Licence de mathématique
Université Paris-Saclay

Groupes et géométrie

N. Perrin

Université de Versailles Saint-Quentin-en-Yvelines
Année 2019-2020

Table des matières

Première partie .

Groupes

1. Morphismes de groupes, sous-groupes

Dans ce premier chapitre, nous faisons des rappels sur les groupes, leurs sous-groupes et les morphismes de groupes.

1.1. La notion de groupe

Définition 1.1.1 (i) Un **groupe** est la donnée d'une paire $(G, \star)$ où G est un ensemble et $\star : G \times G \to G$ est une **loi de composition** telle que les trois propriétés suivantes sont satisfaites :

(Unité) il existe un élément $e \in G$ tel que $e \star g = g \star e = g$ pour tout $g \in G$;

(Inverse) pour tout $g \in G$, il existe $h \in G$ tel que $g \star h = h \star g = e$;

(Associativité) pour tout $(g, h, k) \in G^3$, on a $(g \star h) \star k = g \star (h \star k)$.

(ii) Si de plus on a $g \star h = h \star g$ pour tout $(g, h) \in G^2$, on dire que le groupe G es **commutatif** ou encore **abelien**.

(iii) Le cardinal $|G|$ (fini ou infini) d'un groupe G est appelé **ordre du groupe**.

Remarque 1.1.2 Un groupe n'est jamais vide

Lemme 1.1.3 Soit G un groupe.

(i) L'élément unité e du groupe tel que $e \star g = g \star e = g$ pour tout $g \in G$ est unique.

(ii) Pour tout $g \in G$, l'élémnt $h \in G$ tel que $g \star h = h \star g = e$ est unique. □

Preuve. 1. Soient e et e' des éléments unités. Alors on a $e' = e \star e' = e$.

2. Soient h et h' deux éléments tel que $g \star h = h \star g = e$ et $g \star h' = h' \star g = e$. Alors on a $h' = h' \star e = h' \star (g \star h) = (h' \star g) \star h = e \star h = h$. ■

Définition 1.1.4 Soit G un groupe et $g \in G$. L'unique élémnt $h \in G$ tel que $g \star h = h \star g = e$ est appelé **inverse** de g dans G.

Notation 1.1.5 On utilisera essentiellement deux notations pour la loi de composition d'un groupe :

(i) la **notation multiplicative** dans laquelle le produit $g \star h$ est noté gh et l'unité e est notée 1. L'inverse de g est alors noté g^{-1}. C'est la notation que nous utiliserons par défaut. En particulier dans cette notation, on ne suppose pas le groupe commutatif, donc a priori, on a $gh \neq hg$.

(ii) la **notation additive** ne sera utilisée **que si le groupe G est commutatif**. Le produit $g \star h$ est noté $g + h$ et l'unité e est notée 0. L'inverse de g est alors noté $-g$. Dans cette notation, on a toujours $g + h = h + g$ donc le groupe est commutatif.

Lemme 1.1.6 Soit G un groupe.

(i) Pour $g \in G$, on a $(g^{-1})^{-1} = g$.

(ii) Pour $g, h \in G$, on a $(gh)^{-1} = h^{-1}g^{-1}$.

(iii) Si $(g_i)_{i\in[1,n]}$ sont des éléments de G, on a $(g_1 \cdots g_n)^{-1} = g_n^{-1} \cdots g_1^{-1}$. □

Preuve. 1. En effet, on a $gg^{-1} = g^{-1}g = 1$ donc $(g^{-1})^{-1} = g$.

2. On calcule $(gh)(h^{-1}g^{-1}) = g(hh^{-1})g^{-1}) = gg^{-1}) = 1$ et $(h^{-1}g^{-1})(gh) = h^{-1})hg^{-1}g)h = h^{-1})h = 1$.

3. Par récurrence en utilisant 1. ∎

Corollaire 1.1.7 L'application $f : G \to G$, $g \mapsto g^{-1}$ est bijective.

Preuve. Il suffit de montrer que f est son propre inverse. Mais pour tout $g \in G$, on a $(f \circ f)(g) = f(f(g)) = f(g^{-1}) = (g^{-1})^{-1} = g$. ∎

Exemple 1.1.8 (i) Les ensembles $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ munis de la loi $+$ sont des groupes commutatifs.

(ii) Les ensembles $\mathbb{Q}^*$, $\mathbb{R}^*$ et $\mathbb{C}^*$ munis de la loi $\times$ sont des groupes commutatifs.

(iii) L'ensemble $\mathrm{GL}_n(\mathbb{R})$ des matrices réelles inversibles de taille n est un groupe pour la multiplication des matrices. Il est non commutatif si et seulement si $n \geq 2$.

(iv) L'ensemble $\mathrm{GL}(V)$ des endomorphismes bijectifs d'un $\mathbb{R}-$espace vectoriel V est un groupe pour la composition. Il est non commutatif si et seulement si $\dim V \geq 2$.

(v) L'ensemble $\mathfrak{S}_n$ des permutations de l'ensemble $[1, n]$ est un groupe pour la composition. Son ordre est $n!$. Il est non commutatif si et seulement si $n \geq 3$.

(vi) L'ensemble des rotations planes de centre O forme un groupe pour la composition. Il est commutatif.

(vii) Soit E un ensemble. L'ensemble $\mathfrak{S}(E)$ des bijections de E dans E est un groupe pour la composition.

Notation 1.1.9 Soit G un groupe et $g \in G$.

(i) En notation multiplicative, on définit g^m pour $m \in \mathbb{Z}$ de la manière suivante :

$$g^m = \begin{cases} g \cdot g \cdots g & \text{produit de } m \text{ fois } g & \text{si } m \geq 1 \\ 1 & \text{produit vide} & \text{si } m = 0 \\ g^{-1} \cdot g^{-1} \cdots g^{-1} & \text{produit de } |m| = -m \text{ fois } g^{-1} & \text{si } m \leq -1. \end{cases}$$

(ii) En notation additive, on définit mg pour $m \in \mathbb{Z}$ de la manière suivante :

$$mg = \begin{cases} g + g + \cdots + g & \text{somme de } m \text{ fois } g & \text{si } m \geq 1 \\ 0 & \text{somme vide} & \text{si } m = 0 \\ (-g) + (-g) + \cdots (-g) & \text{somme de } |m| = -m \text{ fois } -g & \text{si } m \leq -1. \end{cases}$$

1.2. Morphisme de groupes

Définition 1.2.1 Soient G et G' deux groupes.

(i) Un **morphisme de groupes** de G dans G' est une application $\varphi : G \to G'$ telle que $\varphi(gh) = \varphi(g)\varphi(h)$ pour tout $(g, h) \in G^2$. L'ensemble des morphisme de groupes de G dans G' est note $\mathrm{Hom}(G, G')$.

(ii) Un morphisme de groupe $\varphi : G \to G'$ est appelé **isomorphisme de groupes** si φ est bijective. L'ensemble des morphisme de groupes de G dans G' est note $\mathrm{Isom}(G, G')$.

(iii) Lorsque G' est égal à G, un morphisme de groupe est appelé **endomorphisme de groupes**. L'ensemble des endomorphismes de groupes de G dans lui-même est note $\mathrm{End}(G)$.

(iv) Lorsque G' est égal à G, un isomorphisme de groupe est appelé **automorphisme de groupes**. L'ensemble des automorphismes de groupes de G dans lui-même est note $\mathrm{Aut}(G)$.

Remarque 1.2.2 On utilise parfois **homomorphisme de groupes** à la place de morphisme de groupes.

Lemme 1.2.3 Soit $\varphi : G \to G'$ un isomorphisme de groupes et soit $\varphi^{-1} : G' \to G$ l'inverse de φ. Alors φ^{-1} est un morphisme de groupes. □

Preuve. Soient $x, y \in G'$, on veut montrer que $\varphi^{-1}(xy) = \varphi^{-1}(x)\varphi^{-1}(y)$.

Posons $g = \varphi^{-1}(x)$ et $h = \varphi^{-1}(y)$. Comme φ est un morphisme de groupes, on a $\varphi(gh) = \varphi(g)\varphi(h) = xy$. En particulier $\varphi^{-1}(xy) = gh = \varphi^{-1}(x)\varphi^{-1}(y)$. ■

Proposition 1.2.4 Soit $\varphi : G \to G'$ un morphisme de groupes. Alors on a les égalités suivantes :

(i) $\varphi(1) = 1$;

(ii) $\varphi(g^{-1}) = \varphi(g)^{-1}$, pour tout $g \in G$;

(iii) $\varphi(g^m) = \varphi(g)^m$, pour tout $g \in G$ et tout $m \in \mathbb{Z}$.

Preuve. 1. On a $\varphi(1) = \varphi(1 \cdot 1) = \varphi(1)\varphi(1)$ et en multipliant (à gauche ou à droite) par $\varphi(1)^{-1}$, on a $\varphi(1) = 1$.

2. On a $\varphi(g^{-1})\varphi(g) = \varphi(g^{-1}g) = \varphi(1) = 1 = \varphi(gg^{-1}) = \varphi(g)\varphi(g^{-1})$. On a donc $\varphi(g^{-1}) = \varphi(g)^{-1}$.

3. Pour $m = 0$ c'est le 1. Pour $m \geq 1$, on procède par récurrence sur m. Pour $m \leq -1$, on procède par récurrence sur $|m| = -m$ en utilisant le 2. ∎

Exemple 1.2.5 (i) L'application $\log : (\mathbb{R}_+^*, \times) \to (\mathbb{R}, +)$ est un isomorphisme de groupes.

(ii) L'application $\exp : (\mathbb{R}, +) \to (\mathbb{R}_+^*, \times)$ est l'isomorphisme de groupe réciproque de log.

(iii) L'application $\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}$ est un morhisme de groupes surjectif (et non injectif si et seulement si $n \geq 2$.

(iv) L'application $\varphi : (\mathbb{R}, +) \to (\mathbb{C}^*, \times)$ définie par $\varphi(x) = e^{2i\pi x}$ est un morphisme de groupes non injectif et non surjectif.

(v) L'application $\varphi : (\mathbb{C}^*, \times) \to (\mathbb{C}^*, \times)$ déinie par $\varphi(z) = z^n$ est un morphisme surjectif mais non injectif de groupes.

Proposition 1.2.6 Soit $\varphi : G \to G'$ et $\psi : G' \to G''$ deux morphismes de groupes. Alors $\psi \circ \varphi : G \to G''$ est un morphisme de groupes.

Preuve. On a $(\psi \circ \varphi)(gh) = \psi(\varphi(gh)) = \psi(\varphi(g)\varphi(h)) = \psi(\varphi(g))\psi(\varphi(h)) = (\psi \circ \varphi)(g)(\psi \circ \varphi)(h)$ ∎

Corollaire 1.2.7 Soit G un groupe, alors $(\mathrm{Aut}(G), \circ)$ est un groupe (c'est un sous-groupe de $\mathfrak{S}(G), \circ)$).

Preuve. L'identité est un automorphisme de groupes. On vient de voir que la composée de deux automorphismes de groupes est encore un automorphisme de groupes. Enfin, on a vu que l'inverse d'un automorphisme de groupes est un automorphisme de groupes. ∎

1.3. Sous-groupes

Définition 1.3.1 Soit G un groupe. Un sous-ensemble $H \subset G$ est appelé **sous-groupe** de G s'il vérifie les trois conditions suivantes :

(i) $1 \in H$;

(ii) si $g \in H$, alors $g^{-1} \in H$;

(iii) si $g, h \in H$, alors $gh \in H$.

Remarque 1.3.2 (i) On vérifie aisément que si $H \subset G$ est un sous-groupe, alors H muni du produit de G est un groupe.

(ii) Si on oublie la condition (ii) ci-dessus, alors H n'est pas nécessairement un sous-groupe (par exemple $H = \mathbb{N} \subset G = \mathbb{Z}$).

Notation 1.3.3 Soit G un groupe.

(i) Les sous-ensembles $\{1\}$ et G forment toujours des sous-groupes de G. On les appele **sous-groupes triviaux** de G.

(ii) Un sous-groupe $H \subset G$ tel que $H \neq G$ est appelé **sous-groupe propre** de G.

Proposition 1.3.4 Soit G un groupe de $H \subset G$ un sous-ensemble de G. Alors H est un sous-groupe de H si et seulement si les deux conditions suivantes sont satisfaites :

(i) H est non vide ;

(ii) si $g, h \in H$, alors $gh^{-1} \in H$.

Preuve. Commençons par supposer que H est un sous-groupe. Alors $1 \in H$ et H est non vide. De plus, si $g, h \in H$, alors $h^{-1} \in H$ et donc $gh^{-1} \in H$.

Réciproquement, si H satisfait les deux conditions ci-dessus, montrons que c'est un sous-groupe. Montrons que $1 \in H$. Soit $g_0 \in H$ un élément quelconque (c'est possible car H est non vide). Alors on a $1 = g_0 g_0^{-1} \in H$ par (ii) appliqué à $(g, h) = (g_0, g_0)$. Soit $h \in H$, montrons que $h^{-1} \in H$. Comme $1 \in H$, on peut appliquer (ii) à $(g, h) = (1, h)$ et on a $h^{-1} = 1h^{-1} \in H$. Finalement, si $g, h \in H$, montrons que $gh \in H$. Par ce qui précède, on sait que $h^{-1} \in H$ donc en appliquant (ii) à $(g, h) = (g, h^{-1})$, on a $gh = g(h^{-1})^{-1} \in H$. ∎

Exemple 1.3.5 (i) Les sous-ensembles $\mathbb{Z}$, $\mathbb{Q}$ et $\mathbb{R}$ sont des sous-groupes de $(\mathbb{C}, +)$.

(ii) Les sous-ensembles $\mathbb{Q}^*$ et $\mathbb{R}^*$ sont des sous-groupes de $(\mathbb{C}^*, \times)$.

(iii) Le sous-ensemble $\{1, -1\}$ de $(\mathbb{Q}^*, \times)$ est un sous-groupe.

(iv) Le sous-ensemble $\mathrm{O}_n(\mathbb{R}) = \{A \in \mathrm{GL}_n(\mathbb{R}) \mid A^{-1} = A^t\}$ où A^t designe la transposé de A est un sous-groupe de $\mathrm{GL}_n(\mathbb{R})$.

(v) Le sous-ensemble $\mathrm{Aff}_+(\mathbb{R}^2)$ défini par

$$\mathrm{Aff}_+(\mathbb{R}^2) = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \;\middle|\; a^2 + b^2 \neq 0 \right\}$$

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

(vi) Le sous-ensemble $\mathrm{Isom}_+(\mathbb{R}^2)$ défini par

$$\mathrm{Isom}_+(\mathbb{R}^2) = \left\{ \begin{pmatrix} a & -b \\ b & a \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}) \;\middle|\; a^2 + b^2 = 1 \right\}$$

est un sous-groupe de $\mathrm{Aff}_+(\mathbb{R}^2)$ et de $\mathrm{GL}_2(\mathbb{R})$.

Lemme 1.3.6 Soit G un groupe.

(i) Si H et K sont des sous-groupes de G, alors $H \cap K$ est un sous-groupe de G.

(ii) Plus généralement, si $(H_\lambda)_{\lambda \in \Lambda}$ est une famille de sous-groupes de G, alors l'intersection $\cap_{\lambda \in \Lambda} H_\lambda$ est un sous-groupe de G. □

Preuve. La première assertion est une conséquence de la seconde. Nous montrons la seconde. Notons $K = \cap_{\lambda \in \Lambda} H_\lambda$. Il suffit de montrer que K est non-vide et que pour tout $g, h \in K$, on a $gh^{-1} \in K$. Comme H_λ est un sous-groupe, on a $1 \in H_\lambda$ pour tout λ et donc $1 \in K$ et K est non-vide. Soient maintenant g et h deux élément de K. Alors $g, h \in H_\lambda$ pour tout λ et donc $gh^{-1} \in H_\lambda$ pour tout λ et donc $gh^{-1} \in K$. ■

Corollaire 1.3.7 Soit $E \subset G$ un sous-ensemble quelconque, alors il existe un plus petit sous-groupe K de G contenant E.

Preuve. Il suffit de prendre pour K l'intersection de tous les sous-groupes de G contenant E. ■

Définition 1.3.8 Soit G un groupe et $E \subset G$ un sous-ensemble de G.

— Le plus petit sous-groupe de G contenant E est appelé **sous-groupe de G engendré par** E et est noté $\langle E \rangle$.

— Si $E = \{g\}$ n'a qu'un seul élément, on note $\langle g \rangle = \langle E \rangle = \langle \{g\} \rangle$.

Remarque 1.3.9 En général, si H et K sont des sous-groupes de G, la réunion $H \cup K$ n'est pas un sous-groupe de G. Ainsi par exemple, $\mathbb{R}$ et $i\mathbb{R}$ sont des sous-groupes de $(\mathbb{C}, +)$ mais $R \cup i\mathbb{R}$ n'est pas un sous-groupe de $\mathbb{C}$. On a

$$\langle \mathbb{R}, i\mathbb{R} \rangle = \mathbb{C}$$

c'est-à-dire que le sous-groupe engendré par $\mathbb{R}$ et $i\mathbb{R}$ est $\mathbb{C}$ tout entier.

Proposition 1.3.10 Soit G un groupe et $g \in G$. Alors on a $\langle g \rangle = \{g^m \in G \mid m \in \mathbb{Z}\}$.

Preuve. Notons $H = \{g^m \in G \mid m \in \mathbb{Z}\}$. Montrons l'inclusion $H \subset \langle g \rangle$. Soit donc $m \in \mathbb{Z}$, il suffit de montrer que $g^m \in \langle g \rangle$. Si $m = 0$, alors $g^m = 1 \in \langle g \rangle$ car $\langle g \rangle$ est un sous-groupe de G. Si $m \geq 1$, alors comme $g \in \langle g \rangle$ et que $\langle g \rangle$ est un groupe donc stable par multiplication, on obtient par récurrence sur m que $g^m \in \langle g \rangle$. Si $m \leq -1$, on commence par remarque que $g^{-1} \in \langle g \rangle$ et on procède comme précedemment.

Réciproquement, montrons que $\langle g \rangle \subset H$. Comme $\langle g \rangle$ est le plus petit sous-groupe contenant g et que $g \in H$, il suffit de montrer que H est un sous-groupe de G. Comme $g \in H$, on a bien que H est non vide. Si $h, h' \in H$, alors $h = g^m$ et $h' = g^{m'}$ avec $m, m' \in \mathbb{Z}$. On a alors $h(h')^{-1} = g^m g^{-m'} = g^{m-m'} \in H$ donc H est un sous-groupe.∎

1.4. Ordre d'un élément

Définition 1.4.1 Soit G un groupe et soit $g \in G$. Le cardinal de $\langle g \rangle$ est appelé **ordre de** g dans G et est noté $\mathrm{ord}_G(g)$ ou $\mathrm{ord}(g)$ s'il n'y a pas de confusion possible sur le groupe G.

Remarque 1.4.2 Soit G un groupe et soit $g \in G$.

(i) L'ordre de g peut être infini.

(ii) On a $\mathrm{ord}(g) = 1$ si et seulement si $g = 1$ (en effet, on a alors que $\langle g \rangle$ est un groupe a un seul élément donc $\langle g \rangle = \{1\}$ mais comme $g \in \langle g \rangle$, on a bien $g = 1$).

Proposition 1.4.3 Soit G un groupe et soit $g \in G$ d'ordre fini.

(i) On a $\mathrm{ord}(g) = \min\{n \in \mathbb{N}^* \mid g^n = 1\}$.

(ii) Si n est un entier tel que $g^n = 1$, alors $\mathrm{ord}(g)$ divise n.

(iii) On a un ismorphisme $\langle g \rangle \simeq \mathbb{Z}/\mathrm{ord}(g)\mathbb{Z}$ donné par $g^m \mapsto [m]$ et de réciproque $[m] \mapsto g^m$.

Preuve. 1. Comme $\mathrm{ord}(g)$ est fini, l'application $\mathbb{Z} \to \langle g \rangle$, $m \mapsto g^m$ ne peut être injective. Il existe donc des entiers m et n distincts tels que $g^m = g^n$. On peut supposer par exemple que $m < n$. On a alors $g^{n-m} = 1$. L'ensemble $\{n \in \mathbb{N}^* \mid g^n = 1\}$ est donc non vide. Notons $n_0 = \min\{n \in \mathbb{N}^* \mid g^n = 1\}$ et montrons que $\langle g \rangle = \{g^r \mid r \in [0, n_0 - 1]\}$. On aura alors $\mathrm{ord}(g) = |\langle g \rangle| = n_0$.

On a l'inclusion $\{g^r \mid r \in [0, n_0 - 1]\} \subset \langle g \rangle = \{g^m \mid m \in \mathbb{Z}\}$ donc il suffit de montrer l'autre inclusion. Soit $m \in \mathbb{Z}$. On fait la division euclidienne de m par n_0 et on a $m = qn_0 + r$ avec $r \in [0, n_0 - 1]$. On a alors $g^m = g^{qn_0+r} = (g^{n_0})^q g^r = 1^q g^r = g^r \in H$ ce qui montre le résultat.

2. Soit n tel que $g^n = 1$. Montrons que $n_0 = \mathrm{ord}(g)$ divise n. On fait la division euclidienne de n par n_0 et on a $n = qn_0 + r$ avec $r \in [0, n_0 - 1]$. Par ailleurs, on a $1 = g^n = g^{qn_0+r} = (g_0^n)^q g^r = 1^q g^r = g^r$. Donc $g^r = 1$ avec $r \in [0, n_0 - 1]$. Par minimalité de n_0, on obtient $r = 0$ et $\mathrm{ord}(g) = n_0$ divise n.

3. On commence par vérifier que les deux applications sont bien définies. Commençons par $\varphi : \langle g\rangle \to \mathbb{Z}/\mathrm{ord}(g)\mathbb{Z}$ avec $\varphi(g^m) = [m]$. Il faut vérifier que si m et n sont tels que $g^m = g^n$, alors $[m] = \varphi(g^m) = \varphi(g^n) = [n]$. Mais on a $g^{m-n} = 1$ et $\mathrm{ord}(g)$ divise $m - n$ donc $[m] = [n]$.

Vérifions que $\psi : \mathbb{Z}/\mathrm{ord}(g)\mathbb{Z} \to \langle g\rangle$ avec $\psi([m]) = g^m$ est bien définie. Il faut vérifier que si $[m] = [n]$, alors $g^m = g^n$. Mais si $[m] = [n]$, alors $\mathrm{ord}(g)$ divise $m - n$ donc $m - n = d\mathrm{ord}(g)$ pour un $d \in \mathbb{Z}$. On a alors $g^{m-n} = g^{d\mathrm{ord}(g)} = (g^{\mathrm{ord}(g)})^d = 1^d = 1$. Donc $g^m = g^n$.

Les deux applications φ et ψ sont donc bien définies et inverses l'une de l'autre. Il reste à montrer que φ (ou ψ) est un morphisme de groupes. On a $\varphi(g^m \cdot g^n) = \varphi(g^{m+n}) = [m + n] = [m] + [n] = \varphi(g^m) + \varphi(g^n)$. ∎

Exemple 1.4.4 Un groupe infini peut avoir des éléments d'ordre fini. Ainsi par exemple $-1 \in \mathbb{R}^*$ est d'ordre 2.

Proposition 1.4.5 Si G est un groupe et $g \in G$ est d'ordre infini, alors $\langle g\rangle$ est isomorphe à $\mathbb{Z}$ via $g^m \leftrightarrow m$.

En particulier, il n'existe pas d'entier n non nul tel que $g^n = 1$.

Preuve. Commençons par montrer qu'il n'existe pas d'entier non nul n tel que $g^n = 1$. En remplaçant g par g^{-1}, on peut supposer $n > 0$. Montrons que si un tel n existe alors, pour tout $m \in \mathbb{Z}$, on a $g^m = g^r$ avec $r \in [0, n-1]$. Ceci étant impossible (car alors $\langle g\rangle$ est fini de cardinal au plus n), on aura terminé. On fait la division euclidienne de m par n. On a $m = qn + r$ avec $r \in [0, n-1]$. On a donc $g^m = g^{qn+r} = (g^n)^q g^r = 1^q g^r = g^r$ ce qu'on voulait démontrer.

Considérons maintenant l'application $\psi : \mathbb{Z} \to \langle g\rangle$ définie par $\psi(m) = g^m$. C'est une application surjective. Montrons qu'elle est injective. Si $\psi(m) = \psi(n)$ avec $m \neq n$, alors $g^m = g^n$ et donc $g^{m-n} = 1$ ce qui est impossible par ce qu'on vient de montrer.

Il reste à vérifier que ψ est un morphisme de groupes. On a $\psi(m + n) = g^{m+n} = g^m g^n = \psi(m)\psi(n)$. ∎

1.5. Noyau et image

Proposition 1.5.1 Soit $\varphi : G \to G'$ un morphisme de groupes et soient $H \subset G$ et $H' \subset G'$ des sous-groupes. On a

(i) l'image $\varphi(H)$ de H est un sous-groupe de G' ;

(ii) l'image réciproque $\varphi^{-1}(H')$ de H' est un sous-groupe de G.

Preuve. 1. On a $1 \in H$ donc $1 = \varphi(1) \in \varphi(H)$. De plus, si $g, h \in H$, alors on a $gh^{-1} \in H$. On a donc $\varphi(g)\varphi(h)^{-1} = \varphi(gh^{-1}) \in \varphi(H)$.

2. On a $\varphi(1) = 1 \in H'$ donc $1 \in \varphi^{-1}(H')$. De plus, si $g, h \in \varphi^{-1}(H')$, alors $\varphi(g), \varphi(h) \in H'$ donc $\varphi(g)\varphi(h)^{-1} \in H'$. On a donc $\varphi(gh^{-1}) = \varphi(g)\varphi(h)^{-1} \in H'$ et $gh^{-1} \in \varphi^{-1}(H')$. ∎

Définition 1.5.2 Soit $\varphi : G \to G'$ un morphisme de groupe, les sous-groupes $\varphi(G) \subset G'$ et $\varphi^{-1}(1) \subset G$ son appelés **image** et **noyau**. On les note $\mathrm{Im}(\varphi)$ et $\mathrm{Ker}(\varphi)$.

Exemple 1.5.3 (i) On a $\mathrm{SL}_n(\mathbb{R}) = \mathrm{Ker}(\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*)$. Ainsi $\mathrm{SL}_n(\mathbb{R})$ est un sous-grope de $\mathrm{GL}_n(\mathbb{R})$. L'image de det est $\mathbb{R}^*$ (det est surjectif).

(ii) L'application $|\cdot| : \mathbb{C}^* \to \mathbb{R}^*$, $z \mapsto |z|$ est un morphisme de groupe. Son noyau $\mathrm{Ker}(|\cdot|) = \mathrm{S}^1 = \mathbb{U} = \{z \in \mathbb{C} \mid |z| = 1\}$ est un sous-groupe de $\mathbb{C}^*$. Son image $\mathrm{Im}(|\cdot|) = \mathbb{R}_+^*$ est un sous-groupe de $\mathbb{R}^*$.

(iii) Si n est un entier plus grand que 1, l'application $p_n : \mathbb{C}^* \to \mathbb{C}^*$, $z \mapsto z^n$ est un morphisme de groupes. Son noyau $\mathrm{Ker}(p_n) = \mu_n = \{z \in \mathbb{C}^* \mid z^n = 1\}$ est le sous-groupe des **racines n-ièmes de l'unité** de $\mathbb{C}^*$. Son image est $\mathrm{Im}(p_n) = \mathbb{C}^*$.

(iv) La signature $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ est un morphisme de groupe surjectif. Son noyau est le **sous-groupe alterné** $\mathrm{Ker}(\varepsilon) = \mathfrak{A}_n$.

Proposition 1.5.4 Soit $\varphi : G \to G'$ un morphisme de groupes. Alors φ est injectif si et seulement si $\mathrm{Ker}(\varphi) = \{1\}$.

Preuve. Si φ est injectif et si $g \in \mathrm{Ker}(\varphi)$, alors $\varphi(g) = 1 = \varphi(1)$ donc $g = 1$. Réciproquement, supposons que l'on ait l'égalité $\mathrm{Ker}(\varphi) = \{1\}$. Soient $g, h \in G$ tels que $\varphi(g) = \varphi(h)$. Alors $1 = \varphi(g)\varphi(h)^{-1} = \varphi(gh^{-1})$ donc $gh^{-1} \in \mathrm{Ker}(\varphi)$ et $gh^{-1} = 1$. On obtient $g = h$. ∎

1.6. produit

Proposition 1.6.1 Soit $(G_i)_{i\in[1,n]}$ une famille de groupes. Alors le produit $G_1 \times \cdots \times G_n$ muni de la loi $(g_1, \cdots, g_n)(h_1, \cdots, h_n) = (g_1h_1, \cdots, g_nh_n)$ est un groupe.

Preuve. On a $(1, \cdots, 1)(g_1, \cdots, g_n) = (g_1, \cdots, g_n)(1, \cdots, 1) = (g_1, \cdots, g_n)$ donc $(1, \cdots, 1)$ est l'unité.

On a $(g_1, \cdots, g_n)((g_1^{-1}, \cdots, g_n^{-1}) = (g_1^{-1}, \cdots, g_n^{-1})(g_1, \cdots, g_n) = (1, \cdots, 1)$ donc $(g_1^{-1}, \cdots, g_n^{-1})$ est l'inverse de $(g_1, \cdots, g_n)$

Enfin, on a les égalités

$$\begin{aligned}[(g_1,\cdots,g_n)(h_1,\cdots,h_n)](k_1,\cdots,k_n) &= (g_1h_1,\cdots,g_nh_n)(k_1,\cdots,k_n)\\ &= (g_1h_1k_1,\cdots,g_nh_nk_n)\\ &= (g_1,\cdots,g_n)(h_1k_1,\cdots,h_nk_n)\\ &= (g_1,\cdots,g_n)[(h_1,\cdots,h_n)(k_1,\cdots,k_n)],\end{aligned}$$

la loi est donc associative. ∎

Définition 1.6.2 Soit $(G_i)_{i\in[1,n]}$ une famille de groupes. La loi de groupe définie sur le produit $G_1\times\cdots\times G_n$ par $(g_1,\cdots,g_n)(h_1,\cdots,h_n)=(g_1h_1,\cdots,g_nh_n)$ est appelée **loi de groupe produit** et la structure de groupe ainsi définie s'appelle **groupe produit**.

Proposition 1.6.3 Soit $(G_i)_{i\in[1,n]}$ une famille de groupes, on muni le produit $G_1\times\cdots\times G_n$ de la loi de groupe produit. Alors la projection $p_i : G_1\times\cdots\times G_n\to G_i$, $(g_1,\cdots,g_n)\mapsto g_i$ est un morphisme de groupes.

Preuve. On a

$$\begin{aligned}p_i((g_1,\cdots,g_n)(h_1,\cdots,h_n)) &= p_i(g_1h_1,\cdots,g_nh_n)\\ &= g_ih_i\\ &= p_i(g_1,\cdots,g_n)p_i(h_1,\cdots,h_n),\end{aligned}$$

ce qui montre le résultat. ∎

Proposition 1.6.4 (Propriété universelle du produit) Soit $(G_i)_{i\in[1,n]}$ une famille de groupes, on muni le produit $G_1\times\cdots\times G_n$ de la loi de groupe produit.

Si G est un groupe tel qu'il existe des morphismes de groupes $f_i : G\to G_i$ pour tout $i\in[1,n]$, alors il existe un unique morphisme de groupe $fG\to G_1\times\cdots G_n$ tel que $f_i=p_i\circ f$ pour tout $i\in[1,n]$.

Preuve. Si f existe, alors la condition $f_i=p_i\circ f$ pour tout $i\in[1,n]$ impose que l'on a $f(g)=(f_1(g),\cdots,f_n(g))$ donc f est unique. Montrons que c'est un morphisme de groupes. On a

$$\begin{aligned}f(gh) &= (f_1(gh),\cdots,f_n(gh))\\ &= (f_1(g)f_1(h),\cdots,f_n(g)f_n(h))\\ &= (f_1(g),\cdots,f_n(g))(f_1(h),\cdots,f_n(h))\\ &= f(g)f(h),\end{aligned}$$

ce qui termine la preuve. ∎

1.7. Conjugaison et centre

Définition 1.7.1 Soit G un groupe.

(i) Soit $g \in G$. On définit l'application $\mathrm{Int}_g : G \to G$ par $\mathrm{Int}_g(h) = ghg^{-1}$. Cette application est appelée **conjugaison par l'élément** g

(ii) On définit le **centre** de G par

$$Z(G) = \{g \in G \mid hg = gh \text{ pour tout } h \in G\}.$$

Proposition 1.7.2 Soit G un groupe.

(i) L'application $\mathrm{Int}_g : G \to G$ est un automorphisme du groupe G.

(ii) L'application $\mathrm{Int} : G \to \mathrm{Aut}(G)$, $g \mapsto \mathrm{Int}_g$ est un morphisme de groupe.

(iii) Le noyau de Int est $Z(G)$.

Preuve. 1. et 2. On a $\mathrm{Int}_g(hk) = ghkg^{-1} = ghg^{-1}gkg^{-1} = \mathrm{Int}_g(h)\mathrm{Int}_g(k)$ donc Int_g est un morphisme de groupes. Montrons que $\mathrm{Int}_g \circ \mathrm{Int}_h = \mathrm{Int}_{gh}$ c'est-à-dire que Int est un morphisme de groupes. On a

$$\mathrm{Int}_g \circ \mathrm{Int}_h(k) = \mathrm{Int}_g(hkh^{-1}) = ghkh^{-1}g^{-1} = (gh)k(gh)^{-1} = \mathrm{Int}_{gh}(k).$$

En particulier, on a $\mathrm{Int}_g \circ \mathrm{Int}_{g^{-1}} = \mathrm{Int}_{g^{-1}} \circ \mathrm{Int}_g = \mathrm{Int}_1 = \mathrm{Id}_G$ donc Int_g est bijective.

3. Le noyau de Int est l'ensemble des éléments g tels que $\mathrm{Int}_g = \mathrm{Id}_G$ c'est-à-dire l'ensemble des éléments $g \in G$ tels que $ghg^{-1} = h$ pour tout $h \in G$ soit $gh = hg$ pour tout $h \in H$. C'est bien le centre de G. ∎

1.8. Les groupes $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$, les groupes monogènes et cycliques

On considèrera que les groupes $(\mathbb{Z}, +)$ et $(\mathbb{Z}/n\mathbb{Z}, +)$ sont connus.

Proposition 1.8.1 Les sous-groupes de $\mathbb{Z}$ sont les sous-ensembles $d\mathbb{Z}$ pour $d \in \mathbb{Z}$.

Preuve. On vérifie aisément que $d\mathbb{Z}$ est bien un sous-groupe de $\mathbb{Z}$. Réciproquement, soit H un sous-groupe de $\mathbb{Z}$. Si $H = \{0\}$, alors $H = 0\mathbb{Z}$. Sinon, il existe un élément $n \in H$ non nul. Si $n < 0$, l'élément $-n$ est encore dans H donc on peut supposer que H contient au moins un élément strictement positif. Soit alors $d = \min\{m \in H \mid m > 0\}$. On montre que $H = d\mathbb{Z}$. Comme $d \in H$ et que H est un groupe, on a $d\mathbb{Z} \subset H$. Soit maintenant $m \in H$. On fait la division euclidienne de m par d. On a $m = dq + r$ avec $r \in [0, d-1]$. Mais $d, m \in H$ donc $r = m - qd \in H$. Par minimalité de d, on doit avoir $r = 0$ donc d divise m et $m \in d\mathbb{Z}$. ∎

La preuve à peu près évidente de la proposition suivante est laissée au lecteur.

Proposition 1.8.2 Le groupe $\mathbb{Z}$ est engendré par l'élément $1 : \mathbb{Z} = \langle 1 \rangle$. Le groupe $d\mathbb{Z}$ est engendré par l'élément $d : d\mathbb{Z} = \langle d \rangle$.

Corollaire 1.8.3 Les groupes $\mathbb{Z}$ et $d\mathbb{Z}$ sont monogènes non cycliques.

Lemme 1.8.4 L'application $\pi_n : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$, $m \mapsto [m]$, où $[m]$ désigne la classe de m modulo n, est un morphisme de groupes surjectif. □

Preuve. Le fait que π_n est surjectif provient du fait tous les éléments de $\mathbb{Z}/n\mathbb{Z}$ représentent les classes modulo n des éléments de $\mathbb{Z}$. Le fait que π_n est un morphisme de groupe provient de la définition de l'addition dans $\mathbb{Z}/n\mathbb{Z}$: $\pi_n(x+y) = [x+y] = [x] + [y] = \pi_n(x) + \pi_n(y)$. ■

Notons $d\mathbb{Z}/n\mathbb{Z}$ le sous ensemble de $\mathbb{Z}/n\mathbb{Z}$ obtenu comme image par π_n de $d\mathbb{Z}$:

$$d\mathbb{Z}/n\mathbb{Z} = \pi_n(d\mathbb{Z}) = \left\{ [m] \in \mathbb{Z}/n\mathbb{Z} \;\middle|\; m \in d\mathbb{Z} \right\} = \left\{ [m] \in \mathbb{Z}/n\mathbb{Z} \;\middle|\; d \text{ divise } m \right\}.$$

Proposition 1.8.5 Soit n un entier non nul.

(i) Les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont les $d\mathbb{Z}/n\mathbb{Z}$ pour d un diviseur de n.

(ii) Si d divise n, le sous-groupe $d\mathbb{Z}/n\mathbb{Z}$ est d'ordre $\frac{n}{d}$ et est engendré par $[d]$.

Preuve. 1. Comme $d\mathbb{Z}$ est un sous-groupe de $\mathbb{Z}$, son image est un sous-groupe de $\mathbb{Z}/n\mathbb{Z}$. Soit maintenant $H \subset \mathbb{Z}/n\mathbb{Z}$ un sous-groupe. Alors $\pi_n^{-1}(H)$ est un sous-groupe de $\mathbb{Z}$ donc $\pi_n^{-1}(H) = d\mathbb{Z}$ pour un certain entier d. De plus, $n\mathbb{Z} = \pi_n^{-1}(\{0\}) \subset \pi_n^{-1}(H) = d\mathbb{Z}$ donc $n \in d\mathbb{Z}$ donc d divise n. Comme pi_n est surjectif, on obtient que $H = \pi_n(\pi_n^{-1}(H)) = \pi_n(d\mathbb{Z}) = d\mathbb{Z}/n\mathbb{Z}$ avec d un diviseur de n.

2. Soit $H = \pi_n(d\mathbb{Z}) = d\mathbb{Z}/n\mathbb{Z}$ avec d un diviseur de n. Comme $d\mathbb{Z}$ est engendré par d, son image $\pi_n(d\mathbb{Z})$ est engendré par $\pi_n(d) = [d]$ donc H est engendré par $[d]$. Écrivons $n = kd$. On a

$$\langle [d] \rangle = \{ m[d] \mid m \in \mathbb{Z} \} = \{ [0], [d], [2d], \cdots, [(k-1)d] \}$$

donc $d\mathbb{Z}/n\mathbb{Z}$ est d'ordre $k = \frac{n}{d}$. ■

Une autre formulation de la proposition précédente est la suivante.

Corollaire 1.8.6 Pour chaque diviseur d de n, il existe un unique sous-groupe d'ordre d de $\mathbb{Z}/n\mathbb{Z}$: le sous-groupe $\langle \left[\frac{n}{d}\right] \rangle$ engendré par $\left[\frac{n}{d}\right]$

Proposition 1.8.7 Soit $[m] \in \mathbb{Z}/n\mathbb{Z}$.

(i) Alors $\mathrm{ord}(m) = \frac{n}{\mathrm{pgcd}(m,n)}$.

(ii) En particulier, on a les équivalences

$$\begin{aligned} m \text{ est premier avec } n &\Leftrightarrow [m] \text{ est un générateur de } \mathbb{Z}/n\mathbb{Z} \\ &\Leftrightarrow \langle [m] \rangle = \mathbb{Z}/n\mathbb{Z}. \end{aligned}$$

Preuve. 1. Posons $d = \text{pgcd}(m, n)$. Il existe des entiers a et b tels que $m = ad$ et $n = bd$ avec $\text{pgcd}(a, b) = 1$.

Rappelons que $\text{ord}(m) = \min\{k \in \mathbb{N}^* \mid k[m] = [0]\}$. On a donc $\text{ord}(m) = \min\{k \in \mathbb{N}^* \mid km \text{ est divisible par } n\}$. Montrons que ce minimum doit être $\frac{n}{\text{pgcd}(m,n)} = \frac{n}{d} = b$.

Soit k tel que $k[m] = [0]$. Alors il existe un entier r tel que $km = rn$. On obtient $kad = rbd$ et donc $ka = rb$. On obtient que b divise ka et comme a et b sont premiers entre eux, on a que b divise k.

Réciproquement, montrons que $b[m] = [0]$. On a $b[m] = \left[\frac{mn}{d}\right]$ et comme $m/d = a \in \mathbb{Z}$, on obtient $b[m] = \left[\frac{mn}{d}\right] = [an] = [0]$. Ainsi $b = \min\{k \in \mathbb{N}^* \mid k[m] = [0]\} = \text{ord}([m])$.

2. Découle directement de 1. ∎

Exemple 1.8.8 Dans $\mathbb{Z}/6\mathbb{Z}$ les ordres des éléments sont les suivants

x	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$	$[5]$
$\text{ord}(x)$	1	6	3	2	3	6

Définition 1.8.9 Soit G un groupe.

(i) Le groupe G est dit **monogène** s'il existe un élément $g \in G$ tel que $G = \langle g \rangle$.

(ii) Le groupe G est dit **cyclique** s'il est monogène et fini.

Proposition 1.8.10 Soit G un groupe monogène.

(i) Si G est infini, alors $G \simeq \mathbb{Z}$.

(ii) Si G est cyclique d'ordre n, alors $G \simeq \mathbb{Z}/n\mathbb{Z}$.

Preuve. Soit g un générateur du groupe c'est-à-dire un élément $g \in G$ tel que $G = \langle g \rangle$. Considérons l'application $\varphi : \mathbb{Z} \to G$, $m \mapsto g^m$.

1. Si $G = \langle g \rangle$ est infini, alors on a vu que φ est un ismorphisme.

2. Si $G = \langle g \rangle$ est fini d'ordre n, alors on a vu que $G = \langle g \rangle \simeq \mathbb{Z}/\text{ord}(g)\mathbb{Z} = \mathbb{Z}/n\mathbb{Z}$. ∎

2. Quotient par un sous-groupe, groupe quotient

2.1. Relations d'équivalence

Nous rappelons la notion de relation d'équivalence et la partition qui est découle.

Définition 2.1.1 Soit E un ensemble.

(i) Une **relation** est une sous-partie R du produit $E \times E$ c'est-à-dire : $R \subset E \times E$.

(ii) Si $(x, y) \in R$, on dit que x **est en relation avec** y, on le note xRy.

(iii) Une relation est dite **réflexive** si tout Íément est en relation avec lui-même, c'est-à-dire si xRx est vrai pour tout $x \in E$.

(iv) Une relation est dite **symétrique** si on a l'implication $(xRy \Rightarrow yRx)$ pour toute paire $(x, y) \in E^2$.

(v) Une relation est dite **antisymétrique** si on a (xRy et $yRx \Rightarrow x = y$) pour toute paire $(x, y) \in E^2$.

(vi) Une relation est dite **transitive** si on a l'implication (xRy et $yRz \Rightarrow xRz$) pour tout triplet $(x, y, z) \in E^3$.

(vii) Une relation est appelée **relation d'équivalence** si elle est reflexive, symétrique et transitive.

(viii) Une relation est appelée **relation d'ordre** si elle est reflexive, antisymétrique et transitive.

Exemple 2.1.2 Soit E un ensemble.

(i) La relation d'égalité est une relation d'équivalence.

(ii) Si $E = \mathbb{Z}$ et $n \in \mathbb{Z}$ est un entier, la relation de congruence modulo n : ($\equiv \pmod{n}$ est une relation d'équivalence.

(iii) Si $E = \mathbb{Z}$, alors la relation $\leq$ est une relation d'ordre sur E. De même, la relation $\geq$ est une relation d'ordre sur E.

Définition 2.1.3 Soit E un ensemble, soit $x \in E$ et soit R une relation d'équivalence sur E. La **classe d'équivalence de** x **pour la relation** R, notée $[x]_R$ ou $[x]$ lorsque la relation R est claire est définie par

$$[x]_R = \{y \in E \mid xRy\}.$$

L'ensemble des classes d'équivalence pour la relation R est noté E/R.

Lemme 2.1.4 Soit E un ensemble, soit R une relation d'équivalence sur E et soient $x, y \in E$. Alors les classes déquivalence $[x]$ et $[y]$ de x et y pour la relation R sont soit égales : $[x] = [y]$, soit disjointes : $[x] \cap [y] = \emptyset$. □

Preuve. Soient x et y des élements de E. Nous devons montrer que l'alternative suivante est vraie : soit on a $[x] = [y]$, soit on a $[x] \cap [y] = \emptyset$. Supposons que $[x] \cap [y] \neq \emptyset$. Alors il existe $z \in [x] \cap [y]$. On a donc xRz et yRz. Par symétrie, on a xRz et zRy et par transitivité on obtient xRy (et yRx par symétrie).

Soit maintenant $t \in [x]$. Alors on a xRt et yRx. On a donc (transitivité) yRt et $t \in [y]$. On a donc $[x] \subset [y]$. On procède pour obtenir $[y] \subset [x]$ et donc $[x] = [y]$. ■

Définition 2.1.5 Soit E un ensemble et $(E_i)_{i \in I}$ une famille de sous-ensembles de E. On dit que cette famille forme une **partition** de E si les propriétés suivantes sont satisfaites :

(i) on a $E_i \cap E_j = \emptyset$ pour $i \neq j$;

(ii) on a $E = \cup_{i \in I} E_i$.

Proposition 2.1.6 Soit E un ensemble et R une relation d'équivalence sur E. Alors les classes déquivalence pour la relation R forment une partition de E.

Preuve. Le lemme précédent montre que la première condition pour avoir une partition est satisfaite. Montrons maintenant que les classes d'équivalence recouvrent E.

Soit E/R l'ensemble des classes d'équivalence. On a clairement l'inclusion $\cup_{[x] \in E/R}[x] \subset E$. Réciproquement, soit $x \in E$, alors par réflexivité, on a xRx et donc $x \in [x]$ d'où l'inclusion $E \subset \cup_{[x] \in E/R}[x]$. ■

Exemple 2.1.7 Si $E = \mathbb{Z}$ et R est la relation de congruence modulo un entier n. Alors les classes d'équivalence pour la relation R sont les ensembles

$$[m] = \{m + kn \in \mathbb{Z} \mid k \in \mathbb{Z}\}.$$

L'ensemble des classes d'équivalences est $\mathbb{Z}/n\mathbb{Z}$.

Définition 2.1.8 Soit E un ensemble et R une relation d'équivalence sur E. L'application $\pi_R : E \to E/R$ définie par $\pi_R(x) = [x]_R$ est appelée **projection canonique**.

Exemple 2.1.9 Si $E = \mathbb{Z}$ et R est la relation de congruence modulo un entier n. Alors la projection canonique est l'application $\mathbb{Z} \to Z/n\mathbb{Z}$, $m \mapsto [m]$.

2.2. Classes à droite et à gauche

Définition 2.2.1 Soit G un groupe et H un sous-groupe. On définit la relation de congruence (à droite) modulo H par $x \sim y \Leftrightarrow y^{-1}x \in H$.

Lemme 2.2.2 Soit G un groupe et H un sous-groupe.

(i) La relation de congruence (à droite) modulo H est une relation d'équivalence.

(ii) La classe d'équivalence de g est $gH = \{gh \in G \mid h \in H\}$.

(iii) On a $x \sim y \Leftrightarrow x \in yH$. □

Preuve. 1. On a $x^{-1}x = e \in H$ donc $x \sim x$ et la relation est reflexive. Si $x \sim y$ alors $y^{-1}x \in H$ et donc son inverse est dans H aussi : $x^{-1}y = (y^{-1}x)^{-1} \in H$ donc $y \sim x$, la relation est symétrique. Enfin, si $x \sim y$ et $y \sim z$, alors $y^{-1}x \in H$ et $z^{-1}y \in H$ donc le produit est dans H : $z^{-1}x = z^{-1}yy^{-1}x \in H$ donc $x \sim z$, la relation est transitive.

2. Soit $[g]$ la classe d'équivalence de g. Soit $g' \in [g]$, alors $(g')^{-1}g \in H$ donc il existe $h \in H$ tel que $(g')^{-1}g = h$ et $g'h = g$ donc $g' = gh^{-1} \in gH$. Réciproquement, si $g' \in gH$, alors il existe $h \in H$ tel que $g' = gh$ et donc $(g')^{-1}g = h^{-1} \in H$ donc $g \sim g'$ et $g' \in [g]$. ■

Définition 2.2.3 Soit G un groupe et H un sous-groupe.

(i) Les classes d'équivalence pour la relation de congruence (à droite) modulo H sont appelées **classes à gauche suivant** H.

(ii) L'ensemble des classes à gauche est noté G/H.

(iii) La projection canonique est notée π_H ou $\pi : G \to G/H$.

Remarque 2.2.4 Soit G un groupe et H un sous-groupe. On peut définir la relation de congruence (à gauche) modulo H par $g \approx h \Leftrightarrow gh^{-1} \in H$. On a alors :

(i) La relation $\approx$ est une relation d'équivalence.

(ii) Les classes d'équivalence de la relation $\approx$ sont appelées les classes à droite et sont de la forme $Hg = \{hg \in G \mid h \in H\}$.

(iii) L'ensemble des classes d'équivalence est noté $H\backslash G$.

(iv) La projection canonique est $\pi : G \to G\backslash H$.

Lemme 2.2.5 Soit G un groupe et H un sous-groupe.

(i) Alors toutes les classes d'équivalence $gH \in G/H$ sont en bijection avec H.

(ii) En particulier, si H est fini, on a $|gH| = |H|$. □

Preuve. 2. Découle de 1. Pour 1., on a la bijection $H \to gH$, $h \mapsto gh$ de bijection réciproque $x \mapsto g^{-1}x$. ■

Corollaire 2.2.6 (Théorème de Lagrange) Soit G un groupe fini et H un sous-groupe.

(i) On a l'égalité $[G] = |H| \cdot |G/H|$.

(ii) En particulier, l'ordre de H divise celui de G.

Preuve. 2. Découle de 1. Pour 1., on rappelle que l'on a une partition

$$G = \coprod_{gH \in G/H} gH.$$

Mais pour tout g, on a $|gH| = |H|$ donc on obtient

$$|G| = \sum_{gH \in G/H} |gH| = \sum_{gH \in G/H} |H| = |H| \sum_{gH \in G/H} 1 = |H| \cdot |G/H|$$

ce qui démontre le résultat. ∎

Définition 2.2.7 Soit G un groupe et $H \subset G$ un sous-groupe. On définit **l'indice de H dans G** noté $[G : H]$ par

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

Corollaire 2.2.8 Si G est un groupe fini et $H \subset G$ est un sous-groupe alors son indice est donné par la formule :

$$[G : H] = \frac{|G|}{|H|}.$$

Corollaire 2.2.9 Soit G un groupe fini et $g \in G$. Alors $\mathrm{ord}(g)$ divise $|G|$.

Preuve. Soit $H = \langle g \rangle$. C'est un sous-groupe d'ordre $\mathrm{ord}(g)$. Son ordre divise $|G|$. ∎

Corollaire 2.2.10 Soit G un groupe fini d'ordre n et soit $g \in G$. Alors, on a $g^n = 1$.

Preuve. On sait que $\mathrm{ord}(g)$ divise n, donc il existe $m \in \mathbb{Z}$ tel que $n = m\mathrm{ord}(g)$. On obtient $g^n = g^{m\mathrm{ord}(g)} = (g^{\mathrm{ord}(g)})^m = 1^m = 1$. ∎

Exemple 2.2.11 Soit $G = \mathfrak{S}_3$ le groupe des permutations sur 3 éléments. On note (abc) la permutation $\tau : \{1, 2, 3\} \to \{1, 2, 3\}$ telle que $\tau(1) = a$, $\tau(2) = b$ et $\tau(3) = c$. Par exemple $1 = \mathrm{Id} = (123)$. Le groupe G est donc formé des éléments suivants :

$$G = \{(123), (132), (213), (231), (312), (321)\}.$$

Soit $\sigma = (213) \in G$. On a $\sigma^2 = (123) = 1$ donc σ est d'ordre 2. Soit maintenant $H = \langle (213) \rangle$ le groupe engendré par σ. Comme σ est d'ordre 2, on a

$$H = \{1, \sigma\} = \{(123), (213)\}.$$

On décrit les classes à gauche de G suivant H. Rappelons que la classe d'une permutation (abc) est $[(abc)] = (abc)H$. On obtient les classes à gauche :

$$\begin{array}{l}[(123)] = (123)H = \{(123), (213)\} = (213)H = [(213)] \ ; \\ [(132)] = (132)H = \{(132), (312)\} = (312)H = [(312)] \ ; \\ [(231)] = (231)H = \{(231), (321)\} = (321)H = [(321)].\end{array}$$

On vérifie aisément que ces classes à gauche forment bien une partition de G.

Soit G un groupe et H un sous-groupe de G. On se pose maintenant la question suivante :

Question 2.2.12 Est-t-il possible de munir l'ensemble quotient G/H d'une sturture de groupe de telle sorte que la projection canonique $\pi_H : G \to G/H$ soit un morphisme de groupes ?

On se demande donc s'il est possible de définir une loi de composition sur G/H telle que $[g] \cdot [g'] = [gg']$.

Exemple 2.2.13 On reprend l'exemple précédent pour montrer que ceci n'est pas possible en général. Soit donc $G = \mathfrak{S}_3$ le groupe des permutations sur 3 éléments, soit $\sigma = (213) \in G$ et soit $H = \langle (213) \rangle = \{1, \sigma\} = \{(123), (213)\}$.

On se demande si on peut définir une loi de composition sur G/H telle que $[g] \cdot [g'] = [gg']$. Ainsi par exemple, on devrait avoir

$$[(123)] \cdot [(132)] = [(123)(132)] = [(132)].$$

Par ailleurs ona $[(123)] = [(213)]$ donc on doit aussi avoir

$$[(123)] \cdot [(132)] = [(213)] \cdot [(132)] = [(213)(132)] = [(231)].$$

On obtient que si une telle loi existait, on aurait $[(132)] = [(231)]$ ce qui est faux ! Il ne peut donc pas exister de telle loi pour G/H dans ce cas.

Au prochain paragraphe, on explique dans quels cas le quotient G/H peut être muni d'une loi de groupe qui répond positivement à la quesion ci-dessus.

2.3. Sous-groupe distingué ou normal

Définition 2.3.1 Soit G un groupe et H un sous-groupe de G. On dit que H est un **sous-groupe distingué** ou **normal** si pour tout $g \in G$, on a $gHg^{-1} \subset H$.

Lorsque H est un sous-groupe distingué de G, on écrira $H \triangleleft G$

Lemme 2.3.2 Soit G un groupe et H un sous-groupe. Les conditions suivantes sont équivalentes :

(i) H est un sous-groupe distingué ;

(ii) $gHg^{-1} \subset H$, pour tout $g \in G$;

(iii) $gHg^{-1} = H$, pour tout $g \in G$;

(iv) $gH = Hg$, pour tout $g \in G$;

(v) la classe à gauche de g est égale à la classe à droite de g, pour tout $g \in G$. □

Preuve. 1. $\Leftrightarrow$ 2. est vrai par définition.

2. $\Rightarrow$ 3. Il suffit de montrer que $H \subset gHg^{-1}$, pour tout $g \in G$, sachant que $gHg^{-1} \subset H$, pour tout $g \in G$. En multipliant la dernière inclusion par g^{-1} à gauche et par g à droite, on que $H \subset g^{-1}Hg$ pour tout $g \in G$ et en remplaçant g par g^{-1}, obtient le résultat.

3. $\Rightarrow$ 4. On a $gHg^{-1} = H$ donc en multipliant à droite par g, on obtient $gH = Hg$.

4. $\Rightarrow$ 1. On a $gH = Hg$ et en multipliant à droite par g^{-1}, on obtient $gHg^{-1} = H$.

4. $\Leftrightarrow$ 5. C'est la définition des classes à gauche et à droite. ■

Corollaire 2.3.3 Si le groupe G est abélien, alors tout sous-groupe est un sous-groupe distingué.

Exemple 2.3.4 Soit G un groupe.

(i) Le sous-groupe $H = \{1\}$ est un sous-groupe distingué de G.

(ii) Le sous-groupe $H = G$ est un sous-groupe distingué de G.

(iii) Si $G = \mathbb{Z}$, alors tous les sous-groupes $H = n\mathbb{Z}$ de G sont distingués.

(iv) Si $G = \mathrm{GL}_n(\mathbb{R})$ et $H = \mathrm{SL}_n(\mathbb{R})$, alors H est un sous-groupe distingué de G.

(v) Si $G = \mathrm{GL}_n(\mathbb{R})$ et $H = \mathrm{O}_n(\mathbb{R})$, alors H n'est pas distingué dans G.

Exemple 2.3.5 Soit $G = \mathfrak{S}_3$ le groupe des permutations sur 3 éléments, soit $\sigma = (213) \in G$ et soit

$$H = \langle (213) \rangle = \{1, \sigma\} = \{(123), (213)\}.$$

Alors H n'est pas un sous-groupe distingué. En effet, on a

$$(132)H(132)^{-1} = \{(132)(123)(132)^{-1}, (132)(213)(132)^{-1}\} = \{(123), (321)\} \neq H.$$

Proposition 2.3.6 Soit G un groupe fini et H un sous-groupe d'indice 2. Alors H est distingué dans G.

Preuve. Les classes à gauche de G suivant H forment une partition et leur nombre est $|G/H| = [G : H] = 2$. Il y a donc deux classes à gauche, l'une est la classe de l'unité $1 \in G : [1] = 1 \cdot H = H$. L'autre est de la forme $[x] = xH$ pour un certain $x \in G$ et doit être le complémentaire de H dans $G : [x] = xH = G \setminus H$. On peut faire la même remarque pour les classes à droite.

Soit maintenant $g \in G$, nous voulons montrer que $gH = Hg$ c'est-à-dire que les classes à gauche et à droite sont les mêmes. Si $gH = H$, alors $g \in H$ et $Hg = H$ donc $gH = Hg$. Sinon, $gH \neq H$ donc $g \notin H$ et $gH = G \setminus H$. Mais si $Hg = H$ alors $g \in H$ absurde donc $Hg \neq H$ donc $Hg = G \setminus H$ et $Hg = gH$. ∎

Théorème 2.3.7 Soit G un groupe et soit $H \triangleleft G$ un sous-groupe distingué. Alors

(i) la loi de composition $G/H \times G/H \to G/H$, $([g], [g']) \mapsto [gg']$ est bien définie,

(ii) elle induit une structure de groupe sur G/H,

(iii) pour cette structure de groupe, la projection canonique $\pi_H : G \to G/H$ est un morphisme de groupes. □

Preuve. 1. Soient $x, y \in G$ tels que $[x] = [g]$ et $[y] = [g']$. Il faut vérifier que $[xy] = [gg']$. La condition $[x] = [g]$ impose $x \in gH$ donc il existe $h \in H$ tel que $x = gh$. De même, il existe $h' \in H$ tel que $y = g'h'$. On a alors $xy = ghg'h' = gg'(g')^{-1}hg'h'$. Mais $(g')^{-1}hg' \in (g')^{-1}Hg' \subset H$ car $H \triangleleft G$. Ainsi $(g')^{-1}hg'h' \in H$ et $xy \ni gg'H$ donc $[xy] = [gg']$.

2. Montrons que $[1]$ est l'unité : on a $[1][g] = [g] = [g][1]$. Montrons que $[g^{-1}]$ est l'inverse de $[g]$: on a $[g][g^{-1}] = [gg^{-1}] = [1] = [g^{-1}][g] = [g^{-1}][g]$. Montrons enfin que la loi de composition est associative : on a $([g][g'])[g''] = [gg'][g''] = [(gg')g''] = [g(g'g'')] = [g][g'g''] = [g]([g'][g''])$.

3. On a $\pi_H(gg') = [gg'] = [g][g'] = \pi_H(g)\pi_H(g')$. ∎

Définition 2.3.8 Soit G un groupe et $H \triangleleft G$ un sous-groupe distingué. La structure de groupe sur le quotient G/H définie au théorème précédent s'appelle **groupe quotient** de G par H.

Exemple 2.3.9 Si $G = \mathbb{Z}$ et $H = n\mathbb{Z}$, alors $H \triangleleft G$ et le groupe quotient G/H est le groupe $\mathbb{Z}/n\mathbb{Z}$ usuel.

Proposition 2.3.10 Soit $H \triangleleft G$ un sous-groupe distingué et soit $H \subset K \subset G$ un sous-groupe de G contenant H. Alors H est distingué dans K *i.e.* $H \triangleleft K$.

Preuve. On doit montrer que $kHk^{-1} \subset H$ pour tout $k \in K$. Mais $K \subset G$ et on a $gHg^{-1} \subset H$ pour tout $g \in G$ d'où le résultat. ∎

Corollaire 2.3.11 Soit $H \triangleleft G$ un sous-groupe distingué de projection canonique $\pi_H : G \to G/H$. On a alors une bijection

$$\{\text{sous-groupes } K \subset G \text{ contenant } H\} \leftrightarrow \{\text{sous-groupes de } G/H\}.$$

Les bijections sont données par $K \mapsto K/H$ et $\bar{K} \mapsto \pi_H^{-1}(\bar{K})$.

Preuve. Notons que comme H est contenu dans K, l'ensemble K/H des classes de K suivant H forme un sous-ensemble de G/H. On a $K/H = \{kH \in G/H \mid k \in K\}$. Comme $H \triangleleft K$, lensemble K/H est un groupe pour la loi $[k][k'] = [kk']$ et c'est donc un sous-groupe de G/H. L'application $K \mapsto K/H$ est donc bien définie.

Si $\bar{K} \subset G/H$ est un sous-groupe, alors $\pi_H^{-1}(\bar{K})$ est un sous-groupe contenant $\pi_H^{-1}([1]) = H$. L'application $\bar{K} \mapsto \pi_H^{-1}(\bar{K})$ est donc bien définie.

On calcule les composées. Si $K \subset G$ est un sous-groupe contenant H, on a

$$\begin{aligned}
\pi_H^{-1}(K/H) &= \{g \in G \mid \pi_H(g) \in K/H\} \\
&= \{g \in G \mid \text{il existe } k \in K \text{ tel que } [g] = [k]\} \\
&= \{g \in G \mid \text{il existe } k \in K \text{ tel que } gH = kH\} \\
&= \{g \in G \mid \text{il existe } k \in K \text{ tel que } g \in kH\} \\
&= \{g \in G \mid g \in K\} \\
&= K.
\end{aligned}$$

Si $\bar{K} \subset G/H$ est un sous-groupe, alors on a

$$\pi_H^{-1}(\bar{K})/H = \{[g] \in G/H \mid \pi_H(g) \in \bar{K}\} = \{[g] \in G/H \mid [g] \in \bar{K}\} = \bar{K}.$$

Les deux applications sont bien inverses l'une de l'autre. ∎

Proposition 2.3.12 Soit $\varphi : G \to G'$ un morphisme de groupes et soient $H \triangleleft G$ et $H' \triangleleft G'$ des sous-groupes distingués.

(i) On a $\varphi^{-1}(H') \triangleleft G$.

(ii) Si φ est surjective, on a $\varphi(H) \triangleleft G'$.

Preuve. 1. Soit $g \in G$. On doit montrer que $g\varphi^{-1}(H')g^{-1} \subset \varphi^{-1}(H')$. Soit donc $x \in \varphi^{-1}(H')$. On a $\varphi(x) \in H'$. On a donc $\varphi(gxg^{-1}) = \varphi(g)\varphi(x)\varphi(g)^{-1} \in \varphi(g)H'varphi(g)^{-1} \subset H'$. Donc $gxg^{-1} \in \varphi^{-1}(H')$ et $\varphi^{-1}(H') \triangleleft G$.

2. Soit $g' \in G'$. On doit montrer que $g'\varphi(H)(g')^{-1} \subset \varphi(H)$. Soit donc $y \in \varphi(H)$. Il existe donc $h \in H$ tel que $y = \varphi(h)$. Comme φ est surjective, il existe $g \in G$ tel que $g' = \varphi(g)$. On a donc $g'y(g')^{-1} = \varphi(g)\varphi(h)\varphi(g)^{-1} = \varphi(ghg^{-1})$. Mais $ghg^{-1} \in gHg^{-1} \subset H$. Donc $g'y(g')^{-1} = \varphi(ghg^{-1} \in \varphi(H)$ et $\varphi(H) \triangleleft G'$. ∎

Exemple 2.3.13 On donne un exemple qui montre que la seconde partie de la proposition précédente est fausse si l'application φ n'est pas surjective. Soit $G = \mathfrak{S}_3$ et $H = \{1, (213)\} \subset G$. On a un morphisme de groupes $\varphi : H \to G$ donné par l'inclusion de H dans G. On a bien sur $H \triangleleft H$ mais $H = \varphi(H)$ n'est pas distingué pas G.

Corollaire 2.3.14 Le noyau d'un morphisme de groupes est toujours un sous-groupe distingué.

Preuve. En effet, $\mathrm{Ker}(\varphi) = \varphi^{-1}(\{1\})$ et $\{1\}$ est toujours un sous-groupe distingué. ∎

Exemple 2.3.15 On a $\mathrm{SL}_n(\mathbb{R}) = \mathrm{Ker}(\det : \mathrm{GL}_n(\mathbb{R}) \to \mathbb{R}^*)$ donc $\mathrm{SL}_n(\mathbb{R}) \lhd \mathrm{GL}_n(\mathbb{R})$.

Corollaire 2.3.16 Soit $H \lhd G$ un sous-groupe distingué de projection canonique $\pi_H : G \to G/H$. On a la bijection

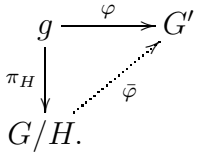
$$\{\text{sous-groupes } K \subset G \text{ contenant } H\} \leftrightarrow \{\text{sous-groupes de } G/H\}.$$

donnée par $K \mapsto K/H$ et $\bar{K} \mapsto \pi_H^{-1}(\bar{K})$ préserve les sous-groupes distingués.

Preuve. C'est la proposition précédente en tenant compte du fait que si K contient H, alors $\pi_H(K) = K/H$ et du fait que π_H est surjective. ∎

Théorème 2.3.17 (Propriété universelle du groupe quotient) Soit $H \lhd G$ un sous-groupe distingué et soit $\varphi : G \to G'$ un morphisme de groupes. On note $\pi_H : G \to G/H$ la projection canonique.

(i) Il existe un morphisme de groupes $\bar{\varphi} : G/H \to G'$ tel que $\varphi = \bar{\varphi} \circ \pi_H$ si et seulement si $H \subset \mathrm{Ker}(\varphi)$.



S'il existe le morphisme $\bar{\varphi}$ est unique.

(ii) Supposons que $\bar{\varphi}$ existe, alors $\mathrm{Ker}(\bar{\varphi}) = \mathrm{Ker}(\varphi)/H$. En particulier $\bar{\varphi}$ est injective si et seulement si $H = \mathrm{Ker}(\varphi)$.

(iii) Supposons que $\bar{\varphi}$ existe, alors $\mathrm{Im}(\bar{\varphi}) = \mathrm{Im}(\varphi)$. En particulier, $\bar{\varphi}$ est surjective si et seulement si φ est surjective. □

Preuve. 1. On commence par montrer que $\bar{\varphi}$ est unique. En effet, soit $[g] = \pi_H(g) \in G/H$, si $\bar{\varphi}$ existe, alors on a $\bar{\varphi}([g]) = \bar{\varphi}(\pi_H(g)) = \bar{\varphi} \circ \pi_H(g) = \varphi(g)$. Donc $\bar{\varphi}$ est uniquement déterminée par φ.

Montrons maintenant que $\bar{\varphi}$ existe si et seulement si $H \subset \mathrm{Ker}(\varphi)$. Si $\bar{\varphi}$ existe, alors on a $\bar{\varphi}([1]) = 1$ donc pour tout $h \in H$, on a $\varphi(h) = \bar{\varphi}(\pi_H(h)) = \bar{\varphi}([h]) = \bar{\varphi}([1]) = 1$. Ainsi $H \subset \mathrm{Ker}(\varphi)$.

Réciproquement, si $H \subset \mathrm{Ker}(\varphi)$, montrons que $\bar{\varphi}$ existe. On pose $\bar{\varphi}([g]) = \varphi(g)$. Ceci n'est *a priori* pas bien défini. Il faut vérifier que si $g' \in G$ est tel que $[g'] = [g]$, alors $\varphi(g') = \bar{\varphi}([g']) = \bar{\varphi}([g]) = \varphi(g)$. Mais $[g'] = [g]$ signifie que $g' \in gH$ donc il existe

$h \in H$ tel que $g' = gh$. On a alors $\varphi(g') = \varphi(gh) = \varphi(g)\varphi(h) = \varphi(g)1 = \varphi(g)$ car $h \in h \subset \mathrm{Ker}(\varphi)$.

On vérifie maintenant que $\bar{\varphi}$ est un morphisme de groupes. On a $\bar{\varphi}([g][g']) = \bar{\varphi}([gg']) = \varphi(gg') = \varphi(g)\varphi(g') = \bar{\varphi}([g])\bar{\varphi}([g'])$.

2. Montrons que $\mathrm{Ker}(\bar{\varphi}) = \mathrm{Ker}(\varphi)/H$, la seconde assertion en découle. Soit $[g] \in \mathrm{Ker}(\bar{\varphi})$, alors $1 = \bar{\varphi}([h]) = \varphi(g)$ donc $g \in \mathrm{Ker}(\varphi)$ et $[g] \in \mathrm{Ker}(\varphi)/H$.

Réciproquement, soit $g \in \mathrm{Ker}(\varphi)$, montrons que $[g] \in \mathrm{Ker}(\bar{\varphi})$. On a $\bar{\varphi}([g]) = \varphi(g) = 1$.

3. Montrons $\mathrm{Im}(\bar{\varphi}) = \mathrm{Im}(\varphi)$, la seconde assertion en découle.

Soit $g' \in \mathrm{Im}(\varphi)$, alors il existe $g \in G$ tel que $g' = \varphi(g)$ et on a $\bar{\varphi}([g]) = \varphi(g) = g'$ donc $g' \in \mathrm{Im}(\bar{\varphi})$.

Réciproquement, soit $g' \in \mathrm{Im}(\bar{\varphi})$, alors il existe $[g] \in G/H$ tel que $g' = \bar{\varphi}([g])$ et on a $\varphi(g) = \bar{\varphi}([g]) = g'$ donc $g' \in \mathrm{Im}(\varphi)$. ∎

Corollaire 2.3.18 Soit $\varphi : G \to G'$ un morphisme de groupes, alors $G/\mathrm{Ker}(\varphi)$ est isomorphe à $\mathrm{Im}(\varphi)$.

Corollaire 2.3.19 Soit $\varphi : G \to G'$ un morphisme de groupes surjectif, alors $G/\mathrm{Ker}(\varphi)$ est isomorphe à G'.

Exemple 2.3.20 On a les isomorphismes suivants.

(i) On a $\mathrm{GL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{R}) \simeq \mathbb{R}^*$ grâce au morphisme de groupe det.

(ii) On a $\mathbb{C}/\mathbb{Z} \simeq \mathbb{C}^*$ grâce au morphisme de groupes $z \mapsto e^z$.

(iii) On a $\mathbb{R}/\mathbb{Z} \simeq S^1$ où $S^1 = \{z \in \mathbb{C} \mid |z| = 1\}$ grâce au morphisme de groupes $x \mapsto e^{2i\pi x}$.

(iv) On a $\mathbb{Q}/\mathbb{Z} \simeq \mu$ grâce au morphisme de groupes $x \mapsto e^{2i\pi x}$ où

$$\mu = \{z \in \mathbb{C} \mid \text{il existe } n \in \mathbb{N} \text{ tel que } z^n = 1\} = \{\text{racines de l'unité}\}.$$

(v) On a $\mathfrak{S}_n/\mathfrak{A}_n \simeq \{\pm 1\}$ grâce à la signature ε.

Définition 2.3.21 Un grope G est dit **simple** si G n'a aucun sous-groupe distingué non trivial, cést-à-dire si on a l'implication : $H \triangleleft G \Rightarrow H = \{1\}$ ou $H = G$.

Proposition 2.3.22 Le groupe $\mathbb{Z}/n\mathbb{Z}$ est simple si et seulement si n est un nombre premier.

Preuve. Comme $\mathbb{Z}/n\mathbb{Z}$ est un groupe commutatif, tous ses sous-groupes sont distingués. ar ailleurs, les sous-groupes de $\mathbb{Z}/n\mathbb{Z}$ sont les $d\mathbb{Z}/n\mathbb{Z}$ avec d un diviseur de n. On veut que les seuls sous-groupes soient $\{1\} = n\mathbb{Z}/n\mathbb{Z}$ et $\mathbb{Z}/n\mathbb{Z} = 1\mathbb{Z}/n\mathbb{Z}$ c'est-à-dire que les seuls diviseurs de n soient 1 et n ou encore que n soit premier. ∎

Définition 2.3.23 Soit G un groupe et $H \subset G$ un sous-groupe. Le **normalisateur de H dans** G est le sous-ensemble $N_G(H)$ de G suivant :

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$

Proposition 2.3.24 Soit G un groupe et $H \subset G$ un sous-groupe.

(i) Le normalisateur $N_G(H)$ est un sous-groupe de G.

(ii) On a $H \lhd N_G(H)$.

(iii) Le normalisateur $N_G(H)$ est le plus grand sous-groupe de G dans lequel H est normal : si K est un sous-groupe de G contenant H tel que $H \lhd K$, alors $K \subset N_G(H)$.

Preuve. 1. On a $1H1^{-1} = H$, donc $1 \in N_G(H)$. Pour $x, y \in N_G(H)$, on a $xHx^{-1} = H$ et $yHy^{-1} = H$. En multipliant à gauche par y^{-1} et à droite par y la seconde égalité, on a $y^{-1}Hy = H$. En multipliant à gauche par x et à droite par x^{-1} cette dernière égalité, on a $xy^{-1}H(xy^{-1})^{-1}) = xy^{-1}Hyx^{-1} = xHx^{-1} = H$, donc $xy^{-1} \in N_G(H)$.

2. C'est la définition du normalisateur.

3. Soit $K \subset G$ un sous-groupe contenant H tel que $H \lhd K$. Alors pour tout $k \in K$, on a $kHk^{-1} = H$ donc $k \in N_G(H)$. ∎

Notation 2.3.25 Soit G un groupe et $E, F \subset G$ des sous-ensembles. On note EF l'ensemble suivant :

$$EF = \{xy \in G \mid x \in E \text{ et } y \in F\}.$$

Théorème 2.3.26 (Premier théorème d'isomorphisme) Soit G un groupe, soit $H \lhd G$ un sous-groupe distingué et soit $K \subset G$ un sous-groupe quelconque.

(i) On a $HK = KH$ et ce sous-ensemble est un sous-groupe de G.

(ii) On a $H \lhd KH$ et $(H \cap K) \lhd K$.

(iii) L'application $\bar{\varphi} : K/(K \cap H) \to KH/H$, $[k]_{K\cap H} = k(K \cap H) \mapsto [k]_H = kH$ est un isomorphisme de groupes. On a donc

$$K/(K \cap H) \simeq KH/H.$$

Preuve. 1. Soit $h \in H$ et $k \in K$, on montre que $hk \in KH$ et $kh \in HK$. On a $hk = k(k^{-1}hk) \in k(k^{-1}Hk) \subset kH$ (car $H \lhd G$) donc $hk \in KH$. De même, on a $kh = (khk^{-1})k \in (kHk^{-1})k \subset Hk \subset HK$. Ceci montre que $HK = KH$. Montrons maintenant que $KH = KH$ est un sous-groupe de G. On a $1 \in H$ et $1 \in K$ donc $1 = 1 \cdot 1 \in HK$. Soient $hk, h'k' \in HK$ avec $h, h' \in H$ et $k, k' \in K$. On a alors $(hk)(h'k')^{-1} = hk(k')^{-1}(h')^{-1} \in HKH = HHK = HK$. Donc HK est un sous-groupe de G.

2. Comme $H \triangleleft G$, et HK sous-groupe de G, on a $H \triangleleft HK$. Soit maintenant $k \in K$. On a $k(H \cap K)k^{-1} \subset kHk^{-1} \subset H$ car $H \triangleleft G$ et on a $k(H \cap K)k^{-1} \subset kKk^{-1} = K$ car $k \in K$. On a donc $k(H \cap K)k^{-1} \subset (H \cap K)$ pour tout $k \in K$ et $(H \cap K) \triangleleft K$.

3. On considère l'application $\varphi : K \to KH/H$ définie par $\varphi(k) = [k]_H = kH$. Montrons que c'est un morphisme de groupes : on a $\varphi(kk') = [kk']_H = [k]_H[k']_H$. Montrons que φ est surjective : soit $[kh]_H \in KH/H$ avec $k \in K$ et $h \in H$, alors $[kh]_H = khH = kH = [k]_H = \varphi(k)$ donc φ est surjective. Finalement montrons que $\mathrm{Ker}(\varphi) = H/capK$. Soit $k \in \mathrm{Ker}(\varphi)$, alors $kH = [k]_H = [1]_H = H$ donc $k \in H$ donc $k/inH \cap K$. Réciproquement, si $k \in H \cap K$, alors $\varphi(k) = [k]_H = kH = H = [1]_H$. En utilisant la propriété universelle du quotient, on obtient un isomorphisme $\bar{\varphi} : K/(H \cap K) \to KH/H$ avec $\bar{\varphi}([k]_{H\cap K}) = [k]_H$. ∎

Théorème 2.3.27 (Deuxième théorème d'isomorphisme) Soit G un groupe, soient $H \triangleleft G$ et $K \triangleleft G$ deux sous-groupes distingués tels que $H \subset K$.

(i) On a $H \triangleleft K$ et $K/H \triangleleft G/H$.

(ii) L'application $\bar{\varphi} : (G/H)/(K/H) \to G/K$, $[[g]_H]_{K/H} = gH \cdot K/H \mapsto [g]_K = gK$ est un isomorphisme de groupes. On a donc

$$(G/H)/(K/H) \simeq G/K.$$

Preuve. 1. Comme $H \triangleleft G$ et $K \subset G$ sous-groupe, on a $H \triangleleft K$. Par ailleurs, la projection canonique $\pi_H : G \to G/H$ est surjective et $K \triangleleft G$ donc $K/H = \pi_H(K) \triangleleft G/H$.

2. Considérons la projection canonique $\pi_K : G \to G/K$ définie par $\pi_K(g) = [g]_K$. C'est un morphime de groupes surjectif. Par ailleurs, $H \subset K = \mathrm{Ker}(\pi_K)$ donc il existe un unique morphisme de groupes $\varphi : G/H \to G/K$ tel que $\varphi([g]_H) = [g]_K$. Ce morphisme de groupes est surjectif. On montre que $\mathrm{Ker}(\varphi) = K/H$. En effet, si $k \in K$, alors $\varphi([k]_H) = [k]_K = kK = K = [1]_K$ donc $[k]_H \in \mathrm{Ker}(\varphi)$ et $K/H \subset \mathrm{Ker}(\varphi)$. Réciproquement, si $[g]_H \in \mathrm{Ker}(\varphi)$, alors $[g]_K = \varphi([g]_H) = [1]_K$ donc $g \in K$ et $[g]_H \in K/H$ et donc $\mathrm{Ker}(\varphi) = K/H$. Par la propriété universelle du quotient, on a un isomorphisme $\bar{\varphi} : (G/H)/(K/H) \to G/K$ tel que $\bar{\varphi}([[g]_H]_{K/H}) = [g]_K$. ∎

2.4. Retour au centre, centralisateur

Pour rappel, le centre $Z(G)$ d'un groupe est le sous-groupe

$$Z(G) = \{g \in G \mid gh = hg \text{ pour tout } h \in G\}.$$

Lemme 2.4.1 Le centre est un groupe commutatif (ou encore $Z(Z(G)) = Z(G)$). □

Preuve. Exercice. ∎

Proposition 2.4.2 Soit G un groupe.

(i) On a $Z(G) \triangleleft G$.

(ii) Si $G/Z(G)$ est monogène, alors G est commutatif.

Preuve. 1. Soit $g \in G$ et $x \in Z(G)$. Alors $gxg^{-1} = xgg^{-1} = x \in Z(G)$ donc $gZ(G)g^{-1} \subset Z(G)$ pour tout $g \in G$ et on a $Z(G) \triangleleft G$.

2. Supposons que $G/Z(G)$ est monogène. Il existe donc $g \in G$ tel que $G/Z(G) = \langle [g] \rangle$. Soient maintenant x et y deux éléments quelconques de G. On veut montrer que $xy = yx$. On a $[x], [y] \in \langle [g] \rangle$ donc il existe $n, m \in \mathbb{Z}$ tels que $[x] = [g^n]$ et $[y] = [g^m]$. Il existe donc $z, t \in Z(G)$ tels que $x = g^n z$ et $y = g^m t$. On a alors (comme z et t commutent avec tout élément) :

$$xy = g^n z g^m t = t g^n g^m z = t g^m g^n z = g^m t g^n z = yx.$$

Le groupe G est donc commutatif. ∎

Définition 2.4.3 Soit G un groupe et soit $E \subset G$ un sous-ensemble. Le **centralisateur de E dans G** noté $Z_G(E)$ est le sous-ensemble de G suivant :

$$Z_G(E) = \{g \in G \mid gh = hg \text{ pour tout } h \in E\}.$$

Lemme 2.4.4 Soit G un groupe et $E \subset G$ un sous-ensemble.

(i) L'ensemble $Z_G(E)$ est un sous-groupe de G.

(ii) On a $Z(G) = Z_G(G)$. □

Preuve. 1. Soit $x \in E$. On a $1 \cdot x = x = x \cdot 1$ donc $1 \in Z_G(E)$. Soient $g, h \in Z_G(E)$, on a $gx = xg$ et $hx = xh$. En multipliant la seconde égalité par h^{-1} à gauche et à droite, on obtient $h^{-1}x = xh^{-1}$. On a alors $gh^{-1}x = gxh^{-1} = xgh^{-1}$ donc $gh^{-1} \in C_G(E)$ ce qui prouve le résultat.

2. C'est la définition du centre. ∎

2.5. Commutateurs et sous-groupe dérivé

Définition 2.5.1 Soit G un groupe.

(i) Soient $x, y \in G$ deux éléments, le **commutateur** (x, y) de x et y est l'élément $(x, y) = xyx^{-1}y^{-1}$.

(ii) Soient $K, K \subset G$ deux sous-groupes de G, le **commutateur** (H, K) de H et K est le sous-groupe suivant de G : $(H, K) = \langle (x, y) \in G \mid x \in H \text{ et } y \in K \rangle$.

(iii) Le **sous-groupe dérivée de** G est le sous-groupe $D(G) = (G, G)$.

Lemme 2.5.2 Soit G un groupe.

(i) On a $D(G) = \{(g_1, h_1) \cdots (g_n, h_n) \mid n \in \mathbb{N} \text{ et } g_i, h_i \in G\}$.

(ii) On a $D(G) \lhd G$.

(iii) Le quotient $G/D(G)$ est commutatif.

(iv) Le groupe $D(G)$ est le plus petit sous-groupe distingué de G tel que $G/D(G)$ est commutatif, *i.e.* si $N \lhd G$ est un sous-groupe distingué de G tel que G/N est commutatif, alors $D(G) \subset N$. □

Preuve. 1. On a clairement l'inclusion "$\supset$". Il suffit donc de montrer l'autre inclusion et pour celà, il suffit de montrer que $H = \{(g_1, h_1) \cdots (g_n, h_n) \mid n \in \mathbb{N} \text{ et } g_i, h_i \in G\}$ est un sous-groupe de G. Pour $n = 0$, on a $1 \in H$. Il est clair que le produit de deux élément de H est encore dans H. Il reste à prouver que l'inverse d'un élément de H est dans H et pour celà, il suffit de montrer que $(g, h)^{-1} \in H$. Mais on a $(g, h)^{-1} = (ghg^{-1}h^{-1})^{-1} = hgh^{-1}g^{-1} = (h, g) \in H$.

2. Soit $x \in G$ et $g, h \in G$, alors on a

$$x(g, h)x^{-1} = xghg^{-1}h^{-1}x^{-1} = xgx^{-1}xhx^{-1}xg^{-1}x^{-1}xh^{-1}x^{-1} = (xgx^{-1}, xhx^{-1}).$$

De ce calcul et de 1., on déduit aisément que $xD(G)x^{-1} \subset D(G)$.

3. On note $[g], [h]$ les classe de $g, h \in G$ dans le quotient $G/D(G)$. On a $[g][h][g]^{-1}[h]^{-1} = [ghg^{-1}h^{-1}] = [1]$. On obtient en multipliant à droite par $[h]$ puis par $[g]$ l'égalité $[g][h] = [h][g]$ ce qui prouve que $G/D(G)$ est commutatif.

4. Soit $N \lhd G$ tel que G/N est commutatif. On vérifie que $D(G) \subset N$. Pour celà, il suffit de vérifier que $(g, h) \in N$ pour tout $g, h \in G$. Il suffit donc de montrer que $[g, h)]_N = [1]_N$. Mais on a $[(g, h)]_N = [ghg^{-1}h^{-1}]_N = [g]_N[h]_N[g]_N^{-1}[h]_N^{-1} = [g]_N[g]_N^{-1}[h]_N[h]_N^{-1} = [1]_N$. ■

3. Groupe symétrique

3.1. Définition

Soit $n \in \mathbb{N}$ un entier tel que $n \geq 1$ et soit $I_n = [1, n]$.

Définition 3.1.1 Le groupe symétrique $\mathfrak{S}_n$ est le le groupe $(\mathrm{Bij}(I_n), \circ)$ des bijections $f : I_n \to I_n$ avc pour loi de composition $\circ$ la composition des applications. Un élément de $\mathfrak{S}_n$ est appelé **permutation**.

Notation 3.1.2 Pour une permutation $\sigma : I_n \to I_n$, on écrira σ sous la forme de la liste des images des éléments de $[1, n]$:

$$\sigma = (\sigma(1), \cdots, \sigma(n)).$$

Lemme 3.1.3 Le groupe symétrique $\mathfrak{S}_n$ muni de la loi de composition $\circ$ est un groupe. □

Preuve. Exercice. ■

Exemple 3.1.4 (i) Le groupe $\mathfrak{S}_1$ a un unique élément : l'application identité notée $\mathrm{Id} = \mathrm{Id}_{I_1} = 1$. On a

$$S_1 = \{\mathrm{Id}\}.$$

(ii) Le groupe $\mathfrak{S}_2$ a deux éléments : l'identité $\mathrm{Id} = \mathrm{Id}_{I_2}$ et l"application $\tau_{1,2}$ définie par $\tau_{1,2}(1) = 2$ et $\tau_{1,2}(2) = 1$. On a

$$\mathfrak{S}_2 = \{\mathrm{Id}_{I_2}, \tau_{1,2}\} = \{(1, 2), (2, 1)\}.$$

(iii) Le groupe $\mathfrak{S}_3$ a 6 éléments :

$$\mathfrak{S}_3 = \{(1, 2, 3), (1, 3, 2), (2, 1, 3), (2, 3, 1), (3, 1, 2), (3, 2, 1)\}.$$

Lemme 3.1.5 Le groupe S_3 n'est pas commutatif. □

Preuve. En effet, on a $(2, 1, 3) \circ (2, 3, 1) = (1, 3, 2)$ et $(2, 3, 1) \circ (2, 1, 3) = (3, 2, 1)$. On a donc $(2, 1, 3) \circ (2, 3, 1) \neq (2, 3, 1) \circ (2, 1, 3)$. ■

Lemme 3.1.6 L'application $\iota_{n+1} : \mathfrak{S}_n \to \mathfrak{S}_{n+1}$ définie par

$$\iota_{n+1}(\sigma)(i) = \begin{cases} \sigma(i) & \text{pour } i \in [1,n] \\ n+1 & \text{pour } i = n+1, \end{cases}$$

est un morphisme injectif de groupes. Son image est le sous-groupe suivant :

$$\iota_{n+1}(\mathfrak{S}_n) = \{\sigma \in \mathfrak{S}_{n+1} \mid \sigma(n+1) = n+1\} = \mathfrak{S}_{n+1}(n+1).$$

Preuve. Montrons que cette application est injective : soient $\sigma, \tau \in \mathfrak{S}_n$ telles que $\iota_{n+1}(\sigma) = \iota_{n+1}(\tau)$. On a alors, pour tout $i \in [1,n]$, l'égalité $\sigma(i) = \iota_{n+1}(\sigma)(i) = \iota_{n+1}(\tau)(i) = \tau(i)$ et donc $\sigma = \tau$.

Soient $\sigma, \tau \in \mathfrak{S}_n$, on a

$$\iota_{n+1}(\sigma \circ \tau)(i) = \begin{cases} \sigma \circ \tau(i) & \text{pour } i \in [1,n] \\ n+1 & \text{pour } i = n+1, \end{cases}$$

Par ailleurs, on a

$$\iota_{n+1}(\sigma) \circ \iota_{n+1}(\tau)(i) = \begin{cases} \iota_{n+1}(\sigma)(\tau(i)) & \text{pour } i \in [1,n] \\ \iota_{n+1}(\sigma)(n+1) & \text{pour } i = n+1, \end{cases} = \begin{cases} \sigma(\tau(i)) & \text{pour } i \in [1,n] \\ n+1 & \text{pour } i = n+1, \end{cases}$$

On en déduit l'égalité $\iota_{n+1}(\sigma \circ \tau) = \iota_{n+1}(\sigma) \circ \iota_{n+1}(\tau)$ donc ι_{n+1} est un morphisme de groupes.

L'image est clairement contenue dans $\mathfrak{S}_{n+1}(n)$. Soit $\sigma \in \mathfrak{S}_{n+1}(n+1)$. On a alors $\sigma(I_n) \subset I_n$ et $\sigma|_{I_n} \in \mathfrak{S}_n$ donc $\iota_{n+1}(\sigma|_{I_n}) = \sigma$. ∎

Corollaire 3.1.7 Le groupe $\mathfrak{S}_n$ n'est pas commutatif pour $n = geq3$.

Preuve. Par récurrence sur n. Pour $n = 3$, c'est le Lemme 3.1.5. On suppose que $\mathfrak{S}_n$ n'est pas commutatif. Il existe donc $\sigma, \tau \in \mathfrak{S}_n$ tels que $\sigma \circ \tau \neq \tau \circ \sigma$. On considère alors $\iota_{n+1}(\sigma), \iota_{n+1}(\tau) \in \mathfrak{S}_{n+1}$. Comme ι_{n+1} est un morphisme de groupes injectif, on a $\iota_{n+1}(\sigma) \circ \iota_{n+1}(\tau) \neq \iota_{n+1}(\tau) \circ \iota_{n+1}(\sigma)$ et donc $\mathfrak{S}_{n+1}$ n'est pas commutatif. ∎

3.2. Transpositions

Définition 3.2.1 Soient $i, j \in [1,n]$ avec $i \neq j$. **La transposition** $\tau_{i,j}$ est la permutation définie par

$$\tau_{i,j}(k) = \begin{cases} j & \text{pour } k = i \\ i & \text{pour } k = j, \\ k & \text{sinon.} \end{cases}$$

Remarque 3.2.2 On a $\tau_{i,j}^2 = \mathrm{Id}_{i_n}$ ou encore $\tau_{i,j}^{-1} = \tau_{i,j}$. En particulier la transposition $\tau_{i,j}$ est d'ordre 2.

Lemme 3.2.3 Soit $\tau_{i,j} \in \mathfrak{S}_n$ une transposition, alors $\iota_{n+1}(\tau_{i,j})$ est la transposition $\tau_{i,j} \in \mathfrak{S}_{n+1}$. □

Preuve. Exercice. ■

Proposition 3.2.4 Tout élément $\sigma \in \mathfrak{S}_n$ est un produit d'au plus $n-1$ transpositions. En particulier

$$\mathfrak{S}_n = \langle \tau_{i,j} \mid i \neq j \rangle.$$

Preuve. Par récurrence sur n. L'assertion est vraie pour $n = 1$ et $n = 2$. Soit $\sigma \in \mathfrak{S}_{n+1}$ et soit $i = \sigma(n+1)$. On pose $\tau = \tau_{i,n+1} \circ \sigma$. On a $\tau(n+1) = \tau_{i,n+1}(i) = n+1$ en particulier $\tau \in \mathfrak{S}_{n+1}(n+1)$ donc $\tau = \iota_{n+1}(\sigma')$ avec $\sigma' \in \mathfrak{S}_n$. Par récurrence, la permutation σ' est un produit d'au plus $n-1$ transpositions $\sigma' = \tau_1 \circ \cdots \circ \tau_r$ avec $r \leq n-1$. Donc $\tau = \iota_{n+1}(\sigma') = \iota_{n+1}(\tau_1) \circ \cdots \iota_{n+1}(\tau_r)$ est un produit de $r \leq n-1$ transposition. Finalement, on a que $\sigma = \tau_{i,n+1} \circ \tau$ doit être un produit de $r+1 \leq n$ transpositions. ■

Proposition 3.2.5 (Principe de conjugaison pour les transpositions) Soit $\tau_{i,j} \in \mathfrak{S}_n$ une transposition et soit $\sigma \in \mathfrak{S}_n$.

(i) On a $\sigma\tau_{i,j}\sigma^{-1} = \tau_{\sigma(i),\sigma(j)}$.

(ii) Il existe $\sigma' \in \mathfrak{S}_n$ telle que $\tau_{1,2} = \sigma'\tau_{i,j}(\sigma')^{-1}$.

(iii) En particulier, deux transpositions sont toujours conjuguées.

Preuve. 1. On calcule $\sigma\tau_{i,j}\sigma^{-1}(k)$. Si $k = \sigma(i)$, on a $\sigma\tau_{i,j}\sigma^{-1}(k) = \sigma(\tau_{i,j}(\sigma^{-1}(\sigma(i))) = \sigma(\tau_{i,j}(i)) = \sigma(j)$. De même si $k = \sigma(j)$, on a $\sigma\tau_{i,j}\sigma^{-1}(k) = \sigma(\tau_{i,j}(\sigma^{-1}(\sigma(j)))) = \sigma(\tau_{i,j}(j)) = \sigma(i)$. Si par contre $k \notin \{\sigma(i), \sigma(j)\}$, alors $\sigma^1(k) \notin \{i, j\}$ et donc $\sigma(\tau_{i,j}(\sigma^{-1}(k))) = \sigma(\sigma^{-1}(k)) = k$. On a donc $\sigma\tau_{i,j}\sigma^{-1} = \tau_{\sigma(i),\sigma(j)}$.

2. Il suffit de prendre pour σ' une permutation telle que $\sigma'(i) = 1$ et $\sigma'(j) = 2$.

3. Si $\tau_{k,l}$ est une autre transposition, on prend $\sigma' \in \mathfrak{S}_n$ telle que $\sigma'(i) = k$ et $\sigma'(j) = l$ et on a $\sigma'\tau_{i,j}(\sigma')^{-1} = \tau_{k,l}$. ■

3.3. Ordre du groupe symétrique

Lemme 3.3.1 Soit $k \in [1, n+1]$ et soit $\iota_k : \mathfrak{S}_n \to \mathfrak{S}_{n+1}$ définie par

$$\iota_k(\sigma) = \tau_{k,n+1} \circ \iota_{n+1}(\sigma) \circ \tau_{k,n+1}^{-1}.$$

Alors ι_k est un morphisme de groupes injectif d'image

$$\iota_k(\mathfrak{S}_n) = \{\sigma \in \mathfrak{S}_{n+1} \mid \sigma(k) = k\} = \mathfrak{S}_{n+1}(k).$$

Preuve. On a $\iota_k = \mathrm{Int}_{\tau_{k,n+1}} \circ \iota_{n+1}$ donc ι_k est un morphisme de groupes injectif en tant que composée d'un morphisme de groupes injectif et d'un automorphisme de $\mathfrak{S}_{n+1}$.

L'image de ι_k est :

$$\iota_k(\mathfrak{S}_n) = \mathrm{Int}_{\tau_{k,n+1}}(\iota_{n+1}(\mathfrak{S}_n)) = \mathrm{Int}_{\tau_{k,n+1}}(\{\sigma \in \mathfrak{S}_{n+1} \mid \sigma(n+1) = n+1\}).$$

Montrons que $\mathrm{Int}_{\tau_{k,n+1}}(\{\sigma \in \mathfrak{S}_{n+1} \mid \sigma(n+1) = n+1\}) = \{\sigma \in \mathfrak{S}_{n+1} \mid \sigma(k) = k\}$. Soit $\sigma \in \mathfrak{S}_{n+1}$ tel que $\sigma(n+1) = n+1$. On a $\mathrm{Int}_{\tau_{k,n+1}}(\sigma)(k) = \tau_{k,n+1}\sigma\tau_{k,n+1}(k) = \tau_{k,n+1}\sigma(n+1) = \tau_{k,n+1}(n+1) = k$ donc $\mathrm{Int}_{\tau_{k,n+1}}(\sigma) \in \mathfrak{S}_{n+1}(k)$. Réciproquement, soit $\sigma \in \mathfrak{S}_{n+1}$ tel que $\sigma(k) = k$. On a $\sigma = \mathrm{Int}_{\tau_{k,n+1}}\mathrm{Int}_{\tau^{-1}_{k,n+1}}(\sigma)$. Soit $\tau = \mathrm{Int}_{\tau^{-1}_{k,n+1}}(\sigma) = \mathrm{Int}_{\tau_{k,n+1}}(\sigma)$, on a $\tau(n+1) = \tau_{k,n+1}\sigma\tau_{k,n+1}(n+1) = \tau_{k,n+1}\sigma(k) = \tau_{k,n+1}(k) = n+1$, donc $\tau = \mathrm{Int}_{\tau_{k,n+1}}(\sigma) \in \mathfrak{S}_{n+1}(n+1)$ et $\sigma = \mathrm{Int}_{\tau_{k,n+1}}(\tau)$. ∎

Lemme 3.3.2 Soit $\mathfrak{S}^i_{n+1} = \{\sigma \in \mathfrak{S}_{n+1} \mid \sigma(n+1) = i\}$. Alors l'application $\mathfrak{S}^i_{n+1} \to \mathfrak{S}_{n+1}(n+1)$ définie par $\sigma \mapsto \tau_{i,n+1} \circ \sigma$ est une bijection. □

Preuve. Commençons par montrer que cette application est bien définie, c'est-à-dire que pour $\sigma \in \mathfrak{S}^i_{n+1}$, on a $\tau_{i,n+1} \circ \sigma \in \mathfrak{S}_{n+1}(n+1)$. En effet, on a $\tau_{i,n+1}\sigma(n+1) = \tau_{,n+1}(i) = n+1$.

On définit une application réciproque $\mathfrak{S}_{n+1}(n+1) \to \mathfrak{S}^i_{n+1}$ par $\sigma \mapsto \tau_{i,n+1} \circ \sigma$. Cette application est bien définie : pour $\sigma \in \mathfrak{S}_{n+1}(n+1)$, on a $\tau_{i,n+1} \circ \sigma(n+1) = \tau_{i,n+1}(n+1) = i$..

On voit aisément que ces applications sont inverses l'une de l'autre. ∎

Corollaire 3.3.3 Le groupe $\mathfrak{S}_n$ est d'ordre $n!$.

Preuve. On procède par récurrence sur n. Pour $n = 1$, c'est vrai. Supposons donc que l'on a $|\mathfrak{S}_n| = n!$. Le groupe $\mathfrak{S}_{n+1}$ peut être réalisé comme l'union disjointe suivante :

$$\mathfrak{S}_{n+1} = \coprod_{i=1}^{n+1} \mathfrak{S}^i_{n+1}.$$

Par le lemme précédent, on a $|\mathfrak{S}^i_{n+1}| = |\mathfrak{S}_{n+1}(n+1)| = |\mathfrak{S}_n| = n!$. On en déduit l'égalité $|\mathfrak{S}_{n+1}| = (n+1) \cdot n! = (n+1)!$. ∎

3.4. Support

Définition 3.4.1 Le support d'une permutation $\sigma \in \mathfrak{S}_n$ est le sous-ensemble $\mathrm{Supp}(\sigma) \subset I_n$ défini par

$$\mathrm{Supp}(\sigma) = \{i \in I_n \mid \sigma(i) \neq i\}.$$

Lemme 3.4.2 Si deux permutations ont un support disjoint, alors elle commutent.□

Preuve. Exercice. ∎

3.5. Matrices de permutation

Définition 3.5.1 Soit $\sigma \in \mathfrak{S}_n$ et soit k un corps. **L'endomorphisme de permutation** associé à σ, noté $f_\sigma \in \mathrm{End}(k^n)$ et la **matrice de permutation** associée à σ, notée $P_\sigma \in M_n(\mathsf{k})$ sont définis de la manière suivante :

$$f_\sigma(e_i) = e_{\sigma(i)} \text{ und } P_\sigma = \mathrm{Mat}_{\mathcal{B}}(f_\sigma),$$

où $\mathcal{B} = (e_1, \cdots, e_n)$ est la base canonique de k^n.

Exemple 3.5.2 Soit $\sigma = (231) \in \mathfrak{S}_3$. On a

$$P_\sigma = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Lemme 3.5.3 Soit k un espace vectoriel et $n \in \mathbb{N}^*$.

(i) Soient $\sigma, \tau \in \mathfrak{S}_n$, on a $f_\sigma \circ f_\tau = f_{\sigma\circ\tau}$ et $P_\sigma \circ P_\tau = P_{\sigma\circ\tau}$.

(ii) Soit $\sigma \in \mathfrak{S}_n$, l'endomorphisme f_σ est un automorphisme d'espaces vectoriels et $P_\sigma \in \mathrm{GL}_n(\mathsf{k})$.

(iii) Les applications $f : \mathfrak{S}_n \to \mathrm{Aut}(\mathsf{k}^n)$, $\sigma \mapsto f_\sigma$ et $P : \mathfrak{S}_n \to \mathrm{GL}_n(\mathsf{k})$, $\sigma \mapsto P_\sigma$ sont des morphismes de groupes. □

Preuve. 1. L'égalité $P_\sigma \circ P_\tau = P_{\sigma\circ\tau}$ découle de l'égalité sur les endomorphisme : $f_\sigma \circ f_\tau = f_{\sigma\circ\tau}$. Comme $\mathcal{B}$ est une base, il suffit de vérifier que $f_\sigma \circ f_\tau(e_i) = f_{\sigma\circ\tau}(e_i)$. Or on a

$$f_\sigma \circ f_\tau(e_i) = f_\sigma(e_{\tau(i)}) = e_{\sigma(\tau(i))} = f_{\sigma\circ\tau}(e_i).$$

2. On a $f_\sigma \circ f_{\sigma^{-1}} = f_{\mathrm{Id}} = \mathrm{Id}$ donc f_σ est inversible. Le résultat sur les matrices en découle.

3. C'est l'égalité du 1. ■

Corollaire 3.5.4 L'application $\varepsilon : \mathfrak{S}_n \to \mathsf{k}^*$ définie par $\sigma \mapsto \det(P_\sigma)$ est un morphisme de groupes.

Preuve. C'est la composée de $P : \mathfrak{S}_n \to \mathrm{GL}_n(\mathsf{k})$ avec $\det : \mathrm{GL}_n(\mathsf{k}) \to \mathsf{k}^*$ qui sont deux morphismes de groupes. ■

Lemme 3.5.5 Soit $\tau_{i.j}$ une transposition, on a $\varepsilon(\tau_{i,j}) = -1$. □

Preuve. On commence par la transposition $\tau_{1,2}$. La matrice $P_{\tau_{1,2}}$ est la matrice

$$\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & I_{n-2} \end{pmatrix}$$

On obtient $\varepsilon(\tau_{1,2}) = \det(P_{\tau_{1,2}}) = -1$.

Dans le cas général, on écrit $\tau_{i,j} = \sigma\tau_{1,2}\sigma^{-1}$. Alors on a les égalités $\varepsilon(\tau_{i,j}) = \det(P_\sigma)\det(P_{\tau_{1,2}})\det(P_\sigma)^{-1} = \det(P_{\tau_{1,2}}) = -1$. ∎

Corollaire 3.5.6 L'application $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ définie par $\varepsilon(\sigma) = \det(P_\sigma)$ est un morphisme de groupes surjectif (pour $n \geq 2$).

Preuve. Il reste à montrer que ε est surjectif à valeurs dans $\{\pm 1\}$. D'après Lemme 3.2.4, on sait que toute permutation σ est un produit $\tau_1 \cdots \tau_k$ de transpositions. On a donc $\varepsilon(\sigma) = \varepsilon(\tau_1)\cdots\varepsilon(\tau_k) = (-1)^k \in \{-1, -1\}$. Le morphisme est surjectif car $\varepsilon(\tau_{1,2}) = -1$. ∎

Définition 3.5.7 Le morphisme de groupe $\varepsilon : \mathfrak{S}_n \to \{\pm 1\}$ défini ci-dessus est appelé **signature**.

3.6. Transpositions élémentaires

Définition 3.6.1 Soit $i \in [1, n-1]$. **La transposition élémentaire** s_i est la transposition $\tau_{i,i+1}$.

Lemme 3.6.2 Soient $i, j \in [1, n]$ avec $i < j$. On a

$$\tau_{i,j} = s_i \cdots s_{j-2} s_{j-1} s_{j-2} \cdots s_i.$$

En particulier, la transposition $\tau_{i,j}$ est un produit de $2(j-i)-1$ transpositions élémentaires. □

Preuve. On procède par récurrence sur $j - i$. Pour $j - i = 1$, on a $j = i + 1$ et $\tau_{i,j} = s_i$. Supposons que $\tau_{i,j} = s_i \cdots s_{j-2} s_{j-1} s_{j-2} \cdots s_i$ et montrons que $\tau_{i-1,j} = s_{i-1} \cdots s_{j-2} s_{j-1} s_{j-2} \cdots s_{i-1}$. On a

$$s_{i-1}\tau_{i,j}s_{i-1} = \tau_{i-1,j}$$

et on obtient le résultat en utilisant l'hypothèse de récurrence. ∎

Théorème 3.6.3 Toute permutation $\sigma \in \mathfrak{S}_n$ est un produit d'au plus $\frac{n(n-1)}{2}$ transpositions élémentaires. □

Preuve. On procède par récurrence sur n. Pour $n = 1$ ou $n = 2$ l'assertion est claire. Supposons que l'assertion est vraie pour $\mathfrak{S}_n$. Soit $\sigma \in \mathfrak{S}_{n+1}$ et soit $i = \sigma(n+1)$. Soit $\tau = s_n \cdots s_i \sigma$. On a $\tau(n+1) = n+1$. On a donc $\tau \in \mathfrak{S}_n$ (ou plutot dans $\mathrm{Im}(\iota_{n+1})$ et par hypothèse de récurrence, il existe $r \leq \frac{n(n-1)}{2}$ transpositions élémentaires $s_{i_1}, \cdots, s_{i_r}$ telles que $\tau = s_{i_1} \cdots s_{i_r}$. On a donc que σ est un produit d'au plus

$$\frac{n(n-1)}{2} + n - i + 1 \leq \frac{n(n-1)}{2} + n = \frac{n(n+1)}{2}$$

transpositions élémentaires. ∎

Lemme 3.6.4 On a

(i) $s_i^2 = \mathrm{Id}$, pour tout $i \in [1, n-1]$;

(ii) $(s_i s_{i+1})^3 = \mathrm{Id}$, pour tout $i \in [1, n-2]$;

(iii) $(s_i s_j)^2 = \mathrm{Id}$, pour tout couple $(i, j) \in [1, n-1]^2$ tel que $|i - j| > 1$. □

Preuve. Exercice. ∎

Définition 3.6.5 Soit $\sigma \in S_n$ et $\sigma \in \mathfrak{S}_n$.

(i) **L'ensemble des inversions de** σ est l'ensemble

$$I(\sigma) = \{(i, j) \in [1, n] \times [1, n] \mid i < j \text{ et } \sigma(i) > \sigma(j)\}$$

(ii) **La longueur de** σ est l'entier $\ell(\sigma) = |I(\sigma)|$.

Théorème 3.6.6 Soit $\sigma \in S_n$, on a $\varepsilon(\sigma) = (-1)^{\ell(\sigma)}$. □

Preuve. On va procéder par récurrence sur $\ell(\sigma)$. Si $\ell(\sigma) = 0$, alors $\sigma(i) < \sigma(i+1)$ pour tout $i \in [1, n-1]$ et $\sigma = \mathrm{Id}$.

Soit donc $\sigma \in \mathfrak{S}_n$ telle que $\ell(\sigma) > 0$. Il existe donc un entier $i \in [1, n-1]$ tel que $\sigma(i) > \sigma(i+1)$. Nous montrons les égalités suivantes :

$$s_i(I(\sigma)) = I(\sigma s_i) \cup \{(i+1, i)\} \text{ et } \ell(\sigma) = \ell(\sigma s_i) + 1.$$

Soit $(k, l) \in I(\sigma)$. Montrons que $s_i(k, l) = (s_i(k), s_i(l)) \in I(\sigma s_i) \cup \{(i+1, i)\}$. On a $k < l$ et $\sigma(k) > \sigma(l)$. On a aussi $s_i(k, l) = (s_i(k), s_i(l))$ et $\sigma s_i(s_i(k)) = \sigma(k) > \sigma(l) = \sigma s_i(s_i(l))$.

Si $(k, l) = (i, i+1)$, alors on a $s_i(k, l) = s_i(i, i+1) = (i+1, i)$. Supposons donc $(k, l) \neq (i, i+1)$. Si $\{k, l\} \cap \{i, i+1\} = \emptyset$, alors on a $s_i(k, l) = (k, l)$ donc $s_i(k) < s_i(l)$. On a donc $(s_i(k), s_i(l)) \in I(\sigma s_i)$. Si $k = i$ et $l \neq i+1$, alors comme $l > k = i$, on a $l > i+1$. On obtient $s_i(k) = i+1 < l = s_i(l)$. Ainsi on a $(s_i(k), s_i(l)) \in I(\sigma s_i)$. Si $l = i+1$ et $k \neq i$, alors comme $k < l = i+1$, on a $k < i$. On obtient $s_i(k) = k < i = s_i(l)$. Ainsi on a $(s_i(k), s_i(l)) \in I(\sigma s_i)$.

On a donc montré l'inclusion $s_i(I(\sigma)) \subset I(\sigma s_i) \cup \{(i+1,i)\}$. Réciproquement, on a $(i+1,i) = s_i(i,i+1) \in s_i I(\sigma)$. Soit $(a,b) = s_i(k,l) \in I(\sigma s_i)$ avec $k = s_i(a)$ et $b = s_i(b)$. Il suffit de montrer que $(k,l) \in I(\sigma)$. On a $\sigma(k) = \sigma s_i(a) > \sigma s_i(b) = \sigma(l)$. Si $(a,b) = (i,i+1)$, alors $\sigma(i+1) = \sigma s_i(a) > \sigma s_i(b) = \sigma(i)$, une contradiction donc $(a,b) \neq (i,i+1)$. Si $\{a,b\} \cap \{i,i+1\} = \emptyset$, alors on a $(k,l) = s_i(a,b) = (a,b)$, donc $k = a < l = b$ et $(k,l) \in I(\sigma)$. Si $a = i$ et $b \neq i+1$, alors comme $b > a = i$, on a $b > i+1$. On obtient $k = s_i(a) = i+1 < b = s_i(b) = l$. Ainsi on a $(k,l) \in I(\sigma)$. Si $b = i+1$ et $a \neq i$, alors comme $a < b = i+1$, on a $k = s_i(a) = a < i = s_i(b) = l$. On obtient $(k,l) \in I(\sigma)$.

On a donc montré l'égalité $s_i(I(\sigma)) = I(\sigma s_i) \cup \{(i+1,i)\}$. On en déduit les égalités $\ell(\sigma) = |I(\sigma)| = |s_i(I(\sigma))| = |I(\sigma s_i)| + 1 = \ell(\sigma s_i) + 1$.

Montrons l'égalité $\varepsilon(\sigma) = (-1)^{\ell(\sigma)}$ par récurrence sur $\ell(\sigma)$. Pour $\ell(\sigma) = 0$, on a $\sigma = 1$ et $\varepsilon(\sigma) = \varepsilon(1) = 1 = (-1)^0 = (-1)^{\ell(\sigma)}$.

Supposons par récurrence que si $\ell(\tau) = r \geq 0$, alors $\varepsilon(\tau) = (-1)^{\ell(\tau)}$. Soit σ telle que $\ell(\sigma) = r+1 > 0$. Il existe donc un entier $i \in [1,n]$ tel que $\sigma(i) > \sigma(i+1)$. On a alors $\ell(\sigma s_i) = \ell(\sigma) - 1 = r$. Par hypothèse de récurrence, on a $\varepsilon(\sigma s_i) = (-1)^{\ell(\sigma s_i)} = (-1)^{\ell(\sigma)-1}$. On en déduit $\varepsilon(\sigma) = \varepsilon(\sigma s_i s_i) = \varepsilon(\sigma s_i)\varepsilon(s_i) = (-1)^{\ell(\sigma)-1} \cdot (-1) = (-1)^{\ell(\sigma)}$. ∎

Proposition 3.6.7 Tout élément de $\mathfrak{S}_n$ est produit de transpositions de la forme $\tau_{1,i}$ pour $i \in [2,n]$, ou encore

$$\mathfrak{S}_n = \langle \tau_{1,i} \mid i \in [2,n] \rangle.$$

Preuve. Il suffit de montrer que toute transposition élémentaire $s_i = \tau_{i,i+1}$ peut-être ecrite comme produit d'éléments de la forme $\tau_{1,i}$ pour $i \in [2,n]$. Par le principe de conjugaison pour les transpositions (Proposition 3.2.5), on a $\tau_{1,i}\tau_{1,i+1}\tau_{1,i} = \tau_{1,i}\tau_{1,i+1}\tau_{1,i}^{-1} = \tau_{\tau_{1,i}(1),\tau_{1,i}(i+1)} = \tau_{i,i+1} = s_i$. ∎

3.7. Déterminant

Nous citons pour rappel le résultat bien connu suivant.

Théorème 3.7.1 Soit k un corps et soit $A \in M_n(\mathsf{k})$ une matrice. Alors on a

$$\det(A) = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{i,\sigma(i)} = \sum_{\sigma \in \mathfrak{S}_n} \varepsilon(\sigma) \prod_{i=1}^{n} a_{\sigma(i),i}.$$

Preuve. La seconde équation découle de la première et de la formule $\det(A^T) = \det(A)$.

Montrons la première formule. Pour ça, il suffit de montrer que la fonction

$$A \mapsto D(A) = \sum_{\sigma \in S_n} \varepsilon \prod_{i=1}^{n} a_{i,\sigma(i)}$$

est une fonction déterminant c'est-à-dire qu'elle est linéaire en les lignes, que $D(A) = 0$ si $\mathrm{Rg}(A) < n$ et que $D(I_n) = 1$.

On commence par calculer $D(I_n)$. On a $I_n = (\delta_{i,j})$ et donc

$$D(I_n) = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} \delta_{i,\sigma(i)}.$$

Mais $\delta_{i,\sigma(i)} \neq 0$ si et seulement si $i = \sigma(i)$. On a donc $\prod_{i=1}^{n} \delta_{i,\sigma(i)} \neq 0$ si et seulement si $i = \sigma(i)$ pour tout $i \in [1, n]$ *i.e.* $\prod_{i=1}^{n} \delta_{i,\sigma(i)} \neq 0$ si et seulement si $\sigma = \mathrm{Id}$. On obtient $D(I_n) = 1$.

Soit $A \in M_n(\mathsf{k})$ et soient $Z_1, \cdots, Z_k, \cdots, Z_n$ les lignes de A. Soit B la matrice dont les lignes sont $Z_1, \cdots, Z_k + Z'_k, \cdots, Z_n$ et C la matrice dont les lignes sont $Z_1, \cdots, Z'_k, \cdots, Z_n$. On écrit $Z_i = (a_{i,1}, \cdots, a_{i,n})$ et $Z'_k = (a'_{k,1}, \cdots, a'_{i,n})$. On a donc $A = (a_{i,j})$, $B = (b_{i,j})$ et $C = (c_{i,j})$ avec

$$b_{i,j} = \begin{cases} a_{i,j} & \text{pour } i \neq k \\ a_{k,j} + a'_{k,j} & \text{pour } i = k. \end{cases} \quad \text{et } c_{i,j} = \begin{cases} a_{i,j} & \text{pour } i \neq k \\ a'_{k,j} & \text{pour } i = k. \end{cases}$$

On a

$$\prod_{i=1}^{n} b_{i,\sigma(i)} = (a_{k,\sigma(k)} + a'_{k,\sigma(k)}) \prod_{i=1,\ i\neq k}^{n} a_{i,\sigma(i)} = \prod_{i=1}^{n} a_{i,\sigma(i)} + a'_{k,\sigma(k)} \prod_{i=1,\ i\neq k}^{n} a_{i,\sigma(i)}$$

donc

$$\prod_{i=1}^{n} b_{i,\sigma(i)} = \prod_{i=1}^{n} a_{i,\sigma(i)} + \prod_{i=1}^{n} c_{i,\sigma(i)}.$$

En obtient $D(B) = D(A) + D(C)$ et D est linéaire en les lignes des matrices.

Soit A une matrice telle que $\mathrm{Rg}(A) < n$. Alors il existe une ligne, disons la ligne k notée Z_k telle que $Z_k = \sum_{t=1,\ t\neq k}^{n} x_t Z_t$ où Z_t est la t-ième ligne de A. Soit A_t la matrice dont les lignes sont $(Z_1, \cdots, Z_{k-1}, Z_t, Z_{k+1}, \cdots, Z_n)$. Par linéarité, on a

$$D(A) = \sum_{t=1,\ t\neq k} x_t D(A_t).$$

Il suffit donc de montrer que l'on a $D(A_t) = 0$. On écrit $A_t = (b_{i,j})$. On a alors

$$D(A_t) = \sum_{\sigma \in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} b_{i,\sigma(i)}.$$

Comme les t-ième et k-ième lignes de A_t sont égales, on a $b_{t,j} = b_{k,j}$ pour tout j. Soit $\tau = \tau_{j,k}$ la transposition qui échange t et k. On a

$$\prod_{i=1}^{n} b_{i,\sigma\tau(i)} = b_{t,\sigma(k)} b_{k,\sigma(t)} \prod_{i\neq t,k}^{n} b_{i,\sigma(i)} = b_{k,\sigma(k)} b_{t,\sigma(t)} \prod_{i\neq t,k}^{n} b_{i,\sigma(i)} = \prod_{i=1}^{n} b_{i,\sigma(i)}.$$

On en déduit l'égalité suivante

$$D(A_t) = \sum_{\sigma\in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} b_{i,\sigma(i)} = \sum_{\sigma\in S_n} \varepsilon(\sigma) \prod_{i=1}^{n} b_{i,\sigma\tau(i)}.$$

En posant $\theta = \sigma\tau$ *i.e.* $\sigma = \theta\tau^{-1} = \theta\tau$, on obtient

$$D(A_t) = \sum_{\theta\in S_n} \varepsilon(\theta\tau) \prod_{i=1}^{n} b_{i,\theta(i)} = -\sum_{\theta\in S_n} \varepsilon(\theta) \prod_{i=1}^{n} b_{i,\theta(i)} = -D(A_t).$$

On a donc $D(A_t) = 0$. ∎

3.8. Cycles

Définition 3.8.1 1. Un élément $\sigma \in \mathfrak{S}_n$ est appelé r**-cycle** s'il existe des éléments $x_1, \cdots, x_r \in [1, n]$ deux à deux distincts tels que

$$\begin{array}{l} \sigma(x_k) = x_{k+1} \text{ pour tout } k \in [1, r-1], \\ \sigma(x_r) = x_1 \text{ et} \\ \sigma(x) = x \text{ pour tout } x \in [1, n] \setminus \{x_1, \cdots, x_r\}. \end{array}$$

Le r-cycle σ est alors noté $\sigma = [x_1, \cdots, x_r]$.

2. L'ensemble $\mathrm{Supp}(\sigma) = \{x_1, \cdots, x_r\}$ est le **support du cycle**. L'entier r est **la longueur du cycle**.

3. Deux cycles σ et σ' sont dits **disjoints** si leurs supports sont disjoints : $\mathrm{Supp}(\sigma) \cap \mathrm{Supp}(\sigma') = \emptyset$.

Exemple 3.8.2 Soit $n \in \mathbb{N}^*$.

(i) Toute transposition $\tau_{i,j}$ est un 2-cycle. On a $\tau_{i,j} = [i, j]$.

(ii) L'élément $(231) \in \mathfrak{S}_3$ est un 3-cycle. On a $(231) = [1, 2, 3]$.

Remarque 3.8.3 La longueur d'un cycle de $\mathfrak{S}_n$ est au plus n.

Lemme 3.8.4 Soit $\sigma = [x_1, \cdots, x_r]$ un cycle de longueur r. Alors $\mathrm{ord}(\sigma) = r$. □

Preuve. Il suffit de montrer que r est le plus petit entier tel que $\sigma^r = 1$. On commence par calculer $\sigma^k(x_1)$ pour $k \in [1, r-1]$. Par une récurrence immédiate, on a $\sigma^k(x_1) = x_{k+1}$. En particulier, on a $\sigma^k \neq 1$ pour $k < r$. Par ailleurs, une autre récurrence montrer que $\sigma^r(x_i) = x_i$ pour tout $i \in [1, r]$ et $\sigma^r(x) = x$ pour tout $x \in [1, n] \setminus \{x_1, \cdots, x_r\}$. On obtient $\sigma^r = 1$ et $\mathrm{ord}(\sigma) = r$. ∎

Lemme 3.8.5 Soit $\sigma = [x_1, \cdots, x_r]$ un cycle de longueur r. Alors son inverse est le r-cycle $[x_1, x_r, x_{r-1}, \cdots, x_2]$. □

Preuve. C'est un calcul direct. ∎

Proposition 3.8.6 Soit $\gamma = \sigma_1 \cdots \sigma_k$ un produit de cycles disjoints et soit $r_i = \mathrm{ord}(\sigma_i)$. Alors on a $\mathrm{ord}(\gamma) = \mathrm{ppcm}(r_1, \cdots, r_k)$.

Preuve. Remarquons que comme les cycles sont disjoints, ils commutent. Ainsi, on a $\gamma^a = \sigma_1^a \cdots \sigma_k^a$. Soit $d = \mathrm{ppcm}(r_1, \cdots, r_k)$. On a $\gamma^d = \sigma_1^d \cdots \sigma_k^d = \mathrm{Id}$ donc $\mathrm{ord}(\gamma)$ divise d. Réciproquement, soit a un entier tel que $\gamma^a = \mathrm{Id}$. On a $\mathrm{Id} = \gamma^a = \sigma_1^a \cdots \sigma_k^a$. Comme les supports sont disjoints, on doit avoir $\gamma_i^a = \mathrm{Id}$ pour tout $i \in [1, k]$ *i.e.* r_i divise a. On a donc que $\mathrm{ppcm}(r_1, \cdots, r_k)$ divise a. ∎

Proposition 3.8.7 (Principe de conjugaison pour les cycles) Soit $n \in \mathbb{N}^*$, soit $\sigma = [x_1, \cdots, x_r]$ un r-cycle et soit $\gamma \in \mathfrak{S}_n$.

(i) On a $\gamma\sigma\gamma^{-1} = [\gamma(x_1), \cdots, \gamma(x_r)]$.

(ii) Dans $\mathfrak{S}_n$, tous les r-cycles sont conjugués.

Preuve. 1. On note $x_{r+1} = x_1$ de telle sorte que $\gamma(x_r) = x_1 = x_{r+1}$. On calcule $\gamma\sigma\gamma^{-1}(k)$. Si $k = \gamma(x_i)$ pour un $i \in [1, r]$, on a $\gamma\sigma\gamma(k) = \gamma(s(\gamma^{-1}(\gamma(x_i)))) = \gamma(\sigma(x_i)) = \gamma(x_{i+1})$. Si $k \notin \{\gamma(x_1), \cdots, \gamma(x_r)\}$, alors $\gamma^{-1}(k) \notin \{x_1, \cdots, x_r\}$ et on a $\gamma(\sigma(\gamma^{-1}(k))) = \gamma(\gamma^{-1}(k)) = k$ ce qui montre le résultat.

2. Si $\sigma' = [y_1, \cdots, y_r]$, alors il suffit de prendre $\gamma \in \mathfrak{S}_n$ telle que $\gamma(x_i) = y_i$ et on a $\sigma' = [y_1, \cdots, y_r] = [\gamma(x_1), \cdots, \gamma(x_r)] = \gamma\sigma\gamma^{-1}$. ∎

Corollaire 3.8.8 On a $\mathfrak{S}_n = \langle [1, 2], [1, 2, \cdots, n] \rangle$.

Preuve. Il suffit de montrer que les transpositions élémentaires sont dans le sous-groupe engendré par $[1, 2]$ et $\sigma = [1, 2, \cdots, n]$. Par le principe de conjugaison des transpositions, on a $\sigma^k[1, 2]\sigma^{-k} = [\sigma^k(1), \sigma^k(2)] = [k+1, k+2] = s_k$ ce qui montre l'assertion. ∎

3.9. Groupe alterné

Définition 3.9.1 Soit $n \in \mathbb{N}^*$.

(i) Une permutation $\sigma \in \mathfrak{S}_n$ est dite **paire** si $\varepsilon(\sigma) = 1$ et **impaire** si $\varepsilon(\sigma) = -1$.

(ii) L'ensemble des permutation paire est appelé **groupe alterné** et est noté $\mathfrak{A}_n$:

$$\mathfrak{A}_n = \{\sigma \in \mathfrak{S}_n \mid \varepsilon(\sigma) = 1\} = \mathrm{Ker}(\varepsilon).$$

Proposition 3.9.2 Le groupe alterné est un sous-groupe distingué de $\mathfrak{S}_n$ et on a $\mathfrak{S}_n/\mathfrak{A}_n \simeq \{\pm 1\}$.

Preuve. C'est un sous-groupe distingué comme noyau d'un morphisme de groupes. L'isomorphisme provient du corollaire à la propriété universelle du quotient. ∎

Théorème 3.9.3 Soit $n \in \mathbb{N}^*$.

(i) Tout élément de $\mathfrak{A}_n$ est un produit d'un nombre pair de transpositions.

(ii) Un r-cycle est dans $\mathfrak{A}_n$ si et seulement si r est impair.

(iii) Le groupe $\mathfrak{A}_n$ est engendré par les 3-cycles. □

Preuve. 1. Toute permutation σ est un produit de transpositions : $\sigma = \tau_1 \cdots \tau_r$. Comme pour toute transposition τ_i, on a $\varepsilon(\tau_i) = -1$ et que $\varepsilon(\sigma) = 1$, on obtient $1 = \varepsilon(\sigma) = \varepsilon(\tau_1 \cdots \tau_r) = \varepsilon(\tau_1) \cdots \varepsilon(\tau_r) = (-1)^r$ et donc r est pair.

2. Soit $\sigma = [x_1, \cdots, x_r]$. On a l'égalité suivante : $\sigma = [x_1, x_2][x_2, x_3] \cdots [x_{r-1}, x_r]$ et donc σ est un produit de $r-1$ transpositions. On a donc $\varepsilon(\sigma) = (-1)^{r-1}$ et le résultat en découle.

3. On sait que tout élément σ de $\mathfrak{A}_n$ est produit d'un nombre pair de transpositions donc σ est produit d'éléments de la forme $\tau_1\tau_2$ où τ_1 et τ_2 sont des transpositions. Un produit de deux transpositions est toujours d'une des formes suivantes : $[x_1, x_2][x_1, x_2]$ ou $[x_1, x_2][x_3, x_4]$ ou encore $[x_1, x_2][x_2, x_3]$ avec x_1, x_2, x_3, x_4 deux à deux distincts. On montre que dans chacun des cas on peut écrire $\tau_1\tau_2$ comme produit de 3-cycles. Dans le premier cas, $\tau_1\tau_2 = [x_1, x_2][x_1, x_2] = 1$ et on a rien à faire. Sinon, on a

$$[x_1, x_2][x_3, x_4] = [x_1, x_3, x_2][x_1, x_3, x_4] \text{ et } [x_1, x_2][x_2, x_3] = [x_1, x_2, x_3].$$

On a donc que tout élément de $\mathfrak{A}_n$ est produit de 3-cycles. ∎

4. Action d'un groupe sur un ensemble

4.1. Définition et premières propriétés

Définition 4.1.1 Soit G un groupe et soit X un ensemble. Une **action** G **sur** X ou **opération de** G **sur** X est la donnée d'une application $G \times X \to X$, $(g, x) \mapsto g \cdot x$ telle que

(i) pour tout $x \in X$, on a $e_G \cdot x = x$;

(ii) pour tout $(g, h) \in G^2$ et tout $x \in X$, on a $(gh) \cdot x = g \cdot (h \cdot x)$.

On dira que G **agit** sur ou **opère** dans X.

Exemple 4.1.2 Soit G un groupe, soit $H \subset G$ un sous-groupe et soit X un sen-semble.

(i) **Action triviale** Elle est définie par l'application $G \times X \to X$ telle que $g \cdot x = x$ pour tout $g \in G$ et tout $x \in X$.

(ii) La **translation à gauche** de G sur lui-même est définie par l'application $G \times G \to G$ telle que $g \cdot h = gh$.

(iii) La **translation à droite** de G sur lui-même est définie par l'application $G \times G \to G$ telle que $g \cdot h = hg^{-1}$.

(iv) La **translation à gauche sur le quotient** G/H est l'application $G \times G/H \to G/H$ telle que $g \cdot [g']_H = [gh]_H$.

(v) La **conjugaison** est l'application $G \times G \to G$ telle que $g \cdot h = ghg^{-1}$.

(vi) **L'action standard de $\mathfrak{S}_n$ sur** $[1, n]$ est l'application $S_n \times [1, n] \to [1, n]$ telle que $\sigma \cdot i = \sigma(i)$.

(vii) **L'action standard de** $\mathrm{GL}_n(\mathsf{k})$ **sur** k^n est l'application $\mathrm{GL}_n(\mathsf{k}) \times \mathsf{k}^n \to \mathsf{k}^n$ telle que $A \cdot v = Av$.

Lemme 4.1.3 Soit $G \times X \to X$, $(g, x) \mapsto g \cdot x$ une action de G sur un ensemble X.

(i) L'application $\Phi(g) : X \to X$ définie par $\Phi(g)(x) = g \cdot x$ est une bijection de X dans lui-même et l'application

$$\Phi : G \to \mathrm{Bij}(X)$$

définie par $g \mapsto \Phi(g)$ est un morphisme de groupes.

(ii) Réciproquement, si $\Phi : G \to \mathrm{Bij}(X)$ est un morphisme de groupes, alors l'application $G \times X \to X$ définie par $(g, x) \mapsto g \cdot x = \Phi(g)(x)$ est une action de G sur X. □

Preuve. 1. On commence par montrer que $\Phi(gh) = \Phi(g) \circ \Phi(h)$. En effet, on a

$$\Phi(gh)(x) = (gh) \cdot x = g \cdot (h \cdot x) = \Phi(g)(h \cdot x) = \Phi(g)\left(\Phi(h)(x)\right) = \left(\Phi(g) \circ \Phi(h)\right)(x).$$

De cette relation, on déduit l'égalité $\Phi(g) \circ \Phi(g^{-1}) = \mathrm{Id}_X = \Phi(g^{-1}) \circ \Phi(g)$ donc $\Phi(g)$ est bijective d'inverse $\Phi(g)^{-1} = \Phi(g^{-1})$. On a aussi que Φ est un morphisme de groupes.

2. On a $e_G \cdot x = \Phi(e_G)(x) = \mathrm{Id}_X(x) = x$ et $g \cdot (h \cdot x) = \Phi(g)(\Phi(h)(x)) = (\Phi(g) \circ \Phi(h))(x) = \Phi(gh)(x) = (gh) \cdot x$ ce qui montre que c'est bien une action. ■

Définition 4.1.4 Soit $G \times X \to X$, $(g, x) \mapsto g \cdot x$ une action de G sur X.

(i) L'action est dite **transitive**, si pour toute paire $(x, y) \in X^2$, il existe un élément $g \in G$ tel que $g \cdot x = y$.

(ii) L'action est dite **fidèle** si l'implication suivante est satisfaite : ($g \cdot x = x$ pour tout $x \in X$) $\Rightarrow$ ($g = e_G$).

(iii) Soit $x \in X$. L'ensemble $G \cdot x = \{g \cdot x \in X \mid g \in G$ est appelé **orbite de** x.

(iv) L'ensemble des orbites est appelé **quotient de** X **par** G est est noté $X/G = \{G \cdot x | x \in X\}$.

(v) Un élément $x \in X$ est appelé **point fixe de l'action** si on a $g \cdot x = x$ pour tout $g \in G$. L'ensemble des points fixes est noté X^G.

(vi) Soit $x \in X$, le **stabilisateur de** x est l'ensemble $G_x = \{g \in G \mid g \cdot x = x\}$.

(vii) Plus généralement, si $Y \subset X$ est un sous-ensemble, le **stabilisateur de** Y est l'ensemble $G_Y = \{g \in G \mid g \cdot Y = Y\}$.

Remarque 4.1.5 L'action $G \times X \to X$ est fidèle si et seulement si le morphisme de groupe $\Phi : G \to \mathrm{Bij}(X)$ correspondant (voir Lemme 4.1.3) est injectif.

Proposition 4.1.6 Soit $G \times G \to G$ l'action de G sur lui-même par translation à gauche. Cette action est transitive et fidèle.

Preuve. Soit $L : G \to \mathrm{Bij}(G) \simeq \mathfrak{S}_n$ définie par $g \mapsto (L_g : G \to G, h \mapsto gh)$. On montre que L est injective ce qui montrera que l'action est fidèle. Soit $g \in \mathrm{Ker}L$, on a $L_g = \mathrm{Id}_G$ donc $L_g(h) = h$ pour tout $h \in G$. On a donc $gh = h$ et donc $g = e_G$.

Montrons que l'action est transitive. Soient $x, y \in G$, on cherche $g \in G$ tel que $g \cdot x = y$ *i.e* $gx = y$. Il suffit de prendre $g = yx^{-1}$. ■

Corollaire 4.1.7 (Théorème de Cayley) Soit G un groupe d'ordre n, alors G est un sous-groupe de $\mathfrak{S}_n$.

Exemple 4.1.8 Soit G un groupe et $H \subset G$ un sous-groupe.

(i) Soit $G \times G/H \to G/H$ l'action par translation à gauche sur le quotient. Alors cette die action est transitive et le stabilisateur $G_{[e_G]}$ de $[e_G] \in G/H$ est H.

(ii) Soit $G \times G \to G$ l'action par conjugaison. Alors le stabilisateur G_H de H est

$$G_H = \{g \in G \mid gHg^{-1} = H\} = \{g \in G \mid gH = Hg\} = Z_G(H).$$

(iii) $X = \{K \subset G \mid K \text{ est un sous-groupe}\}$ l'ensemble des sous-groupes de G. Alors l'application $G \times X \to X$ définie par $g \cdot K = gKg^{-1}$ est une action et on a

$$G_K = \{g \in G \mid g \cdot K = K\} = \{g \in G \mid gKg^{-1} = K\} = N_G(K).$$

$$X^G = \{K \in X \mid gKg^{-1} = K \text{ pour tout } g \in G\} = \{K \in X \mid K \triangleleft G\}.$$

Définition 4.1.9 Soit $G \times X \to X$ une action. On définit la relation suivante sur X : $x \sim y \Leftrightarrow y \in G \cdot x$.

Proposition 4.1.10 Soit $G \times X \to X$ une action

(i) La relation précédente $x \sim y$ est une relation d'équivalence.

(ii) Les classes d'équivalence pour cette relation sont les orbites.

(iii) Soit $x \in X$. L'application $G/G_x \to G \cdot x$ définie par $[g] \mapsto g \cdot x$ est bien définie et bijective.

Preuve. 1. On a $x = e_G \cdot x$ donc $x \sim x$ ainsi $\sim$ est réflexive. Soient $x, y \in X$ tels que $x \sim y$. Alors on a $y \in G \cdot x$ donc il existe $g \in G$ tel que $y = g \cdot x$. On a donc $x = g^{-1} \cdot y$ et $x \in G \cdot y$ *i.e* $y \sim x$ et $\sim$ est symétrique. Soient $x, y, z \in X$ tels que $x \sim y$ et $y \sim z$. On a donc des éléments $g, g' \in G$ tels que $y = g \cdot x$ et $z = g' \cdot y$. On en déduit $z = g'g \cdot x$ et $x \sim z$ donc $\sim$ est transitive.

2. Soit $x \in X$. La classe d'équivalence de x est $\{y \in X \mid x \sim y\} = \{y \in X \mid y \in G \cdot x\} = G \cdot x$.

3. Soient $g, g' \in G$ tels que $[g] = [g']$. Alors il existe $h \in G_x$ tel que $g' = gh$. On a donc $g' \cdot x = (gh) \cdot x = g \cdot (h \cdot x) = g \cdot x$ et l'application est bien définie. L'application est surjective par définition de $G \cdot x$. Soient $g, g' \in G$ tels que $g \cdot x = g' \cdot x$. Alors on a $x = (g^{-1}g') \cdot x$ et $g^{-1}g' = h \in G_x$. On a donc $g' = gh$ et $[g] = [g']$. L'application est injective. ∎

Corollaire 4.1.11 (Formule des classes) Soit $G \times X \to X$ une action avec G fini. On a l'équation

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

Preuve. Par la proposition précédente, on a $|G/G_x| = |G \cdot x|$ et par le théorème de Lagrange, on a $|G/G_x| = [G : G_x] = |G|/|G_x|$. ∎

Théorème 4.1.12 (Équation aux classes) Soit $G \times X \to X$ une action avec X fini. Alors on a l'équation

$$|X| = \sum_{[x] \in X/G} |G \cdot x| = \sum_{[x] \in X/G} [G : G_x].$$

Preuve. Comme les classes d'équivalence forment une partition de X, on a

$$X = \coprod_{[x] \in X/G} G \cdot x.$$

ce qui donne le résultat. ∎

Corollaire 4.1.13 Soit G un groupe fini et $H \subset G$ un sous-groupe. Supposons que le plus petit facteur premier de $|H|$ soit supérieur ou égal à l'indice $[G : H]$. Alors on a $H \triangleleft G$

Preuve. Soit p le plus petit facteur premier de H et soit $X = G/H$. Soit $H \times X \to X$ l'action par translation à gauche : $h \cdot gH = hgH$. Soit $x \in X$. Par la formule des classes, on a que $|H \cdot x|$ est un diviseur de $|H|$ donc $|H \cdot x| = 1$ ou $|H \cdot x| \geq p$. Par l'équation aux classes, on a

$$p \geq [G : H] = |X| = \sum_{[x] \in X/H} |G \cdot x|.$$

Soit $x = [e_G] \in X$. Alors x est un point fixe : $|H \cdot x| = |\{x\}| = 1$. On obtient donc

$$p - 1 \geq \sum_{[x] \in X/H,\ x \neq [e_G]} |G \cdot x|.$$

Comme $|G \cdot x| = 1$ ou $|G \cdot x| \geq p$ on doit avoir $|G \cdot x| = 1$ pour tout $x \in X$. Ainsi pour tout $[g] \in G/H$ et tout $h \in H$, on a $[hg] = [g]$ *i.e.* $g^{-1}hg \in H$ pour tout $g \in G$ et tout $h \in H$ *i.e.* $H \triangleleft G$. ∎

Exemple 4.1.14 Soit G un groupe fini et $H \subset G$ un sous-groupe.

(i) Si $[G : H]$ est le plus petit facteur premier de $|G|$, alors la condition est satisfaite.

(ii) En particulier, si $[G : H] = 2$ on a $H \triangleleft G$.

Définition 4.1.15 Soit p un nombre premier. Un groupe fini G est appelé **p-groupe** si son ordre est une puissance de p *i.e* il existe $k \in \mathbb{N}$ tel que $|G| = p^k$.

Corollaire 4.1.16 Soit G un p-groupe non trivial. Alors son centre n'est pas trivial.

Preuve. Soit $|G| = p^k$ avec $k > 0$. Soit $X = G$ et soit $G \times X \to X$ l'action par conjugaison. Montrons que l'on a $X^G = Z(G)$. Soit $z \in Z(G)$, alors on a $g \cdot z = gzg^{-1} = z$. Réciproquement, soit $z \in X^G$, alors on a $g \cdot z = z$ pour tout $g \in G$ donc $gzg^{-1} = z$ pour tout $g \in G$ *i.e.* $gz = zg$ pour tout $g \in G$.

En particulier, on obtient l'équivalence suivante

$$z \in Z(G) \Leftrightarrow |G \cdot x| = 1.$$

Par la formule des classes, on a

$$z \in Z(G) \Leftrightarrow p \text{ ne divise pas } |G \cdot x|.$$

Par l'équation aux classes, on obtient

$$p^k = |X| = \sum_{[x] \in X/H} |G \cdot x| = \sum_{[x] \in X/G,\ x \in Z(G)} |G \cdot x| + \sum_{[x] \in X/G,\ x \notin Z(G)} |G \cdot x|$$

et donc $p^k = |Z(G)| + \sum_{[x] \in X/G,\ x \notin Z(G)} |G \cdot x|$. Tous les termes de la seconde somme sont divisibles par p ce qui impose que $|Z(G)|$ est aussi divisible par p. Comme $Z(G)$ contient au moins un élément (le neutre), on obtient que $|Z(G)| \geq p > 1$. ∎

4.2. Application au groupe symétrique

Théorème 4.2.1 Soi $n \in \mathbb{N}^*$.

(i) Les cycles à support disjoint commutent.

(ii) Toute permutation $\gamma \in \mathfrak{S}_n$ s'écrit de manière unique (à l'ordre des facteurs près) comme produit de cycles à supports disjoints. □

Preuve. 1. On a déjà vu que deux permutations ayant des supports disjoints commutent.

2. Soit $H = \langle \gamma \rangle$ le sous-groupe engendré par γ. On fait opérer H sur $[1, n]$ par $\gamma^n \cdot x = \gamma^n(x)$. Soit B une orbite de cette action, soit $r = |B|$ et soit $x_1 \in B$. On a

$$B = \{x_1, x_2 = \gamma(x_1), \cdots, x_r = \gamma^{r-1}(x_1)\}.$$

On définit le r-cycle $\sigma_B = [x_1, \cdots, x_r]$. On a pour tout élément $x \in B$ l'égalité $\gamma(x) = \sigma_B(x)$. Comme les orbites forment une partition de $[1, n]$, on a donc

$$\gamma = \prod_{B \in [1,n]/H} \sigma_B.$$

De plus ce produit est un produit de cycles à supports disjoints. On a donc montré l'existence de la décomposition en produit de cycles à supports disjoints.

Montrons l'unicité. Pour toute décomposition de γ en produit de cycles à supports disjoints $\gamma = \prod_k \sigma_k$, l'ensemble des orbites X de l'action de $H = \langle\gamma\rangle$ sur $[1,n]$ est donné par les supports des cycles σ_k. On retrouve la décomposition précédent à l'ordre des facteurs près. ∎

Exemple 4.2.2 Soit $\gamma = (36451872) \in S_8$. Les orbites de γ sont $\{1,3,4,5\}$, $\{2,6,8\}$ et $\{7\}$. On a donc

$$\gamma = [1345][268][7] = [1345][268].$$

Définition 4.2.3 Soit $k \geq 1$ un entier. L'action $G \times X \to X$ d'un groupe G sur un ensemble X est dite k-**transitive** si pour$k$-uplet $(x_1, \cdots x_k) \in X^k$ d'éléments deux-à-deux distincts, et pour tout k-uplet $(y_1, \cdots y_k) \in X^k$ d'éléments deux-à-deux distincts, il existe $g \in G$ tel que

$$g \cdot x_i = y_i \text{ pour tout } i \in [1,k].$$

Exemple 4.2.4 Soit $\mathfrak{S}_n \times [1,n] \to [1,n]$ l'action définie par $\gamma \cdot x = \gamma(x)$. Alors cette action est n-transitive.

Lemme 4.2.5 L'action $A_n \times [1,n] \to [1,n]$ définie par $\gamma \cdot x = \gamma(x)$ est $(n-2)$-transitive. □

Preuve. Soient $x_1, \cdots x_{n-2} \in [1,n]$ deux-à-deux distincts et $y_1, \cdots y_{n-2} \in [1,n]$ deux-à-deux distincts. Soient $x_{n-1}, x_n, y_{n-1}, y_n$ tels que

$$\{x_1, \cdots, x_n\} = [1,n] = \{y_1, \cdots, y_n\}.$$

Comme $\mathfrak{S}_n$ agit n-transitivement sur $[1,n]$, il existe $\gamma \in \mathfrak{S}_n$ tel que $\gamma(x_i) = y_i$ pour tout $i \in [1,n]$. Si $\gamma \in \mathfrak{A}_n$, on a terminé. Sinon, on pose $\gamma' = \gamma \circ [x_{n-1}, x_n]$. Alors $\gamma' \in \mathfrak{A}_n$ et $\gamma(x_i) = y_i$ pour tout $i \in [1, n-2]$. ∎

Proposition 4.2.6 Si $n \geq 5$, alors tous les 3-cycles sont conjugués dans $\mathfrak{A}_n$.

Preuve. 4. Soient $\sigma = [x_1, x_2, x_3]$ et $\sigma' = [y_1, y_2, y_3]$ deux 3-cycles. Comme $n \geq 5$, on a $n - 2 \geq 3$. Comme $\mathfrak{A}_n$ agit $n-2$-transitivement dans $[1,n]$, il existe $\gamma \in \mathfrak{A}_n$ tel que $\gamma(x_i) = y_i$ pour tout $i \in [1,3]$. Par le principe de conjugaison, on a alors $\gamma\sigma\gamma^{-1} = \sigma'$. ∎

On rappelle l'existence d'un sous-groupe d'ordre 4, le groupe de Klein de $\mathfrak{S}_4$:

$$V_4 = \{\mathrm{Id}, [12][34], [13][24], [14][23]\} \subset \mathfrak{S}_4.$$

Corollaire 4.2.7 Soir $n \geq 2$.

(i) On a $D(\mathfrak{S}_n) = \mathfrak{A}_n$.

(ii) On a

$$D(\mathfrak{A}_n) = \begin{cases} \{\mathrm{Id}\} & \text{pour } n = 2, 3 \\ V_4 & \text{pour } n = 4 \\ \mathfrak{A}_n & \text{pour } n \geq 5. \end{cases}$$

Preuve. 1. Comme $\mathfrak{S}_n/\mathfrak{A}_n \simeq \{\pm 1\} \simeq \mathbb{Z}/2\mathbb{Z}$ est commutatif, on a l'inclusion $D(\mathfrak{S}_n) \subset \mathfrak{A}_n$ (Lemme 2.5.2). Pour $n = 2$, on a $\mathfrak{A}_n = \{\mathrm{Id}\}$ donc $\mathfrak{A}_n \subset D(\mathfrak{S}_n)$. Pour $n \geq 3$, on a

$$[a, b, c] = [b, c][a, b][b, c][a, b] = [b, c][a, b][b, c]^{-1}[a, b]^{-1} = [[b, c], [a, b]] \in D(\mathfrak{S}_n).$$

Comme $\mathfrak{A}_n$ est engendré par les 3-cycles, on obtient $\mathfrak{A}_n \subset D(\mathfrak{S}_n)$.

2. Pour $n = 2, 3$, le groupe A_n est commutatif donc $D(\mathfrak{A}_n) = \{\mathrm{Id}\}$. Pour $n = 4$, on a $V_4 = D(\mathfrak{A}_4)$ (cf. feuilles d'exercices). Supposons que l'on a $n \geq 5$ et soient $a, b, c \in [1, n]$ des éléments deux-à-deux distincts. Soient $x, y \in [1, n] \setminus \{a, b, c\}$ distincts. On a

$$\begin{aligned} [a, b, c] &= [a, b, x][a, c, y][a, x, b][a, y, c] \\ &= [a, b, x][a, c, y][a, b, x]^{-1}[a, c, y]^{-1} = ([a, b, x], [a, c, y]) \in D(\mathfrak{A}_n). \end{aligned}$$

On voit que tous les 3-cycles sont contenus dans $D(\mathfrak{A} - n)$ et comme ils engendrent $\mathfrak{A}_n$, on obtient l'inclusion $\mathfrak{A}_n \subset D(\mathfrak{A}_n)$ et donc $D(\mathfrak{A}_n) = \mathfrak{A}_n$. ∎

On a le résultat suivant (cf. feuilles d'exercices pour le cas $n = 5$).

Théorème 4.2.8 Le groupe A_n est simple pour $n \geq 5$. □

5. Théorèmes de Sylow

5.1. Sous-groupes de Sylow

Définition 5.1.1 Soit G un groupe fini et soit p un facteur premier de son ordre $|G|$. On écrit $|G| = p^\alpha m$ avec p ne divisant pas m. Un sous-groupe de G d'ordre p^α est appelé **p-sous-groupe de Sylow de G**.

Remarque 5.1.2 Soit G un groupe fini et p un facteur premier de $|G|$. Un sous-groupe H de G est un p-sous-groupe de Sylow si et seulement si son indice $[G : H]$ est premier avec p.

Exemple 5.1.3 Voici quelques exemples :

(i) Dans $\mathfrak{S}_3$, qui est d'ordre $6 = 2 \times 3$, on a trois 2-sous-groupes de Sylow : les sous-groupes engendrés par une transposition $\langle[12]\rangle$, $\langle[13]\rangle$ et $\langle[23]\rangle$ et on a un seul 3-sous-groupe de Sylow : le sous-groupe engendré par un 3-cycles $\langle[123]\rangle = \langle[132]\rangle$.

(ii) Dans $\mathfrak{S}_4$, qui est d'ordre $24 = 2^3 \times 3$, on a trois 2-sous-groupes de Sylow : $\langle[1234], [13]\rangle$, $\langle[1243], [14]\rangle$ et $\langle[1324], [12]\rangle$ et on a quatre 3-sous-groupes de Sylow : $\langle[123]\rangle$, $\langle[124]\rangle$, $\langle[134]\rangle$ et $\langle[234]\rangle$.

(iii) Soit p un nombre premier, soit $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ et soit $G = \mathrm{GL}_n(\mathbb{F}_p)$. On peut alors calculer l'ordre de G : c'est le nombre de bases de $\mathbb{F}_p^n$ et vaut

$$|G| = (p^n - 1)(p^n - p) \cdots (p^n - p^{n-1}) = p^{\frac{n(n-1)}{2}}(p^n - 1)(p^{n-1} - 1) \cdots (p - 1).$$

En effet, si $\mathcal{B}$ est la base canonique, on a une bijection $M \mapsto M \cdot \mathcal{B}$ entre G et l'ensemble des bases de $\mathbb{F}_p^n$. Pour compter, le nombre de bases, on commence par choisir le premier élément e_1 de la base : c'est un vecteur non nul quelconque donc un élément quelcoque de $\mathbb{F}_p^n \setminus \{0\}$. On a donc $p^n - 1$ choix. Pour le deuxième élément e_2, on doit prendre un vecteur non colinéaire à e_1 donc un élément de $\mathbb{F}_p^n \setminus \langle e_1\rangle$. On a $p^n - p$ choix. Si on a choisi $(e_1, \cdots, e_k)$, pour l'élément e_{k+1}, on doit prendre un vecteur dans $\mathbb{F}_p^n \setminus \langle e_1, \cdots, e_k\rangle$. On a $p^n - p^k$ choix. Le nombre de choix total est donc bien le produit ci-dessus.

Soit maintenant H le sous-groupe de G formé des matrices triangulaires supérieures avec un 1 sur la diagonale. Ce sous-groupe a pour ordre

$$|H| = p^{\frac{n(n-1)}{2}}$$

En effet, chaque élément au-dessus de la diagonale est choisi arbitrairement dans $\mathbb{F}_p$, on a p choix pour chacun de ces $n(n-1)/2$ éléments. Le sous-groupe H est donc un sous-groupe de Sylow de G.

Lemme 5.1.4 Soit G un groupe de cardinal $|G| = n = p^\alpha m$ avec p ne divisant pas m. Soit $H \subset G$ un sous-groupe et soit S un p-sous-groupe de Sylow de G. Alors, il existe un élément $g \in G$ tel que $gSg^{-1} \cap H$ est un p-sous-groupe de Sylow de H. En particulier, H a aussi un p-sous-groupe de Sylow. □

Preuve. On fait agit G sur $X = G/S$ via $G \times X \to X$ la translation à gauche : $g \cdot [g'] = [gg']$. Le stabilisateur de la classe $[g] = gS$ est $G_{[g]} = \{g' \in G \mid g' \cdot [g] = [g]\}$. Montrons que $G_{[}g] = gSg^{-1}$. Si $g' \in gSg^{-1}$, alors $g' = gsg^{-1}$ pour un $s \in S$. On a

$$g' \cdot [g] = [g'g] = [gsg^{-1}g] = [gs] = [g].$$

Réciproquement, si $g' \cdot [g] = [g]$, alors $[g'g] = [g]$ donc il existe $s \in S$ tel que $g'g = gs$ et donc $g' = gsg^{-1} \in gSg^{-1}$.

On fait agir H sur X par restriction de l'action de G donc H agit par $H \times X \to X$ avec $h \cdot [g] = [hg]$. Le stabilisateur de $[g]$ pour cette action est $H_{[g]} = \{h \in H \mid h \cdot [g] = [g]\} = \{h \in H \mid h \in G_{[g]}\} = \{h \in H \mid h \in gSg^{-1}\} = gSg^{-1} \cap H$.

Comme S est un p-groupe (c'est un p-sous-groupe de Sylow donc $|S| = p^\alpha$), il est est de même de tout sous-groupe et en particulier $gSg^{-1} \cap H$ est un p-groupe. Nous montrons qu'il existe un $g \in G$ tel que $|H/(gSg^{-1} \cap H)| = [H : gSg^{-1} \cap H]$ est permier avec p.

Si ce n'est pas le cas, alors par la formule des classes, on a $|H \cdot [g]| = |H|/|H_{[g]}| = |H/(gSg^{-1} \cap H)| = [H : gSg^{-1} \cap H]$ et cet entier est divisible par p pour tout $g \in G$. Mais alors, la formule des classes donne

$$m = |G/S| = |X| = \sum_{[x] \in X/H} |H \cdot x|$$

et comme tous les facteurs de droite sont divisibles par p, l'entier m serait divisible par p ce qui n'est pas possible. ■

5.2. Théorèmes de Sylow

Théorème 5.2.1 (Premier théorème de Sylow) Soit G un groupe et p un diviseur premier de $|G|$. Alors G admet au moins un p-sous-groupe de Sylow. □

Preuve. Soit $n = |G|$ l'ordre de G. Par le théorème de de Cayley, le groupe G est isomorphe à un sous-groupe de $\mathfrak{S}_n$. Par ailleurs, le groupe $\mathfrak{S}_n$ est un sous-groupe de $\mathrm{GL}_n(K)$ pour tout corps K grâce à l'application

$$\sigma \mapsto P_\sigma$$

qui à une permutation σ associe la matrice de permutation P_σ définie par $P_\sigma = (a_{i,j})_{i,j\in[1,n]}$ avec $a_{i,j} = \delta_{\sigma(i),j}$. Ainsi pour $K = \mathbb{F}_p$, le groupe G est un sous-groupe de $\mathrm{GL}_n(\mathbb{F}_p)$. Mais on a vu que $\mathrm{GL}_n(\mathbb{F}_p)$ admet un p-sous-groupe de Sylow donc par le lemme précédent, le groupe G admet un p-sous-groupe de Sylow. ∎

Corollaire 5.2.2 (Théorème de Cauchy) Soit G un groupe et p un facteur premier de son ordre $|G|$. Alors G admet un élément d'ordre p.

Preuve. Soit $|G| = p^\alpha m$ avec m premier avec p. Soit S un p-sous-groupe de Sylow de G. Soit $g \in S \setminus \{e_G\}$. Alors on a $\mathrm{ord}(g) \neq 1$ et $\mathrm{ord}(g)|p^\alpha$. On a donc l'égalité $\mathrm{ord}(g) = p^k$ pour un entier $k \geq 1$. Mais alors on sait que l'on a $\mathrm{ord}(g^{p^{k-1}}) = \frac{p^k}{\mathrm{ggT}(p^k,p^{k-1})} = \frac{p^k}{p^{k-1}} = p$ ce qui prouve le résultat. ∎

Corollaire 5.2.3 Un groupe G est un p-groupe si et seulement si l'ordre de chacun de ses éléments est une puissance de p.

Preuve. Soit G un p-groupe. Par le théorème de Lagrange, l'ordre de chaque élément est un diviseur de $|G|$ et donc est un puissance de p.

Réciproquement, si G n'est pas un p-groupe, alors il admet un facteur premier q différent de p et admet donc un élément d'ordre q qui n'est pas une puissance de p.∎

Corollaire 5.2.4 Soit p un nombre permier et soit G un sous-groupe de $\mathfrak{S}_p$ tel que p divise l'ordre $|G|$ de G et G contient une transposition. Alors on a $G = \mathfrak{S}_p$.

Preuve. On a $|S_p| = p! = pm$ avec p premier avec m. Comme p divise l'ordre de G, on a $|G| = pm'$ avec p preier avec m'. On sait qu'il existe $\sigma \in G$ avec $\mathrm{ord}(\sigma) = p$. Montrons que σ est un p-cycle. On écrit $\sigma = c_1 \cdots c_k$ la décomposition de σ en produit de cycles à supports disjoints. On a $\mathrm{ord}(\sigma) = \mathrm{ppcm}(\mathrm{ord}(c_1), \cdots, \mathrm{ord}(c_k))$ d'après le Corollaire 3.8.6. En particulier p divise $\mathrm{ord}(c_i)$ pour un entier i. Pour cet entier i, on doit avoir $\mathrm{ord}(c_i) = p$ et c_i est un p-cycle. Comme les supports sont disjoints, ce cycle est le seul cycle de σ et $\sigma = c_i$ est un p-cycle. Le groupe G contient donc une transposition τ et un p-cycle σ. On vérifie aisément que $\langle \tau, \sigma \rangle = \mathfrak{S}_p$ donc $G = \mathfrak{S}_p$.∎

Théorème 5.2.5 (Deuxième Théorème de Sylow) Soit p un nombre premier et soit G un groupe d'ordre $|G| = p^\alpha m$ avec p et m premiers entre eux. Soit k le nombre de p-sous-groupes de SYlow de G.

(i) Soit $H \subset G$ un sous-groupe qui est un p-groupe. Alors il existe un p-sous-groupe de Sylow S de G tel que $H \subset S$.

(ii) Tous les p-sous-groupes de Sylow de G sont conjugués.

(iii) Le nombre de p-sous-groupes de Sylow k divise $|G|$.

(iv) On a $k \equiv 1 \pmod{p}$. En particulier k divise m. □

Corollaire 5.2.6 (du Théorème 5.2.5.(ii)) Soit G un groupe et S un p-sous-groupe de Sylow. Alors on a l'équivalence

$$S \triangleleft G \Leftrightarrow S \text{ est l'unique } p\text{-sousgroupe de Sylow de } G \Leftrightarrow k = 1.$$

Preuve. La seconde équivalence est évidente (ici k est e nombre de p-sous-groupes de SYlow de G.

($\Rightarrow$). Soit S un p-sous-groupe de Sylow de G tel que $S \triangleleft G$. Soit T un autre p-sous-groupe de Sylow de G. D'après le Théorème 5.2.5.(ii) ces deux sous-groupes sont conjugués donc il existe $g \in G$ tel que $gSg^{-1} = T$. Mais on a $S \triangleleft G$ donc $S = gSg^{-1} = T$.

($\Leftarrow$). Soit S un p-sous-groupe de Sylow et soit $g \in G$. Alors gSg^{-1} est aussi un p-sous-groupe de SYlow donc $gSg^{-1} = S$ et on a $S \triangleleft G$. ■

Exemple 5.2.7 Soit G un groupe d'ordre 255, alors G n'est pas simple. En effet, on a $255 = 3 \times 5 \times 17$. Prenons $p = 17$. On a alors $|G| = p^\alpha m$ avec $\alpha = 1$ et $m = 3 \times 5 = 15$. Soit k le nombre de p-sous-groupes de Sylow. On a $k \equiv 1 \pmod{p}$ et $k|m$. Les diviseurs de 15 sont 1, 3, 5 et 15. Mais on a $3, 5, 15 \not\equiv 1 \pmod{p}$ donc on doit avoir $k = 1$. Ainsi K_{17} le seul 17-sous-groupe de Sylow de G est distingué donc G n'est pas simple.

Preuve. Commençons par montrer 1. et 2. Soit H un sous-groupe de G qui est aussi un p-groupe et soit S un p-sous-groupe de Sylow. Par le Lemme 5.1.4, il existe un $g \in G$ tel que $gSg^{-1} \cap H$ est un p-sous-groupe de Sylow de H. Comme H est un p-groupe, on doit avoir $gSg^{-1} \cap H = H$ *i.e.* $H \subset gSg^{-1}$. Comme le groupe gSg^{-1} est d'ordre $|S| = p^\alpha$ c'est un p-sous-groupe de Sylow ce qui prouve 1.

Si H est un p-sous-groupe de Sylow de G, on a dans la situation précédente $H \subset gSg^{-1}$ et $|H| = p^\alpha = |gSg^{-1}|$ donc on a $H = gSg^{-1}$, ce qui prouve 2.

3. On considère $X = \{p\text{-sous-groupes de Sylow de } G\}$ et l'action de G sur X par conjugaison $G \times X \to X$ avec $g \cdot S = gSg^{-1}$. Par 2. cette action est transitive. On a donc $G \cdot S = X$. Par la formule des classes, on obtient que $k = |X| = |G \cdot S|$ doit diviser $|G|$.

4. Soit S un p-sous-groupe de Sylow. On considère la restriction de l'opération précédente à S c'est-à-dire l'application $S \times X \to X$ définie par $s \cdot T = sTs^{-1}$. Soit $S \cdot T$ une orbite pour cette action. Par la formule des classes, on a que $|S \cdot T|$ divise $|S|$. On a donc

$$|S \cdot T| = \begin{cases} 1 & \text{si } S \cdot T = \{T\} \text{ } i.e. \text{ } T \text{ est un point fixe} \\ pa & \text{avec } a \in \mathbb{N} \text{ sinon.} \end{cases}$$

On note X^S l'ensemble des points fixes. Par l'équation aux classes, on a

$$|X| = \sum_{[x]\in X/S} |S\cdot x| = \sum_{x\in X^S} |S\cdot x| + \sum_{[x]\in X/S,\ x\notin X^S} |S\cdot x| = |X^S| + pb.$$

On a donc $k = |X| \equiv |X^S| \pmod p$. On va montrer que $X^S = \{S\}$ donc $|X^S| = 1$ ce qui terminera la preuve. Soit $T \in X^S$. Le groupe T est donc un p-sous-groupe de Sylow tel que $sTs^{-1} = T$ pour tout $s \in S$. Soit $H = \langle S, T\rangle$ le sous-groupe engendré par S et T. Alors S et T sont des p-sous-groupes de Sylow de H (car ce sont déjà des p-sous-groupes de Sylow de G). De plus, pour tout $t \in T$, on a $tTt^{-1} = T$. On a aussi $sTs^{-1} = T$ pour tout $s \in S$. On a donc $hTh^{-1} = T$ pour tout $h \in H$ et donc $T \triangleleft H$. Par le Corollaire 5.2.6, le groupe T est l'unique p-sous-groupe de Sylow de H. On doit donc avoir $T = S$ ce qui termine la preuve. ∎

Corollaire 5.2.8 (Décomposition primaire des groupes abéliens) Soit G un groupe fini commutatif. Alors pour tout facteur premier de $|G|$, il existe un unique p-sous-groupe de Sylow G_p de G donné par

$$G_p = \{g \in G \mid \mathrm{ord}(g) \text{ est une puissance de } p\}$$

De plus, on a

$$G = \prod_{p \text{ Primteiler von } |G|} G_p.$$

Preuve. Soit G_p un p-sous-groupe de Sylow. Comme G est commutatif, le sous-groupe G_p est distingué et donc c'est l'unique p-sous-groupe de Sylow de G. Soit $g \in G_p$, lo'rdre de g est un diviseur de $|G_p|$ qui est une puissance de p donc $\mathrm{ord}(g)$ est un puissance de p. On a donc $G_p \subset \{g \in G \mid \mathrm{ord}(g) \text{ est une puissance de } p\}$. Réciproquement, soit $g \in G$ tel que $\mathrm{ord}(g)$ est un puissance de p. Alors $\langle g\rangle$ est un p-groupe et donc est contenu dans un p-sous-groupe de Sylow. Donc $g \in \langle g\rangle \subset G_p$ car G_p est l'unique p-sous-groupe de Sylow.

Soient $p_1, \cdots, p_k$ les facteurs premiers de $|G|$ et soit $f : \prod_{i=1}^k G_{p_i} \to G$ l'application définie par $f(x_1, \cdots, x_k) = x_1 \cdots x_k$. Comme G est commutatif, cette application est un morphisme de groupes. Soit $(x_1, \cdots, x_k) \in \mathrm{Ker} f$. On a alors $x_1x_2\cdots x_k = e_G$. L'ordre de x_i est un puissance de p_i donc $\mathrm{ord}(x_i) = p_i^{\alpha_i}$ pour un entier $\alpha_i \geq 0$. On a donc

$$e_G = (x_1\cdots x_k)^{p_2^{\alpha_2}\cdots p_k^{\alpha_k}} = x_1^{p_2^{\alpha_2}\cdots p_k^{\alpha_k}}.$$

Comme $\mathrm{pgcd}(p_1^{\alpha_1}, p_2^{\alpha_2}\cdots p_k^{\alpha_k}) = 1$, il existe $a, b \in \mathbb{Z}$ tels que $ap_1^{\alpha_1} + bp_2^{\alpha_2}\cdots p_k^{\alpha_k} = 1$. On en déduit

$$x_1 = x_1^{ap_1^{\alpha_1} + bp_2^{\alpha_2}\cdots p_k^{\alpha_k}} = e_G.$$

De même on obtient $x_i = e_G$ pour tout i et f est injective. L'ordre de G est donné par

$$|G| = p_1^{\beta_1}\cdots p_k^{\beta_k}.$$

Par ailleurs, on a $|G_{p_i}| = p_i^{\beta_i}$ et $|\prod_{i=1}^k G_{p_i}| = |G|$. On en déduit que f est bijective et donc un isomorphisme. ∎

Exemple 5.2.9 Soit G un groupe commutatif d'ordre $|G| = p_1 \cdots p_k$. Alors

$$G \simeq \mathbb{Z}/p_1\mathbb{Z} \times \cdots \mathbb{Z}/p_k\mathbb{Z}.$$

On peut même montrer le r÷'esultats suivant :

Théorème 5.2.10 Soit G un groupe commutatif fini, alors il existe des entiers $a_1, \cdots, a_k \in \mathbb{N}$ avec $a_1|a_2|\cdots|a_k$ tels que

$$G \simeq \mathbb{Z}/a_1\mathbb{Z} \times \cdots \times \mathbb{Z}/a_k\mathbb{Z}.$$

6. Produit semi-direct

6.1. Produit de sous-groupes

Soient $H, K \subset G$ deux sous-groupes du groupe G. Rappelons la notation

$$HK = \{hk \in G \mid h, \in H \text{ et } k \in K\}.$$

On se demande à quelle condition l'ensemble HK est un sous-groupe de G.

Proposition 6.1.1 L'ensemble HK est un sous-groupe de G si et seulement si $HK = KH$.

Preuve. Si HK est un sous-groupe. Montrons que $KH \subset HK$. Soit donc $kh \in KH$ avec $h \in H$ et $k \in K$. On a $h^{-1} \in H$ et $k^{-1} \in K$ donc $h^{-1}k^{-1} \in HK$ et donc $kh = (h^{-1}k^{-1})^{-1} \in HK$. Montrons maintenant que $HK \subset KH$. Soit donc $x \in HK$. On a $x^{-1}ßHK$ donc $x^{-1} = hk$ avec $h \in H$ et $k \in K$. On a alors $h^{-1} \in H$ et $k^{-1} \in K$ donc $x = (hk)^{-1} = k^{-1}h^{-1} \in KH$.

Réciproquement, supposons que $HK = KH$. On a $1 \in HK$. Soient $hk \in HK$ et $xy \in HK$, avec $h, x \in H$ et $k, y \in K$. Alors $(hk)(xy)^{-1} = hky^{-1}x^{-1}$. On a $ky^{-1} \in K$ et $x^{-1} \in H$ donc $ky^{-1}x^{-1} \in KH = KH$ et il existe $a \in H$ et $b \in K$ tels que $ky^{-1}x^{-1} = ab$. On obtient $(hk)(xy)^{-1} = xab \in HK$. ∎

Corollaire 6.1.2 Si G est commutatif, le sous-ensemble HK est toujours un sous-groupe de G.

Définition 6.1.3 Soit G un groupe et H, K des sous-groupe de G. On dit que K **normalise** H si $K \subset N_G(H)$ c'est-à-dire si $kHk^{-1} = H$ pour tout $k \in K$.

Proposition 6.1.4 Si K normalise H, alors HK est un sous-groupe de G.

Preuve. Montrons que $HK = KH$. Soit $hk \in HK$ avec $h \in H$ et $k \in K$. Alors $k^{-1}hk = h' \in H$. Ainsi $hk = kh' \in KH$. De même, soit $kh \in KH$ avec $h \in H$ et $k \in K$. Alors $khk^{-1} = h'' \in H$. Ainsi $kh = h''k \in HK$. ∎

Corollaire 6.1.5 Si $H \triangleleft G$ est un sous-groupe distingué et si $K \subset G$ est un sous-groupe quelconque, alors HK est un sous-groupe de G. De plus, si H est K sont finis, on a

$$|HK| = \frac{|H| \cdot |K|}{|H \cap K|}.$$

Preuve. Comme $H \triangleleft G$, il est normalisé par tout sous-groupe de G. Pour la formule sur les ordres de ces groupes, il suffit d'appliquer le premier théorème d'isomorphisme : on a $K/(H \cap K) \simeq HK/H$ donc

$$\frac{|K|}{|H \cap K|} = |K/(H \cap K)| = |HK/H| = \frac{|KH|}{|H|}.$$

Le résultat en découle. ∎

Proposition 6.1.6 Soient $H \triangleleft G$ et $K \triangleleft G$ deux sous-groupes distingués de G. Alors $HK = KH \triangleleft G$ est un sous-groupe distingué.

Preuve. On a déjà vu que $HK = KH$ est un sous-groupe de G. Montrons que c'est un sous-groupe distingué/ Soit $hk \in HK$ avec $h \in H$ et $k \in K$ et soit $g \in G$. On a $g(hk)g^{-1} = ghg^{-1}gkg^{-1}$ et comme H et K sont distingués, on a $ghg^{-1} \in H$ et $gkg^{-1} \in K$ ce qui montre le résultat. ∎

6.2. Produit semi-directs

Lemme 6.2.1 Soient $N \triangleleft G$ un sous-groupe distingué et $H \subset G$ un sous-groupe tels que $N \cap H = \{1\}$. Alors NH est un sous-groupe de G et l'application $f : N \times H \to NH$ définie par $f(n, h) = nh$ est un bijection. □

Preuve. On a déjà vu que NH est un sous-groupe de G. Montrrons que f est une bijection. Elle est surjective par définition de NH. Montrons qu'elle est injective. Soient (n, h) et (n', h') tels que $f(n, h) = f(n', h')$. Alors $nh = n'h'$ donc $(n')^{-1}n = h'h^{-1} \in N \cap H = \{1\}$. On a donc $(n')^{-1}n = 1 = h'h^{-1}$ donc $n = n'$ et $h = h'$. L'application f est injective. ∎

Remarque 6.2.2 L'application ci-dessus n'est pas toujours un isomorphisme de groupes. Par exemple, soit $G = \mathfrak{S}_3$, soit $N = \langle [123] \rangle$ et soit $H = \langle [12] \rangle$. Alors $|G| = 6$, $|N| = 3$ et $|H| = 2$. On a $[G : N] = 6/3 = 2$ donc N est d'incide 2 donc est dinstingué. De plus si $g \in N\cap$ alors l'ordre de g divise 3 et 2 donc vaut 1 et $g = 1$. On a donc $N \cap H = \{1\}$. Ainsi $|NH| = |N||H|/|N \cap H| = 3 \times 2 = 6$ donc $NH = G = \mathfrak{S}_3$ et l'application $f : N \times H \to G$ ci-desus est une bijection.

Ce n'est pas un morphisme de groupes. En effet, $N \times H \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \simeq \mathbb{Z}/6\mathbb{Z}$ est commutatif mais $NH = G = \mathfrak{S}_3$ ne l'est pas. On peut vérifier que

$$f(([123], [12])([123], [12]) = f([123][123], [12][12]) = f([132], \mathrm{Id}) = [132]$$

alors que

$$f([123, [12])f([123][12]) = [123][12][123][12] = \mathrm{Id}.$$

Ainsi $f(([123], [12])([123], [12]) \neq f([123], [12])f([123], [12])$ et f n'est pas un morphisme de groupes.

La notion de produit semi-direct permet de définir un produit sur le produit $N \times H$ de telle sorte que l'application bijective ci-dessus devienne un isomorphisme.

Lemme 6.2.3 Soient N et H deux groupes et soit $\Phi : H \to \mathrm{Aut}(N), h \mapsto \Phi_h$ un morphisme de groupes (où $\mathrm{Aut}(N)$ est le groupe de automorphismes de groupes de N).

Soit $N \rtimes H := N \times_\Phi H := (N \times H, \star)$ le produit $N \times H$ muni du produit "tordu" suivant :

$$(n, h) \star (n', h') = (n\Phi_h(n'), hh').$$

Alors $N \rtimes H$ est un groupe d'élément neutre (e_N, e_H) et d'inverse $(n, h)^{-1} = (\Phi_{h^{-1}}(n^{-1}), h^{-1})$.□

Preuve. Élément neutre : on a $(e_N, e_H) \star (n, h) = (e_N\Phi_{e_H}(n), e_H h) = (\mathrm{Id}_N(n), h) = (n, h)$ und $(n, h) \star (e_N, e_H) = (n\Phi_h(e_N), he_H) = (n, h)$.

Inverse on a $(n, h)\star(\Phi_{h^{-1}}(n^{-1}), h^{-1}) = (n\Phi_h(\Phi_{h^{-1}}(n^{-1})), hh^{-1}) = (n\Phi_{hh^{-1}}(n^{-1}), e_H) = (n\mathrm{Id}_N(n^{-1}), e_H) = (nn^{-1}, e_H) = (e_N, e_H)$. On a aussi $(\Phi_{h^{-1}}(n^{-1}), h^{-1}) \star (n, h) = (\Phi_{h^{-1}}(n^{-1})\Phi_{h^{-1}}(n), h^{-1}h) = (\Phi_{h^{-1}}(n^{-1}n), e_H) = (\Phi_{h^{-1}}(e_G), e_H) = (e_N, e_H)$.

Associativité : on a

$$\begin{aligned}
(n, h) \star ((n', h') \star (n'', h'')) &= (n, h) \star (n'\Phi_{h'}(n''), h'h'') \\
&= (n\Phi_h(n'\Phi_{h'}(n'')), hh'h'') \\
&= (n\Phi_h(n')\Phi_{hh'}(n''), hh'h'') \quad . \\
&= (n\Phi_h(n'), hh') \star (n'', h'') \\
&= ((n, h) \star (n', h')) \star (n'', h'')
\end{aligned}$$

On a donc montré que $N \rtimes H$ muni du produit $\star$ est un groupe. ∎

Définition 6.2.4 Soient N et H deux groupe et soit $\Phi : H \to \mathrm{Aut}(N), h \mapsto \Phi_h$ un morphisme de groupes. Le groupe $N \rtimes H := N \times_\Phi H := (N \times H, \star)$ muni du produit $(n, h) \star (n', h') = (n\Phi_h(n'), hh')$ s'appelle **produit semi-direct de N et H associé à Φ.**

Exemple 6.2.5 Soit $\Phi : H \to \mathrm{Aut}(N)$ défini par $\Phi_h = \mathrm{Id}_N$ pour tout $h \in H$. Alors on a

$$(n, h) \star (n', h') = (n\Phi_h(n'), hh') = (n\mathrm{Id}_N(n'), hh') = (nn', hh')$$

et le produit semi-direct dans ce cas n'est rien d'autre que le produit (direct) des deux groupes.

Lemme 6.2.6 Soit $G = N \rtimes H$ et soient $N' = \{(n, e_H) \mid n \in N\}$ et $H' = \{(e_N, h) \mid h \in H\}$.

(i) Alors N' et H' sont des sous-groupes de G et $N' \triangleleft G$.

(ii) On a des isomorphismes $N \simeq N'$ et $H \simeq H'$ définis par $n \mapsto (n, e_H)$ et $h \mapsto (e_N, h)$.

(iii) On a $N' \cap H' = \{e_G\}$ et $G = N'H'$. □

Preuve. 1. L'application $\pi : G \to H$ définie par $\pi(n,h) = h$ est un morphisme de groupes et $\mathrm{Ker}\pi = N'$. On a donc que N' est un sous-groupe et $N' \triangleleft G$. On a $e_G \in H'$, on a $(e_N,h)^{-1} = (e_N,h^{-1}) \in H'$ et $(e_N,h) \star (e_N,h') = (e_N,hh') \in H'$ donc H' est un sous-groupe de G.

2. On a dans les deux cas les applications réciproques $n \mapsto (n,e_H)$ et $h \mapsto (e_N,h)$ et ces applications sont des morphismes de groupes.

3. On a $N' \cap H' = \{(e_n,e_H)\} = \{e_G\}$ et $(n,h) = (n,e_H) \star (e_N,h)$ donc $G = N'H'$. ■

Théorème 6.2.7 Soit G un groupe, soit $H \subset G$ un sous-groupe et soit $N \triangleleft G$ un sous-groupe distingué.

(i) Si $N \cap H = \{e_G\}$ et $G = NH$, alors en posant $\Phi : H \to \mathrm{Aut}(N)$ avec $\Phi_h(n) = hnh^{-1}$, l'application

$$f : N \times_\Phi H \to G,\ (n,h) \mapsto nh$$

est un isomorphisme de groupes.

(ii) Si de plus on a $H \triangleleft G$, alors l'isomorphisme précédent est un ismorphisme $f : N \times H \to G$ avec le produit direct. □

Preuve. 1. On a

$$f((n,h) \star (n',h')) = f(n\Phi_h(n'),hh') = nhn'h^{-1}hh' = nhn'h' = f(n,h)f(n',h').$$

Donc f est un morphisme de groupes. On a déjà vu que cette application est bijective, c'est donc un isomorphisme de groupes.

2. Soient $h \in H$ et $n \in N$. On a $N \ni n^{-1}(hnh^{-1}) = (n^{-1}hn)h^{-1} \in H$ also donc $n^{-1}hnh^{-1} = e_G$. On a donc $hn = nh$ et $\Phi_h(n) = n$. On a donc $N \rtimes H = N \times H$ ce qui montre le résultat. ■

Exemple 6.2.8 Quelques exemples de produits semi-directs (plus ou moins) bien connus :

(i) Soit $G = \mathfrak{S}_3$, soit $\tau = [123]$ et soit $\sigma = [12]$. Soit $N = \mathfrak{A}_3 = \langle [123] \rangle$ et soit $H = \langle [12] \rangle$. Le sous-groupe N est d'indice 2 dans G donc distingué et $N \cap H = \{1\}$. Comme N est distingué les applications de conjugaison $\mathrm{Int}_s : N \to N$ sont des morphismes de groupes et l'application $\Phi : H \to \mathrm{Aut}(N)$, $\Phi_h = \mathrm{Int}_h$ est un morphisme de groupes.

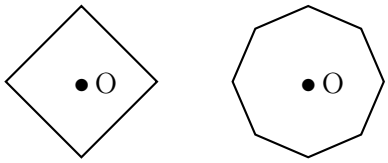
Le théorème précédent nous dit que l'application

$$N \rtimes H \to \mathfrak{S}_3,\ (n,h) \mapsto nh$$

est un isomorphisme de groupes.

(ii) De manière général, on a $\mathfrak{S}_n \simeq \mathfrak{A}_n \rtimes \{\pm 1\}$.

(iii) Groupe diédral Soit R_n un polygôme régulier à n côtés. Par exemple, $R_n = \{e^{\frac{2ik\pi}{n}} \mid k \in [0, n-1]\}$.



$n = 4$ $\qquad$ $n = 8$

Soit $G = D_{2n}$ le groupe des isométries de R_n. On montre facilement que $G = \langle \sigma, \tau \rangle$ où σ est la symétrie par rapport à l'ax horizontal et τ est la rotation d'angle $\frac{2\pi}{n}$. Le groupe G est d'ordre $|G| = 2n$. Soit $N = \langle \tau \rangle$ et $H = \langle \sigma \rangle$. Alors on a $N \triangleleft G$, $N \cap H = \{1\}$ et $G = NH$. Ainsi on a un isomorphisme

$$N \rtimes H \to G, \ (n, h) \mapsto nh.$$

Corollaire 6.2.9 Soient p et q des nombres premiers et soit G un groupe d'ordre $|G| = p^k q^l$ avec $k, l \geq 1$ tels que $q > p^k$. Alors on a $G \simeq G_q \rtimes G_p$ où G_p et G_q sont des p-sous-groupes de Sylow et q-sous-groupes de Sylow quelconques.

Preuve. Par le Corollaire 4.1.13 ou le second théorème de Sylow, ona $N = G_q \triangleleft G$. Soit $H = G_p$. Alors $|N \cap H|$ est un diviseur de $p^k = |G_p|$ et de $q^l = |G_q|$ et donc $|N \cap H| = 1$ donc $N \cap H = G_p \cap G_q = \{e_G\}$. On a donc $|G_p G_q| = |G_p \cdot |G_q| = p^k q^l = |G|$ donc $G = G_q G_p$. L'application $G_q \rtimes G_p \to G, \ (a, b) \mapsto ab$ est donc un isomorphisme par le Théorème 6.2.7. ∎

Théorème 6.2.10 Soit p un nombre premier et G un groupe d'ordre p^2. Alors on a $G \simeq \mathbb{Z}/p^2\mathbb{Z}$ ou $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. □

Preuve. Premier cas, il existe $g \in G$ avec $\mathrm{ord}(g) = p^2$. Alors $\mathbb{Z}/p^2\mathbb{Z} \simeq \langle g \rangle = G$.

Second cas, tous les éléments de G différents de 1 sont d'ordre p. Soit $g \in G \backslash \{1\}$. Alors $|\langle g \rangle| = p$. Il existe donc $h \in G \backslash \langle g \rangle$. Soit $N = \langle g \rangle$ et $H = \langle h \rangle$. Alors on a $p = |N| = |H|$ donc $N \simeq \mathbb{Z}/p\mathbb{Z} \simeq H$. De plus, p est le plus petit facteur premier de $|N|$ (ou de $|H|$) et est plus grand que l'indice de N (ou de H) : $|H| = |N| = p \geq p = [G : N] = [G : H]$. Le Corollaire 4.1.13 nous dit alors que l'on a $N \triangleleft G$ et $H \triangleleft G$.

L'intersection $H \cap N$ est un sous-groupe propre de H car $h \in H \setminus N$. On a donc que $|H \cap N|$ divise p et $|H \cap N| < p$. On doit donc avoir $|N \cap H| = 1$ et $N \cap H = \{e_G\}$. Comme N et H sont distingués, on a $\langle N, H \rangle = NH = HN$. Ce sous-groupe de G est de cardinal $|N| \cdot |H| / |N \cap H| = p^2 = |G|$ donc $NH = G$. Le Théorème 6.2.7 implique maintenant que l'on a un isomorphisme $G \simeq N \times H$ et donc $G \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. ∎

Remarque 6.2.11 Pour les groupes G d'ordre $|G| = p^3$ la classification est déjà plus difficile ainsi que le montrer le cas $p = 2$. En effet, on a vu (en TD) que les groupes suivants sont d'ordre $8 = 2^3$ et non isomorphes :

$$\mathbb{Z}/8\mathbb{Z}, \quad \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad D_8, \quad \mathbb{H}.$$

En fait ce sont tous les groupes d'ordre 8 à isomorphisme près (exercice).

7. Géométrie

7.1. Espaces affines et applications affines

Définition 7.1.1 Soit E un $\mathbb{R}$-espace vectoriel.

(i) **L'espace affine $\mathcal{E}$ d'espace vectoriel direction** E est l'ensemble $\mathcal{E} = E$ muni de l'action $E \times \mathcal{E} \to \mathcal{E}$ de E sur $\mathcal{E}$ définie par $(u, A) \mapsto u \cdot A = A + u$ (on notera par des lettres majuscules les éléments de $\mathcal{E}$ et des lettres minuscules les éléments de E).

(ii) On a un application $\mathcal{E}^2 \to E$ définie par $(A, B) \mapsto \overrightarrow{AB} = B - A$.

(iii) Si $(\mathcal{E}, E)$ est un espace affine d'espace vectoriel direction E et $(\mathcal{F}, F)$ est un espace affine d'espace vectoriel direction F, une **application affine** $f : \mathcal{E} \to \mathcal{F}$ est une application telle qu'il existe une application linéaire $\vec{f} : E \to F$ et un point $O \in cE$ tels que
$$f(A) = f(O) + \vec{f}(\overrightarrow{OA}).$$

(iv) L'ensemble des application affines de $\mathcal{E}$ dans $\mathcal{E}$ est noté $\mathrm{Aff}(E, F)$.

(v) L'ensembles des applications affines de $\mathcal{E}$ dans lui-même est noté $\mathrm{Aff}(E)$.

(vi) On note $\mathrm{GA}(\mathcal{E}) = \{f \in \mathrm{Aff}(\mathcal{E}) \mid f \text{ est bijective } \}$.

Lemme 7.1.2 Soit $f \in \mathrm{Aff}(\mathcal{E}, \mathcal{F})$ et soient $f : E \to F$ et $O \in E$ tels que $f(A) = f(O) + \vec{f}(\overrightarrow{OA})$.

(i) Alors $\vec{f}$ est unique.

(ii) Pour tout $A \in \mathcal{E}$, on a $\vec{f}(\overrightarrow{OA}) = \overrightarrow{f(O)f(A)}$.

(iii) Pour tout $A, P \in \mathcal{E}$, on a $\vec{f}(\overrightarrow{PA}) = \overrightarrow{f(P)f(A)}$.

(iv) Pour tout $A, P \in \mathcal{E}$, on a $f(A) = f(P) + \vec{f}(\overrightarrow{PA})$ et la définition ne dépend pas du choix de O. □

Preuve. 1. et 2. On commence par montrer que 2. est vrai. On a $f(A) = f(0) + \vec{f}(\overrightarrow{OA})$ ce qui donne par définition de $\overrightarrow{f(O)f(A)}$ l'égalité $\overrightarrow{f(O)f(A)} = \vec{f}(\overrightarrow{OA})$.

Soit maintenant $u \in E$ et soit $A = O + u$. On a $\overrightarrow{OA} = u$ et $\vec{f}(u) = \vec{f}(\overrightarrow{OA}) = \overrightarrow{f(O)f(A)}$. Ainsi $\vec{f}$ est complètement déterminée par f et est donc unique.

3. Soit $P \in \mathcal{E}$, on calcule $f(P) + \vec{f}(\overrightarrow{PA}) = f(O) + \vec{f}(\overrightarrow{OP}) + \vec{f}(\overrightarrow{PA}) = f(0) + \vec{f}(\overrightarrow{OP} + \overrightarrow{PA}) = f(O) + \vec{f}(\overrightarrow{OA}) = f(A)$ ce qui montre le résultat. ■

Lemme 7.1.3 Si f et g sont affine, la composée $g \circ f$ est encore affine et $\overrightarrow{g \circ f} = \vec{g} \circ \vec{f}$. □

Preuve. Soient $f : \mathcal{E} \to \mathcal{F}$ et $g : \mathcal{F} \to \mathcal{G}$ des applications affines. On a donc des applications linéaires $\vec{f}$ et $\vec{g}$ tells que $f(A) = f(O)+\vec{f}(\overrightarrow{OA})$ et $g(B) = g(O')+\vec{g}(\overrightarrow{O'B})$. On obtient (avec $O' = f(O)$) :

$$g(f(A)) = g(f(O)) + \vec{g}(\overrightarrow{f(O)f(A)}) = g(f(O)) + \vec{g}(\vec{f}(\overrightarrow{OA})).$$

En posant $\overrightarrow{g \circ f} = \vec{g} \circ \vec{f}$ on obtient $g(f(A)) = g(f(O)) + \overrightarrow{g \circ f}(\overrightarrow{OA})$ qui est donc affine. ■

Lemme 7.1.4 Si $f : \mathcal{E} \to \mathcal{F}$ est affine bijective, alors $\vec{f}$ est bijective. □

Preuve. Soit $u \in E$ tel que $\vec{f}(u) = 0$. On fixe $O \in \mathcal{E}$. On a $f(A) = f(O) + \vec{f}(\overrightarrow{OA})$. On fixe $A \in \mathcal{E}$ tel que $u = \overrightarrow{OA}$. On a alors $f(A) = f(O) + \vec{f}(u) = f(O)$ et comme f est injective, on a $A = O$ et $u = \overrightarrow{OA} = 0$. ■

Lemme 7.1.5 Si $f : \mathcal{E} \to \mathcal{F}$ est affine bijective, son inverse est affine et $\overrightarrow{f^{-1}} = \vec{f}^{-1}$.□

Preuve. Soit $f : \mathcal{E} \to \mathcal{F}$ une application affine bijective et soit $g : \mathcal{F} \to \mathcal{E}$ son inverse. Fixons $O \in \mathcal{E}$ et soit $\Omega = f(O)$. Pour $B \in \mathcal{F}$, posons $A = g(B)$. On a $g(\Omega) = O$ et $f(A) = B$. On a $\vec{f}(\overrightarrow{OA}) = \overrightarrow{f(O)f(A)} = \overrightarrow{\Omega B}$ donc $\vec{f}^{-1}(\overrightarrow{\Omega B}) = \overrightarrow{OA}$. Ainsi, on a

$$g(B) = A = O + \overrightarrow{OA} = \Omega + \vec{f}^{-1}(\overrightarrow{\Omega B}).$$

Ce qui prouve que g est affine et que $\vec{g} = \vec{f}^{-1}$. ■

Corollaire 7.1.6 L'ensemble $\mathrm{GA}(\mathcal{E})$ est un groupe pour la composition.

Corollaire 7.1.7 L'application $\Phi : \mathrm{GA}(E) \to \mathrm{GL}(E)$ définie par $\Phi(f) = \vec{f}$ est un morphisme de groupes surjectif.

Preuve. Nous avons déjà vu aux lemmes précécent que Φ est un morphisme de groupes. Montrons qu'il est surjectif. Pour $\varphi \in \mathrm{GL}(E)$, fixons $O \in \mathcal{E}$ et posons $f(A) = O + \varphi(\overrightarrow{OA})$. Alors $f(O) = O$ et $\vec{f} = \varphi$. ■

7.2. Lien avec le barycentre

Définition 7.2.1 Soient $(A_1, \cdots, A_r)$ des éléments de $\mathcal{E}$ et soient $(\lambda_1, \cdots, \lambda_r)$ des réels tels que $\lambda_1 + \cdots + \lambda_r = 1$. Le **barycentre** des points pondérés $(A_1, \lambda_1), \cdots, (A_r, \lambda_r)$ est l'unique point $G \in \mathcal{E}$ tel qu'il existe un point $O \in \mathcal{E}$ avec

$$\overrightarrow{OG} = \sum_{i=1}^{r} \lambda_i \overrightarrow{OA_i}.$$

Lemme 7.2.2 La définition ci-dessus est indépendante du choix du point O : pour tout $P \in \mathcal{E}$, on a

$$\overrightarrow{OG} = \sum_{i=1}^{r} \lambda_i \overrightarrow{OA_i} \Leftrightarrow \overrightarrow{PG} = \sum_{i=1}^{r} \lambda_i \overrightarrow{PA_i}.$$

Preuve. On calcule

$$\begin{aligned} \overrightarrow{OG} - \textstyle\sum_{i=1}^{r} \lambda_i \overrightarrow{OA_i} &= \overrightarrow{OP} + \overrightarrow{PG} - \textstyle\sum_{i=1}^{r} \lambda_i (\overrightarrow{OP} + \overrightarrow{PA_i}) \\ &= \overrightarrow{OP} - (\textstyle\sum_{i=1}^{r} \lambda_i) \overrightarrow{OP} + \textstyle\sum_{i=1}^{r} \lambda_i \overrightarrow{PA_i}) \\ &= \overrightarrow{PA_i} - \textstyle\sum_{i=1}^{r} \lambda_i \overrightarrow{PA_i}. \end{aligned}$$

Ces deux quantités sont donc nulles en même temps ce qui montre le résultat. ∎

Proposition 7.2.3 Une application $f : \mathcal{E} \to \mathcal{F}$ est affine si et seulement si elle preserve les barycentres.

Preuve. Exercice. ∎

7.3. Quelques sous-groupes de $\mathrm{GA}(\mathcal{E})$

Dans cette section, on définit quelques sous-groupes (plus ou moins) bien connus de $\mathrm{GA}(\mathcal{E})$. Rappelons les faits suivants.

Lemme 7.3.1 Soit E un espace vectoriel.

(i) Le centre $Z(\mathrm{GL}(E))$ du groupe $\mathrm{GL}(E)$ est donné par

$$Z(\mathrm{GL}(E)) = \{\lambda \mathrm{Id}_E \mid \lambda \in \mathbb{R}^\times\}.$$

(ii) On a $Z(\mathrm{GL}(E)) \triangleleft \mathrm{GL}(E)$.

(iii) Le sous-groupe $\{\mathrm{Id}_E, -\mathrm{Id}_E\}$ de $\mathrm{GL}(E)$ est distingué.

(iv) Le sous-groupe $\{\varphi \in \mathrm{GL}(E) \mid \det(\varphi) > 0\} = \det^{-1}(\mathbb{R}_+^\times)$ est distingué dans $\mathrm{GL}(E)$. □

Preuve. 1. Soit $\varphi = \lambda \mathrm{Id}_E$ avec $\lambda \in \mathbb{R}^\times$. Montrons que $\varphi \in Z(\mathrm{GL}(E))$. Soit $\psi / in\, \mathrm{GL}(E)$. On a $\varphi(\psi(u)) = \lambda\psi(u) = \psi(\lambda u) = \psi(\varphi(u))$.

Réciproquement, soit $\varphi \in \mathrm{GL}(E)$, montrons qu'il existe $\lambda \in \mathbb{R}^\times$ tel que $\varphi = \lambda \mathrm{Id}_E$. Remarquons qu'il suffit de montrer qu'il existe $\lambda \in R$ car si un tel λ existe, il doit etre non nul car φ est inversible. Soit $u \in E \setminus \{0\}$ et notons $U = \mathbb{R}u \subset E$ le sous-espace engendré par u. Soit H un supplémentaire de U dans E de telle sorte que $E = U \oplus H$. Soit s la symétrie par rapport à H selon U. L'application s est définie de la manière suivante. Pour $v \in E$, on décompose v selon la somme $U \oplus F$ en $v = v_1 + v_2$ avec

$v_1 \in U$ et $v_2 \in H$. On pose alors $s(v) = -v_1 + v_2$. En particulier U est le sous-espace propre de s associé à la valeur propre -1. On calcule

$$s(\varphi(u)) = \varphi(s(u)) = \varphi(-u) = -\varphi(u).$$

Ainsi $\varphi(u)$ est un vecteur propre de s pour la valeur propre -1 donc $\varphi(u) \in U$. Ainsi il existe un scalaire λ_u (dépendant de u a priori) tel que $\varphi(u) = \lambda_u u$. Ceci est vrai pour tout vecteur $u \in E$. Il nous reste à montrer que λ_u est indépendant de u. Soit $v \in E$ un autre vecteur. Pour $v = 0$, on a $\varphi(v) = 0 = \lambda_v v = \lambda_u v$. Supposons donc v non nul. Si v est colinéaire à u, alors il existe un réel non nul μ tel que $v = \mu u$ et on a $\lambda_v v = \varphi(v) = \varphi(\mu u) = \mu\varphi(u) = \mu\lambda_u u$. On a donc $\mu\lambda_u u = \lambda_u v$ et comme v est non nul, on obtient $\lambda_v = \lambda_u$. Supposons maintenant que u et v forment une famille libre. On calcule alors $\varphi(u+v)$. On a

$$\lambda_{u+v}(u+v) = \varphi(u+v) = \varphi(u) + \varphi(v) = \lambda_u u + \lambda_v v.$$

Comme (u, v) est libre, on obtient $\lambda_{u+v} = \lambda_u$ et $\lambda_{u+v} = \lambda_v$ et on a bien $\lambda_u = \lambda_v$.

2. Découle de 1. car le centre est un sous-groupe distingué.

3. Soit $f = \pm\mathrm{Id}_E$ et $g \in \mathrm{GL}(E)$. Comme f est dans le centre de $\mathrm{GL}(E)$, on a $g \circ f \circ g^{-1} = g \circ g^{-1} \circ f = f$ et donc $\{\pm\mathrm{Id}_E\}$ est un sous-groupe distingué de $\mathrm{GL}(E)$.

4. Comme le groupe multiplicatif $(\mathbb{R}^\times, \times)$ est commutatif, tous ses sous-groupes sont distingués. En particulier, le sous-groupe $R_+^\times \subset \mathbb{R}^\times$ est distingué : $\mathbb{R}_+^\times \triangleleft \mathbb{R}^\times$. Son image réciproque par le morphisme de groupes $\det : \mathrm{GL}(E) \to \mathbb{R}^\times$ est donc aussi un sous-groupe distingué : $\{\varphi \in \mathrm{GL}(E) \mid \det(\varphi) > 0\} = \det^{-1}(\mathbb{R}_+^\times) \triangleleft \mathrm{GL}(E)$. ∎

Définition 7.3.2 Soit E un espace vectoriel et $\mathcal{E}$ l'espace affine associé. Soit $\Phi : \mathrm{GA}(\mathcal{E}) \to \mathrm{GL}(E)$ le morphisme de groupes associé.

(i) Le **groupe des translations** $\mathrm{T}(\mathcal{E})$ est le sous-groupe $\mathrm{T}(\mathcal{E}) = \mathrm{Ker}\Phi$.

(ii) Le **groupe des homothéties translations** $\mathrm{HT}(\mathcal{E})$ est le sous-groupe $\mathrm{HT}(\mathcal{E}) = \Phi^{-1}(Z(\mathrm{GL}(E)) = \{f \in \mathrm{GA}(\mathcal{E}) \mid \exists \lambda \in \mathbb{R},\ \vec{f} = \lambda\mathrm{Id}_E\}$.

(iii) Le **groupe des translations et symétries centrales** $\mathrm{TSC}(\mathcal{E})$ est le sous-groupe $\mathrm{TSC}(\mathcal{E}) = \Phi^{-1}(\{\pm\mathrm{Id}_E\} = \{f \in \mathrm{GA}(\mathcal{E}) \mid \vec{f} = \pm\mathrm{Id}_E\}$.

(iv) Le **groupe des transformations affines positives** $\mathrm{GA}^+(\mathcal{E})$ est le sous-groupe $\mathrm{GA}^+(\mathcal{E})(\mathcal{E}) = \Phi^{-1}(\det^{-1}(\mathbb{R}_+^\times)) = \{f \in \mathrm{GA}(\mathcal{E}) \mid \det(\vec{f}) > 0\}$.

(v) Si $X \subset \mathcal{E}$ le groupe $\mathrm{GA}_X(\mathcal{E})$, le **stabilisateur de** X est défini par $\mathrm{GA}_X(\mathcal{E}) = \{f \in \mathrm{GA}(\mathcal{E}) \mid f(X) = X\}$.

Proposition 7.3.3 Soit E un espace vectoriel et $\mathcal{E}$ l'espace affine associé. Soit $\Phi : \mathrm{GA}(\mathcal{E}) \to \mathrm{GL}(E)$ le morphisme de groupes associé.

(i) On a $\mathrm{T}(\mathcal{E}) \triangleleft \mathrm{GA}(\mathcal{E})$.

(ii) On a $\mathrm{HT}(\mathcal{E}) \triangleleft \mathrm{GA}(\mathcal{E})$.

(iii) On a $\mathrm{TSC}(\mathcal{E}) \triangleleft \mathrm{GA}(\mathcal{E})$.

(iv) On a $\mathrm{GA}^+(\mathcal{E}) \triangleleft \mathrm{GA}(\mathcal{E})$.

Preuve. Dans tous les cas, le sous-groupe est de la forme $\Phi^{-1}(H)$ avec $H \triangleleft \mathrm{GL}(E)$ (voir le Lemme 7.3.1). ∎

Remarque 7.3.4 Dans le cas du plan $\mathcal{E}\mathbb{R}^2$, le groupe $\mathrm{GA}^+(\mathcal{E})$ des transformations affine positive est le groupe des transformations affines qui préservent l'orientation du plan.

Exemple 7.3.5 Soit $X = \{A, B, C\}$ les sommets d'un triangle dans le plan $\mathcal{E} = \mathbb{R}^2$. Alors le groupe $\mathrm{GA}_X(\mathcal{E})$ est isomorphe au groupe $\mathfrak{S}_3$ qui opère sur les sommets du triangle par permutation.

7.4. Isométries

On suppose maintenant que l'espace vectoriel E est muni d'un produit scalaire $(\ ,\ ) : E \times E \to \mathbb{R}$ c'est-à-dire d'une forme bilinéaire symétrique définie positive. On notera $\|\cdot\|$ la norme associée.

Exemple 7.4.1 Si E est de dimension n, alors tout produit scalaire sur E est équivalent au produit scalaire usuel :

$$(x, y) = \sum_{i=1}^{n} x_i y_i$$

où $x = (x_1, \cdots, x_n)$ et $y = (y_1, \cdots, y_n)$ sont des vecteurs de $\mathbb{R}^n$.

Définition 7.4.2 Soit E un espace vectoriel muni d'un produit scalaire $(\ ,\ )$ et soit $\mathcal{E}$ l'espace affine associé.

(i) Une application linéaire $\varphi : E \to E$ est appelée **isométrie vectorielle** si $(\varphi(u), \varphi(v)) = (u, v)$ pour tout $(u, v) \in E^2$. L'ensemble des isométrie vectorielles est noté $\mathrm{Isom}(E)$.

(ii) Une transformation affine $f : \mathcal{E} \to \mathcal{E}$ est appelée **isométrie affine** si $\vec{f}$ est une isométrie vectorielle. L'ensemble des isométrie affines est noté $\mathrm{Isom}(\mathcal{E})$

(iii) Une isométrie vectorielle φ est dite **positive** si $\det(\varphi) > 0$. L'ensemble des isométrie vectorielles positives est noté $\mathrm{Isom}^+(E)$.

(iv) Une isométrie affine f est dite **positive** si $\det(\vec{f}) > 0$. L'ensemble des isométrie affines positives est noté $\mathrm{Isom}^+(\mathcal{E})$.

Proposition 7.4.3 Soit $\varphi : E \to E$ une isométrie, alors $\varphi \in \mathrm{GL}(E)$.

Preuve. Il suffit de montrer que φ est injective. Soit $u \in \mathrm{Ker}(\varphi)$. ALors, pour tout $v \in E$, on a $(u, v) = (\varphi(u), \varphi(v) = (0, \varphi(v)) = 0$. Donc u est orthogonal à tout l'espace E et comme on a un produit scalaire, on obtient $u = 0$. ∎

On rappelle la définition de l'adjoint d'un endomrphisme.

Définition 7.4.4 Soit $\varphi = E \to E$ un endomorphisme. L'adjoint de E (par rapport au produit scalaire $(\ ,\ )$ est l'unique endomorphisme $\varphi^\dagger : E \to E$ tel que pour tout $(u, v) \in E^2$, on ait :

$$(\varphi(u), v) = (u, \varphi^\dagger(v)).$$

On rappelle les résultats (bien connus) suivants.

Proposition 7.4.5 Soit $\varphi \in \mathrm{GL}(E)$. Les propriétés suivantes sont équivalentes

(i) φ est une isométrie ;

(ii) $\|\varphi(u)\| = \|u\|$ pour tout $u \in E$;

(iii) $\varphi^{-1} = \varphi^\dagger$;

(iv) l'image, par φ, d'une base orthonormée de E est une base orthonormée de E ;

(v) la matrice de φ dans une base orthnormée est orthogonale.

Remarque 7.4.6 L'ensemble $\mathrm{Isom}(E)$ des isométries est parfois noté $\mathrm{O}(E)$. L'ensemble $\mathrm{Isom}^+(E)$ des isométries positives est parfois noté $\mathrm{SO}(E)$.

Quelques rappels supplémentaires.

Proposition 7.4.7 Soit E un espace vectoriel muni d'un produit scalaire $(\ ,\ )$.

(i) La composée de deux isométries est une isométrie.

(ii) L'inverse d'une isométrie est un e isométrie.

(iii) L'ensemble $\mathrm{Isom}(E)$ est un sous-groupe de $\mathrm{GL}(E)$.

(iv) L'ensemble $\mathrm{Isom}^+(E)$ est un sous-groupe de $\mathrm{Isom}(E)$.

(v) Pour $\varphi \in \mathrm{Isom}(E)$, on a $\det(\varphi) = \pm 1$.

(vi) On a $\mathrm{Isom}^+(E) = \{\varphi \in \mathrm{Isom}(E) \mid \det(\varphi) = 1\}$.

Remarque 7.4.8 Une isométrie affine est une application qui préserve les distances.

7.5. Isométries en dimensions 2

Les éléments de $\mathrm{Isom}^+(\mathcal{E})$ sont parfois aussi appelés **déplacements**, les éléments de $\mathrm{Isom}(\mathcal{E}) \setminus \mathrm{Isom}^+(\mathcal{E})$ sont parfois aussi appelés **anti-déplacements**. Pour $f : \mathcal{E} \to \mathcal{E}$, on note

$$\mathrm{Fix}(f) = \{A \in \mathcal{E} \mid f(A) = A\}$$

l'ensemble des points fixes de f.

Proposition 7.5.1 (Classification des isométries planes) Soit E un espace vectoriel de dimension 2 et $\mathcal{E}$ le plan affine associé. Soit $f \in \mathrm{Isom}(\mathcal{E})$.

(i) Si $f \in \mathrm{Isom}^+(\mathcal{E})$ est un déplacement, alors on a l'un des cas suivants :
   a) $f = \mathrm{Id}_{\mathcal{E}}$ et $\mathrm{Fix}(f) = \mathcal{E}$;
   b) f est une rotation de centre O et $\mathrm{Fix}(f) = \{O\}$;
   c) f est une translation et $\mathrm{Fix}(f) = \emptyset$.

(ii) Si $f \in \mathrm{Isom}(\mathcal{E}) \setminus \mathrm{Isom}^+(\mathcal{E})$ est un anti-déplacement, alors on a l'un des cas suivants :
   a) f est une symétrie orthogonale par rapport à une droite $\mathcal{D}$ et $\mathrm{Fix}(f) = \mathcal{D}$;
   b) f est une symétrie glissée (composée d'une symétrie et d'une translation de vecteur parallèle à l'axe de symétrie) et $\mathrm{Fix}(\mathcal{F}) = \emptyset$.

Preuve. On commence par le cas des isométries vectorielles. Soit donc $\varphi \in \mathrm{Isom}(E)$. En fixant une base orthonormée, la matrice M de φ est orthogonale et donc de la forme

$$M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

avec $a^2 + b^2 = c^2 + d^2 = a^2 + c^2 = b^2 + d^2 = 1$ et $ab + cd = 0 = ac + bd$. Les premières égalités imposent qu'il existe un $\theta \in \mathbb{R}$ tel que $a = \cos\theta$ et $c = \sin\theta$. On a alors $b = \varepsilon \sin\theta$ et $d = \eta \cos\theta$ avec $\varepsilon = \pm 1$ et $\eta = \pm 1$. Les secondes équations imposent $(\varepsilon + \eta)\sin\theta\cos\theta = 0 = (1 + \varepsilon\eta)\sin\theta\cos\theta$. On a alors deux cas : $\sin\theta\cos\theta = 0$ dans ce cas on a $\theta = k\frac{\pi}{2}$ avec $k \in \mathbb{Z}$ et donc M est l'une des matrices suivantes

Déplacements :

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

identité rotation d'angle π rotation d'angle $-\frac{\pi}{2}$ rotation d'angle $\frac{\pi}{2}$

Antidéplacements :

$$\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \quad \begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$

symétrie selon $x = 0$ symétrie selon $y = 0$ symétrie selon $y = x$ symétrie selon $y = -x$

Dans le second cas, on a $\sin\theta\cos\theta \neq 0$ et alors $\varepsilon = -\eta$. On a donc deux types de matrices

déplacements	antidéplacements
$\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$	$\begin{pmatrix} \cos\theta & \sin\theta \\ \sin\theta & -\cos\theta \end{pmatrix}$
rotation d'angle θ	symétrie

la droite selon laquelle la symétrie de la seconde matrice est obtenue est la droite formant un angle de $\theta/2$ avec l'axe $x = 0$.

Le cas des isométries affines est obtenu par composition d'une isométrie vectorielle avec une translation. Dans le cas des isométries positives (ou déplacements), il faut vérifier que la composée d'une rotation et d'une translation est encore une rotation (exercice). Dans le cas des isométries négatives ou anti-déplacements, si le vecteur u de la translation n'est pas colinéaire à la direction de la droite $\mathcal{D}$ de symétrie, la composée $t_u \circ s_{\mathcal{D}}$ est encore une symétrie selon la droite $\mathcal{D} + \frac{1}{2}u$. Si u est colinéaire à la direction de la droite $\mathcal{D}$, la composée $t_u \circ s_{\mathcal{D}}$ est une symétrie glissée qui est sans point fixe. ∎

Théorème 7.5.2 Soit E un espace vectoriel de dimension 2 muni d'un produit scalaire. Les sous-groupes finis de $\mathrm{Isom}(E)$ sont isomorphes à $\mathbb{Z}/n\mathbb{Z}$ et D_{2n} pour tout $n \geq 1$. □

Preuve. On commence par les sous-groupes de $\mathrm{Isom}^+(E)$. On a un morphisme de groupes surjectif $\mathbb{R} \to \mathrm{Isom}^+(E)$ définie par $\theta \mapsto r_\theta$ où r_θ est la rotation d'angle θ. Le noyau de ce morphisme est $(2\pi)\mathbb{Z}$. On vérifie (exercice) que les sous-groupes H de $\mathbb{R}$ contenant $(2\pi)\mathbb{Z}$ et tels que $H/(2\pi)\mathbb{Z}$ est fini sont de la forme $H = \frac{2\pi}{n}\mathbb{Z}$ et le groupe est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

Si G est un sous-groupe fini de $\mathrm{Isom}(E)$, alors $H \cap \mathrm{Isom}^+(E)$ est un sous-groupe fini de $\mathrm{Isom}^+(E)$ et c'est le noyau de $\det : G \to \{\pm 1\}$. On a donc $H = G$ ou H est d'indice 2 dans G. Dans tous les cas, $H = \langle\tau\rangle$ où τ est une rotation d'ordre n. Dans le premier cas, on a fini. Dans le second cas, si $\sigma \in G$ est une reflexion, alors on pose $K = \langle\sigma\rangle$. On a $G = HK = \langle\sigma, \tau\rangle$ et $G = D_{2n}$. ∎

Corollaire 7.5.3 Soit E un espace vectoriel de dimension 2 muni d'un produit scalaire et soit $\mathcal{E}$ l'espace affine associé. Les sous-groupes finis de $\mathrm{Isom}(\mathcal{E})$ sont isomorphes à $\mathbb{Z}/n\mathbb{Z}$ et D_{2n} pour tout $n \geq 1$.

Preuve. Il suffit de vérifier qu'un tel groupe admet toujours un point fixe. Alors quitte à choisir ce point fixe pour origine de E, ce groupe ce groupe sera un sous-groupe de $\mathrm{Isom}(E)$.

Pour trouver un point fixe, choisissons $O, A \in \mathcal{E}$ deux points quelconques. On définit le point $\Omega \in \mathcal{E}$ par

$$\overrightarrow{O\Omega} = \frac{1}{|G|}\sum_{g\in G} \overrightarrow{Og(A)}.$$

C'est le centre de gravité de l'orbite de A sous l'action de G. Pour $h \in G$, on a

$$\vec{h}(\overrightarrow{O\Omega}) = \frac{1}{|G|}\sum_{g\in G}\vec{h}(\overrightarrow{Og(A)}) = \frac{1}{|G|}\sum_{g\in G}\overrightarrow{h(O)hg(A)}.$$

Comme le centre de gravité ne dépend pas du point de base choisi, on a

$$\overrightarrow{h(O)\Omega} = \frac{1}{|G|}\sum_{g\in G}\overrightarrow{h(O)g(A)} = \frac{1}{|G|}\sum_{g\in G}\overrightarrow{h(O)hg(A)}) = \vec{h}(\overrightarrow{O\Omega}) = \overrightarrow{h(O)h(\Omega)}.$$

On obtient $\Omega = h(\Omega)$ pour tout $h \in G$. ∎

7.6. Isométries en dimensions 3

Définition 7.6.1 Soit E un espace vectoriel et soit $E = F \oplus G$ une décomposition de E en somme directe.

(i) On appelle **reflexion de E par rapport à F parallèlement à G** l'application $s : E \to E$ définie par $s(x) = s(f + g) = f - g$ où $x = f + g$ avec $f \in F$ et $g \in G$ est la décomposition de x selon F et G.

(ii) Lorsque E est muni d'un produit scalaire $(\ ,\ )$, si $F \subset E$ est un sous-espace vectoriel, on a la décomposition $E = F \oplus F^\perp$ avec $F^\perp = \{x \in E \mid (x, y) = 0 \text{ pour tout } y \in F\}$. La symétrie par rapport à F parallèlement à $F^\perp$ est appelée **symétrie orthogonale par rapport à F**

(iii) Si H est un hyperplan (c'est-à-dire un sous-espace vectoriel de codimension 1). La symétrie orthogonale par rapport à H s'appelle **reflexion orthogonale par rapport à H**

Remarque 7.6.2 Soit E un espace vectoriel muni d'un produit scalaire et $F \subset E$ un sous-espace vectoriel. Si s est la symétrie orthogonale par rapport à F, on a $\det(s) = (-1)^{\dim E - \dim F} = (-1)^{\operatorname{codim}_E(F)}$. En particulier, si s est une reflexion, on a $\det(s) = -1$.

Théorème 7.6.3 (Théorème de Cartan-Dieudonné) Soit E un espace vectoriel muni d'un produit scalaire (ou plus généralement d'une forme bilinéaire symétrique non dégénérée $B(\ ,\ )$). Tout élément de $\mathrm{Isom}(E)$ est produit d'au plus $\dim(E)$ réflexions. □

Preuve. On procède par récurrence sur $\dim E$. Si $\dim E = 1$, c'est clair : les éléments de $\mathrm{Isom}(E)$ sont $\pm\mathrm{Id}_E$ et $-\mathrm{Id}_E$ est une reflexion.

Supposons que le résultat est vrai en dimension strictement inférieure à $\dim E$. Soit $\varphi \in \mathrm{Isom}(E)$. On commence par sopposer qu'il existe un vecteur $x \in E$ tel que $B(x, x) \neq 0$ et $\varphi(x) = x$. Posons $H = \langle x\rangle^\perp$. C'est un hyperplan de E (car B est

non dégénérée) et on a $E = \langle x \rangle \oplus H$ (car $B(x,x) \neq 0$). De plus, si $y \in H$, on a $B(x, \varphi(y)) = B(\varphi(x), \varphi(y)) = B(x,y) = 0$ donc $\varphi(y) \in H$ et $\varphi(H) = H$. Si $\mathcal{B}_H$ est une base de H et $\mathcal{B} = \{x\} \cup \mathcal{B}_H$ qui est une base de E, on a

$$\mathrm{Mat}_{\mathcal{B}}^{\mathcal{B}}(\varphi) = \begin{pmatrix} 1 & 0 \\ 0 & \mathrm{Mat}_{\mathcal{B}_H}^{\mathcal{B}_H}(\varphi|_H) \end{pmatrix}.$$

Par hypothèse de récurrence $\varphi|_H$ est produit d'au plus $\dim(H) = \dim(E) - 1$ reflexion donc la même chose est vraie pour φ.

Montrons maintenant que quitte /'a composer par une reflexion, on peut se ramener au cas précédent ce qui terminera la preuve. On peut donc supposer que pour tout $x \in E$ tel que $B(x,x) \neq 0$, on a $\varphi(x) \neq x$. Notons que si $y = \varphi(x)$, on a aussi $B(y,y) = B(\varphi(x), \varphi(x)) = B(x,x) \neq 0$. On calcule

$$B(x-y, x-y) + B(x+y, x+y) = 2B(x,x) + 2B(y,y) = 4B(x,x) \neq 0.$$

On a donc $B(x-y, x-y) \neq 0$ ou $B(x+y, x+y) \neq 0$. On peut supposer $B(x-y, x-y) \neq 0$ (le second cas se traite de la même manière). On pose $H = \S - \dagger^{\perp}$ qui est un hyperplan et on note s la reflexion par rapport à H. On a $B(x-y, x+y) = B(x,x) - B(y,x) + B(x,y) - B(y,y) = B(x,x) - B(y,y) = 0$ donc $x + y \in H$. On pose $\psi = s \circ \varphi$. On a

$$\psi(x) = s(\varphi(x)) = s(y) = s\left(\frac{y-x}{2} + \frac{x+y}{2}\right) = \frac{x-y}{2} + \frac{x+y}{2} = x.$$

Ainsi $\psi(x) = x$ et ψ est produit d'au plus $\dim(E) - 1$ reflexion et $\varphi = s \circ \psi$ est produit d'au plus $\dim(E)$ reflexions. ∎

Corollaire 7.6.4 Soit $\varphi \in \mathrm{SO}_3(\mathbb{R})$ avec $\varphi \neq \mathrm{Id}$. Alors $\mathrm{Fix}(\varphi) = \{x \in E \mid \varphi(x) = x\}$ l'ensemble des points fixes de φ est une droite (un espace vectoriel de dimension 1).

Preuve. Soit $\varphi \in \mathrm{SO}_3(\mathbb{R})$ une isométrie différente de l'identité. Alors φ est produit d'au plus trois reflexions. De plus comme $\det(\varphi) = 1$ et que les reflexion ont un pour déterminant -1, l'isométrie φ est produit d'un nombre pair de reflexions. On a donc $\varphi = s_{H_1} s_{H_2}$ où H_1 et H_2 sont des hyperplans (des plans de l'espace) et $H_1 \neq H_2$ (sinon $\varphi = \mathrm{Id}$). On voit aisément que la droite $H_1 \cap H_2$ est contenue dans $\mathrm{Fix}(\varphi)$ car elle est fixés par les deux reflexions. On remarque aussi que $\mathrm{Fix}(\varphi)$ est un sous-espace vectoriel. Si ce n'est pas la droite $H_1 \cap H_2$, c'est un plan H. Mais alors si $x \in H^{\perp}$ est un vecteur non nul, on a $\varphi(x) = \lambda x$ et comme φ est une isométrie, on a $\varphi(x) = \pm x$ donc φ est l'identité ou la reflexion orthogonale par rapport à H. C'est impossible. ∎

Proposition 7.6.5 (Classification des isométries de l'espace) Soit E un espace vectoriel de dimension 3 et $\mathcal{E}$ le plan affine associé. Soit $f \in \mathrm{Isom}(\mathcal{E})$.

(i) Si $f \in \mathrm{Isom}^+(\mathcal{E})$ est un déplacement, alors on a l'un des cas suivants :

a) $f = \mathrm{Id}_{\mathcal{E}}$ et $\mathrm{Fix}(f) = \mathcal{E}$;

b) f est une rotation autour d'une droite $\mathcal{D}$ et $\mathrm{Fix}(f) = \mathcal{D}$;

c) f est un vissage (composée d'une rotation autour d'une droite $\mathcal{D}$ et d'une translation de vecteur parallèle à la droite $\mathcal{D}$) et $\mathrm{Fix}(f) = \emptyset$.

d) f est une translation et $\mathrm{Fix}(f) = \emptyset$.

(ii) Si $f \in \mathrm{Isom}(\mathcal{E}) \setminus \mathrm{Isom}^+(\mathcal{E})$ est un anti-déplacement, alors on a l'un des cas suivants :

a) f est une reflexion orthogonale par rapport à un plan $\mathcal{P}$ et $\mathrm{Fix}(f) = \mathcal{P}$;

b) f est une reflexion-rotation (composée d'une reflexion par rapport à un plan $\mathcal{P}$ et d'une rotation par rapport à une droite $\mathcal{D}$ non contenue dans $\mathcal{P}$) et $\mathrm{Fix}(\mathcal{F}) = \mathcal{P} \cap \mathcal{D} = \{\text{point}\}$.

c) f est une reflexion-glissée (composée d'une reflexion par rapport à un plan $\mathcal{P}$ et d'une translation de vecteur parallèle au plan $\mathcal{P}$) et $\mathrm{Fix}(\mathcal{F}) = \emptyset$.

Preuve. Exercice. On pourra commencer par le cas des isométries vectorielles et d'utiliser le théorème de Cartan-Dieudonné. ∎

Théorème 7.6.6 Les sous-groupes finis de $\mathrm{SO}_3(\mathbb{R})$ sont isomorphes à $\mathbb{Z}/n\mathbb{Z}$, D_{2n} ou $\mathfrak{A}_4$, $\mathfrak{S}_4$ et $\mathfrak{A}_5$.

Les sous-groupes finis de $\mathrm{O}_3(\mathbb{R})$ sont isomorphes à $\mathbb{Z}/n\mathbb{Z}$, D_{2n} ou $\mathfrak{A}_4$, $\mathfrak{S}_4$ et $\mathfrak{A}_5$ ainsi qu'à $\mathfrak{S}_4$, $\mathfrak{S}_4 \times /Z/2\mathbb{Z}$ et $\mathfrak{A}_5 \times \mathbb{Z}/2\mathbb{Z}$. □

Pour obtenir les groupes $\mathfrak{A}_4$, $\mathfrak{S}_4$ et $\mathfrak{A}_5$ et les groupes $\mathfrak{S}_4$, $\mathfrak{S}_4 \times /Z/2\mathbb{Z}$ et $\mathfrak{A}_5 \times \mathbb{Z}/2\mathbb{Z}$, il faut regarder le groupe des isométries d'un des polyêdres réguliers appelés aussi solide de platon. Voici leur liste et quelques résultats les concernants :

	tétraèdre	cube	octaèdre	dodécaèdre	icosaèdre
sommets	4	8	6	20	12
arêtes	6	12	12	30	30
faces	4	6	8	12	20

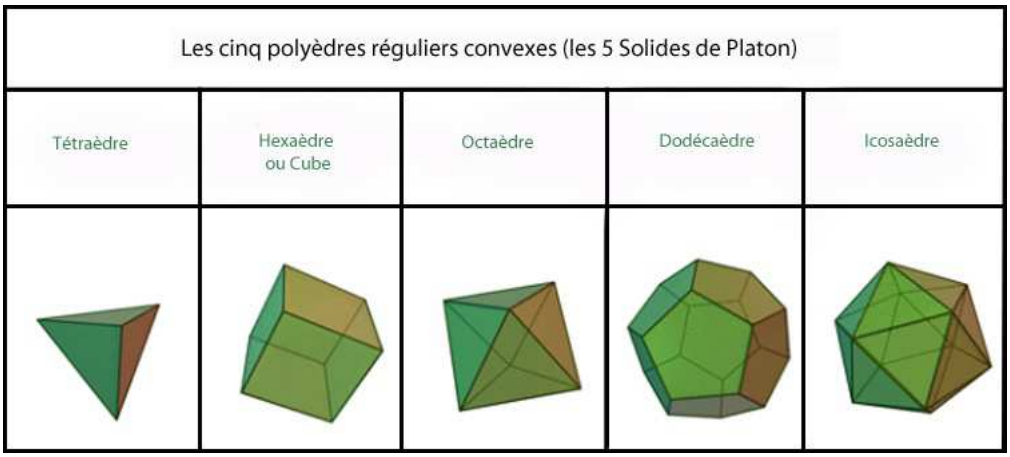
Remarque 7.6.7 Quelques propriétés remarquables :

(i) On voit que si s est le nombres de sommets, a le nombres d'arêtes et f le nombre de faces, alors dans tous les cas, le nombre $s + f - a = 2$ est constant égal à 2. Ceci traduit le fait que "topologiquement" tous les polyêdres sont équivalent à une sphère.

(ii) On voit aussi que les nombres s et f sont échangés entre cube et octaèdre et entre dodécaèdre et icosaèdre alors que ceux du tétrèdre sont inchangés. Ceci traduit la dualité entre polyèdres : si on prendre les milieux des faces d'un polyèdre régulier, on obtient son polyèdre dual. Ainsi le cube et l'octaèdre sont en dualité de même que dodécaèdre et icosaèdre alors que le tétrèdre est autodual (en dualité avec lui-même.

(iii) Cette dualité se traduit par exemple par le fait que les groupes des isométries sont les mêmes pour les polyèdres duaux. Ainsi les sous-groupes de $\mathrm{SO}_3(\mathbb{R})$ et $\mathrm{O}_3(\mathbb{R})$ qui préservent les polyèdres sont donnés dans le tableau suivant :

	tétraèdre	cube	octaèdre	dodécaèdre	icosaèdre
$\mathrm{SO}_3(\mathbb{R})$	$\mathfrak{A}_4$	$\mathfrak{S}_4$	$\mathfrak{S}_4$	$\mathfrak{A}_5$	$\mathfrak{A}_5$
$\mathrm{O}_3(\mathbb{R})$	$\mathfrak{S}_4$	$\mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$	$\mathfrak{S}_4 \times \mathbb{Z}/2\mathbb{Z}$	$\mathfrak{A}_5 \times \mathbb{Z}/2\mathbb{Z}$	$\mathfrak{A}_5 \times \mathbb{Z}/2\mathbb{Z}$



Deuxième partie .

Appendice : le déterminant

8. Algorithme de Gauß

8.1. Matrices élémentaires

Définition 8.1.1 Soit k un corps et n un entier.

(i) Soient $1 \leq p, q \leq n$ des entiers avec $p \neq q$ et soit $a \in \mathsf{k}$. On définit la matrice $T_{p,q}^{(n)}(a) = T_{p,q}(a) = (t_{i,j}) \in M_n(\mathsf{k})$ de la manière suivante :

$$t_{i,j} = \begin{cases} 1 & \text{si } i = j, \\ a & \text{si } (i,j) = (p,q), \\ 0 & \text{sinon.} \end{cases}$$

(ii) Soit $1 \leq p \leq n$ et soit $b \in \mathsf{k}^\times$. On définit la matrice $D_p^{(n)}(b) = D_p(b) = (d_{i,j}) \in M_n(\mathsf{k})$ de la manière suivante :

$$d_{i,j} = \begin{cases} 1 & \text{si } i = j \neq p, \\ a & \text{si } i = j = p, \\ 0 & \text{sinon.} \end{cases}$$

(iii) Soient $1 \leq p, q \leq n$. On définit la matrice $E_{p,q}^{(n)} = E_{p,q} = (e_{i,j}) \in M_n(\mathsf{k})$ de la manière suivante

$$e_{i,j} = \begin{cases} 1 & \text{si } q \neq i = j \neq j, \\ 1 & \text{si } (i,j) = (p,q), \\ 1 & \text{si } (i,j) = (q,p), \\ 0 & \text{sinon.} \end{cases}$$

Les matrices de la forme $T_{p,q}^{(n)}(a)$, $D_p^{(n)}(b)$ et $E_{p,q}^{(n)}$ sont appelées respectivement **matrices élémentaires de type I, II ou III**.

Remarque 8.1.2 On a les égalités $E_{p,q} = E_{q,p} = P_{\tau_{p,q}}$ et $E_{p,p} = I_n$.

Exemple 8.1.3 On a les égalités suivantes :

$$T_{2,3}^{(4)}(a) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & a & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad T_{3,2}^{(4)}(a) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & a & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$D_1^{(4)}(b) = \begin{pmatrix} b & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad D_3^{(4)}(b) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & b & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

$$E_{2,3}^{(4)} = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad E_{1,4}^{(4)}(a) = \begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$$

Lemme 8.1.4 Les matrices $T_{p,q}^{(n)}(a)$, $D_p^{(n)}(b)$ et $E_{p,q}^{(n)}$ sont inversibles. □

Preuve. En effet, on a

$$\begin{aligned} &T_{p,q}^{(n)}(a)T_{p,q}^{(n)}(-a) = I_n = T_{p,q}^{(n)}(-a)T_{p,q}^{(n)}(a) \\ &D_p^{(n)}(b)D_p^{(n)}(b^{-1}) = I_n = D_p^{(n)}(b^{-1})D_p^{(n)}(b) \\ &E_{p,q}^{(n)}E_{p,q}^{(n)} = I_n \end{aligned}$$

Lemme 8.1.5 (Opérations sur les lignes) Soient $A \in M_{m,n}(\mathsf{k})$, $a \in$ et $b \in \mathsf{k}^\times$.

(I) Le produit $T_{p,q}^{(n)}(a)A$ est obtenu à partir de A en ajoutant a fois la q-ième ligne de A à la p-ième ligne de A.

(II) Le produit $D_p^{(n)}(b)A$ est obtenu à partir de A en multipliant la ligne p par b.

(III) Le produit $E_{p,q}^{(n)}A$ est obtenu à partir de A en échangeant les lignes p et q. □

Preuve. Exercice. ■

Définition 8.1.6 Les trois opérations décrites au lemme précédent s'appelent **opérations élémentaires sur les lignes de types I, II et III**.

Lemme 8.1.7 On peut obtenir les opérations de type III sur les lignes par des opérations de types I et II. □

Preuve. En effet, on a $E_{p,q}^{(n)} = D_q^{(n)}(-1)T_{p,q}^{(n)}(1)T_{q,p}^{(n)}(-1)T_{p,q}^{(n)}(1)$. ■

Définition 8.1.8 De la même manière, on définit des opérations sur les colonnes. Les produits $AT_{p,q}^{(n)}(a)$, $AD_p^{(n)}(b)$ et $AE_{p,q}^{(n)}$ sont appelés **opérations élémentaires sur les colonnes de types I, II et III**.

8.2. Algorithme de Gauß

Définition 8.2.1 Une matrice $B = (b_{i,j}) \in M_{m,n}(\mathsf{k})$ est dite **échelonnée réduite** si $B = 0$ ou s'il existe un entier $r \in [1, \min(m,n)]$ et des entiers $1 \leq j_1 < j_2 < \cdots < j_r \leq n$, tels que

(i) pour $1 \leq k \leq r$, on a $b_{k,j} = 0$ si $j < j_k$ (les premières $j_k - 1$ entrées de la ligne k sont nulles) ;

(ii) pour $1 \leq k \leq r$, on a $b_{i,j_k} = \begin{cases} 1 & \text{si } i = k, \\ 0 & \text{sinon.} \end{cases}$ (la k-ième entrée de la colonne j_k est 1, toutes les autres sont nulles) ;

(iii) pour $r+1 \leq k \leq m$, on a $b_{k,j} = 0$ pour tout $1 \leq j \leq n$ (pour $r+1 \leq k \leq m$ la k-ième ligne est nulle).

On note $\text{Echelle}(B) = \{j_1, \cdots, j_r\}$. Pour $B = 0$, on a $\text{Zeilenform}(B) = \emptyset$.

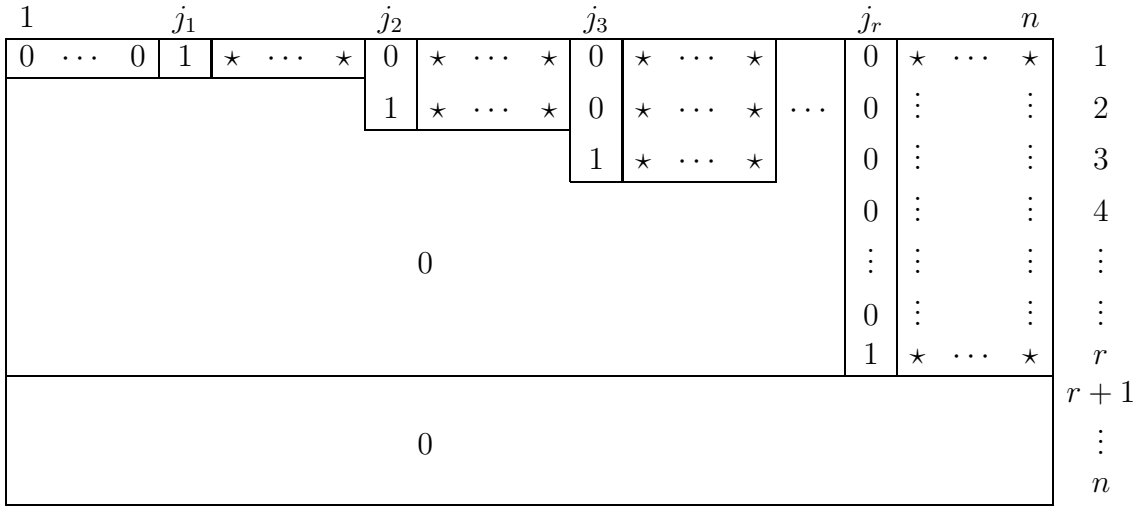
Exemple 8.2.2 Quelques exemples

(i) La matrice

$$B = \begin{pmatrix} 0 & 1 & b_{1,3} & b_{1,4} & 0 & b_{1,6} & 0 & 0 & b_{1,9} & b_{1,10} \\ 0 & 0 & 0 & 0 & 1 & b_{2,6} & 0 & 0 & b_{2,9} & b_{2,10} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & b_{3,9} & b_{3,10} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & b_{4,9} & b_{4,10} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

est échelonnée réduite avec $r = 4$ et $\text{Echelle}(B) = \{2, 5, 7, 8\}$.

(ii) En général, une matrice échelonnée réduite est de la forme suivante :



où les $\star$ représentent des éléments de k. Ici $\text{Echelle}(B) = \{j_1, \cdots, j_r\}$.

Théorème 8.2.3 (Algorithme de Gauß) Soit $A = (a_{i,j}) \in M_{m,n}(\mathsf{k})$ une matrice, alors il existe des matrices élémentires $T_1, \cdots T_t$ telles que $B = T_1 \cdots T_t A$ est échelonnée réduite. On dit alors que B est **est une forme échelonnée réduite de** A. □

Preuve. Si $A = 0$, on a fini. Supposons donc que l'on a $A \neq 0$. On pose $A^{(0)} = (a^{(0)}_{i,j}) = A$. Soit $j_1 = \min\{s \in [1,n] \mid \text{il existe } p \in [1,m] \text{ avec } a^{(0)}_{p,s} \neq 0\}$. L'entier j_1 est l'indice de la première colonne non nulle.

Soit $p = \min\{l \in [1,m] \mid a^{(0)}_{l,j_1} \neq 0\}$. L'entier p est l'indice de la ligne du premier coefficient non nul dans la colonne j_1. On pose

$$C^{(0)} = (c^{(0)}_{i,j}) = D_1((a^{(0)}_{p,j_1})^{-1}) E_{1,p} A^{(0)} \text{ et}$$

$$A^{(1)} = (a^{(1)}_{i,j}) = T_{m,1}(-c^{(0)}_{m,j_1}) \cdots T_{2,1}(-c^{(0)}_{2,j_1}) C^{(0)}.$$

On voit alors que la première ligne de $C^{(0)}$ est de la forme

$$(\underbrace{0 \cdots, 0}_{j_1 - 1 \text{ termes}}, 1, \star, \cdots, \star)$$

où $\star$ désigne un élément de k. On remarque également que les $j_1 - 1$ premières colonnes de $A^{(1)}$ sont nulles et que la j_1-ième colonne est de la forme

$$\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Par récurrence, on définit des matrices $A^{(k)} \in M_{m,n}(\mathsf{k})$ et des entiers $j_1 < \cdots < j_k$ de la manière suivante : supposons que l'on a déjà construit $A^{(k-1)} = (a^{(k-1)}_{i,j})$ et $j_1 < \cdots < j_{k-1}$. Soit

$$j_k = \min\{s \in [j_{k-1} + 1, n] \mid \text{il existe } p \in [k,m] \text{ tel que } a^{(k-1)}_{p,s} \neq 0\}.$$

L'entier j_k est donc l'indice de la première colonne plus grande que j_{k-1} ayant des termes non nuls sur les lignes d'indice plus grand que k. Si un tel entier n'existe pas, l'algorithme s'arrête.

Si j_k existe, on pose

$$p = \min\{l \in [k,m] \mid a^{(k-1)}_{l,j_k} \neq 0\}.$$

C'est l'indice de la première ligne plus grande que k ayant un terme non nul sur la colonne j_k. On pose

$$C^{(k-1)} = (c^{(k-1)}_{i,j}) = D_1((a^{(k-1)}_{p,j_k})^{-1}) E_{k,p} A^{(0)} \text{ et } A^{(k)} = (a^{(k)}_{i,j}) \text{ mitavec}$$

$$A^{(k)} = T_{m,k}(-c_{m,j_k}^{(k-1)}) \cdots T_{k+1,k}(-c_{k+1,j_k}^{(k-1)}) T_{k-1,k}(-c_{k-1,j_k}^{(k-1)}) \cdots T_{1,k}(-c_{1,j_k}^{(k-1)}) C^{(k-1)}.$$

On vérifie que la matrice de taille $(m \times j_k)$ obtenue à partir des j_k premières colonnes de $A^{(k)}$ est échelonnée réduite.

On vérifie ensuite aisément que l'algorithme s'arrête après au plus $\min(m, n)$ étapes et que la matrice obtenue est échelonnée réduite. ∎

Exemple 8.2.4 Si la matrice A est inversible, la matrice échelonnée réduite obtenue est la matrice identité.

9. Le déterminant

9.1. Fonction déterminant

Définition 9.1.1 Une application det : $M_n(\mathsf{k}) \to \mathsf{k}$ s'appelle **fonction déterminant** si elle vérifie les trois conditions suivantes :

(i) l'application det est linéaire en chacune des lignes de la matrice ;

2. si $\mathrm{Rg}(A) < n$, alors $\det(A) = 0$;

3. on a $\det(I_n) = 1$.

Remarque 9.1.2 Dire que det est linéaire en chacune de ses lignes signifie que les égalités suivantes sont vraies :

$$\det \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a_{i,1} & \cdots & a_{i,n} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix} = \det \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a'_{i,1} & \cdots & a'_{i,n} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix} + \det \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a''_{i,1} & \cdots & a''_{i,n} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix}$$

pour toute matrice $(a_{i,j}) \in M_n(\mathsf{k})$ telle que $a_{i,j} = a'_{i,j} + a''_{i,j}$ pour $i, j \in [1, n]$ et

$$\det \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ \lambda a_{i,1} & \cdots & \lambda a_{i,n} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix} = \lambda \det \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a_{i,1} & \cdots & a_{i,n} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix}.$$

Lemme 9.1.3 Soit det : $M_n(\mathsf{k}) \to \mathsf{k}$ une application déterminant et soit T une matrice élémentaire dans $M_n(\mathsf{k})$. Pour $A \in M_n(\mathsf{k})$, on a :

(i) $\det(TA) = \det(A)$, si T est de type I ;

(ii) $\det(TA) = \lambda \det(A)$, si $T = D_p(\lambda)$ est de type II (on peut avoir $\lambda = 0$) ;

(iii) $\det(TA) = -\det(A)$, si T est de type III. □

Preuve. On va utiliser la linéarité sur les lignes. On écrit la matrice A en ligne

$$A = \begin{pmatrix} Z_1 \\ \vdots \\ Z_n \end{pmatrix}.$$

1. Soit $i \neq j$ et $T = T_{i,j}^{(n)}(a)$ une matrice de type I. On a

$$\det(TA) = \det \begin{pmatrix} Z_1 \\ \vdots \\ Z_i + aZ_j \\ \vdots \\ Z_j \\ \vdots \\ Z_n \end{pmatrix} = \det \begin{pmatrix} Z_1 \\ \vdots \\ Z_i \\ \vdots \\ Z_j \\ \vdots \\ Z_n \end{pmatrix} + a \det \begin{pmatrix} Z_1 \\ \vdots \\ Z_j \\ \vdots \\ Z_j \\ \vdots \\ Z_n \end{pmatrix} = \det(A) + 0.$$

2. Soit $T = D_i(\lambda)$ une matrice de type II, on a

$$\det(TA) = \det \begin{pmatrix} Z_1 \\ \vdots \\ \lambda Z_i \\ \vdots \\ Z_n \end{pmatrix} = \lambda \det \begin{pmatrix} Z_1 \\ \vdots \\ Z_i \\ \vdots \\ Z_n \end{pmatrix} = \lambda \det(A).$$

3. Soient $i, j \in [1, n]$ et soit $T = E_{i,j}^{(n)}$ une matrice de type III. On a

$$\det(TA) = \det \begin{pmatrix} Z_1 \\ \vdots \\ Z_j \\ \vdots \\ Z_i \\ \vdots \\ Z_n \end{pmatrix}.$$

On commence par remarquer que l'on a la l'égalité

$$0 = \det \begin{pmatrix} Z_1 \\ \vdots \\ Z_i + Z_j \\ \vdots \\ Z_j + Z_i \\ \vdots \\ Z_n \end{pmatrix} = \det \begin{pmatrix} Z_1 \\ \vdots \\ Z_i \\ \vdots \\ Z_j \\ \vdots \\ Z_n \end{pmatrix} + \det \begin{pmatrix} Z_1 \\ \vdots \\ Z_i \\ \vdots \\ Z_i \\ \vdots \\ Z_n \end{pmatrix} + \det \begin{pmatrix} Z_1 \\ \vdots \\ Z_j \\ \vdots \\ Z_j \\ \vdots \\ Z_n \end{pmatrix} + \det \begin{pmatrix} Z_1 \\ \vdots \\ Z_j \\ \vdots \\ Z_i \\ \vdots \\ Z_n \end{pmatrix}.$$

On en déduit $0 = \det(A) + \det(TA)$. ∎

Corollaire 9.1.4 Si det est une fonction déterminant, si T est une matrice élémentaire et si $A \in M_n(K)$, on a

$$\det(AT) = \det(A)\det(T).$$

On a aussi

$$\det(T) = \begin{cases} 1 & \text{si } T \text{ est de type I,} \\ \lambda & \text{si } T = D_p(\lambda) \text{ est de type II,} \\ -1 & \text{si } T \text{ est de type III.} \end{cases}$$

Preuve. Par le lemme précédent pour $A = I_n$, on a $\det(T) = 1$ pour T de type I, $\det(T) = \lambda$ pour $T = D_p(\lambda)$ de type II et $\det(T) = -1$ pour T de type III. Le cas général vient du lemme précédent pour A général et de ces égalités. beliebig. ∎

Corollaire 9.1.5 Soit det une fonction déterminant, alors pour $A, B \in M_n(K)$ on a

$$\det(AB) = \det(A)\det(B).$$

Preuve. Si A ou B n'est pas inversible, la même chose est vraie de AB. Dans ce cas, on a $\det(AB) = 0 = \det(A)\det(B)$. Supposons donc que A et B sont inversibles. Il existe alors des matrices élémentaires $T_1, \cdots, T_t$ et $U_1, \cdots, U_u$ telles que $T_t \cdots T_1 A = I_n$ et $U_u \cdots U_1 B = I_n$. On obtient alors (rappelons que l'inverse T^{-1} d'une matrice élémentaire T est encore un matrice élémentaire) :

$$\begin{aligned} \det(AB) &= \det(T_1^{-1} \cdots T_t^{-1} U_1^{-1} \cdots U_u^{-1}) \\ &= \det(T_1^{-1}) \cdots \det(T_t^{-1}) \det(U_1^{-1}) \cdots \det(U_u^{-1}) \\ &= \det(T_1^{-1} \cdots T_t^{-1}) \det(U_1^{-1} \cdots U_u^{-1}) \\ &= \det(A)\det(B). \end{aligned}$$

Corollaire 9.1.6 Soit det une fonction déterminant et soit $A \in M_n(K)$ une matrice. On a l'équivalence (A est inversible $\Leftrightarrow \det(A) \neq 0$).

Preuve. Si A n'est pas inversible, on a $\det(A) = 0$. Si A est inversible, il existe des matrices élémentaires $T_1, \cdots, T_t$ telles que $A = T_1 \cdots T_t$. On obtient $\det(A) = \det(T_1) \cdots \det(T_t)$. Mais pour toute matrice élémentaire T, on a $\det(T) \neq 0$, donc on a $\det(A) \neq 0$. ∎

9.2. Existence

Théorème 9.2.1 (Formule de Laplace) Il existe une et une seule fonction déterminant $\det : M_n(\mathsf{k}) \to \mathsf{k}$. De plus, pour tout $j \in [1, n]$, on a

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{i,j} \det(A_{i,j}),$$

où $A_{i,j}$ est la sous-matrice de A obtenue en enlevant la i-ème ligne et la j-ième colonne (on a $A_{i,j} \in M_{n-1}(\mathsf{k})$). □

Preuve. On procède par récurrence sur n. Pour $n = 0$, on a $\det(A) = 1$ par définition. Pour $n = 1$, on a par linéarité $\det(A) = \det(a_{1,1}I_1) = a_{1,1} = (-1)^{1+1}a_{1,1}\det(A_{1,1})$.

Soit $n > 1$, on suppose le résultat vrai pour $n-1$. Soit $A \in M_n(\mathsf{k})$, on pose

$$\det(A) = \sum_{i=1}^{n}(-1)^{i+j}a_{i,j}\det(A_{i,j})$$

et on montre que det est une fonction déterminant.

On commence par la linéarité. Soient A, A' et A'' des matrices de la forme

$$A = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a_{k,1} & \cdots & a_{k,n} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix},\ A' = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a'_{k,1} & \cdots & a'_{k,n} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix} \text{ et } A'' = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ a''_{k,1} & \cdots & a''_{k,n} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix}$$

telles que $a_{k,j} = a'_{k,j} + a''_{k,j}$ pour tout $j \in [1, n]$. On a

$$a_{i,j}\det(A_{i,j}) = \begin{cases} (a'_{k,j} + a''_{k,j})\det(A_{k,j}) & \text{pour } i = k \\ a_{i,j}(\det((A')_{i,j}) + \det((A'')_{i,j})) & \text{pour } i \neq k. \end{cases}$$

Remarquons qu'on a $A_{k,j} = A'_{k,j} = A''_{k,j}$. On obtient donc

$$\begin{aligned} \det(A) &= \sum_{i=1}^{n}(-1)^{i+j}a_{i,j}\det(A_{i,j}) \\ &= a'_{k,j}\det(A'_{k,j}) + a''_{k,j}\det(A''_{k,j}) + \sum_{i\neq k}(-1)^{i+j}a_{i,j}(\det((A')_{i,j}) + \det((A'')_{i,j})) \\ &= \sum_{i=1}^{n}(-1)^{i+j}a'_{i,j}\det((A')_{i,j}) + \sum_{i=1}^{n}(-1)^{i+j}a''_{i,j}\det((A'')_{i,j}) = \det(A') + \det(A'') \end{aligned}$$

Soit maintenant

$$B = \begin{pmatrix} a_{1,1} & \cdots & a_{1,n} \\ \vdots & & \vdots \\ \lambda a_{k,1} & \cdots & \lambda a_{k,n} \\ \vdots & & \vdots \\ a_{n,1} & \cdots & a_{n,n} \end{pmatrix}.$$

On a

$$b_{i,j}\det(B_{i,j}) = \begin{cases} \lambda a_{k,j}\det(A_{k,j}) & \text{pour } i = k \\ a_{i,j}\lambda\det(A_{i,j}) & \text{pour } i \neq k. \end{cases}$$

On obtient $\det(B) = \lambda\det(A)$ et det est linéaire par rapport aux lignes.

Soit maintenant A une matrice telle que $\mathrm{Rg}(A) < n$. Nous montrons que $\det(A) = 0$. La condition $\mathrm{Rg}(A) < n$ impose qu'une des lignes de A, disons la k-ième, est combinaison linéaire des autres :

$$Z_k = \sum_{i \neq k} x_i Z_i$$

où les Z_i sont les lignes de A. Par linéarité, on obtient

$$\det(A) = \det \begin{pmatrix} Z_1 \\ \vdots \\ Z_k \\ \vdots \\ Z_n \end{pmatrix} = \sum_{i \neq k} x_i \det \begin{pmatrix} Z_1 \\ \vdots \\ Z_i \\ \vdots \\ Z_n \end{pmatrix}.$$

Chacune des matrices apparaissant dans la somme de droite a une ligne apparaissant deux fois. Il reste donc à montrer que pour une telle matrice, la fonction det s'annule. Soit donc

$$B = \begin{pmatrix} Z_1 \\ \vdots \\ Z_i \\ \vdots \\ Z_i \\ \vdots \\ Z_n \end{pmatrix}$$

une matrice dont la ligne i et la ligne k sont égales (à la ligne Z_i). On a $\mathrm{Rg}(B_{l,j}) < n-1$ pour $l \neq i$ et $l \neq k$. En particulier notre hypothèse de récurrence donne $\det(B_{l,j}) = 0$ pour $l \neq i$ et pour $l \neq k$. Par définition de det, on obtient

$$\det(B) = (-1)^{i+j} b_{i,j} \det(B_{i,j}) + (-1)^{k+j} b_{k,j} \det(B_{k,j}).$$

Par ailleurs, on a $b_{i,j} = b_{k,j}$ et $B_{i,j} = E^{(n-1)}_{i,i+1} \cdots E^{(n-1)}_{k-2,k-1} B_{k,j}$. On obtient donc

$$\begin{aligned} \det(B) &= (-1)^{i+j} b_{i,j} \det(B_{i,j}) + (-1)^{k+j} (-1)^{k-i-1} b_{i,j} \det(B_{i,j}) \\ &= (-1)^{i+j} b_{i,j} \det(B_{i,j}(1-1) = 0. \end{aligned}$$

Montrons maintenant que $\det(I_n) = 1$. On a $\det(I_n) = (-1)^{j,j} \det((I_n)_{j,j}) = \det(I_{n-1}) = 1$ par récurrence. On a donc bient montré que det est une fonction déterminant.

Montrons maintenant l'unicité. Soient det et $\det'$ deux fonctions déterminant. Pour A non inversible, on a $\det(A) = 0 = \det'(A)$. Pour A inversible, il existe des matrices élémentaires $T_1, \cdots, T_t$ tells que $T_t \cdots T_1 A = I_n$. Comme les fonctions det et $\det'$ sont les mêmes pour les matrices élémentaires, on obtient

$$\det(A) = \det(T_1^{-1}) \cdots \det(T_t^{-1}) = \det'(T_1^{-1}) \cdots \det'(T_t^{-1}) = \det'(A).$$

On a donc $\det(A) = \det'(A)$. ∎

Index