Introduction à la Théorie des Groupes
Deuxième Partie

Farouk Boucekkine

http://dma.ens.fr/culturemath

Dans cette Seconde Partie, nous allons détailler certaines notions vues dans la Première Partie, et ouvrir des perspectives d'appronfondissement.

Comme nous touchons à une partie plus "technique" du sujet, nous entrerons moins dans les détails que dans la première partie, nous contentant souvent de donner des énoncés précis sans démonstration, et une référence pour aller plus loin si le lecteur le désire.

Dans le même soucis de concision, et pour ne pas trop nous disperser, nous avons pris le parti de nous cantonner, pour les exemples, aux groupes *finis* (en revanche, les énoncés et définitions des notions sont donnés en toute généralité.)

En effet, ces exemples ont l'avantage de ne pas nécessiter de connaissances hors du champ des groupes, contrairement, par exemple, au groupe linéaire , capital mais qui implique des connaissances d'algèbre linéaire qu'il serait fastidieux de développer ici.

Par ailleurs, nous allons survoler - sans entrer dans les détails - divers développements plus récents ("Botanique" des groupes, Représentations) et applications historiques qui font le grand intérêt de cette théorie (équation polynômiales et topologie algébrique).

Références

[1] Daniel Perrin, *Cours d'algèbre*, Ed. Ellipses-Marketing. (La référence en matière de cours d'algèbre complet... et très lisible)

[2] Jean-Pierre Serre, *Construction des polygones réguliers*, Ed. hermann (ou Springer Verlag... en Anglais !)

[3] Ian Stewart, *Ah, les beaux groupes*, Ed. Belin (c'est une BD très amusante et instructive)

[4] Ian Stewart, *Galois Theory*, Ed. Chapman and Hall (en Anglais... mais très bien)

[5] Jean-Pierre Escoffier, *Théorie de Galois*, Ed. Dunod (cours et exercices corrigés).

[6] Rached Mneimné et Frédéric Testard, *Introduction à la théorie des groupes de Lie classiques*, Ed. Hermann (pour l'aspect géométrico-topologique que nous n'avons pas pu même effleurer ici)

[7] Claude Godbillon, *Eléments de topologie algébrique*, Ed. Hermann

[8] Hermann Weyl, Symétrie et mathématique moderne, Ed. Flammarion.

Table des matières

1 Quelques exemples plus approfondis

1.1 Groupes monogènes et groupes abéliens

Dans la Première Partie, nous avons vu la notion de groupe engendré par une partie, et en particulier par un singleton. Regardons donc à présent plus en détail les groupes les plus simples que l'on puisse considérer, les groupes engendrés par un seul élément.

Définition 1.1.1 *Un groupe* monogène *est un groupe engendré par un de ses éléments. Si, de plus, il est fini, on dit alors qu'il est* cyclique.

Exemple 1.1.2 $\mathbb{Z}$ *est monogène, car engendré par* 1. *Pour tout* $n \in \mathbb{N}$, *le groupe* C_n *est cyclique, car engendré par* $e^{\frac{2i\pi}{n}}$ *et fini.*

Un groupe monogène est toujours de la forme $\langle x \rangle := \{x^k, k \in \mathbb{Z}\}$ où x est un de ses générateurs. Il est donc forcément abélien car

$$\forall k, l \in \mathbb{N},\ x^k.x^l = x^k + l = x^l.x^k.$$

Attention, il peut y avoir plusieurs générateurs ! par exemple dans $C_3 = \{1, j, j^2\}$, j comme j^2 sont générateurs.

Remarque 1.1.3 *Notons également que, dans le cas des groupes cycliques, l'écriture* x^k *n'est pas unique, puisque*

$$\forall n \in \mathbb{Z}, x^{k+n.o(x)} = x^k$$

où $o(x)$ *est l'ordre de* x. *Par exemple, dans* C_3, $j^2 = j^5 = j^8 = j^{-1} = \ldots$.

A présent, la propriété suivante nous montre que les exemples ci dessus sont en fait, *à isomorphisme près*, les seuls !

Propriété 1.1.4 *Si* $\langle x \rangle$ *et* $\langle y \rangle$ *sont deux groupes cycliques de même cardinal (c'est à dire que* x *et* y *ont même ordre), alors ils sont isomorphes.*

Il suffit en effet de construire les isomorphismes réciproques $\phi : x^k \longmapsto y^k$ et $\psi : y^k \longmapsto x^k$ (attention ! il faut vérifier qu'ils sont bien définis : cf. **Remarque 1.1.3**.)

Ainsi, C_n est un "modèle" standard pour les groupes cycliques de cardinal n. Nous en verrons un autre au § **2.1** : $\mathbb{Z}/n\mathbb{Z}$.

Le résultat suivant résulte du précédent et est un bon exercice, arrivés à ce point du texte :

Corollaire 1.1.5 *Soit* p *un nombre premier, et* G *un groupe de cardinal* p. *Alors* $G \simeq C_p$.

Remarquons à présent que le produit d'un nombre fini de groupes monogènes est toujours un groupe abélien engendré par un nombre fini de générateurs. Par exemple $C_3 \times \mathbb{Z}^2$ est engendré par l'ensemble

$$\{(j,0,0);(1,1,0);(1,0,1)\}$$

Le théorème suivant nous permet de constater que la réciproque est vraie *à isomorphisme près* :

Théorème 1.1.6 *Soit G un groupe abélien engendré par un nombre fini d'éléments, alors il existe des entiers $l, n_1, \ldots, n_r, m_1, \ldots m_r$ tels que*

$$G \simeq (C_{n_1})^{m_1} \times \ldots (C_{n_r})^{m_r} \times \mathbb{Z}^l.$$

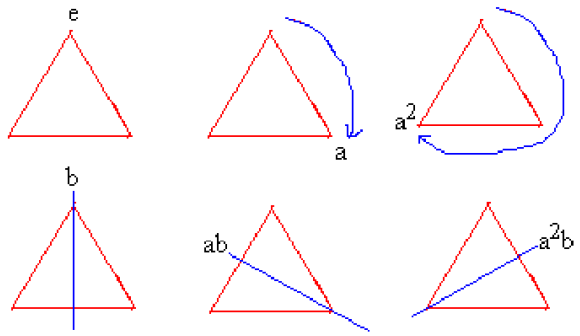
La démonstration de ce théorème se trouve par exemple dans [1].

1.2 Groupes diédraux

On va voir un exemple de groupe engendré par deux générateurs, et constater que c'est tout de suite plus compliqué qu'avec un seul...

On a vu au paragraphe **à préciser** le groupe des isométries du cube. En dimension 2, on peut s'intéresser d'une manière générale aux isométries d'un n-gone régulier de centre O.

Regardons le cas $n = 3$: les isométries qui conservent un triangle équilatéral sont les rotations et les les symétries axiales suivantes :



On constate aisément qu'on peut toutes les obtenir à partir d'une rotation et d'une réflexion (exercice !). Ce résultat se généralise à tout $n \in \mathbb{N}$:

Définition-Propriété 1.2.1 *Le groupe des isométries du n-gone, appelé* groupe diédral d'ordre n*, est le sous-groupe de $\mathcal{O}(\mathcal{P})$ engendré par une réflexion et une rotation laissant fixe le $n-$gone.*

Son cardinal est $2n$ (n réflexions et n rotations.)

On peut alors constater que ce groupe n'est pas abélien (dès que $n \geq 3$). Comme on peut toujours construire un groupe abélien à partir de deux générateurs, on peut en déduire que deux générateurs d'ordres donnés ne créent pas forcément un seul groupe à isomorphisme près comme c'était le cas pour les groupes monogènes.

Remarque 1.2.2 *Le cas de la dimension 3 est plus complexe : en effet on ne peut pas construire autant de solides réguliers qu'on veut. Il n'en existe que cinq : le tétraèdre, le cube, l'octogone, le dodécaèdre et l'icosaèdre. Ce résultat, connu sous la forme de conjecture "philosophique" depuis l'antiquité grecque, peut être démontré en utilisant la théorie des groupes !*

1.3 Le Groupe Symétrique $\mathfrak{S}_n$ et le Groupe Alterné $\mathfrak{A}_n$

Nous avons déjà vu la définition du groupe symétrique, considérons à présent les orbites de $\{1, ..., n\}$ sous l'action de $\mathfrak{S}_n$. On peut constater que, par définition, une permutation agit sur ses différentes orbites *indépendamment*, ce qui nous amène à considérer les permutations suivantes comme particulièrement dignes d'intérêt :

Définition 1.3.1 *Un* cycle *est une permutation n'ayant qu'une seule orbite non-triviale (i.e. ayant plus d'un élément). Cette orbite est appelée* support *du cycle*

Pour être plus précis, si $k \geq 2$, on appelle $k-$cycle un cycle dont le support a pour cardinal k.

Les $2-$cycles sont appelés transpositions.

Exemple 1.3.2 *L'élément de $\mathfrak{S}_6$ défini par*

$$1 \longmapsto 3,\ 2 \longmapsto 2,\ 3 \longmapsto 6,\ 4 \longmapsto 1,\ 5 \longmapsto 5,\ 6 \longmapsto 4$$

est un $4-$cycle, alors que celui qui est défini par

$$1 \longmapsto 3,\ 2 \longmapsto 1,\ 3 \longmapsto 2,\ 4 \longmapsto 6,\ 5 \longmapsto 5,\ 6 \longmapsto 4$$

n'est pas un cycle.

Le nom donné à ces permutations particulières ne doit rien au hasard ! Si σ est $k-$cycle de $\mathfrak{S}_n$, alors il existe k éléments de $\{1, \ldots, n\}$, *distincts*, tels que σ soit défini par :

$$\begin{array}{ccc} a_1 & \longmapsto & a_2 \\ a_2 & \longmapsto & a_3 \\ \vdots & & \vdots \\ a_{k-2} & \longmapsto & a_{k-1} \\ a_{k-1} & \longmapsto & a_k \\ a_k & \longmapsto & a_1 \end{array}$$

Son support est alors $\{a_1, \ldots, a_k\}$.

Notation 1.3.3 *Le $k-$cycle σ, de support $\{a_1, \ldots, a_k\}$ défini comme ci-dessus est noté*

$$\sigma = (a_1, a_2, \ldots, a_{k-1}, a_k)$$

Exemples 1.3.4

(i) Considérons dans $\mathfrak{S}_n$ la permutation où l'on se contente d'intervertir 1 et 2. C'est une transposition (i.e. un $2-$cycle), de support $\{1, 2\}$. On la note $(1, 2)$.

(ii) Le $4-$cycle vu dans l'**Exemple** précédent est noté $(1,3,6,4)$.

(iii) L'inverse d'un cycle $(a_1, a_2, \ldots, a_{k-1}, a_k)$ est le cycle $(a_k, a_{k-1}, \ldots, a_2, a_1)$.

Voyons a présent comment les cycles forment des "briques" de base pour construire les permutations.

Propriété 1.3.5 (Décomposition des permutations en produits de cycles)

i) Si c_1 et c_2 sont deux cycles de supports disjoints *alors $c_1.c_2 = c_2.c_1$.*

ii) Toute permutation $\sigma \in \mathfrak{S}_n$ se décompose de manière unique (à commutation près) en un produit

$$\sigma = c_1 \ldots c_r$$

où c_1,...,c_r sont des cycles à supports disjoints. Leurs supports sont exactement les orbites non-triviales de σ.

Exemple 1.3.6 *L'élément de $\mathfrak{S}_8$ défini par*

$$1 \longmapsto 3,\ 2 \longmapsto 1,\ 3 \longmapsto 2,\ 4 \longmapsto 6,\ 5 \longmapsto 8,\ 6 \longmapsto 4,\ 7 \longmapsto 5,\ 8 \longmapsto 7$$

est égal au produit $(1,3,2).(4,6).(7,5,8)$, ou à $(8,7,5).(4,6).(2,1,3)$ (mais pas à $(1,2,3).(4,6).(7,5,8)$!)

Cette décomposition permet de faciliter grandement les calculs, en particulier de conjugaison grâce au lemme suivant (à démontrer !) :

Lemme 1.3.7 *considérons le cycle $c = (a_1, \ldots, a_r) \in \mathfrak{S}_n$ et $\sigma \in \mathfrak{S}_n$, on a alors :*

$$\sigma.c.\sigma^{-1} \text{ est le cycle } (\sigma(a_1), \ldots, \sigma(a_r))$$

Exemples 1.3.8 *A vérifier !*

(i) $(1,2).(1,2,3).(1,2) = ...?$

(ii) Un $k-$cycle $(a_1, \ldots, a_k)$ est toujours conjugué au $k-$cycle "standard" $(1,2,3,\ldots,k-1,k)$.

Nous allons à présent nous intéresser à la parité des permutation, notion qui nécessite quelques préambules.

Considérons le *nombre d'inversions* d'une permutation $\sigma \in \mathfrak{S}_n$, c'est à dire le nombre

$$I(\Sigma) := |\{i \in \{1,\ldots,n\} \text{ tels que } \sigma(i) < i\}|\,.$$

Définition 1.3.9 *On dit qu'une permutation $\sigma \in \mathfrak{S}_n$ est* paire *si son nombre d'inversions est pair, et* impaire *dans le cas contraire.*

Exemples 1.3.10 *A vérifier !*

(i) La transposition $(1,2)$ est toujours impaire dans tous les $\mathfrak{S}_n$, $n \geq 2$. Que dire des autres transpositions ?

(ii) Le $3-$cycle $(1,2,3)$ est toujours pair dans tous les $\mathfrak{S}_n$, $n \geq 3$. Que dire des autres $3-cycles$?

(iii) Le $4-$cycle $(1,2,3,4)$ est toujours pair dans tous les $\mathfrak{S}_n$, $n \geq 4$. Que dire des autres $4-cycles$?

(iv) les permutations $(1,2)(3,4)$ et $(1,3)(2,4)$ sont paires dans tous les $\mathfrak{S}_n$, $n \geq 4$.

(v) les permutations $(1,2)(3,4,5)$ et $(1,3)(2,5,4)$ sont impaires dans tous les $\mathfrak{S}_n$, $n \geq 5$.

Considérons à présent l'application $\varepsilon : \mathfrak{S}_n \longrightarrow C_2,\ \sigma \longmapsto (-1)^{I(\sigma)}$, c'est à dire

$\sigma \longmapsto 1$ si σ est une permutation paire ;
$\sigma \longmapsto -1$ si σ est une permutation impaire ;

Définition-Propriété 1.3.11 *Pour $n \geq 2$, ε est un morphisme surjectif de $\mathfrak{S}_n$ dans C_2 appelé* signature. *Son noyau est appelé* groupe alterné *et noté $\mathfrak{A}_n$, il est donc composé des éléments pairs de $\mathfrak{S}_n$.*

La propriété essentielle sur cette question est la suivante. Elle va nous permettre de répondre aux questions posées dans l'**Exemple 1.3.10**.

Propriété 1.3.12 *La signature d'un $k-$cycle est $(-1)^{k+1}$.*

En effet, si σ est un $k-$cycle, alors il existe d'après l'**Exemple 1.3.8** une permutation τ telle que $\sigma = \tau.(1,2,3,\ldots,k-1,k).\tau^{-1}$. On a alors

$$\begin{aligned} \varepsilon(\sigma) &= \varepsilon(\tau.(1,2,3,\ldots,k-1,k).\tau) \\ &= \varepsilon(\tau).\varepsilon((1,2,3,\ldots,k-1,k)).\varepsilon(\tau)^{-1} \\ &= \varepsilon((1,2,3,\ldots,k-1,k)). \end{aligned}$$

Il reste à vérifier que $\varepsilon((1,2,3,\ldots,k-1,k)) = (-1)^{k+1}$, ce qui peut se faire par récurrence (par exemple en remarquant que $(1,2,3,\ldots,k-1,k) = (1,2,3,\ldots,k-1).(k-1,k).$)

Corollaire 1.3.13 *Par conséquent, pour connaître la parité d'une permutation, on la décompose en produit de cycles, et on multiplie les signatures de ces derniers.*

Exemple 1.3.14 *Avec ce qui a été vu dans ce paragraphe on peut déterminer le groupe $\mathfrak{A}_4$:*

$\mathfrak{A}_4$={ Id ; (1,2,3) ;(1,3,2) ;(1,2,4) ;(1,4,2) ;(1,3,4) ;(1,4,3) ;(2,3,4) ;(2,4,3) ;
(1,2)(3,4) ;(1,3)(2,4) ;(1,4)(2,3)}

2 Sous-groupes distingués. Groupes simples. Dévissage

Soient G un groupe et N un sous-groupe de G. Lorsqu'on a défini, au § **3** de la Première Partie, l'action de N sur G par translation à gauche, on a dit qu'on pouvait, sous certaines conditions, *transférer la structure de groupe de G sur l'ensemble G/N*. Explicitons à présent ces conditions.

2.1 Revoyons l'action au ralenti

Rappelons que N agit sur G par

$$\forall n \in N, \forall x \in G,\ n.x := nx.$$

G/N est alors l'ensemble des orbites de cette action. Une telle orbite alors notée Nx $(= \{nx,\ n \in N\})$, où l'on a choisi un *représentant* x de cette orbite (c'est à dire un de ses éléments).

Cependant, cette notation n'est absolument unique : si $x_0 = n_0 x$ avec $n_0 \in N$, on aura alors évidemment que les orbites Nx et Nx_0 sont égales, autrement dit que x_0 et x sont des représentants d'un même élément de G/N... Et c'est justement ce qui complique la tâche lorsque l'on veut mettre une structure de groupe *naturelle* sur G/N.

Que veut-on dire par *naturelle* ? On peut a priori poser de nombreuses structures de groupes sur un même ensemble : il suffit de le mettre en bijection avec un groupe déjà connu.

Ici, on ne veut pas prendre n'importe quelle structure, on en veut une qui ait un sens : G et G/N étant liés par l'application canonique $\Phi_N : G \longrightarrow G/N,\ x \longmapsto Nx$, il faut que la structure de G/N soit telle que Φ_N soit un morphisme de groupe, ce qui implique des conditions très strictes sur l'opération que l'on va donner à G/N. Notons "." cette opération et $e_{G/N}$ son élément neutre, on doit avoir :

$$\forall x \in G,\ \begin{cases} Nx.Ny = \Phi_N(x).\Phi_N(y) = \Phi_N(xy) = Nxy \\ e_{G/N} = \Phi_N(e_G) = Ne_G = N \end{cases}$$

On peut vérifier aisément qu'une loi vérifiant ces conditions vérifie automatiquement les axiomes d'une loi de groupe (cela découle du fait que G est un groupe).

Cependant, cette condition est nécessaire mais pas encore suffisante : en effet, poser $Nx.Ny := Nxy$ ne définit pas rigoureusement une opération sur G/N, car cela implique de choisir des représentants x et y dans les orbites Nx et Ny.

Or l'opération ne doit pas dépendre de ces choix arbitraires, et notre définition est donc légitime si et seulement si Nxy ne dépend pas des représentants choisi pour Nx et Ny.

Autrement dit, si $x' \in Nx$ et $y' \in Ny$ alors on doit avoir $x'y' \in Nxy$.

Or $x' \in Nx$ si et seulement si $\exists n \in N$ tel que $x' = n.x$ (de même $y' \in Ny \iff \exists m \in N$ tel que $y' = m.x$). Ainsi, notre définition est valide si et seulement si :

$$\forall x, y \in G, \forall n, m \in N,\ \exists l \in N \textit{ tel que } nxmy = lxy$$

Simplifiant à droite par y et à gauche par n on obtient l'expression équivalente :

$$\forall x \in G, \forall m \in N,\ \exists l \in N \textit{ tel que } xm = lx$$

ce qui équivaut à

$$\forall x \in G, \forall m \in N,\ xmx^{-1} \in N$$

ce que l'on note usuellement

$$\forall x \in G,\ xNx^{-1} \in N.$$

Voici donc une condition nécessaire et suffisante pour que l'on puisse définir une loi de groupe sur G/N par $Nx.Ny := Nxy$, sans qu'il y ait de problème de choix de représentant. C'est donc aussi la condition nécessaire et suffisante pour qu'on puisse mettre une structure de groupe sur G/N, *naturelle* au sens vu ci-dessus.

Maintenant, il est normal de se demander si cette condition est vérifiée par tout sous-groupe N de tout groupe G. La réponse est négative comme on peut s'en convaincre en considérant $G := \mathfrak{S}_3$ et $N := \langle (1,2) \rangle$. Prenant $x = (2,3) \in G$ et appliquant le **lemme 1.3.7** on obtient

$$x.(1,2).x^{-1} = (1,3) \notin N.$$

Il est donc désormais naturel de "distinguer" des autres sous-groupes ceux à partir desquels on peut fabriquer une structure naturelle sur G/N :

Définition 2.1.1 *Soit G un goupe et $N < G$, alors N est dit* distingué *ou* normal *dans G si*

$$\forall x \in G,\ x^{-1}.N.x \subset N$$

On note alors $N \lhd G$, et on appelle groupe quotient *l'ensemble G/N muni de l'opération*

$$xN.yN := xyN$$

et morphisme quotient *l'application*

$$\Phi_N : x \longmapsto xN.$$

Remarques 2.1.2 • *On peut montrer (exercice) que*

$$x^{-1}.N.x \subset N \iff x^{-1}.N.x = N.$$

• *Remarquons, comme nous l'avions annoncé dans* **l'Exemple 3.2.7** *de la Première Partie, que les sous-groupes distingués sont bien les points fixes de l'action par conjugaison de G sur l'ensemble $\mathcal{S}(G)$ de ses sous-groupes.*

Exemples 2.1.3 *A vérifier !*

(i) Si G est abélien, alors tous sous-groupes sont distingués.

(ii) A l'inverse, la plupart des sous-groupe d'un groupe non-abélien ne le sont pas. L'exemple typique (et généralisable à loisir) étant celui vu ci-dessus où $G := \mathfrak{S}_n$ et $N = \langle (1,2) \rangle$ pour $n \geq 3$.

(iii) Voyons à présent l'un des exemples les plus importants. Soit $n \in \mathbb{N}$, $n\mathbb{Z}$ est alors un sous-groupe de $\mathbb{Z}$, distingué puisque $\mathbb{Z}$ est abélien. Le groupe quotient $\mathbb{Z}/n\mathbb{Z}$ est alors un groupe cyclique à n éléments (donc $\mathbb{Z}/n\mathbb{Z} \simeq C_n$) . Ses éléments sont les *classes de congruences modulo n dans* $\mathbb{Z}$ et son générateur est la classe de 1.

(iv) Si N et K sont deux groupes alors il y a deux sous-groupes distingués naturels dans leur produit $N \times K$: $N \times \{e_K\}$ et $\{e_N\} \times K$.

Comme ces sous-groupes sont évidemment isomorphes respectivement à N et à K, on dira souvent, par un abus de langage fort commode, que N et K sont distingués dans $N \times K$.

Enfin, avec cet abus de langage, on a $N \times K/N \simeq K$ et $N \times K/K \simeq N$.

(v) On peut vérifier à la main en utilisant le **Lemme 1.3.7** (faites-le !), que $\{Id; (1,2)(3,4); (1,3)(2,4); (1,4)(2,3)\}$ est un sous-groupe distingué de $\mathfrak{A}_4$. Quel est le quotient ? (penser au **Corollaire 1.1.5**

(vi) On a toujours $\mathfrak{A}_n \lhd \mathfrak{S}_n$. En effet,

$$\forall x \in \mathfrak{S}_n, \forall \sigma \in \mathfrak{A}_n,\ \varepsilon(x^{-1}.\sigma.x) = \varepsilon(x)^{-1}.\varepsilon(\sigma).\varepsilon(x) = \varepsilon(\sigma) = 1.$$

Donc $\forall x \in \mathfrak{S}_n, x^{-1}.\mathfrak{A}_n.x \in An$.Ceci est un cas particulier de la proposition $fondamentale$ suivante (démonstration en exercice !).

Propriété 2.1.4 (i) *Soient $H < G$. Alors H est distingué dans G si et seulement s'il existe un groupe K et un morphisme $\varphi : G \longrightarrow K$ tel que*

$$Ker\ \varphi = H.$$

(ii) (Factorisation canonique) *Dans ce cas, on a alors*

$$Im\ \varphi \simeq G/H.$$

Indication pour démontrer la deuxième partie : on peut poser $\overline{\varphi} : G/H \longrightarrow Im\ \varphi$ qui à $Nx \in G/H$ associe $\varphi(x) \in Im\ \varphi$. Il faut alors **vérifier que cette définition ne dépend pas du choix du représentant x choisi !** Puis on montre que $\overline{\varphi}$ est injective et surjective.

Exemple 2.1.5 *Le groupe (isomorphe à C_n) des rotations qui préservent un $n-$gone régulier est distingué dans D_n. En effet, considérons l'application ω : $D_n \longrightarrow C_2$ défini par*

$$\begin{array}{ll} s \longmapsto 1 & \textit{si } s \textit{ préserve l'orientation} \\ s \longmapsto -1 & \textit{si } s \textit{ inverse l'orienation} \end{array}$$

ω est clairement un morphisme de groupes, et son noyau est constitué par les rotations, qui forment donc un sous-groupe distngué de D_n.

Commentaire 2.1.6 *La factorisation canonique, annoncée dans le* **Commentaire 3.3.4** *de la Première Partie, permet de voir de manière directe que, si $f : G \longrightarrow H$ est un morhisme de groupes, alors $|Ker\ f|.|Im\ f| = |G|$.*

Il existe de nombreux résultats sur les sous-groupes distingués. Bornons-nous, à citer l'un d'entre-eux, exercice classique dont nous nous servirons un peu plus loin dans ce texte.

Propriété 2.1.7 *Soient $H < G$ tels que $[G : H] = 2$ (c'est à dire, selon la* **Notation 3.3.1** *de la Première Partie), $|G/H| = 2$), alors $H \lhd G$.*

Notons que d'après le **Corollaire 1.1.5**, on a dans ce cas $G/H \simeq C_2$. C'est ce qui se produit pour les exemples $\mathfrak{A}_n \lhd \mathfrak{S}_n$ et $C_n \lhd D_n$.

2.2 Groupes simples, extensions et dévissage

Lorsqu'on a $N \lhd G$, on peut considérer que G est formé en "collant" N et G/N. Mais un tel collage est-il unique ? Autrement dit, pourrait-on recoller les groupes N et G/N et obtenir un groupe H *non-isomorphe à* G tel que $N \lhd H$ et $H/N \simeq G/N$?

Commentaire 2.2.1 *Observons le cas des espaces vectoriels de dimension finie (qui sont des groupes abéliens munis d'un surcroît de structure). Soient W un $K-ev$, et U un sous-ev de W, alors il existe toujours un sous-ev $V < W$, isomorphe à W/U tel que*

$$W = U \oplus V\ (\simeq U \times V).$$

Ainsi dans ce cas, le collage est unique.

Qu'en est-il dans le cas des groupes ? Remarquons tout de suite qu'on peut toujours recoller deux groupes N et K : il suffit de poser $G := N \times K$, et on a alors $N \lhd G$ et $G/N \simeq K$ comme vu précédemment.

Cependant, on peut parfois aussi recoller les groupes autrement : prenons $N = K = C_2$, on a alors $C_2 \lhd C_4$ et $C_4/C_2 \simeq C_2$ (vérifiez !). Donc C_4 et $(C_2)^2$ sont formés par recollement des mêmes groupes, or ils ne sont pas isomorphes (cf. Première Partie, **Exemple 2.4.4, (i)**) !

Ce qui fait la différence, ce sont les morphismes $C_2 \longrightarrow C_4 \longrightarrow C_2$ et $C_2 \longrightarrow (C_2)^2 \longrightarrow C_2$, qui ne s'agencent pas de la même manière. Ceci constitue le début de la théorie des *extensions de groupes*, qui étudie la manière de recoller les groupes ainsi, ou de *dévisser* un groupe en sous-groupes distingués et quotients.

Ainsi, les groupes qui n'ont pas de sous-groupes distingués font figure de "briques élémentaires" dans le dévissage des groupes. Ces groupes sont appelés *groupes simples*.

On peut remarquer que les groupes simples abéliens sont exactement les groupes de la forme C_p pour p premier. *Pourquoi ?*

Notons également, grâce à une propriété vue dans la Première Partie (*laquelle ? ?*), que, pour p premier, les C_p sont également les seuls $p-$groupes simples.

Une autre famille importante de groupes simples est donnée par le théorème suivant.

Théorème 2.2.2 *Les groupes $\mathfrak{A}_n$ sont simples pour $n \geq 5$.*

Voir [1] pour la démonstration de ce théorème.

3 Pour aller plus loin

3.1 Les réciproques au théorème de Lagrange

Commençons par nous poser une question simple : nous savons que le cardinal de sous-groupe d'un groupe fini G divise $|G|$, mais si l'on considère un entier q tel que $q \mid |G|$, existe-t-il forcément un sous-groupe de G de cardinal q ?

Considérons l'exemple suivant : le groupe $\mathfrak{A}_4$, d'ordre 12, a-t-il un sous-groupe d'ordre 6 ?

Nous allons montrer, par l'absurde, que ce n'est pas le cas : soit $H < G$ tel que $|H| = 6$.

Comme $[G : H] = 2$, d'après la **Propriété 2.1.7** on a $H \lhd G$. Par conséquent, si $\sigma \in H$, tous les conjugués de σ par un élément de $\mathfrak{A}_4$ seront dans H. Utilisons à présent la decription complète de $\mathfrak{A}_4$ vue dans l'**Exemple 1.3.14** pour obtenir une contradiction. Soit $\Sigma \in H$ tel que $\Sigma \neq Id$, alors σ est soit un $3-$cycle soit un produit de $2-$cycles à supports disjoints. Montrons que ces deux cas sont également impossibles :

- Si σ est un $3-$cycle, on peut obtenir tous les autres $3-$cycles de $\mathfrak{A}_4$ en conjugant σ par un élément bien choisi du groupe (calcul laissée au lecteur). On obtient ainsi que tous les $3-$cycles de $\mathfrak{A}_4$ sont dans H, donc $|H| \geq 9$, d'où une contradiction !
- De même, si σ est le produit de deux transpositions à supports disjoints, un calcul adéquat montre que les autres éléments de cette forme sont conjugués à σ. Or, $\{Id; (1,2)(3,4); (1,3)(2,4); (1,4)(2,3)\}$ forme un groupe K (isomorphe à $(C_2)^2$) de cardinal 4. comme $K < H$, on a donc $4 \mid |H|$ ce qui est aussi une contradiction.

Il existe cependant des réciproques partielles au théorème de Lagrange, les plus importantes étant les théorème de Cauchy et Sylow.

Théorème 3.1.1 (Cauchy) *Soit G un groupe fini, et p un nombre premier divisant $|G|$. Alors il existe un sous-groupe $H < G$ tel que*

$$|H| = p.$$

Théorème 3.1.2 (Sylow) *Soit G un groupe fini, et p un nombre premier tel que $|G| = p^n.m$, avec $m \wedge p = 1$. Alors il existe un sous-groupe $H < G$ tel que*

$$|H| = p^n.$$

Un tel sous-groupe est un $p-$sous-groupe maximal *(ou $p-sylow$) de G.*

De plus, tous les $p-$sous-groupes maximaux de G sont conjugués et leur nombre N_p vérifie les propriétés suivantes :

i) $N_p \equiv 1$ *mod. p ;*

ii) $N_p \mid m$.

Notons que, enconséquence de la deuxième partie de ce théorème, si $N_p = 1$, alors l'unique $p-$sylow de G est distingué.

Pour des démonstrations de ces théorèmes, voir [1].

3.2 Botanique des groupes : l'Atlas des groupes finis simples

Une fois qu'on a compris l'importance des groupes simples, comme briques fondamentales dans le dévissage des groupes, une question s'impose : peut-on déterminer tous les groupes finis simples ?

Ce travail herculéen a été achevé en 1982 après plus d'un siècle de calculs. Notons que cette classification, regroupée au sein de l'*Atlas des groupes finis simples*, a nécessité l'utilisation de l'informatique - ce qui fait que certains mathématiciens la récusent comme "impure"...

Théorème 3.2.1 (Conjecturé par Burnside en 1902, démontré par Feit et Thompson en 1963) *Tous les groupes finis simples non cycliques sont de cardinal pair !*

Théorème 3.2.2 *Les groupes finis simples se répartissent ainsi :*

i) Les groupes cycliques C_p, avec p premier.

ii) Les groupes alternés $\mathfrak{A}_n$ pour $n \geq 5$.

iii) Les groupes finis du type de Lie.

iv) Les 26 groupes sporadiques - nommés ainsi car ils ne correspondent pas à une répartition en "familles" cohérentes comme les autres.

Remarque 3.2.3 *La cardinal du* Monstre (de Fischer)*, le plus gros des groupes sporadiques, est :*

$2^{46} \times 320 \times 5^9 \times 7^6 \times 11^2 \times 13^3 \times 17 \times 19 \times 23 \times 29 \times 31 \times 41 \times 47 \times 59 \times 71 (\simeq 8.10^{53} \ldots)$.

3.3 Engendrer des groupes par générateurs et relations

On a vu qu'un groupe cyclique était défini par la donnée d'un élément générateur et de l'ordre de cet élément. D'une manière plus générale, les groupes peuvent être définis *par générateurs et relations*, c'est à dire en se donnant une famille de générateurs et des relations les liant.

Notation 3.3.1 *On notera* $G := \langle a_1, ..., a_n \mid relations \rangle$ *le groupe engendré par les générateurs* $a_1, ..., a_n$*, munis des relations notées (par exemple* $a_1^3 = 1$*,* $a_1.a_3 = a_3.a_1 ...$*). Il est usuel d'utiliser "1" pour l'élément neutre.*

Exemple 3.3.2 *Cette théorie étant à la fois difficile théoriquement et très calculatoire, nous nous contenterons de donner des exemples sans essayer de donner de définition générale, ni de prouver qu'une telle notation définit bien un groupe. Citons plusieurs manières d'engendrer certains des groupes que nous avons déjà rencontrés.*

(i) $\mathbb{Z}$ peut s'écrire $\langle a \mid \rangle$. **Attention !** En revanche, $\langle a, b \mid \rangle$ n'est pas $\mathbb{Z}^2$! En effet, on n'a pas stipulé que a et b commutaient ! Le groupe défini ainsi est appelé groupe libre à deux générateurs, c'est le groupe le plus général possible engendré par deux générateurs (et son étude est un domaine en soi, nous nous arrêterons donc là !).

En fait, $\mathbb{Z}^2 \simeq \langle a, b \mid ab = ba \rangle$.

(ii) De même $C_n \simeq \langle a \mid a^n = 1 \rangle$, $C_n \times C_m \simeq \langle a, b \mid a^n = 1, b^m = 1, ab = ba \rangle$.

Notons cependant qu'un résultat classique d'arithmétique, le *lemme chinois*, nous dit que, si $m \wedge n = 1$, alors $C_m \times C_n \simeq C_{mn}$. Nous obtenons donc sous ces hypothèses deux définitions par générateurs et relations différentes pour C_{mn} !

(iii) Le groupe diédral D_n peut être défini par

$$D_n = \langle s, t \mid s^2 = 1, t^2 = 1, stst = 1 \rangle$$

ou

$$D_n = \langle s, \rho \mid s^2 = 1, \rho^n = 1, \rho.s.\rho = s \rangle$$

Vérifiez ! (*indication :* deux réflexions dans le premier cas, une réflexion et une rotation dans le second)

(iv) Le groupe symétrique $\mathfrak{S}_n$ peut être défini par

$$\mathfrak{S}_n = \langle s_1, ..., s_{n-1} \mid \forall i, s_i^2 = 1,\ s_i.s_{i+1}.s_i = s_{i+1}.s_i.s_{i+1} \rangle$$

Les s_i sont les transpositions $(i, i+1)$. On peut noter aisément avec cette écriture que $\mathfrak{S}_3 \simeq D_3$.

On peut aussi engendrer $\mathfrak{S}_n$ avec deux générateurs : $(1, 2)$ et $(1, 2, 3, ..., n-1, n)$, mais les relations sont plus compliquées...

4 Les Groupes face au Reste du Monde

4.1 Associer un groupe à un objet mathématique

4.1.1 Equations algébriques et Groupe de Galois

La notion de groupe a initialement émergé des travaux d'Abel et de Galois sur la résolution par radicaux des équations polynômiales sur $\mathbb{Q}$. Les équations de degré 2, 3 et 4 avaient été résolues par des méthodes n'utilisant, outre les opérations élémentaires, que des extractions successives de racines nièmes. Abel, puis Galois ont montré que ce procédé (**résolution par radicaux** de l'équation) devenait insuffisant pour les équations de degré 5 ou plus.

Galois alla plus loin en introduisant ce qui deviendrait plus tard la notion de groupe afin de donner une condition nécessaire pour la résolution par radicaux d'une équation.

Le principe de sa théorie est, en termes modernes, d'associer un groupe à l'équation étudiée, le *Groupe de Galois de l'équation*. Ce groupe est contitué, en termes vagues, des transformations qu'on peut faire subir à l'équation sans en modifier la nature. Le génie de Galois consiste à avoir trouvé une condition opératoire sur ce groupe qui est nécessaire pour que l'équation de départ soit résoluble par radicaux.

Définition 4.1.1 *Un groupe* fini G *est dit* **résoluble** *s'il existe une suite de sous-groupes distingués*

$$\{0\} = G_0 \lhd G_1 \lhd G_2 \lhd \cdots \lhd G_{n-1} \lhd G_n = G$$

tels que

$$\forall i, 1 \leq i \leq n,\ G_i/G_{i-1} \text{ est abélien.}$$

Exemples 4.1.2

Tout groupe abélien est résoluble.

(ii) Tout groupe simple non-abélien n'est pas résoluble.

(iii) $\mathfrak{S}_3$,$\mathfrak{A}_4$ et D_n ($\forall n \in \mathbb{N}$) sont résolubles (cf. **Exemple 2.1.3**).

(iv) Si G est résoluble et si $N \lhd G$, alors N est résoluble également. En effet,si (G_i) est la suite de sous-groupes associée à G, il suffit de poser $N_i := G_i \bigcap N$, et on a bien $\{0\} = N_0 \lhd N_1 \lhd N_2 \lhd \cdots \lhd N_{n-1} \lhd N_n = N$. De plus, on peut vérifier (faites-le !) qu'il existe des injections

$$j_i : N_i/N_{i-1} \longrightarrow G_i/G_{i-1}.$$

Ainsi, N_i/N_{i-1} est isomorphe à un sous-groupe du groupe abélien (par hypothèse) G_i/G_{i-1} et est donc lui-même abélien.

D'une manière similaire, on pourrait montrer qu'avec les mêmes hypothèses, G/N est résoluble également.

(v) L'exemple précédent peut permettre de conclure à la non-résolubililté de certains groupes. Ainsi, en le combinant avec l'exemple *(ii)*, on peut conclure que, pour $n \geq 5$, $\mathfrak{S}_n$n'est pas résoluble (cf. **Théorème 2.2.2**).

Passons à présent à l'énoncé du théorème de Galois :

Théorème 4.1.3 (Galois) *Si une équation polynômiale à coefficients dans* $\mathbb{Q}$ *est résoluble par radicaux, alors son groupe de Galois est résoluble.*

Un exemple d'équation du cinquième degré non résoluble par radicaux : Soit $P(X) = X^5 - 6X + 3 \in \mathbb{Q}[X]$. On peut montrer que le groupe de Galois de l'équation $P(X) = 0$ est $\mathfrak{S}_5$, qui n'est pas résoluble, cett eéquation n'est donc pas résoluble par radicaux !

4.1.2 Toplogie algébrique et Groupe fondamental

La structure d'espace toplogique est certainement l'une des plus "molles" en mathématiques. On a vu que "l'identité structurelle" pour les groupes se formalisait par la notion d'isomorphisme. En ce qui concerne les espaces topologiques, on va considérer que deux espaces XC et Y ont la même structure lorsqu'il existe deux bijections réciproques *continues* $f : X \longrightarrow Y$ et $g : Y \longrightarrow X$. On dit alors que X et Y sont *homéomorphes* et f et g sont des homéomorphismes réciproques.

Or de tels homéomorphismes peuvent être très compliqués, et la notion même de continuité, qui est une idée géométrique et non algébrique, échappe à la quantification et au calcul. Comment donc montrer que deux espaces *nont se pas homéomorphes ?*

le principe de la topologie algébrique est d'associer aux objets topologiques des *invariants* algébriques, c'est à dire des objets *calculables* dont la valeur ne change par homéomorphisme.

Le premier invariant est le nombre de morceaux (ou *composantes connexes*) d'un espace. Cet invariant simple permet de faire la différence entre un plan et la réunion de deux plans parallèles. Mais il ne permet pas de faire la différence entre une droite et un cercle, ou entre un plan et un plan troué... Pourtant tous ces espaces sont différents.

On a donc commencé à associer des invariants plus complexes aux espaces, le plus important d'entre-eux étant le *groupe fondamental.* Ce groupe est construit à partit des "boucles" de l'espace, et compte les tours qu'on peut effectuer dans cet espace. Ainsi, dans une droite ou un plan, toutes les boucles peuvent s'obtenir les une des autres par déformation, et le groupe fondamental est donc trivial.

En revanche, dans le plan troué, par exemple, on ne pourra jamais déforme une boucle qui fait le tour du trou et obtenir une autre boucle qui passe à côté du trou sans sans l'englober. Le groupe est non trivial (c'est $\mathbb{Z}$ dans ce cas).

Ainsi, n'ayant pas le même groupe fondamental, un plan et un plan troué ne sont pas homéomorphes. Notons que la topologie est vraiment compliquée : pour tous groupe G il existe des espaces dont le groupe fondamental est G ! De fait, le groupe fondamental n'est pas un invariant suffisant pour l'objectif initial, et de nombreux autres l'ont suivi.

Nous consacrerons un texte à cet invariant capital, et à l'idée qui le sous-tend : la *fonctorialité*.

4.2 Représentations linéaires des groupes

On a longuement parlé de la notion d'action d'un groupe G sur un ensemble E au § 3. On a évoqué l'idée d'agir conformément à une structure donnée sur E. Or, comme on l'a vu, une action c'est essentiellement la donnée d'un morphisme de G dans $\mathfrak{S}_n(E)$, donc pour agir conformément à la structure de E il suffit de restreindre ce morphisme aux éléments de $\S(E)$ qui conservent cette structure.

Dans ce paragraphe, nous allons voir un exemple très important de ce type d'actions spécifiques : on va faire agir G sur un espace vectoriel V et ne considérer que les actions qui préservent la structure linéaire de V, ce qui nous amène à considérer la définition suivante :

Définition 4.2.1 *Soit G un groupe et K un corps. On appelle* $K-$représentation linéaire de G *la donnée d'un $K-$espace vectoriel V et d'un morphisme de groupe $\rho : G \longrightarrow GL_K(V)$. Si $g \in G$, on note généralement ρ_g l'image de g par ρ.*

En effet, $GL_K(V)$ étant un sous-groupe de $\mathfrak{S}_n(V)$, ρ définit bien, d'une part, une action de G sur V, telle que, d'autre part, toutes les applications $\rho_g : V \longrightarrow V$ sont bien des applications linéaires et ne "cassent" donc pas la structure de V.

Commentaire 4.2.2 *Notons que cette définition correspond exactement à* représenter *les éléments de G par des bijections* **linéaires** *de V sur lui-même, de la même manière que l'on représente ces éléments par une bijection de E sur lui-même lorsqu'on fait agir classiquement G sur un ensemble E.*

Exemples 4.2.3

(0) La représentation triviale : on prend $V = K$ et...

(i) Une représentation de $\mathfrak{S}_n$ sur K consiste à associer à tout élément de $\mathfrak{S}_n$ la matrice de permutation lui correspondant.

(ii) Si G agit sur un ensemble E, on peut créer le $K-$espace vectoriel K^E de base E, on obtient ainsi une représentation de G. Exemple typique et fondamental : La représentation régulière, notée $K[G]$, obtenue en appliquant ce procédé à l'action de G sur G.

(iii) Deux représentations de rang 2 de C_2 :

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

(iv) Une représentation de rang 2 de C_n

$$e^{\frac{2i\pi}{n}} \longmapsto \begin{pmatrix} cos(\frac{2\pi}{n}) & -sin(\frac{2\pi}{n}) \\ sin(\frac{2\pi}{n}) & cos(\frac{2\pi}{n}) \end{pmatrix}$$

Intérêt de cette notion : Ce développement de la théorie, commencé au XIX° siècle et qui constitue l'essentiel de la recherche des XX° et XXI° (jusqu'ici !) siècles est capital pour les mathématiques, mais également pour la physique et la chimie.

En effet, en physique quantique, le langage des représentations est utilisé pour "nommer" méthodiquement les particules, indexées par... des représentations de certains groupes de symétrie capitaux dans cette théorie !

En Chimie théorique, les calculs de niveau d'énergies de molécules exigent des diagonalisations de matrices énormes. Cependant, les symétries de la molécule peuvent être prises en compte pour simplifier ces calculs massifs, et les représentations du groupe des symétrie de cette molécule permettent ces simplification, en automatisant des techniques de diagonalisations par blocs.

On voit ainsi deux applications radicalement différentes, l'une théorique, permettant de mieux nommer et conceptualiser des objets physiques (voire de *prévoir leur existence...*), et l'autre purement opératoire, permettant de simplifier grandement des calculs effectifs.

5 Conclusion : la notion de symétrie

Comme le suggère la fin du dernier paragraphe, le centre de la théorie des groupes est la notion de *symétrie*. Que ce soit en géométrie ou dans le cas des équations algébriques, les pionniers qui dégagèrent cette notion avaient en tête le besoin de formaliser mathématiquement la notion de symétrie, si naturelle.

De même, dans la physique d'aujourd'hui, l'une des notions centrales est celle de symétrie. Ainsi, la relativité restreinte implique l'étude du Groupe de Poincaré, c'est à dire le groupe des symétries de l'espace plat. Dans ce cadre, l'étude du champ électromagnétique nécessite-t-elle... d'étudier les représentations de ce groupe !

Une intéressante réflexion sur la notion de symétrie nous est livrée par le mathématicien et physicien Hermann Weyl dans [8]. Nous consacrerons sans doute des ressources à ce sujet à l'avenir...