupes $f : G \to G'$, $Ker(f) \lhd G$, donc $G/Ker(f)$ est un groupe, dont les éléments sont :

  $$\forall x \in G, \qquad \overline{x} = x(Ker(f)) = \{xu,\ u \in Ker(f)\}.$$

5) Théorème d'isomorphisme

Théorème 11 (Théorème d'isomorphisme pour les groupes)
Soit $f : G \to G'$ un morphisme de groupes. Alors, les groupes $G/Ker(f)$ et $Im(f)$ sont isomorphes, via l'isomorphisme

$$\overline{f} : \left\{ \begin{array}{ccc} G/Ker(f) & \longrightarrow & Im(f) \\ \overline{x} & \longmapsto & f(x) \end{array} \right. .$$

Preuve
C'est un cas particulier du théorème de factorisation. En notant $\mathcal{R}$ la relation d'équivalence sur G

modulo le sous-groupe distingué $Ker(f)$, le morphisme de groupes $f : G \to G'$ vérifie :

$$x\mathcal{R}y \iff x^{-1}y \in Ker(f) \iff f(x^{-1}y) = e' \iff f(x) = f(y),$$

donc l'application f passe au quotient en une bijection :

$$\overline{f} : \left\{ \begin{array}{ccc} G/Ker(f) & \longrightarrow & Im(f) \\ \overline{x} & \longmapsto & f(x) \end{array} \right. .$$

Reste à vérifier que $\overline{f}$ est un morphisme de groupes :

$$\overline{f}(\overline{x}\ \overline{y}) = \overline{f}(\overline{xy}) = f(xy) = f(x)f(y) = \overline{f}(\overline{x})\overline{f}(\overline{y}).$$

Notation
On notera $A \simeq B$ pour exprimer que deux groupes A et B sont isomorphes.

Exemple

- Pour $n \geq 2$, la signature $\varepsilon : (S_n, \circ) \to (\{-1, 1\}, \times)$ est un morphisme de groupes surjectif, de noyau $Ker(\varepsilon) = \{\sigma \in S_n,\ \varepsilon(\sigma) = 1\} = A_n$, le "groupe alterné d'ordre n". Donc $A_n \lhd S_n$, et $S_n/A_n \simeq \{-1, 1\}$.
- Pour $n \neq 1$, $\det : (GL_n(\mathbb{R}), \times) \to (\mathbb{R}^*, \times)$ est un morphismes de groupes surjectif, avec $Ker(\det) = \{A \in \mathcal{M}_n(\mathbb{R}),\ \det(M) = 1\} = SL_n(\mathbb{R})$, donc $SL_n(\mathbb{R}) \lhd GL_n(\mathbb{R})$ et $GL_n(\mathbb{R})/SL_n(\mathbb{R}) \simeq \mathbb{R}^*$.
- Pour $n \neq 1$, $z \mapsto z^n$ est un automorphisme du groupe $(\mathbb{C}^*, \times)$, de noyau $\mathbb{U}_n = \{z \in \mathbb{C},\ z^n = 1\}$, donc $\mathbb{U}_n \lhd \mathbb{C}^*$ et $\mathbb{C}^*/\mathbb{U}_n \simeq \mathbb{C}^*$.
- **Important** : tout groupe cyclique G (i.e. monogène et fini) est isomorphe à $(\mathbb{Z}/n\mathbb{Z}, +)$, où $n = Card(G)$.
  En effet, si $G = \langle a \rangle = \{e, a, \cdots, a^{n-1}\}$, avec $n = ord(a)$, alors l'application $f : \left\{ \begin{array}{ccc} (\mathbb{Z}, +) & \longrightarrow & (G, \cdot) \\ k & \longmapsto & a^k \end{array} \right.$
  est un morphisme de groupes surjectif, de noyau $Ker(f) = \{k \in \mathbb{Z},\ a^k = e\} = n\mathbb{Z}$ (les multiples de l'ordre de a), donc f passe au quotient, en un isomorphisme :

  $$\overline{f} : \left\{ \begin{array}{ccc} (\mathbb{Z}/n\mathbb{Z}, +) & \longrightarrow & (G, \cdot) \\ \overline{k} & \longmapsto & a^k \end{array} \right. ,$$

  ce qui montre que $G \simeq \mathbb{Z}/n\mathbb{Z}$.

Remarque
Tout groupe G monogène et infini est isomorphe à $(\mathbb{Z}, +)$ car l'application $f : \left\{ \begin{array}{ccc} (\mathbb{Z}, +) & \longrightarrow & (G, \cdot) = \langle a \rangle \\ k & \longmapsto & a^k \end{array} \right.$ est déjà un isomorphisme de groupes dans ces conditions.
En effet, $Ker(f) = \{k \in \mathbb{Z},\ a^k = e\} = \{0\}$, sinon l'élément a serait d'ordre fini, et donc $G = \langle a \rangle$ serait fini.

6) Anneaux quotients

Dans la suite, on considère un anneau $(A, +, \times)$ commutatif, dont les éléments neutres respectifs sont notés 0 et 1.
On a vu que pour tout sous-groupe I de $(A, +)$, l'ensemble A/I possède une structure de groupe (puisque la commutativité de $(A, +)$ entraîne que $I \lhd A$).

On a donc défini une somme sur les classes :

$$+ : \left\{ \begin{array}{ccc} A/I \times A/I & \longrightarrow & A/I \\ (\overline{x}, \overline{y}) & \longmapsto & \overline{x} + \overline{y} = \overline{x + y} \end{array} \right. ,$$

où pour tout $x \in A$, $\overline{x} = x + I = I + x$ est la classe de x modulo I.
La question qui se pose naturellement est alors : peut-on également munir A/I d'une structure d'anneau (commutatif) ? La réponse est oui si le sous-groupe $(I, +)$ possède une propriété supplémentaire : la **propriété d'absorption** ($\forall a \in A,\ \forall x \in I,\ ax \in I$).

On dispose donc du théorème suivant :

Théorème 12 (Structure d'anneau quotient)
Soit $(A,+,\times)$ un anneau commutatif et soit I un **idéal** *de A (sous-groupe de $(A,+)$ tel que $\forall a \in A,\ \forall x \in I,\ ax \in I$). Alors A/I possède une structure d'anneau commutatif, pour les lois :*

$$+ : \left\{ \begin{array}{ccc} A/I \times A/I & \longrightarrow & A/I \\ (\overline{x},\overline{y}) & \longmapsto & \overline{x}+\overline{y}=\overline{x+y} \end{array} \right. ,$$

$$\times : \left\{ \begin{array}{ccc} A/I \times A/I & \longrightarrow & A/I \\ (\overline{x},\overline{y}) & \longmapsto & \overline{x}\times\overline{y}=\overline{xy} \end{array} \right. .$$

Les neutres respectifs de ces deux lois sont $\overline{0}=I$ et $\overline{1}=1+I$.
Enfin, la surjection canonique $\pi : \left\{ \begin{array}{ccc} A & \longrightarrow & A/I \\ x & \longmapsto & \overline{x} \end{array} \right.$ est un morphisme d'anneaux.

Preuve
On sait déjà que $(A/I,+)$ est un groupe commutatif.
On cherche à donner un sens au produit de deux classes, et il faut pour cela que le résultat $\overline{xy}$ ne dépende pas des représentants choisis dans les classes $\overline{x}$ et $\overline{y}$. Vérifions-le : si $\overline{x}=\overline{x'}$ et $\overline{y}=\overline{y'}$, alors il existe $(i,j) \in I^2$ tels que $x'=x+i$ et $y'=y+j$ donc

$$x'y' = xy + \underbrace{(xj+iy+ij)}_{\in I \text{ car } I \text{ idéal}},$$

donc $\overline{x'y'}=\overline{xy}$, ce qui montre la bonne définition de la loi $\times$ sur l'ensemble quotient A/I.
Reste à vérifier que cette loi $\times$ est associative, commutative, distributive sur $+$, et de neutre $\overline{1}$, mais tout cela est élémentaire.

Remarque
Si A n'est pas commutatif, alors on peut quand même fabriquer une structure d'anneau sur le quotient A/I, du moment que I est un idéal **bilatère** *de A, c'est-à-dire que I est un sous-groupe de $(A,+)$ tel que $\forall a \in A,\ \forall x \in I,\ ax \in I$* **et** *$xa \in I$.*
Le programme de l'agrégation interne se limite au cas des quotients d'anneaux commutatifs.

Théorème 13 (Théorème d'isomorphisme pour les anneaux)
Si $f : A \to A'$ est un morphisme d'anneaux (avec A commutatif), alors les anneaux $A/Ker(f)$ et $Im(f)$ sont isomorphes, via l'isomorphisme

$$\overline{f} : \left\{ \begin{array}{ccc} A/Ker(f) & \longrightarrow & Im(f) \\ \overline{x} & \longmapsto & \overline{f}(\overline{x})=f(x) \end{array} \right. .$$

Preuve
On sait que $Ker(f)$ est un idéal de A, donc $A/Ker(f)$ est bien un anneau. De plus, d'après le théorème de factorisation pour les groupes, on a un isomorphisme de groupes additifs :

$$\overline{f} : \left\{ \begin{array}{ccc} A/Ker(f) & \longrightarrow & Im(f) \\ \overline{x} & \longmapsto & \overline{f}(\overline{x})=f(x) \end{array} \right. .$$

Reste à vérifier que $\overline{f}$ est en fait un morphisme d'anneaux, ce qui est élémentaire (on obtient facilement $\overline{f}(\overline{1})=1$ et $\overline{f}(\overline{x}\times\overline{y})=\overline{f}(\overline{x})\overline{f}(\overline{y})$).

Application : le théorème chinois : si $m \geq 1$ et $n \geq 1$ sont deux entiers premiers entre eux, alors le morphisme d'anneaux

$$f : \left\{ \begin{array}{ccc} \mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z} \\ x & \longmapsto & (\dot{x},\hat{x}) \end{array} \right.$$

de noyau $Ker(f)=mn\mathbb{Z}$, passe au quotient en un isomorphisme d'anneaux

$$\overline{f} : \left\{ \begin{array}{ccc} \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & Im(f) \\ \overline{x} & \longmapsto & (\dot{x},\hat{x}) \end{array} \right. .$$

Or, $Im(f) \subset \mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$ et par isomorphisme, $Card(Im(f)) = Card(\mathbb{Z}/mn\mathbb{Z}) = mn = Card(\mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z})$, donc $Im(f) = \mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z}$, d'où un isomorphisme :

$$\overline{f} : \left\{ \begin{array}{ccc} \mathbb{Z}/mn\mathbb{Z} & \longrightarrow & \mathbb{Z}/m\mathbb{Z}\times\mathbb{Z}/n\mathbb{Z} \\ \overline{x} & \longmapsto & (\dot{x},\hat{x}) \end{array} \right. .$$

7) Espaces vectoriels quotients

Ici, $\mathbb{K}$ désigne un corps.
Tout comme pour les anneaux, la structure d'espace vectoriel contient celle de groupe additif, donc étant donné un $\mathbb{K}$-espace vectoriel E et un sous-espace vectoriel F, on a en particulier un groupe additif E/F, puisque F est un sous-groupe distingué de $(E,+)$.
Et sans surprise, le groupe quotient E/F possède tout comme E une structure d'espace vectoriel :

Théorème 14 (Structure d'espace vectoriel quotient)
Soit $(E,+,\cdot)$ un $\mathbb{K}$-espace vectoriel et F un sous-espace vectoriel de E. Alors E/F possède une structure de $\mathbb{K}$-espace vectoriel, pour les lois :

$$+ : \left\{ \begin{array}{ccc} E/F\times E/F & \longrightarrow & E/F \\ (\overline{x},\overline{y}) & \longmapsto & \overline{x}+\overline{y} = \overline{x+y} \end{array} \right. ,$$

$$\cdot : \left\{ \begin{array}{ccc} \mathbb{K}\times E/F & \longrightarrow & E/F \\ (\lambda,\overline{x}) & \longmapsto & \lambda\cdot\overline{x} = \overline{\lambda\cdot x} \end{array} \right. .$$

Enfin, la surjection canonique $\pi : \left\{ \begin{array}{ccc} E & \longrightarrow & E/F \\ x & \longmapsto & \overline{x} \end{array} \right.$ est une application linéaire.

Preuve
La seule chose à vérifier est que le produit externe $\lambda\cdot\overline{x} = \overline{\lambda\cdot x}$ ne dépend pas du représentant de la classe $\overline{x}$: si on a $\overline{x} = \overline{x'}$, alors $x'-x \in F$, donc

$$\lambda\cdot x' - \lambda\cdot x = \lambda\cdot(x'-x) \in F$$

(car F est un sev de E), donc $\overline{\lambda\cdot x'} = \overline{\lambda\cdot x}$.
Le reste se vérifie immédiatement.

Théorème 15 (Théorème d'isomorphisme pour les espaces vectoriels)
Soit $f : E \to E'$ une application linéaire. Alors les espaces vectoriels $E/Ker(f)$ et $Im(f)$ sont isomorphes, via l'isomorphisme

$$\overline{f} : \left\{ \begin{array}{ccc} E/Ker(f) & \longrightarrow & Im(f) \\ \overline{x} & \longmapsto & \overline{f}(\overline{x}) = f(x) \end{array} \right. .$$

Preuve
On sait que $Ker(f)$ est un sev de E, donc $E/Ker(f)$ est bien un espace vectoriel. De plus, d'après le théorème de factorisation pour les groupes, on a un isomorphisme de groupes additifs :

$$\overline{f} : \left\{ \begin{array}{ccc} E/Ker(f) & \longrightarrow & Im(f) \\ \overline{x} & \longmapsto & \overline{f}(\overline{x}) = f(x) \end{array} \right. .$$

Reste à vérifier que $\overline{f}$ est en fait une application linéaire, ce qui est immédiat par linéarité de f.

II Actions de groupes

1) Définitions et exemples

Définition 16 (Action d'un groupe sur un ensemble)
Soit E un ensemble et G un groupe (de neutre e). Une **action** *de G sur E (ou* **opération** *de G sur E) est une application $\bullet : \left\{ \begin{array}{ccc} G \times E & \longrightarrow & E \\ (g,x) & \longmapsto & g \bullet x \end{array} \right.$ qui vérifie :*

(i) $\forall x \in E,\ e \bullet x = x$;

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

Vocabulaire
On parle aussi "d'action à gauche" d'un groupe G sur un ensemble E.

Notation
Pour tout ensemble E, on notera $S(E)$ l'ensemble des bijections de E. $(S(E), \circ)$ est un groupe.

Proposition 17 (Formulation équivalente d'une action de groupe)
La donnée d'une action d'un groupe G sur un ensemble E est équivalent à la donnée d'un morphisme de groupes

$$\rho : \left\{ \begin{array}{ccc} G & \longrightarrow & S(E) \\ g & \longmapsto & \rho(g) \end{array} \right. ,$$

en posant $\rho(g)(x) = g \bullet x$ pour tout $(g,x) \in G \times E$.

Preuve

$\boxed{\Rightarrow}$ Si on a une action $\bullet : \left\{ \begin{array}{ccc} G \times E & \longrightarrow & E \\ (g,x) & \longmapsto & g \bullet x \end{array} \right.$, alors pour tout $g \in G$, l'application $\rho(g) : \left\{ \begin{array}{ccc} E & \longrightarrow & E \\ x & \longmapsto & g \bullet x \end{array} \right.$ est une bijection, d'inverse $\rho(g^{-1})$, puisque

$$\forall x \in E, \quad \left(\rho(g^{-1}) \circ \rho(g)\right)(x) = g^{-1} \bullet (g \bullet x) = (g^{-1}g) \bullet x = e \bullet x = x,$$

$$\left(\rho(g) \circ \rho(g^{-1})\right)(x) = g \bullet (g^{-1} \bullet x) = (gg^{-1}) \bullet x = e \bullet x = x,$$

c'est-à-dire $\rho(g^{-1}) \circ \rho(g) = \rho(g) \circ \rho(g^{-1}) = Id_E$.
Cela permet de définir une application $\rho : \left\{ \begin{array}{ccc} G & \longrightarrow & S(E) \\ g & \longmapsto & \rho(g) \end{array} \right.$, qui est en fait un morphisme de groupes car :

$$\forall (g,g') \in G^2,\ \forall x \in E, \qquad (\rho(g) \circ \rho(g'))(x) = g \bullet (g' \bullet x) = (gg') \bullet x = \rho(gg')(x),$$

c'est-à-dire $\rho(g) \circ \rho(g') = \rho(gg')$.

$\boxed{\Leftarrow}$ Si $\rho : \left\{ \begin{array}{ccc} G & \longrightarrow & S(E) \\ g & \longmapsto & \rho(g) \end{array} \right.$ est un morphisme de groupes, alors en considérant

$$\bullet : \left\{ \begin{array}{ccc} G \times E & \longrightarrow & E \\ (g,x) & \longmapsto & g \bullet x = \rho(g)(x) \end{array} \right. ,$$

on a bien une action de G sur E car pour tout $(x,g,g') \in E \times G \times G$:

$$e \bullet x = \rho(e)(x) = Id_E(x) = x,$$

$$g' \bullet (g \bullet x) = \rho(g')\left(\rho(g)(x)\right) = \left(\rho(g') \circ \rho(g)\right)(x) = \rho(g'g)(x) = (g'g) \bullet x.$$

Remarque
On peut aussi définir des "actions à droite" :

$$\bullet : \left\{ \begin{array}{ccc} E \times G & \longrightarrow & E \\ (x,g) & \longmapsto & x \bullet g \end{array} \right. ,$$

qui vérifient $x \bullet e = x$ et $(x \bullet g) \bullet g' = x \bullet (gg')$, et cela revient à se donner un **anti-morphisme** *de groupes, c'est-à-dire une application*

$$\tilde{\rho} : \left\{ \begin{array}{ccc} G & \longrightarrow & S(E) \\ g & \longmapsto & \tilde{\rho}(g) \end{array} \right.$$

telle que $\tilde{\rho}(gg') = \tilde{\rho}(g') \circ \tilde{\rho}(g)$ pour tout $(g, g') \in G^2$.

Définition 18 (Différents types d'actions de groupe)

(*i*) *Une action est dite* **fidèle** *lorsque le morphisme de groupes $\rho : G \to S(E)$ est injectif. Cela revient à dire*

$$(\forall x \in E,\ g \bullet x = x) \implies g = e$$

(e est le seul élément de G qui fixe tous les éléments de E).

(*ii*) *Une action est dite* **transitive** *lorsque : lorsque pour tout $(x, y) \in E^2$, il existe au moins un $g \in G$ tel que $y = g \bullet x$.*

(*iii*) *Une action est dite* **simple** *(ou* **libre***) lorsque pour tout $(x, y) \in E^2$, il existe au plus un $g \in G$ tel que $y = g \bullet x$.*

(*iv*) *Une action est dite* **simplement transitive** *lorsque pour tout $(x, y) \in E^2$, il existe un unique $g \in G$ tel que $y = g \bullet x$.*

Remarque ("Libre implique fidèle")
Toute action libre est fidèle.
En effet, si l'action est libre, alors en posant $y = x$ dans la définition, on obtient que pour tout $x \in E$, il existe au plus un $g \in G$ tel que $x = g \bullet x$: il s'agit de $g = e$. On a donc bien l'implication

$$(\forall x \in E,\ g \bullet x = x) \implies g = e.$$

qui est la définition d'une action fidèle.

Exemple (Exemples importants d'actions de groupes)

(*i*) **Action d'un groupe G sur lui-même par translation** :

$$\bullet : \left\{ \begin{array}{ccc} G \times G & \longrightarrow & G \\ (g, x) & \longmapsto & gx \end{array} \right. .$$

Ici, pour tout $g \in G$, $\rho(g) : \left\{ \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & gx \end{array} \right. \in S(G)$ n'est pas un morphisme de groupes en général.
Cette action est simplement transitive (donc fidèle, libre et transitive), puisque

$$\forall (x, y) \in G^2, \qquad y = gx \iff g = yx^{-1}.$$

(*ii*) **Action d'un groupe G sur lui-même par conjugaison** :

$$\bullet : \left\{ \begin{array}{ccc} G \times G & \longrightarrow & G \\ (g, x) & \longmapsto & gxg^{-1} \end{array} \right. .$$

Ici, pour tout $g \in G$, $\rho(g) : \left\{ \begin{array}{ccc} G & \longrightarrow & G \\ x & \longmapsto & gxg^{-1} \end{array} \right. \in Aut(G)$ est l'automorphisme intérieur associé à G.
On notera $\varphi_g = \rho(g)$.
Cette action n'est pas fidèle (donc pas libre) et pas transitive en général :

* si par exemple G est commutatif, alors $\varphi_g(x) = x$ pour tout $x \in G$, c'est-à-dire $\rho(g) = Id$ pour tout $g \in G$, ce qui montre que le morphisme $\rho : G \to Aut(G)$ n'est pas injectif. Donc l'action n'est pas fidèle dans ce cas (c'est certes un cas extrême mais il y en a d'autres).
* étant donnés $x, y \in G^2$, il n'existe pas toujours $g \in G$ tel que $y = gxg^{-1}$ (par exemple, si $G = GL_n(\mathbb{K})$, alors deux matrices inversibles ne sont pas nécessairement semblables), donc l'action n'est pas transitive en général.

(*iii*) **Action du groupe symétrique** $(S(E),\circ)$ **sur un ensemble** E :

$$\bullet : \left\{ \begin{array}{ccc} S(E)\times E & \longrightarrow & E \\ (\sigma,x) & \longmapsto & \sigma(x) \end{array} \right.$$

(l'action consiste à permuter les éléments de E).
Ici, pour tout $\sigma\in S(E)$, $\rho(\sigma) : \left\{ \begin{array}{ccc} E & \longrightarrow & E \\ x & \longmapsto & \sigma(x) \end{array} \right.$, donc $\rho(\sigma)=\sigma$.
Cette action est fidèle car $\rho = Id_{S(E)}$ est injectif.
Elle est transitive car pour tout $(x,y)\in E^2$, il existe une permutation $\sigma\in S(E)$ telle que $y=\sigma(x)$ (par exemple, $\sigma=\tau_{x,y}$, la transposition qui échange x et y).
Mais elle n'est pas simple en général, car plusieurs permutations σ peuvent envoyer x sur y.

(*iv*) **Action du groupe linéaire** $(GL(E),\circ)$ **sur un espace vectoriel** E :

$$\bullet : \left\{ \begin{array}{ccc} GL(E)\times E & \longrightarrow & E \\ (u,x) & \longmapsto & u(x) \end{array} \right. .$$

Cette action est fidèle ($\rho : u\mapsto u$), mais pas transitive (si $x\neq 0_E$, alors il n'existe pas d'automorphisme $u\in GL(E)$ tel que $u(x)=0_E$), et pas libre en général (plusieurs automorphismes peuvent envoyer x sur y).

(*v*) **Action du groupe des automorphismes** $(Aut(G),\circ)$ **sur un groupe** G :

$$\bullet : \left\{ \begin{array}{ccc} Aut(G)\times G & \longrightarrow & G \\ (u,x) & \longmapsto & u(x) \end{array} \right. .$$

Cette action est fidèle ($\rho : u\mapsto u$).

(*vi*) **Structure d'espace affine** :
Etant donné un ensemble E et un $\mathbb{K}$-espace vectoriel $\overrightarrow{E}$, on dit que E est un espace affine de direction $\overrightarrow{E}$ lorsque le groupe $(\overrightarrow{E},+)$ "des translations" agit simplement et transitivement sur E, et on note l'action "à droite" :

$$\bullet : \left\{ \begin{array}{ccc} E\times \overrightarrow{E} & \longrightarrow & E \\ (M,\overrightarrow{u}) & \longmapsto & M+\overrightarrow{u} \end{array} \right. .$$

Mais $(\overrightarrow{E},+)$ est commutatif, donc cela revient à une action à gauche.
L'action se traduit par les propriétés suivantes :

* $\forall M\in E,\quad M+\overrightarrow{0}=M$;
* $\forall(\overrightarrow{u},\overrightarrow{v})\in E^2,\quad \forall M\in E,\ (M+\overrightarrow{u})+\overrightarrow{v}=M+(\overrightarrow{u}+\overrightarrow{v})$.

Et le fait que l'action soit simplement transitive signifie que :

$$\forall(M,N)\in E^2,\ \exists!\,\overrightarrow{u}\in E,\quad N=M+\overrightarrow{u}$$

(on note alors $\overrightarrow{u}=\overrightarrow{MN}$).

2) Orbites, stabilisateurs

On considère dans la suite une action d'un groupe G sur un ensemble E :

$$\bullet : \left\{ \begin{array}{ccc} G\times E & \longrightarrow & E \\ (g,x) & \longmapsto & g\bullet x \end{array} \right. .$$

Définition 19 (Orbite)
*Soit $x\in E$. L'***orbite** *de x sous l'action de G est*

$$\mathcal{O}(x)=\{g\bullet x,\ g\in G\}\subset E.$$

Remarque

- *Les orbites des éléments de E sont les classes d'équivalence de la relation d'équivalence $\mathcal{R}$ définie par :*
$$\forall (x,y) \in E^2, \qquad x\mathcal{R}y \iff \exists g \in G,\ y = g \bullet x.$$
Donc **les orbites partitionnent E.**
- *Une action est transitive si et seulement si il y a une seule orbite ($\forall x \in E,\ \mathcal{O}(x) = E$).*

Définition 20 (Stabilisateur)
Soit $x \in E$. Le **stabilisateur** *de x est*
$$G_x = \{g \in G,\ g \bullet x = x\}.$$

Proposition 21 (Propriétés des orbites/stabilisateurs)
(i) Pour tout $x \in E$, G_x est un sous-groupe de G.
(ii) Si $\mathcal{O}(x) = \mathcal{O}(y)$, alors les stabilisateurs G_x et G_y sont conjugués, donc isomorphes.

Preuve

(*i*) Soit $x \in E$. On a $e \in G_x$ car $e \bullet x = x$. D'autre part, si $(g_1, g_2) \in G_x$, alors $g_1^{-1}g_2 \in G_x$ car $(g_1^{-1}g_2) \bullet x = g_1^{-1} \bullet (g_2 \bullet x) = g_1^{-1} \bullet x = g_1^{-1} \bullet (g_1 \bullet x) = (g_1^{-1}g_1) \bullet x = e \bullet x = x$.
Donc G_x est bien un sous-groupe de G.

(*ii*) Si $\mathcal{O}(x) = \mathcal{O}(y)$, alors il existe $h \in G$ tel que $y = h \bullet x$. Montrons alors que G_x et G_y sont conjugués. Pour tout $g \in G$:
$$g \in G_y \iff g \bullet y = y \iff g \bullet (h \bullet x) = h \bullet x \iff (h^{-1}gh) \bullet x = x,$$
donc
$$g \in G_y \iff h^{-1}gh \in G_x,$$
ou encore
$$g \in G_x \iff hgh^{-1} \in G_y,$$
ce qui montre que G_y est l'image de G_x par l'automorphisme intérieur $\varphi_h : \left\{ \begin{array}{ccc} G & \longrightarrow & G \\ g & \longmapsto & hgh^{-1} \end{array} \right.$.
Ainsi, les groupes G_x et G_y sont bien isomorphes.

3) Formule des classes, formule de Burnside

Théorème 22 (Formule des classes)
Si le groupe G et l'ensemble E sont finis, alors pour tout $x \in E$,
$$Card(\mathcal{O}(x))Card(G_x) = Card(G),$$
donc en notant $\mathcal{O}(x_1), \cdots, \mathcal{O}(x_k)$ les orbites distinctes de E :
$$Card(E) = \sum_{i=1}^{k} Card(\mathcal{O}(x_i)) = \sum_{i=1}^{k} \frac{Card(G)}{Card(G_{x_i})}.$$

Preuve
Fixons $x \in E$.
L'idée est de partitionner G en fonction du résultat de l'action $g \bullet x$. L'application
$$f : \left\{ \begin{array}{ccc} G & \longrightarrow & \mathcal{O}(x) \\ g & \longmapsto & g \bullet x \end{array} \right.$$
est surjective et on a la réunion disjointe :
$$G = \bigcup_{y \in \mathcal{O}(x)} f^{-1}(\{y\}).$$
Déterminons alors les "fibres" $f^{-1}(\{y\})$. Pour $y \in \mathcal{O}(x)$ fixé :

* Il existe $g_0 \in G$ tel que $y = g_0 \bullet x$ (la fibre est non vide par surjectivité de f).
* Pour tout $g \in G$:

$$g \in f^{-1}(\{y\}) \iff y = g \bullet x \iff g_0 \bullet x = g \bullet x \iff (g_0^{-1}g) \bullet x = x \iff g_0^{-1}g \in G_x.$$

Ceci montre que chaque fibre $f^{-1}(\{y\})$ est en bijection avec le stabilisateur G_x, via l'application $\begin{cases} f^{-1}(\{y\}) & \longrightarrow & G_x \\ g & \longmapsto & g_0^{-1}g \end{cases}$. Donc

$$\forall y \in \mathcal{O}(x), \quad Card(f^{-1}(\{y\})) = Card(G_x),$$

et on en déduit

$$Card(G) = \sum_{y \in \mathcal{O}(x)} Card(G_x) = Card(\mathcal{O}(x))Card(G_x),$$

puisque les termes de la somme ne dépendent pas de y.
Enfin, la seconde formule résulte du fait que les orbites partitionnent E :

$$E = \bigcup_{i=1}^{k} \mathcal{O}(x_i)$$

(réunion disjointe).

Remarque
Vu qu'à l'intérieur de la même orbite, tous les stabilisateurs sont isomorphes, ils ont le même cardinal. On peut donc réécrire la formule des classes avec les notations suivantes :

- Ω = *ensemble des orbites distinctes de E sous l'action de G*
- *pour toute orbite $\omega \in \Omega$: $c_\omega = Card(G_x)$ pour tout $x \in \omega$*
- *on a alors*

$$Card(E) = Card(G) \sum_{\omega \in \Omega} \frac{1}{c_\omega}$$

Corollaire 23 (Formule de Burnside)
Le nombre d'orbites sous l'action de G vaut

$$k = \frac{1}{Card(G)} \sum_{g \in G} Card(Fix(g)),$$

où pour tout $g \in G$, $Fix(g) = \{x \in E,\ g \bullet x = x\}$.

Remarque
Avec les notations précédentes, la formule de Burnside se réécrit :

$$Card(\Omega) = \frac{1}{Card(G)} \sum_{g \in G} Card(Fix(g)).$$

Preuve
On dénombre les couples (g, x) tels que $g \bullet x = x$ de deux manières, selon g ou selon x.
On note donc $X = \{(g, x) \in G \times E,\ g \bullet x = x\}$. D'une part :

$$X = \bigcup_{g \in G} \{(g, x),\ x \in E,\ g \bullet x = x\} = \bigcup_{g \in G} \{(g, x),\ x \in Fix(g)\},$$

donc (la réunion étant disjointe) :

$$Card(X) = \sum_{g \in G} Card(Fix(g)).$$

D'autre part :

$$X = \bigcup_{x\in E} \{(g,x),\ g\in G,\ g\bullet x = x\} = \bigcup_{x\in E} \{(g,x),\ g\in G_x\},$$

donc (la réunion étant disjointe), on obtient d'après la formule des classes :

$$Card(X) = \sum_{x\in E} Card(G_x) = \sum_{x\in E} \frac{Card(G)}{Card(\mathcal{O}(x))} = Card(G) \sum_{x\in E} \frac{1}{Card(\mathcal{O}(x))}.$$

En notant $\mathcal{O}(x_1), \cdots, \mathcal{O}(x_k)$ les orbites distinctes, on a donc

$$Card(X) = Card(G) \sum_{i=1}^{k} \left(\sum_{x\in\mathcal{O}(x_i)} \frac{1}{Card(\mathcal{O}(x))} \right)$$

$$= Card(G) \sum_{i=1}^{k} \left(\underbrace{\sum_{x\in\mathcal{O}(x_i)} \frac{1}{Card(\mathcal{O}(x_i))}}_{=1} \right) = Card(G) \times k.$$

Finalement, en égalant les deux calculs de $Card(X)$, on obtient :

$$\sum_{g\in G} Card(Fix(g)) = Card(G) \times k.$$