QUELQUES NOTIONS UTILES EN THÉORIE DES GROUPES

A. El Kacimi

Ce texte rassemble des réponses (que j'ai données sous forme écrite) à quelques-unes des questions que m'ont posées des étudiants sur ceci ou cela en théorie des groupes. Elles ne sont pas toutes détaillées mais chacune d'elles donne au moins une idée.

1. La notion de section

1.1. En général

Soient X et B deux ensembles (non vides bien sûr) et $\pi : X \longrightarrow B$ une application surjective. Pour tout $b \in B$:

$$X_b = \pi^{-1}(b) = \{x \in X : \pi(x) = b\}$$

est une partie non vide de X appelée *fibre* de π au-dessus de b. Si $b \neq b'$, les deux fibres X_b et $X_{b'}$ sont disjointes. La famille $\{X_b\}_{b\in B}$ (indexée par B) est donc une partition de X.

Dans chaque fibre X_b, on peut choisir un et un seul élément $\sigma(b)$. Ceci est évident si l'ensemble B est fini ; c'est aussi clair si B est dénombrable. Pour B non dénombrable, l'axiome du choix nous permet de faire cela. On définit ainsi une application :

$$\sigma : b \in B \longmapsto \sigma(b) \in X \quad \text{avec} \quad \sigma(b) \in X_b. \tag{1}$$

On a donc $\pi \circ \sigma =$identité de B. Une vérification immédiate montre que σ est injective. On dira que σ est une *section* de π. Cette section σ permet de "remonter" l'ensemble B dans X et l'y plonger de telle sorte que la restriction de π à $\Sigma = \sigma(B)$ soit une bijection sur B.

Du point de vue ensembliste, une surjection $\pi : X \longrightarrow B$ admet donc toujours une section $\sigma : B \longrightarrow X$. Si les ensembles X et B ont une structure supplémentaire et que π préserve cette structure, il est alors souhaitable que σ la préserve aussi ! Expliquons cela sur des exemples :

- Si X et B sont des espaces métriques (ou généralement des espaces topologiques) et π est continue, il serait bien que σ soit aussi continue.
- Si X et B sont des groupes et π est un homomorphisme, il serait bien que σ soit aussi un homomorphisme.
- Si X et B sont des espaces vectoriels et π est linéaire, il serait bien que σ soit aussi linéaire.
- Si X et B sont des espaces normés et π est linéaire continue, il serait bien que σ soit aussi linéaire et continue.

On peut multiplier les exemples mais déjà ceux-là expliquent suffisamment les choses. Il n'est malheureusement pas toujours possible d'avoir de telles sections ; nous allons voir

cela sur quelques exemples : un sur lequel ça marche et deux autres sur lesquels ça ne marche pas.

1.2. Exemples

– Supposons que X et B soient des espaces vectoriels sur le corps K ($\mathbb{R}$ ou $\mathbb{C}$) et π linéaire. Alors π admet toujours une section linéaire $\sigma : B \longrightarrow X$. En effet, soit $\{b_i\}_{i\in I}$ une base de B ; pour chaque $i \in I$, soit x_i un vecteur de X tel que $\pi(x_i) = b_i$. Comme n'importe quel vecteur b de B s'écrit $b = \lambda_{i_1} b_{i_1} + \cdots + \lambda_{i_n} b_{i_n}$ (avec $\lambda_{i_1}, \cdots, \lambda_{i_n} \in \mathbb{K}$), on définit $\sigma(b)$ en posant :

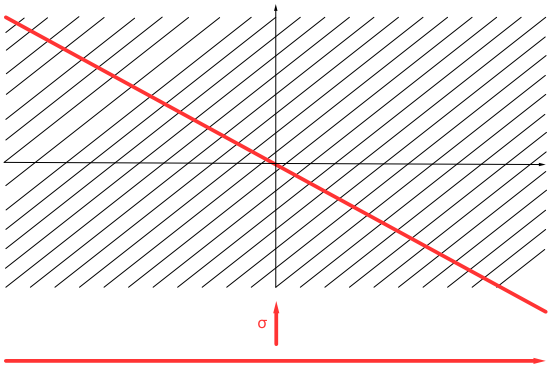
$$\sigma(b) = \lambda_{i_1} x_{i_1} + \cdots + \lambda_{i_n} x_{i_n}. \tag{2}$$

L'application $\sigma : B \longrightarrow X$ ainsi définie est bien une section linéaire de π. Si X et B sont en plus normés et π est continue, alors une section continue $\sigma : B \longrightarrow X$ n'existe pas toujours si la dimension de B est infinie (la construction d'un exemple à cet effet est un peu plus laborieuse). Mais si $\dim(B) < +\infty$, une telle section existe toujours. Regardons l'exemple simple qui suit.

– Supposons $X = \mathbb{R}^2$, $B = \mathbb{R}$ (chacun de ces espaces est muni de l'une de ses normes usuelles) et π définie par $\pi(x, y) = x - y$ (π est linéaire continue). Alors les fibres X_b de π sont les droites affines $x - y = c$ avec c une constante (variant dans $\mathbb{R}$). Toute application linéaire :

$$\sigma_\mu : x \in \mathbb{R} \longmapsto (x, \mu x) \in \mathbb{R} \tag{3}$$

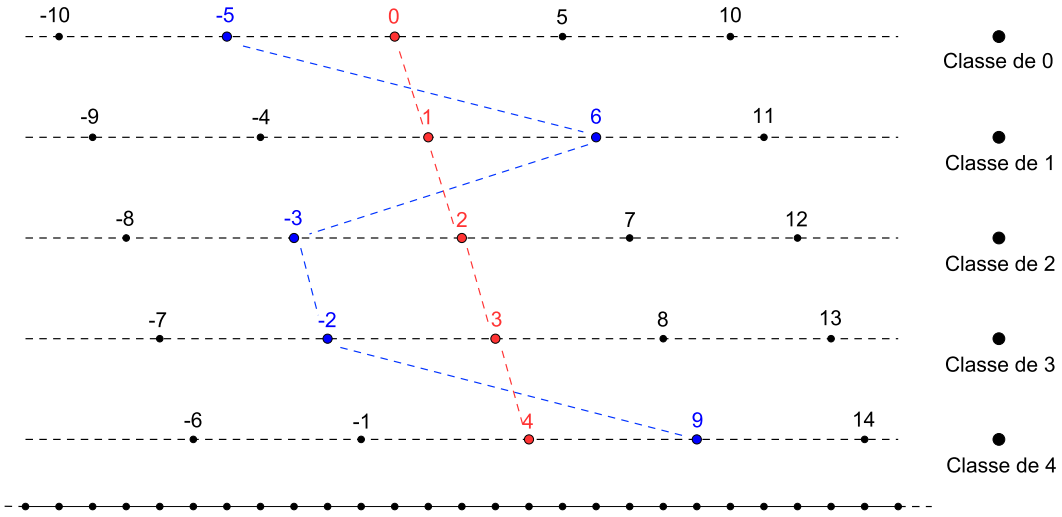
où μ est un réel tel que $\mu \neq 1$, est alors une section linéaire continue de π.



Les droites affines en noir sont les fibres de l'application linéaire π. La droite vectorielle en rouge est l'image de la section $\sigma_\mu : \mathbb{R} \longrightarrow \mathbb{R}^2$. Elle coupe chacune des fibres en un et un seul point : elle "sectionne" les fibres, d'où son appellation.

– Supposons $X = \mathbb{Z}$; soit H le sous-groupe $n\mathbb{Z}$ des multiples de n où n est un entier strictement supérieur à 1. Alors H est un sous-groupe distingué de $X = \mathbb{Z}$ et le quotient

$B = X/H$ n'est rien d'autre que le groupe $\mathbb{Z}/n\mathbb{Z}$ des classes modulo n de $\mathbb{Z}$. La projection canonique $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z}$ est un morphisme surjectif de groupes. L'application π admet des sections au sens ensembliste (*cf.* dessin qui suit pour $n = 5$) mais aucune d'elles ne saurait être un morphisme de groupes. En effet, si $\sigma : \mathbb{Z}/n\mathbb{Z} \longrightarrow \mathbb{Z}$ est un "homomorphisme section" de π, l'image de $\overline{1}$ est un entier non nul k de $\mathbb{Z}$; comme $\overbrace{\overline{1} + \cdots + \overline{1}}^{n \text{ fois}} = \overline{n} = \overline{0}$, l'entier $\overbrace{k + \cdots + k}^{n \text{ fois}} = nk$ doit être nul, ce qui est absurde !



2. Extensions de groupes

On se donne deux groupes quelconques H et Γ. *Peut-on en construire d'autres à partir de ces deux-là* ? La réponse est oui et nous allons donner un procédé de construction. Pour éviter des confusions éventuelles, on note $+$ la loi sur H, 0 sera l'élément neutre de H et 1 celui de Γ.

2.1. Définition. *On appelle* ***extension*** *de Γ par H (ou de H par Γ) toute suite exacte courte de groupes et de morphismes :*

$$0 \longrightarrow H \xrightarrow{j} G \xrightarrow{\pi} \Gamma \longrightarrow 1. \tag{4}$$

Cela signifie que j est injectif, π est surjectif et le noyau de π est égal à l'image de j.

Bien sûr le groupe G est plus gros que H puisqu'il le contient mais aussi plus gros que Γ puisqu'il se surjecte dessus. (Dans la littérature mathématique, on parle souvent d'extension de Γ par H même si c'est plutôt H qu'on étend !)

2.2. Produit direct ou extension triviale

On pose $G = H \times \Gamma$; sur cet ensemble on définit la loi de composition interne :

$$(h, \gamma) \cdot (h', \gamma') = (h + h', \gamma\gamma'). \tag{5}$$

Il est facile de voir qu'on obtient ainsi un groupe dans lequel l'élément neutre est $(0,1)$ et l'inverse de (h,γ) est $(-h,\gamma^{-1})$. Tout élément de la forme $(h,1)$ commute avec tout élément de la forme $(0,\gamma)$. On dira que $G = H \times \Gamma$ est le *produit direct* des deux groupes H et Γ.

On définit les morphismes $j : H \longrightarrow G$ et $\pi : G \longrightarrow \Gamma$ par $j(h) = (h,1)$ et $\pi(h,\gamma) = \gamma$. On vérifie immédiatement que la suite :

$$0 \longrightarrow H \xrightarrow{j} G \xrightarrow{\pi} \Gamma \longrightarrow 1$$

est exacte. On dira que G est une *extension triviale* de Γ par H.

2.3. Produit semi-direct

On rappelle qu'un *automorphisme* de H n'est rien d'autre qu'un isomorphisme de groupes $H \longrightarrow H$. L'ensemble des automorphismes de H muni de la composition des applications est un groupe qu'on note $\mathrm{Aut}(H)$.

Une *représentation* de Γ dans H est un morphisme de groupes $\rho : \Gamma \longrightarrow \mathrm{Aut}(H)$. Il permet de définir une action du groupe Γ sur H :

$$(\gamma, h) \in \Gamma \times H \longmapsto \rho(\gamma)(h) \in H.$$

Ainsi, un élément quelconque γ de Γ est vu, à l'aide de ρ, comme un automorphisme de H. Pour simplifier, et quand il n'y a pas de confusion sur la représentation ρ, l'élément $\rho(\gamma)(h)$ (transformé de h par l'automorphisme $\rho(\gamma)$) sera noté $\gamma \cdot h$. On munit $H \times \Gamma$ de la loi de composition interne :

$$(h',\gamma') \cdot (h,\gamma) = (\gamma' \cdot h + h', \gamma'\gamma). \tag{6}$$

qui fait de $H \times \Gamma$ un groupe. Son élément neutre est $(0,1)$ et l'inverse de (h,γ) est $(-(\gamma^{-1} \cdot h), \gamma^{-1})$. Le groupe G ainsi construit se note $H \rtimes_\rho \Gamma$ et s'appelle produit *semi-direct* de H par Γ relativement à ρ. Il est évident que si ρ est le morphisme trivial, c'est-à-dire si $\rho(\gamma) =$ identité de H pour tout $\gamma \in \Gamma$, $H \rtimes_\rho \Gamma$ est le produit direct $H \times \Gamma$.

Là aussi on définit les morphismes $j : H \longrightarrow G$ et $\pi : G \longrightarrow \Gamma$ par $j(h) = (h,1)$ et $\pi(h,\gamma) = \gamma$ et on vérifie immédiatement que la suite :

$$0 \longrightarrow H \xrightarrow{j} H \rtimes_\rho \Gamma \xrightarrow{\pi} \Gamma \longrightarrow 1 \tag{7}$$

est exacte. On a donc une extension de Γ par H. Mais c'est une extension qui possède une propriété en plus : le morphisme π admet l'application :

$$\sigma : \gamma \in \Gamma \longmapsto (0,\gamma) \in G$$

comme section. On peut dire en quelque sorte que H et l'image de Γ par la section σ sont deux facteurs qui permettent de fabriquer le groupe G. Ceci est illustré par le :

2.4. Théorème. *Soient H et Γ deux sous-groupes d'un groupe G tels que :*

- *H est distingué dans G ;*
- *$H \cap \Gamma = \{1\}$;*
- *l'application $\phi : (h, \Gamma) \in H \times \Gamma \longmapsto h\gamma \in G$ est bijective.*

Soit ρ le morphisme de Γ dans $\mathrm{Aut}(G)$ qui à γ associe l'automorphisme intérieur φ_γ. Alors l'application $\phi : (h, \gamma) \in H \rtimes_\rho \Gamma \longmapsto h\gamma \in G$ est un isomorphisme de groupes. On dira que G est le produit semi-direct ***interne*** *de ses deux sous-groupes H et Γ.*

3. Divers

Une extension $0 \longrightarrow H \xrightarrow{j} G \xrightarrow{\pi} \Gamma \longrightarrow 1$ est dite *scindée* si le morphisme π admet une section $\sigma : \Gamma \longrightarrow G$ (bien sûr σ doit être un morphisme de groupes) ; autrement on dira qu'elle est *non scindée*.

3.1. Nous avons vu que si G est le produit semi-direct d'un groupe H par un groupe Γ, alors l'extension : $0 \longrightarrow H \xrightarrow{j} H \rtimes_\rho \Gamma \xrightarrow{\pi} \Gamma \longrightarrow 1$ est scindée. Réciproquement, soit $0 \longrightarrow H \xrightarrow{j} G \xrightarrow{\pi} \Gamma \longrightarrow 1$ une extension scindée par une section $\sigma : \Gamma \longrightarrow G$. Notons $\widetilde{\Gamma}$ le sous-groupe de G image de Γ par σ ($\sigma : \Gamma \longrightarrow \widetilde{\Gamma}$ est un isomorphisme). Alors :

- H est distingué dans G puisque noyau du morphisme π.
- $H \cap \widetilde{\Gamma} = \{e\}$. En effet, soit $g \in H \cap \widetilde{\Gamma}$ qui est de la forme $g = \sigma(\gamma)$; donc $\gamma = \pi(g) = \pi(\sigma(\gamma)) = 1$ puisque $g \in H = \ker(\pi)$; comme σ est un morphisme $g = \sigma(\gamma) = \sigma(1) = e$.
- L'application $\phi : (h, \widetilde{\gamma}) \in H \times \widetilde{\Gamma} \longmapsto h\widetilde{\gamma} \in G$ est une bijection. Montrons qu'elle est injective. À cet effet soient $(h_1, \widetilde{\gamma}_1)$ et $(h_2, \widetilde{\gamma}_2)$ deux éléments de $H \times \widetilde{\Gamma}$ tels que $h_1\widetilde{\gamma}_1 = h_2\widetilde{\gamma}_2$; alors $\widetilde{\gamma}_1\widetilde{\gamma}_2^{-1} = h_1^{-1}h_2$, ce qui montre que $\widetilde{\gamma}_1$ et $\widetilde{\gamma}_2$ sont équivalents modulo H, donc égaux puisque $\widetilde{\Gamma}$ ne contient qu'un et un seul élément de chaque classe d'équivalence. L'égalité $\widetilde{\gamma}_1 = \widetilde{\gamma}_2$ implique automatiquement $h_1 = h_2$. Montrons maintenant que ϕ est surjective. Soit $g \in G$ et posons $\gamma = \pi(g)$. De façon évidente, g et $\widetilde{\gamma} = \sigma(\gamma)$ sont équivalents modulo H ; il existe donc $h \in H$ tel que $g\widetilde{\gamma}^{-1} = h$, d'où $g = h\widetilde{\gamma} = \phi(h, \widetilde{\gamma})$.

Pour finir, H étant distingué dans G, $\widetilde{\Gamma}$ agit dessus par automorphismes intérieurs (par conjugaison si on préfère). D'après le théorème 2.4. G est le produit semi-direct interne de H et $\widetilde{\Gamma}$.

3.2. Soient G un groupe et A une partie de G. On appelle *centralisateur* de A l'ensemble $\mathcal{C}(A)$ de tous les éléments de G qui commutent à tout élément de A :

$$\mathcal{C}(A) = \{g \in G : ga = ag \quad \text{pour tout } a \in A\}.$$

On vérifie immédiatement que, si A est symétrique ($a \in A \Longrightarrow a^{-1} \in A$), $\mathcal{C}(A)$ est un sous-groupe de G. Le centralisateur $\mathcal{C}(G)$ de tout le groupe G est appelé *centre* de G ; il y est distingué.

Soit $0 \longrightarrow H \xrightarrow{j} G \xrightarrow{\pi} \Gamma \longrightarrow 1$ une extension scindée par une section $\sigma : \Gamma \longrightarrow G$. Supposons que σ est à valeurs dans le centralisateur $\mathcal{C}(H)$. Alors l'extension considérée est

triviale *i.e.* le groupe G est isomorphe au produit direct $H \times \Gamma$. C'est le cas en particulier d'une *extensions centrale* scindée (*i.e.* pour laquelle $H \subset \mathcal{C}(G)$). (Les vérifications sont laissées au lecteur.)

4. Exemples d'extensions

4.1. Voici une extension dont on a déjà parlé mais cela ne fait pas de mal de la reprendre. On prend $G = \mathbb{Z}$ et $H = n\mathbb{Z}$ le sous-groupe des multiples de n où n est un entier strictement supérieur à 1. Le quotient $\Gamma = G/H$ est le groupe des classes résiduelles $\mathbb{Z}/n\mathbb{Z}$ modulo n. Notons $j : H \hookrightarrow G$ l'inclusion et $\pi : G \longrightarrow \Gamma$ la projection canonique. Nous avons alors une suite exacte :

$$0 \longrightarrow n\mathbb{Z} \overset{j}{\hookrightarrow} \mathbb{Z} \overset{\pi}{\longrightarrow} \mathbb{Z}/n\mathbb{Z} \longrightarrow 0 \tag{8}$$

donc une extension de $\mathbb{Z}/n\mathbb{Z}$ par $n\mathbb{Z}$. Comme on l'a déjà vu, le morphisme projection π n'a pas de morphisme section et donc l'extension (8) n'est pas scindée. C'est l'exemple le plus simple d'extension non scindée qu'on puisse donner si jamais la question est posée !

4.2. Soit $\mathcal{P}$ un espace affine dirigé par un espace vectoriel $\overrightarrow{\mathcal{V}}$ (réel ou complexe) de dimension n. On rappelle que la structure affine sur $\mathcal{P}$ est définie par une application $\Phi : (M, N) \in \mathcal{P} \times \mathcal{P} \longmapsto \overrightarrow{MN} \in \overrightarrow{\mathcal{V}}$ telle que :

(i) $\overrightarrow{ML} + \overrightarrow{LN} = \overrightarrow{MN}$ (relation de Chasles) ;

(ii) pour tout $O \in \mathcal{P}$, l'application partielle $\Phi_O : M \in \mathcal{P} \longmapsto \overrightarrow{OM} \in \overrightarrow{\mathcal{V}}$ est une bijection. Tout point M de $\mathcal{P}$ s'écrit ainsi de façon unique $M = O + \overrightarrow{u}$ avec $\overrightarrow{u} \in \overrightarrow{\mathcal{V}}$.

L'ensemble des bijections affines de $\mathcal{P}$ forment un groupe appelé *groupe affine* de $\mathcal{P}$ et noté $\mathrm{Aff}(\mathcal{P})$. Il se surjecte sur le *groupe linéaire* $\mathrm{GL}(\overrightarrow{\mathcal{V}})$ de l'espace vectoriel $\overrightarrow{\mathcal{V}}$ par le morphisme π qui à toute application affine f associe sa direction $\overrightarrow{f}$. Le noyau de π est le sous-groupe $\mathcal{T}$ des translations de $\mathcal{P}$. Nous avons ainsi une suite exacte :

$$0 \longrightarrow \mathcal{T} \overset{j}{\hookrightarrow} \mathrm{Aff}(\mathcal{P}) \overset{\pi}{\longrightarrow} \mathrm{GL}(\overrightarrow{\mathcal{V}}) \longrightarrow 1 \tag{9}$$

donc une extension de $\mathrm{GL}(\overrightarrow{\mathcal{V}})$ par $\mathcal{T}$. Cette extension est scindée. En effet, si O est un point de $\mathcal{P}$, on peut munir $\mathcal{P}$ d'une structure d'espace vectoriel pour laquelle la bijection $\Phi_O : M \in \mathcal{P} \longmapsto \overrightarrow{OM} \in \overrightarrow{\mathcal{V}}$ est un isomorphisme. Ainsi, pour cette structure d'espace vectoriel sur $\mathcal{P}$, les applications linéaires sont exactement les applications affines qui fixent le point O. À tout isomorphisme linéaire $\overrightarrow{f}$ de $\overrightarrow{\mathcal{V}}$ on associe alors l'isomorphimse affine $f = \sigma(\overrightarrow{f})$ défini par le diagramme commutatif :

$$\begin{array}{ccc} \mathcal{P} & \overset{\Phi_O}{\longrightarrow} & \overrightarrow{\mathcal{V}} \\ f \downarrow & & \downarrow \overrightarrow{f} \\ \mathcal{P} & \overset{\Phi_O}{\longrightarrow} & \overrightarrow{\mathcal{V}} \end{array}$$

Il est facile de vérifier que σ est un homomorphisme de $\mathrm{GL}(\overrightarrow{\mathcal{V}})$ dans $\mathrm{Aff}(\mathcal{P})$ et qu'il vérifie $\pi \circ \sigma =$ identité de $\mathrm{GL}(\overrightarrow{\mathcal{V}})$, c'est-à-dire σ est une section de π. Ce qui montre que l'extension

(9) est scindée. (Le scindement qu'on vient de construire dépend bien entendu du choix du point O.)

Lorsque $\mathcal{P}$ est l'espace vectoriel $\mathbb{R}^n$ muni de sa structure affine canonique, le groupe linéaire $\mathrm{GL}(n,\mathbb{R})$ est un sous-groupe de $\mathrm{Aff}(\mathbb{R}^n)$ et la section σ n'est rien d'autre que l'injection $\mathrm{GL}(n,\mathbb{R}) \hookrightarrow \mathrm{Aff}(\mathbb{R}^n)$; le groupe additif $(\mathbb{R}^n,+)$ est vu comme le sous-groupe des translations. Ainsi :

$$\mathrm{Aff}(\mathbb{R}^n) = \mathbb{R}^n \rtimes \mathrm{GL}(n,\mathbb{R}). \tag{10}$$

Un exemple plus simple à comprendre est le groupe GA des transformations affines préservant l'orientation de la droite réelle $\mathbb{R}$. (Ce sont les transformations de la forme $x \in \mathbb{R} \longmapsto ax+b \in \mathbb{R}$ avec $a \in \mathbb{R}_+^*$ et $b \in \mathbb{R}$.) Le groupe multiplicatif $\mathbb{R}_+^*$ agit (par automorphismes) sur le groupe additif $\mathbb{R}$:

$$(a,t) \in \mathbb{R}_+^* \times \mathbb{R} \longmapsto at \in \mathbb{R}.$$

Le produit semi-direct $\mathbb{R} \rtimes \mathbb{R}_+^*$ associé à cette action n'est alors rien d'autre que le groupe GA qu'on appelle *groupe affine* de la droite réelle.

4.3. Le groupe linéaire $\mathrm{GL}(n,\mathbb{R})$ et le groupe affine $\mathrm{Aff}(\mathbb{R}^n)$ contiennent de nombreux sous-groupes extrêmement intéressants et dont pas mal d'entre eux sont des produits semi-directs. Ils s'obtiennent dès qu'on impose aux transformations de préserver une structure géométrique supplémentaire sur l'espace vectoriel $\mathbb{R}^n$. Voici des exemples concrets.

• Munissons $\mathbb{R}^n$ de son produit scalaire usuel $\langle x,y\rangle = x_1y_1 + \cdots + x_ny_n$. Ce produit scalaire définit une norme $||x|| = \sqrt{\langle x,x\rangle}$ sur l'espace vectoriel $\mathbb{R}^n$ et une distance $d(x,y) = ||x-y||$ sur l'espace affine $\mathbb{R}^n$! On dira qu'un automorphisme linéaire $\varphi \in \mathrm{GL}(n,\mathbb{R})$ est *orthogonal* s'il vérifie :

$$\langle \varphi(x), \varphi(y)\rangle = \langle x,y\rangle \quad \text{pour tous } x,y \in \mathbb{R}^n.$$

Ces automorphismes forment un sous-groupe de $\mathrm{GL}(n,\mathbb{R})$ noté $\mathrm{O}(n)$ et appelé *groupe orthogonal* de $\mathbb{R}^n$; les éléments $\varphi \in \mathrm{O}(n)$ de déterminant 1 en forment un sous-groupe $\mathrm{SO}(n)$ appelé *groupe orthogonal spécial* de $\mathbb{R}^n$. Ces groupes agissent naturellement sur $\mathbb{R}^n$ et donnent lieu à des extensions scindées :

$$0 \longrightarrow \mathbb{R}^n \overset{j}{\hookrightarrow} \mathrm{Isom}(\mathbb{R}^n) \overset{\pi}{\longrightarrow} \mathrm{O}(n) \longrightarrow 1 \tag{11}$$

et

$$0 \longrightarrow \mathbb{R}^n \overset{j}{\hookrightarrow} \mathrm{Isom}^+(\mathbb{R}^n) \overset{\pi}{\longrightarrow} \mathrm{SO}(n) \longrightarrow 1 \tag{12}$$

où $\mathrm{Isom}(\mathbb{R}^n)$ (resp. $\mathrm{Isom}^+(\mathbb{R}^n)$) est le groupe des isométries affines de $\mathbb{R}^n$ (resp. des isométries affines de $\mathbb{R}^n$ qui préservent l'orientation). Le sous-groupe $\mathrm{SO}(n)$ est le noyau

du morphisme dét de $\mathrm{O}(n)$ sur le groupe mltiplicatif $\{1,-1\}$ qui à φ associe son déterminant dét(φ). On a donc une extension :

$$1 \longrightarrow \mathrm{SO}(n) \hookrightarrow \mathrm{O}(n) \xrightarrow{\text{dét}} \{1,-1\} \longrightarrow 1. \tag{13}$$

Elle est scindée : une section de dét est obtenue en envoyant -1 sur n'importe quel automorphisme orthogonal d'ordre 2 (*i.e.* de carré trivial) et qui ne respecte pas l'orientation de $\mathbb{R}^n$, par exemple une réflexion par rapport à un hyperplan vectoriel.

• Soit A une matrice carrée d'ordre n inversible. Pour tout entier relatif k on note A^k la puissance $|k|^{\text{ème}}$ de A si $k>0$, de A^{-1} si $k<0$; $A^0 = I$ (matrice identité). Supposons que A est à coefficients entiers et de déterminant 1 ; alors son inverse A^{-1} est aussi à coefficients entiers. Si A est d'ordre infini (A^k différente de la matrice identité pour tout $k \in \mathbb{Z}$), elle engendre une action fidèle de $\Gamma = \mathbb{Z}$ sur $H = \mathbb{Z}^n$:

$$(k, \mathbf{m}) \in \mathbb{Z} \times \mathbb{Z}^n \longmapsto A^k(\mathbf{m}) \in \mathbb{Z}^n.$$

Cette action permet de construire le produit semi-direct $G = \mathbb{Z}^n \rtimes_A \mathbb{Z}$, donc une extension scindée :

$$0 \longrightarrow \mathbb{Z}^n \hookrightarrow G \longrightarrow \mathbb{Z} \longrightarrow 0.$$

Lorsque la matrice A a toutes ses valeurs propres réelles, positives et différentes de 1, ces groupes possèdent des propriétés dynamiques extrêmement riches.

4.4. Soit $\mathbb{K}$ un corps commutatif quelconque (c'est par exemple $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ ou un corps fini). Soit G le groupe de matrices :

$$G = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} : x, y, z \in \mathbb{K} \right\}.$$

C'est un groupe non commutatif mais nilpotent (le lecteur peut le vérifier). Son centre $H = \mathcal{C}(G)$ est constitué des matrices de la forme $\begin{pmatrix} 1 & 0 & z \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$ et est isomorphe au groupe additif $(\mathbb{K}, +)$. L'application $\pi : \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} \in G \longmapsto (x, y) \in \mathbb{K}^2$ est un homomorphisme surjectif de noyau H. On a donc un isomorphisme $\Gamma = G/H \xrightarrow{\simeq} \mathbb{K}^2$ ($\mathbb{K}^2$ est muni de sa structure habituelle de groupe additif) et par suite une extension :

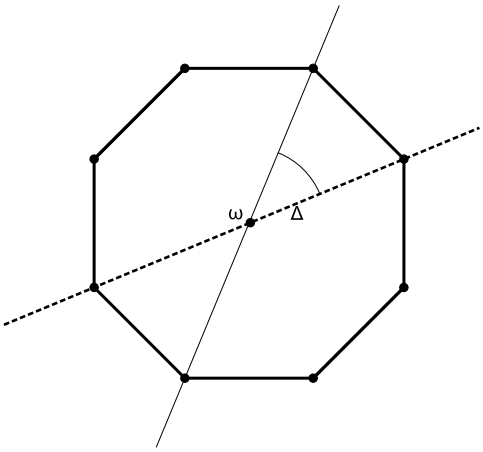
$$0 \longrightarrow \mathbb{K} \longrightarrow G \longrightarrow \mathbb{K}^2 \longrightarrow 0.$$

Cette extension est non scindée : en effet, toute section $\sigma : \Gamma \longrightarrow G$ arrive dans le centralisateur de H (puisque H est le centre de G) et donc G sera isomorphe au produit direct $\mathbb{K} \times \mathbb{K}^2 \simeq \mathbb{K}^3$, ce qui n'est pas le cas puisque G n'est pas commutatif.

4.5. Soit $\mathfrak{P}_n$ un polygone régulier à n côtés (avec $n \geq 3$) dans le plan affine euclidien. Pour $n = 3$, c'est un triangle équilatéral, pour $n = 4$, c'est un carré *etc.* Un tel polygone est toujours inscrit dans un cercle γ dont on notera ω le centre.

Soit Δ la droite passant par ω et l'un des sommets de $\mathfrak{P}_n$ et posons $\theta_n = \frac{2\pi}{n}$. Un examen de la figure ci-dessous montre immédiatement que la réflexion s d'axe Δ et la rotation ρ de centre ω et d'angle θ_n sont des isométries de $\mathcal{P}$ qui préservent le polygone $\mathfrak{P}_n$. Elles engendrent un groupe noté D_n qu'on appelle *groupe diédral* d'ordre $2n$ (nombre de ses éléments). En fait D_n est le groupe des symétries de $\mathfrak{P}_n$. La rotation ρ engendre un groupe cyclique $C_n = \{1, \rho, \rho^2, \cdots, \rho^{n-1}\}$ d'ordre n (isomorphe à $\mathbb{Z}/n\mathbb{Z}$), les autres éléments sont $s\rho, \cdots, s\rho^{n-1}$ et sont les réflexions par rapport aux droites passant par ω et les autres sommets du n-gone (autres que celui qu'on a fixé). En fait, le groupe D_n est un produit semi-direct $C_n \rtimes \mathbb{Z}/2\mathbb{Z}$.

Quant à $D_1 \simeq \mathbb{Z}/2\mathbb{Z}$, c'est le groupe des symétries d'un triangle isocèle qui n'est pas équilatéral ; $D_2 \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ est celui d'un rectangle qui n'est pas un carré.



5. Groupes résolubles, groupes nilpotents

Soit G un groupe d'élément neutre e. On appelle *commutateur* de $x, y \in G$, l'élément $xyx^{-1}y^{-1}$; on dira que x et y *commutent* si $xyx^{-1}y^{-1} = e$. Évidemment, dans un groupe abélien, tout commutateur est trivial. Le groupe G n'est pas abélien s'il admet au moins un commutateur non trivial. Ces commutateurs vont permettre de "mesurer" le "degré de non commutativité" du groupe. Pour simplifier $xyx^{-1}y^{-1}$ sera noté $[x, y]$.

On note G_1 ou $[G, G]$ le sous-groupe de G engendré par tous les commutateurs, c'est-à-dire le plus petit sous-groupe contenant la partie $\{[x, y] : x, y \in G\}$. On vérifie facilement que G_1 est un sous-groupe distingué de G. On pose :

$$G_0 = G \quad \text{et, pour tout } k \geq 1, \quad G_k = [G_{k-1}, G_{k-1}].$$

De façon immédiate, on a $\cdots G_k \subset G_{k-1} \subset \cdots \subset G_2 \subset G_1 \subset G_0 = G$; d'autre part, pour tout $k \geq 1$, G_k est un sous-groupe distingué de G_{k-1}.

5.1. Définition. *On dira que le groupe G est* ***résoluble*** *s'il existe $k \geq 1$ tel que $G_k = \{e\}$.*

Le plus petit entier k tel que $G_k = \{e\}$ et $G_{k-1} \neq \{e\}$ est appelé *degré de résolubilité* du groupe G. Si $k = 1$, le groupe G est commutatif. Plus l'entier k est "petit" plus G paraît "proche" d'un groupe commutatif. Les groupes résolubles forment une classe très importante et sont à la base de la *théorie de Galois* (résolution des équations algébriques par radicaux).

Il existe une catégorie intermédiaire entre les groupes abéliens et les groupes résolubles. Elle joue aussi un rôle important en géométrie et dans pas mal d'autres domaines en algèbre. Posons :

$$G^0 = G \quad \text{et, pour tout } k \geq 1, \quad G^k = [G^{k-1}, G].$$

On vérifie aussi facilement que $\cdots G^k \subset G^{k-1} \subset \cdots \subset G^2 \subset G^1 \subset G^0 = G$ et que, pour tout $k \geq 1$, G^k est un sous-groupe distingué de G^{k-1}.

5.2. Définition. *On dira que le groupe G est* ***nilpotent*** *s'il existe $k \geq 1$ tel que $G^k = \{e\}$.*

Le plus petit entier k tel que $G^k = \{e\}$ et $G^{k-1} \neq \{e\}$ est appelé *degré de nilpotence* du groupe G. Si $k = 1$, le groupe G est commutatif ; si $k = 2$, on dira que G est *métabélien*.

Comme $G_k \subset G^k$ pour tout k, un groupe nilpotent est forcément résoluble. On a donc la suite d'inclusions entre catégories de groupes :

$$\{\text{groupes abéliens}\} \subset \{\text{groupes nilpotents}\} \subset \{\text{groupes résolubles}\}.$$

Ces inclusions sont évidemment strictes.

5.3. Exemple résoluble non nilpotent

Soit G le groupe des transformations affines préservant l'orientation de la droite réelle $\mathbb{R}$, c'est-à-dire les applications de la forme :

$$g : x \in \mathbb{R} \longmapsto ax + b \in \mathbb{R}$$

avec $a \in \mathbb{R}_+^*$ et $b \in \mathbb{R}$. Si l'élément $g \in G$ est défini par le couple (a, b) et g' par le couple (a', b') alors gg' est défini par le couple $(a'a, a'b + b')$: facile à voir, il suffit de composer les applications g et g' dans l'ordre $g' \circ g$ (faire attention à cela dans la suite des calculs). L'inverse de g est donné par le couple $\left(\frac{1}{a}, -\frac{b}{a}\right)$.

• Le groupe multiplicatif $\mathbb{R}_+^*$ agit sur le groupe additif par homothéties :

$$(a, t) \in \mathbb{R}_+^* \times \mathbb{R} \longmapsto at \in \mathbb{R}.$$

Cette action permet de construire le produit semi-direct $\mathbb{R} \rtimes \mathbb{R}_+^*$ dont il est facile de voir que c'est exactement le groupe G.

• Montrons que G est résoluble. Soient $g = (a, b)$ et $g' = (a', b')$ deux éléments de G. On a :

$$(a, b)^{-1} = \left(\frac{1}{a}, -\frac{b}{a}\right) \quad \text{et} \quad (a', b')^{-1} = \left(\frac{1}{a'}, -\frac{b'}{a'}\right)$$

et donc :

$$(a,b)(a',b')(a,b)^{-1}(a',b')^{-1} = \left(1, \frac{b}{a} - \frac{b'}{a'} + \frac{1}{aa'}(b'-b)\right).$$

Ceci montre que le groupe dérivé $[G,G]$ de G est contenu dans le sous-groupe $\{1\} \times \mathbb{R}$. En fait, il y a égalité car, pour tout $\lambda \in \mathbb{R}$, $(1,\lambda)$ est le commutateur $\left[(\frac{1}{2}, -\lambda), (2,0)\right]$. Comme $G_1 = [G,G]$ est abélien, $G_2 = [G_1, G_1]$ est réduit à $(1,0)$, donc G est résoluble.

• Un calcul similaire au précédent permet de montrer que $G^2 = [G_1, G] = G_1$ et par suite :

$$G^3 = [G^2, G] = \cdots = [G^n, G] = \cdots = G_1.$$

Comme G_1 n'est pas le groupe trivial, G n'est pas nilpotent. ♢

5.4. Exemple nilpotent non abélien

Nous donnons juste le groupe et nous laissons le travail de vérification au lecteur. Il s'agit de l'exemple 4.4. On prend $\mathbb{K}$ un corps commutatif quelconque et G le groupe de matrices :

$$G = \left\{ \begin{pmatrix} 1 & x & z \\ 0 & 1 & y \\ 0 & 0 & 1 \end{pmatrix} : x, y, z \in \mathbb{K} \right\}.$$

6. Automorphismes de certains produits de groupes

Soient X et Y deux groupes finis d'ordres respectifs p et q premiers entre eux et $G = X \times Y$. Alors le groupe $\mathrm{Aut}(G)$ *des automorphismes de G est le produit direct* $\mathrm{Aut}(X) \times \mathrm{Aut}(Y)$.

Soit G un groupe de loi multiplicative et d'élément neutre noté 1. Si $g \in G$ et $m \in \mathbb{Z}^*$, g^m sera le composé $|m|$ fois de g si $m > 0$ et de g^{-1} si $m < 0$. Par convention $g^0 = 1$.

6.1. Soit $g \in G$; on appelle *exposant* de g tout entier $m \in \mathbb{Z}$ tel que $g^m = 1$. Si g a au moins un exposant non nul, l'ensemble $\mathcal{E}(g)$ de ses exposants est un idéal non réduit à $\{0\}$ de $\mathbb{Z}$: en effet, si $m, n \in \mathcal{E}(g)$ et $k, \ell \in \mathbb{Z}$, alors $g^{km+\ell n} = g^{km} g^{\ell n} = (g^m)^k (g^n)^\ell = 1$. Il existe donc un entier $\theta(g) > 0$ tel que $\mathcal{E}(g) = \theta(g)\mathbb{Z}$; $\theta(g)$ est le plus petit exposant strictement positif de g ; on l'appelle *ordre* de g. Si $g^m \neq 0$ pour tout $m \in \mathbb{Z}^*$, on dira que g est d'*ordre infini*. Supposons g d'ordre fini ; on a alors les assertions suivantes :

i) Si $g \neq 1$, $\theta(g) \geq 2$.
ii) $\theta(g)$ divise tout exposant de g.
iii) Si G est fini, son cardinal $|G|$ est un exposant de g (donc $\theta(g)$ divise $|G|$).
iv) Soit $\gamma : G \longrightarrow G'$ un homomorphisme de groupes. Alors tout exposant de $g \in G$ est un exposant de $\gamma(g) \in G'$. Si en plus γ est injectif, $\theta(\gamma(g)) = \theta(g)$.

Il existe des groupes infinis dont tous les éléments sont d'ordre fini : par exemple le groupe quotient $(\mathbb{Q}/\mathbb{Z}, +)$.

6.2. Rappelons qu'un *automorphisme* de G est un isomorphisme de G sur lui-même. Les automorphismes de G forment un groupe noté $\mathrm{Aut}(G)$. Un automorphisme du type $\varphi_g : x \in G \longmapsto g^{-1}xg \in G$ avec $g \in G$ est dit *intérieur*. Soit H un sous-groupe de G. On dit que H est *distingué* (*normal* ou *invariant*) si, pour tout $g \in G$, $\varphi_g(H) \subset H$. On

dit que H est *caractéristique* si, pour tout $\gamma \in \mathrm{Aut}(G)$, $\gamma(H) \subset H$. Évidemment, si H est caractéristique, il est distingué ; la réciproque est en général trivialement fausse.

Comme exemples : le centre $Z(G)$ de G (sous-groupe des éléments qui commutent à tout élément de G) et son premier groupe dérivé $[G, G]$ sont caractéristiques.

6.3. Revenons aux groupes X, Y et G de l'énoncé. L'élément neutre $(1, 1)$ de G sera noté 1. On regardera X et Y respectivement comme les sous-groupes $X \times \{1\}$ et $\{1\} \times Y$ par les identifications $x = (x, 1)$ et $y = (1, y)$. Nous allons montrer que X et Y sont des sous-groupes caractéristiques de G *i.e.*, pour tout $\gamma \in \mathrm{Aut}(G)$, $\gamma(X) \subset X$ et $\gamma(Y) \subset Y$. Faisons-le pour X.

Soient $\gamma \in \mathrm{Aut}(G)$ et $x = (x, 1) \in X$. Il s'agit de montrer que $\gamma(x, 1)$ est de la forme $(x', 1)$. Si $x = 1$, on a clairement $\gamma(x, 1) = (1, 1)$; on prend donc $x \neq 1$. A priori $\gamma(x) = (x', y')$ avec $x' \in X$ et $y' \in Y$. Supposons $y' \neq 1$. Comme $x \in X$, p est un exposant de x *i.e.* $x^p = 1$. Mais $y' = \pi \circ \gamma(x, 1)$ où π est le morphisme $\pi : (x', y') \in X \times Y \longmapsto y' \in Y$, donc p est un exposant de y' (*cf.* assertion iv) de la section **1**), par suite p est un multiple de $\theta(y')$ qui est supérieur ou égal à 2 puisque y' est supposé distinct de 1. Comme d'autre part $y' \in Y$, q est aussi un exposant de y', donc un multiple de $\theta(y')$. En résumé, les entiers p et q ont $\theta(y') \geq 2$ comme diviseur commun ; ceci est impossible puisque ils sont supposés premiers entre eux. Par suite, l'hypothèse $y' \neq 1$ est absurde : on a forcément $y' = 1$, ce qui signifie que l'image de X par γ est contenue dans X. Le sous-groupe X est stable par tout automorphisme de G, il est donc caractéristique. Le même raisonnement vaut pour le sous-groupe Y.

6.4. Montrons maintenant que $\mathrm{Aut}(G) = \mathrm{Aut}(X) \times \mathrm{Aut}(Y)$. Soient $\varphi \in \mathrm{Aut}(X)$ et $\psi \in \mathrm{Aut}(Y)$. Il est alors évident que $\gamma(x, y) = (\varphi(x), \psi(y))$ est un automorphisme de G. Donc $\mathrm{Aut}(X) \times \mathrm{Aut}(Y) \subset \mathrm{Aut}(G)$.

Soit $\gamma \in \mathrm{Aut}(G)$. Comme X (resp. Y) est caractéristique, la restriction φ (resp. ψ) de γ à X (resp. à Y) est un automorphisme de X (resp. de Y). On a alors :

$$\begin{aligned}
\gamma(x, y) &= \gamma((x, 1)(1, y)) \\
&= \gamma(x, 1)\gamma(1, y) \\
&= \varphi(x)\psi(y) \\
&= (\varphi(x), 1)(1, \psi(y)) \\
&= (\varphi(x), \psi(y))
\end{aligned}$$

ce qui montre que $\gamma \in \mathrm{Aut}(X) \times \mathrm{Aut}(Y)$ donc $\mathrm{Aut}(G) \subset \mathrm{Aut}(X) \times \mathrm{Aut}(Y)$. On a finalement montré que $\mathrm{Aut}(G)$ est le produit direct $\mathrm{Aut}(X) \times \mathrm{Aut}(Y)$. ♢

6.5. Comme exemple, on peut prendre pour X et Y les groupes cycliques C_p et C_q avec p et q premiers entre eux. Alors :

$$\mathrm{Aut}(C_p \times C_q) = \mathrm{Aut}(C_p) \times \mathrm{Aut}(C_q) \simeq \mathcal{R}_p \times \mathcal{R}_q$$

où $\mathcal{R}_p$ et $\mathcal{R}_q$ sont les groupes multiplicatifs des éléments inversibles respectivement des anneaux $\mathbb{Z}/p\mathbb{Z}$ et $\mathbb{Z}/q\mathbb{Z}$; leurs ordres sont égaux respectivement à $\phi(p)$ et $\phi(q)$ où $\phi : \mathbb{N}^* \longrightarrow \mathbb{N}$ est l'*indicateur d'Euler* :

$$\phi(n) = \#\{k : 1 \leq k \leq n \text{ et } k \text{ premier avec } n\}.$$

De façon générale, soient $G_1, \cdots, G_k$ des groupes finis d'ordres respectifs $n_1, \cdots, n_k$ et $G = G_1 \times \cdots \times G_k$ leur produit direct. Supposons $n_i \wedge n_j = 1$ pour $i \neq j$. Alors, pour tout $i \in \{1, \cdots, k\}$, G_i est un sous-groupe caractéristique de G et on a :

$$\mathrm{Aut}(G) = \mathrm{Aut}(G_1) \times \cdots \times \mathrm{Aut}(G_k).$$

Exercice 1. Soient C_p et C_q les groupes cycliques d'ordres respectifs p et q. On suppose p et q premiers entre eux. Montrer que le produit direct $G = C_p \times C_q$ est cyclique.

Exercice 2. Soit G un ensemble fini muni d'une loi de composition interne qui à tout (x, y) dans $G \times G$ associe $xy \in G$; on suppose qu'elle est associative et que tout élément $a \in G$ est *simplifiable*, c'est-à-dire :

$$ax = ay \Longrightarrow x = y \qquad \text{et} \qquad xa = ya \Longrightarrow x = y.$$

Montrer que G est un groupe.

Solution

Pour tout $a \in G$ on note a^i le produit de a par lui-même i fois (avec $i \in \mathbb{N}^*$). La loi étant associative, on a $a^i a^j = a^{i+j}$.

Soit $a \in G$. Comme G est fini, il existe $i, k \in \mathbb{N}^*$ tels que $a^{i+k} = a^i$. Alors $e = a^k$ est un élément neutre à gauche. En effet, soit $x \in G$; on a $a^i e = a^i$, donc $(a^i e)x = a^i x$ c'est-à-dire $a^i(ex) = a^i x$ (la loi est associative). Comme tout élément est simplifiable, cette relation implique $ex = e$. De la même manière on montre que e est aussi élément neutre à droite.

Soit maintenant $x \in G$. Si $x = e$, il est inversible et $x^{-1} = e$. Supposons $x \neq e$. Alors il existe $i \in \mathbb{N}$ avec $i \geq 2$ tel que $x^i = e$; donc x est inversible d'inverse $x^{-1} = x^{i-1}$. $\diamondsuit$

De ce qu'on vient de démontrer on déduit de façon immédiate la proposition qui suit (quelquefois assez pratique).

Proposition. *Soient G un groupe et H un sous-ensemble fini de G. Alors H est un sous-groupe si, et seulement si, H est stable par composition.* $\diamondsuit$