5.8. **Le théorème de Jordan–Hölder.** [14] Chaque nombre naturel a une décomposition primaire, qui est unique à une permutation des facteurs près. Quelque chose semblable est vrai pour chaque groupe fini.

On dit qu'un groupe K est *simple* si ses seuls sous-groupes normaux sont les sous-groupes triviaux K et $\{\mathbf{1}_K\}$. Un sous-groupe normal $N \lhd G$ est dit *maximal* si $N \neq G$ et s'il n'y a pas de sous-groupe normal $M \lhd G$ contenant N, sauf $M = N$ et $M = G$. Ou, ce qui est équivalent par le théorème de correspondance, $N \lhd G$ est maximal si et seulement si $N \neq G$ et G/N est simple.

Un des très grands théorèmes du 20-ième siècle est l'achèvement autour de 1981 de la classification de tous les groupes simple finis (à isomorphisme près, bien sûr). La preuve actuelle prend environ 5000 pages ![15] Exemples sont les groupes cycliques C_p, si p est un nombre premier; les groupes Alt_n, si $n > 4$ (un résultat de Galois [4, p.241]); ou les groupes $\mathrm{PGL}(n, \mathbb{F}_q)$, si $(n, q) \neq (2, 2)$ ou $(2, 3)$ [4, p.362] (ici, PGL est le groupe quotient de GL par le sous-groupe normal des matrices scalaire $c\mathbf{1}$), et des généralisations. Il y a plusieures séries de groupes simples dépendantes de paramètres (comme les exemples déjà données), et 28 groupes sporadiques, qui n'appartiennent pas à une série infinie. Le plus grand groupe simple sporadique s'appelle le monstre, et est d'ordre

$$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$$

construit (ou plutôt son existence montré) en 1981. Un théorème important utilisé est celui de Feit-Thompson (1963), qui dit qu'un groupe fini simple d'ordre impair est cyclique d'ordre premier. La preuve originale de ce résultat prend déjà 255 pages.

Si G est fini et non-trivial alors G contient toujours un sous-groupe normal maximal G_1. Si G_1 n'est pas trivial, il contient un sous-groupe normal maximal $G_2 \lhd G_1$ (mais G_2 n'est pas nécessairement un sous-groupe normal de G). On continue et on trouve une *suite de décomposition* (ou une suite de Jordan–Hölder) de G :

$$\{\mathbf{1}_G\} = G_s \lhd G_{s-1} \lhd G_{s-2} \lhd \ \ldots \ \lhd G_2 \lhd G_1 \lhd G_0 := G.$$

Par exemple :

$$\{\mathbf{1}\} \lhd \{\mathbf{1}, (1,2)(3,4)\} \lhd V_4 \lhd \ \mathrm{Alt}_4 \lhd S_4.$$

En général il y a plusieurs choix pour G_1, et puis pour G_2, etc. Toute de même la longueur d'une telle suite sera toujours la même, et les mêmes groupes simple G_i/G_{i+1} (à isomorphisme près) (les *facteurs simples* de G) vont apparaître avec les mêmes multiplicités. C'est ça le théorème de Jordan–Hölder.

Exercice 5.28. Trouver plusieures suites de décomposition du groupe $B(3, \mathbb{F}_3)$, des matrices 3×3 inversibles triangulaires de coefficients dans $\mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}$.

Théorème 5.8 (Théorème de Jordan–Hölder)**.** *Soit G un groupe fini et soient*

$$G_s = \{\mathbf{1}_G\} \lhd G_{s-1} \lhd G_{s-2} \lhd \ \ldots \lhd G_2 \lhd G_1 \lhd G_0 = G,$$

[14] **Pas de matière examen !**

[15] Mais récemment on avait encore trouvé un trou dans la preuve, pour le remplir on a écrit tout un livre. Voir M. Aschbacher, The status of the classification of the finite simple groups, Notices of the American Mathematical Society, **51**, 2004, p. 736–740

et

$$K_t = \{\mathbf{1}_G\} \lhd K_{t-1} \lhd K_{t-2} \lhd \ldots \lhd K_2 \lhd K_1 \lhd K_0 = G,$$

deux suites de décomposition, en particulier $G_{i+1} \lhd G_i$ *et* $K_{i+1} \lhd K_i$ *sont maximal pour chaque* i.

Alors $s = t$ *et il existe une permutation* $\pi \in S_s$ *de* $\{1, 2, \ldots, s\}$ *telle que*

$$G_{i-1}/G_i \simeq K_{\pi(i)-1}/K_{\pi(i)},$$

pour chaque $1 \leq i \leq s$.

Lemme 5.1. *Soient* N *et* M *deux sous-groupes normaux d'un groupe* G. *Supposons que* $N \not\subset M$ *et que* M *est maximal. Alors* $(N \cap M) \lhd N$ *est aussi maximal, et*

$$N/(N \cap M) \simeq G/M.$$

Preuve. Parce que $G = N_G M$ et donc $N < N_G M$ on peut appliquer le deuxième théorème d'isomorphisme. On obtient $NM < G$ et un isomorphisme $NM/M \simeq N/N \cap M$. On a même que $NM \lhd G$, parce que si $g \in G$, $n \in N$, $m \in M$ on a $gnmg^{-1} = gng^{-1} \cdot gmg^{-1} \in NM$. Puisque $M \lhd NM \lhd G$ et M est un sous-groupe normal maximal il suit que $G = NM$ et $G/M \simeq N/N \cap M$. Le groupe G/M est simple, donc aussi le groupe $N/N \cap M$ est simple et $N \cap M \lhd N$ est maximal. □

Preuve du théorème. Nous montrons le théorème par induction sur la cardinalité de G. Le cas où $O(G) = 1$ est trivial. Donc supposons que le théorème est vrai pour tous les groupes d'ordre plus petit que $O(G)$. Et soient deux suites de décomposition données comme dans l'énoncé du théorème.

Par le lemme précédent $(G_1 \cap K_1) \lhd G_1$ et $(G_1 \cap K_1) \lhd K_1$ sont des sous-groupes maximaux. Soit

$$L_u = \{\mathbf{1}_G\} \lhd L_{u-1} \lhd \ldots L_3 \lhd L_2 := (G_1 \cap K_1)$$

une suite de décomposition de $(G_1 \cap K_1)$. Alors

$$L_u = \{\mathbf{1}_G\} \lhd L_{u-1} \lhd \ldots \lhd L_3 \lhd L_2 \lhd G_1$$

et

$$G_s = \{\mathbf{1}_G\} \lhd G_{s-1} \lhd G_{s-2} \lhd \ldots \lhd G_2 \lhd G_1$$

sont deux suites de décomposition de G_1. Par induction on obtient $s = u$ et on obtient aussi une permutation des facteurs simples. Donc aussi les facteurs simples des deux suites de G

$$L_s = \{\mathbf{1}_G\} \lhd L_{s-1} \lhd \ldots \lhd L_3 \lhd L_2 \lhd G_1 \lhd G$$

et

$$G_s = \{\mathbf{1}_G\} \lhd G_{s-1} \lhd G_{s-2} \lhd \ldots \lhd G_2 \lhd G_1 \lhd G$$

sont permutés.

Aussi

$$L_u = \{\mathbf{1}_G\} \lhd L_{u-1} \lhd \ldots \lhd L_3 \lhd L_2 \lhd K_1$$

et

$$K_t = \{\mathbf{1}_G\} \lhd K_{t-1} \lhd K_{t-2} \lhd \ldots \lhd K_2 \lhd K_1$$

sont deux suites de décomposition de K_1, et par induction on a $t = u$. Donc $s = t$. Et les facteurs simples des deux suites de composition de G :

$$L_s = \{\mathbf{1}_G\} \lhd L_{s-1} \lhd \ldots \lhd L_3 \lhd L_2 \lhd K_1 \lhd G$$

et

$$K_s = \{\mathbf{1}_G\} \lhd K_{s-1} \lhd K_{s-2} \lhd \ \ldots \lhd K_2 \lhd K_1 \lhd G$$

sont permutés.

Parce que $G/K_1 \simeq G_1/L_2$ et $G/G_1 \simeq K_1/L_2$ par le lemme précédent, on a aussi que les facteurs simples des suites de composition de G :

$$L_s = \{\mathbf{1}_G\} \lhd L_{s-1} \lhd \ \ldots \lhd L_3 \lhd L_2 \lhd G_1 \lhd G$$

et

$$L_s = \{\mathbf{1}_G\} \lhd L_{u-1} \lhd \ \ldots \lhd L_3 \lhd L_2 \lhd K_1 \lhd G$$

sont permutés.

Donc les facteurs simples des suites de décomposition énoncé dans le théorème sont permutés. □

Exemple 5.2. Les suites de décomposition de $\mathbb{Z}/12\mathbb{Z}$ sont

$$< 0 + 12\ \mathbb{Z} > \lhd \ < 6 + 12\ \mathbb{Z} > \lhd \ < 3 + 12\ \mathbb{Z} > \lhd \mathbb{Z}/12\mathbb{Z};$$

$$< 0 + 12\ \mathbb{Z} > \lhd \ < 6 + 12\ \mathbb{Z} > \lhd \ < 2 + 12\ \mathbb{Z} > \lhd \mathbb{Z}/12\mathbb{Z};$$

$$< 0 + 12\ \mathbb{Z} > \lhd \ < 4 + 12\ \mathbb{Z} > \lhd \ < 2 + 12\ \mathbb{Z} > \lhd \mathbb{Z}/12\mathbb{Z}.$$

Les trois facteurs simples sont $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z}$ et $\mathbb{Z}/3\mathbb{Z}$ (à une permutation près).

Exercice 5.29. Soit $n = p_1^{m_1} \cdots p_s^{m_s}$ la décomposition primaire du nombre naturel n. Montrer que le groupe cyclique C_n a les facteurs simples C_{p_i} avec la multiplicité m_i.

Exercice 5.30. Si G est un groupe fini abélien et simple, alors G est cyclique d'ordre premier.

Exercice 5.31. Montrer qu'un groupe fini G est soluble (dans le sens que $G^{(n)} = \mathbf{1}$ pour $n >> 0$ si et seulement si les facteurs simples dans une suite de décomposition de G sont tous abélien.

Le grand problème irrésolu dans la théorie des groupes finis est de construire tous les groupes avec des facteurs simple de Jordan-Hölder donnés, appelé le problème d'extension. En particulier, soient donnés deux groupes simple G_1 et G_2. Trouver les groupes G (à isomorphisme près) ayant un sous-groupe normal N isomorphe à G_1 tel que le groupe quotient G/N est isomorphe à G_2.

6. Opérations d'un groupe sur un ensemble

Dans les sciences on considère souvent des groupes de symétries d'un objet X. L'objet peut être physique, comme un cristal ou un molécule, ou mathématique, comme une courbe dans l'espace. Alors chaque $g \in G$ est une symétrie: une application (par exemple une rotation) qui préserve la structure de X.

Nous considérons ici le cas ou X est un ensemble. En pratique, un ensemble a plus de structure (par exemple une opération interne ou une notion de distance) et on est souvent intéressé aux symmétries qui préservent ce structure aussi.

6.1. **Opérations.** Soit $(G, \circ)$ un groupe et X un ensemble. Une *G-action* (ou une action de G ou une *G-opération*) sur X est une règle

$$(g, x) \mapsto g \bullet x \in X,$$

pour chaque $g \in G$ et $x \in X$, satisfaisant les propriétés

$$\mathbf{1}_G \bullet x = x$$

$$(g_1 \circ g_2) \bullet x = g_1 \bullet (g_2 \bullet x))$$

pour chaque $g_1, g_2 \in G$ et $x \in X$. On dit que $(X, \bullet)$ est un *G-ensemble*, ou simplement que X est un G-ensemble (où la G-opération est fixée).

Soient X et Y deux G-ensembles. Une application $f : Y \longrightarrow X$ est une *G-application* si

$$f(g \bullet y) = g \bullet f(y),$$

pour chaque $g \in G$ et $y \in Y$. On définit de façon analogue les *G-bijections*.

Un *sous-G-ensemble* de X est un sous-ensemble Y d'un G-ensemble X tel que $g \bullet y \in Y$, pour chaque $g \in G$ et $y \in Y$. L'inclusion $Y \longrightarrow X$ est une G-application.

Exercice 6.1. L'intersection et la réunion d'une famille de sous-G-ensembles d'un G-ensemble sont aussi des sous-G-ensembles. Le complément d'un sous-G-ensemble est un sous-G-ensemble.

Un sous-G-ensemble non-vide de X qui ne contient pas un sous-G-ensemble propre non-vide s'appelle une *orbite* (ou une G-orbite) de X. Donc les orbites sont les plus petits G-sous-ensembles non-vide. Soit O une orbite et $x \in O$, on verra que

$$O = G \bullet x := \{g \bullet x; g \in G\}.$$

On dit que l'action sur X est *transitive*, si G opère avec seulement une seule orbite.

Soit $x \in X$, alors on appelle le *stabilisateur* de x le sous-groupe de G défini par

$$G_x := \{g \in G;\ g \bullet x = x\}.$$

Autre notations pour G_x sont $\mathrm{Stab}_G(x)$ ou $\mathrm{Stab}(x)$.

Le *noyau* de l'opération est

$$G_X := \{g \in G;\ \forall x \in X :\ g \bullet x = x\},$$

l'ensemble des éléments de G qui agissent trivialement sur X.

Exercice 6.2. Montrer que G_x est un sous-groupe de G et que $G_{g\bullet x} = gG_xg^{-1}$. Montrer que G_X est un sous-groupe normal de G.

On dénote

$$X^G := \{x \in X;\ \forall g \in G :\ g \bullet x = x\}$$

pour l'ensemble des *points fixes*. Une orbite contient seulement un élément x si et seulement si x est un point fixe.

On dénote l'ensemble des G-orbites de X par X/G (on va voir que les orbites sont disjointes). Donc un élément de l'ensemble X/G est une G-orbite de X. On verra que chaque x est dans une unique orbite; l'application surjective

$$\mathrm{Orb} :\ X \longrightarrow X/G$$

associe à chaque $x \in X$ l'unique G-orbite $\mathrm{Orb}(x)$ contenant x.

Exemple 6.1. Soit X un ensemble et G un sous-groupe de S_X. Alors $g \bullet x := g(x)$ définit une opération de G sur X. Soit H un sous-groupe de $\mathrm{GL}(n, \mathbb{R})$, alors H opère sur l'espace linéaire $\mathbb{R}^n$ par la multiplication matricielle.

Exemple 6.2. Soit $(G, \circ)$ un groupe, alors G opère sur soi-même par multiplication à gauche:

$$g \bullet x := g \circ x,$$

où $g, x \in G$. Soit H un sous-groupe de G (pas nécessairement normal), alors l'ensemble des translatés G/H devient un G-ensemble avec la G-opération

$$g \bullet (x \circ H) := (g \circ x) \circ H,$$

pour $g \in G$ et $x \circ H \in G/H$. Évidemment $\mathbf{1}_G \bullet (x \circ H) = x \circ H$ et $g_1 \bullet (g_2 \bullet (x \circ H)) = (g_1 \circ g_2) \bullet (x \circ H)$. Pour cette G-opération transitive on va adopter le même symbole (ici $\circ$) pour l'opération interne du groupe et la G-opération sur G/H. L'application naturelle $\nu : G \longrightarrow G/H$ est une G-application entre deux G-ensembles.

Exercice 6.3. Il existe d'autres opérations naturelles sur l'ensemble G/H, où $H < G$. Définissons $K := N_G(H)/H$. Montrer que

$$((g, nH), xH) \mapsto (g, nH) \bullet xH := gxn^{-1}H$$

donne une $G \times K$-opération bien définie sur G/H. Définir une opération de $G \times K$ sur $H\backslash G$, l'ensemble des translatés à droite.

Exercice 6.4. Le groupe diédral D_6 opère naturellement sur $\mathbb{R}^2$. Trouver ses orbites, ses stabilisateurs, ses points fixe. Décrire $\mathbb{R}^2/D_6$ par donner un représentant de chaque orbite.

Exercice 6.5. Un exemple important dans la théorie des nombres algébriques. Soit Σ la sphère de Riemann

$$\Sigma = \mathbb{C} \cup \{\infty\}.$$

Le groupe $\mathrm{SL}(2, \mathbb{R})$ agit sur Σ par

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \bullet z := \frac{az + b}{cz + d}.$$

Par exemple,

$$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \bullet \infty := \frac{1\infty+1}{0\infty+1} = \infty;$$

$$\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix} \bullet \infty := \frac{1\infty+0}{1\infty+1} = \frac{1+0}{1+1/\infty} = 1$$

$$\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix} \bullet i := \frac{i+0}{i+1} = \frac{i+1}{2} = \begin{pmatrix}1 & 1\\ 0 & 2\end{pmatrix} \bullet i,$$

où $i^2 = -1$.

(a) Vérifier que les axiomes d'une action sont satisfaits.

(b) Montrer que $\mathrm{SL}(2,\mathbb{R})$ agit avec trois orbites. Calculer le noyau de l'opération et les stabilisateurs de i, $-i$, 1 et ∞.

(c) Chaque sous-groupe de $\mathrm{SL}(2,\mathbb{R})$ opère aussi sur Σ. Dessiner les orbites de $U(2,\mathbb{R})$ (le groupe des matrices triangulaire supérieures de valeurs propres 1), T_2 (les matrices diagonales de déterminant 1) et de $\mathrm{SO}(2)$ (les matrices orthogonales).

(d) Trouver un représentant dans chaque orbite de $\mathrm{SL}(2,\mathbb{Z})$ agissant sur Σ. Indice : le groupe $\mathrm{SL}(2,\mathbb{Z})$ est engendré par les deux matrices

$$\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} \quad \text{et} \quad \begin{pmatrix}0 & 1\\ -1 & 0\end{pmatrix}.$$

(Pour montrer ça, utiliser la division avec reste !)

6.2. **Théorème fondamental des opérations.** Le théorème suivant donne la structure des G-ensembles. Chaque G-ensemble est la réunion disjointe de ses orbites et chaque orbite est en G-bijection avec un G/H pour un sous-groupe $H < G$.

Théorème 6.1. *Soit $(G,\circ)$ un groupe et $(X,\bullet)$ un G-ensemble.*

(i) X est la réunion disjointe de ses G-orbites.

(ii) Chaque $x \in X$ est contenu dans une unique G-orbite, notée $\mathrm{Orb}(x)$ *et*

$$\mathrm{Orb}(x) = G \bullet x := \{g \bullet x;\ g \in G\}.$$

(iii) Posons $H := \mathrm{Stab}_G(x)$. Alors il existe une G-bijection entre les G-ensembles $\mathrm{Orb}(x)$ *et G/H.*

Preuve. L'intersection de deux orbites est un G-sous-ensemble, donc par minimalité on obtient que si deux orbites ne sont pas disjointes, alors elles sont égales.

Pour $x \in X$ soit O_x l'intersection de tous les sous-G-ensembles contenant x. Alors O_x est un sous-G-ensemble contenant x, contenu dans chaque G-sous-ensemble contenant x. Supposons que O_x n'est pas une orbite. Alors il existe un sous-G-ensemble propre non-vide $E \subset O_x$ contenant x. Ce qui est une contradiction avec la construction de O_x. Alors chaque élément $x \in X$ est inclus dans une unique orbite et on a montré (i).

O_x contient $G \bullet x := \{g \bullet x;\ g \in G\}$ comme sous-ensemble, parce que O_x est un G-sous-ensemble. Mais $G \bullet x$ est soi-même un sous-G-ensemble contenant x, parce que $x = \mathbf{1}_G \bullet x$ et $g_1 \bullet (g_2 \bullet x) = (g_1 \circ g_2) \bullet x$. Donc $O_x = \{g \bullet x;\ g \in G\}$ et (ii) est montré.

Définissons l'application

$$\phi : \ G \bullet x \longrightarrow G/H$$

par $\phi(g \bullet x) := g \circ H$. Il faut d'abord montrer que ϕ est bien-définie, qu'elle ne dépend pas du choix de $g \in G$ pour représenter $g \bullet x \in O_x$. Donc supposons $g_1 \bullet x = g_2 \bullet x$. Alors $g_2^{-1} \circ g_1 \in H$, parce que

$$(g_2^{-1} \circ g_1) \bullet x = g_2^{-1} \bullet (g_1 \bullet x) = g_2^{-1} \bullet (g_2 \bullet x) = (g_2^{-1} \circ g_2) \bullet x = \mathbf{1}_G \bullet x = x,$$

donc ($g_2^{-1} \circ g_1 \in \mathrm{Stab}(x) = H$; alors $g_1 \circ H = g_2 \circ H$ et ϕ est bien-définie.

Pour chaque y in $\mathrm{Orb}(x) = G \bullet x$ il existe un $k \in G$ tel que $k \bullet x = y$. Alors $\phi(g \bullet y) = \phi(g \bullet (k \bullet x)) = \phi((g \circ k) \bullet x) = (g \circ k) \circ H = g \circ (k \circ H) = g \circ \phi(y)$, et ϕ est donc une G-application.

L'injectivité de ϕ : Si $\phi(g_1 \bullet x) = \phi(g_2 \bullet x)$, alors $g_1 \circ H = g_2 \circ H$. Donc, il existe un $h \in H$ tel que $g_1 = g_2 \circ h$. Alors

$$g_1 \bullet x = (g_2 \circ h) \bullet x = g_2 \bullet (h \bullet x) = g_2 \bullet x,$$

parce que $H = \mathrm{Stab}(x)$.

La surjectivité de ϕ : Soit $g \circ H \in G/H$ quelconque, alors $g \circ H = \phi(g \bullet x)$. □

6.3. **L'équation de classe.** Comme corollaire immédiat du Théorème 6.1 on obtient :

Corollaire 6.1 (Équation de classe)**.** *Soit X un G-ensemble fini. Alors*

$$|X| = \sum_{O \in X/G} |O| = |X^G| + \sum_{O \in X/G, |O|>1} |O|,$$

où X^G est l'ensemble des points fixe.

Soit $O \in X/G$ et $x \in O$. Alors

$$|O| = (G : \mathrm{Stab}_G(x)).$$

En particulier, la cardinalité de chaque orbite est un diviseur de l'ordre du groupe.

Exemple 6.3. Soit K en sous-groupe d'un groupe $(L, \circ)$. Alors K opère sur L par l'opération

$$k \bullet x := x \circ k^{-1},$$

$k \in K, x \in L$. Les K-orbites sont les translatés à gauche de K, les stabilisateurs sont tous triviaux et les orbites ont toutes la cardinalité $O(K)$. Donc l'équation de classes devient ici $O(L) = \sum_{O \in L/K} |O| = |L/K| \cdot O(K)$, et $|L/K|$ est l'index $(L : K)$. Donc on peut voir l'équation de classe comme une généralisation du théorème de Lagrange.

Exercice 6.6. Supposons un groupe cyclique d'ordre premier p opère sur un ensemble de $p^2 + p + 1$ éléments. Montrer qu'il existe au moins un point fixe.

6.4. **Existence de points fixe.** Une première application de la formule de classe est l'existence d'un point fixe pour certaines actions. Si l'ensemble X est trop petit pour un groupe G, alors G peut seulement opérer trivialement.

Lemme 6.1. *Soit p le plus petit diviseur premier d'un group fini G et soit X un G ensemble. Si x n'est pas un point fixe alors l'orbite contenant x a au moins p éléments. En particulier, si $X - X^G$ a moins que p éléments alors nécessairement G agit trivialement : $X = X^G$.*

Preuve. On a $|\mathrm{Orb}(x)|$ divise $O(G)$ et p est le plus petit diviseur de $O(G)$. □

Le lemme suivant est aussi presque trivial, mais ces applications sont nombreuses.

Lemme 6.2. *Soit p un nombre premier et P un groupe d'ordre p^r. Soit X un P-ensemble fini. Alors $|X| - |X^P|$ est divisible par p. En particulier, si p ne divise pas $|X|$, alors il existe un point fixe $x \in X^G$.*

Preuve. Soit O une orbite de X, alors la cardinalité de O divise la cardinalité de P, donc est une puissance de p. On a $|O| \neq 1$ si et seulement si O ne contient pas un point fixe si et seulement si p divise $|O|$. Par l'équation de classes il suit que $|X| - |X^P|$ est divisible par p. □

6.5. **Le théorème de Cayley généralisé.** Si G opère sur X, alors chaque g induit une bijection de X, d'où une application $G \longrightarrow S_X$. Les propriétés d'une opération impliquent que cette application est un morphisme. En effet, donner une action sur un ensemble est équivalent à donner un homomorphisme de groupe de G vers S_X. Les G-actions sur X sont en correspondance avec les homomorphismes $G \longrightarrow S_X$.

Théorème 6.2. *Soit G un groupe et X un ensemble.*

(i) Si $(g, x) \longrightarrow g \bullet x$ est une G-opération sur X, alors l'application $f : G \longrightarrow S_X$ définie par

$$[f(g)](x) := g \bullet x$$

est un homomorphisme de groupes avec noyaux G_X.

(ii) Si $f : G \longrightarrow S_X$ est un homomorphisme de groupes alors

$$(g, x) \mapsto g \bullet x := [f(g)](x)$$

est une G-opération sur X.

(iii) Les G-opérations sur X sont en correspondance biunivoque avec les homomorphismes

$$f : G \longrightarrow S_X.$$

Preuve. (i) Soit $(g, x) \mapsto g \bullet x$ une G-opération sur X et $[f(g)](x) := g \bullet x$. Alors

$$[f(g_1 \circ g_2)](x) = (g_1 \circ g_2) \bullet x = g_1 \bullet (g_2 \bullet x) = [f(g_1)]([f(g_2)](x)) = [f(g_1) \circ f(g_2)](x).$$

Donc f est un homomorphisme. La preuve de (ii) est similaire. La correspondance suit de (i) et (ii). □

Exercice 6.7. Supposons que $f : G \longrightarrow S_X$ correspond à l'opération $g \bullet x$. Montrer que le noyau de f est exactement le noyau de l'opération. Montrer que le noyau de l'opération est l'intersection de tous les stabilisateurs G_x.

Supposons que G agit transitivement sur X, et $x \in X$. Montrer que le noyau G_X est le plus grand sous-groupe normal de G contenu dans G_x.

Exercice 6.8. Pourquoi ce théorème est une généralisation du théorème de Cayley?

Département de mathématiques et de statistique, Université de Montréal, C.P. 6128, succursale Centre-ville, Montréal (Québec), Canada H3C 3J7

E-mail address: broera@DMS.UMontreal.CA