L3 Mathématiques - Informatique
Algèbre et géométrie 1

Patrick Le Meur

Table des matières

CHAPITRE 1

Groupes

1. Définition et premiers exemples

1.a. Lois de composition interne

Définition.
Soit G un ensemble. Une loi de composition interne *sur G est une application $G \times G \to G$.*

Par défaut, une loi de composition interne est notée $\times$. Si $(a, b) \in G \times G$ alors l'image de (a, b) est notée $a \times b$. Dans le cadre de ce cours, et lorsqu'il n'y a pas de confusion possible sur $\times$ (*e.g.* le contexte ne considère qu'une seule loi de composition interne) on utilise aussi la notation ab. On parle alors de notation *multiplicative*

Une loi de composition interne $\times$ sur G est dite *commutative* si : $(\forall (a, b) \in G \times G)\ \ ab = ba$. Dans un tel cas on la note plutôt $+$.

Exemple.

(1) l'addition sur un $\mathbb{R}$-espace vectoriel,
(2) à $n \geqslant 1$ fixé, l'addition des matrices sur $M_n(\mathbb{R})$,
(3) à $n \geqslant 1$ fixé, le produit des matrices sur $M_n(\mathbb{R})$.
(4) $G = \mathbb{R}$ et $\times$ est la multiplication.

1.b. Groupes

Définition.
Un groupe *est un couple $(G, \times)$ où G est un ensemble et $\times$ est d'une loi de composition interne sur G, vérifiant les conditions suivantes*

(1) $\times$ est associative : $(\forall a, b, c \in G)\ a(bc) = (ab)c$,
(2) $\times$ admet un élément neutre *:* $(\exists e \in G)\ (\forall a \in G)\ ae = ea = a$,
(3) tout élément a un inverse pour $\times$: $(\forall a \in G)\ (\exists b \in G)\ ab = ba = e$.

L'existence d'un élément neutre implique que si $(G, \times)$ est un groupe, alors G est non vide.

Proposition (Unicité de l'élément neutre et de l'inverse dans un groupe)**.**
Soit $(G, \times)$ un groupe.

(1) Il y a un unique élément neutre dans G.

(2) Si $a \in G$ alors a a un unique inverse.

Démonstration. (1) Soient $e, e' \in G$ éléments neutres. Alors $ee' = e$ (car e' est élément neutre) et $ee' = e'$ (car e est élément neutre). Donc $e = e'$.

(2) Soit $g \in G$. Soient $h, k \in G$ tels que $gh = hg = e$ et $gk = kg = e$. Alors $h = he = h(gk) = (hg)k = ek = k$. □

Dans un groupe $(G, \times)$, l'inverse d'un élément $a \in G$ est noté a^{-1}. L'élément neutre sera noté e. La propriété de l'élément neutre entraîne donc que $e^{-1} = e$. Si le groupe est commutatif, l'inverse sera noté $-a$ (on parlera alors plutôt d'*opposé*) et l'élément neutre sera noté 0.

Attention ! Dans un groupe $(G, \times)$, le passage à l'inverse et l'application de la loi de composition interne sont deux opérations qui ne commentent pas. Ainsi, si $a, b \in G$, alors $(ab)^{-1} = b^{-1}a^{-1}$ (et non $a^{-1}b^{-1}$). Cela suit de ce que $abb^{-1}a^{-1} = e$ (ce qui utilise l'associativité) et de l'unicité de l'inverse d'un élément dans un groupe.

Soit $a \in G$. Soit $n \in \mathbb{N}$. On note a^n l'élément de G défini récursivement par : $a^0 = e$ et $a^{n+1} = a\,a^n$ si $n \geqslant 0$. On note a^{-n} l'élément $(a^{-1})^n$ de G.

Exercice.
Soit $(G, \times)$ un groupe. Soit $a \in G$. Soient $n, p \in \mathbb{Z}$. À partir de la définition, et à l'aide d'une récurrence et de l'associativité, démontrer les égalités suivantes

(1) $a^n a^p = a^{n+p}$,
(2) $(a^{-1})^n = a^{-n}$,
(3) $(a^n)^{-1} = a^{-n}$.

Exercice.
Soit $(G, \times)$ un groupe. Soit $g \in G$. Démontrer que les applications $G \to G$ respectivement définies par $h \mapsto gh$ et $h \mapsto hg$ sont des bijections. Déterminer leur application inverse.

1.c. Premiers exemples de groupes

Exemple.

(1) $(\mathbb{Z}, +)$,
(2) $(\mathbb{R}, +)$,
(3) $(\mathbb{R}^*, \times)$,
(4) $(\mathbb{R}_+^*, \times)$,
(5) $(\mathrm{GL}_n(\mathbb{R}), \times)$,
(6) $(\mathrm{SL}_n(\mathbb{R}), \times)$, où $\mathrm{SL}_n(\mathbb{R}) = \{M \in \mathrm{M}_n(\mathbb{R}) \mid \det M = 1\}$,
(7) $(E, +)$ où E est un $\mathbb{R}$-espace vectoriel.
(8) $G = \{-1, 1\}$ et $\times$ est la multiplication (l'élément neutre est 1).

L'exemple qui suit est fondamental.

Exemple.
L'ensemble des nombres complexes de module 1 est noté $\mathbb{U}$. C'est un groupe pour la multiplication des nombres complexes. Son élément neutre est 1. L'inverse (pour la loi de groupe) d'un élément $z \in \mathcal{U}$ est égal à l'inverse pour la multiplication des nommbres complexes.

Étant donné un ensemble E, la composition de deux bijections de E dans E est une bijection de E dans E. Étant donnée une bijection de E dans E, son application réciproque est aussi une bijection de E vers E. Les propriétés usuelles de la composition des applications (notamment l'associativité et le fait que l'application identité $\mathrm{Id}_E \colon E \to E$ définie par $x \mapsto x$ est un élément neutre pour la composition) justifient donc que l'ensemble des applications bijectives de E dans E est un groupe pour la composition des applications.

Définition.
Soit E un ensemble. On appelle groupe symétrique *de E le groupe noté $(\mathscr{S}_E, \circ)$ (ou $(\mathscr{S}(E), \circ)$) des applications de E dans E qui sont bijectives, pour la composition des applications. Si n est un entier naturel non nul, on note $\mathscr{S}_n$ pour $\mathscr{S}_{\{1,\dots,n\}}$.*

2. Sous-groupes

Définition.
Soit $(G, \times)$ un groupe. Un sous-groupe *de $(G, \times)$ est un sous-ensemble H de G tel que*

(1) $e \in H$,

(2) $(\forall g_1, g_2 \in G)$ $g_1 \in H$ et $g_2 \in H \Rightarrow g_1 g_2 \in H$,

(3) $(\forall g \in G)$ $g \in H \Rightarrow g^{-1} \in H$.

On utilise alors la notation $H < G$.

Il revient au même de dire que H est un sous-ensemble non vide de G tel que, pour tous $g, h \in H$, on a $gh^{-1} \in H$ (**vérifier cela en détail**).

Si H est un sous-groupe de $(G, \times)$, alors l'application $H \times H \to H$, $(g, h) \mapsto gh$ est bien définie et munit H d'une structure de groupe dont l'élément neutre est l'élément neutre de $(G, \times)$.

Étant donné un groupe $(G, \times)$, il admet toujours $\{e\}$ et G comme sous-groupes.

Exercice.
Soit E un ensemble soit F un sous-ensemble de E. Démontrer que l'ensemble des applications bijectives f de E dans E telles que $f(F) = F$ est un sous-groupe de $\mathscr{S}_E$.

Exercice.
Soit $(G, \times)$ un groupe. On appelle *centre* de G le sous-ensemble $\{x \in G \mid (\forall g \in G)\ gx = xg\}$. On le note $Z(G)$. Démontrer que $Z(G) < G$.

Un groupe est d'autant mieux compris que ses sous-groupes sont mieux connus. Cependant, les déterminer tous est un problème difficile en général. Dans le cas particulier de $(\mathbb{Z}, +)$ une réponse complète peut être énoncée. Étant donné $n \in \mathbb{Z}$ on note $n\mathbb{Z}$ l'ensemble des entiers relatifs multiples de n.

Proposition (Les sous-groupes de $(\mathbb{Z}, +)$). *(1) Soit n un entier naturel. Alors $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.*

(2) Soit H un sous-groupe de $\mathbb{Z}$. Il existe un et un seul entier naturel n tel que $H = n\mathbb{Z}$.

Démonstration. (1) Le sous-ensemble $n\mathbb{Z}$ est non vide et la différence de deux entiers relatifs multiples de n est multiple de n. Donc $n\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$.

(2) Si $H = \{0\}$ alors $n = 0$ convient. On suppose donc que $H \neq \{0\}$. Vu que, pour tout $x \in H$ on a $-x \in H$, on déduit que l'ensemble $\{x \in H \mid x > 0\}$ est une partie non vide de $\mathbb{N}$. Elle a donc un plus petit élément qu'on note n. On démontre que $H = n\mathbb{Z}$. Soit $x \in H$. On écrit la division euclidienne de x par n

$$(\exists q, r \in \mathbb{Z}) \quad \begin{cases} x = qn + r \\ r \in \{0, \ldots, n-1\}. \end{cases}$$

Or $qn \in H$ (**vérifier cela en détail**). Donc $r = x - qn \in H$ (**vérifier cela en détail**). Comme $0 \leqslant r \leqslant n-1$, la minimalité de n entraîne $r = 0$. Ainsi $x = nq \in n\mathbb{Z}$. Ceci démontre que $H \subseteq n\mathbb{Z}$. On par ailleurs $n\mathbb{Z} \subseteq H$ car $n \in H$ et H est un groupe (**vérifier cela en détail**). □

Exemple (Le groupe des racines n-èmes de 1).
Soit n un entier naturel non nul. Soit $\mathbb{U}_n = \{z \in \mathbb{C}^* \mid z^n = 1\}$. On a $1 \in \mathbb{U}_n$. Si $z \in \mathbb{U}_n$ et $z' \in \mathbb{U}_n$ alors $(zz')^n = z^n z'^n = 1$, donc $zz' \in \mathbb{U}_n$. Si $z \in \mathbb{U}_n$ alors $(z^{-1})^n = (z^n)^{-1} = 1$, donc $z^{-1} \in \mathbb{U}_n$. Autrement dit, C_n est un sous-groupe de $(\mathbb{Z}^*, \times)$. On l'appelle *groupe des racines n-èmes de* 1.

3. Sous-groupe engendré par une partie

Lemme.
Soit $(G, \times)$ un groupe. Soit I un ensemble non vide. Soit, pour chaque $i \in I$ un sous-groupe $G_i < G$. Alors $\cap_{i \in I} G_i$ est un sous-groupe de G.

Démonstration. (**vérifier cela en détail**) □

Définition.
Soit $(G, \times)$ un groupe. Soit $A \subseteq G$ un sous-ensemble. Le sous-groupe intersection des sous-groupes de G qui contiennent A est appelé sous-groupe de G engendré par *A. On le note $\langle A \rangle$ (si A est fini et constitué des éléments $g_1, \ldots, g_n$, on le note $\langle g_1, \ldots, g_n \rangle$).*

Le groupe G est dit de type fini *si il admet une partie génératrice finie. Il est dit* monogène *si il est engendré par un élément. Il est dit* cyclique *si il est fini et engendré par un élément.*

Exercice.
Soit $(G, \times)$ un groupe. Soit A un sous-ensemble de G. Soit H un sous-groupe de G. Démontrer que $H = \langle A \rangle$ si et seulement si les conditions suivantes sont satisfaites

(a) $A \subseteq H$,

(b) pour tout sous-groupe K de G tel que $A \subseteq K$ on a $H \subseteq K$.

On dit que $\langle A \rangle$ est *le plus petit sous-groupe de G contenant A.*

Proposition.
Soit $(G, \times)$ un groupe. Soit $g \in G$. Alors $\langle g \rangle = \{g^n \mid n \in \mathbb{Z}\}$.

Démonstration. On pose $H = \{g^n \mid n \in \mathbb{Z}\}$. C'est un sous-groupe de G (**vérifier cela en détail**). Comme $g \in H$ on a $\langle g \rangle \subseteq H$.
Soit K un sous-groupe de G contenant g. En particulier il contient g^n pour tout $n \in \mathbb{Z}$ (**vérifier cela en détail**). Donc $H \subseteq K$. Donc H est contenu dans l'intersection des sous-groupes contenant g. Autrement dit $H \subseteq \langle g \rangle$. □

Exemple.
Soit n un entier naturel non nul. On rappelle que $\mathbb{U}_n$ désigne le sous-groupe de $(\mathbb{C}^*, \times)$ des racines n-èmes de 1. Soit $\zeta = \exp(\frac{2i\pi}{n})$. Alors $\mathbb{U}_n = \{\zeta^k \mid k \in \{0, \ldots, n-1\}\}$. Donc $\mathbb{U}_n = \langle \zeta \rangle$.

Exercice.
Soient $g_1, \ldots, g_n$ des éléments d'un même groupe. Démontrer que $\langle g_1, \ldots, g_n \rangle$ est l'ensemble des éléments du groupe de la forme $g_{i_1}^{n_1} g_{i_2}^{n_2} \cdots g_{i_\ell}^{n_\ell}$ où $\ell \in \mathbb{N}$, $i_1, \ldots, i_l \in \{1, \ldots, n\}$ et $n_1, \ldots, n_\ell \in \mathbb{N}$ sont quelconques, en convenant qu'un tel élément est e lorsque $\ell = 0$.

4. Ordre d'un groupe, ordre d'un élément

Soit $(G, \times)$ un groupe.

Définition.
Si G est fini, on appelle ordre *de G son cardinal.*

Dans la suite, le cardinal d'un ensemble A est noté $\mathrm{Card}(A)$ ou $|A|$.

Exemple.
Si n est un entier naturel non nul alors le groupe des racines n-èmes de 1 est d'ordre n (**vérifier cela en détail**). On verra plus loin que si E est un ensemble à n éléments alors $\mathscr{S}_E$ est d'ordre $n!$.

Proposition (Sur le sous-groupe engendré par un élément)**.**
Soit $g \in G$. Le sous-groupe $\langle g \rangle$ est fini si et seulement si il existe un entier naturel non nul n tel que $g^n = e$. Si $\langle g \rangle$ est fini de cardinal n, alors

(1) $\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$,

(2) $n = \min\{t \in \mathbb{N}\backslash\{0\} \mid g^t = e\}$.

Démonstration. Si $\langle g\rangle$ est fini alors l'application de $\mathbb{N}$ dans $\langle g\rangle$ définie par $n \mapsto g^n$ n'est pas injective. Donc il existe $\ell, m \in \mathbb{N}$ distincts tels que $g^\ell = g^m$. Par exemple $\ell > m$. On pose $n = \ell - m$. Donc $g^n = e$ (**vérifier cela en détail**).
Réciproquement on suppose qu'il existe un entier $n \geqslant 1$ tel que $g^n = 1$. Soit $m \in \mathbb{Z}$. On note $q \in \mathbb{Z}$ et $r \in \{0, \ldots, n-1\}$ le quotient et le reste de la division euclidienne de m par n, alors $g^m = g^r$ (**vérifier cela en détail**). Donc $\langle g\rangle = \{g^r \mid r \in \{0, \ldots, n-1\}\}$. En particulier $\langle g\rangle$ est fini.

On suppose que $\langle g\rangle$ est fini et de cardinal n. On pose $N = \min\{k \in \mathbb{N} \mid k \geqslant 1, \text{ et } g^k = e\}$. Le premier argument de la démonstration peut être réutilisé ici : la minimalité de N entraîne alors que $e, g, \ldots, g^{N-1}$ sont deux-à-deux distincts (**vérifier cela en détail**). Par ailleurs on vient de voir que $\langle g\rangle = \{e, g, \ldots, g^{N-1}\}$ (du fait que $g^N = e$). Donc $n = N$. D'où (1) et (2). □

Définition.
Soit $g \in G$. On dit que g est d'ordre fini *si il existe un entier $n \geqslant 1$ tel que $g^n = e$, et* d'ordre infini *sinon. Si g est d'ordre fini, on appelle* ordre de g *le plus petit entier $n \geqslant 1$ tel que $g^n = 1$.*

Exemple.
Soit n un entier naturel non nul. Soit $\zeta = \exp(\frac{2i\pi}{n})$. Il suit de l'équivalence "$\exp(\frac{2ik\pi}{n}) = 1 \Leftrightarrow n|k$" que ζ est un élément d'ordre n de $\mathbb{U}$.

Exercice.
Soit $g \in G$. Démontrer que g est d'ordre fini si et seulement si il existe $n \in \mathbb{N}$ tel que $g^{-1} = g^n$.

Le théorème suivant est fondamental dans l'étude des groupes. Il est conséquence de résultats plus généraux relatifs aux opérations de groupes.

Théorème (Théorème de Lagrange)**.**
Soit $(G, \times)$ un groupe fini. Soit H un sous-groupe de G. Alors Card(H) *divise* Card(G).

Démonstration. Étant donné $g \in G$ on note gH le sous-ensemble $\{gh \mid h \in H\}$ de G. Pour démontrer le théorème de Lagrange il suffit de démontrer que les sous-ensembles gH, pour g parcourant G, forment une partition de G et qu'ils sont tous de cardinal Card(H).
- Soit $g \in G$. L'application de H dans gH, définie par $h \mapsto gh$ est bien définie et bijective, son application réciproque est donnée par $x \mapsto g^{-1}x$. Donc Card(gH) = Card(H).
- Soient $g_1, g_2 \in G$. On suppose que $g_1H \cap g_2H \neq \emptyset$. Donc il existe $h_1, h_2 \in H$ tels que $g_1h_1 = g_2h_2$. Pour tout $h \in H$ on a donc $g_1h = g_1h_1h_1^{-1}h = g_2h_2(h_2^{-1}h)$. Or $h_2^{-1}h \in H$ car $H < G$. Ceci démontre que $g_1H \subseteq g_2H$. En inversant les rôles de g_1 et g_2, cet argument démontre aussi que $g_2H \subseteq g_1H$. Donc $g_1H = g_2H$. Autrement dit, deux sous-ensembles de G de la forme gH sont soit égaux soit disjoints.

□

Le corollaire au théorème de Lagrange suivant est immédiat.

Corollaire (Ordre d'un élément dans un groupe fini)**.**
Si G est fini, alors tout élément de G est d'ordre fini, d'ordre divisant Card(G).

Démonstration. (**vérifier cela en détail**) □

5. Homomorphismes de groupes

5.a. Définition et premiers exemples

Définition.
Soient des groupes G et H. Un homomorphisme de groupes de G dans H est une application $f\colon G \to H$ telle que : $(\forall g_1, g_2 \in G)\ f(g_1 g_2) = f(g_1) f(g_2)$.

Comme dans le cas des applications linéaires entre espaces vectoriels, on ne fera pas de distinction entre l'élément neutre de G et l'élément neutre de H (sauf lorsqu'il aura un risque d'ambigüité).

Exemple.

(1) L'application exponentielle $(\mathbb{R}, +) \to (\mathbb{R}_+^*, \times)$ définie par $x \mapsto \exp(x)$ est un homomorphisme de groupes.
(2) L'application logarithme népérien $(\mathbb{R}_+^*, \times) \to (\mathbb{R}, +)$ définie par $x \mapsto \ln(x)$ est un homomorphisme de groupes.
(3) Si E, F sont des espaces vectoriels sur un même corps, et si $f\colon E \to F$ est une application linéaire, alors f est un homomorphisme de groupes de $(E, +)$ dans $(F, +)$.
(4) Soit $n \geqslant 1$. L'application $\det\colon \mathrm{M}_n(\mathbb{R}) \to \mathbb{R}^*$, $M \mapsto \det(M)$ est un homomorphisme de groupes.

Exercice.

(1) Soit $f\colon G \to H$ un homomorphisme de groupes. Démontrer que $f(e) = e$ et que, pour tout $g \in G$, on a $f(g^{-1}) = f(g)^{-1}$.
(2) Soit $(G, \times)$ un groupe. Soit H un sous-groupe de G. Démontrer que l'application d'inclusion $H \to G$, définie par $h \mapsto h$, est un homomorphisme de groupes.

Étant donné un groupe $(G, \times)$ et un sous-groupe H de G, l'application d'inclusion $H \to G$ est appelée *injection canonique.*

5.b. Homomorphismes de $(\mathbb{Z}, +)$ dans un groupe

Soit $(G, \times)$ un groupe. Les homomorphismes de groupes de $(\mathbb{Z}, +)$ dans G sont particulièrement importants. Ils sont aussi très simples à comprendre.

Soit f un homomorphisme de groupes de $\mathbb{Z}$ dans G. On pose $x = f(1)$. On vérifie alors par récurrence que si n est un entier naturel que $f(n) = x^n$; en effet si $n \in \mathbb{N}$ est un entier naturel tel que $f(n) = x^n$, alors $f(n+1) = f(n) f(1)$ car f est un homomorphisme de groupes, donc $f(n+1) = x^n\, x = x^{n+1}$. Ainsi, pour tout entier naturel n on a $f(n) = x^n$. Il suit alors des propriétés de f énoncées au paragraphe précédent que, si $n \in \mathbb{N}$, alors $f(-n) = x^{-n}$. En conclusion, pour tout $n \in \mathbb{Z}$, on a $f(n) = x^n$. En particulier, f est uniquement déterminé par la donnée de x.

Réciproquement, soit $x \in G$. Soit f l'application de $\mathbb{Z}$ dans G définie par $f(n) = x^n$. Il suit alors des propriétés de l'élévation à la puissance dans un groupe que f est un homomorphisme de groupes (**vérifier cela en détail**). Ces arguments démontrent donc le résultat fondamental suivant.

Théorème.
Soit $(G, \times)$ un groupe. L'application définie sur l'ensemble des homomorphismes de groupes de $(\mathbb{Z}, +)$ dans G, à valeurs dans G, définie par $f \mapsto f(1)$ est bijective. Son application réciproque associe à chaque $x \in G$, l'homomorphisme f tel que $f(n) = x^n$ pour tout $n \in \mathbb{Z}$.

On note que le groupe G considéré n'a pas besoin d'être abélien pour que le théorème puisse s'appliquer. Le fait que $\mathbb{Z}$ est abélien se traduit, pour un homomorphisme de groupes f donné de $\mathbb{Z}$ dans G, par le fait que le sous-groupe $\langle f(x) \rangle$ est abélien.

Exercice.
Soit $(G, \times)$ un groupe. Soit n un entier naturel non nul.

(1) Démontrer que si f est un homomorphisme de groupes de $\mathbb{U}_n$ dans G alors $f(1)$ est d'ordre fini divisant n.

(2) Soit $g \in G$ tel que $g^n = 1$. Démontrer qu'il existe un et un seul homomorphisme de groupes de $\mathbb{U}_n$ dans G transformant 1 en g.

5.c. Composition des homomorphismes, isomorphismes

Proposition.

(1) Soit φ un homomorphisme d'un groupe $(G, \times)$ dans un groupe $(H, \times)$. Soit ψ un homomorphisme de H dans un groupe $(K, \times)$. Alors $\psi \circ \varphi$ est un homomorphisme de groupes de G dans K.

(2) Soit φ un homomorphisme d'un groupe $(G, \times)$ dans un groupe $(H, \times)$. Si l'application φ est bijective alors l'application inverse φ^{-1} est un homomorphisme de groupes de H dans G.

Démonstration. (1) se démontre directement à partir de la définition des homomorphismes de groupes (**vérifier cela en détail**).

(2) Soient $h, h' \in H$. Alors $\varphi(\varphi^{-1}(h)\varphi^{-1}(h')) = \varphi(\varphi^{-1}(h))\varphi(\varphi^{-1}(h')) = hh'$. En appliquant φ^{-1} à cette égalité on déduit que $\varphi^{-1}(h)\varphi^{-1}(h') = \varphi^{-1}(hh')$. Donc φ^{-1} est bien un homomorphisme de groupes. □

Définition.
On apelle isomorphisme de groupes *un homomorphisme de groupes qui est bijectif. Étant donné un groupe $(G, \times)$, on appelle* automorphisme *de G un isomorphisme de groupes de G dans G. L'ensemble des automorphismes de G est noté* $\mathrm{Aut}(G)$.

Si $(G, \times)$ est un groupe, alors $\mathrm{Aut}(G)$ est un sous-groupe de $(\mathscr{S}(G), \circ)$ comme le justifie la proposition précédente (**vérifier cela en détail**).

Exercice.
Soit $(G, \times)$ un groupe.

(1) Soit $g \in G$. Démontrer que l'application de G dans G définie par $x \mapsto gxg^{-1}$ est un automorphisme de G. Un tel automorphisme est dit *intérieur*.

(2) L'ensemble des automorphismes intérieurs de G est noté $\mathrm{Int}(G)$. Démontrer que $\mathrm{Int}(G) < \mathrm{Aut}(G)$.

(3) Démontrer que l'application de G dans $\mathrm{Int}(G)$ qui à un élement $g \in G$ associe l'automorphisme intérieur correspondant est un homomorphisme de groupes.

5.d. Sous-groupes associés à un homomorphisme

Définition (Noyau et image d'un homomorphisme de groupes)**.**
Soit f un homomorphisme de groupes de G dans H.

(1) On appelle noyau *de f et on note* $\mathrm{Ker}(f)$ *le sous-ensemble* $\{g \in G \mid f(g) = e\} \subseteq G$.

(2) On appelle image *de f et on note* $\mathrm{Im}(f)$ *l'image directe de G par f.*

Si E, F sont des espaces vectoriels sur un même corps et si $f\colon E \to F$ est une application linéaire, alors le noyau (resp. l'image) de l'application linéaire $f\colon E \to F$ est égal au noyau (resp. à l'image) de l'homomorphisme de groupes $f\colon (E, +) \to (F, +)$.

Proposition.
Soit $f\colon G \to H$ un homomorphisme de groupes.

(1) $\mathrm{Ker}(f)$ *est un sous-groupe de G et* $\mathrm{Im}(f)$ *est un sous-groupe de H.*

(2) f est une application injective si et seulement si $\mathrm{Ker}(f) = \{e\}$.

(3) Si $G_1 < G$ alors $f(G_1)$ est un sous-groupe de H.

(4) Si $H_1 < H$ alors $f^{-1}(H_1)$ est un sous-groupe de G contenant $\mathrm{Ker}(f)$.

(5) Si f est, de plus, une application surjective alors l'application définie sur l'ensemble des sous-groupes de H, à valeurs dans l'ensemble des sous-groupes de G contenant $\mathrm{Ker}(f)$*, qui à un sous-groupe $H_1 < H$ associe $f^{-1}(H)$, est bijective.*

Démonstration. Pour éviter toute confusion, on notera e_G, e_H les éléments neutres respectifs de G et H.

(1) L'affirmation relative à $\mathrm{Ker}(f)$ suit de (4) appliqué au cas où $H_1 = \{e_H\}$.
On a $e_H \in \mathrm{Im}(f)$ car $f(e_G) = e_H$. Soient $h_1, h_2 \in \mathrm{Im}(f)$. Donc il existe $g_1, g_2 \in G$ tels que $f(g_1) = h_1$ et $f(g_2) = h_2$. Donc $h_1 h_2^{-1} = f(g_1)f(g_2)^{-1} = f(g_1 g_2^{-1}) \in \mathrm{Im}(f)$. Donc $\mathrm{Im}(f) < H$.

(2) Si f est une application injective il est nécessaire que $\mathrm{Ker}(f) = \{e\}$. Réciproquement on suppose que $\mathrm{Ker}(f) = \{e\}$. Soient $g_1, g_2 \in G$. On suppose que $f(g_1) = f(g_2)$. Donc $f(g_1 g_2^{-1}) = f(g_2)f(g_2)^{-1} = e$. Donc $g_1 g_2^{-1} \in \mathrm{Ker}(f)$ puis $g_1 g_2^{-1} = e$. Ainsi $g_1 = g_1 g_2^{-1} g_2 = g_2$. Donc f est injective.

(3) On note $i\colon G_1 \to G$ l'inclusion canonique. C'est un homomorphisme de groupes donc la composée $f \circ i$ est un homomorphisme de groupes de G_1 dans H. Or $f(G_1) = \mathrm{Im}(f \circ i)$ (**vérifier cela en détail**). Donc $f(G_1) < H$.

(4) On a $e_H \in H_1$ et $e_H = f(e_G)$ donc $e_G \in f^{-1}(H_1)$. Soient $g_1, g_2 \in f^{-1}(H_1)$; donc $f(g_1), f(g_2) \in H_1$; de plus $f(g_1 g_2^{-1}) = f(g_1)f(g_2)^{-1}$; puisque $H_1 < H$ on déduit que $f(g_1 g_2^{-1}) \in H_1$. Donc $f^{-1}(H_1) < G$.

(5) Soit H_1 un sous-groupe de H. Alors $f^{-1}(H) < G$ et $f^{-1}(H)$ contient $f^{-1}(\{e_H\}) = \mathrm{Ker}(f)$. Donc l'application de l'énoncé est bien définie.

Comme f est surjective, pour tout sous-ensemble A de H on a $f(f^{-1}(A)) = A$ (**vérifier cela en détail**). Donc, si H_1, H_2 sont des sous-groupes de H tels que $f^{-1}(H_1) = f^{-1}(H_2)$ alors $H_1 = H_2$. L'application de l'énoncé est donc injective.

Soit G_1 un sous-groupe de G. Donc $f(G_1) < H$. Pour démontrer que l'application de l'énoncé est surjective, il suffit donc de démontrer que $G_1 = f^{-1}(f(G_1))$. On a certainement $G_1 \subseteq f^{-1}(f(G_1))$. Soit $g \in f^{-1}(f(G_1))$. Donc $f(g) \in f(G_1)$. Donc il existe $g_1 \in G$ tel que $f(g) = f(g_1)$. En particulier $g g_1^{-1} \in \mathrm{Ker}(f) \subseteq G_1$ (**vérifier cela en détail**). Donc $g = (g g_1^{-1}) g_1 \in G_1$. Ceci démontre que $f^{-1}(f(G_1)) \subseteq G_1$ et donc que $G_1 = f^{-1}(f(G_1))$. □

CHAPITRE 2

Opérations de groupes

1. Passage au quotient par une relation d'équivalence

1.a. Relations d'équivalence

Étant donné un ensemble X, une *relation binaire* sur X est la donnée d'un sous-ensemble de $X \times X$. Si $x, y \in X$ on dira que x *est en relation avec* y (pour cette relation) si (x, y) appartient à ce sous-ensemble. Si la relation est notée $\mathcal{R}$, on notera $x\mathcal{R}y$ lorsque x et y sont en relation.

Une relation d'*équivalence* sur X est une relation binaire $\mathcal{R}$ sur X vérifiant les conditions suivantes

- $\mathcal{R}$ est *réflexive :* $x\mathcal{R}x$ pour tout $x \in X$,
- $\mathcal{R}$ est *symétrique :* pour tous $x, y \in X$, on a $x\mathcal{R}y$ si et seulement si $y\mathcal{R}x$,
- $\mathcal{R}$ est *transitive :* pour tous $x, y, z \in X$, si $x\mathcal{R}y$ et $y\mathcal{R}z$, alors $x\mathcal{R}z$.

Exemple.

(1) La relation "*être égal à*" est une relation d'équivalence.

(2) La relation "*être différent de*" est une relation binaire qui n'est pas réflexive.

(3) La relation "*a la même parité que*" est une relation d'équivalence sur l'ensemble des entiers relatifs.

Exercice.
Soit f une application d'un ensemble E dans un ensemble F. On définit une relation binaire associée à f par : $x\mathcal{R}y$ si et seulement si $f(x) = f(y)$, pour tout $x, y \in E$. Démontrer que $\mathcal{R}$ est une relation d'équivalence.

Exercice.
Démontrer que $\mathcal{R}$ est une relation d'équivalence dans les cas suivants.

(1) $X = \mathbb{Z}$, et $\mathcal{R}$ est définie par $p\mathcal{R}q$ si et seulement si n divise $p - q$.

(2) $X = \{(p, q) \in \mathbb{Z} \times \mathbb{N} \mid q \neq 0\}$, et $\mathcal{R}$ est définie par $(p, q)\mathcal{R}(p', q')$ si et seulement si $pq' = p'q$.

(3) $X = \mathbb{R}^n \backslash \{(0, \ldots, 0)\}$ et $\mathcal{R}$ est définie par $(x_1, \ldots, x_n)\mathcal{R}(y_1, \ldots, y_n)$ si et seulement si il existe $\lambda \in \mathbb{R}^*$ tel que $(x_1, \ldots, x_n) = \lambda(y_1, \ldots, y_n)$.

1.b. Classes d'équivalence et ensemble quotient

Soit $\mathcal{R}$ une relation d'équivalence sur un ensemble X. Si $x \in X$, alors le sous-ensemble $\{y \in X \mid x\mathcal{R}y\}$ de X est appelé la *classe d'équivalence* de x. On la note $\overline{x}$ si il n'y a pas d'ambigüité sur la relation d'équivalence manipulée. Bien sûr

$$(\forall x \in X) \quad x \in \overline{x}$$

(**vérifier cela en détail**). Il suit de la transitivité et de la symétrie des relations d'équivalence que

$$(\forall x, y \in X) \quad x\mathcal{R}y \Leftrightarrow \overline{x} = \overline{y}$$

(**vérifier cela en détail**). L'ensemble des classes d'équivalences de X est noté $X/\mathcal{R}$. On l'appelle *ensemble quotient* de X par $\mathcal{R}$. L'application de X dans $X/\mathcal{R}$ qui à un élément x associe sa classe d'équivalence est surjective par définition de l'ensemble quotient, elle est appelée *surjection canonique.* La propriété précédente sur les classes d'équivalences signifie que deux classes d'équivalence sont égales dès qu'elles sont d'intersection non vide. En conséquence, $X/\mathcal{R}$ et une partition de X

$$X = \bigsqcup_{C \in X/\mathcal{R}} C\,.$$

Exemple.

(1) Sur $\mathbb{Z}\backslash\{0\}$, la relation binaire "*a le même signe que*" est une relation d'équivalence. Il y a deux classes d'équivalences : l'ensemble des entiers positifs, et l'ensemble des entiers négatifs.

(2) Soit f une application d'un ensemble E dans un ensemble F. Soit $\mathcal{R}$ la relation d'équivalence sur E associée à f. Étant donnés $x, y \in E$ on a $x\mathcal{R}y$ si et seulement si $f(x) = f(y)$, c'est-à-dire, si et seulement si $y \in f^{-1}(f(x))$. La classe d'équivalence d'un élément $x \in E$ est donc $f^{-1}(f(x))$. L'ensemble quotient $E/\mathcal{R}$ est donc l'ensemble des parties de E de la forme $f^{-1}(a)$ où $a \in F$ (**vérifier cela en détail**).

1.c. Passage au quotient

Proposition (Passage au quotient par une relation d'équivalence)**.**
Soit f une application d'un ensemble X dans un ensemble Y. Soit $\mathcal{R}$ une relation d'équivalence sur X. On suppose que

$$(\forall x_1, x_2 \in X) \quad x_1\mathcal{R}x_2 \Rightarrow f(x_1) = f(x_2)\,.$$

Alors il existe une et une seule application $\overline{f}\colon X/\mathcal{R} \to Y$ telle que, pour tout $x \in X$, on ait $\overline{f}(\overline{x}) = f(x)$.

Démonstration. Soit C une classe d'équivalence. Si $x, y \in C$ alors $x\mathcal{R}y$. Donc $f(x) = f(y)$. La fonction f est donc constante sur le sous-ensemble C de X. On note $f_C \in Y$ la valeur prise par f sur C. On définit $\overline{f}\colon X/\mathcal{R} \to Y$ par $\overline{f}(C) = f_C$. Ainsi, pour tout $x \in X$, on a $\overline{f}(\overline{x}) = f_{\overline{x}} = f(x)$ car $x \in \overline{x}$. Ceci démontre l'existence de $\overline{f}$. L'unicité est immédiate. □

Exercice.
Reprendre les situations de l'exercice précédent. Démontrer qu'il existe une application bijective de $X/\mathcal{R}$ dans

(1) $\mathbb{U}_n$,

(2) $\mathbb{Q}$,

(3) l'ensemble des sous-espaces vectoriels de dimension 1 de $\mathbb{R}^n$.

2. Définition, premiers exemples

Définition (Opération d'un groupe sur un ensemble)**.**
Soit $(G, \times)$ un groupe. Soit X un ensemble. Une opération de $(G, \times)$ sur X *(à gauche) est la donnée d'une application $G \times X \to X$ (par laquelle l'image d'un couple (g, x) sera notée $g \cdot x$ par défaut) vérifiant les conditions suivantes*

(1) $(\forall x \in X) \quad e \cdot x = x$,

(2) $(\forall g, h \in G) \quad (\forall x \in X)\ g \cdot (h \cdot x) = (gh) \cdot x$.

Par défaut toutes les opérations de groupe sont à gauche. Une opération de groupe à droite de G sur X est définie de manière analogue, à ceci près qu'il s'agit d'une application de $X \times G$ dans X (l'image d'un couple (x, g) étant donnée $x \cdot g$) vérifiant les deux conditions

(1') $(\forall x \in X) \quad x \cdot e = x$,

(2') $(\forall g, h \in G)\ (\forall x \in X) \quad (x \cdot g) \cdot h = x \cdot (gh)$.

Il ne faut cependant pas confondre les deux notions (opération à gauche, et opération à droite). Étant donnée une opération à gauche d'un groupe $(G, \times)$ sur un ensemble X, on peut poser $x * g = g \cdot x$ et ainsi définir une application $X \times G \to X$ qui à un couple (x, g) associe $x * g$. Les axiomes des opérations de groupe à gauche impliquent alors que $(x * g) * h = x * (hg)$ pour tous $g, h \in G$ et $x \in X$ (et non pas $(x * g) * h = x * (gh)$). L'application $X \times G \to X$ ainsi obtenue n'est *a priori* pas une opération de G sur X à droite. Bien sûr, lorsque le groupe G est commutatif, les notions d'opération à gauche et à droite coïncident.

Pour un groupe donné, il existe plusieurs ensembles sur lequel il agit. Pour un groupe et un ensemble donnés, il peut exister plusieurs actions de ce groupe sur cet ensemble.

Exercice.
Soit $(G, \times)$ un groupe agissant sur un ensemble X. Soit H un sous-groupe de G. Vérifier que l'application $H \times X \to X\,, (h, x) \mapsto h \cdot x$ est une action de H sur X. On dit que cette action est obtenue à partir de l'action de G sur X par *restriction* à H.

Au moyen d'outils qui seront développés dans ce chapitre, chaque action de groupe est une source d'informations sur le groupe et sur l'ensemble sur lequel le groupe agit. De ce point de vue, la meilleure façon de bien comprendre un groupe

donné est d'étudier les actions de ce groupe (l'ensemble sur lequel il agit pouvant varier).

Exercice.
Soit $(G, \times)$ un groupe. Soit X un ensemble.

(1) Soit $\varphi\colon G \to \mathscr{S}_X$ un homomorphisme de groupes. Démontrer que l'application $G \times X \to X$ définie par $g \cdot x = \varphi(g)(x)$ est une opération de $(G, \times)$ sur X.

(2) Démontrer que toute opération de $(G, \times)$ sur X peut être obtenue de cette façon.

Exemple.

(1) $(\mathrm{GL}_n(\mathbb{R}), \times)$ agit sur $\mathrm{M}_n(\mathbb{R})$ par multiplication à gauche : $g \cdot x = gx$ si $g \in \mathrm{GL}_n(\mathbb{R})$ et $x \in \mathrm{M}_n(\mathbb{R})$.

(2) $(\mathrm{GL}_n(\mathbb{R}), \times)$ agit sur $\mathrm{M}_n(\mathbb{R})$ par conjugaison : $g \cdot x = gxg^{-1}$ si $g \in \mathrm{GL}_n(\mathbb{R})$ et $x \in \mathrm{M}_n(\mathbb{R})$.

(3) $(\mathrm{GL}_n(\mathbb{R}))$ agit sur l'ensemble des bases de $\mathbb{R}^n$ de la façon suivante : si $g \in \mathrm{GL}_n(\mathbb{R})$ et si $(e_1, \ldots, e_n)$ est une base de $\mathbb{R}^n$, alors $g \cdot (e_1, \ldots, e_n) = (g(e_1), \ldots, g(e_n))$ (ici on a identifié la matrice g à l'endomorphisme de $\mathbb{R}^n$ dont g est la matrice dans la base canonique.

(4) Si X est un ensemble, alors $(\mathscr{S}_X, \circ)$ agit sur X de la façon suivante : $g \cdot x = g(x)$ pour $g \in \mathscr{S}_X$ et $x \in X$

(5) Soient deux ensembles E, F. Soit X l'ensemble des applications de E dans F. Le groupe $\mathscr{S}_E$ agit naturellement à droite sur X et le groupe $\mathscr{S}_F$ agit naturellement à gauche sur X de la façon suivante
- $g \cdot f = g \circ f$ pour tous $g \in \mathscr{S}_F$ et $f \in X$,
- $f \cdot g = f \circ g$ pour tous $g \in \mathscr{S}_E$ et $f \in X$.

Soit une opération (resp. une opération de groupe à droite) d'un groupe $(G, \times)$ sur un ensemble X. On lui associe la relation binaire suivante qu'on note $\mathcal{R}$: pour tout $x, y \in X$, on a $x \mathcal{R} y$ si et seulement si il existe $g \in G$ tel que $y = g \cdot x$ (resp. $y = x \cdot g$). Cette relation binaire est une relation d'équivalence.

Exercice.
Démontrer que la relation binaire $\mathcal{R}$ est une relation d'équivalence. Étant donné $x \in X$, démontrer que la classe d'équivalence de x pour $\mathcal{R}$ est $\{y \in X \mid (\exists g \in G)\ \ g \cdot x = y\}$.

Définition.
Soit une action d'un groupe $(G, \times)$ sur un ensemble X. L'action est dite
- transitive *lorsque, pour tous $x, y \in X$, il existe $g \in G$ tel que $g \cdot x = y$,*
- libre *lorsque, pour tous $x \in X$, $g \in G$, si $g \cdot x = x$ alors $g = e$,*
- fidèle *lorsque, pour tout $g \in G$, si $g \cdot x = x$ pour tout $x \in X$ alors $g = e$.*

Exercice.
Une action libre est-elle fidèle ? Une action fidèle est-elle libre ? Parmi les actions données en exemple précédemment, lesquelles sont transitives (resp. fidèles, resp. libres) ?

3. Orbites, stabilisateurs, ensemble quotient

On fixe un groupe $(G, \times)$ opérant sur un ensemble X.

Définition.
Soit $x \in X$.

*(1) L'*orbite *de x est le sous-ensemble $\{y \in X \mid (\exists g \in G)\ g \cdot x = y\}$ de X. On le note $G \cdot x$.*

(2) Le stabilisateur *de x est le sous-ensemble $\{g \in G \mid g \cdot x = x\}$ de G. On le note* $\mathrm{Stab}_G(x)$.

(3) L'ensemble des orbites est appelé ensemble quotient *de X par (l'action de) $(G, \times)$. On le note $G\backslash X$.*

(4) Un système complet de représentants *pour cette action est la donnée d'un sous-ensemble E de X qui contient exactement un élément de chaque orbite.*

Il suit de ces définitions que l'orbite de $x \in X$ n'est autre que la classe d'équivalence de x pour la relation d'équivalence associée à l'opération de G sur X ; également, $G\backslash X$ est l'ensemble quotient de X par cette relation d'équivalence (**vérifier cela en détail**).

On peut définir les notions analogues pour les actions à droite. Elle sont alors notées de la même façon, sauf pour l'ensemble quotient qui est alors noté X/G au lieu de $G\backslash X$.

Exercice.

(1) Soit $x \in X$. Démontrer que $\mathrm{Stab}_G(x) < G$.
(2) À l'aide du paragraphe précédent, trouver des exemples d'une action de groupe et d'un élément $x \in X$ tel que $G \cdot x = \{x\}$.
(3) Même question avec cette fois-ci la propriété $G \cdot x = X$.
(4) Même question avec cette fois-ci la propriété $\{x\} \subsetneq G \cdot x \subsetneq X$.
(5) Soit $x \in X$. À quelle condition nécessaire et suffisante sur $\mathrm{Stab}_G(x)$ a-t-on $G \cdot x = \{x\}$?

Exercice.

(1) Caractériser le fait que l'action soit transitive en termes du nombre d'orbites.
(2) Caractériser le fait que l'action soit libre en termes des stabilisateurs des éléments de X.
(3) Caractériser le fait que l'action soit fidèle en termes des stabilisateurs des éléments de X.

On connaît d'autant mieux un groupe qu'on sait décrire ses sous-groupes et préciser les relations d'inclusion entre ces derniers. En ce sens, les actions de groupes sont utiles dans la mesure où chaque élément d'un ensemble sur lequel le groupe agit fournit un nouveau sous-groupe, à savoir le stabilisateur de cet élément.

Exercice.
Pour chacun des exemples du paragraphe précédent, retrouver un résultat ou un problème d'algèbre linéaire qui est naturellement associé à la description des orbites.

Le résultat suivant est fondamental, il justifie l'intérêt des systèmes complets de représentants pour une action donnée.

Théorème (Les orbites partitionnent l'ensemble)**.**
Soit $(G, \times)$ un groupe opérant (à gauche ou à droite) sur un ensemble X. Alors tout élément de X appartient à une unique orbite.

Cela peut s'énoncer sous diverses formes, par exemple : *l'ensemble quotient ($G\backslash X$ ou G/X) est une partition de X*, ou bien *les orbites de l'action de $(G, \times)$ sur X forment une partition de X*, ou encore, *deux orbites sont égales ou disjointes.* Ce théorème suit de ce que l'ensemble des classes d'équivalences d'une relation d'équivalence sur X est une partition de X.

4. Les actions classiques

Soit $(G, \times)$ un groupe. Deux actions lui sont associées de façon intrinsèque. Pour ces deux actions, l'ensemble X est égal à G.

4.a. L'action par translation à gauche d'un groupe sur lui-même

La loi de composition interne $G \times G \to G$, $(g, x) \mapsto gx$ du groupe G est une opération à gauche de $(G, \times)$ sur G. Cette action est appelée l'*action de G sur lui-même par translation à gauche.*

Exercice.
Vérifier qu'il s'agit bien d'une action de groupes. Pour chaque axiome de la définition des actions de groupes, identifier le (ou les) axiome(s) de la définition des groupes qui le justifie(nt).

Proposition.
Pour l'action de G sur lui-même par translation, il n'y a qu'une seule orbite, à savoir G. Tous les stabilisateurs sont égaux à $\{e\}$.

Exercice.
Démontrer cette proposition. Que signifie-t-elle en termes de liberté, fidélité et transitivité ?

4.b. L'action sur un groupe par un sous-groupe par translation à gauche

En restreignant à un sous-groupe l'action d'un groupe sur lui-même par translation (à gauche ou à droite) on obtient une nouvelle action. La description qui suit est immédiate à vérifier.

Proposition.
Soit H un sous-groupe de G. L'application $H \times G \to G$ définie par $(h, g) \mapsto hg$ est une action de H sur G. Si on note $\mathcal{R}$ la relation d'équivalence associée à cette action de groupe, alors

$$(\forall g_1, g_2 \in G) \quad g_1 \mathcal{R} g_2 \Leftrightarrow g_1 g_2^{-1} \in H\,.$$

Pour tout $g \in G$ l'orbite de g pour cette action est $Hg = \{hg \mid h \in H\}$, l'application $H \to Hg$, $h \mapsto hg$ est bijective.

Soit H un sous-groupe de G. L'action considérée dans la proposition qui précéde est appelée action de H sur G par *translation à gauche.* De façon analogue, l'application de $G \times H$ dans G définie par $(g, h) \to gh$ est une action *à droite* du groupe H sur G. On l'appelle action de H sur G par *translation à droite.*

Exercice.
Soit H un sous-groupe de G. Énoncer et démontrer une proposition pour l'action de H sur G par translation à droite qui soit analogue à la proposition précédente.

Exercice.
On suppose que G est fini. Soit H un sous-groupe de G. Démontrer que $\mathrm{Card}(G) = \mathrm{Card}(H) \cdot \mathrm{Card}(H\backslash G)$ et $\mathrm{Card}(G) = \mathrm{Card}(H) \cdot \mathrm{Card}(G/H)$. Retrouver ainsi le théorème de Lagrange.

Définition.
Soit H un sous-groupe de G. Étant donné $g \in G$, l'orbite de g pour l'action de H sur G par translation à gauche (resp. à droite) est appelée classe de g à gauche (resp. à droite) modulo H.

Le cas où $(G, \times)$ est le groupe abélien $(\mathbb{Z}, +)$ est particulièrement important. Soit un sous-groupe de $\mathbb{Z}$. Il est donc de la forme $n\mathbb{Z}$ pour un certain $n \in \mathbb{N}$. On suppose que $n \neq 0$.

L'action de $n\mathbb{Z}$ sur $\mathbb{Z}$ par translation à gauche est donnée par $nm \cdot q = nm + q$ *(attention la loi de composition interne du groupe $\mathbb{Z}$ est l'addition).* On note momentanément $\equiv$ la relation d'équivalence sur $\mathbb{Z}$ associée à cette action. Ainsi

$$(\forall p, q \in \mathbb{Z}) \quad p \equiv q \Leftrightarrow (\exists m \in \mathbb{Z}) \quad p = q + nm\,.$$

Autrement dit, la relation $\equiv$ n'est autre que *"a le même reste par la division euclidienne par n que"* ou encore *"être congru à $\cdot$ modulo n.* Donc cette action a exactement n orbites, à savoir $n\mathbb{Z}, 1+n\mathbb{Z}, \ldots, (n-1)+n\mathbb{Z}$. Dans cette liste, l'orbite

$i + n\mathbb{Z}$ n'est autre que l'ensemble des entiers relatifs dont la division euclidienne par n est i (où $i \in \{0, \ldots, n-1\}$).

L'ensemble des orbites pour cette action a donc n éléments, et un système complet de représentants est $\{0, \ldots, n-1\}$.

4.c. L'action d'un groupe sur lui-même par conjugaison

L'application $G \times G \to G$, $(g, x) \mapsto gxg^{-1}$ est une action de $(G, \times)$ sur G. On l'appelle *action de G sur lui-même par conjugaison.*

Exercice.
Vérifier qu'il s'agit d'une action de groupe.

Pour cette action, l'orbite d'un élément $x \in G$ est appelée *classe de conjugaison* de x, et le stabilisateur de x n'est autre que $\{g \in G \mid gx = xg\}$, on l'appelle *centralisateur* de x (dans G) que l'on note parfois $C_G(x)$ (ou $C(x)$ si le groupe G est implicite).

Si le groupe $(G, \times)$ est commutatif, alors $gxg^{-1} = x$ pour tous $g \in G$ et $x \in X$. Donc, pour tout $x \in G$, l'orbite de x est $\{x\}$ et son stabilisateur est G.

4.d. L'action d'un groupe sur l'ensemble de ses sous-groupes

Soit un groupe $(G, \times)$. Étant donné un sous-groupe H de G et $g \in G$, le sous-ensemble gHg^{-1} est l'image directe de H par l'automorphisme intérieur de G associé à g ; donc c'est un sous-groupe de G ; on le note parfois ${}^gH$.

Exercice.
Soit$(G, \times)$ un groupe. Soit H un sous-groupe de G. Démontrer que ${}^eH = H$ et que ${}^{gh}H = {}^g({}^hH)$ pour tous $g, h \in H$.

L'application $(g, H) \mapsto {}^gH$ est donc une opération de groupe de G sur l'ensemble de ses sous-groupes. Si H est un sous-groupe de G alors $\mathrm{Stab}_G(H)$ est un sous-groupe de G contenant H.

Exemple.
Si $(G, \times)$ est un groupe abélien alors tout sous-groupe de G est un point fixe pour l'action de G par conjugaison.

4.e. L'action d'un groupe sur les classes à droite modulo un sous-groupe

Soit $(G, \times)$ un groupe. Soit H un sous-groupe de G. Il existe une et une seule application $G \times G/H \to G/H$ telle que, pour tous $g, x \in G$ l'image de (g, xH) soit gxH.

Exercice.
(1) Démontrer l'existence et l'unicité d'une telle application.
(2) Démontrer que cette application est une opération de groupe de G sur G/H.

(3) Soit $x \in H$. Démontrer que le stabilisateur de xH pour cette action est le sous-groupe xHx^{-1}.

Cette action de groupe est appelée *l'action de G sur G/H par translation à gauche.*

5. Aspects numériques des actions de groupes

5.a. Les orbites sont des ensembles de classes à droite modulo un sous-groupe

L'action d'un sous-groupe de G sur G par translation est un prototype des actions de groupes en général. Plus précisément, ces actions permettent de décrire les orbites d'une action de G sur un ensemble X.

Théorème (Les orbites sont des ensembles quotients)**.**
Soit une opération d'un groupe $(G, \times)$ sur un ensemble X. Soit $x \in X$. Il existe une application bijective

$$G/\mathrm{Stab}_G(x) \xrightarrow{\sim} G \cdot x$$

telle que, pour tout $g \in G$, l'image de la classe à droite $g\mathrm{Stab}_G(x)$ soit égale à $g \cdot x$.

Le théorème s'énonce plus savamment avec le passage au quotient d'une application par une relation d'équivalence de la façon suivante. *Soit $x \in X$. Soit $\mathcal{R}$ la relation d'équivalence associée à l'action de $\mathrm{Stab}_G(x)$ sur G par translation à droite. Alors l'application de G dans X définie par $g \mapsto g \cdot x$ est à valeurs dans $G \cdot x$ et passe au quotient par la relation d'équivalence $\mathcal{R}$. L'application de $G/\mathrm{Stab}_G(x)$ dans $G \cdot x$ qui en résulte est alors bijective.*

La démonstration du théorème faite ci-dessous suit ce dernier point de vue.

Démonstration. Soit φ l'application de G dans $G \cdot x$ définie par $g \mapsto g \cdot x$. On démontre que φ passe au quotient par $\mathcal{R}$. Soient $g_1, g_2 \in G$ tels que $g_1 \mathcal{R} g_2$. Donc il existe $h \in \mathrm{Stab}_G(x)$ tel que $g_1 = g_2 h$. Ainsi

$$\varphi(g_1) = g_1 \cdot x = (g_2 h) \cdot x = g_2 \cdot (h \cdot x) = g_2 \cdot x = \varphi(g_2)\,.$$

L'application φ passe donc au quotient par $\mathcal{R}$. Il existe donc une et une seule application $\overline{\varphi}$ de $G/\mathrm{Stab}_G(x)$ dans $G \cdot x$ telle que

$$(\forall g \in G) \quad \overline{\varphi}(g\mathrm{Stab}_G(x)) = g \cdot x\,.$$

Pour obtenir le théorème il ne reste donc plus qu'à démontrer que $\overline{\varphi}$ est une application bijective.

- Soit $y \in G \cdot x$. Donc il existe $g \in G$ tel que $y = g \cdot x$. En particulier, si on pose $\alpha = g\mathrm{Stab}_G(x)$ alors $\alpha \in G/\mathrm{Stab}_G(x)$ et $\overline{\varphi}(\alpha) = g \cdot x = y$. Ceci démontre que $\overline{\varphi}$ est une application surjective.
- Soient $\alpha, \beta \in G/\mathrm{Stab}_G(x)$ tels que $\overline{\varphi}(\alpha) = \overline{\varphi}(\beta)$. Il existe $g, h \in G$ tels que $\alpha = g\mathrm{Stab}_G(x)$ et $\beta = h\mathrm{Stab}_G(x)$. Donc

  $$g \cdot x = \overline{\varphi}(\alpha) = \overline{\varphi}(\beta) = h \cdot x\,.$$

  Donc $x = (g^{-1}h) \cdot x$. On pose $k = g^{-1}h$. Donc $k \cdot x = x$, autrement dit $k \in \mathrm{Stab}_G(x)$. De plus $gk = h$, autrement dit $g\mathcal{R}h$, ou encore $g\mathrm{Stab}_G(x) = h\mathrm{Stab}_G(x)$. Donc $\alpha = \beta$. Ceci démontre que $\overline{\varphi}$ est une application injective, donc bijective.

□

5.b. L'équation aux classes

Si deux ensembles finis sont en bijection alors ils ont le même cardinal. Le théorème ci-dessous suit donc :

- du théorème qui précéde,
- de ce que $|G/H| = \frac{|G|}{|H|}$ pour tout sous-groupe H d'un groupe $(G, \times)$,
- de ce que les orbites d'une action de groupe sur un ensemble forment une partition de cet ensemble.

Théorème (Équation aux classes)**.**
Soit une opération d'un groupe $(G, \times)$ sur un ensemble X. On suppose que X et G sont finis.

(1) Pour tout $x \in X$, on a $\mathrm{Card}(G \cdot x) = \frac{\mathrm{Card}(G)}{\mathrm{Card}(\mathrm{Stab}_G(x))}$*. En particulier,* $\mathrm{Card}(\mathrm{Stab}_G(x))$ *divise* $\mathrm{Card}(G)$ *et ne dépend que de l'orbite $G \cdot x$, et non de x.*

(2) Soit, pour chaque orbite ω de cette action, un élément x_ω de cette orbite. Alors $\mathrm{Card}(X) = \sum_{\omega \in G\backslash X} \frac{\mathrm{Card}(G)}{\mathrm{Card}(\mathrm{Stab}_G(x_\omega))}$.

5.c. Application aux p-groupes

Soit p un entier premier. On appelle *p-groupe* tout groupe fini de cardinal une puissance (strictement positive) de p.

Corollaire.
Soit $(G, \times)$ un p-groupe agissant sur un ensemble fini X. On note X^G

l'ensemble des points fixes de cette action, c'est-à-dire $\{x \in X \mid (\forall g \in G)\ g \cdot x = x\}$. *Alors*

$$|X^G| = |X| \bmod p\,.$$

Démonstration. Étant donné $x \in X$, l'orbite de x est de cardinal 1 (on dit que l'orbite est *pontctuelle*) si et seulement si $x \in X^G$.
Soit $C_1, \ldots, C_n$ une énumération des orbites de l'action de G sur X. Soit $i \in \{1, \ldots, n\}$; soit $x \in C_i$; alors $|C_i| = \frac{|G|}{|\mathrm{Stab}_G(x)|}$. Puisque G est un p-groupe on déduit que $|C_i|$ vaut 1 ou est disible par p selon que l'orbite est ponctuelle ou non. Or $|X| = \sum_{i=1}^{n} |C_i|$. D'où la conclusion. □

Exercice.
Soit $(G, \times)$ un groupe fini. On suppose que $p||G|$. On pose $\xi = e^{\frac{2i\pi}{p}}$.

(1) Démontrer qu'il existe une action du groupe $\mathbb{U}_p$ des racines p-èmes de 1 sur G^n telle que $\xi \cdot (g_1, \ldots, g_n) = (g_2, \ldots, g_n, g_1)$ pour tout $(g_1, \ldots, g_n) \in G^n$.

(2) Déterminer les points fixes de cette action.

(3) En déduire qu'il existe dans G un élément d'ordre p.

Exercice.
Soit $(G, \times)$ un p-groupe. Déterminer les points fixes de l'action de G sur lui-même par conjugaison et en déduire que le centre de G contient un élément distinct de l'élément neutre.

CHAPITRE 3

Groupe symétrique

1. Définition, éléments remarquables

Définition.
Soit $n \geqslant 1$. On appelle n-ème groupe symétrique *le groupe des applications bijectives de $\{1, \ldots, n\}$ dans $\{1, \ldots, n\}$ pour la composition des applications. On le note $\mathscr{S}_n$. Les éléments de $\mathscr{S}_n$ sont appelés* permutations *de $\{1, \ldots, n\}$.*

Étant donnée une permutation σ de $\{1, \ldots, n\}$, on appelle support *de σ et on note* $\mathrm{supp}(\sigma)$ *l'ensemble des $i \in \{1, \ldots, n\}$ tels que $\sigma(i) \neq i$.*

Le groupe $\mathscr{S}_1$ est le groupe trivial $\{\mathrm{Id}\}$. On fixe un entier naturel non nul n.

Lemme.
Le groupe $(\mathscr{S}_n, \circ)$ est d'ordre $n!$.

Démonstration. On démontre l'affirmation du lemme par récurrence sur $n \geqslant 1$. Le résultat est vrai pour $n = 1$. Soit $n \geqslant 2$. On suppose que $\mathscr{S}_{n-1}$ est d'ordre $(n-1)!$. Pour chaque $i \in \{1, \ldots, n\}$ soit $S(i)$ le sous-ensemble $\{\sigma \in \mathscr{S}_n \mid \sigma(i) = n\}$. Alors $\{S_i\}_{i \in \{1,\ldots,n\}}$ est une partition de $\mathscr{S}_n$ (**vérifier cela en détail**). Soit $i \in \{1, \ldots, n\}$. L'application de $S(i)$ dans $\mathscr{S}_{n-1}$ qui à $\sigma \in \mathscr{S}_n$ associe la permutation de $\{1, \ldots, n-1\}$ définie par $j \mapsto \begin{cases} \sigma(j) & \text{si } 1 \leqslant j \leqslant i-1 \\ \sigma(j+1) & \text{si } i \leqslant j \leqslant n-1 \end{cases}$ est bijective (**vérifier cela en détail**). Donc $\mathscr{S}_n$ est d'ordre $n!$ (**vérifier cela en détail**). □

Étant donnée une bijection $f \colon \{1, \ldots, n\} \to \{1, \ldots, n\}$. 0n a coutume de représenter f sous la forme d'un tableau

$$\begin{pmatrix} 1 & \cdots & n \\ f(1) & \cdots & f(n) \end{pmatrix}.$$

La notation "$\circ$" pour la composition des applications est omise pour alléger l'écriture.

Soit $l \in \{1, \dots, n\}$. Soient $a_1, \dots, a_l \in \{1, \dots, n\}$ deux-à-deux distincts. On note $(a_1 \dots a_l)$ la permutation de $\{1, \dots, n\}$ définie par

$$\begin{array}{rcll} \{1,\dots,n\} & \to & \{1,\dots,n\} & \\ i & \mapsto & i & \text{si } i \neq a_1, \dots, a_l \\ a_1 & \mapsto & a_2 & \\ a_2 & \mapsto & a_3 & \\ & \vdots & & \\ a_{l-1} & \mapsto & a_l & \\ a_l & \mapsto & a_1 & \end{array}$$

Elle est injective car $a_1, \dots, a_l$ sont deux-à-deux distincts. En tant que telle elle est donc bijective (**vérifier cela en détail**).

Définition (Cycles et transpositions)**.**
Soit $l \in \{1, \dots, n\}$. Un l-cycle *de $\mathscr{S}_n$ est une permutation de la forme $(a_1 \dots a_l)$ où $a_1, \dots, a_l \in \{1, \dots, n\}$ sont deux-à-deux distincts. Il est alors dit de longueur l. Si $l = 2$ on dit que c'est une* transposition.

Le support du cycle $(a_1 \cdots a_l)$ est $\{a_1, \dots, a_l\}$. L'ordre des entiers dans la définition d'un cycle a de l'importance. Ainsi $(123) \neq (132)$. En revanche, si $a_1, \dots, a_l \in \{1, \dots, n\}$ sont deux-à-deux distincts, alors $(a_1 \cdots a_l) = (a_2 \cdots a_l a_1)$.

Exercice.

(1) Soit une transposition $(a_1\, a_2)$. Déterminer toutes ses puissances.

(2) Soit un 3-cycle $(a_1\, a_2\, a_3)$. Déterminer toutes ses puissances.

(3) Soit un 4-cycle $(a_1\, a_2\, a_3\, a_4)$. Déterminer toutes ses puissances.

(4) Soit un l-cycle $(a_1 \dots a_l)$ de $\mathscr{S}_n$. Soit une permutation $\sigma \in \mathscr{S}_n$. Démontrer que $\sigma(a_1 \dots a_n)\sigma^{-1} = (\sigma(a_1) \dots \sigma(a_n))$.

(5) Soient deux permutations σ_1, σ_2 de $\{1, \dots, n\}$. On suppose que les supports de σ_1 et σ_2 sont disjoints. Démontrer que $\sigma_1\sigma_2 = \sigma_2\sigma_1$.

Exercice.
Soit σ un cycle de longueur l de $\mathscr{S}_n$. Soit $x \in \mathrm{supp}(x)$. Démontrer que $\sigma = (x\, \sigma(x) \cdots \sigma^{l-1}(x))$.

Comme $\mathscr{S}_n$ est d'ordre fini, il suit du corollaire au théorème de Lagrange que tout élément de $\mathscr{S}_n$ est d'ordre fini divisant $n!$. L'ordre d'un cycle est particulièrement facile à déterminer.

Proposition.
Soit $l \in \{1, \dots, n\}$. Tout l-cycle de $\mathscr{S}_n$ est d'ordre l.

Démonstration. Soit un l-cycle $(a_1 \cdots a_l)$. On le note σ. Par récurrence sur $t \in \{1, \ldots, l\}$ on démontre que $\sigma^t(a_1) = \begin{cases} a_t & \text{si } 1 \leqslant t \leqslant l-1 \\ a_1 & \text{si } t = l \end{cases}$ (**vérifier cela en détail**). Comme $a_2 = \sigma(a_1)$ on déduit que $\sigma^l(a_2) = a_2$, puis, par récurrence sur i suivant le même argument, que $\sigma^l(a_i) = a_i$ pour tout $i \in \{1, \ldots, l\}$ (**vérifier cela en détail**). Ces arguments démontrent que $\sigma^t \neq \mathrm{Id}$ si $1 \leqslant t \leqslant l-1$ et que $\sigma^l = \mathrm{Id}$. Donc σ est d'ordre l. □

Définition (Double transpositions).
On appelle double transposition *de $\mathscr{S}_n$ une permutation de de $\mathscr{S}_n$ la forme $\tau\tau'$ où τ, τ' sont des transpositions de $\mathscr{S}_n$ à supports disjoints.*

Exemple.

(1) $(12)(34)$ est une double transposition de $\mathscr{S}_4$.
(2) $\mathscr{S}_2 = \{\mathrm{Id}, (1\,2)\}$,
(3) $\mathscr{S}_3 = \{\mathrm{Id}\,(1\,2), (1\,3), (2\,3), (1\,2\,3), (1\,3\,2)\}$.

Exercice.
Décrire $\mathscr{S}_4$ à l'aide des cycles et des double transpositions.

2. Décomposition en cycles

Soit n un entier naturel non nul.

2.a. Le théorème de décomposition

La décomposition des permutations de $\mathscr{S}_n$ en produits de cycles à supports deux-à-deux disjoints repose sur l'étude fondamentale suivante.

Soit σ une permutation de $\mathscr{S}_n$. On utilise l'action à gauche du groupe $\langle\sigma\rangle$ sur $\{1, \ldots, n\}$ (où $g \cdot i = g(i)$ si $g \in \langle\sigma\rangle$ et $i \in \{1, \ldots, n\}$).

Soit $\mathcal{C}$ une orbite pour cette action. On note l son cardinal. Alors
- $\mathcal{C} = \{x, \sigma(x)^l, \ldots, \sigma(x)^{l-1}\}$ pour tout $x \in \mathcal{C}$ (**vérifier cela en détail**),
- les cycles $(x\,\sigma(x) \cdots \sigma^{l-1}(x))$ et $(y\,\sigma(y) \cdots \sigma^{l-1}(y))$ sont égaux pour tous $x, y \in \mathcal{C}$ (**vérifier cela en détail**).

On note $c_{\mathcal{C}}$ le cycle $(x\,\sigma(x) \cdots \sigma^{l-1}(x))$ où $x \in \mathcal{C}$ est quelconque (étant entendu que ce cycle ne dépend pas de $x \in \mathcal{C}$). En particulier $c_{\mathcal{C}}$ est un cycle de longueur $\mathrm{Card}(\mathcal{C})$, de support $\mathcal{C}$, et tel que $\sigma(x) = c_{\mathcal{C}}(x)$ pour tout $x \in \mathcal{C}$.

Théorème.
Soit $\sigma \in \mathscr{S}_n \backslash \{\mathrm{Id}\}$. Il existe une suite $c_1, \ldots, c_p$ de cycles de $\mathscr{S}_n$ de longueur au moins 2 et à supports deux-à-deux disjoints telle que $\sigma = c_1 \cdots c_p$. Cette suite est unique à l'ordre près des termes.

Démonstration. *Existence de la décomposition.* Soit $\mathcal{C}_1, \dots, \mathcal{C}_p$ une énumération des orbites non ponctuelles (*i.e.* ayant au moins deux éléments) de l'action de $\langle\sigma\rangle$ sur $\{1, \dots, n\}$. Pour chaque $i \in \{1, \dots, p\}$ on pose $c_i = c_{\mathcal{C}_i}$. Alors $c_1, \dots, c_p$ sont des cycles de $\mathscr{S}_n$ de longueur au moins 2, à supports deux-à-deux disjoints (**vérifier cela en détail**), et tels que $\sigma = c_1 \cdots c_p$ (**vérifier cela en détail**).

Unicité de la décomposition. Soient $\sigma_1, \dots, \sigma_s$ des cycles de longueur au moins 2, à supports deux-à-deux disjoints, et tels que $\sigma = \sigma_1 \cdots \sigma_s$. On note $\mathrm{Cyc}(\sigma)$ l'ensemble des cycles $c_{\mathcal{C}}$, pour $\mathcal{C}$ parcourant l'ensemble des orbites non ponctuelles de l'action de $\langle\sigma\rangle$ sur $\{1, \dots, n\}$. Il suffit de démontrer que $\{\sigma_1, \dots, \sigma_s\} = \mathrm{Cyc}(\sigma)$.
Soit $c \in \{\sigma_1, \dots, \sigma_s\}$. On note l la longueur de c. Soit $x \in \mathrm{supp}(c)$.
– Une récurrence sur $t \geqslant 0$ démontre que

$$(\forall t \in \mathbb{N}) \quad \begin{cases} \sigma^t(x) = c^t(x) \\ \sigma^t(x) \in \mathrm{supp}(c) \end{cases}$$

(**vérifier cela en détail**). Donc $\langle\sigma\rangle \cdot x = \{x, c(x), \dots, c^{l-1}(x)\}$ (**vérifier cela en détail**).
– $\mathrm{supp}(c) = \{x, c(x), \dots, c^{l-1}(x)\}$ et $c = (x\, c(x) \cdots c^{l-1}(x))$.
Ainsi, $c = c_{\langle\sigma\rangle \cdot x} = (x\, \sigma(x) \cdots \sigma^{l-1}(x))$ et l'orbite $\langle\sigma\rangle \cdot x$ a $l \geqslant 2$ éléments, de sorte que $c \in \mathrm{Cyc}(\sigma)$. Ceci démontre que $\{\sigma_1, \dots, \sigma_s\} \subseteq \mathrm{Cyc}(\sigma)$.
Réciproquement soit $c \in \mathrm{Cyc}(\sigma)$. On note $\mathcal{C}$ l'orbite non ponctuelle de l'action de $\langle\sigma\rangle$ sur $\{1, \dots, n\}$ telle que $c = c_{\mathcal{C}}$. On note l la longueur de c. Soit $x \in \mathcal{C}$. Comme $\mathcal{C}$ est une orbite non ponctuelle, $\sigma(x) \neq x$. Donc $x \in \mathrm{supp}(\sigma)$. Comme $\sigma = \sigma_1 \cdots \sigma_s$ et que $\sigma_1, \dots, \sigma_s$ sont à supports deux-à-deux disjoints, $\mathrm{supp}(\sigma) = \sqcup_j \mathrm{supp}(\sigma_j)$ (**vérifier cela en détail**). On note $j \in \{1, \dots, s\}$ l'indice tel que $x \in \mathrm{supp}(\sigma_j)$ et on note l_j la longueur de σ_j.
– L'étude préliminaire démontre que $c = (x\, \sigma(x) \cdots \sigma^{l-1}(x))$ et $\langle\sigma\rangle \cdot x = \{x, \sigma(x), \dots, \sigma^{l-1}(x)\}$.
– Il suit de la démonstration de l'inclusion $\{\sigma_1, \dots, \sigma_s\} \subseteq \mathrm{Cyc}(\sigma)$ que $\sigma_j = (x\, \sigma(x) \cdots \sigma^{l_j}(x))$ et $\langle\sigma\rangle \cdot x = \{x, \sigma(x), \dots, \sigma^{l_j-1}(x)\}$.
Donc $l = l_j$ puis $c = \sigma_j \in \{\sigma_1, \dots, \sigma_s\}$. Ceci démontre que $\{\sigma_1, \dots, \sigma_s\} = \mathrm{Cyc}(\sigma)$. □

Exemple.

(1) La décomposition en cycles d'un élément de $\mathscr{S}_4 \backslash \{\mathrm{Id}\}$ a l'une des formes suivantes : (ab), (abc), $(abcd)$, $(ab)(cd)$ où $a, b, \dots \in \{1, 2, 3, 4\}$ sont deux-à-deux distincts.

(2) La décomposition en cycles d'un élément de $\mathscr{S}_5 \backslash \{\mathrm{Id}\}$ a l'une des formes suivantes : (ab), (abc), $(abcd)$, $(abcde)$, $(ab)(cd)$, $(ab)(cde)$ où $a, b, \dots \in \{1, 2, 3, 4, 5\}$ sont deux-à-deux distincts.

Le théorème de décomposition en cycles a le corollaire suivant.

Corollaire.
Soit $n \geqslant 2$. L'ensemble des transpositions engendre $\mathscr{S}_n$.

2.b. Interprétation en termes d'actions de groupes

Un des enseignements essentiels de la démonstration de la décomposition des permutations de $\mathscr{S}_n$ en produit de cycles de longueur au moins 2 et à supports deix-à-deux disjoints est le suivant. Pour tout $\sigma \in \mathscr{S}_n$, les supports des cycles apparaissant dans la décomposition de σ sont exactement les orbites non ponctuelles de l'action de $\langle\sigma\rangle$ sur $\{1, \dots, n\}$. De plus, si c est un de ces cycles, si $\mathcal{C}$ désigne son support, et si l désigne sa longueur, alors $c = (x\, \sigma(x) \cdots \sigma^{l-1})$ pour tout $x \in \mathcal{C}$.

2.c. Ordre d'une permutation

Proposition.
Soit σ une permutation de $\mathscr{S}_n$. Soit $\sigma = c_1 \cdots c_p$ la décomposition de σ en produit de cycles de longueur au moins 2 et à supports deux-à-deux disjoints. Pour chaque i on note l_i la longueur de c_i. Alors l'ordre de σ est $\mathrm{ppcm}(l_1, \ldots, l_p)$.

Démonstration. Puisque $\mathscr{S}_n$ est fini, le théorème de Lagrange implique que σ est d'ordre fini. On note d l'ordre de σ. Puisque $c_1, \ldots, c_p$ sont à supports deux-à-deux disjoints, ces cycles commutent deux-à-deux. Donc, pour tout $N \in \mathbb{N}$, on a $\sigma^N = c_1^N \cdots c_p^N$ (**vérifier cela en détail**).

On pose $l = \mathrm{ppcm}(l_1, \ldots, l_p)$. Donc $\sigma^l = c_1^l \cdots c_p^l$. Or $l_i | l$ et l_i est l'ordre de c_i de sorte que $c_i^l = \mathrm{Id}$ pour tout $i \in \{1, \ldots, p\}$, puis $\sigma^l = \mathrm{Id}$. Donc $d | l$.

Pour démontrer que $l = d$ il suffit donc de démontrer que $l_i | d$ (c'est-à-dire $c_i^d = \mathrm{Id}$) pour tout $i \in \{1, \ldots, p\}$. Soit $i \in \{1, \ldots, p\}$; soit $x \in \{1, \ldots, n\}$ appartenant au support de c_i ; il suit de la démonstration du théorème de décomposition que $x, \sigma(x), \ldots, \sigma^{l_i - 1}(x)$ sont deux-à-deux distincts, que $\sigma^{l_i}(x) = x$ et que $c_i = (x\, \sigma(x) \cdots \sigma^{l_i - 1}(x))$; donc, pour tout $N \in \mathbb{N}$ on a $c_i^N(x) = \sigma^N(x) = \sigma^r(x)$ où $r \in \{0, \ldots, l_i - 1\}$ désigne le reste de la division euclidienne de N par l_i (**vérifier cela en détail**) ; ceci est vrai lorsque $N = d$, on en déduit que $\sigma^d(x) = x$ puis que $r = 0$, c'est-à-dire $l_i | d$. □

3. La signature

Définition.
Soit $n \geqslant 2$. Soit $\sigma \in \mathscr{S}_n$. On appelle signature *de σ et on note $\varepsilon(\sigma)$ le rationnel non nul*

$$\prod_{1 \leqslant i < j \leqslant n} \frac{\sigma(i) - \sigma(j)}{i - j}\,.$$

Dans la proposition suivante, $\{-1, 1\}$ est considéré comme groupe, c'est le sous-groupe de $(\mathbb{C}^\times, \times)$ des racines carrées de 1.

Proposition.

(1) La signature d'une transposition quelconque de $\mathscr{S}_n$ est -1.

(2) Pour tout $\sigma \in \mathscr{S}_n$ on a $\varepsilon(\sigma) \in \{-1, 1\}$.

(3) La signature d'un cycle de $\mathscr{S}_n$ est égale à $(-1)^{l-1}$ si l désigne la longueur du cycle.

(4) L'application ε de $\mathscr{S}_n$ dans $\{-1, 1\}$ définie par $\sigma \mapsto \varepsilon(\sigma)$ est un homomorphisme surjectif de groupes.

Démonstration. On démontre d'abord que ε est un homomorphisme de groupes de $\mathscr{S}_n$ dans $(\mathbb{Q}^\times, \times)$.
Soient $\sigma, \tau \in \mathscr{S}_n$. On pose $C = \{(i,j) \in \{1,\dots,n\}^2 \mid i < j\}$:

$$\varepsilon(\sigma\circ\tau) = \prod_{(i,j)\in C} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{i-j} = \prod_{(i,j)\in C} \frac{\sigma(\tau(i)) - \sigma(\tau(j))}{\tau(i)-\tau(j)} \cdot \underbrace{\prod_{(i,j)\in C} \frac{\tau(i)-\tau(j)}{i-j}}_{=\varepsilon(\tau)}.$$

L'application $f\colon C \to C$ définie par $f(i,j) = \begin{cases} (\tau(i),\tau(j)) & \text{si } \tau(i) < \tau(j) \\ (\tau(j),\tau(i)) & \text{si } \tau(j) < \tau(i) \end{cases}$ est bijective (**vérifier cela en détail**). En faisant le changement de variable $(k,l) = f(i,j)$ on a $\prod_{(i,j)\in C} \frac{\sigma(\tau(i))-\sigma(\tau(j))}{\tau(i)-\tau(j)} = \prod_{(k,l)\in C} \frac{\sigma(k)-\sigma(l)}{k-l}$. Donc $\varepsilon(\sigma\circ\tau) = \varepsilon(\sigma)\varepsilon(\tau)$. Ainsi, ε est un homomorphisme de groupes de $\mathscr{S}_n$ dans $\mathbb{Q}^\times$.

(1)

$$\varepsilon((1\,2)) = \frac{\tau(1)-\tau(2)}{1-2} \cdot \prod_{2<j} \frac{\tau(1)-\tau(j)}{1-j} \cdot \prod_{2<j} \frac{\tau(2)-\tau(j)}{2-j} \cdot \prod_{2<i<j} \frac{\tau(i)-\tau(j)}{i-j} = -1$$

Soient $k,l \in \{1,\dots,n\}$ distincts. Soit σ une permutation de $\mathscr{S}_n$ telle que $\sigma(1) = k$ et $\sigma(2) = l$. Donc $\sigma\circ(1\,2)\circ\sigma^{-1} = (k\,l)$ (**vérifier cela en détail**). Comme $\mathbb{Q}^\times$ est commutatif et ε est un homomorphisme de groupes, on a $\varepsilon((k\,l)) = \varepsilon((1\,2)) = -1$.

(2) suit des arguments qui précédent et de ce que $\mathscr{S}_n$ est engendré par les transpositions (**vérifier cela en détail**).

(3) Soit un l-cycle $(a_1\cdots a_l)$. Il est égal à $(a_1\,a_2)\circ(a_2\,a_3)\circ\cdots\circ(a_{l-1}\,a_l)$ (**vérifier cela en détail**). Donc $\varepsilon((a_1\cdots a_l)) = (-1)^{l-1}$ (**vérifier cela en détail**).
(4) suit de ce qui précéde (**vérifier cela en détail**). □

On peut calculer la signature d'une permutation suivant les méthodes suivantes.
- Si $m \in \mathbb{N}$, alors un produit de m transpositions est de signature $(-1)^m$.
- Étant donnée $\sigma \in \mathscr{S}_n$, si $l_1,\dots,l_p$ est la suite des longueurs des cycles apparaissant dans la décomposition de σ en produit de cycles de longueur au moins 2 et à supports deux-à-deux disjoints, alors $\varepsilon(\sigma) = (-1)^{(l_1-1)+\cdots+(l_p-1)}$.
- Étant donnée $\sigma \in \mathscr{S}_n$, si N est le nombre d'orbites de l'action de $\langle\sigma\rangle$ sur $\{1,\dots,n\}$, alors $\varepsilon(\sigma) = (-1)^{n-N}$. Cela suit de l'écriture précédente et du lien entre cette action et la décomposition de σ en produit de cycles de longueur au moins 2 et à supports disjoints (**vérifier cela en détail**).

Théorème (Caractérisation de la signature)**.**
Soit $n \geqslant 2$. La signature est un homomorphisme de groupes surjectif de $\mathscr{S}_n$ dans $(\{-1,1\},\times)$. C'est l'unique homomorphisme de groupes non trivial de $\mathscr{S}_n$ dans $(\{-1,1\},\times)$.

Démonstration. La première assertion a déjà été démontrée. Soit φ un homomorphisme de groupes de $\mathscr{S}_n$ dans $\{-1,1\}$. On suppose que $\varphi((1\,2)) = 1$. L'argument démontrant (1) dans la proposition précédente démontre que $\varphi(\tau) = 1$ pour toute transposition τ (**vérifier cela en détail**). Comme $\mathscr{S}_n$ est engendré par l'ensemble de ses transpositions, on déduit que $\varphi(\sigma) = 1$ pour tout $\sigma \in \mathscr{S}_n$ (**vérifier cela en détail**). Donc φ est trivial. Par contraposée, si φ est non trivial, alors $\varphi((1\,2)) = -1$. Donc $\varphi(\tau) = -1$ pour toute transposition τ de $\mathscr{S}_n$ (**vérifier cela en détail**). Donc $\varphi = \varepsilon$ (**vérifier cela en détail**). □

Exercice.
Soit un entier $n \geqslant 2$.

(1) Démontrer qu'il existe une et une seule application de $\mathscr{S}_n/\mathrm{Ker}(\varepsilon)$ dans $\{-1, 1\}$ telle que pour tout $\sigma \in \mathscr{S}_n$, l'image de $\sigma\mathrm{Ker}(\varepsilon)$ soit $\varepsilon(\sigma)$.

(2) Démontrer que cette application est bijective.

(3) En déduire que $\mathrm{Ker}(\varepsilon)$ est d'ordre $\frac{n!}{2}$.

Définition.
Soit un entier $n \geqslant 1$. Le noyau de la signature sur $\mathscr{S}_n$ est appelé groupe alterné *et noté $\mathscr{A}_n$.*

CHAPITRE 4

Sous-groupes distingués, groupes quotients

1. Comparaison des classes à gauche et des classes à droite

Soit $(G, \times)$ un groupe, soit H un sous-groupe de G. On note π la surjection canonique de G dans l'ensemble quotient G/H. On rappelle que, pour tout $g \in G$, on a $\pi(g) = gH$. On rappelle également que la classe à gauche (resp. à droite) d'un élément $g \in G$ modulo H est l'élément Hg (resp. gH) de l'ensemble quotient $H\backslash G$ (resp. G/H).

Exercice.
Soit $(G, \times)$ un groupe. Soit H un sous-groupe de G.

(1) Démontrer qu'il existe une et une seule application de G/H dans $H\backslash G$ qui, pour tout $g \in G$, associe la classe à droite $g^{-1}H$ à la classe à gauche Hg.

(2) Démontrer qu'il n'existe pas, en général, d'application de l'ensemble quotient G/H dans l'ensemble quotient $H\backslash G$ qui, pour tout $g \in G$, associe la classe à droite gH à la classe à gauche Hg.

Il suit du théorème sur le passage au quotient d'une application par une relation d'équivalence et de la démonstration de ce théorème que

(1) pour toute application Ψ de $G/H \times G/H$ dans G/H, l'application ψ de $G \times G$ dans G/H définie par $(g_1, g_2) \mapsto \Psi(g_1H, g_2H)$ vérifie la propriété suivante notée $(\star)$

$$(\forall (g_1, g_2) \in G \times G)\ (\forall (g_1', g_2') \in G \times G)\quad \left\{ \begin{array}{l} g_1H = g_1'H \\ g_1H = g_2'H \end{array} \right. \Rightarrow \psi(g_1, g_2) = \psi(g_1', g_2')$$

(2) pour toute application ψ de $G \times G$ dans G/H vérifiant $(\star)$ il existe une et une seule application Ψ de $G/H \times G/H$ dans G/H telle que, pour tout $(g_1, g_2) \in G \times G$, on a $\Psi(g_1H, g_2H) = \psi(g_1, g_2)$,

(**vérifier cela en détail**).

Exercice.
Quelle est la relation d'équivalence sur $G \times G$ telle que les points (1) et (2) ci-dessus correspondent exactement à l'énoncé du passage au quotient par cette relation d'équivalence des applications définies sur $G \times G$?

Proposition.
Soit $(G, \times)$ un groupe. Soit H un sous-groupe de G. Les conditions suivantes sont équivalentes.

(i) Pour tout $g \in G$, les classes à gauche et à droite de g modulo H coïncident.

(ii) Pour tout $g \in G$, on a $gHg^{-1} = H$.

(iii) Pour tous $g \in G$, on a $gHg^{-1} \subseteq H$.

(iv) Il existe une structure de groupe sur l'ensemble G/H telle que la surjection canonique $G \to G/H$ soit un homomorphisme de groupes.

Lorsque ces conditions sont satisfaites, la structure de groupe sur G/H telle que dans (iii) est unique. Si on note $\times$ la loi de composition interne associée, elle vérifie

$$(\forall g_1, g_2 \in G) \quad g_1H \times g_2H = g_1g_2H\,.$$

Démonstration. On rappelle que si A est un sous-ensemble de G et si $g, h \in G$ alors on note gAh le sous-ensemble $\{x \in G \mid (\exists a \in A)\ x = gah\}$ de G. En particulier, $gH = gHe$ et $Hg = eHg$. Par ailleurs, pour tous $g', h' \in G$ on a $g'(gAh)h' = (g'g)A(hh')$ (**vérifier cela en détail**).

Il suit de ce rappel que, pour tout $g \in G$, on a

$$gH = Hg \Leftrightarrow gHg^{-1} = H\,.$$

D'où l'équivalence $(i) \Leftrightarrow (ii)$.

Comme l'application de G dans G définie par $g \mapsto g^{-1}$ est bijective (**vérifier cela en détail**), il suit aussi de ce rappel que les deux assertions suivantes sont équivalentes

(i) $(\forall g \in G)\ gHg^{-1} \subseteq H$,

(ii) $(\forall g \in G)\ H \subseteq gHg^{-1}$,

(**vérifier cela en détail**). D'où l'équivalence $(ii) \Leftrightarrow (iii)$.

On suppose à présent que les conditions équivalentes (i), (ii) et (iii) sont satisfaites et on démontre (iv).
Soit ψ l'application de $G \times G$ dans G/H définie par $(g_1, g_2) \mapsto g_1g_2H$. On démontre que ψ vérifie la condition $(\star)$ énoncée avant la proposition. Soient (g_1, g_2) et (g_1', g_2') dans $G \times G$ tels que $g_1H = g_1'H$ et $g_2H = g_2'H$. Donc, en utilisant successivement que $g_2H = g_2'H$, $g_2'H = Hg_2'$ $((i))$ et $g_1H = g_1'H$, on obtient $\psi(g_1, g_2) = \psi(g_1', g_2')$ (**vérifier cela en détail**). Il existe donc une et une seule application ψ de $G/H \times G/H$ dans G/H telle que, pour tout $(g_1, g_2) \in G \times G$, on a $\Psi(g_1H, g_2H) = g_1g_2H$.
On démontre maintenant que $\psi\colon G/H \times G/H \to G/H$ munit G/H d'une structure de groupe. Pour simplifier on note $\alpha \times \beta$ au lieu de $\psi(\alpha, \beta)$. Soient $\alpha, \beta, \gamma \in G/H$, il existe $g, h, k \in G$ tels que $\alpha = gH$, $\beta = hH$ et $\gamma = kG$ et
– $(\alpha \times \beta) \times \gamma = (ghk)H = \alpha \times (\beta \times \gamma)$ (**vérifier cela en détail**),
– $\alpha \times H = \psi(gH, eH) = gH = \psi(eH, gH) = H \times \alpha$,
– $\alpha \times g^{-1}H = g^{-1}H \times \alpha = H$ (**vérifier cela en détail**),
en particulier l'élément neutre de $(G/H, \times)$ est $H = eH$, et l'inverse de $\alpha = gH$ est $g^{-1}H$. Pour cette structure de groupe sur G/H la surjection canonique $\pi\colon G \to G/H$ est, par construction, un homomophisme de groupes (**vérifier cela en détail**).
Enfin, l'unicité de la structure de groupe de G/H telle que la surjection canonique $G \to G/H$ soit un homomorphisme suit de l'unicité de ψ (**vérifier cela en détail**).

Pour terminer la démonstration on suppose (iv) et on démontre (iii). Soit $g \in G$. L'élément neutre de G/H étant la classe H, on a

$$\pi(g) = H \Leftrightarrow gH = H \Leftrightarrow g \in H\,.$$

Donc $H = \mathrm{Ker}(\pi)$. Soit $h \in H$. Donc $\pi(ghg^{-1}) = \pi(g)\pi(h)\pi(g)^{-1}$. Or $\pi(h) = H$ est l'élément neutre de G/H de sorte que $\pi(ghg^{-1}) = H$. Donc $ghg^{-1} \in H$. Ceci démontre que, pour tout $g \in G$, on a $gHg^{-1} \subseteq H$. D'où (iii). □

Définition (Sous-groupe distingué et groupe quotient)**.**
Soit $(G, \times)$ un groupe.

(1) Un sous-groupe distingué *de G est un sous-groupe H de G tel que, pour tout $g \in G$, on a $gHg^{-1} = H$. Cette propriété est notée $H \lhd G$.*

(2) Soit H un sous-groupe distingué de G. Le groupe quotient *de G par H est l'ensemble quotient G/H muni de la structure de groupe unique telle que la surjection canonique $G \to G/H$ soit un homomorphisme de groupes.*

Il suit de la démonstration de la proposition précédente que si $H \lhd G$ alors H est le noyau de la surjection canonique.

Si H est un sous-groupe distingué de G, alors la loi de composition interne du groupe quotient G/H est telle que

$$(\forall g_1, g_2 \in G) \quad g_1H \times g_2H = g_1g_2H\,.$$

L'élément neutre est la classe $H = eH$. L'inverse d'une classe gH est $g^{-1}H$. En particulier, si G est abélien, alors G/H est abélien.

Étant donné deux sous-ensembles A, B de G, on note $A \cdot B$ le sous-ensemble $\{ab \mid a \in A, b \in B\}$. Une classe à droite gH modulo un sous-groupe H de G n'est alors autre que $g \cdot H$. On a donc $g_1H \cdot g_2H = g_1g_2H$ (au sens de la notation introduite) pour tous $g_1, g_2 \in H$ si et seulement si $H \lhd G$. Ainsi, les sous-groupes distingués de G sont exactement ceux pour lesquels l'opération $\cdot$ est une structure de groupe sur l'ensemble des classes à droite de G modulo ce sous-groupe.

Exemple.

(1) Soit $(G, \times)$ un groupe. Alors $\{e\} \lhd G$ et $G \lhd G$.

(2) Le sous-groupes d'un groupe abélien sont tous distingués.

(3) Soit un entier $n \geqslant 1$. Alors $n\mathbb{Z} \lhd \mathbb{Z}$. Le groupe quotient $\mathbb{Z}/n\mathbb{Z}$ est cyclique d'ordre n. Si on note $i \bmod n$ la classe modulo $n\mathbb{Z}$ d'un élément $i \in \mathbb{Z}$, alors $\mathbb{Z}/n\mathbb{Z}$ est engendré par $1 \bmod n$.

Soit un entier $n \geqslant 1$. Le groupe abélien quotient $(\mathbb{Z}/n\mathbb{Z}, +)$ est donc tel que pour tous $a, b \in \mathbb{Z}$ on a

- $0 \bmod n$ est l'élément neutre du groupe,
- $(a \bmod n) + (b \bmod n) = (a + b) \bmod n$,
- $-(a \bmod n) = (-a) \bmod n$.

Il est d'ordre n et engendré par l'élément $1 \bmod n$ (**vérifier cela en détail**).

Exercice.
Soit un entier $n \geqslant 1$. Soit π la surjection canonique de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$. Soit $i \in \mathbb{Z}$.

(1) Démontrer que $\pi(i)$ est un générateur de $\mathbb{Z}/n\mathbb{Z}$ si et seulement si $\text{pgcd}(i,n) = 1$.

(2) Démontrer que l'ordre de $\pi(i)$ est égal à $\frac{n}{\text{pgcd}(n,i)}$.

Exercice.
Soit φ un homomorphisme de groupes de G dans un groupe $(K, \times)$.

(1) Démontrer que si $H \lhd K$ alors $\varphi^{-1}(H) \lhd G$.

(2) On suppose que l'application φ est surjective. Démontrer que si $H \lhd G$ alors $\varphi(H) \lhd K$.

Exercice.

(1) Soit H un sous-groupe de G. On suppose que $\psi(H) \subseteq H$ pour tout automorphisme ψ de G. Démontrer que $H \lhd G$.

(2) Déduire de la question précédente que $Z(G) \lhd G$.

Exercice.

(1) Démontrer que les sous-groupes distingués du groupe alterné $\mathscr{A}_4$ sont $\{\text{Id}\}$, $\{\text{Id}, (12)(34), (13)(24), (14)(23)\}$ et $\mathscr{A}_4$.

(2) On note V_4 le seul sous-groupe distingué de $\mathscr{A}_4$ qui soit d'ordre 4. Démontrer que $V_4 \lhd \mathscr{S}_4$.

(3) Démontrer que le groupe quotient $\mathscr{A}_4/V_4$ est cyclique. Est-ce qu'il en est de même pour $\mathscr{S}_4/V_4$?

2. Caractérisation des sous-groupes distingués

La proposition suivante caractérise les sous-groupes distingués d'un groupe donné comme les noyaux des homomorphismes de groupes de G dans un groupe.

Proposition.
Soit $(G, \times)$ un groupe. Soit H un sous-groupe de G. Les conditions suivantes sont équivalentes.

(i) $H \lhd G$.

(ii) Il existe un homomorphisme de groupes φ de G dans un groupe tel que que $\text{Ker}(\varphi) = H$.

Démonstration. Si $H \lhd G$ alors H est la surjection canonique de G dans G/H est un homomorphisme de groupes et son noyau est H. Réciproquement, si il existe un groupe $(K, \times)$ et un homomorphisme de groupes φ de G dans K tel que $H = \text{Ker}(\varphi)$ alors, pour tous $g \in G$ et $h \in H$ on a

$$\varphi(ghg^{-1}) = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(g)\varphi(g)^{-1} = e$$

de sorte que $ghg^{-1} \in \text{Ker}(\varphi)$. Donc $gHg^{-1} \subseteq H$ pour tout $g \in G$. Donc $H \lhd G$. □

Exemple.
Soit n un entier naturel non nul. Le groupe alterné $\mathscr{A}_n$ est le noyau de la signature $\epsilon : \mathscr{S}_n \to \{\pm 1\}$. Donc $\mathscr{A}_n \lhd \mathscr{S}_n$.

Exercice.
Démontrer que $\text{SL}_n(\mathbb{R}) \lhd \text{GL}_n(\mathbb{R})$ et que $\text{SO}_n(\mathbb{R}) \lhd \text{GL}_n(\mathbb{R})$.

3. Passage au quotient d'un homomorphisme de groupes

Théorème.
Soit φ un homomorphisme d'un groupe $(G, \times)$ dans un goupe $(K, \times)$. Soit H un sous-groupe distingué de G. On note $\pi\colon G \to G/H$ la surjection canonique. Les conditions suivantes sont équivalentes.

(i) $H \subseteq \mathrm{Ker}(\varphi)$.

(ii) Il existe un homomorphisme de groupes $\overline{\varphi}\colon G/H \to K$ tel que $\overline{\varphi} \circ \pi = \varphi$.

Lorsque ces conditions sont satisfaites, l'homomorphisme $\overline{\varphi}$ tel que dans (ii) est unique. Il vérifie $\overline{\varphi}(gH) = \varphi(g)$ pour tout $g \in G$. De plus, $\mathrm{Im}(\varphi) = \mathrm{Im}(\overline{\varphi})$.

Démonstration. On suppose (i). Soit $\mathcal{R}$ la relation d'équivalence sur G définie par l'action de H à droite sur G par translation. Donc

$$(\forall g_1, g_2) \in G) \quad g_1 \mathcal{R} g_2 \Leftrightarrow g_1 H = g_2 H\,.$$

On rappelle que $G/\mathcal{R} = G/H$ et que la classe d'équivalence d'un élément $g \in G$ quelconque est gH.
Soient $g_1, g_2 \in G$ tels que $g_1 \mathcal{R} g_2$. Donc il existe $h \in H$ tel que $g_2 = g_1 h$. Donc $\varphi(g_2) = \varphi(g_1)$ (**vérifier cela en détail**). D'après le théorème de passage au quotient des applications par les relations d'équivalence, il existe une unique application $\overline{\varphi}$ de G/H dans K telle que $\overline{\varphi} \circ \pi = \varphi$. En particulier, pour tout $g \in G$, on a $\overline{\varphi}(gH) = \overline{\varphi}(\pi(g)) = \varphi(g)$.
Pour démontrer (ii) il suffit donc de démontrer que $\overline{\varphi}$ est un homomorphisme de groupes. Soient $\alpha, \beta \in G/H$. Il existe $g_1, g_2 \in G$ tels que $\alpha = \pi(g_1)$ et $\beta = \pi(g_2)$. Comme π et φ sont des homomorphismes de groupes, on déduit que

$$\overline{\varphi}(\alpha\beta) = \overline{\varphi}(\pi(g_1 g_2)) = \varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = \overline{\varphi}(\alpha)\overline{\varphi}(\beta)\,.$$

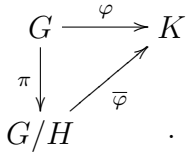
Ceci démontre (ii).

On suppose que (i) et (ii) sont satisfaites. L'égalité $\mathrm{Im}(\overline{\varphi}) = \mathrm{Im}(\varphi)$ suit de l'égalité $\overline{\varphi} \circ \pi = \varphi$ et de ce que π est une application surjective (**vérifier cela en détail**). □

Exercice.
Sous les hypothèses du théorème précédent et en conservant les mêmes notations, démontrer les assertions suivantes

(1) $H \lhd \mathrm{Ker}(\varphi)$,
(2) le noyau de $\overline{\varphi}$ est égal à $\mathrm{Ker}(\varphi)/H$.

En reprenant les notations et hypothèses du résultat précédent, on dit que $\overline{\varphi}\colon G/H \to K$ est obtenu à partir de $\varphi\colon G \to K$ par *passage au quotient* par H. On traduit la propriété "$\overline{\varphi} \circ \pi = \varphi$" en disant que le diagramme suivant *commute*



Un *diagramme commutatif* est un dessin sur comportant des noms de groupes et des flèches représentant des homomorphismes entre ce groupes. La commutativité signifie que si deux chemins partent du même groupe et arrivent dans le même

groupe, alors les compositions correspondantes sont égales. Parmi les flèches, on utilise "$\twoheadrightarrow$" (resp. "$\hookrightarrow$") pour désigner les surjections (resp. inclusions) canoniques.

Exemple.
Soit $(G, \times)$ un groupe. Soit un entier $n \geqslant 1$. Soit $\pi\colon \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ la surjection canonique. Si on combine le résultat précédent et la description des homomorphismes de groupes de $\mathbb{Z}$ dans G, on retrouve que la donnée d'un homomorphisme de groupes φ de $\mathbb{Z}/n\mathbb{Z}$ dans G est équivalente à celle d'un élément $g \in G$ tel que $g^n = e$. Si on note $\bar{i}$ la classe à gauche d'un élément $i \in \mathbb{Z}$ modulo $n\mathbb{Z}$ alors cette correspondance est telle que $\varphi(\bar{i}) = g^i$.

Exercice.
Soit un entier $n \geqslant 1$.

(1) Démontrer qu'il existe un unique homomorphisme de groupes de $(\mathbb{Z}/n\mathbb{Z}, +)$ dans $(\mathbb{U}_n, \times)$ tel que l'image de $1 \bmod n$ soit $\exp\left(\frac{2i\pi}{n}\right)$.

(2) Démontrer que cet homomorphisme est un isomorphisme.

Étant donnés deux groupes $(G, \times)$ et $(K, \times)$ ainsi qu'un homomorphisme de groupes φ de G dans K, si on note ι l'inclusion canonique de $\mathrm{Im}(\varphi)$ dans K (définie par $\iota(x) = x$ pour tout $x \in \mathrm{Im}(\varphi)$), alors l'application de G dans $\mathrm{Im}(\varphi)$ définie par $g \mapsto \varphi(g)$ est correctement définie et c'est un homomorphisme de groupes (**vérifier cela en détail**). C'est même l'unique homomorphisme de groupes de G dans $\mathrm{Im}(\varphi)$ dont la composition avec ι est égale à φ (**vérifier cela en détail**). Le noyau de cet homomorphisme est égal à celui de φ (**vérifier cela en détail**).

Corollaire.
Soit φ un homomorphisme d'un groupe $(G, \times)$ dans un groupe K. Soit π la surjection canonique de G dans $G/\mathrm{Ker}(\varphi)$. Soit ι l'injection canonique de $\mathrm{Im}(\varphi)$ dans K (définie par $\iota(x) = x$). Il existe un et un seul homomorphisme de groupes $\tilde{\varphi}$ de $G/\mathrm{Ker}(\varphi)$ dans $\mathrm{Im}(\varphi)$ tel que $\varphi = \iota \circ \tilde{\varphi} \circ \pi$. De plus $\tilde{\varphi}$ est un isomorphisme.

Démonstration. D'après la caractérisation des sous-groupes distingués, on a $\mathrm{Ker}(\varphi) \lhd G$.
Soit $\overline{\varphi}$ l'homomorphisme obtenu à partir de φ par passage au quotient par $\mathrm{Ker}(\varphi)$. Donc $\mathrm{Im}(\overline{\varphi}) = \mathrm{Im}(\varphi)$.
On démontre que $\overline{\varphi}$ est injectif. Soit $x \in G/\mathrm{Ker}(\varphi)$ tel que $\overline{\varphi}(x) = e$. Il existe $g \in G$ tel que $x = \pi(g)$. Donc $\overline{\varphi}(\pi(g)) = e$, c'est-à-dire $\varphi(g) = e$. Donc $g \in \mathrm{Ker}(\varphi)$ puis $x = e$ (**vérifier cela en détail**). Donc $\overline{\varphi}$ est bien injectif.
D'après la discussion précédant le corollaire il existe un unique homomorphisme de groupes $\tilde{\varphi}$ de $G/\mathrm{Ker}(\varphi)$ dans $\mathrm{Im}(\varphi)$ tel que $\iota \circ \tilde{\varphi} = \overline{\varphi}$. Il suit de cette même discussion et des propriétés de $\overline{\varphi}$ énoncées ci-dessus que $\tilde{\varphi}$ convient (**vérifier cela en détail**). □

Au sens évoqué précédemment, le diagramme suivant est donc commutatif

$$\begin{array}{ccc} G & \xrightarrow{\varphi} & K \\ \downarrow & & \uparrow \iota \\ G/\mathrm{Ker}(\varphi) & \xrightarrow[\tilde{\varphi}]{\sim} & \mathrm{Im}(\varphi)\,. \end{array}$$

Le corollaire précédent est souvent appliqué comme suit. Étant donné φ un homomorphisme surjectif de groupes de $(G, \times)$ dans $(K, \times)$ il existe un unique isomorphisme de groupes $\tilde{\varphi}$ de $G/\mathrm{Ker}(\varphi)$ dans K tel que $\tilde{\varphi} \circ \pi = \varphi$.

4. Théorème d'isomorphisme

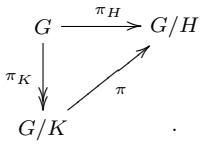
Théorème.
Soit $(G, \times)$ un groupe. Soient H, K des sous-groupes distingués de G. On suppose que $K \subseteq H$. On note $\pi_H \colon G \to G/H$ et $\pi_K \colon G \to G/K$ les surjections canoniques. Soit $\iota \colon K \to H$ l'inclusion canonique.

(1) H/K est un sous-groupe distingué de G/K, égal à $\pi_K(H)$.

(2) Il existe un unique homomorphisme surjectif de groupes de G/K dans G/H tel que l'image de gK soit gH pour tout $g \in G$. Son noyau est H/K. Par passage au quotient par H/K il induit isomorphisme de $(G/K)/(H/K)$ dans G/H.

Démonstration. (1) Soit $\alpha \in H/K$. Il existe $h \in H$ tel que $\alpha = hK$. Donc $\alpha \in G/K$. Ainsi $H/K \subseteq G/K$. On a $H/K = \pi_K(H)$ (**vérifier cela en détail**). Comme π_K est un homomorphisme surjectif de groupes et comme $H \lhd G$ on déduit par ailleurs que $H/K \lhd G$ (**vérifier cela en détail**).

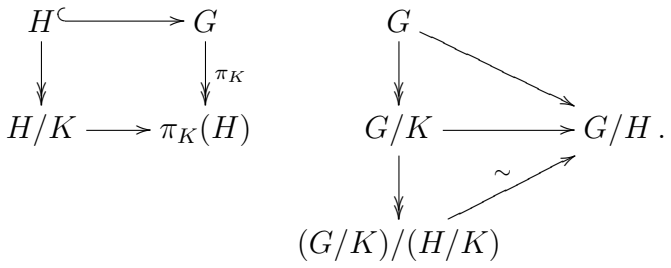
(2) On a $K \subseteq H$ et $H = \mathrm{Ker}(\pi_H)$. Donc il existe un unique homomorphisme de groupes π de G/K dans G/H tel que le diagramme suivant soit commutatif



.

De plus $\mathrm{Im}(\pi) = \mathrm{Im}(\pi_K)$ donc π est un homomorphisme surjectif. On détermine le noyau de π. On a $\mathrm{Ker}(\pi) = \pi^{-1}(\{e\})$. On s'appuie sur l'égalité $\pi_H = \pi \circ \pi_K$. Elle donne $\pi_H^{-1}(\{e\}) = \pi_K^{-1}(\pi^{-1}(\{e\}))$, c'est-à-dire $H = \pi_K^{-1}(\mathrm{Ker}(\pi))$. Or π_K est une application surjective de sorte que $\pi_K(\pi_K^{-1}(\mathrm{Ker}(\pi))) = \mathrm{Ker}(\pi)$ (**vérifier cela en détail**). Donc $\pi_K(H) = \mathrm{Ker}(\pi)$. Ainsi $\mathrm{Ker}(\pi) = H/K$. Puisque π est une application surjective, son passage au quotient par H/K induit bien un isomorphisme de $(G/K)/(H/K)$ dans G/H. □

Le résultat précédent se comprend mieux au moyen des diagrammes commutatifs suivants



CHAPITRE 5

Théorèmes de Sylow

1. Définition et exemples

Définition.
Soit $(G, \times)$ un groupe fini. Soit p un entier premier divisant $|G|$. Soient $\alpha, m \in \mathbb{N}\backslash\{0\}$ tels que $|G| = p^\alpha m$ et $p \not| m$. On appelle p-sous-groupe de Sylow de G tout sous-groupe d'ordre p^α.

D'après le théorème de Lagrange, si $(G, \times)$ est un groupe et si p est un entier premier divisant son ordre alors un sous-groupe H de G est un p-sous-groupe de Sylow si et seulement si

(a) H est un p-groupe,

(b) p ne divise pas $\frac{|G|}{|H|}$.

Exemple.
On suppose que G est cyclique d'ordre $p^\alpha m$ où p, α, m sont tels que dans la définition. Soit g un générateur de G. Alors $\langle g^m \rangle$ est l'unique sous-groupe de G d'ordre p^α (**vérifier cela en détail**).

Exemple.
Les 3-sous-groupes de Sylow de $\mathscr{S}_3$ sont d'ordre 3. Ce sont donc les sous-groupes engendrés par les 3-cycles. Donc il n'y a qu'un seul 3-sous-groupe de Sylow dans $\mathscr{S}_3$, c'est $\langle (123) \rangle$.

Exemple.
Les 3-sous-groupes de Sylow de $\mathscr{S}_4$ sont d'ordre 3. Ce sont donc les sous-groupes engendrés par les 3-cycles.

Exercice.
Démontrer que le nombre de 3-sous-groupes de Sylow de $\mathscr{S}_4$ est 4. Dresser la liste de ces sous-groupes.

Exemple.
Les 2-sous-groupes de Sylow de $\mathscr{S}_4$ sont d'ordre 8. Pour en trouver un on utilise l'action de $\mathscr{S}_4$ sur l'ensemble de ses sous-groupes par conjugaison. Si deux permutations de $\mathscr{S}_4$ sont conjuguées alors elles engendrent des sous-groupes conjugués de $\mathscr{S}_4$ (**vérifier cela en détail**). Les sous-groupes de $\mathscr{S}_4$ qui sont cycliques et d'ordre 4 forment donc une orbite ; un tel sous-groupe contient deux 4-cycles et il est déterminé par ceux-là ; enfin un 4-cycle donné appartient a exactement un sous-groupe cyclique d'ordre 4. Puisqu'il y a six 4-cycles dans $\mathscr{S}_4$ on déduit qu'il y a $\frac{6}{2} = 3$ sous-groupes de $\mathscr{S}_4$ qui sont cycliques et d'ordre 4. On déduit de

l'équation aux classes que le stabilisateur de l'un deux est d'ordre $\frac{24}{3} = 8$. Le stabilisateur du sous-groupe engendré par un 4-cycle est donc un 2-sous-groupe de Sylow de $\mathscr{S}_4$.

Exercice. (1) Démontrer que $\langle (1234), (13) \rangle$ est un 2-sous-groupe de Sylow de $\mathscr{S}_4$. Dresser la liste de ses éléments.

(2) Démontrer que le nombre de 2-sous-groupes de Sylow de $\mathscr{S}_4$ est 3.

2. Le premier théorème de Sylow

2.a. Sur le nombre de parties de cardinal p^α d'un groupe

Lemme.
Soit p un entier premier. Soit m un entier naturel non nul. Alors

$$C_{mp^\alpha}^{p^\alpha} = m \bmod p\,.$$

Démonstration. *Idée directrice de la démonstration :* lorsqu'un p-groupe agit sur un ensemble de cardinal N de sorte que l'action a n points fixes, il suit de l'équation aux classes que $N = n \bmod p$; la démonstration introduit donc une action de groupe de sorte que la congruence de l'énoncé découle ainsi de l'équation l'équation aux classes.

Soit $G = \mathbb{Z}/p^\alpha\mathbb{Z}$. Soit $A = \{1, \ldots, m\}$. Donc $|G \times A| = p^\alpha m$. On fait agir G sur $G \times A$ par $g \cdot (x, a) = (gx, a)$. On note $\mathcal{C}$ l'ensemble des parties de $G \times A$ de cardinal p^α. Donc $\mathcal{C}$ a $C_{mp^\alpha}^{p^\alpha}$ éléments. Étant donné $P \in \mathcal{C}$ et $g \in G$ on note $g \cdot P$ la partie $\{(x, a) \in G \times A \mid (\exists (y, b) \in G \times A)\ (x, a) = g \cdot (y, b)\}$ de $G \times A$; elle est de cardinal p^α. Ceci définit une action de G sur $\mathcal{C}$ (**vérifier cela en détail**).

Soit $P \in \mathcal{C}$ tel que $g \cdot P = P$ pour tout $g \in G$; soit $(x, a) \in P$; soit $g \in G$ alors $(g, a) = gx^{-1} \cdot (x, a) \in P$; ainsi $G \times \{a\} \subseteq P$; pour des raisons de cardinal on déduit que $P = G \times \{a\}$. Réciproquement pour tout $a \in A$ la partie $G \times \{a\}$ de $G \times A$ est de cardinal p^α et son stabilisateur est G (**vérifier cela en détail**). Ainsi il y a autant d'éléments de $\mathcal{C}$ dont le stabilisateur est G que d'éléments dans A, à savoir m.

La congruence annoncée suit donc de ce dénombrement et du corollaire à l'équation aux classes pour les p-groupes. □

2.b. L'existence des sous-groupes de Sylow

Théorème.
Soit $(G, \times)$ un groupe fini. Soit p un entier premier divisant son cardinal. Il existe un p-sous-groupe de Sylow dans G.

Démonstration. Soient α et m les entiers naturels non nuls tels que $|G| = p^\alpha m$ et $p \not| m$.

Idée directrice de la démonstration : G agit naturellement (par translation) sur l'ensemble de ses parties de cardinal p^α ; la congruence du paragraphe précédent et le fait que $p \not| m$ impliquent (*via* l'équation aux classes) qu'il existe une partie P dont le cardinal de l'orbite n'est pas divisible par p ; en utilisant à nouveau l'équation aux classes on conclut que le stabilisateur de P est p^α, en particulier c'est un p-sous-groupe de Sylow.

Soit $\mathcal{C}$ l'ensemble des parties de G de cardinal p^α. Étant donné $P \in \mathcal{C}$ et $g \in G$ on note $g \cdot P$ la partie $\{x \in G \mid (\exists y \in P)\ x = gy\}$ de G, elle est de cardinal p^α car la multiplication de G dans G par un élément de G donné est bijective. Ceci définit une action de G sur $\mathcal{C}$. On a $|\mathcal{C}| = C^{p^\alpha}_{mp^\alpha}$ et, si toutes les orbites étaient de cardinal divisible par p, on aurait (d'après l'équation aux classes) $C^{p^\alpha}_{mp^\alpha} = 0 \bmod p$; cela serait en contradiction avec la congruence du lemme précédent (vu que $p \not| m$ et que p est premier). Il existe donc $P \in \mathcal{C}$ tel que p ne divise pas le cardinal de l'orbite de P (qui est égal à $\frac{|G|}{|\mathrm{Stab}_G(P)|}$). Donc p^α divise $|\mathrm{Stab}_G(P)|$, en particulier $|\mathrm{Stab}_G(P)| \geqslant p^\alpha$. Pour conclure, soit $x \in P$ alors $\mathrm{Stab}_G(P)x$ est contenu dans P et a autant d'éléments que $\mathrm{Stab}_G(P)$ (**vérifier cela en détail**), donc $|\mathrm{Stab}_G(P)| \leqslant p^\alpha$. Ainsi, $\mathrm{Stab}_G(P)$ est un p-sous-groupe de Sylow de G. □

3. Le deuxième théorème de Sylow

3.a. Comment trouver un sous-groupe de Sylow d'un sous-groupe

Proposition.
Soit $(G, \times)$ un groupe fini. Soit p un entier premier divisant son ordre. Soit S un p-sous-groupe de Sylow de G. Soit H un sous-groupe de G. Il existe $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-sous-groupe de Sylow de H.

Démonstration. L'action de G sur G/S par translation se restreint en une action de H sur G/S (si $h \in H$ et si gS est une classe à droite alors $h \cdot gS = hgS$) que l'on prend en compte dans cette démonstration.
Idée directrice de la démonstratrion : étant donné $g \in G$, le sous-groupe $gSg^{-1} \cap H$ est le stabilisateur de gS pour cette action ; dire que $gSg^{-1} \cap H$ est un p-sous-groupe de Sylow est équivalent à dire que l'orbite de gS (sous l'action de H) est de cardinal non divisible par p ; l'existence d'une telle orbite est garantie par l'équation aux classes et le fait que $|G/S|$ n'est pas divisible par p.

D'après l'équation aux classes, $|G/S|$ est égal à la somme des cardinaux des orbites de l'action de H sur G/S. Par ailleurs $p \not| |G/S|$ puisque S est un p-sous-groupe de Sylow de G. Il existe donc $g \in G$ tel que l'orbite de gS ait un cardinal non divisible par p. On note gS cette classe. Le stabilisateur de gS pour l'action de G sur G/S par translation est gSg^{-1}. Donc, par restriction, le stabilisateur de gS pour l'action de H sur G/S est $gSg^{-1} \cap H$ (**vérifier cela en détail**). Ainsi,
- d'après le théorème de Lagrange, le sous-groupe $gSg^{-1} \cap H$ du p-groupe gSg^{-1} est d'ordre une puissance de p, et
- l'orbite de gS (pour l'action de H) est de cardinal $\frac{|H|}{|gSg^{-1} \cap H|}$ (lequel n'est donc pas divisible par p).

Donc $gSg^{-1} \cap H$ est un p-sous-groupe de Sylow de H. □

3.b. Les p-sous-groupes de Sylow sont tous conjugués

Théorème.
Soit $(G, \times)$ un groupe fini. Soit p un entier premier divisant son ordre. Soient α et m les entiers naturels non nuls tels que $|G| = p^\alpha m$ et $p \not| m$.

(1) Les p-sous-groupes de Sylow forment une orbite pour l'action de conjugaison de G sur l'ensemble de ses sous-groupes.

(2) leur nombre est congru à 1 modulo p et divise m.

Démonstration. (1) Soient deux p-sous-groupes de Sylow S_1 et S_2 de G. D'après le paragraphe précédent il existe $g \in G$ tel que $gS_1g^{-1} \cap S_2$ soit un p-sous-groupe de Sylow de S_2. Or S_2 est d'ordre une puissance de p donc il est son unique p-sous-groupe de Sylow. Donc $S_2 = gS_1g^{-1} \cap S_2$, puis $S_2 = gS_1g^{-1}$ pour des raisons de cardinal.

(2) Soit $\mathcal{S}$ l'ensemble des p-sous-groupes de Sylow de G. Soit $S \in \mathcal{S}$. Si $g \in G$ (resp. $g \in S$) et si $S' \in \mathcal{S}$ alors $gS'g^{-1} \in S'$, de sorte que G (resp. S) agit sur $\mathcal{S}$ par conjugaison. Le stabilisateur d'un élément S' de $\mathcal{S}$ pour cette action est noté $\mathrm{Stab}_G(S')$ (resp. $\mathrm{Stab}_S(S')$). On démontre que S, vu comme élément de $\mathcal{S}$, est l'unique point fixe de l'action de S sur $\mathcal{S}$. Puisque S est un sous-groupe de G on a $gSg^{-1} = S$ pour tout $g \in S$, donc S est bien un point fixe de cette action. Réciproquement soit $S' \in \mathcal{S}$ tel que $gS'g^{-1} = S'$ pour tout $g \in S$; alors $S \subseteq \mathrm{Stab}_G(S')$, de sorte que S et S' sont deux p-sous-groupes de Sylow de $\mathrm{Stab}_G(S')$ (**vérifier cela en détail**); or $S' \lhd \mathrm{Stab}_G(S')$ par définition de l'action de G par conjugaison sur $\mathcal{S}$, tandis que les p-sous-groupes de Sylow de $\mathrm{Stab}_G(S')$ sont tous conjugués, donc S' est l'unique p-sous-groupe de Sylow de $\mathrm{Stab}_G(S')$; donc $S = S'$.
Ainsi, S est un p-groupe agissant sur $\mathcal{S}$, et l'action associée admet un unique point fixe. Le corollaire de l'équation aux classes pour les p-groupes implique donc que $|\mathcal{S}| = 1 \bmod p$. Comme $\mathcal{S}$ est une orbite pour l'action de G par conjugaison sur l'ensemble de ses sous-groupes, il suit donc de l'équation aux classes que $|\mathcal{S}|$ divise $|G| = p^\alpha m$. Donc $|\mathcal{S}|$ divise m, d'après le lemme de Gauss. □

3.c. Conséquences des théorèmes de Sylow

Corollaire.
Soit $(G, \times)$ un groupe fini. Soit p un entier premier divisant son ordre.

(1) Soit H un sous-groupe de G qui soit un p-groupe, alors il existe un p-sous-groupe de Sylow de G qui contienne H.

(2) Soit S un p-sous-groupe de Sylow de G. C'est l'unique p-sous-groupe de Sylow de G si et seulement si $S \lhd G$.

Démonstration. (1) Soit S un p-sous-groupe de Sylow de G. D'après la proposition qui précéde le deuxième théorème de Sylow il existe $g \in G$ tel que $gSg^{-1} \cap H$ soit un p-sous-groupe de Sylow de H. Puisque H est un p-groupe, il est son unique p-sous-groupe de Sylow. Donc $gSg^{-1} \cap H = H$. Ainsi, H est contenu dans gSg^{-1} qui est un p-sous-groupe de Sylow de H.

(2) suit de ce que les p-sous-groupes de Sylow de G sont tous conjugués (voir la démonstration du théorème précédent).

□

4. Exemples d'utilisation

Les théorèmes de Sylow permettent une meilleure connaissance d'un groupe donné parce qu'ils facilitent la description de certains sous-groupes de ce dernier.

4.a. Dénombrement des sous-groupes de Sylow

Exemple.
Dans un groupe abélien tout sous-groupe est distingué, donc il y a un et un seul p-sous-groupe de Sylow pour chaque entier premier p divisant l'ordre de ce groupe.

Exemple.
Soit $(G, \times)$ un groupe d'ordre 6. Soit n_3 le nombre de 3-sous-groupes de Sylow de G. Alors $n_3 = 1 \bmod 3$ et $n_3|6$. Donc $n_3 = 1$. Ainsi, G a un unique 3-sous-groupe de Sylow qui est donc distingué.

Exercice.
Soit $(G, \times)$ un groupe d'ordre 15. Démontrer qu'il y a dans G un unique 3-sous-groupe (resp. 5-sous-groupe) de Sylow.

Exemple.
Soit $(G, \times)$ un groupe d'ordre 60. Soit n_5 le nombre de 5-sous-groupes de Sylow de G. Alors $n_5 = 1 \bmod 5$ et $n_5|12$. Donc $n_5 \in \{1, 6\}$. En particulier, si G est de plus simple (*i.e.* G et $\{e\}$ sont les deux seuls sous-groupes distingués de G) alors un 5-sous-groupe de Sylow ne peut pas être distingué de sorte que $n_5 = 6$.

4.b. Construction de nouveau sous-groupes

On peut en trouver parmi les stabilisateurs des sous-groupes de Sylow pour l'action de conjugaison.

Exemple.
Soit n_3 le nombre de 3-sous-groupes de Sylow de $\mathscr{S}_5$. Un 3-sous-groupe de Sylow de $\mathscr{S}_5$ est cyclique d'ordre 3 et contient donc 2 éléments d'ordre 3 (**vérifier cela en détail**). Comme 3 est premier, deux 3-sous-groupes de Sylow distincts n'ont que l'élément neutre en commun (**vérifier cela en détail**). Donc un élément d'ordre 3 $\mathscr{S}_3$ appartient à un et un seul 3-sous-groupe de Sylow de $\mathscr{S}_5$ (**vérifier cela en détail**). Il y a donc deux fois moins de 3-sous-groupes de Sylow de $\mathscr{S}_5$ qu'il y a d'éléments d'ordre 3 dans $\mathscr{S}_5$. Les éléments d'ordre 3 de $\mathscr{S}_5$ sont les 3-cycles, il y en a 20 (**vérifier cela en détail**). Donc $n_3 = 10$.

Puisque les 3-sous-groupes de Sylow de $\mathscr{S}_5$ forment une orbite pour l'action de conjugaison de $\mathscr{S}_5$ sur l'ensemble de ses sous-groupes, l'équation aux classes implique que le stabilisateur d'un 3-sous-groupe de Sylow de $\mathscr{S}_5$ est d'ordre $\frac{|\mathscr{S}_5|}{n_3} = 6$.

Exercice.
Démontrer que le groupe $\mathscr{S}_5$ a autant de sous-groupes d'ordre 6 qu'il a de 3-sous-groupes de Sylow et que les sous-groupes d'ordre 6 forment une orbite pour l'action de conjugaison.

4.c. Non existence de sous-groupe d'un ordre donné

Exemple.
On suppose qu'il existe un sous-groupe H de $\mathscr{S}_5$ qui soit d'ordre 15. Alors H a un et un seul 3-sous-groupe de Sylow (**vérifier cela en détail**). On note ce dernier S. En particulier $S \lhd H$. Donc H est contenu dans le stabilisateur de H pour l'action de $\mathscr{S}_5$ par conjugaison sur l'ensemble de ses sous-groupes (**vérifier cela en détail**). Or ce stabilisateur est d'ordre 6 (voir l'exemple précédent). C'est absurde car H est d'ordre 15.

Il n'existe donc pas dans $\mathscr{S}_5$ de sous-groupe d'ordre 15.