GROUPES ET ANNEAUX 2

Notations générales : sauf indication contraire, G sera toujours un groupe. On travaillera souvent avec un corps $\Bbbk$, qui sera choisit parmi $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ou même $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ pour un nombre premier $p \in \mathbb{N}$.

1. Pré-requis

Les notions suivantes doivent être connues.

(*i*) Sous-groupes de G. **Notation :** $H < G$ signifie "H est un sous-groupe de G".

(*ii*) Ordre d'un élément $g \in G$. **Notation :** $\mathrm{ord}(g)$.

(*iii*) Morphismes de groupes (également appelés homomorphismes), isomorphismes et automorphismes.

(*iv*) $\ker f$ et $\mathrm{im}\, f$ pour un homomorphisme f.

Les résultats suivants doivent être connus.

Théorème 1.1 (Lagrange, Théorème 3.4.12 de HAX501X)**.** *Si G est un groupe fini et $H < G$, alors $|H|$ divise $|G|$.*

Proposition 1.2 (Propositions 3.4.5 & 3.4.7, Exercice 50 de HAX501X)**.** *Soit G un groupe et $g \in G$.*

(*i*) *Si* $\mathrm{ord}(g) = m$*, alors $\langle g \rangle$ est un sous-groupe d'ordre m isomorphe à $\mathbb{Z}/m\mathbb{Z}$.*

(*ii*) *Si $g^n = e$, alors* $\mathrm{ord}(g)$ *divise n.*

(*iii*) *Si* $\mathrm{ord}(g) = m$*, alors* $\mathrm{ord}(g^n) = \frac{m}{\mathrm{pgcd}(m,n)}$ *pour tout $n \in \mathbb{N}$.*

Proposition 1.3 (Proposition 3.3.9 de HAX501X)**.** *Un morphisme de groupes $f : G \to G'$ est injectif si et seulement si* $\ker f = \{e\}$.

2. Quelques exemples de groupes

Exemple 2.1. Voilà quelques exemples importants de groupes.

(*i*) Muni de la multiplication usuelle entre nombres complexes, $\mathbb{C}^\times$ est un groupe. Le sous-groupe

$$\boldsymbol{\mu}_n := \{z \in \mathbb{C}^\times \mid z^n = 1\}$$

est le *groupe des racines nèmes de l'unité*. Il est isomorphe à $\mathbb{Z}/n\mathbb{Z}$ via l'isomorphisme

$$\begin{aligned} f : \mathbb{Z}/n\mathbb{Z} &\to \boldsymbol{\mu}_n \\ [k] &\mapsto e^{\frac{2k\pi \mathrm{i}}{n}}. \end{aligned}$$

(*ii*) Soit $\mathrm{GL}_n(\Bbbk)$ le *groupe général linéaire de dégré n de* $\Bbbk$, qui est par définition le groupe des matrices inversibles de taille $n \times n$ à coefficients dans $\Bbbk$. Si $\Bbbk = \mathbb{F}_p$, alors $\mathrm{GL}_n(\Bbbk)$ est un groupe fini. Pour déterminer son cardinal, on remarque qu'une matrice $X \in \mathrm{GL}_n(\mathbb{F}_p)$ n'est rien d'autre qu'une liste ordonnée de n vecteurs colonne $X_1, \ldots, X_n$ tels que

$$X_1 \neq 0, \quad X_2 \notin \mathbb{F}_p X_1, \quad X_3 \notin \mathrm{vect}_{\mathbb{F}_p}(X_1, X_2), \quad \ldots, \quad X_n \notin \mathrm{vect}_{\mathbb{F}_p}(X_1, \ldots, X_{n-1}).$$

Donc, pour X_1 nous avons $|\mathbb{F}_p^n \smallsetminus \{0\}| = p^n - 1$ choix, pour X_2 nous avons $|\mathbb{F}_p^n \smallsetminus \mathbb{F}_p X_1| = p^n - p$ choix, pour X_3 nous avons $|\mathbb{F}_p^n \smallsetminus \mathrm{vect}_{\mathbb{F}_p}(X_1, X_2)| = p^n - p^2$ choix, etc. Donc

$$|\mathrm{GL}_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p)(p^n - p^2) \cdots (p^n - p^{n-1}).$$

En particulier, pour $p = n = 2$, on trouve $|\mathrm{GL}_2(\mathbb{F}_2)| = 6$. On verra que $\mathrm{GL}_2(\mathbb{F}_2) \cong \mathfrak{S}_3$.

(*iii*) On fixe $n > 1$. Soit $R \in \mathrm{GL}_2(\mathbb{R})$ la rotation d'un angle $\frac{2\pi}{n}$ dans le sens anti-horaire autour de l'origine. Soit S la réflexion par rapport à l'axe des abscisses. En identifiant $\mathbb{R}^2$ avec $\mathbb{C}$, on obtient

$$R(z) = e^{\frac{2\pi \mathrm{i}}{n}} z, \qquad S(z) = \bar{z}.$$

On en déduit que $SR^kS = R^{-k}$ pour tout $k \in \mathbb{Z}$, car

$$S(R^k(S(z))) = S(R^k(\bar{z})) = S(e^{\frac{2k\pi \mathrm{i}}{n}} \bar{z}) = e^{-\frac{2k\pi \mathrm{i}}{n}} z = R^{-k}(z)$$

pour tout $z \in \mathbb{C}$. On prétend que

$$\mathscr{D}_n = \{I, R, \ldots, R^{n-1}\} \cup \{S, RS, \ldots, R^{n-1}S\}$$

est un sous-groupe de $\mathrm{GL}_2(\mathbb{R})$. On remarque que

$$R^i R^j = R^{i+j}, \quad R^i(R^j S) = R^{i+j}S, \quad (R^i S)R^j = R^{i-j}S, \quad (R^i S)(R^j S) = R^{i-j}.$$

Donc $\mathscr{D}_n$ est clos par multiplication. De plus, le premier et le dernier produit impliquent respectivement que

$$(R^i)^{-1} = R^{-i}, \qquad (R^i S)^{-1} = R^i S.$$

Donc $\mathscr{D}_n$ est clos par inversion. Ce groupe s'appelle le *groupe diédral de* $2n$ *éléments*. Si $n > 2$, alors $\mathscr{D}_n$ n'est pas commutatif.

3. Actions

Soit X ensemble et G un groupe.

Définition 3.1. Une *action* de G sur X est une fonction

$$\begin{aligned} G \times X &\to X \\ (g, x) &\mapsto g \cdot x \end{aligned}$$

telle que

(*i*) $e \cdot x = x$ pour tout $x \in X$;

(*ii*) $(gg') \cdot x = g \cdot (g' \cdot x)$ pour tout $g, g' \in G$ et $x \in X$.

De temps en temps, un ensemble muni d'une action d'un groupe G sera appelé un *G-ensemble*.

Exercice 3.2. Si X est un ensemble muni d'une action d'un groupe G, alors la fonction $\rho : G \to \mathfrak{S}_X$ définie par $\rho(g)(x) := g \cdot x$ pour tout $g \in G$ et $x \in X$ est un morphisme de groupes, où $\mathfrak{S}_X$ désigne le groupe des bijections de X. Réciproquement, si $\rho : G \to \mathfrak{S}_X$ est un morphisme de groupes, alors $g \cdot x := \rho(g)(x)$ définit une action de G sur X.

Exemple 3.3. Voilà quelques exemples d'actions de groupes.

(*i*) Le groupe $\mathfrak{S}_n$ agit naturellement sur l'ensemble $\{1, \ldots, n\}$.

(*ii*) On identifie $\Bbbk^n$ avec l'ensemble des vecteurs colonne à coefficients dans $\Bbbk$. Le groupe $\mathrm{GL}_n(\Bbbk)$ agit alors sur $\Bbbk^n$ par produit matriciel, en posant $A \cdot v = Av$ pour tout $A \in \mathrm{GL}_n(\Bbbk)$ et $v \in \Bbbk^n$.

(*iii*) Pour tout $g \in \mathscr{D}_n$ et $\zeta \in \boldsymbol{\mu}_n$, l'élément $g(\zeta)$ est encore une racine $n$ème de l'unité. Afin de le voir, il suffit de le vérifier pour les générateurs $R, S \in \mathscr{D}_n$:

$$R(\zeta)^n = \left(e^{\frac{2\pi \mathrm{i}}{n}}\zeta\right)^n = e^{\frac{2n\pi \mathrm{i}}{n}}\zeta^n = 1, \qquad S(\zeta)^n = \left(\bar{\zeta}\right)^n = \zeta^{-n} = 1.$$

On obtient donc une action de $\mathscr{D}_n$ sur $\boldsymbol{\mu}_n$.

(*iv*) Soit $H < G$ un sous-groupe d'un groupe G.

(a) H agit sur G par le morphisme de groupes $\rho_{\mathrm{L}} : H \to \mathfrak{S}_G$ obtenu en posant $\rho_{\mathrm{L}}(h)(g) := hg$ pour tout $h \in H$ et $g \in G$. Cela est l'*action de H sur G par translation à gauche*.

(b) H agit sur G par le morphisme de groupes $\rho_{\mathrm{R}} : H \to \mathfrak{S}_G$ obtenu en posant $\rho_{\mathrm{R}}(h)(g) := gh^{-1}$ pour tout $h \in H$ et $g \in G$. Cela est l'*action de H sur G par translation à droite*. Le lecteur devra vérifier que la formule précédente est bien cohérente, et qu'en écrivant $h \cdot g = gh$ on n'obtient pas une action.

Dans l'exemple précédent, on a vu qu'un sous-groupe $H < G$ peut agir de deux manières différentes. Finalement, ces actions ne sont pas si différentes que ça. Pour exprimer cela de façon précise, on a besoin d'une définition.

Définition 3.4. Soient X et Y deux G-ensembles. Une fonction $f : X \to Y$ est dite *G-équivariante*, ou une *G–fonction*, si $f(g \cdot x) = g \cdot (f(x))$ pour tout $g \in G$ et $x \in X$.

On peut maintenant exprimer le fait que les actions par translation à droite et à gauche sont "les mêmes".

Exercice 3.5. Soit $H < G$ un sous-groupe. Soit G_{L} l'ensemble G muni de l'action par translations à gauche de H, à savoir, $\rho_{\mathrm{L}}(h)(g) = hg$ pour tout $h \in H$ et $g \in G_{\mathrm{L}}$. Soit G_{R} l'ensemble G muni de l'action par translations à droite de H, à savoir, $\rho_{\mathrm{R}}(h)(g) = gh^{-1}$ pour tout $h \in H$ et $g \in G_{\mathrm{R}}$. Montrer que la fonction $\_^{-1} : G_{\mathrm{L}} \to G_{\mathrm{R}}$ est une bijection H-équivariante.

Si l'ensemble X est muni d'une structure additionnelle, on s'intéresse souvent aux actions qui préservent cette structure.

Définition 3.6. Soit G un groupe.

(*i*) Soit Γ un groupe et $G \times \Gamma \to \Gamma$ une action. On dit que G *agit par homomorphismes* si

$$g \cdot (\gamma\gamma') = (g \cdot \gamma)(g \cdot \gamma')$$

pour tout $g \in G$ et $\gamma, \gamma' \in \Gamma$. Cela arrive si et seulement si la bijection $\rho(g)$ définie dans l'Exercice 3.2 est un morphisme de groupes pour tout $g \in G$. Dans ce cas, $\operatorname{im}\rho < \operatorname{Aut}(\Gamma)$, donc, sans changer de nom, l'action de G sur Γ est donnée par un homomorphisme $\rho : G \to \operatorname{Aut}(\Gamma)$.

(*ii*) Soit V un espace vectoriel sur un corps $\Bbbk$ et $G \times V \to V$ une action. On dit que cette action est *linéaire* si

$$g \cdot (v + v') = g \cdot v + g \cdot v', \qquad g \cdot (\lambda v) = \lambda(g \cdot v)$$

pour tout $g \in G$, $v, v' \in V$ et $\lambda \in \Bbbk$. Cela arrive si et seulement si la bijection $\rho(g)$ définie dans l'Exercice 3.2 est une application linéaire pour tout $g \in G$. Dans ce cas, $\operatorname{im}\rho < \mathrm{GL}_{\Bbbk}(V)$, donc, sans changer de nom, l'action de G sur V est donnée par un homomorphisme $\rho : G \to \mathrm{GL}_{\Bbbk}(V)$.

Exemple 3.7. Voilà des exemples et des non-exemples.

(*i*) L'action d'un sous-groupe $H < G$ sur G par translation à gauche est une action par homomorphismes si et seulement si $H = \{e\}$. En effet,

$$\begin{aligned} & h \cdot (gg') = (h \cdot g)(h \cdot g') && \forall\, h \in H \\ \Leftrightarrow \quad & hgg' = hghg' && \forall\, h \in H \\ \Leftrightarrow \quad & e = (hg)^{-1}(hgg')(g')^{-1} = (hg)^{-1}(hghg')(g')^{-1} = h && \forall\, h \in H. \end{aligned}$$

(*ii*) L'action de $\mathrm{GL}_n(\Bbbk)$ sur $\Bbbk^n$ est clairement linéaire.

L'un des exemples les plus importantes d'actions par homomorphismes est le suivant.

Exemple 3.8. Si $H < G$ est un sous-groupe, alors H agit sur G par le morphisme de groupes $\rho_{\mathrm{C}} : H \to \mathrm{Aut}(G) < \mathfrak{S}_G$ obtenu en posant $\rho_{\mathrm{C}}(h)(g) := hgh^{-1}$ pour tout $h \in H$ et $g \in G$. Cela est l'*action de H sur G par conjugaison*. Il s'agit d'une action par homomorphismes, car

$$h \cdot (gg') = hgg'h^{-1} = hgh^{-1}hg'h^{-1} = (h \cdot g)(h \cdot g')$$

pour tout $h \in H$ et $g, g' \in G$.

L'idée même d'action donne directement des résultats non-triviaux.

Théorème 3.9 (Cayley)**.** *Si G est un groupe d'ordre n, alors G est isomorphe à un sous-groupe de $\mathfrak{S}_n$.*

Démonstration. On considère l'action de G sur lui même par translation à gauche. D'après l'Exercice 3.2, on obtient un morphisme de groupes $\rho_{\mathrm{L}} : G \to \mathfrak{S}_G \cong \mathfrak{S}_n$. Il est clair que

$$g \in \ker \rho_{\mathrm{L}} \Rightarrow \rho_{\mathrm{L}}(g)(e) = e \Rightarrow g = e.$$

Donc ρ est injectif, et $\rho : G \to \mathrm{im}\,\rho < \mathfrak{S}_n$ est isomorphisme. □

Malgré son apparence spectaculaire, le théorème de Cayley n'est pas si puissant que ça. En effet, les sous-groupes d'un groupe symétrique ne sont pas faciles à déterminer.

Exemple 3.10. Posons $\zeta = e^{\frac{2\pi \mathrm{i}}{5}}$. On a $\boldsymbol{\mu}_5 = \{\zeta^1, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$. En faisant agir $\boldsymbol{\mu}_5$ par translation à gauche sur lui même, on obtient un homomorphisme injectif

$$\begin{aligned} \rho_{\mathrm{L}} : \boldsymbol{\mu}_5 &\hookrightarrow \mathfrak{S}_{\boldsymbol{\mu}_5} \cong \mathfrak{S}_5 \\ \zeta^k &\mapsto (1\ 2\ 3\ 4\ 5)^k. \end{aligned}$$

Définition 3.11. Soit X un ensemble muni d'une action d'un groupe G, et soit $x \in X$ un élément.

(*i*) Un sous-ensemble $Y \subset X$ est *stable par G* si $G \cdot Y \subset Y$, où $G \cdot Y$ dénote l'ensemble $\{g \cdot y \mid g \in G, y \in Y\}$.

(*ii*) L'*orbite de x* est $\mathrm{orb}(x) = \{g \cdot x \mid g \in G\} \subset X$. On écrira parfois $G \cdot x$ pour $\mathrm{orb}(x)$. Clairement, $\mathrm{orb}(x)$ est stable par G.

(*iii*) Le *stabilisateur de x* est $\mathrm{st}(x) = \{g \in G \mid g \cdot x = x\}$. On écrira parfois G_x pour $\mathrm{st}(x)$. Clairement, $\mathrm{st}(x)$ est un sous-groupe de G.

(*iv*) On dit que x est un *point fixe* si $g \cdot x = x$ pour tout $g \in G$, c'est-à-dire si $G_x = G$. L'ensemble des points fixes est noté X^G.

(*v*) On dit que l'action est *transitive* si X consiste en une seule orbite, c'est-à-dire si $X = G \cdot x$ pour quelque (en fait pour tout) $x \in X$. Dans ce cas, X est appelé aussi un *espace homogène*.

(*vi*) On dit que l'action est *libre* si tous les stabilisateurs sont triviaux, c'est à dire si $G_x = \{e\}$ pour tout $x \in X$.

Exemple 3.12. Voilà quelques exemples.

(*i*) Le groupe $G = \mathrm{GL}_n(\Bbbk)$ agit naturellement sur $\Bbbk^n$. Si $n = 2$, et si $\{e_1, e_2\}$ dénote la base standard de $\Bbbk^2$, alors $G \cdot e_1 = \Bbbk^2 \smallsetminus \{0\}$, car

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{cases} \begin{pmatrix} x & 0 \\ y & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} & \text{si } x \neq 0, \\ \begin{pmatrix} x & 1 \\ y & 0 \end{pmatrix} \cdot \begin{pmatrix} 1 \\ 0 \end{pmatrix} & \text{si } y \neq 0 \end{cases} \in G \cdot e_1 \qquad \forall \begin{pmatrix} x \\ y \end{pmatrix} \in \Bbbk^2 \smallsetminus \{0\},$$

et $G \cdot 0 = \{0\}$. L'action est donc transitive sur $\Bbbk^2 \smallsetminus \{0\}$, et 0 est l'unique point fixe. De plus,

$$G_{e_1} = \left\{ \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \;\middle|\; b, d \in \Bbbk, d \neq 0 \right\}.$$

Il suit que $\Bbbk^2$ n'est pas un espace homogène, et que l'action n'est pas libre.

(*ii*) Soit $H < G$ un sous-groupe d'un groupe G.

(a) En faisant agir H par translation à gauche, les stabilisateurs sont triviaux, $\mathrm{st}(g) = \{e\}$ pour tout $g \in G$, et les orbites sont les classes à droite, $\mathrm{orb}(g) = Hg = \{hg \mid h \in H\}$ pour tout $g \in G$. Donc l'action est libre, et elle est transitive si et seulement si $H = G$.

(b) En faisant agir H par translation à droite, les stabilisateurs sont triviaux, $\mathrm{st}(g) = \{e\}$ pour tout $g \in G$, et les orbites sont les classes à gauche, $\mathrm{orb}(g) = gH = \{gh \mid h \in H\}$ pour tout $g \in G$. Donc l'action est libre, et elle est transitive si et seulement si $H = G$.

Exercice 3.13 (Exercice 1.(*ii*), Feuille TD1)**.** Soit $\mathbb{P}^{n-1}(\Bbbk)$ l'*espace projectif de dimension* $n-1$ *sur* $\Bbbk$, qui est par définition l'ensemble des droites vectorielles de $\Bbbk^n$. De manière équivalente, $\mathbb{P}^{n-1}(\Bbbk)$ peut être défini comme le quotient de $\Bbbk^n \smallsetminus \{0\}$ par la relation d'équivalence

$$v \sim v' \Leftrightarrow \exists\, \lambda \in \Bbbk \smallsetminus \{0\} : v' = \lambda v.$$

Le groupe $G = \mathrm{GL}_n(\Bbbk)$ agit naturellement sur $\mathbb{P}^{n-1}(\Bbbk)$ par $A \cdot [v] = [Av]$ pour tout $[v] \in \mathbb{P}^1(\Bbbk)$ et $A \in G$. En prenant $n = 2$, montrer que cette action n'est pas libre, mais qu'elle est transitive.

Exercice 3.14 (Exercice 5, Feuille TD1)**.** En utilisant l'action de $\mathrm{GL}_2(\mathbb{F}_2)$ sur l'espace projectif $\mathbb{P}^1(\mathbb{F}_2)$, montrer que $\mathrm{GL}_2(\mathbb{F}_2) \cong \mathfrak{S}_3$.

Il s'avère que les actions transitives et libres sont "uniques".

Exercice 3.15. Soit X un ensemble muni d'une action libre et transitive d'un groupe G, et soit $x \in X$ un de ses éléments. Alors la fonction $\varphi : G \to X$ définie par $\varphi(g) = g \cdot x$ est une bijection G-équivariante.

4. Quotients

Soit X un G-ensemble.

Définition 4.1. Le *quotient de* X *par* G est l'ensemble X/G des orbites de G. La *projection canonique* est la fonction $\pi : X \twoheadrightarrow X/G$ qui à tout $x \in X$ associe son orbite $\mathrm{orb}(x) \in X/G$.

Exemple 4.2. Voilà quelques exemples.

(*i*) Considérons l'action naturelle de $G = \mathrm{GL}_2(\Bbbk)$ sur $X = \Bbbk^2$. Alors, comme vu dans l'Exemple 3.12, on a $X/G = \{\{0\}, \Bbbk^2 \smallsetminus \{0\}\}$.

(*ii*) Le groupe $G = \Bbbk^\times$ agit sur $X = \Bbbk^n \smallsetminus \{0\}$ par multiplication scalaire, en posant $\lambda \cdot v = \lambda v$ pour tout $\lambda \in G$ et $v \in X$. Toute orbite est alors une droite vectorielle privée de l'origine, et $X/G \cong \mathbb{P}^{n-1}(\Bbbk)$.

(*iii*) Soit $H < G$ un sous-groupe d'un groupe G. En utilisant la notation introduite dans l'Exercice 3.5, on obtient les ensembles quotients des classes à gauche $G_{\mathrm{L}}/H = \{Hg \mid g \in G\}$ et celui des classes à droite $G_{\mathrm{R}}/H = \{gH \mid g \in G\}$. On écrira parfois $H\backslash G$ pour G_{L}/H et G/H pour G_{R}/H.

Proposition 4.3. *Si $H < G$ est un sous-groupe d'un groupe G, alors il existe une bijection $H\backslash G \to G/H$.*

Démonstration. On a vu dans l'Exercice 3.5 que l'inversion $\_^{-1} : G_{\mathrm{L}} \to G_{\mathrm{R}}$ définit une bijection H-équivariante. Les orbites sont alors en bijection. □

Exemple 4.4. Pour $G = \mathscr{D}_3$ et $H = \langle S \rangle$, on trouve

$$H\backslash G = \{\{I, S\}, \{R, R^2S\}, \{R^2, RS\}\},$$
$$G/H = \{\{I, S\}, \{R, RS\}, \{R^2, R^2S\}\}.$$

Définition 4.5. L'*indice de H dans G* est $[G : H] := |H\backslash G| = |G/H|$.

On en profite pour rappeler le Théorème 1.1 : si G est fini, alors

$$[G : H] = |G|/|H|,$$

car chacune des orbites gH contient exactement $|H|$ éléments, et il y a, par définition, $[G : H]$ orbites.

Voilà la propriété universelle satisfaite par les quotients, dont la preuve est tautologique.

Proposition 4.6. *Si X est un G-ensemble et Y est un ensemble, alors, pour toute fonction $f : X \to Y$ qui est constante sur les orbites, il existe une unique fonction*

$$\bar{f} : X/G \to Y$$

telle que $\bar{f}(\mathrm{orb}(x)) = f(x)$.

Si $H < G$ est un sous-groupe d'un groupe G, alors une propriété très importante du quotient G/H est le fait qu'il admet encore une action naturelle de G par translation à gauche. En effet, si on pose $g \cdot g'H = gg'H$ pour tout $g \in G$ et $g'H \in G/H$, on peut vérifier facilement qu'il s'agit d'une action. Dans la théorie, cette action joue un rôle de premier plan, car elle est le prototype d'une action transitive.

Lemme 4.7. *Soit X un G-ensemble, et soit $x \in X$ un de ses éléments.*

(*i*) *La fonction $\varphi_x : G/G_x \to G \cdot x$ définie par $\varphi_x(gG_x) = g \cdot x$ pour tout $g \in G$ est une bijection.*

(*ii*) *La bijection $\varphi_x : G/G_x \to G \cdot x$ est G-équivariante par rapport aux actions de G sur G/G_x (par translation à gauche) et sur $G \cdot x$ (par restriction de l'action sur X).*

(*iii*) *Les stabilisateurs des éléments d'une même orbite sont tous conjugués par $G_{g\cdot x} = gG_xg^{-1}$.*

Démonstration. La preuve est évidente, mais on la reproduit ici pour aider le lecteur à retenir les définitions.

(*i*) Si $g'G_x = gG_x$, alors $g' = gs$ pour quelque $s \in G_x$, et

$$g' \cdot x = (gs) \cdot x = g \cdot (s \cdot x) = g \cdot x.$$

Donc la fonction φ_x est bien définie. Elle est surjective par définition d'orbite. Elle est injective car

$$\varphi_x(gG_x) = \varphi_x(g'G_x) \Leftrightarrow g \cdot x = g' \cdot x \Leftrightarrow g^{-1} \cdot (g \cdot x) = g^{-1} \cdot (g' \cdot x)$$
$$\Leftrightarrow x = (g^{-1}g') \cdot x \Leftrightarrow g^{-1}g' \in G_x \Leftrightarrow gG_x = g'G_x.$$

(*ii*) Pour tout $g \in G$ et $g'G_x \in G/G_x$ on a

$$\varphi_x(g \cdot g'G_x) = \varphi_x(gg'G_x) = (gg') \cdot x = g \cdot (g' \cdot x) = g \cdot \varphi_x(g'G_x).$$

(*iii*) Pour tout $g \in G$ on a

$$s \in G_{g \cdot x} \Leftrightarrow s \cdot (g \cdot x) = g \cdot x \Leftrightarrow g^{-1} \cdot (s \cdot (g \cdot x)) = g^{-1} \cdot (g \cdot x) \Leftrightarrow (g^{-1}sg) \cdot x = x$$
$$\Leftrightarrow g^{-1}sg \in G_x \Leftrightarrow s \in gG_xg^{-1}.$$

□

Corollaire 4.8. *Si X est un G-espace homogène, c'est-à-dire un G-espace constitué d'une seule orbite, alors il existe un sous-groupe $H < G$ et une bijection G-équivariante $\varphi : G/H \to X$.*

Démonstration. On choisit $x \in X$, on pose $H = G_x$, et on applique le Lemme 4.7. □

Corollaire 4.9 (Formule des classes)**.** *Soit G un groupe fini et X un G-espace fini.*

(*i*) *Pour tout $x \in X$ on a*

$$|G \cdot x| = [G : G_x].$$

(*ii*) *Si $X = (G \cdot x_1) \sqcup \ldots \sqcup (G \cdot x_n)$, alors*

$$|X| = \sum_{i=1}^{n} |G \cdot x_i| = \sum_{i=1}^{n} \frac{|G|}{|G_{x_i}|}.$$

Démonstration. L'énoncé est une conséquence directe du Lemme 4.7.(*ii*).

(*i*) La fonction

$$\varphi_x : G/G_x \to G \cdot x$$
$$gG_x \mapsto g \cdot x$$

est une bijection, donc $|G \cdot x| = |G/G_x|$. Mais $|G/G_x| = [G : G_x]$ par définition.

(*ii*) Comme $X = (G \cdot x_1) \sqcup \ldots \sqcup (G \cdot x_n)$, on a

$$|X| = \sum_{i=1}^{n} |G \cdot x_i|.$$

En utilisant la bijection φ_x on déduit que $|G \cdot x_i| = |G/G_{x_i}| = |G|/|G_{x_i}|$ pour tout entier $1 \leqslant i \leqslant n$.

□

Exemple 4.10. Voilà quelques exemples d'applications du Corollaire 4.9.

(*i*) Considérons l'espace projectif $\mathbb{P}^1(\Bbbk)$, sur lequel le groupe $\mathrm{GL}_2(\Bbbk)$ agit transitivement, comme vu dans l'Exercice 3.13.(*iii*). Un utilisant le Lemme 4.7, on obtient une bijection $\mathrm{GL}_2(\Bbbk)$-équivariante

$$\mathrm{GL}_2(\Bbbk)/B \to \mathbb{P}^1(\Bbbk),$$

où $B = \mathrm{st}([e_1])$ est le groupe des matrices triangulaires supérieures inversibles.

(*ii*) Le groupe additif $\mathbb{R}$ agit sur le cercle $S^1 \cong \{z \in \mathbb{C} \mid |z| = 1\}$ par rotations, en posant $t \cdot z = e^{2t\pi \mathrm{i}} z$. Clairement, cette action est transitive. De plus, $\mathrm{st}(1) = \mathbb{Z}$. Alors la fonction

$$\begin{aligned} \mathbb{R} &\to S^1 \\ \vartheta &\mapsto e^{2t\pi \mathrm{i}} \end{aligned}$$

définit une bijection entre $\mathbb{R}/\mathbb{Z}$ et S^1.

Exemple 4.11. Soit p un nombre premier et G un groupe fini d'ordre p^n. On note $\mathrm{Z}(G)$ son centre. On fait agir G sur lui même par conjugaison, c'est-à-dire $g \cdot x = gxg^{-1}$ pour tout $g, x \in G$. On note $\mathrm{cl}(g)$ l'orbite de $x \in G$, qui coïncide avec la classe de conjugaison de x. Si $|G|/|\mathrm{st}(x)| > 1$, alors $|G|/|\mathrm{st}(x)| \equiv 0 \pmod p$. Si $|G|/|\mathrm{st}(x)| = 1$, alors $\mathrm{cl}(x) = \{x\}$, donc $x \in \mathrm{Z}(G)$. La formule des classes implique

$$|G| \equiv |\mathrm{Z}(G)| \pmod p.$$

Par conséquent, $|\mathrm{Z}(G)| \equiv 0 \pmod p$. En particulier, $|\mathrm{Z}(G)| \neq 1$. Cela nous permet de montrer que *tout groupe d'ordre p^2 est abélien*. En effet, si $n = 2$, alors $|\mathrm{Z}(G)|$ est soit p, soit p^2. Supposons par l'absurde que $|\mathrm{Z}(G)| = p$. Alors, il existe $x \in G \smallsetminus \mathrm{Z}(G)$. Soit $\mathrm{C}_G(x) = \{g \in G \mid gx = xg\}$ le *centralisateur de x dans G*. C'est facile de voir que $\mathrm{C}_G(x)$ est un sous-groupe de G, qu'il contient le centre $\mathrm{Z}(G)$, et qu'il contient le sous-groupe $\langle x \rangle$ engendré par x. Alors $p = |\mathrm{Z}(G)| < |\mathrm{C}_G(x)| \mid |G| = p^2$, donc $\mathrm{C}_G(x) = G$. Cela signifie que x commute avec tous les éléments de G, donc $x \in \mathrm{Z}(G)$, une contradiction.