Agrégation interne de mathématiques **RK**

Séance n° 2

Thème : Groupes (II)

Document en cours de rédaction !

Table des matières

1 Notes de cours

1.1 Conjugaison

Soient X et X' sont deux ensembles et $\phi : X \to X'$ une bijection. À toute application $f : X \to X$, on peut associer une application $g : X' \to X'$ qui est en quelque sorte égale à f « transformée » par ϕ, selon le diagramme :

$$\begin{array}{ccc} X & \xrightarrow{f} & X \\ {\scriptstyle\phi}\downarrow & & \downarrow{\scriptstyle\phi} \\ X' & \xrightarrow[g=\phi f \phi^{-1}]{} & X' \end{array}$$

L'application $g = \phi f \phi^{-1}$ s'appelle la conjuguée de f par ϕ. Si X et X' sont munis d'une structure algébrique (telle que groupe, espace vectoriel, ...), si ϕ est un isomorphisme pour cette structure et si f est un morphisme, alors g sera aussi un morphisme qui possédera exactement les mêmes propriétés "géométriques" que f (en qualifiant de géométrique une propriété qui s'exprime à l'aide de la structure de X).

Si par exemple X et X' sont deux plans euclidiens orientés, $f \in L(X)$ et ϕ isométrie bijective directe de X dans X' (=isomorphisme d'espace vectoriel euclidien orienté) alors
f symétrie orthogonale par rapport à $F \implies g$ symétrie orthogonale par rapport à $\phi(F)$
f rotation d'angle $\theta \implies g$ rotation d'angle θ
Si ϕ est indirecte au lieu de directe, f rotation d'angle $\theta \implies g$ rotation d'angle $-\theta$.

Si on note $\mathrm{Iso}(X)$ le groupe des isomorphismes de X (pour la structure envisagée), et si ϕ est un isomorphisme de X dans X', alors la conjugaison par ϕ

$$\begin{array}{ccc} \mathrm{Iso}(X) & \to & \mathrm{Iso}(X') \\ f & \mapsto & \phi \circ f \circ \phi^{-1} \end{array}$$

est un isomorphisme de groupe. En particulier si $X = X'$, c'est un automorphisme de $\mathrm{Iso}(X)$

Il est remarquable qu'on puisse ensuite « abstraire » cette dernière situation à un groupe quelconque au lieu d'un groupe d'application $\mathrm{Iso}(X)$. Soit en effet un groupe quelconque G, et $a \in G$. L'application

$$\begin{array}{rccc} t_a \ : & G & \to & G \\ & g & \mapsto & aga^{-1} \end{array}$$

est un automorphisme de G, appelé automorphisme intérieur de G. Deux éléments (ou deux sous-groupes de G) images l'un de l'autre par un automorphisme intérieur sont dit conjugués.

1.2 Sous-groupes distingués, groupe quotient

Soit $f : G \to G'$ un morphisme de groupe. Le noyau $H = \mathrm{Ker}(f)$ de f est un sous-groupe de G, on le sait, mais ne peut pas être n'importe quel sous-groupe. On a en effet la propriété :

$$x^{-1}y \in H \iff f(x^{-1}y) = e \iff f(x) = f(y) \iff f(yx^{-1}) = e \iff yx^{-1} \in H$$

C'est-à-dire que les congruences à gauche et à droite modulo H sont les mêmes relations d'équivalence. Ce qui s'écrit aussi :

$$(*) \quad \forall x \in G,\ xH = Hx$$

Un sous-groupe H de G qui possède cette propriété est dit distingué dans G (ou normal, ou encore invariant[1]), ce que l'on note

$$H \lhd G$$

On vérifie aisément que $(*)$ équivaut à

$$\forall x \in G,\ xH \subset Hx$$

ou bien

$$\forall x \in G,\ xHx^{-1} \subset H \quad \text{ ou encore } \quad \forall x \in G,\ xHx^{-1} = H$$

Le noyau d'un morphisme est, comme on vient de le voir, un sous-groupe distingué. Ce qui suit montrera que, réciproquement, tout sous-groupe distingué est le noyau d'un certain morphisme.

Soient maintenant G un groupe et $\mathcal{R}$ une relation d'équivalence sur G. On dit que $\mathcal{R}$ est compatible avec la loi de G si $[xy]_{\mathcal{R}}$ ne dépend pas du choix de x et de y dans leur classe d'équivalence respectives. En d'autres termes :

$$\forall x, x', y, y' \in G,\ x\mathcal{R}x' \text{ et } y\mathcal{R}y' \implies xy\mathcal{R}x'y'$$

Lorsque c'est le cas (et seulement lorsque c'est le cas), on peut munir $G/\mathcal{R}$ d'une loi de composition interne en posant

$$[x]_{\mathcal{R}}[y]_{\mathcal{R}} = [xy]_{\mathcal{R}}$$

[1] Parce qu'il est invariant par les automorphismes intérieurs de G. Un automorphisme intérieur de G induit donc sur H distingué un automorphisme qu'on pourrait être tenté de qualifier « d'extérieur » !

Il est alors immédiat qu'il s'agit d'une loi de groupe et que $x \mapsto [x]_{\mathcal{R}}$ est un morphisme de groupe. Notons H son noyau. C'est un sous-groupe distingué de G et l'on a

$$x\mathcal{R}y \iff [x]_{\mathcal{R}} = [y]_{\mathcal{R}} \iff [xy^{-1}]_{\mathcal{R}} \iff x^{-1}y \in H$$

On voit ainsi que $\mathcal{R}$ est la congruence modulo le sous-groupe distingué H.
Réciproquement, si H est un sous-groupe distingué, la congruence modulo H (à gauche ou à droite : ce sont les mêmes relations) est compatible avec la loi de G. L'ensemble $G/\mathcal{R}$ est ainsi muni d'une structure de groupe. Ce groupe est noté G/H. L'application

$$\begin{array}{rccc} \pi_H & : & G & \to & G/H \\ & & x & \mapsto & [x]_H = xH = Hx \end{array}$$

est un morphisme de G dans G/H dont le noyau est H.

Soient maintenant G, G' des groupes, $f : G \to G'$ un morphisme et $H \lhd G$. Comme dans le cas des groupes abéliens, l'application f est compatible avec la congruence modulo H si et seulement si $H \subset \mathrm{Ker}(f)$. Dans ce cas, f induit un morphisme $g : G/H \to G'$ (qui vérifie donc $g([x]_H) = f(x)$).

$$\begin{array}{ccc} G & \xrightarrow{f} & G' \\ {\scriptstyle \pi_H}\downarrow & \nearrow_{\overline{f}} & \\ G/H & & \end{array} \qquad f = \overline{f} \circ \pi_H$$

1.3 Groupe symétrique

Soit X un ensemble. On appelle groupe symétrique de X le groupe $S(X)$ des permutations de X (= bijections de X dans lui-même). Pour un élément σ de $S(X)$, il faut savoir faire la différence entre une propriété « purement algébrique » et une propriété « géométrique » de σ. Les premières s'expriment uniquement à l'aide de la loi du groupe, tandis que les formulations des secondes utilise les propriétés de σ en tant qu'application. Par exemple le fait que σ vérifie $\sigma^2 = \mathrm{Id}_X$ est une propriété algébrique. Que σ soit une transposition est une propriété géométrique.

Ainsi qu'on l'a vu, si X et X' sont deux ensembles et $\phi : X \to X'$ est une bijection, alors la conjugaison par ϕ :

$$\begin{array}{ccc} S(X) & \to & S(X') \\ f & \mapsto & \phi \circ f \circ \phi^{-1} \end{array} \qquad \begin{array}{ccc} X & \xrightarrow{f} & X \\ {\scriptstyle \phi}\downarrow & & \downarrow{\scriptstyle \phi} \\ X' & \xrightarrow[\phi f \phi^{-1}]{} & X' \end{array}$$

est un isomorphisme de groupe. En particulier, si $X = \{x_1, x_2, \ldots, x_n\}$ est fini, $S(X)$ est isomorphe à $S_n = S(\llbracket 1, n \rrbracket)$ (mieux : S_n opère sur $\llbracket 1, n \rrbracket$ exactement comme $S(X)$ opère sur X).

Un élément σ de S_n peut être indiqué par un tableau qui indique explicitement pour chaque $k \in \llbracket 1, n \rrbracket$ son image :

$$\sigma = \begin{pmatrix} 1 & 2 & \ldots & n \\ \sigma(1) & \sigma(2) & \ldots & \sigma(n) \end{pmatrix}$$

Si $\sigma \in S(X)$, on appelle support de σ l'ensemble des points de X qui sont affectés par σ : $\mathrm{Supp}(\sigma) = \{x \in X;\ \sigma(x) \neq x\}$. Un instant de réflexion convainc que deux permutations à supports disjoints commutent.

Si $a_1, a_2, \ldots, a_p$ sont des éléments distincts de X, on note $c = (a_1, a_2, \ldots, a_p)$ la permutation $c \in S(X)$ qui envoie a_k sur a_{k+1} pour $k \in [\![1, p-1]\!]$, a_p sur a_1 et fixe tout autre élément de X. Cette permutation est qualifiée de cycle de longueur p. L'ensemble $\{a_1, a_2, \ldots, a_p\}$ est le support du cycle. Un cycle de longueur 2 est appelé transposition.

Si $a_1, a_2, \ldots, a_p, a_{p+1}, \ldots, a_q$ sont des éléments deux à deux distincts de X, on a la formule suivante utile, qui signifie que le produit de deux cycles dont les supports se rencontrent en un point unique est un cycle :

$$(a_1, a_2, \ldots, a_p)(a_p, a_{p+1}, \ldots, a_q) = (a_1, a_2, \ldots, a_q)$$

Une autre formule d'usage fréquent est la suivante. Soient un cycle $c = (a_1, a_2, \ldots, a_p)$ et $\sigma \in S(X)$:

$$\begin{array}{ccc} X & \xrightarrow{c} & X \\ {\scriptstyle\sigma}\downarrow & & \downarrow{\scriptstyle\sigma} \\ X & \xrightarrow[\sigma c \sigma^{-1}]{} & X \end{array}$$

Alors le conjugué $c' = \sigma c \sigma^{-1}$ de c par σ est un cycle similaire à c, mais qui opère sur les images des a_i par σ :

$$\sigma(a_1, a_2, \ldots, a_p)\sigma^{-1} = (\sigma(a_1), \sigma(a_2), \ldots, \sigma(a_p))$$

(cette formule est une évidence dès lors qu'on a compris ce qu'est une conjugaison)

Soit X un ensemble fini et $\sigma \in S(X)$. La relation sur $x \mathcal{R} y \iff \exists n \in \mathbb{Z};\ y = \sigma^n(x)$ est une relation d'équivalence. Les classes d'équivalence sont appelées orbites de σ. Les classes d'équivalence réduite à un point sont constituées d'un point fixe. Soient $C_1, C_2, \ldots, C_q$ les classes d'équivalences non réduites à un point. Chaque classe C_k est stable par σ qui induit une permutation de C_k, laquelle, on le voit aisément, est un cycle dont le support est C_k. Si on note $c_k \in S(X)$ le cycle qui coïncident avec σ sur C_k et laisse fixe tout autre élément de X, on a

$$\sigma = c_1 c_2 \ldots c_q$$

Ainsi toute permutation se décompose en produit de cycles à supports disjoints. On vérifie que cette décomposition est unique à l'ordre des facteurs près.

Soient $\eta \in S(X)$, $\sigma \in S(X)$. Si on décompose η en produit de cycles disjoints : $\eta = c_1 c_2 \ldots c_q$, alors la décomposition en produit de cycles disjoints est

$$\sigma \eta \sigma^{-1} = (\sigma c_1 \sigma^{-1})(\sigma c_2 \sigma^{-1}) \ldots (\sigma c_q \sigma^{-1})$$

On voit ainsi que deux éléments conjugués ont, pour tout entier ℓ, le même nombre de cycles de longueur ℓ et on vérifie aisément que cette condition est aussi suffisante.

Soit X un ensemble fini. Les transpositions forment une famille génératrice de $S(X)$. En effet, si σ est une permutation distincte de l'identité et si l'on choisit $x \in X$ tel que $\sigma(x) \neq x$, alors $(x, \sigma(x)) \circ \sigma$ possède au moins un point fixe de plus que σ. Une récurrence descendante sur le nombre de points fixes atteste alors de l'existence de transpositions $\tau_1, \ldots, \tau_q$ telles que $\tau_q \tau_{q-1} \ldots \tau_1 \sigma = \mathrm{Id}$, d'où $\sigma = \tau_1 \tau_2 \ldots \tau_q$.

Étant donné $\sigma \in S_n$, on dit qu'une paire $P = \{i, j\} \subset [\![1, n]\!]$ $(i \neq j)$ est une inversion pour σ si $(\sigma(j) - \sigma(i))(j - i) < 0$. On désigne par signature de σ la valeur $\varepsilon(\sigma) = +1$ ou -1 selon que le nombre

d'inversions de σ est pair ou impair. Si on pose, pour une paire donnée, $s_\sigma(P) = 1$ ou -1 selon que P est ou non une inversion, on a $\varepsilon(\sigma) = \prod_P s_\sigma(P)$, d'où (en notant $\sigma(\{i,j\}) = \{\sigma(i), \sigma(j)\}$)

$$\varepsilon(\sigma' \circ \sigma) = \prod_P s_{\sigma' \circ \sigma}(P) = \prod_P s_{\sigma'}(\sigma(P)) s_\sigma(P) = \prod_P s_{\sigma'}(\sigma(P)) \prod_P s_\sigma(P) = \varepsilon(\sigma)\varepsilon(\sigma')$$

Ainsi, ε est un morphisme de S_n dans $\{-1, 1\}$. Son noyau, $A_n = \mathrm{Ker}(\varepsilon)$ est appelé le groupe alterné de degré n. Une permutation de signature 1 est dite paire. Une permutation de signature -1 est dite impaire.
On note que si c est un cycle de longueur ℓ, alors $\varepsilon(\ell) = (-1)^{\ell+1}$ (donc c et ℓ sont de « parités opposées » !). On en déduit :
Si σ est le produit de q transpositions, alors $\varepsilon(\sigma) = (-1)^q$
Si σ possède s orbites, alors $\varepsilon(\sigma) = (-1)^{n-s}$.

1.4 Action d'un groupe sur un ensemble

Soit G un groupe. Si on veut avoir une image « géométrique » de G, on peut tenter de « réaliser » G comme sous-groupe du groupe des permutation d'un ensemble X, c'est-à-dire de trouver un morphisme injectif de G dans $S(X)$. Une représentation moins « fidèle » est fournie par un morphisme quelconque de G dans $S(X)$. D'où les définitions :
Soit G un groupe et X un ensemble. Une opération (ou action) de G sur X est la donnée d'un morphisme $\rho : G \to S(X)$. On convient de noter, pour $g \in G$ et $x \in X$: $g.x = \rho(g)(x)$. On note que :

$$\forall g, g' \in G,\ \forall x \in X,\ g.(g'.x) = (gg').x \qquad \forall x \in X,\ e_G.x = x$$

Réciproquement, toute application $. : G \times X \to X$ vérifiant ces deux points définit une opération de G sur X (en posant $\rho(g)(x) = g.x$; attention, le premier point ne suffit pas). L'action est dite fidèle si ρ est injective.

Voici quelques exemples classiques d'actions de groupe :
• $S(X)$ opère fidèlement sur X (en posant $\sigma.x = \sigma(x)$).
• Si E est un K-espace vectoriel, $\mathrm{GL}(E)$ opère fidèlement sur E ($\rho : GL(E) \to S(E)$ est l'injection canonique et $g.x = g(x)$).
• Plus généralement, si X est un ensemble muni d'une structure donnée, $\mathrm{Iso}(X)$ opère fidèlement sur X.
• Si G est un groupe, E un $\mathbb{C}$-espace vectoriel, et $\rho : G \to GL(E)$ un morphisme, G opère "linéairement" sur E. On dit que ρ est une représentation linéaire de G (la théorie des représentations linéaires est passionnante !).
• Si X est une partie d'un espace affine euclidien $\mathcal{E}$, l'ensemble G des isométries de $\mathcal{E}$ qui laissent X globalement invariant est un sous-groupe de G de $Is(\mathcal{E})$ qui opère naturellement sur X (par $g.x = g(x)$). L'opération est fidèle si et seulement si X "engendre" $\mathcal{E}$, c'est-à-dire n'est contenu dans aucun sous-espace affine strict. On définit ainsi le groupe du cube, le groupe du tétraèdre, etc.
• Si G est un groupe, alors G opère sur lui-même par translation à gauche, c'est-à-dire en posant : $\forall g \in G, \forall x \in X,\ g.x = gx$
• Une autre action usuelle de G sur lui-même est l'action par conjugaison : $g.x = gxg^{-1}$.
• G opère par translation à gauche sur l'ensemble des classes à gauche modulo H (où H est un sous-groupe) : $g.(xH) = gxH$.
• G opère par conjugaison sur l'ensemble de ses sous-groupes : $x.H = xHx^{-1}$.
Ces quatre actions sont fort utiles pour obtenir des résultats théoriques sur les groupes finis.

Soit G un groupe opérant sur un ensemble X. On définit :

- L'orbite de $x \in X$, qu'on notera : $\omega_x = \{g.x,\ g \in G\}$
- Le stabilisateur de $x \in X$, qu'on notera : $G_x = \{g \in G;\ g.x = x\}$.
- L'ensemble des points fixes de $g \in G$, qu'on notera $X^g = \{x \in X;\ g.x = x\}$

L'action est dite transitive lorsqu'il n'y a qu'une seule orbite.
Il faut avoir à l'esprit que deux points x et $y \in X$ d'une même orbite ont des rôles similaires relativement à G. Par exemple, si $y = h.x$ alors $g \in G_y \iff g.y = y \iff gh.x = h.x \iff h^{-1}gh \in G_x \iff g \in hG_xh^{-1}$, d'où

$$G_y = hG_xh^{-1}$$

Quelques relations fructueuses relient les cardinaux de ces parties :

• En premier lieu, il est naturel de penser que plus nombreux sont les éléments de G qui fixent x, moins l'orbite de x est vaste. Plus précisément :

$$\forall x \in X,\ [G : G_x] = |\omega_x| \qquad (\text{si } |G| \text{ est fini, } \frac{|G|}{|G_x|} = |\omega_x|)$$

En effet, l'application surjective $x \mapsto g.x$ de G dans ω_x définit une relation d'équivalence sur G (avoir même image) qui n'est autre que la congruence à gauche modulo G_x ($g.x = h.x \iff g^{-1}h.x = x \iff g^{-1}h \in G_x$).

• Les orbites constituent une partition de X. Si X est fini, on a, en notant Ω l'ensemble des orbites, la relation évidente

$$|X| = \sum_{\omega \in \Omega} |\omega|$$

Lorsque $|G|$ est fini, on peut l'écrire, C désignant une partie de X contenant un et un seul élément de chaque orbite :

$$|X| = \sum_{a \in C} \frac{|G|}{|G_a|}$$

C'est ce qu'on appelle « l'équation aux classes ».
Il est fréquent qu'on l'utilise en isolant les orbites réduites à un point. En notant $X^G = \{x \in X;\ \forall g \in G, g.x = x\}$ et C' une partie contenant un et un seul représentant de chaque orbite non réduite à un point (par exemple $C' = C \setminus X^G$) :

$$|X| = |X^G| + \sum_{a \in C'} \frac{|G|}{|G_a|}$$

En particulier, lorsque G est un p-groupe (groupe d'ordre p^n, p premier), il vient

$$|X| \equiv |X^G| \quad [p]$$

• Si G et X sont finis, on peut envisager le nombre moyen de points fixes des éléments de G et constater que

Le nombre d'orbites est égal au nombre moyen de points fixes des éléments de G.

C'est la formule de Burnside. On l'obtient facilement en dénombrant « horizontalement » et « verticalement » les éléments de $\{(g, x) \in G \times X;\ g.x = x\}$. C'est en effet d'une part $\sum_{g \in G} |X^g|$ et, d'autre part,

$$\sum_{x \in X} |G_x| = \sum_{x \in X} \frac{|G|}{|\omega_x|} = \sum_{\omega \in \Omega} |\omega| \times \frac{|G|}{|\omega|} = |G||\Omega|$$

D'où

$$|\Omega| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

2 Annexes

Ces thèmes ne sont pas explicitement au programme

2.1 Produit semi-direct

Soit G un groupe et H, K deux sous-groupes. On a déjà vu que si

$$H \cap K = \{e\}, \quad HK = G \quad \text{et} \quad hk = kh \text{ pour tous } h \in H, k \in K,$$

alors

$$\begin{array}{rccc} p \ : & H \times K & \to & G \\ & (h,k) & \mapsto & hk \end{array}$$

est un isomorphisme de groupe. L'hypothèse $H \cap K = \{e\}$ équivaut à l'injectivité, $HK = G$ à la surjectivité et $hk = kh$ au fait que p soit un morphisme.

Conservons les hypothèses $H \cap K = \{e\}$, $HK = G$ et omettons la dernière. L'application p est toujours bijective mais n'est plus, a priori, un morphisme. L'idée est maintenant de transporter sur $H \times K$ la loi de G par p en posant :

$$(h,k) * (h',k') = p^{-1}(hkh'k')$$

$H \times K$ est alors muni d'une structure de groupe pour laquelle p est un isomorphisme. On est en général bien en peine de préciser ce que vaut ce produit. Cependant, lorsque $H \lhd K$, cette loi peut être explicitée. On a en effet $hkh'k' = (hkh'k^{-1})(kk')$ d'où, puisque $hkh'k^{-1} \in H$ et $kk' \in K$,

$$(h,k) * (h',k') = (hkh'k^{-1}, kk')$$

Ce que nous voudrions maintenant, c'est obtenir un procédé pour construire un groupe G à partir de deux groupes H et K de manière à retrouver une situation comparable à celle que l'on vient d'étudier. Mais pour connaître $kh'k^{-1}$, il faut savoir comment H et K se "mélangent" dans G. Faut-il donc connaître à l'avance l'objet que l'on veut construire, auquel cas la méthode ne serait guère productive ? En fait non. On remarque en effet que, dans notre étude, l'application

$$\begin{array}{rccc} \Phi \ : & K & \to & \mathrm{Aut}(H) \\ & k & \mapsto & \Phi_k = h \mapsto khk^{-1} \end{array}$$

est un morphisme et que le produit est donné par $(h,k) * (h',k') = (h\Phi_k(h'), kk')$. On a coutume de dire que le produit de h et h' est « tordu » par Φ_k.

Il est maintenant facile de vérifier que, réciproquement, si H et K sont deux groupes et $\Phi : K \to \mathrm{Aut}(H)$ un morphisme (dont on note Φ_k l'image de k pour faciliter la lecture), alors on munit $G = H \times K$ d'une structure de groupe en posant

$$(h,k) * (h',k') = (h\Phi_k(h'), kk')$$

De plus, $H' = H \times \{e_K\}$ et $K' = \{e_H\} \times K$ sont des sous-groupes de G et l'on a bien $H' \lhd G$, $H' \cap K' = \{e_G\}$, $H'K' = G$. Ce groupe est qualifié de produit semi-direct de H par K et noté $H \rtimes_\Phi K$.

Il n'y a donc pas un groupe semi-direct de H par K mais des produits semi-directs (autant que de morphismes de K dans $\mathrm{Aut}(H)$).

Considérons par exemple le groupe S_3. Posons $c = (1,2,3)$ et $\tau = (1,2)$. Alors $H =< c >= A_3 \lhd S_3$ est d'ordre 3 et $K =< \tau >$ est d'ordre 2. Comme $H \cap K = \{e\}$, on a $|HK| = |H||K| = 6$ d'où $HK = S_3$. Ainsi, S_3 est un produit semi-direct de H par K. Le morphisme $\Phi : K \to \mathrm{Aut}(H)$ est complètement déterminé par : $\Phi_\tau(c) = (\tau(1), \tau(2), \tau(3)) = c^{-1}$.
Comme $H \simeq \mathbb{Z}/3\mathbb{Z}$ par $K \simeq \mathbb{Z}/2\mathbb{Z}$, on peut écrire

$$S_3 \simeq \mathbb{Z}/3\mathbb{Z} \rtimes_\Phi \mathbb{Z}/2\mathbb{Z}$$

où Φ est l'unique morphisme non trivial de $\mathbb{Z}/2\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/3\mathbb{Z}) \simeq \mathbb{Z}/2\mathbb{Z}$.
Plus généralement, en notant D_n le groupe diédral d'indice n (qui est d'ordre $2n$), on a

$$D_n \simeq \mathbb{Z}/n\mathbb{Z} \rtimes_\Phi \mathbb{Z}/2\mathbb{Z}$$

où $\Phi : \mathbb{Z}/2\mathbb{Z} \to \mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ est complètement déterminé par la relation $\Phi_{[1]_2}([1]_n) = [-1]_n$.

Une autre façon d'aborder la problématique du produit semi-direct est la suivante. Soit G un groupe et H un sous-groupe distingué de G. Est-il possible de reconstituer G si l'on se donne H et G/H ? En d'autres termes, étant donnés deux groupes H et K, quels sont les groupes G contenant un sous-groupe distingué H' isomorphe à H et tel que G/H' soit isomorphe à K ? Ce problème est soluble (dans le bourgogne) mais complexe (il est traité par exemple dans l'excellent (et méconnu) « Algebra » de Pierre Grillet, Wiley-Interscience). Si néanmoins, on recherche seulement les groupes G dans lesquels G/H peut-être « relevé » dans G, c'est-à-dire tels qu'il existe un sous-groupe K de G pour lequel l'application

$$\begin{array}{rccc} \pi|_K : & K & \to & G/H \\ & x & \mapsto & [x]_H \end{array}$$

est un isomorphisme, alors la solution est claire, puisque l'on a dans ce cas $H \lhd G$, $HK = G$, $H \cap K = \{e_G\}$. Ce sont tous les produits semi-directs de H par K.

2.2 Théorèmes de Sylow

Soient G un groupe et p un diviseur de $|G|$. Posons $|G| = p^s m$, $\mathrm{pgcd}(p, m) = 1$. On appelle p-Sylow de G tout sous-groupe d'ordre p^s.
Le théorème de Sylow affirme l'existence, pour tout p premier divisant $|G|$ d'un p-Sylow (noter qu'il est faux que, pour tout diviseur d de $|G|$, $|G|$ admette un sous-groupe d'ordre d ; par exemple A_4 n'admet aucun sous-groupe d'ordre 6). Il est même beaucoup plus précis :

Théorème 1 *(Sylow) Soit G un groupe et p un diviseur premier de $|G|$.*

1. *G admet un p-Sylow.*
2. *Deux p-Sylow quelconques de G sont conjugués.*
3. *Tout sous-groupe de G d'ordre p^r (où $r \leqslant s$) est contenu dans un p-Sylow.*
4. *Le nombre k de p-Sylow divise m et l'on a $k \equiv 1\ [p]$.*

1. On prouve le premier point par récurrence sur $n = |G|$. Si $|G| = p$, G est lui-même un p-Sylow. Supposons $|G| > p$. On posera $|G| = p^s m$, $\mathrm{pgcd}(p, m) = 1$. Considérons l'action par conjugaison

de G sur lui-même : $g.h = ghg^{-1}$. Les orbites sont les classes de conjugaison et les orbites réduites à un point sont les éléments du centre $Z(G)$ de G. L'équation aux classes donne :

$$|G| = |Z(G)| + \sum_{g \in A'} |C(g)|$$

où l'on note $C(g)$ la classe de conjugaison de g et A' une partie de G contenant un et un seul élément par classe de conjugaison non réduite à un point. Si, pour un certain $g \in A'$, on a $|C(g)|$ premier à p alors, puisque $|G| = [G : G_g]|G_g|$ et $|C(g)| = [G : G_g]$, on a $|G_g| = p^s m'$, où m' est un diviseur strict de m. Par l'hypothèse de récurrence, G_g admet un p-Sylow qui est aussi un p-Sylow de G. On peut donc supposer $p||C(g)|$ pour tout g. Il en résulte $p||Z(G)|$, d'où l'existence de $a \in Z(G)$ d'ordre p. On a $< a > \lhd G$ et $G/ < a >$, qui est un groupe d'ordre $p^{s-1}m < n$, admet un p-Sylow H (si $s = 1$, on prend $H = \{e\}$). Si on note $\pi : G \to G/ < a >$ la surjection canonique, $\pi^{-1}(H)$ est un p-Sylow de G.

2. Soient maintenant H et K deux p-Sylow. Posons $X = G/H$ (ensemble des classes à gauche modulo H) et faisons opérer K sur X par translation à gauche : $k.(gH) = kgH$. Le stabilisateur de gH est $K_{gH} = K \cap gHg^{-1}$ et l'équation aux classes indique

$$|G/H| = \sum_{h \in A'} [K : K_{gH}]$$

où $A' \subset H$ est telle que les gH, $g \in A'$, forment un système de représentants distincts des orbites. Comme p ne divise pas $|G/H|$, il existe $g \in A'$ tel que p ne divise pas $[K : K_{gH}]$, c'est-à-dire, puisque K est d'ordre p^s, $K_{gK} = K$, d'où $K \subset gHg^{-1}$.

3. Soit H un p-Sylow et K un sous-groupe d'ordre p^r, $r \leqslant s$. La même preuve que dans le point 2 montre qu'il existe $g \in G$ tel que $K \subset gHg^{-1}$.

4. Soit maintenant X l'ensemble des p-Sylow de G. Le groupe G opère sur X par conjugaison : $g.H = gHg^{-1}$. Comme l'opération est transitive (point 2), on a $|X| = [G : G_H]$ d'où $|X|$ divise $|G|$.

   Considérons maintenant un p-Sylow particulier H et restreignons à H cette action sur X. Comme H est un groupe d'ordre p^s, l'équation aux classe donne

$$|X| \equiv |X^H| \ [p]$$

   (où X^H est l'ensemble des points de X fixes par tous les éléments de H). Or, d'une part $H \in X^H$ de manière évidente, d'autre part, si $K \in X^H$, alors en notant N le sous-groupe de G engendré par $H \cup K$, H et K sont deux p-Sylow de N, donc sont conjugués dans N par le point 2, tandis que $K \lhd N$ (car $hKh^{-1} = K$ pour tout $h \in H$), d'où $K = H$. Ainsi, $|X^H| = 1$ et $|X| \equiv 1 \ [p]$.

2.3 Groupes de petit cardinal

On détermine ici tous les groupes d'ordre au plus 15*. On donne, quand c'est possible (*$n \leqslant 11$*), des démonstration très élémentaires (c'est-à-dire sans le théorème de structure des groupes abéliens finis, sans produit semi-direct ni sous-groupes de Sylow), mais aussi des preuves plus sophistiquées.*

• Groupes d'ordre 2, 3, 5, 7, 11 et 13

C'est vite fait : un groupe d'ordre p premier est isomorphe à $\mathbb{Z}/p\mathbb{Z}$.

• Groupes d'ordre 4, 9 (et p^2)

Un groupe d'ordre p^2, p premier, est abélien (exercice 4). S'il n'est pas cyclique, tous les éléments

distincts du neutre sont d'ordre p. Soit, dans ce cas, $a \neq e$ et $b \notin < a >$. Ce sont deux éléments d'ordre p et $< a > \cap < b >= \{e\}$. Donc $| < a >< b > | = p^2$, d'où $< a >< b >= G$ puis $G \simeq < a > \times < b > \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$. Les seuls groupes d'ordre p^2 sont donc $\mathbb{Z}/p^2\mathbb{Z}$ et $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$

• Groupes d'ordre 6, 10 et 14 (et $2p$).
Soit G d'ordre 6.
Preuve élémentaire : Si G admet un élément d'ordre 6, il est isomorphe à $\mathbb{Z}/6\mathbb{Z}$.
Sinon, les éléments de G sont d'ordre 1, 2 ou 3. On sait (lemme de Cauchy, voir exercice 14) que G admet un élément a d'ordre 3 et un élément b d'ordre 2. Si $ab = ba$, alors ab est d'ordre 6, ce qui contredit l'hypothèse. Donc $ab \neq ba$. Or $H =< a >$ étant d'ordre 3 et b d'ordre 2, on a $b \notin H$, d'où $G = H \cup bH = \{e, a, a^2, b, ba, ba^2\}$. Pour « connaître » la loi de G, il suffit de savoir à quel élément de cette liste est égal ab. Or $G = H \cup Hb$ donc $bH = Hb$ (voir exercice 2) et $ab \in \{b, ba, ba^2\}$. Or $ab = b$ est évidemment exclu, ainsi que $ab = ba$. Donc $ab = ba^2$. On peut alors « remplir » d'au plus une manière la table de la loi du groupe, ce qui montre qu'il existe au plus un groupe non abélien d'ordre 6 (attention, à ce stade, rien n'assure de l'existence d'une telle loi). Comme on connaît un tel groupe, à savoir S_3, on peut conclure que S_3 est, à isomorphisme près, l'unique groupe non abélien d'ordre 6.

Preuve plus élaborée : Soient a d'ordre 3 et b d'ordre 2. On pose $H =< a >$, $K =< b >$. On a $H \lhd G$ car $[G : H] = 2$ et $H \cap K = \{e\}$, $HK = G$. Donc G est un produit semi-direct de $\mathbb{Z}/3\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$. Il n'en existe que deux, le produit direct (cas $\forall k\ \Phi_k = \mathrm{Id}_{\mathbb{Z}/3\mathbb{Z}}$ avec les notations utilisées dans l'exposé) qui donne $\mathbb{Z}/6\mathbb{Z}$ et l'autre, qui donne S_3.

Cette preuve s'adapte à la détermination des groupes d'ordre $2p$, p premier impair : Il existe a d'ordre p et b d'ordre 2. On pose $H =< a >$, $K =< b >$. On a $H \lhd G$ car $[G : H] = 2$ et $H \cap K = \{e\}$, $HK = G$. Donc G est un produit semi-direct de $\mathbb{Z}/p\mathbb{Z}$ par $\mathbb{Z}/2\mathbb{Z}$. Or $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$ est isomorphe à $\mathbb{Z}/(p-1)\mathbb{Z}$ et il n'y a exactement deux morphismes de $\mathbb{Z}/2\mathbb{Z}$ dans $\mathbb{Z}/(p-1)\mathbb{Z}$. Donc il y a deux morphismes de $\mathbb{Z}/2\mathbb{Z}$ dans $\mathrm{Aut}(\mathbb{Z}/p\mathbb{Z})$. L'un est le morphisme trivial, l'autre envoie l'élément non nul de $\mathbb{Z}/2\mathbb{Z}$ sur $x \mapsto -x$ (unique automorphisme d'ordre 2 de $\mathbb{Z}/p\mathbb{Z}$). Ainsi il y a deux groupes d'ordre $2p$. Le premier est $\mathbb{Z}/2p\mathbb{Z}$, le second n'est autre que le groupe diédral D_p.

Noter qu'il est tout à fait possible de présenter cette preuve sans faire explicitement allusion au produit semi-direct. On écrit $G = H \cup bH = \{e, a, a^2, \ldots, a^{p-1}, b, ba, ba^2, \ldots, ba^{p-1}\}$. Pour « connaître » la loi de G, il suffit de savoir à quel élément de cette liste est égal ab. Or $G = H \cup Hb$ donc $bH = Hb$ (voir exercice 2) et $ab \in \{b, ba, ba^2, \ldots, ba^{p-1}\}$. De plus, $x \mapsto b^{-1}xb$ est un isomorphisme de H dont le carré $x \mapsto b^{-2}xb^2 = x$ est l'identité. Or les isomorphisme de H sont de la forme $x \mapsto x^j$, $j \in \{1, 2, \ldots, p-1\}$ et ceux dont le carré vaut Id_H sont Id_H et $x \mapsto x^{-1}$. Donc $b^{-1}ab = a$ ou $b^{-1}ab = a^{-1} = a^{p-1}$ et $ab = ba$ ou $ab = ba^{p-1}$. Dans le premier cas, le groupe est isomorphe à $\mathbb{Z}/p\mathbb{Z}$, dans le second il est isomorphe à D_p.

• Groupes d'ordre 8.
On connaît $\mathbb{Z}/8\mathbb{Z}$, $\mathbb{Z}/4Z \times \mathbb{Z}/4Z$, $(\mathbb{Z}/2Z)^3$, D_4 (groupe diédral d'indice 4) et Q (groupe « quaternionique »). Rappelons des présentations de D_4 et Q.
Le groupe D_4 est le groupe des isométries du carré. Il est engendré par la rotation r d'angle $\pi/4$ et une symétrie orthogonale s (par rapport à une droite) laissant invariant le carré et l'on a

$$D_4 = \{e, r, r^2, r^3, s, sr, sr^2, sr^3\}$$

Le groupe Q est un sous-groupe du groupe des inversibles de l'algèbre des quaternions :

$$Q = \{1, -1, i, -i, j, -j, k, -k\}$$

et l'on a $ij = -ji = k$, $jk =_k j = i$ et $ki = -ik = j$ (l'associativité et le fait que $-1 \in Z(Q)$ permette de trouver tous les autres produits).
On va vérifier que ces cinq groupes sont les seuls groupes d'ordre 8.

Soit G d'ordre 8. Supposons G non cyclique. Si $\forall x \in G,\ x^2 = e$ alors $(xy)^2 = e$ d'où $xy = y^{-1}x^{-1} = yx$ et G est abélien. Il apparaît alors naturellement muni d'une structure de $\mathbb{Z}/2\mathbb{Z}$-espace vectoriel, d'où $G \simeq (\mathbb{Z}/2\mathbb{Z})^3$.
Sinon, G admet un élément a d'ordre 4. Posons $H =< a >$. On a $[G : H] = 2$ donc $H \lhd G$. S'il existe un élément b d'ordre 2 dans $G \setminus H$, on peut continuer la démonstration comme dans le cas d'un groupe d'ordre $2p$ et G est isomorphe à $\mathbb{Z}/4\mathbb{Z}$ ou à D_4. Sinon, tout élément de $G \setminus H$ est d'ordre 4. Dans ce cas, puisque $x \notin H \implies x^2 \in H$ (car H est d'indice 2), on a $\forall x \in G \setminus H, x^2 = a^2$. Fixons $b \in G \setminus H$. On a $G = \{e, a, a^2, a^3, b, ba, ba^2, ba^3\}$ et $b^2 = a^2$. Il suffit maintenant de savoir à quel élément de cette liste est égal ab pour connaître la loi du groupe. Or $b^{-1}ab$ a même ordre que a. Si $b^{-1}ab = a$, alors $ab = ba$, le groupe est abélien et $(ab)^2 = a^2b^2 = e$, ce qui contredit l'hypothèse selon laquelle $G \setminus H$ ne contient pas d'élément d'ordre 2. Donc $b^{-1}ab = a^3$ et $ab = ba^3$. On reconnaît ici la loi de Q (en identifiant a et i ainsi que b et j).

• Groupes d'ordre 12.
Exercice 16.

• Groupes d'ordre 15.
On utilise ici les théorèmes de Sylow. Soit G d'ordre 15. Le nombre de 5-Sylow (c'est-à-dire, ici, de sous-groupes d'ordre 5) divise 3 et est congru à 1 modulo 5. Donc il vaut 1. Ainsi, G admet un unique 5-Sylow H, lequel est donc un sous-groupe distingué. Par ailleurs, G admet un 3-Sylow K (c'est-à-dire, ici, un sous-groupe d'ordre 5). On a $K \cap H = \{e\}$ d'où, puisque $|H||K| = |G|$, $HK = G$. Ceci montre que G est un produit semi-direct de H par K. Or $\mathrm{Aut}(H) \simeq \mathbb{Z}/4\mathbb{Z}$ et le seul morphisme de K dans $\mathrm{Aut}(H)$ est le morphisme trivial. Donc $G \simeq H \times K \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \simeq \mathbb{Z}/15\mathbb{Z}$.

Voici le tableau récapitulatif des groupes d'ordre inférieur à 15 :

2	$\mathbb{Z}/2\mathbb{Z}$
3	$\mathbb{Z}/3\mathbb{Z}$
4	$\mathbb{Z}/4\mathbb{Z}$ $(\mathbb{Z}/2\mathbb{Z})^2$
5	$\mathbb{Z}/5\mathbb{Z}$
6	$\mathbb{Z}/6\mathbb{Z}$ $S_3 \simeq D_3$
7	$\mathbb{Z}/7\mathbb{Z}$
8	$\mathbb{Z}/8\mathbb{Z}$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$ $(\mathbb{Z}/2\mathbb{Z})^3$ D_4 Q
9	$\mathbb{Z}/9\mathbb{Z}$ $(\mathbb{Z}/3\mathbb{Z})^2$
10	$\mathbb{Z}/10\mathbb{Z}$ D_5
11	$\mathbb{Z}/11\mathbb{Z}$
12	$\mathbb{Z}/12\mathbb{Z}$ $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$ D_6 A_4 T
13	$\mathbb{Z}/13\mathbb{Z}$
14	$\mathbb{Z}/14\mathbb{Z}$ D_7
15	$\mathbb{Z}/15\mathbb{Z}$

3 Exercices

1. Soit G un groupe. Montrer que $\mathrm{Int}(G)$ (groupe des automorphismes intérieurs de G) est un sous-groupe distingué de $\mathrm{Aut}(G)$ (groupes des automorphismes de G).
2. Soit G un groupe et H un sous-groupe d'indice 2. Prouver $H \lhd G$.
3. Soient G un groupe fini, p le plus petit diviseur premier de G, et H un sous-groupe d'indice p. On va montrer que H est distingué dans G. Pour cela, on introduit l'ensemble G/H des classes à gauche, et on définit une action de G sur G/H en posant $g.(xH) = gxH$. Montrer que l'image de cette action (en tant qu'application de G dans $S(G/H)$) est de cardinal p. Conclure en montrant que le noyau de cette action est H.
4. Soit $Z(G) = \{g \in G; \forall h \in G, gh = hg\}$ le centre de G.
   (a) Montrer que $Z(G)$ est un sous-groupe distingué de G.
   (b) Montrer que si $G/Z(G)$ est cyclique, alors G est abélien (et donc $Z(G) = G$).
   (c) Montrer que si G est un p-groupe, alors $Z(G)$ n'est pas trivial (ie pas réduit au neutre). On pourra considérer l'action par conjugaison de G sur lui-même.
   (d) Montrer qu'un groupe d'ordre p^2, p premier, est abélien.
5. Soient G un groupe, H et K deux sous-groupes de G. On suppose $H \lhd G$, $K \lhd G$, $H \cap K = \{e\}$. Prouver $\forall h \in H, \forall k \in K,\ hk = kh$ (moralité : si G est le produit semi-direct (« interne ») de H par K et de K par H alors c'est le produit direct).
6. Montrer que les seuls morphismes de S_n dans $\mathbb{C}^*$ (ie les caractères de S_n) sont le morphisme trivial et la signature.
7. Montrer que A_n est engendré par les 3-cycles.
8. Donner un représentant de chaque classe de conjugaison de S_3 puis de S_4. Déterminer, à conjugaison près, tous les sous-groupes de S_3 puis de S_4. Mêmes questions avec A_4 (attention il y a un piège...).
9. Montrer que A_5 est simple (c'est-à-dire que ses sous-groupes distingués sont triviaux).
10. Montrer que A_n est l'ensemble des carrés de S_n. En déduire qu'un automorphisme de S_n conserve la signature.
11. Montrer que, pour $n \neq 6$, les automorphismes de S_n sont tous intérieurs (on pourra chercher une caractérisation algébrique - par opposition à géométrique - des transpositions).
12. Soit E un plan euclidien. Déterminer tous les sous-groupes finis de $O(E)$ (on pourra utiliser l'exercice 2).
13. Soit C l'ensemble des sommets d'un cube de $\mathbb{R}^3$ euclidien. Déterminer le groupe des isométries laissant invariant le cube. On pourra commencer par considérer l'action naturelle de G sur C, vérifier qu'elle est transitive, identifier le stabilisateur d'un sommet et en déduire l'ordre de G. Même question avec un tétraèdre.
14. Soit G un groupe fini et p un diviseur premier de son ordre. On pose $X = \{(x_0, x_1, \ldots, x_{p-1}) \in G;\ x_0x_1 \ldots x_{p-1} = e\}$. Évaluer $|X|$ puis, en considérant l'action de $\mathbb{Z}/p\mathbb{Z}$ sur X définie par $k.(x_0, x_1, \ldots, x_p) = (x_k, x_{k+1}, \ldots, x_{k+p-1})$ (les indices sont additionnés modulo p), montrer que G admet un élément d'ordre p (lemme de Cauchy).
15. *Les colliers de Polya.* Soient $n \in \mathbb{N}^*$ et p un entier premier. On considère un ensemble C de n couleurs et des colliers constitués de p perles, chacune pouvant être coloriée de l'une des n

couleurs. Deux colliers sont considérés comme étant identiques lorsqu'on obtient l'un à partir de l'autre par rotation (mais pas par symétrie...). Combien existe-t-il de tels colliers ? Même question, p n'étant plus supposé premier.

16. On détermine ici les groupes d'ordre 12. Soit G un tel groupe. Par le théorème de Sylow, G admet un sous-groupe H d'ordre 4 et un sous-groupe K d'ordre 3.
    (a) Montrer que si K n'est pas distingué dans G, alors G contient 4 sous-groupes d'ordre 3. En déduire que, dans ce cas, H est distingué dans G.
    (b) Montrer que G est isomorphe à l'un des groupes suivants : $\mathbb{Z}/12\mathbb{Z}$, $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/6\mathbb{Z}$, D_6, A_4, $T = \mathbb{Z}/3\mathbb{Z} \rtimes_\Phi \mathbb{Z}/4\mathbb{Z}$ (préciser Φ).

17. Dans cet exercice, on cherche les sous-groupes fini de $O^+(E)$, où E est un espace euclidien de dimension 3. Soit G un tel sous-groupe. On note S la sphère unité de E et pose
$$X = \{x \in S;\ \exists g \in G \setminus \{e\}; g.x = x\}$$
    (a) Montrer que X est fini, stable par $x \mapsto -x$, et que G opère naturellement sur X.
    (b) Soit $x \in X$. Montrer $G_x = G_{-x}$ et prouver que G_x est cyclique. Que dire s'il existe un point fixe commun à tous les éléments de G ? Dans la suite, on suppose que ce n'est pas le cas.
    (c) Soient p le nombre d'orbites, $\omega_1, \dots, \omega_p$ les orbites et $n_i = \dfrac{|G|}{|\omega_i|}$ (n_i est l'ordre du stabilisateur d'un élément de ω_i). Prouver :
$$\sum_{i=1}^{p} \left(1 - \frac{1}{n_i}\right) = 2 - \frac{2}{|G|}$$
    (d) En déduire $p = 3$, puis, en supposant par exemple $n_1 \leqslant n_2 \leqslant n_3$, $n_1 = 2$ et $n_2 \in \{2, 3\}$.
    (e) Conclure à l'une des possibilités suivante :
        1) $n_1 = 2$, $n_2 = 2$, $|G|$ pair et $n_3 = \dfrac{1}{2}|G|$.
        2) $n_1 = 2$, $n_2 = 3$, $n_3 = 3$, $|G| = 12$.
        3) $n_1 = 2$, $n_2 = 3$, $n_3 = 4$, $|G| = 24$.
        4) $n_1 = 2$, $n_2 = 3$, $n_3 = 5$, $|G| = 60$.
    (f) On se place dans le cas **1)**. Montrer qu'il existe $a \in S$ tel que $\omega_3 = \{a, -a\}$ et décrire G (on prouvera que G est isomorphe au groupe dièdral).
    (g) On se place dans le cas **2)**. Montrer que les éléments de ω_2 n'appartiennent pas à un même plan affine, puis que G est isomorphe au groupe des permutations paires de l'ensemble ω_2. En déduire que les élément de ω_2 sont les sommet d'un tétraèdre et décrire G.
    (h) On se place dans le cas **3)**.
    (i) On se place dans le cas **4)**. Montrer que G est isomorphe à A_5 (on peut prouver que ω_5 est un icosaèdre (polyèdre régulier admettant 12 sommets, 30 arêtes et dont les 20 faces sont des triangles et que G est le groupes des isométries le laissant invariant).