Groupes de permutations et groupes d'isométries

Antoine Ducros
Cours de Licence 2 de l'Université Pierre-et-Marie Curie

Année universitaire 2016-2017, premier semestre

Introduction

Ce cours est consacré à l'étude de la notion de *groupe*, que nous aborderons essentiellement à travers l'étude de quelques *groupes de transformations* (permutations, isométries).

Précisons un peu de quoi il retourne. Vous connaissez l'ensemble $\mathbb{Z}$ des entiers relatifs, et les deux opérations usuelles sur celui-ci : l'addition et la multiplication. C'est l'addition qui est importante pour notre propos, et nous allons en rappeler quelques propriétés.

- L'addition est *associative* : pour tout triplet (x, y, z) d'entiers relatifs, on a $(x + y) + z = x + (y + z)$.
- L'élément 0 de $\mathbb{Z}$ est *neutre* pour l'addition, c'est-à-dire qu'additionner 0 à un entier relatif n'a aucun effet : $x + 0 = 0 + x = x$ pour tout $x \in \mathbb{Z}$.
- Tout élément x de $\mathbb{Z}$ possède un *symétrique* pour l'addition, c'est-à-dire un élément y tel que $x + y$ et $y + x$ soient tous deux égaux à l'élément neutre 0 (prendre pour y l'opposé de x).

Vous aurez peut-être remarqué qu'il y a une propriété très importante que nous n'avons pas fait figurer dans cette liste, à savoir la *commutativité* : $x+y = y+x$ pour tout couple (x, y) d'éléments de $\mathbb{Z}$; mais c'est à dessein que nous l'avons omise, nous verrons pourquoi un peu plus bas.

Maintenant, considérons un ensemble quelconque X (qui peut être vide, fini, infini... nous ne faisons aucune hypothèse), et soit S l'ensemble des bijections de X dans X, c'est-à-dire l'ensemble des applications $f\colon X \to X$ telles que pour tout élément y de X, il existe un et un seul élément x de X tel que $f(x) = y$. On dispose d'une opération naturelle sur S, la *composition* des bijections $\circ$, définie par la formule

$$f \circ g = x \mapsto f(g(x))$$

Cette opération possède les propriétés suivantes :

- Elle est associative : si f, g et h sont trois éléments de S on a l'égalité $f \circ (g \circ h) = (f \circ g) \circ h$.
- L'application $\mathrm{Id}_X\colon x \mapsto x$ est neutre pour la composition, c'est-à-dire que composer avec l'identité n'a aucun effet : $f \circ \mathrm{Id}_X = \mathrm{Id}_X \circ f = f$ pour toute $f \in S$.
- Toute bijection $f \in S$ possède un symétrique pour la composition, c'est-à-dire une bijection $g \in S$ telle que $f \circ g$ et $g \circ f$ soient tous deux égaux à l'élément neutre Id_X (prendre pour g la bijection réciproque de f, qui envoie un élément x de X sur son unique antécédent par f).

On observe ainsi une certaine similitude entre l'addition des entiers relatifs et la composition des bijections (et c'est pour mettre cette similitude en évidence que nous n'avons pas inclus la commutativité dans la liste des propriétés de l'addition : la composition des bijections n'est en effet pas commutative dès que l'ensemble X a au moins trois éléments).

Lorsqu'ils font face comme ici à des objets d'origines et de natures différentes qui partagent un certain nombre de propriétés, les mathématiciens ont souvent tendance à *axiomatiser* la situation. Cela signifie qu'ils oublient (momentanément) les objets concrets en jeu, et travaillent avec des objets abstraits dont ils supposent simplement qu'ils satisfont les propriétés évoquées (qui deviennent donc des axiomes), sans autres hypothèses. Les avantages de cette approche sont les suivants :

- elle permet d'éviter de refaire dix fois la même démonstration dans des contextes différents, puisque tout ce qu'on arrive à démontrer sur les objets abstraits à partir de leurs propriétés axiomatiques est valable dans les différents cas concrets auxquels on s'intéressait initialement ;
- elle permet de se focaliser sur les propriétés qui servent vraiment dans les démonstrations, et de ne pas s'encombrer l'esprit avec des hypothèses parasites, peut-être satisfaites dans tel ou tel cas concret mais qui ne jouent en fait aucun rôle.

Lorsqu'on met en œuvre cette démarche pour les deux cas décrits plus haut (l'addition des entiers relatifs, la composition des bijections), on est conduit à introduire la notion de groupe. C'est ce que nous ferons au début de ce cours ; nous alternerons ensuite considérations générales sur les groupes abstraits et étude détaillée de groupes plus concrets (pour la plupart, des groupes de bijections).

1 Un peu de théorie des ensembles

Le but de cette section est de faire quelques brefs rappels sur les notions ensemblistes, que nous utiliserons régulièrement par la suite.

(1.1) Commençons par rappeler le sens de quelques notations de base.

(1.1.1) La notation $x \in E$ signifie que x appartient à E, ou encore que x est élément de l'ensemble E.

(1.1.2) La notation $E \subset F$ signifie que l'ensemble E est inclus dans l'ensemble F, c'est-à-dire que tout élément de E appartient à F. On dit aussi que E est un sous-ensemble de F.

(1.1.3) Si F est un sous-ensemble de E, on note $E \setminus F$ le complémentaire de F dans E, c'est-à-dire l'ensemble des éléments de E qui n'appartiennent pas à F.

(1.1.4) On désigne par $E \cap F$ l'intersection des ensembles E et F : on a $x \in E \cap F$ si et seulement si $x \in E$ et $x \in F$.

(1.1.5) On désigne par $E \cup F$ la réunion des ensembles E et F : on a $x \in E \cup F$ si et seulement si $x \in E$ ou $x \in F$ (le «ou» n'est pas exclusif : x peut très bien appartenir à E et à F).

(1.1.6) Si E et F sont deux ensembles dont l'intersection est vide, on écrira parfois $E \coprod F$ plutôt que $E \cup F$, si l'on veut mettre en valeur le caractère disjoint

de E et F (et on parle alors d'union *disjointe* de E et F). Si X est un ensemble et si E et F sont deux parties de X, on a $X = E \coprod F$ si et seulement si $F = X \setminus E$.

(1.1.7) On désigne par $\{x_1, \ldots, x_n\}$ l'ensemble dont les éléments sont les x_i ; l'ordre dans lequel on les écrit n'a aucune importance : par exemple, l'ensemble $\{0, 1, 2\}$ est égal à l'ensemble $\{1, 0, 2\}$. En particulier, $\{x\}$ désigne l'ensemble ayant x comme unique élément ; un tel ensemble est appelé un *singleton*.

(1.1.8) On désigne par $\varnothing$ l'ensemble vide, c'est-à-dire l'unique ensemble qui n'a aucun élément. Il ne présente évidemment aucun intérêt par lui-même, mais lorsqu'on définit un ensemble au cours d'un raisonnement (l'ensemble des solutions d'une équation, l'intersection de deux ensembles déjà construits, etc.), il se peut très bien qu'il soit vide ; il est donc préférable, pour ne pas devoir sans cesse traiter cette situation à part, qu'elle soit bien couverte par la théorie générale.

(1.2) Soient E et F deux ensembles. On appelle *produit cartésien* de E et F, et l'on note $E \times F$, l'ensemble des listes *ordonnées* (x, y) avec $x \in E$ et $y \in F$, que l'on appelle en général *couples*. Par exemple si $E = F = \mathbb{Z}$ les trois couples $(2, 3)$, $(3, 2)$ et $(4, 4)$ sont trois éléments deux à deux distincts de $\mathbb{Z} \times \mathbb{Z}$.

On peut plus généralement faire le produit cartésien d'un nombre arbitraire d'ensembles : $E_1 \times E_2 \times \ldots \times E_n$ désigne l'ensemble des listes ordonnées (ou n-uplets) $(x_1, \ldots, x_n)$ avec $x_i \in E_i$ pour tout i ; on écrira E^n au lieu de $\underbrace{E \times \ldots \times E}_{n \text{ facteurs}}$.

(1.3) De manière informelle, une *application* f d'un ensemble E vers un ensemble F est une règle associant à un élément x de E un élément de F noté $f(x)$.

On peut donner une définition rigoureuse de cette notion, que nous indiquons pour la curiosité du lecteur (elle ne servira pas ici) : une application f de E vers F est un sous-ensemble de $E \times F$ tel que pour tout $x \in E$ il existe un unique élément y de F tel que $(x, y) \in f$, et c'est cet unique élément y qu'on note $f(x)$.

(1.3.1) Si E est un ensemble, l'application $x \mapsto x$ de E dans E est appelée l'*identité* de E et est notée Id_E, ou parfois simplement Id si l'ensemble E est clairement indiqué par le contexte.

(1.3.2) Soit $f\colon E \to F$ une application. Si A est une partie de E on note $f(A)$ le sous-ensemble $\{f(x)\}_{x \in E}$ de F (on dit que $f(A)$ est l'*image* de A ; si $A = E$ on parle parfois aussi d'image de f). Si B est une partie de F on note $f^{-1}(B)$ le sous-ensemble de E constitué des éléments x tels que $f(x) \in B$ (on dit que $f^{-1}(B)$ est l'*image réciproque* de B). Si y est un élément de F on écrira $f^{-1}(y)$ au lieu de $f^{-1}(\{y\})$: c'est l'ensemble des antécédents de y par f, c'est-à-dire l'ensemble des éléments x de E tels que $f(x) = y$.

Par exemple, soit f l'application de $\{1, 2, 3, 4, 5\}$ dans $\{1, 2, 3, 4\}$ donnée par les formules

$$1 \mapsto 1, 2 \mapsto 1, 3 \mapsto 4, 4 \mapsto 4, 5 \mapsto 3.$$

On a $f(\{1, 2, 3\}) = \{1, 4\}$; on a $f^{-1}(\{1, 4\}) = \{1, 2, 3, 4\}$ et $f^{-1}(2) = \varnothing$.

(1.3.3) Soient $f\colon E \to F$ et $g\colon F \to G$ deux applications. On note $g \circ f$ l'application de E vers G qui envoie un élément x de E sur $g(f(x))$, et on

l'appelle la *composée* de g et f ; si $F = E$ on a $g \circ \mathrm{Id}_E = g$; si $G = F$ on a $\mathrm{Id}_F \circ f = f$.

Soit $h\colon G \to H$ une troisième application. On a alors $h \circ (g \circ f) = (h \circ g) \circ f$: on vérifie en effet aussitôt que ces deux applications envoient un élément x de E sur $h(g(f(x)))$.

Par exemple, soit f l'application de $\{1,2,3,4\}$ dans $\{a,b,c\}$ qui envoie 1 sur a, 2 sur b, 3 sur b et 4 sur c. Et soit g l'application de $\{a,b,c\}$ dans $\{\alpha,\beta\}$ qui envoie a sur α et b et c sur β. L'application $g \circ f$ va alors de $\{1,2,3,4\}$ vers $\{\alpha,\beta\}$ et l'on a :

- $g \circ f(1) = g(f(1)) = g(a) = \alpha$;
- $g \circ f(2) = g(f(2)) = g(b) = \beta$;
- $g \circ f(3) = g(f(3)) = g(b) = \beta$;
- $g \circ f(4) = g(f(4)) = g(c) = \beta$.

(1.3.4) Une application $f\colon E \to F$ est dite *injective* si

$$(f(x) = f(y)) \Rightarrow (x = y)$$

pour tout couple $(x,y) \in E \times F$, c'est-à-dire encore si tout élément de F a *au plus* un antécédent par f.

Elle est dite *surjective* si tout élément de F a *au moins* un antécédent par f, c'est-à-dire encore si $f(E) = F$.

Elle est dite *bijective* si elle est à la fois injective et surjective, c'est-à-dire si tout élément de F a un et un seul antécédent par f. Dans ce dernier cas, l'application de F dans E qui envoie un élément y de F sur son unique antécédent est notée f^{-1} (attention : c'est la même notation que celle introduite au 1.3.2, mais avec un sens un peu différent). L'application f^{-1} est également bijective, et $(f^{-1})^{-1} = f$: si $x \in E$, on a en effet pour tout $y \in F$ l'équivalence $f^{-1}(y) = x \iff y = f(x)$, et $f(x)$ est donc bien l'unique antécédent de x par f^{-1} ; on dit que f^{-1} est la *bijection réciproque* de f. On a par ailleurs $f \circ f^{-1} = \mathrm{Id}_F$ et $f^{-1} \circ f = \mathrm{Id}_E$. En effet, si y est un élément de F alors $f^{-1}(y)$ est l'unique antécédent de y par f, d'où l'égalité $f(f^{-1}(y)) = y$; et si x est un élément de E, c'est l'unique antécédent de $f(x)$ par f, d'où l'égalité $f^{-1}(f(x)) = x$.

Par exemple, l'application f de $\{1,2,3\}$ dans $\{a,b,c\}$ définie par les formules

$$1 \mapsto a,\ 2 \mapsto b,\ 3 \mapsto c\,;$$

sa réciproque f^{-1} est définie par les formules

$$a \mapsto 1,\ b \mapsto 2,\ c \mapsto 3.$$

(1.3.5) Soient $f\colon E \to F$ et $g\colon F \to G$ deux bijections. La composée $g \circ f$ est alors bijective, et $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$ (attention au renversement de l'ordre). En effet, soit $z \in G$. Pour tout $x \in E$ on a les équivalences

$$\begin{aligned} g(f(x)) = z &\iff f(x) = g^{-1}(z) \\ &\iff x = f^{-1}(g^{-1}(z)). \end{aligned}$$

Ainsi z a un et un seul antécédent dans E, égal à $f^{-1}(g^{-1}(z))$, ce qu'il fallait démontrer.

(1.4) Soit $f\colon E \to F$ une application. Soit E' un sous-ensemble de E, et soit F' un sous-ensemble de F. Si $f(E') \subset F'$, la formule $x \mapsto f(x)$ définit une application de E' vers F', qu'on dit *induite* par f. C'est simplement «l'application f dont on a restreint les ensembles de départ et d'arrivée». Si f est injective, l'application $E' \to F'$ induite par f est encore injective.

Par exemple, soit f l'application de $\{1,2,3,4,5\}$ dans $\{1,2,3,4\}$ donnée par les formules

$$1 \mapsto 1, 2 \mapsto 1, 3 \mapsto 4, 4 \mapsto 4, 5 \mapsto 3.$$

On a $f(\{1,2,3\}) = \{1,4\} \subset \{1,3,4\}$. Par conséquent, f induit une application de $\{1,2,3\}$ dans $\{1,3,4\}$, donnée par les formules $1 \mapsto 1, 2 \mapsto 1, 3 \mapsto 4$.

(1.5) Le cas limite de l'ensemble vide. La plupart des notions et résultats usuels de la théorie des ensembles s'appliquent sans problème à l'ensemble vide, et nous nous proposons dans ce paragraphe de donner quelques explications et exemples à ce sujet. Si ce qui suit vous paraît un peu étrange ou effrayant, vous pouvez l'oublier et simplement retenir que la théorie est suffisamment bien faite pour s'appliquer à l'ensemble vide sans même avoir à y penser ; si au contraire cette gymnastique mentale vous amuse, nous vous invitons à réfléchir un peu à ces questions.

(1.5.1) La remarque fondamentale à avoir en tête lorsqu'on se pose une question à propos de l'ensemble vide est la suivante : lorsqu'un énoncé logique commence par $\forall x \in \varnothing$, il est automatiquement vrai (peu importe ce qui suit). Pour s'en convaincre, il suffit de regarder sa négation : elle commence par $\exists x \in \varnothing$ et est donc fausse.

Si cela vous perturbe, méditez cette phrase un peu plus concrète : «tous les êtres humains mesurant plus de 5 mètres sont blonds». Est-ce vrai ou faux ? C'est vrai car dans le cas contraire il existerait un être humain mesurant plus de 5 mètres et n'étant pas blond, ce qui est absurde puisque de toutes façons, il n'existe pas d'êtres humains mesurant plus de 5 mètres (et on voit bien que «sont blonds» aurait pu être remplacé par n'importe quoi).

(1.5.2) Soit F un ensemble. Si E est un sous-ensemble de F, on dispose d'une application d'inclusion $x \mapsto x$ de E dans F.

Ceci s'applique notamment lorsque $E = \varnothing$: on dispose d'une application d'inclusion i de $\varnothing$ dans E. En termes un peu informels, cette application «ne fait rien», puisqu'elle ne peut de toutes façons rien faire, l'ensemble de départ n'ayant pas d'éléments. Si on veut être rigoureux (1.3), on doit la définir comme un sous-ensemble de $\varnothing \times F = \varnothing$ satisfaisant une condition qui commence par $\forall x \in \varnothing$ et sera donc automatiquement vérifiée, *cf.* 1.5.1 ; on prend bien entendu comme sous-ensemble de $\varnothing$ l'ensemble vide lui-même (on n'a de toutes façons pas le choix).

Cette application i est la seule application de $\varnothing$ vers F : en effet si l'on se donne une application j de $\varnothing$ vers F on a $i = j$, l'énoncé logique correspondant étant

$$\forall x \in \varnothing, j(x) = i(x),$$

qui commence par $\forall x \in \varnothing$.

L'application i est injective, l'énoncé logique correspondant étant

$$\forall x \in \varnothing, \forall y \in \varnothing, (i(x) = i(y)) \Rightarrow (x = y),$$

qui commence par $\forall x \in \varnothing$.

Si F est non vide, i n'est pas surjective (aucun élément de F n'a d'antécédents). Si F est vide, i est bijective, et même égale à l'identité, l'énoncé logique correspondant étant

$$\forall x \in \varnothing, i(x) = x,$$

qui commence par $\forall x \in \varnothing$.

(1.5.3) Terminons ces considérations par une remarque sur nos notations. Lorsque nous écrirons quelque chose du type $e_1, \ldots, e_n$, cela signifiera plus précisément qu'on considère la famille des e_i pour tous les indices i tels que $1 \leqslant i \leqslant n$; si $n = 0$ il n'y a *pas* de tel indice, et la famille considérée est donc vide.

2 La notion de groupe ; premiers exemples

(2.1) Définition. Soit E un ensemble. Une *loi de composition interne* sur E est une application de $E \times E$ vers E.

(2.2) Définition. Un *groupe* est un ensemble G muni d'une loi de composition interne $(g, g') \mapsto g * g'$ qui satisfait les propriétés suivantes :

(1) elle est *associative*, c'est-à-dire que $(g * g') * g'' = g * (g' * g'')$ pour tout $(g, g', g'') \in G^3$;

(2) elle possède un *élément neutre*, c'est-à-dire un élément e de G tel que $g * e = e * g = g$ pour tout $g \in G$;

(3) tout élément g de G possède un *symétrique* pour la loi $*$, c'est-à-dire un élément h tel que $g * h = h * g = e$.

(2.3) Commentaires sur la définition d'un groupe.

(2.3.1) Lorsqu'on dit que G est *muni* d'une loi de composition interne, cela signifie que cette loi *fait partie des données* : cela n'a pas de sens de dire qu'un ensemble ≪tout seul≫ est un groupe, il est indispensable de spécifier la loi interne qu'on considère.

(2.3.2) L'élément neutre e de (2) est unique. En effet, soit f un autre élément neutre pour la loi $*$. On a alors $f = e * f = e$ (la première égalité provient du fait que e est neutre, et la seconde du fait que f est neutre). Ainsi, $f = e$.

(2.3.3) Si g est un élément de G, son symétrique h est unique. Supposons en effet donné un autre symétrique h' de g. On a alors

$$h = e * h = (h' * g) * h = h' * (g * h) = h' * e = h'$$

(notez les justifications des différentes égalités : la première vient du fait que e est neutre, la seconde du fait que h' est un symétrique de g, la troisième de l'associativité de $*$, la quatrième du fait que h est un symétrique de g, et la cinquième à nouveau du fait que e est neutre).

(2.3.4) Grâce à l'associativité de $*$, on peut éviter l'emploi de parenthèses : puisque $(g * g') * g'' = g * (g' * g'')$ pour tout $(g, g', g'') \in G^3$, on pourra écrire simplement $g * g' * g''$ sans risque d'ambiguité.

(2.4) Conventions. Nous emploierons souvent des expressions comme «soit G un groupe». C'est un peu abusif : cela signifiera en réalité qu'on s'est donné un ensemble G *et une loi de composition interne sur* G qui satisfait les axiomes (1), (2) et (3) de la définition 2.2. Dans ce cas, et sauf mention expresse du contraire :

- la loi de composition interne de G sera notée $(g, g') \mapsto gg'$, donc sans symbole particulier : on juxtapose simplement les éléments, comme on le fait souvent pour la multiplication ordinaire ; pour cette raison, on se permettra de dire que gg' est le *produit* de g et g' ;
- l'élément neutre sera noté e, ou éventuellement e_G s'il est nécessaire de préciser dans quel groupe on se trouve ;
- le symétrique d'un élément g sera noté g^{-1}, et souvent appelé son *inverse*.

(2.5) Soit G un groupe.

(2.5.1) L'ensemble G est non vide, puisqu'il possède par définition au moins un élément, à savoir le neutre.

(2.5.2) On a $ee = e$; par conséquent, e est son propre inverse.

(2.5.3) Si $g \in G$ alors comme $gg^{-1} = g^{-1}g = e$, on voit que g est l'inverse de g^{-1} : autrement dit, $(g^{-1})^{-1} = g$.

(2.5.4) Attirons l'attention sur un point important : si g et h sont deux éléments de G, les produits gh et hg n'ont en général aucune raison de coïncider (nous verrons des exemples un peu plus bas).

(2.5.5) On peut «simplifier les égalités» dans G, au sens suivant : si g, g' et h sont trois éléments de G tels que $gh = g'h$ alors $g = g'$; de même, si $hg = hg'$ alors $g = g'$.

En effet, supposons que $gh = g'h$; en multipliant par h^{-1} à droite des deux côtés, il vient $ghh^{-1} = g'hh^{-1}$, soit encore $ge = g'e$, et partant $g = g'$. On procède de même si $hg = hg'$.

Notons un cas particulier important : si $gh = e$ alors $h = g^{-1}$ (car $gh = e$ peut se récrire $gh = gg^{-1}$) ; de même, si $hg = e$ alors $h = g^{-1}$. Pour vérifier que h est l'inverse de g, il suffit donc de s'assurer que l'un des deux produits hg ou gh est égal à e (et l'autre le sera alors automatiquement).

(2.5.6) Si g et h sont deux éléments de G alors $(gh)^{-1} = h^{-1}g^{-1}$: *l'inversion renverse le sens des produits*. En effet, on a

$$(gh)(h^{-1}g^{-1}) = ghh^{-1}g^{-1} = gg^{-1} = e,$$

ce qui suffit à conclure d'après le dernier paragraphe de 2.5.5.

(2.5.7) Soit g un élément de G et soit n un entier positif ou nul. On pose

$$g^n = \underbrace{gg\dots g}_{n \text{ termes}}$$

(si $n = 0$ on se retrouve donc avec le *produit vide*, que l'on prend par convention égal à l'élément neutre e). On a $g^{n+m} = g^n g^m$ et $(g^n)^m = g^{nm}$ pour tout couple (n, m) d'entiers positifs ou nuls (notez que la convention $g^0 = e$ est indispensable à la validité de ces formules).

Si $n < 0$, on pose $g^n = (g^{-1})^{(-n)}$. Nous vous laissons vérifier que les formules $g^{n+m} = g^n g^m$ et $(g^n)^m = g^{nm}$ restent valables pour tout couple (n, m) d'entiers relatifs.

(2.6) Groupes abéliens ; notation additive. Un groupe G est dit *commutatif* ou *abélien* si $gh = hg$ pour tout couple (g, h) d'éléments de G.

Il arrive qu'on adopte pour un groupe abélien G la *notation additive* : la loi interne est notée $(g, g') \mapsto g + g'$; le neutre est noté 0 ou 0_G ; le symétrique d'un élément g est noté $-g$ (et est appelé son *opposé*) ; on écrit $g - g'$ au lieu de $g + (-g')$; on écrit ng au lieu de g^n.

(2.7) Exemples.

(2.7.1) Soit X un singleton $\{x\}$. Il y a une seule loi de composition interne possible sur X (celle qui envoie (x, x) sur x) ; on vérifie aussitôt qu'elle fait de $\{x\}$ un groupe (dont le neutre est évidemment x). Un tel groupe réduit à son élément neutre est dit *trivial*.

(2.7.2) Le groupe $\mathbb{Z}$. L'ensemble $\mathbb{Z}$ des entiers relatifs, *muni de l'addition*, est un groupe abélien. L'élément neutre est 0, le symétrique d'un élément est son opposé (c'est évidemment de cet exemple qu'est inspirée la notation additive dont on a parlé au 2.6).

Lorsqu'on parlera du groupe $\mathbb{Z}$, il sera désormais toujours sous-entendu que sa loi de composition interne est l'addition.

(2.7.3) Les groupe $\mathbb{R}^\times$ et $\mathbb{C}^\times$. L'ensemble $\mathbb{R}^\times$ (resp. $\mathbb{C}^\times$) des nombres réels (resp. complexes) non nuls, *muni de la multiplication*, est un groupe abélien. L'élément neutre est 1, et le symétrique d'un élément est son inverse.

Lorsqu'on parlera du groupe $\mathbb{R}^\times$ (resp. $\mathbb{C}^\times$), il sera désormais toujours sous-entendu que sa loi de composition interne est la multiplication.

(2.7.4) Le groupe des permutations d'un ensemble. Soit X un ensemble et soit S_X l'ensemble des bijections de X dans X, que l'on appelle également les *permutations* de X. Si σ et τ sont deux permutations de X, leur composée est une permutation de X (1.3.5). La formule $(\sigma, \tau) \mapsto \sigma \circ \tau$ définit donc une loi de composition interne sur S_X.

Il résulte de 1.3.3, que cette loi est associative et que Id_X en est un élément neutre. Et si $\sigma \in S_X$, la bijection réciproque σ^{-1} est un symétrique de σ pour la loi $\circ$ (1.3.4).

L'ensemble S_X *muni de la composition des permutations* est donc un groupe. Lorsqu'on parlera du groupe S_X, il sera désormais toujours sous-entendu que sa loi de composition interne est la composition des permutations. Lorsque cela ne prêtera pas à confusion, on se permettra d'écrire $\sigma\tau$ plutôt que $\sigma \circ \tau$ (cela allège les notations, et est en accord avec nos conventions générales sur les groupes abstraits). On écrira aussi parfois simplement Id au lieu de Id_X, s'il n'y a pas d'ambiguïté sur X.

(2.7.5) Donnons quelques exemples de groupes de permutations.

(i) *Le cas de l'ensemble vide.* L'ensemble vide possède une seule permutation, à savoir l'identité (on sait même que toute application de $\varnothing$ dans lui-même est automatiquement égale à l'identité, *cf.* 1.5.2). Le groupe $S_\varnothing$ est donc égal à $\{\mathrm{Id}\}$; il est trivial.

(ii) *Le cas d'un singleton.* Un singleton $\{x\}$ possède une seule permutation, à savoir l'identité (une application de $\{x\}$ dans lui-même envoie en effet nécessairement x sur x). Le groupe $S_{\{x\}}$ est par conséquent égal à $\{\mathrm{Id}\}$ et est donc là encore trivial.

(iii) *Le cas où X possède deux éléments.* Supposons que $X = \{a, b\}$ avec $a \neq b$. Le groupe S_X comporte alors deux éléments : l'identité, et la permutation τ qui échange a et b. Le groupe S_X n'est donc pas trivial : il est égal à $\{\mathrm{Id}, \tau\}$. On a $\tau^2 = \mathrm{Id}$ (et τ est donc son propre inverse) ; le groupe S_X est abélien.

(iv) *Le cas où X possède au moins trois éléments.* On peut dès lors choisir trois éléments distincts a, b et c dans X. Soit τ la permutation de X qui échange a et b et fixe tous les autres éléments de X (y compris c) et soit σ celle qui échange a et c et fixe tous les autres éléments de X (y compris b). On a les égalités

$$(\sigma\tau)(a) = \sigma(\tau(a)) = \sigma(b) = b$$

et

$$(\tau\sigma)(a) = \tau(\sigma(a)) = \tau(c) = c.$$

Ainsi, $\sigma\tau \neq \tau\sigma$: le groupe S_X n'est pas abélien.

(2.8) Le groupe $\mathbb{Z}/n\mathbb{Z}$. On fixe un entier $n \geqslant 1$.

(2.8.1) Soit a un entier. La *classe de a modulo n* est l'ensemble des entiers b tels que $b - a$ soit multiple de n. En d'autres termes, cette classe est l'ensemble des entiers de la forme $a + kn$ avec $k \in \mathbb{Z}$; elle contient a (prendre $k = 0$).

Soit b un élément de la classe de a modulo n, et soit c un entier quelconque. On a $c - a = c - b + (b - a)$. Comme $b - a$ est multiple de n, on voit que si $c - b$ est multiple de n alors $c - a$ est multiple de n ; en écrivant $c - b = c - a - (b - a)$ on voit de même que si $c - a$ est multiple de n alors $c - b$ est multiple de n. Par conséquent, $c - a$ est multiple de n si et seulement si $c - b$ est multiple de n ; autrement dit, la classe de a modulo n est égale à la classe de b modulo n.

La classe de a modulo n sera notée $\overline{a}$.

(2.8.2) Soient a et b deux entiers. On a $\overline{a} = \overline{b}$ si et seulement si b appartient à $\overline{a}$, c'est-à-dire si et seulement si $b - a$ est multiple de n (on dit alors que a et b sont *égaux modulo n*.

En effet, si $\overline{a} = \overline{b}$ alors comme b appartient à $\overline{b}$, il appartient à $\overline{a}$. Et si b appartient à $\overline{a}$, on a $\overline{b} = \overline{a}$ d'après 2.8.1.

(2.8.3) On note $\mathbb{Z}/n\mathbb{Z}$ l'ensemble des classes modulo n ; on dit parfois que $\mathbb{Z}/n\mathbb{Z}$ est le *quotient de $\mathbb{Z}$ modulo n*. Les éléments de $\mathbb{Z}/n\mathbb{Z}$ sont donc les $\overline{a}$ pour a parcourant $\mathbb{Z}$; on dispose ainsi d'une surjection $a \mapsto \overline{a}$ de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$, qui est appelée la *réduction modulo n*. D'après 2.8.2, on a $\overline{a} = \overline{b}$ si et seulement si $b - a$ est multiple de n.

(2.8.4) Remarque. Bien que les éléments de $\mathbb{Z}/n\mathbb{Z}$ soient rigoureusement définis comme des classes modulo n, c'est-à-dire comme des sous-ensembles de $\mathbb{Z}$, il vaut mieux ne pas y penser ainsi pour éviter d'avoir mal à la tête.

Ce qui est vraiment utile, c'est ce qui est expliqué au 2.8.3 ci-dessus : on a une surjection $a \mapsto \overline{a}$ de $\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$, et $\overline{a} = \overline{b}$ si et seulement si $b - a$ est multiple de n (et peu importe en fait la définition technique de $\overline{a}$). On peut ainsi voir

$\mathbb{Z}/n\mathbb{Z}$ comme un ensemble de nombres fabriqué en partant des entiers relatifs usuels et en rajoutant (par décret, en quelque sorte) une règle qui dit que deux nombres coïncident dès que leur différence est multiple de n.

Supposons par exemple que $n = 5$. Travailler avec les classes modulo 5, cela revient à travailler avec les entiers usuels, mais en décidant que deux entiers coïncident dès que leur différence est un multiple de 5 : on aura donc $\overline{3} = \overline{8}$ ou $\overline{(-5)} = \overline{0}$.

(2.8.5) Soit a un élément de $\mathbb{Z}$. La théorie de la division euclidienne assure qu'il existe un unique couple (q, r) d'éléments de $\mathbb{Z}$ tels que $r \in \{0, \dots, n-1\}$ et $a = nq + r$. On a donc $\overline{a} = \overline{r}$.

Soit s un entier appartenant à $\{0, \dots, n-1\}$. On a $\overline{s} = \overline{r}$ si et seulement si $s - r$ est multiple de n. Mais comme s et r sont tous deux compris entre 0 et $n-1$, la différence $r - s$ est multiple de n si et seulement $r - s = 0$, c'est-à-dire si et seulement si $s = r$. Autrement dit, r est l'unique entier compris entre 0 et $n-1$ dont la classe modulo n est égale à $\overline{r}$.

Récapitulons : tout élément de $\mathbb{Z}/n\mathbb{Z}$ est égal à $\overline{r}$ pour un unique élément r de $\{0, \dots, n-1\}$. Par conséquent, les élements $\overline{0}, \dots, \overline{n-1}$ de $\mathbb{Z}/n\mathbb{Z}$ sont deux à deux distincts, et $\mathbb{Z}/n\mathbb{Z} = \{\overline{0}, \dots, \overline{n-1}\}$. Le cardinal de $\mathbb{Z}/n\mathbb{Z}$ est donc égal à n.

Considérons par exemple le cas où $n = 3$. L'ensemble $\mathbb{Z}/3\mathbb{Z}$ compte 3 éléments, à savoir $\overline{0}, \overline{1}$ et $\overline{2}$. Si a est un entier quelconque, pour savoir auquel de ces 3 éléments la classe $\overline{a}$ est égale, on calcule le reste de la division euclidienne de a par 3. Par exemple, $581 = 3 \cdot 193 + 2$, et l'on a donc $\overline{581} = \overline{2}$; et $(-47) = 3 \cdot (-16) + 1$, d'où l'égalité $\overline{(-47)} = \overline{1}$.

(2.8.6) Constructions d'applications de source $\mathbb{Z}/n\mathbb{Z}$. Revenons au cas où n est un entier > 0 quelconque, et soit f une application de $\mathbb{Z}$ vers un ensemble donné E. Peut-on définir une application de $\mathbb{Z}/n\mathbb{Z}$ dans E par la formule $\overline{a} \mapsto f(a)$? La réponse est non en général. En effet, cette formule est *a priori* ambiguë, pour la raison suivante : il pourrait très bien exister deux éléments a et b dans $\mathbb{Z}$ distincts tel que $\overline{a} = \overline{b}$ mais $f(a) \neq f(b)$, et l'application évoquée devrait alors envoyer $\overline{a} = \overline{b}$ à la fois sur $f(a)$ et $f(b)$, ce qui est absurde.

On dit que f *passe au quotient modulo* n si $f(a) = f(b)$ dès que $\overline{a} = \overline{b}$. Dans ce cas le problème évoqué ci-dessus ne se produit pas, et la formule $\overline{a} \mapsto f(a)$ définit bien une application de $\mathbb{Z}/n\mathbb{Z}$ vers E, que l'on dira *induite* par f.

Donnons maintenant deux exemples, dans le cas où $n = 2$.

- Considérons l'application sin de $\mathbb{Z}$ dans $\mathbb{R}$. Elle ne passe pas au quotient modulo 2 : en effet $\sin 0 = 0$ mais $\sin 2 \neq 0$, alors que $\overline{2} = \overline{0}$. On ne peut donc pas définir d'application de $\mathbb{Z}/2\mathbb{Z}$ dans $\mathbb{R}$ par la formule $\overline{a} \mapsto \sin a$: cette application devrait en effet envoyer $\overline{0} = \overline{2}$ à la fois sur $\sin 0$ et $\sin 2$, ce qui est absurde puisque $\sin 2 \neq \sin 0 = 0$.
- Considérons l'application $f\colon a \mapsto (-1)^a$ de $\mathbb{Z}$ dans $\mathbb{R}$. Elle passe au quotient modulo 2 : en effet si a et b sont deux entiers tels que $b - a$ soit pair alors $(-1)^a = (-1)^{a+b-a} = (-1)^b$. Par conséquent, f induit une application de $\mathbb{Z}/2\mathbb{Z}$ dans $\mathbb{R}$, donnée par la formule $\overline{a} \mapsto (-1)^a$. Cette application envoie $\overline{0}$ sur $(-1)^0 = 1$ et $\overline{1}$ sur $(-1)^1 = (-1)$.

Ces considérations se généralisent au cas d'applications de $\mathbb{Z}^r$ vers E (où r est un entier positif) : si une telle application f passe au quotient modulo n, c'est-à-dire est telle que $f(a_1, \dots, a_r) = f(b_1, \dots, b_r)$ dès que $\overline{a_i} = \overline{b_i}$ pour

tout i, alors f induit une application de $(\mathbb{Z}/n\mathbb{Z})^r$ vers E, donnée par la formule $(\overline{a_1}, \ldots, \overline{a_r}) \mapsto f(a_1, \ldots, a_r)$.

(2.8.7) L'addition dans $\mathbb{Z}/n\mathbb{Z}$. Nous allons donner une application importante de ce qui précède. Considérons l'application de $\mathbb{Z} \times \mathbb{Z}$ vers $\mathbb{Z}/n\mathbb{Z}$ qui envoie un couple (a, b) sur $\overline{a+b}$.

Elle passe au quotient modulo n. En effet, donnons-nous quatre éléments a, α, b et β de $\mathbb{Z}$, et supposons que $\overline{a} = \overline{\alpha}$ et $\overline{b} = \overline{\beta}$. Il s'agit de montrer que $\overline{a+b} = \overline{\alpha+\beta}$. On a

$$\alpha + \beta - (a+b) = \alpha + \beta - a - b = (\alpha - a) + (\beta - b).$$

Or $\alpha - a$ est multiple de n car $\overline{a} = \overline{\alpha}$, et $\beta - b$ est multiple de n car $\overline{b} = \overline{\beta}$. Par conséquent, $\alpha + \beta - (a+b)$ est multiple de n et $\overline{a+b} = \overline{\alpha+\beta}$, comme annoncé.

Cette application induit donc une application de $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ vers $\mathbb{Z}/n\mathbb{Z}$, donnée par la formule $(\overline{a}, \overline{b}) \mapsto \overline{a+b}$. On la note encore $+$. On a ainsi défini une loi de composition interne $+$ sur $\mathbb{Z}/n\mathbb{Z}$, donnée par la formule

$$\overline{a} + \overline{b} = \overline{a+b}.$$

Cette loi est associative. En effet, donnons-nous trois éléments $\overline{a}, \overline{b}$ et $\overline{c}$ de $\mathbb{Z}/n\mathbb{Z}$. On a alors

$$\begin{aligned}
\overline{a} + (\overline{b} + \overline{c}) &= \overline{a} + \overline{b+c} && (1)\\
&= \overline{a + (b+c)} && (2)\\
&= \overline{(a+b) + c} && (3)\\
&= \overline{a+b} + \overline{c} && (4)\\
&= (\overline{a} + \overline{b}) + \overline{c}. && (5)
\end{aligned}$$

Précisons que les égalités (1), (2), (4) et (5) proviennent de la formule qui définit la loi interne $+$ de $\mathbb{Z}/n\mathbb{Z}$, et que (3) provient de l'associativité de l'addition de $\mathbb{Z}$.

L'élément $\overline{0}$ de $\mathbb{Z}/n\mathbb{Z}$ est neutre pour la loi $+$. En effet, donnons-nous un élément $\overline{a}$ de $\mathbb{Z}/n\mathbb{Z}$. On a alors

$$\overline{a} + \overline{0} = \overline{a+0} = \overline{a},$$

où la première égalité provient de la formule qui définit la loi interne $+$ de $\mathbb{Z}/n\mathbb{Z}$, et la seconde du fait que 0 est neutre pour l'addition dans $\mathbb{Z}$. On montre de même que $\overline{0} + \overline{a} = \overline{a}$.

Tout élément de $\mathbb{Z}/n\mathbb{Z}$ possède un symétrique pour $+$. En effet, donnons-nous un élément $\overline{a}$ de $\mathbb{Z}/n\mathbb{Z}$. On a alors $\overline{a} + \overline{(-a)} = \overline{a + (-a)} = \overline{0}$, où la première égalité provient de la formule qui définit la loi interne $+$ de $\mathbb{Z}/n\mathbb{Z}$, et la seconde du fait que $a + (-a) = 0$ dans $\mathbb{Z}$. On montre de même que $\overline{(-a)} + \overline{a} = 0$. Ainsi, $\overline{(-a)}$ est le symétrique de $\overline{a}$ pour la loi $+$; on dit aussi que c'est l'opposé de $\overline{a}$, et on le note souvent $-\overline{a}$, et l'on écrira $\overline{a} - \overline{b}$ plutôt que $\overline{a} + (-\overline{b})$. Avec ces conventions, on a $\overline{a} - \overline{b} = \overline{a} + \overline{(-b)} = \overline{a-b}$.

L'ensemble $\mathbb{Z}/n\mathbb{Z}$ muni de l'addition qu'on a définie est ainsi un groupe. Lorsqu'on parlera du groupe $\mathbb{Z}/n\mathbb{Z}$, il sera désormais toujours sous-entendu que sa loi de composition interne est l'addition telle que définie ci-dessus.

Le groupe $\mathbb{Z}/n\mathbb{Z}$ est abélien. En effet si $\overline{a}$ et $\overline{b}$ sont deux élements de $\mathbb{Z}/n\mathbb{Z}$, on a

$$\begin{aligned} \overline{a}+\overline{b} &= \overline{a+b} && (6)\\ &= \overline{b+a} && (7)\\ &= \overline{b}+\overline{a}. && (8) \end{aligned}$$

Précisons que les égalités (6) et (8) proviennent de la formule qui définit la loi interne + de $\mathbb{Z}/n\mathbb{Z}$, et que (7) provient du fait que $\mathbb{Z}$ est un groupe abélien.

(2.8.8) Quelques exemples.

- *Le cas où $n = 1$.* Le groupe $\mathbb{Z}/1\mathbb{Z}$ a pour cardinal 1 : il est réduit à $\{\overline{0}\}$ et est donc trivial.
- *Le cas où $n = 2$.* Le groupe $\mathbb{Z}/2\mathbb{Z}$ comprend deux éléments, à savoir $\overline{0}$ et $\overline{1}$. On a $\overline{1}+\overline{1} = \overline{1+1} = \overline{2} = \overline{0}$; ainsi, $\overline{1} = -\overline{1}$.
- *Le cas où $n = 3$.* Le groupe $\mathbb{Z}/3\mathbb{Z}$ comprend trois éléments : $\overline{0}, \overline{1}$ et $\overline{2}$. On a $\overline{1}+\overline{2} = \overline{3} = \overline{0}$: ainsi, $\overline{2} = -\overline{1}$.
- *Remarques générales.* Supposons n quelconque. On a $\overline{n-1} = \overline{n}-\overline{1} = -\overline{1}$, et de même $\overline{n-2} = -\overline{2}$, etc. On a souvent intérêt à s'en souvenir pour simplifier les calculs. Par exemple, supposons que $n = 23$, et imaginons qu'on veuille calculer $\overline{17}+\overline{21}$. On peut calculer $17 + 21$, ce qui fait 38, puis remarquer que $38 = 23 + 15$, d'où l'égalité $\overline{17}+\overline{21} = \overline{15}$. Mais on peut aussi directement remarquer que $\overline{21} = -\overline{2}$. Il vient alors

$$\overline{17}+\overline{21} = \overline{17}-\overline{2} = \overline{15}.$$

3 Étude détaillée des groupes de permutation

(3.1) Nous rencontrerons souvent dans la suite les groupes de permutations $S_{\{1,\dots,n\}}$; pour alléger un peu les notations, nous écrirons S_n au lieu de $S_{\{1,\dots,n\}}$; notons que $S_0 = S_{\{1,\dots,0\}} = S_\varnothing$ Pour décrire un élément de S_n, on le présente sous forme d'un tableau : la première ligne comporte tous les entiers compris entre 1 et n, et sous chacun d'eux on écrit son image. Ainsi le tableau

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

désigne l'élément de S_3 qui envoie 1 sur 2, 2 sur 3 et 3 sur 1 ; quant à

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix},$$

c'est simplement l'identité de $\{1, 2, 3\}$.

(3.2) Factorielle d'un entier. Soit n un entier $\geqslant 0$. On appelle *factorielle* de n, et l'on note $n!$, le produit $\prod_{1\leqslant i\leqslant n} i$; notez que lorsque $n = 0$ on obtient le

produit vide, que l'on prend par convention égal à 1. On a donc

$$\begin{array}{lcll} 0! & = & 1 & \\ 1! & = & 1 & \\ 2! & = & 1 \cdot 2 & = 2 \\ 3! & = & 1 \cdot 2 \cdot 3 & = 6 \\ 4! & = & 1 \cdot 2 \cdot 3 \cdot 4 & = 24 \\ 5! & = & 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 & = 120 \\ 6! & = & 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 & = 720, \end{array}$$

etc. On a pour tout n l'égalité $(n+1)! = (n+1) \cdot n!$ (y compris lorsque $n = 0$, grâce à la convention $0! = 1$).

(3.3) Lemme. *Soit n un entier $\geqslant 0$ et soient X et Y deux ensembles de cardinal n. L'ensemble des bijections de X sur Y a pour cardinal $n!$. En particulier – c'est le cas où $Y = X$ – le groupe S_X a pour cardinal $n!$.*

Démonstration. On procède par récurrence sur n.

Le cas où $n = 0$. On a alors $X = Y = \varnothing$. Or si i est une application de l'ensemble vide dans lui-même, on a vu au 1.5.2 que $i = \mathrm{Id}$. Il y a donc dans ce cas une unique bijection de X sur Y (à savoir l'identité), et la propriété requise est démontrée puisque $0! = 1$.

Supposons $n > 0$ et la propriété vraie en rang $< n$. Comme $n > 0$ l'ensemble X est non vide ; on choisit $x \in X$. Pour tout y dans Y, on note B_y l'ensemble des bijections de X vers Y qui envoient x sur y. Le cardinal de B est alors égal à $\sum_{y \in Y} \mathrm{card}(B_y)$.

Soit $y \in Y$. Se donner une bijection de X sur Y qui envoie x sur y revient à se donner une bijection de $X \setminus \{x\}$ sur $Y \setminus \{y\}$ (une fois qu'on a imposé que l'image de x soit égale à y, il reste à déterminer les images des autres éléments de X, nécessairement différentes de y). Comme $X \setminus \{x\}$ et $Y \setminus \{y\}$ sont de cardinal $n-1$, l'hypothèse de récurrence assure qu'il y a $(n-1)!$ bijections de $X \setminus \{x\}$ sur $Y \setminus \{y\}$; le cardinal de B_y est par conséquent égal à $(n-1)!$. Il vient

$$\begin{aligned} \mathrm{card}(B) &= \sum_{y \in Y} \mathrm{card}(B_y) \\ &= \sum_{y \in Y} (n-1)! \\ &= \mathrm{card}(Y) \cdot (n-1)! \\ &= n \cdot (n-1)! \\ &= n!. \quad \square \end{aligned}$$

(3.4) Nous allons maintenant donner la liste explicite de tous les éléments de S_n pour les petites valeurs de n.

(3.4.1) Il résulte de 2.7.5 (i) (ii) que $S_0 = \{\mathrm{Id}\}$ et $S_1 = \{\mathrm{Id}\}$.

(3.4.2) Il résulte de 1.5.2 (iii) que S_2 comprend deux éléments qui sont les suivants (avec la présentation par tableau que nous avons décrite au 3.1) :

$$\begin{pmatrix} 1 & 2 \\ 1 & 2 \end{pmatrix} \quad \text{et} \quad \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}.$$

(3.4.3) Donnons la liste des éléments de S_3. La théorie assure qu'il y en a $3! = 6$ (lemme 3.3). Pour être certain de n'en oublier aucun, on procède méthodiquement : on fixe l'image de 1, puis celle de 2 (on n'a alors plus le choix pour celle de 3). On obtient :

$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$

(3.4.4) Donnons la liste des éléments de S_4. La théorie assure qu'il y en a $4! = 24$ (lemme 3.3). Pour être certain de n'en oublier aucun, on procède méthodiquement : on fixe l'image de 1, puis celle de 2, puis celle de 3 (on n'a alors plus le choix pour celle de 4). On obtient :

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 4 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 2 & 4 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 2 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix} \quad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 3 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 1 & 2 \end{pmatrix} \qquad \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}$$

Donnons un ou deux exemples de calcul dans S_4. L'inverse de

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$$

est

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 1 & 4 & 2 \end{pmatrix}$$

(on écrit sous chaque élément son antécédent par la permutation qu'on veut inverser).

Le produit

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 1 & 4 \end{pmatrix}$$

est égal à

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$$

(on procède «à la main» : la permutation de droite envoie 2 sur 3, celle de gauche envoie 3 sur 1, la composée envoie donc 2 sur 1, etc.).

(3.5) Support d'une permutation. Soit X un ensemble. Soit σ un élément de S_X. Un *point fixe* de σ est un élément x de X tel que $\sigma(x) = x$; on note $\mathrm{Fix}(\sigma)$ l'ensemble des points fixes de σ. On appelle *support* de σ l'ensemble des éléments x de X tels que $\sigma(x) \neq x$; on le note $\mathrm{Supp}(\sigma)$. Par construction, on a $X = \mathrm{Fix}(\sigma) \coprod \mathrm{Supp}(\sigma)$ (1.1.6).

(3.5.1) On a $\mathrm{Supp}(\sigma) = \varnothing$ si et seulement si $\mathrm{Fix}(\sigma) = X$, c'est-à-dire encore si et seulement si $\sigma(x) = x$ pour tout $x \in X$, donc si et seulement si $\sigma = \mathrm{Id}$.

(3.5.2) Pour tout $x \in X$ on a $\sigma(x) = x$ si et seulement si x est son propre antécédent par σ, c'est-à-dire si et seulement si $\sigma^{-1}(x) = x$. Il en résulte que $\mathrm{Fix}(\sigma^{-1})$ est égal à $\mathrm{Fix}(\sigma)$, puis que $\mathrm{Supp}(\sigma^{-1}) = \mathrm{Supp}(\sigma)$ par passage au complémentaire.

(3.5.3) Exemple concret. Si $X = \{1, 2, 3, 4, 5\}$ et

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 1 & 5 \end{pmatrix}$$

alors $\mathrm{Fix}(\sigma) = \{3, 5\}$ et $\mathrm{Supp}(\sigma) = \{1, 2, 4\}$.

(3.5.4) Revenons au cas d'un ensemble X et d'une permutation $\sigma \in S_X$ quelconques. Soit $x \in X$. Comme σ est injective, on a $\sigma(\sigma(x)) = \sigma(x)$ si et seulement si $\sigma(x) = x$. Autrement dit $\sigma(x) \in \mathrm{Fix}(\sigma) \iff x \in \mathrm{Fix}(\sigma)$; par passage au complémentaire, $\sigma(x) \in \mathrm{Supp}(\sigma) \iff x \in \mathrm{Supp}(\sigma)$.

Ainsi, l'image et l'antécédent par σ d'un élément de $\mathrm{Supp}(\sigma)$ appartiennent à $\mathrm{Supp}(\sigma)$ (on en déduit par récurrence que $\sigma^i(x) \in \mathrm{Supp}(\sigma)$ pour tout $i \in \mathbb{Z}$ et tout $x \in \mathrm{Supp}(\sigma)$). Par conséquent, σ induit une bijection de $\mathrm{Supp}(\sigma)$ sur lui-même, qui n'a pas de point fixe (puisque par définition, $\mathrm{Supp}(\sigma)$ ne contient

aucun point fixe de σ). De même, σ induit une bijection de $\mathrm{Fix}(\sigma)$ sur lui-même qui n'est autre que l'identité, par définition de $\mathrm{Fix}(\sigma)$.

Ainsi, si l'on reprend σ comme au 3.5.3 ci-dessus, σ induit l'identité de $\mathrm{Fix}(\sigma) = \{3, 5\}$ dans lui-même, et la bijection $1 \mapsto 2, 2 \mapsto 4$ et $4 \mapsto 1$ de $\mathrm{Supp}(\sigma) = \{1, 2, 4\}$ dans lui-même (qui n'a pas de point fixe).

(3.5.5) Support d'un produit de permutations. Soient $\sigma_1, \ldots, \sigma_n$ des permutations de X. Si $\sigma_i(x) = x$ pour tout i, on a $(\sigma_1\sigma_2 \ldots \sigma_n)(x) = x$; par conséquent, $\bigcap_i \mathrm{Fix}(\sigma_i) \subset \mathrm{Fix}(\sigma_1 \ldots \sigma_n)$. Par passage au complémentaire, $\mathrm{Supp}(\sigma_1 \ldots \sigma_n) \subset \bigcup_i \mathrm{Supp}(\sigma_i)$. Autrement dit, le support du produit est contenu dans la réunion des supports.

En particulier, $\mathrm{Supp}(\sigma^d) \subset \mathrm{Supp}(\sigma)$ pour toute permutation σ de X et tout $d \in \mathbb{N}$; cela vaut en fait pour tout $d \in \mathbb{Z}$ car $\mathrm{Supp}(\sigma^{-1}) = \mathrm{Supp}(\sigma)$ (3.5.2).

(3.5.6) Attention : en général, le support du produit est *strictement* contenu dans la réunion des supports. Par exemple si σ est une permutation de X différente de l'identité, on a $\mathrm{Supp}(\sigma) = \mathrm{Supp}(\sigma^{-1}) \neq \varnothing$, mais le support de $\sigma\sigma^{-1} = \mathrm{Id}$ est vide.

(3.6) Produit de permutations à supports disjoints. Soit X un ensemble. Soient $\sigma_1, \ldots, \sigma_n$ des permutations de X à supports *deux à deux disjoints*. Soient $S_1, \ldots, S_n$ des sous-ensembles deux à deux disjoints de X tels que $\mathrm{Supp}(\sigma_i) \subset S_i$ pour tout i (on peut prendre par exemple S_i égal à $\mathrm{Supp}(\sigma_i)$ pour tout i).

(3.6.1) Soit x appartenant à S_i. Si $x \in \mathrm{Fix}(\sigma_i)$ alors $\sigma_i(x) = x$, et $\sigma_i(x) \in S_i$. Si $x \in \mathrm{Supp}(\sigma_i)$ alors $\sigma_i(x) \in \mathrm{Supp}(\sigma_i) \subset S_i$ en vertu de 3.5.4. Ainsi, $\sigma_i(x) \in S_i$ pour tout $x \in S_i$.

(3.6.2) Soit x un élément de X. Si x n'appartient à aucun des S_i il est fixe par tous les σ_i, et l'on a donc $(\sigma_1 \ldots \sigma_n)(x) = x$.

Supposons maintenant qu'il existe i tel que $x \in S_i$; notons que cet entier i est unique car les S_i sont deux à deux disjoints. Si $j > i$ alors x n'appartient pas à S_j, et l'on a donc $\sigma_j(x) = x$. Par conséquent $(\sigma_{i+1} \ldots \sigma_n)(x) = x$ et $(\sigma_i\sigma_{i+1} \ldots \sigma_n)(x) = \sigma_i(x)$ L'image $\sigma_i(x)$ appartient à S_i (puisque c'est le cas de x, et en vertu de 3.6.1) ; elle n'appartient donc pas à S_j dès que $j < i$, et l'on a donc

$$\begin{aligned}(\sigma_1 \ldots \sigma_n)(x) &= (\sigma_1 \ldots \sigma_{i-1})(\sigma_i\sigma_{i+1} \ldots \sigma_n)(x) \\ &= (\sigma_1 \ldots \sigma_{i-1})(\sigma_i(x)) \\ &= \sigma_i(x).\end{aligned}$$

(3.6.3) Récapitulons : pour tout $x \in X$, on a $(\sigma_1 \ldots \sigma_n)(x) = x$ si x n'appartient à aucun des S_i ; dans le cas contraire x appartient à S_i pour un unique i, et l'on a $(\sigma_1 \ldots \sigma_n)(x) = \sigma_i(x)$. On voit grâce à ces formules que le produit $\sigma_1 \ldots \sigma_n$ ne change pas si l'on change l'ordre des σ_i : *le produit de permutations à supports deux à deux disjoints est commutatif.*

Comme $\sigma_i(x) \neq x$ dès que $x \in \mathrm{Supp}(\sigma_i)$, on déduit de ce qui précède que $(\sigma_1 \ldots \sigma_n)(x) = x$ *si et seulement si* x n'appartient à aucun des $\mathrm{Supp}(\sigma_i)$. Par conséquent, $\mathrm{Supp}(\sigma_1 \ldots \sigma_n)$ est égal à $\coprod_i \mathrm{Supp}(\sigma_i)$. Comme $\sigma_1 \ldots \sigma_n = \mathrm{Id}$ si et seulement si son support est vide, il en résulte que $\sigma_1 \ldots \sigma_n = \mathrm{Id}$ si et seulement si $\mathrm{Supp}(\sigma_i)$ est vide pour tout i, c'est-à-dire si et seulement si $\sigma_i = \mathrm{Id}$ pour tout i.

(3.6.4) Soit $d \in \mathbb{Z}$. En vertu de 3.5.5, on a $\mathrm{Supp}(\sigma_i^d) \subset \mathrm{Supp}(\sigma_i) \subset S_i$ pour tout i. Les résultats de 3.6.3 s'appliquent donc en remplaçant σ_i par σ_i^d pour tout i : si x est un élément de X n'appartenant à aucun des S_i alors $(\sigma_1^d \dots \sigma_n^d)(x) = x$; si x appartient à S_i pour un certain entier i nécessairement unique on a alors $(\sigma_1^d \dots \sigma_n^d)(x) = \sigma_i^d(x)$.

Notons que $\sigma_1^d \dots \sigma_n^d$ est par ailleurs égal à $(\sigma_1 \dots \sigma_n)^d$ puisque les σ_i commutent d'après 3.6.3 (on peut aussi le vérifier directement à l'aide de la formule explicite donnée ci-dessus).

(3.6.5) Remarque. On a donné en 2.7.5 (iv) un exemple de deux permutations ne commutant pas. Il découle de 3.6.3 que leurs supports ne peuvent pas être disjoints. Nous invitons le lecteur à le vérifier directement. Plus précisément il pourra s'assurer, en reprenant les notations de *loc. cit.*, que $\mathrm{Supp}(\tau) = \{a, b\}$ et $\mathrm{Supp}(\sigma) = \{a, c\}$; l'intersection des deux supports est égale à $\{a\}$, et est donc bien non vide.

(3.7) Cycles. Soit X un ensemble.

(3.7.1) Soient $a_1, \dots, a_\ell$ des éléments *deux à deux distincts* de X où ℓ est un entier au moins égal à 2. On note $(a_1 a_2 \dots a_\ell)$ la permutation σ de X définie comme suit :

- si $x \notin \{a_1, \dots, a_\ell\}$, alors $\sigma(x) = x$;
- pour tout i compris entre 1 et $\ell - 1$, on a $\sigma(a_i) = a_{i+1}$;
- on a $\sigma(a_\ell) = a_1$.

Une telle permutation est appelée un *ℓ-cycle*, ou un *cycle de longueur ℓ*, ou une *permutation circulaire de longueur ℓ*.

(3.7.2) Exemple. Supposons que $X = \{1, 2, 3, 4\}$. Le 3-cycle (134) est la permutation qui fixe 2, envoie 1 sur 3, envoie 3 sur 4 et envoie 4 sur 1. Autrement dit, c'est la permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}.$$

(3.7.3) Transpositions. Revenons au cas où X est un ensemble quelconque. Un 2-cycle de X est également appelé une *transposition*. Soient a_1 et a_2 deux éléments distincts de X. La transposition $(a_1 a_2)$ est la permutation qui échange a_1 et a_2 et fixe tous les autres éléments de X.

(3.8) Soit X un ensemble, soit ℓ un entier au moins égal à 2 et soient $a_1, \dots, a_\ell$ des éléments deux à deux distincts de X. Soit σ le ℓ-cycle $(a_1 \dots a_\ell)$.

(3.8.1) Il résulte de la définition de σ que $\mathrm{Supp}(\sigma) = \{a_1, \dots, a_\ell\}$.

(3.8.2) L'écriture de σ sous la forme $(a_1 \dots a_\ell)$ *n'est pas unique*. En effet, comme σ envoie a_2 sur a_3, a_3 sur a_4, …, a_ℓ sur a_1 et a_1 sur a_2 on peut également écrire $\sigma = (a_2 \dots a_\ell a_1)$, et plus généralement $\sigma = (a_i \dots a_\ell a_1 \dots a_{i-1})$ pour tout i compris entre 1 et ℓ.

Par exemple si $X = \{1, 2, 3, 4, 5\}$ et $\sigma = (1\ 3\ 4\ 2)$ alors σ est aussi égal à (3 4 2 1), à (4 2 1 3) et à (2 1 3 4).

(3.8.3) La bijection réciproque σ^{-1} envoie a_ℓ sur $a_{\ell-1}$, $a_{\ell-1}$ sur $a_{\ell-2}$, …, a_3 sur a_2, a_2 sur a_1 et a_1 sur a_ℓ. Par conséquent, σ^{-1} est le ℓ-cycle $(a_\ell a_{\ell-1} \dots a_3 a_2 a_1)$; autrement dit, l'inverse d'un cycle est un cycle, obtenu par renversement de l'ordre des termes.

Ainsi si $X = \{1, 2, 3, 4, 5\}$ et $\sigma = (1\ 3\ 4\ 2)$ alors $\sigma^{-1} = (2\ 4\ 3\ 1)$.

(3.8.4) Soit $c \in \mathbb{Z}/\ell\mathbb{Z}$. Il existe un unique entier $n \in \{1, \dots, \ell\}$ tel que $c = \overline{n}$, et nous poserons $a_c = a_n$. Par exemple, $a_{\overline{1}} = a_1$ et $a_{\overline{0}} = a_{\overline{\ell}} = a_\ell$. Cette notation est commode pour décrire l'action de σ sur $\{a_1, \dots, a_\ell\}$ sans avoir à traiter à part le cas de a_ℓ. On a en effet $\sigma(a_n) = a_{n+1}$ pour tout n compris entre 1 et $\ell - 1$, et $\sigma(a_\ell) = a_1$. Mais comme $\overline{1} = \overline{\ell} + \overline{1}$, on voit qu'on peut finalement écrire $\sigma(a_{\overline{n}}) = a_{\overline{n}+\overline{1}}$ pour tout n, et donc également $\sigma^{-1}(a_{\overline{n}}) = a_{\overline{n}-\overline{1}}$ pour tout n. On en déduit immédiatement que $\sigma^d(a_{\overline{n}}) = a_{\overline{n}+\overline{d}}$ pour tout $d \in \mathbb{Z}$ et tout n.

Par exemple, supposons que X est l'ensemble $\{1, 2, 3, 4, 5, 6, 7\}$, que $\ell = 7$ et que $a_1 = 2, a_2 = 4, a_3 = 1, a_4 = 5, a_5 = 7, a_6 = 6$ et $a_7 = 3$. Le cycle σ est donc $(2\ 4\ 1\ 5\ 7\ 6\ 3)$. Calculons $\sigma^{-283}(5)$. On a $\sigma^{-283}(5) = \sigma^{-283}(a_4) = a_{\overline{4}-\overline{283}}$. Mais comme $280 = 7 \times 40$ on a $-\overline{283} = \overline{0}$. Il vient $a_{\overline{4}-\overline{283}} = a_{\overline{4}-\overline{3}} = a_{\overline{1}} = a_1 = 2$. On a donc $\sigma^{-283}(5) = 2$.

(3.8.5) On a pour tout n l'égalité $\sigma^\ell(a_{\overline{n}}) = a_{\overline{n}+\overline{\ell}} = a_{\overline{n}}$: autrement dit, on a $\sigma^\ell(x) = x$ pour tout $x \in \mathrm{Supp}(\sigma)$. Comme il est clair que $\sigma^\ell(x) = x$ si $x \in \mathrm{Fix}(\sigma)$ on a $\sigma^\ell(x) = x$ pour tout $x \in X$, et partant $\sigma^\ell = \mathrm{Id}$.

Soit d un entier strictement compris entre 0 et ℓ. On a l'égalité $\sigma^d(a_{\overline{1}}) = a_{\overline{1}+\overline{d}}$, et ce dernier terme diffère de $a_{\overline{1}}$ car $\overline{d} \neq \overline{0}$; par conséquent, $\sigma^d(a_1) \neq a_1$, et $\sigma^d \neq \mathrm{Id}$. L'entier ℓ est donc le plus petit élément de $\{d > 0, \sigma^d = \mathrm{Id}\}$.

(3.8.6) Soit $x \in \mathrm{Supp}(\sigma)$. On a $\sigma^d(x) \in \mathrm{Supp}(\sigma)$ pour tout $d \in \mathbb{Z}$ (c'est vrai pour n'importe quelle permutation, *cf.* 3.5.4). Réciproquement, tout élément y de $\mathrm{Supp}(\sigma)$ est de la forme $\sigma^d(x)$ pour un certain $d \in \mathbb{Z}$, qu'on peut même choisir dans $\{0, \dots, \ell - 1\}$. En effet, choisissons i et j tels que $x = a_{\overline{i}}$ et $y = a_{\overline{j}}$. Il existe alors un unique entier d dans $\{0, \dots, \ell - 1\}$ tel que $\overline{d} = \overline{j} - \overline{i}$, et l'on a $\sigma^d(x) = \sigma^d(a_{\overline{i}}) = a_{\overline{i}+\overline{d}} = a_{\overline{j}} = y$.

On a donc $\mathrm{Supp}(\sigma) = \{\sigma^d(x)\}_{d \in \mathbb{Z}}$.

(3.9) Soit X un ensemble et soit S un sous-ensemble fini de X, de cardinal $\ell \geqslant 2$. Comment donner la liste de tous les cycles de support S ? Il faut faire un peu attention : si l'on se donne deux numérotations différentes $a_1, \dots, a_\ell$ et $b_1, \dots, b_\ell$ des éléments de S, il se peut que les deux cycles $(a_1 \dots a_\ell)$ et $(b_1 \dots, b_\ell)$ soient égaux (3.8.2).

On procède donc comme suit : on choisit (arbitrairement) un élément x de S. On sait que tout cycle de support S peut toujours s'écrire sous la forme $(x\alpha_1 \dots \alpha_{\ell-1})$ (on l'a signalé au 3.8.2). Et il se trouve que le fait de fixer le premier élément de l'écriture du cycle (on le prend égal à x) lève toute ambiguïté : en effet, si un cycle σ s'écrit $(x\alpha_1 \dots \alpha_{\ell-1})$, on a nécessairement $\alpha_1 = \sigma(x), \alpha_2 = \sigma(\alpha_1) = \sigma^2(x)$, etc. : les α_i sont uniquement déterminés.

Se donner un cycle de support S revient donc à choisir une numérotation $\alpha_1, \dots, \alpha_{\ell-1}$ des éléments de $S \setminus \{x\}$, deux numérotations différentes conduisant à deux cycles différents. On a ainsi autant de cycles qu'il y a de telles numérotations ; mais une numérotation $\alpha_1, \dots, \alpha_{\ell-1}$ des éléments de $S \setminus \{x\}$ est simplement une bijection de $\{1, \dots, \ell - 1\}$ sur $S \setminus \{x\}$ (celle qui envoie i sur α_i), et il y en a donc exactement $(\ell - 1)!$ (lemme 3.3).

Par exemple, supposons que $X = \{1, \dots, 11\}$ et que $S = \{1, 4, 8, 11\}$. Il y a alors $(4 - 1)! = 6$ cycles de support S, qui sont les suivants, en décidant de les écrire en commençant par 1 :

(1 4 8 11) (1 4 11 8) (1 8 4 11) (1 8 11 4) (1 11 4 8) (1 11 8 4).

(3.10) Le théorème qui suit joue un rôle absolument central dans la théorie des permutations des ensembles finis. Il permet dans de nombreux cas de ramener l'étude d'une permutation quelconque à celle de permutations circulaires, qui sont très faciles à manipuler.

(3.11) Théorème. *Soit X un ensemble fini et soit σ une permutation de X. Il existe une famille finie $C_1, \dots, C_r$ de cycles sur X à supports deux à deux disjoints tels que $\sigma = C_1 C_2 \dots C_r$. De plus, cette écriture est «unique à permutation près des C_i». Cela signifie précisément que si $D_1 D_2 \dots D_s$ est une autre écriture de σ comme produit de cycles à supports deux à deux disjoints, alors $r = s$ et il existe une permutation τ de $\{1, \dots, r\}$ telle que $D_i = C_{\tau(i)}$ pour tout i.*

Démonstration. Elle est assez longue, et comprend plusieurs étapes.

(3.11.1) *Construction de cycles.* Soit x un élément de $\mathrm{Supp}(\sigma)$. Commençons par montrer qu'il existe $d > 0$ tel que $\sigma^d(x) = x$. On remarque tout d'abord que comme X est fini, l'ensemble $\{\sigma^i(x)\}_{i\in\mathbb{N}}$ est fini. Il existe donc nécessairement deux entiers distincts $i > j$ tels que $\sigma^i(x) = \sigma^j(x)$; en appliquant σ^{-j} aux deux membres de l'égalité il vient $\sigma^{i-j}(x) = x$, d'où notre assertion (en prenant $d = i - j$).

L'ensemble $\{d > 0, \sigma^d(x) = x\}$ étant non vide, il possède un plus petit élément ℓ. On a $\sigma^\ell(x) = x$, ce qui entraîne que $\ell \geqslant 2$ car $\sigma(x) \neq x$ puisque $x \in \mathrm{Supp}(\sigma)$. De plus, si $i > j$ sont deux entiers positifs distincts strictement inférieurs à ℓ alors $\sigma^i(x) \neq \sigma^j(x)$: en effet si l'on avait $\sigma^i(x) = \sigma^j(x)$ on aurait aussi $\sigma^{i-j}(x) = x$ (par application de σ^{-j} des deux côtés), ce qui est absurde puisque $0 < i - j < \ell$. Les éléments $x, \sigma(x), \dots, \sigma^{\ell-1}(x)$ de X sont donc deux à deux distincts. Soit C_x le ℓ-cycle $(x\sigma(x)\dots\sigma^{\ell-1}(x))$.

Soit y appartenant à $\mathrm{Supp}(C_x)$. Il résulte de la définition de C_x et de l'égalité $x = \sigma^\ell(x)$ que $C_x(y) = \sigma(y)$ et $C_x^{-1}(y) = \sigma^{-1}(y)$. On en déduit immédiatement par récurrence qu'on a plus généralement l'égalité $C_x^d(y) = \sigma^d(y)$ pour tout $d \in \mathbb{Z}$. La formule $\mathrm{Supp}(C_x) = \{C_x^d(y)\}_{d\in\mathbb{Z}}$ (3.8.6) peut alors se récrire

$$\mathrm{Supp}(C_x) = \{\sigma^d(y)\}_{d\in\mathbb{Z}}.$$

(3.11.2) Soient x et x' deux éléments du support de σ tels que

$$\mathrm{Supp}(C_x) \cap \mathrm{Supp}(C_{x'}) \neq \varnothing.$$

On a alors $C_x = C_{x'}$. En effet, choisissons $y \in \mathrm{Supp}(C_x) \cap \mathrm{Supp}(C_{x'})$. On a d'après 3.11.1

$$\mathrm{Supp}(C_x) = \{\sigma^d(y)\}_{d\in\mathbb{Z}} = \mathrm{Supp}(C_{x'})$$

et $C_x(z) = \sigma(z) = C_{x'}(z)$ pour tout $z \in \mathrm{Supp}(C_x) = \mathrm{Supp}(C_{x'})$. Les permutations C_x et $C_{x'}$ ayant même support et coïncidant sur ce support commun, elles sont égales.

(3.11.3) *Existence de la décomposition.* On a expliqué au 3.11.1 ci-dessus comment associer à chaque élément x de $\mathrm{Supp}(\sigma)$ un cycle C_x. Soit $\mathscr{C}$ l'ensemble des cycles de la forme C_x pour $x \in \mathrm{Supp}(\sigma)$. Soit r le cardinal de $\mathscr{C}$; on

choisit une numérotation $C_1, \ldots, C_r$ des éléments de $\mathscr{C}$. D'après 3.11.1 on a $C_i(x) = \sigma(x)$ pour tout i et tout $x \in \mathrm{Supp}(C_i)$; et en vertu de 3.11.2 les supports des C_i sont deux à deux disjoints.

Soit $x \in X$. Supposons tout d'abord que x n'appartient à aucun des $\mathrm{Supp}(C_i)$. Dans ce cas x n'appartient pas au support de σ, car sinon x appartiendrait au support de C_x, qui est l'un des C_i ; on a donc $\sigma(x) = x$. Supposons maintenant que x appartient au support de C_i pour un certain i (nécessairement unique). On a alors $\sigma(x) = C_i(x)$.

Récapitulons : les C_i sont des cycles à supports deux à deux disjoints ; si x n'appartient à aucun des $\mathrm{Supp}(C_i)$ alors $\sigma(x) = x$; si x appartient au support de C_i pour un certain i alors $\sigma(x) = C_i(x)$. Ceci implique en vertu de 3.6 que $\sigma = C_1 \ldots C_r$, et achève la preuve de la partie «existence» du théorème.

(3.11.4) *Unicité de la décomposition.* Supposons que σ s'écrive $D_1 \ldots D_s$ où les D_i sont des cycles à supports deux à deux disjoints. Le support de σ est alors la réunion disjointe des supports des D_i.

Fixons i. Soit $d \in \mathbb{Z}$. Comme $\sigma = D_1 \ldots D_s$, il résulte de 3.6.4 que

$$(*) \quad \forall y \in \mathrm{Supp}(D_i),\ \sigma^d(y) = D_i^d(y).$$

Choisissons $x \in \mathrm{Supp}(D_i)$. On a

$$\mathrm{Supp}(D_i) = \{D_i^d(x)\}_{d\in\mathbb{Z}} = \{\sigma^d(x)\}_{d\in\mathbb{Z}} = \mathrm{Supp}(C_x)$$

(la première égalité provient de 3.8.6, la seconde de $(*)$ et la troisième de 3.11.1). On a par ailleurs pour tout élément y de $\mathrm{Supp}(D_i) = \mathrm{Supp}(C_x)$ les égalités $D_i(y) = \sigma(y) = C_x(y)$ (la première provient de $(*)$ et la seconde de 3.11.1). Les permutations D_i et C_x ont donc même support, et elles coïncident sur ce support commun ; en conséquence, elles sont égales.

On déduit de ce qui précède que $\{D_1, \ldots, D_s\}$ est exactement l'ensemble des cycles de la forme C_x pour $x \in \mathrm{Supp}(\sigma)$. Autrement dit, l'ensemble $\{D_1, \ldots, D_s\}$ est égal à $\{C_1, \ldots, C_r\}$, ce qui achève la démonstration. □

(3.12) Commentaire. Dans le théorème 3.11, $\sigma = C_1 \ldots C_r$ peut également s'écrire comme le produit des C_i effectué dans n'importe quel ordre, car le produit de permutations à supports deux à deux disjoints est commutatif (3.6) ; on ne peut donc espérer mieux que l'unicité «à permutation près».

Malgré cette petite restriction, on parlera souvent de *la* décomposition d'une permutation en produit de cycles à supports deux à deux disjoints.

(3.13) Exemples triviaux. Soit X un ensemble fini.

(3.13.1) L'écriture de Id_X comme produit de cycles à supports deux à deux disjoints est simplement son écriture comme *produit vide* de tels cycles ; il n'y a donc *aucun cycle* dans la décomposition de Id_X.

(3.13.2) Soit C un cycle de X. L'écriture de C comme produit de cycles à supports deux à deux disjoints est simplement l'écriture $C = C$; il y a donc un seul cycle dans la décomposition de C, à savoir C lui-même.

(3.14) Nous allons maintenant décrire l'algorithme permettant d'écrire une permutation quelconque σ d'un ensemble fini X comme produit de cycles à supports deux à deux disjoints. Cet algorithme est directement inspiré de la preuve du théorème 3.11.

(3.14.1) Le cœur de cette preuve consistait à associer à un élément x de $\mathrm{Supp}(\sigma)$ un cycle C_x. Il découle de la définition de ce dernier qu'il s'écrit $(x_1 \dots x_\ell)$ où (x_i) est la suite construite récursivement par le procédé suivant :

- $x_1 = x$;
- si $\sigma(x_i) = x$, on arrête ; sinon on pose $x_{i+1} = \sigma(x_i)$.

(3.14.2) La décomposition de σ s'obtient alors comme suit. Si $\sigma = \mathrm{Id}$ il n'y a rien à faire (3.13.1). Sinon, on construit une suite $y_1, \dots, y_s$ d'éléments de $\mathrm{Supp}(\sigma)$ par le procédé récursif suivant :

- on prend pour y_1 n'importe quel élément de $\mathrm{Supp}(\sigma)$;
- si la réunion des supports des cycles $C_{y_1}, \dots, C_{y_i}$ est égale au support de σ (c'est-à-dire si tout élément de X en dehors de $\mathrm{Supp}(C_{y_1}) \coprod \dots \coprod \mathrm{Supp}(C_{y_i})$ est fixe sous σ), on arrête ; sinon, on prend pour y_{i+1} n'importe quel élément de $\mathrm{Supp}(\sigma)$ en dehors de $\mathrm{Supp}(C_{y_1}) \coprod \dots \coprod \mathrm{Supp}(C_{y_i})$.

L'écriture cherchée est alors $\sigma = C_{y_1} C_{y_2} \dots C_{y_s}$. (Bien entendu, les cycles C_{y_i} sont eux-mêmes construits par le procédé décrit au 3.14.1).

(3.15) Un exemple concret. On prend pour X l'ensemble $\{1, 2, \dots, 17\}$ et pour σ la permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 \\ 3 & 5 & 7 & 10 & 11 & 8 & 1 & 6 & 4 & 16 & 13 & 12 & 17 & 2 & 15 & 9 & 14 \end{pmatrix}$$

Nous allons appliquer pas à pas l'algorithme décrit ci-dessus. La permutation σ est différente de l'identité, on va donc construire une suite $(y_1, \dots, y_s)$ comme au 3.14.2. On prend pour y_1 n'importe quel élément du support de σ, disons 1. Pour décrire le cycle C_1, on procède comme indiqué au 3.14.1 : on itère σ jusqu'au moment où on retombe sur 1. On a

$$\begin{aligned} \sigma(1) &= 3 \\ \sigma(3) &= 7 \\ \sigma(7) &= 1. \end{aligned}$$

Le cycle C_1 est donc égal à (1 3 7). Son support est $\{1, 3, 7\}$. Il y a des éléments de $\mathrm{Supp}(\sigma)$ qui n'appartiennent pas à ce dernier, par exemple 2. On pose donc $y_2 = 2$. Calculons C_2. On a

$$\begin{aligned} \sigma(2) &= 5 \\ \sigma(5) &= 11 \\ \sigma(11) &= 13 \\ \sigma(13) &= 17 \\ \sigma(17) &= 14 \\ \sigma(14) &= 2. \end{aligned}$$

Le cycle c_2 est donc égal à (2 5 11 13 17 14). La réunion des supports de C_1 et C_2 est égale à $\{1, 2, 3, 5, 7, 11, 13, 14, 17\}$. Il y a des éléments de $\mathrm{Supp}(\sigma)$ qui n'appartiennent pas à ce dernier, par exemple 4. On pose donc $y_3 = 4$. Calculons

C_4. On a

$$\begin{aligned}\sigma(4) &= 10\\ \sigma(10) &= 16\\ \sigma(16) &= 9\\ \sigma(9) &= 4.\end{aligned}$$

Le cycle C_4 est donc égal à (4 10 16 9). La réunion des supports de C_1, C_2 et C_4 est égale à $\{1, 2, 3, 4, 5, 7, 9, 10, 11, 13, 14, 16, 17\}$. Il y a des éléments de $\mathrm{Supp}(\sigma)$ qui n'appartiennent pas à ce dernier, par exemple 6. On pose donc $y_4 = 6$. Calculons C_6. On a

$$\begin{aligned}\sigma(6) &= 8\\ \sigma(8) &= 6.\end{aligned}$$

Le cycle C_6 est donc égal à $(6; 8)$. La réunion des supports de C_1, C_2, C_4 et C_6 est égale à $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 13, 14, 16, 17\}$. Les deux éléments restants sont 12 et 15, qui sont tous deux fixes par σ. L'algorithme s'arrête donc ici et l'écriture de σ comme produit de cycles à supports deux à deux disjoints est la suivante :

$$\begin{aligned}\sigma &= C_{y_1}C_{y_2}C_{y_3}C_{y_4}\\ &= C_1C_2C_4C_6\\ &= (1\ 3\ 7)\ (2\ 5\ 11\ 13\ 17\ 14)\ (4\ 10\ 16\ 9)\ (6\ 8).\end{aligned}$$

(3.16) En 3.4.4, nous avons donné la liste de tous les éléments de S_4, présentés par tableau. Nous allons maintenant la redonner en considérant les différents types possibles de décomposition en produit de cycles à supports deux à deux disjoints (le «type» d'une décomposition est le nombre de cycles de chaque longueur qu'elles met en jeu) ; pour donner explicitement la liste des permutations de chaque type, nous avons utilisé la description des cycles de support fixé donnée en 3.9.

- *Aucun cycle :* Id.
- *Une transposition* :$(1\ 2), (1\ 3), (1\ 4), (2\ 3), (2\ 4), (3\ 4)$.
- *Un* 3*-cycle* :
  $(1\ 2\ 3), (1\ 3\ 2), (1\ 2\ 4), (1\ 4\ 2), (1\ 4\ 3), (1\ 3\ 4), (2\ 3\ 4), (2\ 4\ 3)$.
- *Un* 4*-cycle* :
  $(1\ 2\ 3\ 4), (1\ 2\ 4\ 3), (1\ 3\ 2\ 4), (1\ 3\ 4\ 2), (1\ 4\ 2\ 3), (1\ 4\ 3\ 2)$.
- *Deux transpositions* : $(1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)$.

(3.17) Soit X un ensemble.

(3.17.1) Soient $a_1, \ldots, a_\ell$ des éléments deux à deux distincts de X. On vérifie immédiatement que

$$(a_1a_2 \ldots a_\ell) = (a_1a_2)(a_2a_3) \ldots (a_{\ell-1}a_\ell).$$

Un cycle de longueur ℓ peut donc toujours s'écrire comme le produit de $\ell - 1$ transpositions.

(3.17.2) Si X est fini, le théorème 3.11, assure que toute permutation de X peut s'écrire comme un produit de cycles (à supports deux à deux disjoints).

Comme tout cycle sur X est produit de transpositions en vertu de 3.17.1, on voit que *toute permutation de X est produit de transpositions.*

(3.18) Nous nous proposons maintenant d'introduire un invariant fondamental d'une permutation, sa *signature*. Nous la définirons d'abord dans le cas où $X = \{1, \ldots, n\}$, nous verrons plus tard comment l'étendre à un ensemble fini quelconque.

(3.19) Soit n un entier $\geqslant 0$ et soit $\sigma \in S_n$. Soit $\mathscr{P}$ l'ensemble des parties de $\{1, \ldots, n\}$ de cardinal 2. Si $A = \{i, j\}$ est un élément de $\mathscr{P}$, son image $\sigma(A) = \{\sigma(i), \sigma(j)\}$ est encore un élément de $\mathscr{P}$ (en effet comme σ est injective on a $\sigma(i) \neq \sigma(j)$ et $\sigma(A)$ est donc bien de cardinal 2). Si $B = \{u, v\}$ est un élément de $\mathscr{P}$, il existe un unique élément A de $\mathscr{P}$ tel que $\sigma(A) = B$, à savoir $\{\sigma^{-1}(u), \sigma^{-1}(v)\}$. La formule $A \mapsto \sigma(A)$ définit donc une bijection de $\mathscr{P}$ sur lui-même.

On dit qu'un élément $A = \{i, j\}$ de $\mathscr{P}$ est une *inversion* de σ si $j - i$ et $\sigma(j) - \sigma(i)$ sont de signes opposés, soit encore, en termes un peu plus informels, si σ renverse l'ordre de i et j. On note $\mathrm{I}(\sigma)$ le nombre d'inversions de σ. Supposons par exemple que $n = 4$ et que σ est la permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}.$$

Les inversions de σ sont $\{1, 4\}$, $\{2, 4\}$ et $\{3, 4\}$, et $\mathrm{I}(\sigma) = 3$.

(3.20) Théorème. *Soit n un entier et soient σ et τ deux permutations de $\{1, \ldots, n\}$. L'entier $\mathrm{I}(\sigma) + \mathrm{I}(\tau) - \mathrm{I}(\sigma\tau)$ est pair.*

Démonstration. Soit $\mathscr{P}$ l'ensemble des parties de $\{1, \ldots, n\}$ de cardinal 2. Soit E^+ le sous-ensemble de $\mathscr{P}$ constitué des parties A telles que τ ne renverse pas l'ordre des éléments de A, et soit E^- le sous-ensemble de $\mathscr{P}$ constitué des parties A telles que τ renverse l'ordre des éléments de A ; autrement dit, E^- est l'ensemble des inversions de τ. On définit F^+ et F^- de façon analogue avec σ à la place de τ.

Soit $A \in \mathscr{P}$. La permutation $\sigma\tau$ renverse l'ordre des éléments de A si et seulement si on est dans l'un des deux cas suivants :

- τ ne renverse pas l'ordre des éléments de A, et σ renverse l'ordre des éléments de $\tau(A)$ – autrement dit, $A \in E^+$ et $\tau(A) \in F^-$;
- τ renverse l'ordre des éléments de A, et σ ne renverse pas l'ordre des éléments de $\tau(A)$ – autrement dit, $A \in E^-$ et $\tau(A) \in F^+$.

Soit G^- le sous-ensemble de $\mathscr{P}$ constitué des parties A dont l'image par τ appartient à F^-. Puisque $A \mapsto \sigma(A)$ définit une bijection de $\mathscr{P}$ sur lui-même (*cf.* 3.19), le cardinal de G^- est égal à celui de F^-, c'est-à-dire à $\mathrm{I}(\sigma)$. Par ce qui précède, la permutation $\sigma\tau$ renverse l'ordre des éléments de A si et seulement si A appartient à E^- et pas à G^-, ou A appartient à G^- et pas à E^-. Il vient

$$\begin{aligned} \mathrm{I}(\sigma\tau) &= (\mathrm{card}(E^-) - \mathrm{card}(E^- \cap G^-)) + (\mathrm{card}(G^-) - \mathrm{card}(E^- \cap G^-)) \\ &= \mathrm{card}(E^-) + \mathrm{card}(G^-) - 2 \cdot \mathrm{card}(E^- \cap G^-) \\ &= \mathrm{I}(\tau) + \mathrm{I}(\sigma) - 2 \cdot \mathrm{card}(E^- \cap G^-.) \end{aligned}$$

Ainsi

$$\mathrm{I}(\sigma) + \mathrm{I}(\tau) - \mathrm{I}(\sigma\tau) = 2 \cdot \mathrm{card}(E^- \cap G^-)$$

est bien pair. □

(3.21) Soit n un entier et soit $\sigma \in S_n$. On appelle *signature* de σ, et l'on note $\varepsilon(\sigma)$, l'élément $(-1)^{\mathrm{I}(\sigma)}$ de $\{-1, 1\}$. On dit que σ est paire si sa signature vaut 1 (ce qui veut dire qu'elle a un nombre pair d'inversions), et impaire si sa signature vaut (-1), ce qui veut dire qu'elle a un nombre impair d'inversions.

Par exemple l'identité est paire (aucune inversion) ; la permutation considérée à la fin de 3.19 est impaire (trois inversions).

(3.22) Nous allons maintenant énoncer la propriété fondamentale de la signature. Soit n un entier et soient σ et τ deux éléments de S_n. On a alors

$$\varepsilon(\sigma\tau) = \underbrace{(-1)^{\mathrm{I}(\sigma\tau)} = (-1)^{\mathrm{I}(\sigma)+\mathrm{I}(\tau)}}_{\text{d'après le th. 3.20}} = (-1)^{\mathrm{I}(\sigma)} \cdot (-1)^{\mathrm{I}(\tau)} = \varepsilon(\sigma)\varepsilon(\tau).$$

Notons une première conséquence de ce fait : on a pour tout $\sigma \in S_n$ l'égalité

$$1 = \varepsilon(\mathrm{Id}) = \varepsilon(\sigma\sigma^{-1}) = \varepsilon(\sigma)\varepsilon(\sigma^{-1}),$$

ce qui entraîne que $\varepsilon(\sigma) = \varepsilon(\sigma^{-1})^{-1} = \varepsilon(\sigma^{-1})$ (un élément de $\{-1, 1\}$ est égal à son propre inverse pour la multiplication).

(3.23) Quelques calculs de signature. Soit n un entier.

(3.23.1) Le cas d'une transposition. Soit $\tau = (ab)$ une transposition de S_n ; comme $(ab) = (ba)$ on peut toujours supposer que $a < b$.

Soient i et j deux entiers avec $i < j$. On déduit de la description directe de τ que l'on a $\tau(i) > \tau(j)$ si et seulement si on est dans l'un des deux cas suivants :

- $i = a$ et $a < j \leqslant b$;
- $a \leqslant i < b$ et $j = b$.

Il y a $b - a$ couples (i, j) qui satisfont la première condition, et $b - a$ couples (i, j) qui satisfont la seconde. Il y a par ailleurs exactement un couple qui satisfait les deux, à savoir (a, b). Il vient

$$\mathrm{I}(\tau) = b - a + b - a - 1 = 2(b - a) - 1,$$

et $\mathrm{I}(\tau)$ est donc impair. Par conséquent $\varepsilon(\tau) = -1$: une transposition est impaire.

(3.23.2) Le cas d'un cycle. Soit ℓ un entier compris entre 2 et n et soit c un ℓ-cycle de S_n. On a vu au 3.17.1 que c est le produit de $\ell - 1$ transpositions. Comme la signature d'une transposition est (-1), il vient $\varepsilon(c) = (-1)^{\ell-1}$. La parité d'un cycle est donc opposée à celle de sa longeur.

(3.23.3) Le cas d'une permutation quelconque. Soit σ une permutation quelconque de $\{1, \ldots, n\}$. Pour calculer $\varepsilon(\sigma)$, le plus simple est de calculer la décomposition de σ en produit de cycles à supports deux à deux disjoints par l'algorithme décrit plus haut, puis d'appliquer 3.23.2, et la multiplicativité de la signature.

Par exemple, soit σ la permutation de $\{1, \ldots, 17\}$ étudiée au 3.15. On a vu que σ s'écrit comme le produit de quatre cycles (à supports deux à deux disjoints) : un de longueur 3, un de longueur 6, un de longueur 4 et un de longueur 2. Par conséquent, $\varepsilon(\sigma) = (-1)^{2+5+3+1} = (-1)^{11} = (-1)$ (penser à retrancher 1 à la longueur de chaque cycle pour calculer la signature !).

Comparez l'efficacité de cette méthode à celle qui consisterait à compter le nombre d'inversions de σ (il y aurait $\frac{17\times 16}{2} = 136$ ensembles $\{i, j\}$ à tester !).

(3.24) Signature et écriture comme produit de transpositions. Soit n un entier et soit $\sigma \in S_n$. On a vu que σ peut toujours s'écrire comme un produit de transpositions $\tau_1 \dots \tau_r$. Mais attention : ni cette écriture ni même l'entier r (le nombre de transpositions impliquées) ne sont uniques : par exemple dans S_3 le 3-cycle (123) est égal à (3 1)(1 2), à (1 2)(2 3), ou encore à (3 2)(2 1)(3 2)(2 1) (vérifiez-le !).

Par contre, la *parité* de r est bien déterminée : r est pair si σ est paire, et impair dans le cas contraire. En effet comme la signature d'une transposition est égale à (-1), on a $\varepsilon(\sigma) = (-1)^r$.

4 Sous-groupes

(4.1) Définition. Soit G un groupe. Un *sous-groupe* de G est un sous-ensemble H de G possédant les propriétés suivantes :

- $e \in H$;
- pour tout élément h de H on a $h^{-1} \in H$ (on dit aussi que «H est stable par inversion») ;
- pour tout couple (h, h') d'éléments de H on a $hh' \in H$ (on dit aussi que «H est stable par produit»).

Si H est un sous-groupe de G, la formule $(h, h') \mapsto hh'$ définit une application de $H \times H$ vers H (puisque H est stable par produit), et donc une loi de composition interne sur H. Cette loi est associative – puisque le produit est associatif sur G tout entier. Elle possède un élément neutre, à savoir e (qui appartient à H par hypothèse). Et tout élément h de H a un symétrique pour cette loi, à savoir h^{-1} (qui appartient à H puisque ce dernier est stable par inversion). Ainsi, cette loi fait de H un groupe. Pour des raisons évidentes, on dit parfois que cette structure de groupe est *héritée* de celle de G.

Lorsqu'on considérera un sous-groupe de G, il sera toujours implicitement considéré comme muni de la structure de groupe héritée de celle de G.

(4.2) Exemples.

(4.2.1) *Les cas triviaux.* Si G est un groupe, G et $\{e\}$ sont des sous-groupes de G.

(4.2.2) Le sous-ensemble $\mathbb{R}^\times$ de $\mathbb{C}^\times$ en est un sous-groupe (et sa structure de groupe héritée de celle de $\mathbb{C}^\times$ est sa structure de groupe usuelle).

(4.2.3) Le sous-ensemble $\{-1, 1\}$ de $\mathbb{R}^\times$ en est un sous-groupe.

(4.2.4) Soit K le sous-ensemble $\{\mathrm{Id}, (12)(34), (13)(24), (14)(23)\}$ de S_4. Il contient l'identité, il est stable par inversion (vérifiez que chacun de ses éléments est égal à son propre inverse), et par produit (vérifiez que

$$(12)(34)(13)(24) = (14)(23)$$

et qu'on a les deux autres égalités analogues). C'est donc un sous-groupe de S_4.

(4.2.5) Donnons maintenant deux exemples un peu plus théoriques. Soit G un groupe.

- Soit H un sous-groupe de G et soit H' un sous-ensemble de H. L'ensemble H' est un sous-groupe de H si et seulement si c'est un sous-groupe de G. En effet, les trois conditions que doit vérifier H' pour être un sous-groupe de H sont les mêmes que celles qu'il doit satisfaire pour être un sous-groupe de G (écrivez-les !).
- Soit $(H_i)_{i\in I}$ une famille de sous-groupes de G indexée par un certain ensemble d'indices I. L'intersection des H_i est alors un sous-groupe de G. Expliquons brièvement pourquoi.
  Comme chacun des H_i est un sous-groupe de G, on a $e \in H_i$ pour tout I, et donc $e \in \bigcap H_i$.
  Soit $h \in \bigcap H_i$. Pour tout i, l'élément h de G appartient à H_i, ce qui entraîne que $h^{-1} \in H_i$ puisque H_i est un sous-groupe de G ; comme ceci vaut quel que soit i, on a $h^{-1} \in \bigcap H_i$.
  Soient h et h' deux éléments de $\bigcap H_i$. Pour tout i, les éléments h et h' de G appartiennent à H_i, ce qui entraîne que $hh' \in H_i$ puisque H_i est un sous-groupe de G ; comme ceci vaut quel que soit i, on a $hh' \in \bigcap H_i$, et $\bigcap H_i$ est donc bien un sous-groupe de G.

(4.3) Sous-groupe engendré par un élément. Soit G un groupe et soit $g \in G$.

(4.3.1) Si H est un sous-groupe de G contenant g, il contient $g^n = \underbrace{gg\dots g}_{n \text{ termes}}$ pour tout $n \in \mathbb{N}$ (puisqu'il est stable par produit), et même en fait g^n pour tout $n \in \mathbb{Z}$ (puisqu'il est stable par inversion).

Par ailleurs, $\{g^n\}_{n\in\mathbb{Z}}$ est lui-même un sous-groupe de G, qui contient évidemment $g = g^1$; en effet il contient $e = g^0$, est stable par produit ($g^n g^{n'} = g^{n+n'}$ pour tout (n, n')) et par inversion ($(g^n)^{-1} = g^{-n}$ pour tout n). C'est donc le plus petit sous-groupe de G contenant g ; on l'appelle le *sous-groupe engendré par* g et on le note souvent $\langle g\rangle$.

(4.3.2) Attention : si G est un groupe abélien noté additivement, $\langle g\rangle$ est l'ensemble $\{ng\}_{n\in\mathbb{Z}}$.

(4.3.3) Exemple. Supposons que $G = S_4$ et $g = (12)$. On a $g^2 = \mathrm{Id}$ et donc $g^{2n} = \mathrm{Id}$ pour tout n et $g^{2n+1} = g$ pour tout n. Ainsi $\langle g\rangle$ est simplement l'ensemble à deux éléments $\{\mathrm{Id}, g\} = \{\mathrm{Id}, (12)\}$.

(4.3.4) Exemple. Supposons que $G = S_4$ et $g = (1234)$. On a $g^4 = \mathrm{Id}$. Soit n un entier relatif. Effectuons la division euclidienne de n par 4. Elle fournit une écriture $n = 4q + r$ avec $0 \leqslant r \leqslant 3$. On a alors

$$g^n = g^{4q+r} = (g^4)^q g^r = e^q g^r = g^r.$$

Ainsi $\langle g\rangle$ est simplement $\{\mathrm{Id}, g, g^2, g^3\}$. Comme $3 = 4-1$ on a $g^3 = g^{-1} = (1432)$. Quant à g^2, un calcul direct montre que c'est la permutation

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix} = (13)(24).$$

Ainsi $\langle g\rangle = \{\mathrm{Id}, (1234), (13)(24), (1432)\}$.

(4.3.5) Exemple. Supposons que $G = \mathbb{Z}$, sans faire d'hypothèse particulière sur g. Le sous-groupe $\langle g\rangle$ de $\mathbb{Z}$ est l'ensemble des entiers de la forme $ng = gn$

avec $n \in \mathbb{Z}$; c'est donc tout simplement l'ensemble des multiples de g, que l'on note en général $g\mathbb{Z}$.

Ainsi le sous-groupe de $\mathbb{Z}$ engendré par 2 est l'ensemble $2\mathbb{Z}$ des entiers pairs, celui engendré par 3 est l'ensemble $3\mathbb{Z}$ des multiples de 3, etc.

Le théorème ci-dessous montre que *tous* les sous-groupes de $\mathbb{Z}$ s'obtiennent ainsi.

(4.4) Théorème. *Soit G un sous-groupe de $\mathbb{Z}$. Il existe un unique entier $d \geqslant 0$ tel que $G = d\mathbb{Z}$.*

Démonstration. Montrons tout d'abord l'existence. Si $G = \{0\}$ alors $G = 0\mathbb{Z}$. Supposons maintenant G non trivial ; le groupe G possède alors un élément g non nul. Il possède même un élément strictement positif : en effet c'est clair si $g > 0$, et si $g < 0$ il suffit de prendre $(-g)$. L'ensemble des éléments strictement positifs de G étant non vide, il possède un plus petit élément d. Nous allons montrer que $G = d\mathbb{Z}$. Comme G est un sous-groupe de $\mathbb{Z}$ contenant d, il contient le sous-groupe de $\mathbb{Z}$ engendré par d, qui est précisément $d\mathbb{Z}$.

Il reste à montrer l'inclusion réciproque $G \subset d\mathbb{Z}$. Soit $g \in G$. Comme $d > 0$ on peut effectuer la division euclidienne de g par d. Elle fournit un couple (q, r) d'entiers avec $0 \leqslant r < d$ tels que $g = dq + r$. On a donc $r = g - dq$. Par l'inclusion $d\mathbb{Z} \subset G$ déjà établie, $-dq \in G$. Puisque G est stable par somme, $g - dq \in G$. Autrement dit, $r \in G$. Puisque $0 \leqslant r < d$ et puisque d est le plus petit élément strictement positif de G, on a $r = 0$ et $g = dq$; en particulier, $g \in d\mathbb{Z}$ et $G \subset d\mathbb{Z}$.

Il reste à s'assurer de l'unicité de d. Soit donc δ un entier $\geqslant 0$ tel que $G = d\mathbb{Z} = \delta\mathbb{Z}$. Si $d = 0$ alors $G = 0\mathbb{Z} = \{0\}$, et δ est donc nul puisque δ appartient à $G = \delta\mathbb{Z}$. Supposons $d \neq 0$. Comme d est un élément de $G = \delta\mathbb{Z}$ il existe $a \in \mathbb{Z}$ tel que $d = a\delta$; de manière symétrique, il existe $b \in \mathbb{Z}$ tel que $\delta = bd$. On a donc $d = abd$, soit encore $d(ab - 1) = 0$. Puisque $d \neq 0$, on a $ab = 1$. Comme a et b sont entiers, ils sont ou bien tous deux égaux à 1, ou bien tous deux égaux à (-1). Mais dans ce dernier cas on aurait $\delta = bd = -d$ ce qui est absurde car $\delta \geqslant 0$. Ainsi $a = b = 1$ et $\delta = bd = d$. □

(4.5) Théorème-définition. *Soit G un groupe fini et soit H un sous-groupe de G. Le cardinal de H divise le cardinal de G. Le quotient* $\mathrm{card}(G)/\mathrm{card}(H)$ *est appelé* indice *de H dans G est est noté $[G : H]$.*

Démonstration. Pour tout $g \in G$, on note gH le sous-ensemble de G formé des éléments de la forme gh avec $h \in H$. La clef de la preuve réside dans l'étude de ces ensembles gH ; nous allons donc commencer par en établir quelques propriétés.

(4.5.1) *Si $g \in G$, le cardinal de gH est égal au cardinal de H.* En effet, l'application de H dans G qui envoie h sur gh est injective (c'est la propriété de simplification, *cf.* 2.5.5). Son image, qui n'est autre que gH par définition de ce dernier, a donc un cardinal égal à celui de H.

(4.5.2) *Si $g \in G$ et si $a \in gH$ alors $gH = aH$.* En effet, comme $a \in gH$ on peut écrire $a = gh_0$ pour un certain $h_0 \in H$; on a alors $g = ah_0^{-1}$ (multiplier à droite par h_0^{-1} les deux membres de l'égalité). Pour tout élément h de H on a $ah = gh_0h \in gH$ car $h_0h \in H$ (puisque H est un sous-groupe de G) ; et on a également $gh = ah_0^{-1}h \in aH$ car $h_0^{-1}h \in H$ (puisque H est un sous-groupe de G). Ainsi $aH \subset gH$ et $gH \subset aH$, d'où l'égalité annoncée $gH = aH$.

(4.5.3) *Si g et g' sont deux éléments de G tels que $gH \cap g'H \neq \varnothing$ alors $gH = g'H$.* En effet, choisissons $a \in gH \cap g'H$. Il résulte alors de 4.5.2 que $gH = aH = g'H$.

(4.5.4) *Conclusion.* Soit $\mathscr{P}$ l'ensemble des parties de G qui sont de la forme gH pour un certain $g \in G$; notons r le cardinal de $\mathscr{P}$, et choisissons une numérotation arbitraire $P_1, \ldots, P_r$ des éléments de $\mathscr{P}$. En vertu de 4.5.1 le cardinal de P_i est égal au cardinal de H pour tout i, et il résulte de 4.5.3 que les P_i sont deux à deux disjoints. Par ailleurs, pour tout $g \in G$ on a $g = ge \in gH$; ainsi, $G = \bigcup P_i$.

Conclusion : G est la réunion disjointe des ensembles P_i, et chacun d'eux a un cardinal égal à celui de H. Il vient

$$\mathrm{card}(G) = \sum_{i=1}^{r} \mathrm{card}(P_i) = r \cdot \mathrm{card}(H).$$

Par conséquent, $\mathrm{card}(H)$ divise $\mathrm{card}(G)$. □

(4.5.5) Exemple. Le groupe S_4 a pour cardinal $4! = 24$. Tout sous-groupe de S_4 a donc un cardinal divisant 24, c'est-à-dire égal à $1, 2, 3, 4, 6, 8, 12$ ou 24 (notez que les deux sous-groupes de S_4 considérés en 4.3.3 et 4.3.4 sont de cardinaux respectifs 2 et 4, qui figurent dans cette liste). Il n'y a donc pas par exemple de sous-groupe de S_4 de cardinal $5, 7$ ou 10.

(4.5.6) Soit G un groupe dont le cardinal est un nombre premier p. Si H est un sous-groupe de G le cardinal de H est un diviseur de p, et est donc égal à 1 ou à p, ce qui veut dire que $H = \{e\}$ ou $H = G$: le groupe G n'a donc pas de sous-groupes intéressants.

(4.6) Stabilisateurs et orbites. Soit X un ensemble, soit G un sous-groupe de S_X et soit x in X.

(4.6.1) Soit $x \in X$. On appelle *stabilisateur* de x dans G, et l'on note en général G_x, l'ensemble des éléments g de G tels que $g(x) = x$. C'est un sous-groupe de G. En effet, on a $\mathrm{Id}(x) = x$, et donc $\mathrm{Id} \in G_x$. Si g et h sont deux éléments de G_x on a alors $(gh)(x) = g(h(x)) = g(x) = x$ et gh appartient donc à G_x. Enfin, si $g \in G_x$ l'égalité $g(x) = x$ entraîne que $x = g^{-1}(x)$, et g^{-1} appartient donc à G_x. Par conséquent ce dernier est un sous-groupe de G, comme annoncé.

(4.6.2) On appelle *orbite* de x sous G l'ensemble des éléments de X de la forme $g(x)$ pour $g \in G$. Nous la noterons $O_G(x)$. Notons que $x = \mathrm{Id}(x)$ appartient à $O_G(x)$.

(4.6.3) Lemme. *Supposons G fini. Le cardinal de $O_G(x)$ égal à $[G : G_x]$.*

Démonstration Soit p l'application de G dans X qui envoie g sur $g(x)$. Par définition, $O_G(x)$ est égale à l'image de p. Soit $y \in O_G(x)$. Il existe $g_0 \in G$ tel que $y =: g_0(x)$, et pour tout $g \in G$ on a les équivalences

$$\begin{aligned}
p(g) = y \quad &\Longleftrightarrow \quad g(x) = y \\
&\Longleftrightarrow \quad g(x) = g_0(x) \\
&\Longleftrightarrow \quad g_0^{-1} g(x) = x \\
&\Longleftrightarrow \quad g_0^{-1} g \in G_x \\
&\Longleftrightarrow \quad \exists \gamma \in G_x \text{ t.q. } g_0^{-1} g = \gamma \\
&\Longleftrightarrow \quad \exists \gamma \in G_x \text{ t.q. } g = g_0 \gamma.
\end{aligned}$$

Ainsi, $p^{-1}(y)$ est l'ensemble des éléments de G de la forme $g_0\gamma$ avec $\gamma \in G_x$. Puisque $\gamma \mapsto g_0\gamma$ est injective (par simplification, *cf.* 2.5.5), le cardinal de $p^{-1}(y)$ est égal au cardinal de G_x.

Comme G est la réunion disjointe des $p^{-1}(y)$ pour y parcourant O, on voit que

$$\begin{aligned}\mathrm{card}(G) &= \sum_{y\in O_G(x)} \mathrm{card}(p^{-1}(y)) \\ &= \sum_{y\in O_G(x)} \mathrm{card}(G_x) \\ &= \mathrm{card}(O_G(x)) \cdot \mathrm{card}(G_x).\end{aligned}$$

Ainsi $\mathrm{card}(O_G(x)) = \mathrm{card}(G)/\mathrm{card}(G_x) = [G : G_x]$. □

(4.6.4) Lemme. *Soit y un point de $O_G(x)$. On a $O_G(y) = O_G(x)$.*

Démonstration. Par définition, il existe $g_0 \in G$ tel que $y = g_0(x)$, ce qui entraîne que $x = g_0^{-1}(y)$. On a alors pour tout $g \in G$ les égalités

$$g(y) = g(g_0(x)) = (gg_0)(x) \in O_G(x).$$

Ainsi, $O_G(y) \subset O_G(x)$. Mais on a aussi pour tout $g \in G$ les égalités

$$g(x) = g(g_0^{-1}(y)) = (gg_0^{-1})(y) \in O_G(y).$$

Ainsi, $O_G(x) \subset O_G(y)$, et l'on a finalement $O_G(y) = O_G(x)$. □

(4.6.5) Corollaire. *L'ensemble X est la réunion disjointe des orbites sous G.*

Démonstration. Tout point de X appartient à sa propre orbite. Et si y et z sont deux points de X tels que l'intersection $O_G(y) \cap O_G(z)$ soit non vide, alors $O_G(x) = O_G(y)$: en effet on choisit un élément t dans$O_G(y) \cap O_G(z)$ et on a alors $O_G(y) = O_G(t) = O_G(z)$ d'après le lemme 4.6.4. Les orbites sont donc deux à deux disjointes. □

(4.7) Exemples.

(4.7.1) Soit n un entier. Pour tout $b \in \mathbb{Z}$, notons f_b l'application de $\mathbb{Z}$ dans lui-même de la forme qui envoie a sur $a + nb$. Soit $b \in \mathbb{Z}$. Pour tout $c \in \mathbb{Z}$ il existe un unique entier z tel que $a+nb = c$, à savoir $c-nb = f_{-b}(c)$. Ainsi f_b est bijective et $(f_b)^{-1} = f_{-b}$. Soit G le sous-ensemble de $S_{\mathbb{Z}}$ formé des bijections de la forme f_b avec $b \in \mathbb{Z}$. Il contient l'identité, qui est égale à f_0. On a vu ci-dessus qu'il est stable par inversion. Soient b et b' deux éléments de $\mathbb{Z}$. On a pour tout $a \in \mathbb{Z}$ les égalités

$$f_{b'}(f_b(a)) = f_{b'}(a + nb) = a + nb + nb' = a + n(b + b') = f_{b+b'}(a).$$

Ainsi $f_b f_{b'} = f_{b+b'}$, et G est donc stable par produit. Par conséquent, G est un sous-groupe de $S_{\mathbb{Z}}$.

Soit $a \in \mathbb{Z}$. Le stabilisateur G_a est l'ensemble des applications f_b telles que $f_b(a) = a + nb = a$; mais cette égalité n'est possible que si $b = 0$, et l'on a donc $G_a = \{f_0\} = \{\mathrm{Id}\}$. Quant à l'orbite de a, c'est

$$\{f_b(a)\}_{b\in\mathbb{Z}} = \{a + nb\}_{b\in\mathbb{Z}},$$

qui n'est autre que la classe de a modulo n.

(4.7.2) Soit σ l'application $n \mapsto -n$ de $\mathbb{Z}$ dans lui-même. Tout élément n de $\mathbb{Z}$ a un unique antécédent par σ, à savoir $-n = \sigma(n)$. Par conséquent σ est bijective et $\sigma^{-1} = \sigma$, ce qui veut signifie que $\sigma^2 = \mathrm{Id}$. Le sous-ensemble $H := \{\mathrm{Id}, \sigma\}$ de $S_{\mathbb{Z}}$ en est donc un sous-groupe.

Soit $a \in \mathbb{Z}$. On a $\sigma(a) = a$ si et seulement si $a = 0$. Le stabilisateur H_a de a est donc égal à H tout entier si $a = 0$, et à $\{\mathrm{Id}\}$ sinon. La théorie assure dès lors que $O_H(a)$ doit compter un élément si $a = 0$, et deux éléments sinon. Mais on peut le vérifier directement : l'orbite $O_H(a)$ est égale à $\{a, -a\}$ pour tout $a \in \mathbb{Z}$; elle est donc réduite à $\{0\}$ si $a = 0$, et possède exactement deux éléments si $a \neq 0$ car a et $-a$ sont alors distincts.

(4.7.3) Soit n un entier strictement positif. L'orbite de 1 sous S_n est alors égale à $\{1, \ldots, n\}$ tout entier : en effet pour tout $i \in \{1, \ldots, n\}$ il existe une permutation de $\{1, \ldots, n\}$ envoyant 1 sur i (prendre l'identité si $i = 1$, et la transposition $(1i)$ sinon). La théorie assure alors que le stabilisteur de 1 dans S_n soit avoir pour cardinal $\frac{n!}{n} = (n-1)!$. On peut le vérifier directement : se donner une permutation de $\{1, \ldots, n\}$ qui fixe 1 revient en effet à choisir une permutation de $\{2, \ldots, n\}$ (une fois qu'on a décidé que 1 est fixe, il reste à choisir les images des autres éléments), et comme le cardinal de $\{2, \ldots, n\}$ est égal à $n-1$ il y a $(n-1)!$ telles permutations.

5 Morphismes de groupes

(5.1) Définition. Soient G et H deux groupes. Un *morphisme de groupes* de G vers H est une application f de G dans H telle que $f(gg') = f(g)f(g')$.

(5.1.1) Commentaires sur la terminologie. On rencontre parfois également le terme *homomorphisme de groupes*, mais il a tendance à tomber en désuétude. Par ailleurs, nous dirons souvent dans ce cours simplement «morphisme» plutôt que «morphisme de groupes» (en mathématiques, à chaque fois ou presque qu'on définit une classe d'objets intéressants, on définit une classe d'applications intéressantes entre objets du type considéré, qu'on appelle en général «morphismes de ...», à compléter par le nom des objets : il y a des morphismes de groupes, d'anneaux, etc. Mais d ce cours il n'y aura normalement pas d'ambiguïté, puisque nous nous focalisons sur les groupes).

(5.1.2) Un morphisme de G vers H est donc une application de G vers H qui se comporte bien vis-à-vis des lois internes de G et H. Mais ce bon comportement s'étend en fait automatiquement aux éléments neutres et à l'inversion. En effet, soit f un morphisme de G dans H. On a alors

$$f(e_G)e_H = f(e_G) = \underbrace{f(e_G^2) = f(e_G)^2}_{\text{car } f \text{ est un morphisme}}$$

et donc $f(e_G) = e_H$ par simplification (2.5.5). On en déduit que l'on a pour tout $g \in G$ les égalités

$$e_H = f(e_G) = f(gg^{-1}) = f(g)f(g^{-1}),$$

ce qui entraîne que $f(g^{-1}) = f(g)^{-1}$, là encore par simplification.

(5.2) Exemples.

(5.2.1) Les cas triviaux. Soit G un groupe. L'identité $\mathrm{Id}\colon G \to G$ est un morphisme. Pour tout sous-groupe H de G, l'inclusion $H \hookrightarrow G$ est un morphisme. Pour tout groupe G', l'application constante $g \mapsto e_{G'}$ de G dans G' est un morphisme.

(5.2.2) Soient $f\colon G \to G'$ et $f'\colon G' \to G''$ deux morphismes de groupes. La composée $f' \circ f\colon G \to G''$ est alors un morphisme de groupes : on a en effet pour tout $(g_1, g_2) \in G^2$ les égalités

$$\begin{aligned}(f \circ f')(g_1 g_2) &= f(f('g_1 g_2)) \\ &= f(f'(g_1)f'(g_2)) \\ &= f(f'(g_1))f(f'(g_2)) \\ &= (f \circ f')(g_1)(f \circ f')(g_2)\end{aligned}$$

(la deuxième égalité vient du fait que f' est un morphisme, et la troisième du fait que f est un morphisme).

(5.2.3) On a signalé au 4.2.3 que $\{-1, 1\}$ est un sous-groupe de $\mathbb{R}^\times$. Pour tout entier n, la signature est un morphisme de S_n dans $\{-1, 1\}$: cela résulte de 3.22.

(5.2.4) Soit n un entier > 0. L'application $a \mapsto \overline{a}$ de $\mathbb{Z}$ dans $\mathbb{Z}/n\mathbb{Z}$ est un morphisme de groupes : cela résulte du fait que $\overline{a+b} = \overline{a}+\overline{b}$ pour tout $(a, b) \in \mathbb{Z}^2$ par définition de la loi de groupe sur $\mathbb{Z}/n\mathbb{Z}$.

(5.3) . Soit $f\colon G \to H$ un morphisme de groupes.

(5.3.1) Soit G' un sous-groupe de G. Montrons que l'image $f(G')$ est un sous-groupe de H.

- Comme $e_G \in G'$ (car G' est un sous-groupe de G) et $f(e_G) = e_H$ on a $e_H \in f(G')$.
- Soient h et h' deux éléments de $f(G')$. Par définition, il existe deux éléments g et g' de G' tels que $f(g) = h$ et $f(g') = h'$. On a alors $hh' = f(g)f(g') = f(gg')$; puisque $gg' \in G'$ (car G' est un sous-groupe de G) on voit que $hh' \in f(G')$.
- Soit h un élément de $f(G')$. Par définition, il existe alors $g \in G'$ tel que $f(g) = h$. On a alors $h^{-1} = f(g)^{-1} = f(g^{-1})$; puisque $g^{-1} \in G'$ (car G' est un sous-groupe de G), on voit que $h^{-1} \in H$.

Ainsi, $f(G')$ est bien un sous-groupe de H. En particulier, $f(G)$ est un sous-groupe de H.

(5.3.2) Soit H' un sous-groupe de H. Montrons que l'image réciproque $f^{-1}(H')$ est un sous-groupe de H.

- Comme $e_H \in H'$ (car H' est un sous-groupe de H) et comme $f(e_G) = e_H$ on a $e_G \in f^{-1}(H')$.
- Soient g et g' deux éléments de $f^{-1}(H')$. Par définition, $f(g) \in H'$ et $f(g') \in H'$. On a alors $f(gg') = f(g)f(g') \in H'$ (car H' est un sous-groupe de H). Ainsi, $gg' \in f^{-1}(H')$.
- Soit g un élément de $f^{-1}(H')$. Par définition, $f(g) \in H'$. On a alors $f(g^{-1}) = f(g)^{-1} \in H'$ (car H' est un sous-groupe de H). Ainsi, g^{-1} appartient à $f^{-1}(H')$.

Il s'ensuit que $f^{-1}(H')$ est un sous-groupe de G, comme annoncé. En particulier,

$$f^{-1}(e_H) = f^{-1}(\{e_H\}) = \{g \in G, f(g) = e_H\}$$

est un sous-groupe de G, que l'on appelle le *noyau* de f et que l'on note parfois Ker f.

(5.4) Exemples. Soit n un entier et soit $\varepsilon\colon S_n \to \{-1, 1\}$ la signature. Son noyau est par ce qui précède un sous-groupe de S_n, que l'on note en général A_n ; par définition, A_n est constitué des permutations paires.

(5.4.1) *Supposons que* $n = 0$ *ou* $n = 1$. On a alors $S_n = \{\mathrm{Id}\}$, et $\varepsilon(\mathrm{Id})$ est égale à 1. On en déduit que $A_n = S_n = \{\mathrm{Id}\}$, et que l'image de ε est égale à $\{1\}$.

(5.4.2) *Supposons* que $n \geqslant 2$. Le groupe S_n contient alors la transposition (12). Sa signature est (-1) ; par conséquent l'image de ε est $\{-1, 1\}$ tout entier : la signature est surjective.

Et le groupe A_n (qui ne contient pas (12)) est un sous-groupe *strict* de S_n. Lorsque $n = 2$ on a $S_n = \{\mathrm{Id}, (12)\}$ et A_n est donc égal à $\{\mathrm{Id}\}$; mais si $n \geqslant 3$ alors A_n est non trivial, car il contient (123).

(5.5) Nous allons maintenant énoncer deux résultats théoriques importants sur le noyau, qui vous rappelleront sans doute des énoncés d'algèbre linéaire : vous avez probablement déjà rencontré le lemme 5.6 dans ce contexte, et la proposition 5.7 est quant à elle un analogue de la ≪formule du rang≫.

(5.6) Lemme. *Soit $f\colon G \to H$ un morphisme de groupes. Le morphisme f est injectif si et seulement si son noyau est trivial.*

Démonstration. Supposons f injective et soit $g \in \mathrm{Ker}\ f$. On a alors

$$f(g) = e_H = f(e_G),$$

donc $g = e_G$ par injectivité de f et Ker f est trivial.

Réciproquement, supposons que Ker f est trivial et soient g et g' deux éléments de G tels que $f(g) = f(g')$. On a alors $f(g'g^{-1}) = f(g')f(g^{-1}) = e_H$; par conséquent $g^{-1}g' \in \mathrm{Ker}\ f$ et comme celui-ci est trivial, on a $g^{-1}g' = e_G$ et partant $g = g'$. Ainsi, f est injective. □

(5.7) Proposition. *Soit $f\colon G \to H$ un morphisme de groupes. Supposons que G est fini. On a alors l'égalité*

$$\mathrm{card}(f(G)) \cdot \mathrm{card}(\mathrm{Ker}\ f) = \mathrm{card}(G).$$

Démonstration. On procède en plusieurs étapes.

(5.7.1) *Montrons que pour tout $h \in f(G)$ on a* $\mathrm{card}(f^{-1}(h)) = \mathrm{card}(\mathrm{Ker}\ f)$. Soit h un élément de $f(G)$. Choisissons $g_0 \in G$ tel que $f(g_0) = h$ (il en existe

au moins un par définition). Soit $g \in G$. On a les équivalences

$$\begin{aligned} f(g) = h &\iff f(g) = f(g_0) \\ &\iff f(g)f(g_0)^{-1} = e_H \\ &\iff f(gg_0^{-1}) = e_H \\ &\iff gg_0^{-1} \in \operatorname{Ker} f \\ &\iff \exists \gamma \in \operatorname{Ker} f \text{ t.q. } gg_0^{-1} = \gamma \\ &\iff \exists \gamma \in \operatorname{Ker} f \text{ t.q. } g = \gamma g_0. \end{aligned}$$

On voit donc que $f^{-1}(h) = \{\gamma g_0\}_{\gamma \in \operatorname{Ker} f}$. L'application de G dans G qui envoie un élément γ sur γg_0 est injective (2.5.5). Par conséquent le cardinal de $\{\gamma g_0\}_{\gamma \in \operatorname{Ker} f}$ est égal à $\operatorname{card}(\operatorname{Ker} f)$, comme annoncé.

(5.7.2) Le groupe G est la réunion disjointe des $f^{-1}(h)$ pour h parcourant $f(G)$. On a donc

$$\begin{aligned} \operatorname{card}(G) &= \sum_{h \in f(G)} \operatorname{card}(f^{-1}(h)) \\ &= \sum_{h \in f(G)} \operatorname{card}(\operatorname{Ker} f) \\ &= \operatorname{card}(f(G)) \cdot \operatorname{card}(\operatorname{Ker} f) \end{aligned}$$

(la seconde égalité provient de 5.7.1). □

(5.8) Exemple. Soit n un entier $\geqslant 2$. On a vu au 5.4.2 que le morphisme signature $\varepsilon \colon S_n \to \{-1, 1\}$ est surjectif. Il vient

$$n! = \operatorname{card}(S_n) = \operatorname{card}(A_n) \cdot \operatorname{card}(\{-1, 1\}) = \operatorname{card}(A_n) \cdot 2,$$

d'où l'égalité

$$\operatorname{card}(A_n) = \frac{n!}{2}.$$

Vérifions-la explicitement pour les petites valeurs de n.

(5.8.1) *Le cas* $n = 2$. On a vu que $A_2 = \mathrm{Id}$, qui est bien de cardinal $1 = \frac{2!}{2}$.

(5.8.2) *Le cas* $n = 3$. Une permutation de $\{1, 2, 3\}$ est ou bien l'identité, ou bien une transposition, ou bien un 3-cycle (aucun autre type de décomposition en produit de cycles à supports deux à deux disjoints n'est possible). L'identité et les 3-cycles sont paires, et les transpositions sont impaires. Comme un 3-cycle de $\{1, 2, 3\}$ a pour support $\{1, 2, 3\}$ tout entier, il y a exactement deux tels 3-cycles : (123) et (132). On déduit de ce qui précède que

$$A_3 = \{\mathrm{Id}, (123), (132)\}.$$

Son cardinal est bien égal à $3 = \frac{3!}{2}$.

(5.8.3) *Le cas* $n = 4$. Nous avons donné au 3.16 la liste des éléments de S_4, classés en fonction du type de leur écriture comme produit de cycles à supports deux à deux disjoints. L'identité et les 3-cycles sont paires, ainsi que les produits de deux transpositions ; les transpositions et les 4-cycles sont impaires. Le groupe A_4 est par conséquent égal à

$$\{\mathrm{Id}, (123), (132), (124), (142), (134), (143), (234), (243), (12)(34), (13)(24), (14)(23)\}.$$

Et l'on a bien $\mathrm{card}(A_4) = 12 = \frac{24!}{2}$.

(5.9) Soit $f\colon G \to H$ un morphisme de groupes. On dit que f est un *isomorphisme* (de groupes) si l'application f est bijective.

Supposons que ce soit le cas, et soient h et h' deux éléments de H. On a $h = f(f^{-1}(h))$ et $h' = f(f^{-1}(h'))$. Il vient

$$hh' = f(f^{-1}(h))f(f^{-1}(h')) = f(f^{-1}(h)f^{-1}(h')),$$

et partant

$$f^{-1}(hh') = f^{-1}(h)f^{-1}(h').$$

La bijection réciproque f^{-1} est ainsi elle aussi un morphisme de groupes – et donc un isomorphisme.

La composée de deux bijections est une bijections, et la composée de deux morphismes est un morphisme. La composée de deux isomorphismes est donc un isomorphisme.

(5.10) Soient G et H deux groupes. On dit que G et H sont *isomorphes* s'il existe un isomorphisme $f\colon G \simeq H$.

Supposons que ce soit le cas (notez que H est alors isomorphe à G *via* f^{-1}). L'application f est une bijection qui préserve le produit, l'élément neutre et l'inversion, et il en va de même de sa réciproque d'après 5.9. On en déduit le principe suivant, à l'énoncé volontairement un peu vague (mais auquel on pourrait donner un sens précis) : si une propriété peut être décrite uniquement en termes de la loi de groupe, de l'élément neutre et de l'inversion, alors elle est vraie pour G si et seulement si elle est vraie pour H.

(5.10.1) Par exemple, le groupe G est abélien si et seulement si le groupe H est abélien. Si on veut le démontrer directement sans faire appel au principe un peu informel que l'on vient d'évoquer, on procède comme suit. Supposons que G est abélien, et soient h et h' deux éléments de H. On a

$$\begin{aligned} h'h &= f(f^{-1}(h'))f(f^{-1}(h)) && (1)\\ &= f(f^{-1}(h')f^{-1}(h)) && (2)\\ &= f(f^{-1}(h)f^{-1}(h')) && (3)\\ &= f((f^{-1}(h))f(f^{-1}(h')) && (4)\\ &= hh' && (5) \end{aligned}$$

(les égalités (2) et (4) proviennent du fait que f est un morphisme, et l'égalité (3) du fait que G est abélien). Ainsi, H est abélien. Par symétrie, l'abélianité de H entraîne celle de G.

(5.10.2) Donnons deux autres exemples (le lecteur pourra en rédiger les preuves détaillées sur le modèle de 5.10.1 s'il le souhaite) : G est trivial si et seulement si H est trivial ; on a $g^2 = e_G$ pour tout $g \in G$ si et seulement si $h^2 = e_H$ pour tout $h \in H$.

(5.11) Ordre d'un élément. Soit G un groupe et soit g un élément de G. Si l'ensemble des entiers $n > 0$ tels que $g^n = e$ est non vide, son plus petit élément est appelé l'*ordre* de g ; dans le cas contraire, on dit que g est *d'ordre infini*.

Il résulte de la définition que g est d'ordre 1 si et seulement si $g = e$.

(5.12) Soit G un groupe et soit g un élément de G. Soit f l'application de $\mathbb{Z}$ dans G qui envoie un entier n sur g^n. Comme $g^{n+n'} = g^n g^{n'}$ pour tout $(n, n') \in \mathbb{Z}^2$, l'application f est un morphisme de groupes. Son image $f(\mathbb{Z})$ est par définition $\{g^n\}_{n\in\mathbb{Z}}$: c'est donc le sous-groupe $\langle g\rangle$ de G. On distingue maintenant deux cas.

(5.12.1) *Supposons que l'ordre de g est infini.* Dans ce cas $g^n \neq e$ pour tout $n > 0$; il s'ensuit que si $n < 0$ on a également $g^n \neq e$ (car sinon on aurait $g^{-n} = (g^n)^{-1} = e$). Par conséquent, $\mathrm{Ker}\, f = \{0\}$ et f est donc injective. On en déduit que $f = n \mapsto g^n$ induit un isomorphisme $\mathbb{Z} \simeq \langle g\rangle$. En particulier, $\langle g\rangle$ est infini.

(5.12.2) *Supposons que l'ordre de g est fini.* Dans ce cas il existe $n > 0$ tel que $g^n = e$, et f n'est donc pas injective. Son noyau $\mathrm{Ker}\, f$ est un sous-groupe de $\mathbb{Z}$, et est donc de la forme $d\mathbb{Z}$ pour un certain $d > 0$ (th. 4.4). Notons que dans ce cas, le plus petit entier $n > 0$ tel que $g^n = e$, c'est-dire tel que $n \in \mathrm{Ker}\, f$, est égal à d : par conséquent, d est l'ordre de g. Nous désignons par $a \mapsto \overline{a}$ l'application de réduction modulo d.

Si n et m sont deux éléments de $\mathbb{Z}$ tels que $\overline{n} = \overline{m}$, on a $g^{n-m} = e$ car $n - m$ appartient à $d\mathbb{Z} = \mathrm{Ker}\, f$, et donc $g^n = g^m$. Ainsi, la formule $\overline{n} \mapsto g^n$ définit une application $\overline{f}$ de $\mathbb{Z}/d\mathbb{Z}$ vers $\langle g\rangle$. On a pour tout $(n, m) \in \mathbb{Z}^2$ les égalités

$$\overline{f}(\overline{n} + \overline{m}) = \overline{f}(\overline{n+m}) = g^{n+m} = g^n g^m = \overline{f}(\overline{n})\overline{f}(\overline{m})$$

(la première égalité vient de la définition de l'addition dans $\mathbb{Z}/d\mathbb{Z}$, et la seconde et la dernière de la définition de $\overline{f}$). Ainsi, $\overline{f}$ est un morphisme de groupes. Il est surjectif par définition. Par ailleurs on a pour tout n dans $\mathbb{Z}$ les équivalences

$$\overline{f}(\overline{n}) = e \iff g^n = e \iff n \in \mathrm{Ker}\, f = d\mathbb{Z} \iff \overline{n} = \overline{0}.$$

Par conséquent, $\overline{f}$ est injective, et finalement bijective. On a donc démontré que $\overline{a} \mapsto g^a$ induit un isomorphisme $\mathbb{Z}/d\mathbb{Z} \simeq \langle g\rangle$. En particulier, les éléments g^i pour $0 \leqslant i \leqslant d-1$ sont deux à deux distincts, $\langle g\rangle = \{g^0, g, g^2, \ldots, g^{d-1}\}$ et $\langle g\rangle$ est de cardinal d.

(5.12.3) Supposons que G soit fini, et notons n son cardinal. Le sous-groupe $\langle g\rangle$ de G ne peut être infini, et g est donc d'ordre fini, noté d. Il résulte de 5.12.2 que $\langle g\rangle$ est de cardinal d. En vertu du théorème 4.5, d divise n.

Il résulte également de 5.12.2 que pour tout entier m on a $g^m = e$ si et seulement si d divise m ; en particulier, $g^n = e$.

(5.13) Groupes d'ordre premier. Soit p un nombre premier et soit G un groupe de cardinal p. Soit g un élément non trivial de G – il en existe un car $p > 1$. L'ordre de g divise p, et n'est pas égal à 1 puisque $g \neq e$. Par conséquent cet ordre est p ; le sous-groupe $\langle g\rangle$ de G est donc égal à G tout entier. En particulier, $G \simeq \mathbb{Z}/p\mathbb{Z}$.

Nous venons de démontrer qu'il y a à isomorphisme près un seul groupe d'ordre p, à savoir $\mathbb{Z}/p\mathbb{Z}$.

(5.14) Ordre d'une permutation. Soit X un ensemble fini, soit n son cardinal et soit σ appartenant à S_X. Le groupe S_X est fini de cardinal $n!$. D'après 5.12.3, la permutation σ est d'ordre fini divisant $n!$.

(5.14.1) Comment calculer cet ordre ? Si σ est donné par un tableau de valeurs, on peut évidemment utiliser l'algorithme grossier consistant à calculer

les puissances successives de σ jusqu'à ce que l'on obtienne l'identité. Mais nous allons en présenter un qui est autrement plus efficace.

(5.14.2) La permutation σ peut s'écrire comme un produit $C_1 \dots C_r$ de cycles à supports deux à deux disjoints (théorème 3.11), et l'on a décrit aux paragraphes 3.14 *et sq.* un algorithme permettant d'obtenir cette décomposition.

Pour tout i, désignons par ℓ_i la longueur de C_i. On a vu au 3.8.5 que ℓ_i est le plus petit entier $m > 0$ tel que $C_i^m = \mathrm{Id}$; autrement dit, l'ordre de C_i est égal à ℓ_i. D'après 5.12.2, le noyau du morphisme $m \mapsto C_i^m$ est alors précisément égal à $\ell_i\mathbb{Z}$: pour tout entier m, on a donc $C_i^m = \mathrm{Id}$ si et seulement si ℓ_i divise m.

Soit m un entier. On a

$$\sigma^m = (C_1 \dots C_r)^m = C_1^m C_2^m \dots C_r^m$$

car les C_i commutent deux à deux, étant à supports deux à deux disjoints (3.6.3). Par ailleurs, le support de C_i^m est contenu pour tout i dans le support de C_i (3.5.5) et les C_i^m sont donc encore à supports deux à deux disjoints. Il s'ensuit en vertu de *loc. cit.* que $C_1^m \dots C_r^m = \mathrm{Id}$ si et seulement si $C_i^m = \mathrm{Id}$ quel que soit i.

L'ordre de σ est donc le plus petit entier $m > 0$ tel que $C_i^m = \mathrm{Id}$ pour tout i, c'est-à-dire tel que ℓ_i divise m pour tout i. Par conséquent, *l'ordre de σ est égal au PPCM des ℓ_i.*

(5.14.3) Supposons que $X = \{1, \dots, 17\}$ et que σ est la permutation étudiée au 3.15. On a vu dans ce dernier paragraphe que la décomposition de σ en produit de cycles à supports deux à deux disjoints comprenait un 3-cyle, un 6-cycle, un 4-cycle et une transposition. L'ordre de σ est donc égal à

$$\mathrm{PPCM}(3, 6, 4, 2) = 12.$$

(5.15) Bijections ensemblistes et isomorphismes entre groupes de permutations. Soient X et Y deux ensembles et soit $\varphi\colon X \to Y$ une bijection.

(5.15.1) *Motivations heuristiques.* La bijection φ met en correspondance «parfaite» les éléments de X et ceux de Y : à un élément x de X correspond l'élément $\varphi(x)$ de Y, et à un élément y de Y correspond l'élément $\varphi^{-1}(y)$ de X.

Elle fait du même coup correspondre à tout objet «ensembliste» défini sur X un objet de même nature défini sur Y. C'est par exemple le cas en ce qui concerne les permutations. Plus précisément, soit σ une permutation de X, et soit x un élément de X. L'élément de Y qui correspond à x est $\varphi(x)$; l'élément de Y qui correspond à $\sigma(x)$ est $\varphi(\sigma(x))$. La permutation τ de Y qui correspond à σ doit alors envoyer $\varphi(x)$ sur $\varphi(\sigma(x))$. Autrement dit, on doit avoir

$$\tau(\varphi(x)) = \varphi(\sigma(x))$$

pour tout $x \in X$, c'est-à-dire $\tau \circ \varphi = \varphi \circ \sigma$, c'est-à-dire encore $\tau = \varphi \circ \sigma \circ \varphi^{-1}$.

(5.15.2) Le paragraphe 5.15.1 ci-dessus amène à introduire l'application $\Phi\colon S_X \to S_Y$ définie par la formule $\Phi(\sigma) = \varphi \circ \sigma \circ \varphi^{-1}$ (notez que si $\sigma \in S_X$ alors $\varphi \circ \sigma \circ \varphi^{-1}\colon Y \to Y$ est bien une bijection, en tant que composée de bijections).

L'application Φ est un morphisme de groupes. En effet, soient σ et σ' deux éléments de S_X. On a alors (en notant pour une fois les loi internes de S_X et

S_Y par le symbole $\circ$ de composition, car c'est indispensable pour comprendre ce qui se passe)

$$\begin{aligned}\Phi(\sigma\circ\sigma') &= \varphi\circ\sigma\circ\sigma'\circ\varphi^{-1}\\ &= \varphi\circ\sigma\circ\varphi^{-1}\circ\varphi\circ\sigma'\circ\varphi^{-1}\\ &= \Phi(\sigma)\circ\Phi(\sigma').\end{aligned}$$

Le morphisme Φ est un isomorphisme. En effet, soit τ une permutation de σ. Pour tout $\sigma\in S_X$ on a alors les équivalences

$$\begin{aligned}\Phi(\sigma)=\tau &\iff \varphi\circ\sigma\circ\varphi^{-1}=\tau\\ &\iff \sigma=\varphi^{-1}\circ\tau\circ\varphi.\end{aligned}$$

Ainsi, τ n'a qu'un antécédent par Φ, à savoir $\varphi^{-1}\circ\tau\circ\varphi$. Le morphisme Φ est donc bijectif, de réciproque $\tau\mapsto\varphi^{-1}\circ\tau\circ\varphi$ (notons que ce morphisme réciproque est celui induit par la bijection φ^{-1} de Y sur X).

(5.15.3) Pour travailler avec l'isomorphisme Φ introduit ci-dessus, il est en général plus commode d'utiliser l'égalité $\Phi(\sigma)\circ\varphi=\varphi\circ\sigma$ plutôt que la formule $\Phi(\sigma)=\varphi\circ\sigma\circ\varphi^{-1}$ (les deux sont bien entendu équivalentes).

Par exemple, fixons un entier ℓ et supposons que σ est un ℓ-cycle $(a_1\dots a_\ell)$; nous allons calculer $\Phi(\sigma)$. Puisque $\Phi(\sigma)\circ\varphi=\varphi\circ\sigma$, on a pour tout $x\in X$ l'égalité

$$\Phi(\sigma)(\varphi(x))=\varphi(\sigma(x)).$$

Soit x un point fixe de σ, c'est-à-dire un élément de X n'appartenant pas à $\{a_1,\dots,a_r\}$. On a alors $\Phi(\sigma(\varphi(x))=\varphi(\sigma(x))=\varphi(x)$. Ainsi, $\varphi(x)$ est fixe sous $\Phi(\sigma)$.

Soit i compris entre 1 et r. On a alors $\Phi(\sigma)(\varphi(a_i))=\varphi(\sigma(a_i))$, et partant $\Phi(\sigma)(\varphi(a_i))=\varphi(a_{i+1})$ si $i<r$ et $\Phi(\sigma)(\varphi(a_r))=\varphi(a_1)$.

On voit ainsi que $\Phi(\sigma)$ est le ℓ-cycle $(\varphi(a_1)\dots\varphi(a_\ell))$.

(5.16) Nous avons défini en 3.21 la signature d'une permutation de $\{1,\dots,n\}$. Nous allons utiliser les résultats précédents (autour de l'isomorphisme Φ) pour étendre cette définition au cas d'une permutation d'en ensemble fini quelconque.

(5.17) Proposition. *Soit X un ensemble fini et soit σ une permutation de X. Soit $\tau_1\dots\tau_r$ une écriture de σ comme produit de transpositions (il existe toujours une telle écriture d'après 3.17.2). L'élément $(-1)^r$ de $\{-1,1\}$ ne dépend que de σ, et pas de l'écriture choisie. On l'appelle la* signature *de σ et on le note $\varepsilon(\sigma)$; l'application $\sigma\colon S_X\to\{-1,1\}$ est un morphisme de groupes. Le noyau de ε est appelé le groupe des permutations* paires *de X.*

Démonstration. Soit n le cardinal de l'ensemble X. Choisissons une bijection $\varphi\colon X\to\{1,\dots,n\}$ et notons $\Phi\colon S_X\simeq S_n$ l'isomorphisme induit (5.15.2). On a $\Phi(\sigma)=\Phi(\tau_1)\dots\Phi(\tau_r)$, et en vertu de 5.15.3 (appliqué avec $\ell=2$), la permutation $\Phi(\tau_i)$ est pour tout i une transposition de $\{1,\dots,n\}$. Ainsi, $\Phi(\sigma)$ est un produit de r transpositions ; par conséquent, $(-1)^r$ est la signature de $\Phi(\sigma)$ (3.24), qui ne dépend bien que de σ et pas de l'écriture choisie.

Si σ' est une permutation de X s'écrivant comme un produit $\tau'_1\dots\tau'_s$ de transpositions, on a alors

$$\sigma\sigma'=\tau_1\dots\tau_r\tau'_1\dots\tau'_s$$

et donc $\varepsilon(\sigma\sigma')=(-1)^{r+s}=(-1)^r(-1)^s=\varepsilon(\sigma)\varepsilon(\sigma')$. Par conséquent, ε est un morphisme de groupes. □

6 Isométries planes

(6.1) Dans cette section, nous identifions $\mathbb{R}^2$ à $\mathbb{C}$ de sorte qu'un point (x, y) de $\mathbb{R}^2$ est vu comme le nombre complexe $x+iy$. On note $\mathbb{U}$ l'ensemble des nombres complexes de module 1. Il est clair que $1 \in \mathbb{U}$, que zz' appartient à $\mathbb{U}$ pour tout $(z, z') \in \mathbb{U}^2$, et que $z^{-1} \in \mathbb{U}$ pour tout $z \in \mathbb{U}$. Autrement dit, $\mathbb{U}$ est un sous-groupe de $\mathbb{C}^\times$.

Nous supposerons connue l'interprétation géométrique du module et de l'argument, ainsi que les notions de rotation et de symétrie orthogonale par rapport à une droite. Mais nous allons les décrire par des formules explicites que le lecteur poura prendre comme définition s'il le souhaite, d'autant que toutes les propriétés utiles seront (re)démontrées à partir de ces formules.

(6.2) On définit la *classe modulo* 2π d'un réel r comme l'ensemble des réels de la forme $r+2k\pi$ avec $k \in \mathbb{Z}$. On démontre (exactement comme en 2.8 *et sq.*) que deux réels r et r' ont même classe modulo 2π si et seulement si leur différence est un multiple entier de 2π, et si c'est le cas on dit qu'ils sont égaux modulo 2π.

On définit de même les notions de classe et d'égalité modulo π (ou modulo tout autre nombre réel, mais nous ne nous en servirons pas).

(6.2.1) Si b est un élément de $\mathbb{C}$ nous noterons T_b l'application $z \mapsto z + b$ de $\mathbb{C}$ dans lui-même ; c'est la translation de vecteur b.

(6.2.2) Si z est un nombre complexe, on peut toujours l'écrire sous la forme $re^{i\varphi}$ où r est un réel positif ou nul et φ un réel. Si $z \neq 0$ cette écriture est essentiellement unique : on a nécessairement $r = |z|$ et $\varphi = \mathrm{Arg}(z)$ modulo 2π ; si $z = 0$ on a nécessairement $r = 0$ et n'importe quel φ convient.

Il sera souvent utile de ≪centrer cette écriture ailleurs qu'en l'origine≫. Plus précisément, un nombre complexe z_0 étant fixé, tout nombre complexe z peut s'écrire sous la forme $z_0 + re^{i\varphi}$ où r est un réel positif ou nul et φ un réel (appliquer ce qui précède à $z - z_0$) ; on a alors nécessairement $r = |z - z_0|$ et $\varphi = \mathrm{Arg}(z - z_0)$ modulo 2π si $z \neq z_0$; si $z = z_0$ on a nécessairement $r = 0$ et φ peut être choisi quelconque.

(6.2.3) Nous noterons Σ la conjugaison complexe ; c'est un élément d'ordre 2 de $S_\mathbb{C}$, qui s'interprète géométriquement comme la symétrie orthogonale par rapport à l'axe réel. Le sous-groupe $\langle\Sigma\rangle$ de $S_\mathbb{C}$ est égal à

$$\{\Sigma^0, \Sigma^1\} = \{\mathrm{Id}, \Sigma\}$$

(et pour tout $n \in \mathbb{Z}$ on a $\Sigma^n = \mathrm{Id}$ si n est pair, et $\Sigma^n = \Sigma$ si n est impair).

On vérifie immédiatement qu'on a les égalités suivantes pour tout $n \in \mathbb{Z}$, tout $(z, z') \in \mathbb{C}^2$, tout $\lambda \in \mathbb{R}$ et tout $w \in \mathbb{C}^\times$:

- $(\Sigma^n)^2 = \Sigma^{2n} = \mathrm{Id}$.
- $\Sigma^n(zz') = \Sigma^n(z)\Sigma^n(z')$;
- $\Sigma^n(z + \lambda z') = \Sigma^n(z) + \Sigma^n(z')$;
- $|\Sigma^n(z)| = |z|$;
- $\Sigma^n(w^{-1}) = \Sigma^n(w)^{-1}$.

(6.3) Définition. Une *isométrie* (plane) est une application de $\mathbb{C}$ dans $\mathbb{C}$ qui est de la forme $z \mapsto a\Sigma^n(z) + b$ avec $a \in \mathbb{U}$, $n \in \mathbb{Z}$ et $b \in \mathbb{C}$.

(6.4) Commentaires. Soit $u\colon \mathbb{C} \to \mathbb{C}$ une isométrie.

(6.4.1) On peut décrire u par une formule $z \mapsto a\Sigma^n(z) + b$ comme ci-dessus. Nous allons montrer que cette formule est essentiellement unique, et plus précisément que l'élément a de $\mathbb{U}$, l'élément b de $\mathbb{C}$ et l'élément Σ^n de $\langle\Sigma\rangle$ sont uniquement déterminés (la dernière condition peut se retraduire en disant que n est uniquement déterminé modulo 2).

Pour le voir, on commence par remarquer que $u(0) = a\Sigma^n(0) + b = b$; par conséquent, b est nécessairement égal à $u(0)$.

On a ensuite $u(1) = a\Sigma^n(1) + b = a + u(0)$, et a est donc nécessairement égal à $u(1) - u(0)$.

Enfin $u(i) = a\Sigma^n(i) + b$ et l'on a donc $u(i) = ai + b$ si $\Sigma^n = \mathrm{Id}$ (*i.e.* si n est pair) et $u(i) = -ai + b$ si $\Sigma^n = \Sigma$ (*i.e* si n est impair). En conséquence le nombre complexe

$$\frac{u(i) - b}{a} = \frac{u(i) - u(0)}{u(1) - u(0)}$$

est égal à i ou $(-i)$, et dans le premier (resp. le second) cas Σ^n est nécessairement égal à Id (resp. Σ).

On dit que u est *directe* si $\Sigma^n = \mathrm{Id}$, c'est-à-dire encore si n est pair ; on dit que u est indirecte si $\Sigma^n = \Sigma$, c'est-à-dire encore si n est impair.

(6.4.2) Pour tout couple $(z, z') \in \mathbb{C}^2$ on a

$$|u(z) - u(z')| = |a| \cdot |\Sigma^n(z) - \Sigma^n(z')| = |\Sigma^n(z - z')| = |z - z'|.$$

En fait on démontre (nous ne le ferons pas ici et ne nous en servirons pas) qu'une application v de $\mathbb{C}$ dans lui-même est une isométrie *si et seulement si* $|v(z)-v(z')| = |z-z'|$ pour tout $(z, z') \in \mathbb{C}^2$. Bien entendu, c'est cette propriété qui est à l'origine du terme «isométrie».

(6.5) Quelques exemples.

(6.5.1) *Les translations.* Soit b un nombre complexe. La translation T_b est donnée par la formule $z \mapsto z+b$; c'est donc une isométrie directe. On a $T_0 = \mathrm{Id}$, et si $b \neq 0$ alors T_b n'a aucun point fixe.

Tout nombre complexe z a un unique antécédent par T_b, à savoir $z - b$; en conséquence T_b est une bijection de réciproque T_{-b}.

Notons que le vecteur b est uniquement déterminé par la translation T_b : il est égal à $T_b(0)$ (c'est un cas particulier de ce qui a été vu au 6.4.1) ; il est donc licite d'évoquer *le* vecteur d'une translation.

(6.5.2) *Les rotations.* Soit θ un nombre réel et soit $z_0 \in \mathbb{C}$. La rotation $R_{z_0,\theta}$ de centre z_0 et d'angle θ envoie un nombre complexe $z = z_0 + re^{i\varphi}$ (avec $r \in \mathbb{R}_+$ et $\varphi \in \mathbb{R}$) sur

$$\begin{aligned} z_0 + re^{i(\varphi+\theta)} &= z_0 + re^{i\varphi}e^{i\theta} && (1)\\ &= z_0 + (z - z_0)e^{i\theta} && (2)\\ &= e^{i\theta}z + z_0(1 - e^{i\theta}). && (3) \end{aligned}$$

Cette formule montre que $R_{z_0,\theta}$ est une isométrie directe (qui ne dépend en fait que de z_0 et de la classe de θ modulo 2π) ; elle entraîne aussi en vertu de 6.4.1 que $e^{i\theta}$ est uniquement déterminé par $R_{z_0,\theta}$; par conséquent, θ est uniquement

déterminé modulo 2π par $R_{z_0,\theta}$ et il est donc licite d'évoquer *l'*angle (modulo 2π) d'une rotation.

Il faut par contre faire un peu attention au centre. On a en effet $R_{z_0,0} = \mathrm{Id}$ et ce, indépendamment de la valeur de z_0. L'identité apparaît ainsi comme la rotation d'angle nul et de *n'importe quel centre*. Mais si θ est non nul modulo 2π alors $e^{i\theta} \neq 1$, d'où pour tout $z \in \mathbb{C}$ les équivalences

$$z = e^{i\theta}z + z_0(1 - e^{i\theta}) \iff (1 - e^{i\theta})z = (1 - e^{i\theta})z_0 \iff z = z_0$$

et z_0 est donc uniquement déterminé par $R_{z_0,\theta}$ dans ce cas : c'est son unique point fixe ; il est en conséquence licite d'évoquer *le* centre d'une rotation d'angle non nul modulo 2π.

Soit $z \in \mathbb{C}$. En utilisant la description de $R_{z_0,\theta}$ *via* la formule (2) on voit qu'on a pour tout $w \in \mathbb{C}$ les équivalences

$$\begin{aligned} R_{z_0,\theta}(w) = z \quad &\iff \quad z_0 + e^{i\theta}(w - z_0) = z \\ &\iff \quad w - z_0 = e^{-i\theta}(z - z_0) \\ &\iff \quad w = z_0 + = e^{-i\theta}(z - z_0) = R_{z_0,-\theta}(z). \end{aligned}$$

Ainsi $R_{z_0,\theta}$ est bijective, et sa réciproque est la rotation $R_{z_0,-\theta}$ (ce à quoi on s'attendait évidemment).

(6.5.3) *Les symétries orthogonales.* Soit Δ une droite de $\mathbb{C}$; on note Σ_Δ la symétrie orthogonale par rapport à Δ (lorsque Δ est l'axe réel Σ_Δ est donc la conjugaison complexe qu'on note simplement Σ). Notons θ l'angle (bien défini modulo π) de Δ avec la droite horizontale et choisissons un point γ sur Δ. La droite Δ est alors $\{\gamma + \lambda e^{i\theta}\}_{\lambda\in\mathbb{R}}$.

Pour tout nombre réel φ, le symétrique de φ par rapport à θ est le réel $\theta-(\varphi-\theta) = 2\theta-\varphi$. La symétrie Σ_Δ envoie donc un nombre complexe $z = \gamma+re^{i\varphi}$ (avec $r \in \mathbb{R}_+$ et $\varphi \in \mathbb{R}$) sur

$$\begin{aligned} \gamma + re^{i(2\theta-\varphi)} &= \gamma + e^{2i\theta}re^{-i\varphi} && (4) \\ &= \gamma + e^{2i\theta}\overline{re^{i\varphi}} && (5) \\ &= \gamma + e^{2i\theta}(\overline{z - \gamma}) && (6) \\ &= e^{2i\theta}\overline{z} + \gamma - e^{2i\theta}\overline{\gamma}. && (7) \end{aligned}$$

Il s'ensuit que Σ_Δ est une isométrie indirecte.

Remarquons que la formule (7) ci-dessus semble dépendre du choix d'un point γ sur la droite Δ, mais nous allons vérifier qu'il n'en est rien (et heureusement, puisqu'elle est censée décrire Σ_Δ qui ne dépend que de Δ, et pas du choix d'un point sur celle-ci). Soit donc δ un (autre) point de Δ. On a alors $\delta = \gamma + \lambda e^{i\theta}$ pour un certain λ appartenant à $\mathbb{R}$, si bien que

$$\begin{aligned} \delta - e^{2i\theta}\overline{\delta} &= \gamma + \lambda e^{i\theta} - e^{2i\theta}(\overline{\gamma + \lambda e^{i\theta}}) \\ &= \gamma + \lambda e^{i\theta} - e^{2i\theta}(\overline{\gamma} + \lambda e^{-i\theta}) \\ &= \gamma - e^{2i\theta}\overline{\gamma} + \lambda e^{i\theta} - \lambda e^{i\theta} \\ &= \gamma - e^{2i\theta}\overline{\gamma}. \end{aligned}$$

On constate ainsi que si l'on remplace γ par δ, la formule (7) ne change pas.

Soit $z \in \mathbb{C}$. En utilisant la description de Σ_Δ *via* la formule (6) on voit qu'on a pour tout $w \in \mathbb{C}$ les équivalences

$$\begin{aligned}
\Sigma_\Delta(w) = z \quad &\iff \quad \gamma + e^{2i\theta}(\overline{w-\gamma}) = z \\
&\iff \quad e^{2i\theta}(\overline{w-\gamma}) = z - \gamma \\
&\iff \quad e^{-2i\theta}(w-\gamma) = \overline{z-\gamma} \\
&\iff \quad w = \gamma + e^{2i\theta}\overline{z-\gamma} = \Sigma_\Delta(z).
\end{aligned}$$

Ainsi Σ_Δ est bijective et est son propre inverse (ce qui veut dire que $\Sigma_\Delta^2 = \mathrm{Id}$) ; le calcul confirme l'intuition géométrique.

Mentionnons pour terminer que la droite Δ est uniquement déterminée par Σ_Δ : c'est en effet l'ensemble de ses points fixes. Pour le voir, choisissons $z \in \mathbb{C}$. On a alors les équivalences

$$\begin{aligned}
\Sigma_\Delta(z) = z \quad &\iff \quad z = \gamma + e^{2i\theta}(\overline{z-\gamma}) \\
&\iff \quad z - \gamma = e^{2i\theta}(\overline{z-\gamma}) \\
&\iff \quad e^{-i\theta}(z-\gamma) = e^{i\theta}(\overline{z-\gamma}) \\
&\iff \quad e^{-i\theta}(z-\gamma) = \overline{e^{-i\theta}(z-\gamma)},
\end{aligned}$$

ce qui est le cas si et seulement si $e^{-i\theta}(z-\gamma)$ est réel. Cela revient à demander q'uil existe $\lambda \in \mathbb{R}$ tel que $e^{-i\theta}(z-\gamma) = \lambda$, ce que l'on peut récrire $z = \gamma + \lambda e^{i\theta}$. L'ensemble des points fixes de Σ_Δ est donc exactement l'ensemble $\{\gamma + \lambda e^{i\theta}\}_{\lambda \in \mathbb{R}}$, qui est bien la droite Δ. Celle-ci est parfois appelée *l'axe* de Σ_Δ.

(6.5.4) *Les symétries glissées.* Soit Δ une droite et soit b un vecteur parallèle à Δ. On appelle *symétrie glissée* d'axe Δ et de vecteur de glissement b la composée $\Sigma_{\Delta,b} := T_b \circ s_\Delta$; c'est une bijection (puisque c'est une composée de deux bijections) ; notons que $\Sigma_{\Delta,0}$ n'est autre que Σ_Δ. Par définition, on a pour tout $z \in \mathbb{C}$ les égalités

$$\begin{aligned}
\Sigma_{\Delta,b}(z) &= \Sigma_\Delta(z) + b \\
&= e^{2i\theta}\overline{z} + \gamma - e^{2i\theta}\overline{\gamma} + b
\end{aligned}$$

(d'après la formule 7 de 6.5.3). Par conséquent, $\Sigma_{\Delta,b}$ est une isométrie indirecte.

L'intuition géométrique assure que Σ_Δ et T_b commutent. Nous allons le vérfier par le calcul. Choisissons un point γ sur Δ, et soit θ l'angle que Δ fait avec l'axe réel (il est bien déterminé modulo π). Le vecteur b est alors de la forme $\lambda e^{i\theta}$ avec $\lambda \in \mathbb{R}$. Soit z un nombre complexe. La formule (7) de 6.5.3 assure que $\Sigma_\Delta(z) = e^{2i\theta}\overline{z} + \gamma - e^{2i\theta}\overline{\gamma}$. Il vient

$$\begin{aligned}
\Sigma_\Delta(T_b(z) &= s_\Delta(z + \lambda e^{i\theta}) && (8)\\
&= e^{2i\theta}(\overline{z} + \lambda e^{-i\theta}) + \gamma - e^{2i\theta}\overline{\gamma} && (9)\\
&= e^{2i\theta}\overline{z} + \gamma - e^{2i\theta}\overline{\gamma} + \lambda e^{i\theta} && (10)\\
&= s_\Delta(z) + b && (11)\\
&= T_b(\Sigma_\Delta(z)), && (12)
\end{aligned}$$

comme annoncé. Notons une première conséquence de cette commutation : on a

$$\Sigma_{\Delta,b}^2 = \underbrace{(\Sigma_\Delta \circ T_b)^2 = \Sigma_\Delta^2 \circ T_b^2}_{\text{car } \Sigma_\Delta \text{ et } T_b \text{ commutent}} = T_{2b}.$$

Ainsi $\Sigma_{\Delta,b}^2$ est une translation de vecteur de $2b$, et le vecteur b est donc uniquement déterminé par $\Sigma_{\Delta,b}$: il est égal à la moitié du vecteur de la translation $\Sigma_{\Delta,b}^2$. Il s'ensuit que $\Sigma_\Delta = T_{-b} \circ \Sigma_{\Delta,b}$ est elle aussi uniquement déterminé par $\Sigma_{\Delta,b}$; et puisque l'axe Δ est l'ensemble des points fixes de $\Sigma_\Delta = T_{-b} \circ \Sigma_{\Delta,b}$, il est lui aussi uniquement déterminé par $\Sigma_{\Delta,b}$. Il est ainsi licite d'évoquer *l*'axe et *le* vecteur de glissement d'une symétrie glissée.

Comme $\Sigma_{\Delta,b} = T_b \circ \Sigma_\Delta$ on a

$$\Sigma_{\Delta,b}^{-1} = \Sigma_\Delta^{-1} \circ T_b^{-1} = \Sigma_\Delta \circ T_{-b} = \Sigma_{\Delta,-b}.$$

L"inverse d'une symétrie glissée est donc la symétrie glissée de même axe et de vecteur de glissement opposé.

Mentionnons pour conclure que si $b \neq 0$ alors $\Sigma_{\Delta,b}$ n'a pas de point fixe : en effet si l'on avait $\Sigma_{\Delta,b}(z) = z$ pour un certain nombre complexe z, on aurait alors $\Sigma_{\Delta,b}^2(z) = z$, mais on sait que $\Sigma_{\Delta,b}^2(z) = T_{2b}(z) = z + 2b$, qui est différent de z puisque $b \neq 0$.

(6.6) Nous allons maintenant montrer que les exemples que nous avons décrits ci-dessus couvrent en réalité *toute*s les isométries.

(6.6.1) *Le cas des isométries directes.* Soit a un élément de $\mathbb{U}$ et soit b un nombre complexe. Soit u l'isométrie directe $z \mapsto az + b$. Soit θ l'argument de a (qui est bien défini modulo 2π) ; on a $a = e^{i\theta}$. Si $a = 1$ (*i.e.* si $\theta = 0$ modulo 2π) alors $u = T_b$. Supposons maintenant que $a \neq 1$. L'équation $z = az + b$ a alors une unique solution, à savoir $z_0 := \frac{b}{1-a}$; en termes géométriques, z_0 est l'unique point fixe de u. Soit $z \in \mathbb{C}$. On a

$$\begin{aligned} u(z) &= az + b \\ &= z_0 - z_0 + az + b \\ &= z_0 - az_0 - b + az + b \\ &= z_0 + a(z - z_0) \\ &= z_0 + e^{i\theta}(z - z_0). \end{aligned}$$

On reconnaît la formule (2) de 6.5.2 et l'on voit ainsi que u est la rotation de centre z_0 et d'angle θ.

(6.6.2) *Le cas des isométries indirectes.* Soit a un élément de $\mathbb{U}$, soit b un nombre complexe, et soit u l'isométrie indirecte $z\colon z \mapsto a\overline{z} + b$. On désigne par β le nombre complexe $e^{-i\theta/2}b$, et par β_1 et β_2 ses parties réelle et imaginaire. Soit $z \in \mathbb{C}$. On a

$$\begin{aligned} u(z) &= a\overline{z} + b \\ &= e^{i\theta}\overline{z} + e^{i\theta/2}\beta \\ &= e^{i\theta}\overline{z} + e^{i\theta/2}\beta_1 + ie^{i\theta/2}\beta_2 \\ &= ie^{i\theta/2}\frac{\beta_2}{2} + e^{i\theta}(\overline{z} + ie^{-i\theta/2}\frac{\beta_2}{2}) + e^{i\theta/2}\beta_1 \\ &= ie^{i\theta/2}\frac{\beta_2}{2} + e^{i\theta}\overline{(z - ie^{i\theta/2}\frac{\beta_2}{2})} + e^{i\theta/2}\beta_1. \end{aligned}$$

Posons $\gamma = ie^{i\theta/2}\frac{\beta_2}{2}$. On a par ce qui précède

$$u(z) = \gamma + e^{i\theta}(\overline{z-\gamma}) + e^{i\theta/2}\beta_1.$$

On voit donc que $u = T_{e^{i\theta/2}\beta_1} \circ v$, où v est l'isométrie indirecte donnée par la formule $z \mapsto \gamma + e^{i\theta}(\overline{z-\gamma})$. D'après la formule (6) de 6.5.3, v est la symétrie orthogonale d'axe $D := \{\gamma + \lambda e^{i\theta/2}\}_{\lambda\in\mathbb{R}}$. Comme le vecteur $e^{i\theta/2}\beta_1$ est parallèle à D, l'isométrie u est la symétrie glissée d'axe D et de vecteur de glissement $e^{i\theta/2}\beta_1$.

(6.7) On désigne par I l'ensemble des isométries de $\mathbb{C}$. Par ce qui précède, les éléments de I sont les translations, les rotations et les symétries glissées ; on a vu en 6.5.1, 6.5.2 et 6.12.2 que chacune de ces transformations est une bijection, dont la réciproque est une isométrie de même nature. Par conséquent, I est un sous-ensemble de $S_{\mathbb{C}}$ stable par inversion. Il contient par ailleurs l'identité (qui est aussi bien la translation de vecteur nul que la rotation de n'importe quel centre et d'angle nul). Nous allons vérifier qu'il est stable par composition, ce qui montrera que c'est un sous-groupe de $S_{\mathbb{C}}$.

Soient u_1 et u_2 deux isométries de $\mathbb{C}$, décrites par les formules respectives

$$z \mapsto a_1\Sigma^{n_1}(z) + b_1 \text{ et } z \mapsto a_2\Sigma^{n_2}(z) + b_2$$

où les a_i appartiennent à $\mathbb{U}$, les b_i à $\mathbb{C}$ et les n_i à $\mathbb{Z}$. On a pour tout $z \in \mathbb{C}$ les égalités

$$\begin{aligned} u_1(u_2(z)) &= u_1(a_2\Sigma^{n_2}(z) + b_2) \\ &= a_1\Sigma^{n_1}(a_2\Sigma^{n_2}(z) + b_2) + b_1 \\ &= a_1\Sigma^{n_1}(a_2)(\Sigma^{n_1+n_2}(z)) + a_1\Sigma^{n_1}(b_2) + b_1 \\ &= a_3\Sigma^{n_3}(z) + b_3 \end{aligned}$$

où $a_3 = a_1\Sigma^{n_1}(a_2)$, où $b_3 = a_1\Sigma^{n_1}(b_2) + b_1$ et où $n_3 = n_1 + n_2$. Comme $a_1\Sigma^{n_1}(a_2)$ est de module 1 car a_1 et a_2 sont de module 1, la composée $u_1 \circ u_2$ est une isométrie. Ainsi I est stable par composition et est un sous-groupe de $S_{\mathbb{C}}$, comme annoncé.

(6.8) Quelques morphismes et quelques sous-groupes.

(6.8.1) Pour tout entier n, l'élément $(-1)^n$ de $\{-1, 1\}$ ne dépend que de la parité de n, et donc que de l'élément Σ^n de $\langle\Sigma\rangle$. La formule

$$[z \mapsto a\Sigma^n + b] \mapsto (-1)^n$$

définit donc une application f de I dans $\{-1, 1\}$, qui envoie par construction toute isométrie directe sur 1 et toute isométries indirecte sur (-1). L'égalité $n_3 = n_1 + n_2$ de 6.7 entraîne que $f(uu') = f(u)f(u')$ pour tout couple (u, u') d'isométries de $\mathbb{C}$; autrement dit, f est un morphisme de groupes. En termes plus concrets, cela signife que le produit uu' de deux isométries u et u' de $\mathbb{C}$ est :

- direct si u et u' sont ou bien toutes deux directes, ou bien toutes deux indirectes ;
- indirect si l'une des deux isométries u et u' est directe et l'autre indirecte.

Le noyau de f est l'ensemble des isométries directes de $\mathbb{C}$; ce dernier est donc un sous-groupe de I, que nous noterons I^+.

(6.8.2) Soit g l'application de I^+ dans $\mathbb{U}$ qui envoie une isométrie directe donnée par la formule $z \mapsto az + b$ (avec $a \in \mathbb{U}$ et $b \in \mathbb{C}$) sur l'élément a de $\mathbb{U}$. L'égalité $a_3 = a_1\Sigma_1^{n_1}(a_2)$ de 6.7 devient simplement $a_3 = a_1a_2$ lorsque $\Sigma^{n_1} = \mathrm{Id}$, et elle entraîne donc que $g(uu') = g(u)g(u')$ pour tout couple (u, u') d'isométries directes ; autrement dit, g est un morphisme de groupes.

Le noyau de g est par définition l'ensemble des isométries directes données par une formule $z \mapsto az + b$ comme ci-dessus avec $a = 1$, c'est-à-dire l'ensemble T des translations. Ce dernier est donc un sous-groupe de I^+. Puisque l'on a $T_{b+c} = T_b \circ T_c$ pour tout couple (b, c) de nombres complexes, la formule $b \mapsto T_b$ définit un morphisme de groupes de $\mathbb{C}$ vers T. Il est surjectif par définition d'une translation, et injectif car le vecteur d'une translation est uniquement déterminé (*cf.* 6.5.1) ; c'est donc un isomorphisme.

(6.8.3) Soit $z_0 \in \mathbb{C}$. Le stabilisateur $\mathsf{I}^+_{z_0}$ de z_0 dans I^+ est un sous-groupe de I^+. Une translation qui n'est pas l'identité n'ayant pas de point fixe, la seule translation appartenant à $\mathsf{I}^+_{z_0}$ est l'identité, qui est égale à $R_{z_0,0}$. Par ailleurs, une rotation d'angle non nul modulo 2π a un unique point fixe (son centre) ; elle appartient donc à $\mathsf{I}^+_{z_0}$ si et seulement si son centre est z_0. On en déduit que $\mathsf{I}^+_{z_0}$ est exactement l'ensemble $\{R_{z_0,\theta}\}_{\theta\in\mathbb{R}}$.

Soit h l'application de $\mathbb{U}$ dans $\mathsf{I}^+_{z_0}$ qui envoie un élément a de $\mathbb{U}$ sur l'isométrie $z \mapsto z_0 + a(z - z_0)$ (qui est la rotation de centre z_0 et d'argument $\mathrm{Arg}(a)$). C'est une application surjective d'après la description de $\mathsf{I}^+_{z_0}$, et injective d'après 6.5.2.

On a par ailleurs pour tout a et b dans $\mathbb{U}$ et tout $z \in \mathbb{C}$ les égalités

$$\begin{aligned} h(a)(h(b)(z)) &= h(a)z_0 + b(z - z_0) \\ &= z_0 + a(z_0 + b(z - z_0) - z_0) \\ &= z_0 + ab(z - z_0) \\ &= h(ab)(z). \end{aligned}$$

Ainsi $h(ab) = h(a) \circ h(b)$; par conséquent, h est un morphisme de groupes, et donc un isomorphisme puisque c'est une bijection. On vérifie immédiatement que h^{-1} est la restriction à $\mathsf{I}^+_{z_0}$ du morphisme g défini au 6.8.2.

Les groupes $\mathbb{U}$ et $\mathsf{I}^+_{z_0}$ sont ainsi isomorphes. Notons une conséquence fondamentale de ce fait : *le groupe $\mathsf{I}^+_{z_0}$ est abélien.*

(6.8.4) Disons maintenant quelque mot du stabilisateur I_{z_0} de z_0 dans I. C'est un sous-groupe de I ; son intersection avec I^+ est le groupe $\mathsf{I}^+_{z_0}$, c'est-à-dire par ce qui précède l'ensemble des rotations de centre z_0.

Soit u une isométrie indirecte. Il résulte de 6.6.2 que u est une symétrie glissée ; en vertu de 6.12.2, l'isométrie u a un point fixe si et seulement si son vecteur de glissement est nul, c'est-à-dire si et seulement si c'est une symétrie orthogonale (dont l'axe est alors l'ensemble des points fixes). Par conséquent, $u \in \mathsf{I}_{z_0}$ si et seulement si u est une symétrie orthogonale par rapport à une droite passant par z_0.

Le groupe I_{z_0} est ainsi constitué des rotations de centre z_0 et des symétries orthogonales par rapport à une droite passant par z_0.

(6.9) Composition d'isométries directes : quelques compléments. Soient u et v deux isométries directes. On peut écrire $u = z \mapsto e^{i\theta}z + b$ et

$v = z \mapsto e^{i\varphi}z + c$ où θ et φ sont des nombres réels, et b et c des nombres complexes. La composée $u \circ v$ est alors en vertu de 6.8.2 une isométrie directe donnée par une formule du type $z \mapsto e^{i\theta}e^{i\varphi}z + d = e^{i(\theta+\varphi)}z + d$, où d est un nombre complexe (qu'on pourrait expliciter à l'aide de 6.7 mais nous n'en aurons pas besoin). Distinguons maintenant quatre cas.

(6.9.1) *Supposons que les angles θ et φ sont tous deux nuls modulo 2π.* On a alors $e^{i\theta} = e^{i\varphi} = e^{i(\theta+\varphi)} = 1$, et les isométries u, v et $u \circ v$ sont des translations.

(6.9.2) *Supposons que l'un des deux angles θ et φ (disons θ) est nul modulo 2π et l'autre non.* Dans ce cas $e^{i\theta} = 1$ et u est une translation, tandis que $e^{i\varphi} \neq 1$ et que v est une rotation d'angle φ. On a alors $e^{i(\theta+\varphi)} = e^{i\varphi}$ et $u \circ v$ est donc également une rotation d'angle φ – mais en général, son centre n'est pas le même que celui de v (si c'est le même elle coïncide avec v, ce qui n'est possible que si $u = \mathrm{Id}$, c'est-à-dire si $b = 0$).

(6.9.3) *Supposons que θ, φ et $\theta + \varphi$ sont tous trois non nuls modulo 2π.* Dans ce cas $e^{i\theta}$, $e^{i\varphi}$ et $e^{i(\theta+\varphi)}$ sont tous trois différents de 1 ; par conséquent u est une rotation d'angle θ, v est une rotation d'angle φ, et $u \circ v$ est une rotation d'angle $\theta + \varphi$. On ne peut rien dire de particulier sur son centre, sauf si u et v ont même centre z_0 : dans ce cas le centre de $u \circ v$ est aussi égalà z_0.

(6.9.4) *Supposons que les angles θ et φ sont tous deux non nuls modulo 2π, et que $\theta + \varphi = 0$ modulo 2π.* Dans ce cas $e^{i\theta}$ et $e^{i\varphi}$ sont tous deux différents de 1, et $e^{i(\theta+\varphi)} = 1$; par conséquent u est une rotation d'angle θ et v est une rotation d'angle $\varphi = -\theta$ (modulo 2π), tandis que $u \circ v$ est une translation. Le vecteur de $u \circ v$ est nul si et seulement si $v = u^{-1}$, c'est-à-dire encore si et seulement si u et v ont même centre.

(6.10) Compositions d'isométries indirectes : quelques compléments. Soient u et v deux isométries indirectes. On peut écrire

$$u = z \mapsto e^{i\theta}\overline{z} + b \text{ et } v = z \mapsto e^{i\varphi}\overline{z} + c,$$

où θ et φ sont des nombres réels, et b et c des nombres complexes. La composée $u \circ v$ est alors en vertu de 6.8.2 une isométrie directe donnée par une formule du type $z \mapsto e^{i\theta}e^{-i\varphi}z + d = e^{i(\theta-\varphi)}z + d$, où d est un nombre complexe (qu'on pourrait expliciter à l'aide de 6.7 mais nous n'en aurons pas besoin). Distinguons maintenant deux cas, en remarquant tout d'abord qu'en vertu de 6.6.2 les isométries u et v sont des symétries glissées, dont les axes respectifs seront notés Δ_u et Δ_v : d'après *loc. cit.*, l'angle de Δ_u (resp. Δ_v) avec l'axe réel est égal à $\theta/2$ (resp. $\varphi/2$).

(6.10.1) *Supposons que $\theta - \varphi$ est non nul modulo 2π.* Cela signifie que $\theta/2 - \varphi/2$ est non nul modulo π, c'est-à-dire que les axes Δ_u et Δ_v ne sont pas parallèles. La composée $u \circ v = z \mapsto e^{i(\theta-\varphi)}z + d$ est alors une rotation d'angle non nul $\theta - \varphi$; notez que $\theta - \varphi = 2(\theta/2 - \varphi/2)$: cet angle est donc le double de l'angle $(\widehat{\Delta_v, \Delta_u})$. Il n'y a rien de particulier à dire sur le centre de cette rotation, excepté lorsque les vecteurs glissement de u et v sont nuls, c'est-à-dire celui lorsque u est la symétrie Σ_{Δ_u} et où v est la symétrie Σ_{Δ_v}. Dans ce cas l'axe Δ_u est l'ensemble des points fixes de u, et l'axe Δ_v est l'ensemble des points fixes de v. Les droites Δ_u et Δ_v n'étant pas parallèles, leur intersection est un singleton $\{z_0\}$, qui est fixe à la fois sous u et v, et donc sous $u \circ v$; c'est par conséquent le centre de la rotation (d'angle non nul) $u \circ v$.

(6.10.2) *Supposons que $\theta-\varphi$ est nul modulo 2π.* Cela signifie que $\theta/2-\varphi/2$ est nul modulo π, c'est-à-dire que les axes Δ_u et Δ_v sont parallèles. La composée $u\circ v = ze^{i(\theta-\varphi)}z+d = z+d$ est alors une translation.

Disons quelques mots de son vecteur. Pour ce faire, commençons par noter qu'il existe un unique vecteur ω orthogonal à la direction commune de Δ_u et Δ_v, c'est-à-dire multiple réel de $ie^{i\theta/2}$, tel que $\Delta_u = T_\omega(\Delta_v)$. Pour le voir, on choisit γ sur Δ_u et δ sur Δ_v, on pose $\varepsilon = e^{-i\theta/2}(\gamma-\delta)$, et l'on note ε_1 et ε_2 les parties réelle et imaginaire de ε. On a alors $\gamma = \delta+e^{i\theta/2}\varepsilon = \delta+ie^{i\theta/2}\varepsilon_2+e^{i\theta/2}\varepsilon_1$ et

$$\Delta_u = \underbrace{\{\gamma+\lambda e^{i\theta/2}\}_{\lambda\in\mathbb{R}} = \{\delta+\mu e^{i\theta/2}+i\varepsilon_2 e^{i\theta/2}\}_{\mu\in\mathbb{R}}}_{\text{poser } \mu=\lambda-\varepsilon_1} = T_\omega(\Delta_v)$$

avec $\omega = i\varepsilon_2 e^{i\theta/2}$, d'où l'existence. Et si ω' est un autre vecteur répondant aux conditions requises alors $\delta+\omega$ et $\delta+\omega'$ appartiennent tous deux à Δ_u, et leur différence $\omega-\omega'$ est de ce fait un multiple réel de $e^{i\theta/2}$; mais c'est aussi un multiple réel de $ie^{i\theta/2}$ (car c'est déjà le cas de ω et ω'), et cette différence est donc nulle ; il vient $\omega'=\omega$, d'où l'unicité.

Le vecteur de glissement de u est de la forme $\lambda e^{i\theta/2}$ avec $\lambda\in\mathbb{R}$, celui de v est de la forme $\mu e^{i\theta/2}$ avec $\mu\in\mathbb{R}$, et ω est de la forme $\nu ie^{i\theta/2}$ avec $\nu\in\mathbb{R}$. On a d'après la formule (6) de 6.12.2 les égalités

$$\begin{aligned}
u(v(\delta)) &= u(\delta+e^{i\theta}(\overline{\delta-\delta})+\mu e^{i\theta/2})\\
&= u(\delta+\mu e^{i\theta/2})\\
&= \gamma+e^{i\theta}(\overline{\delta+\mu e^{i\theta/2}-\gamma})+\lambda e^{i\theta/2}\\
&= \delta+ie^{i\theta/2}\varepsilon_2+e^{i\theta}(\overline{\mu e^{i\theta/2}-i\nu e^{i\theta/2}})+\lambda e^{i\theta/2}\\
&= \delta+i\nu e^{i\theta/2}+e^{i\theta}(\mu e^{-i\theta/2}+i\nu e^{-i\theta/2})+\lambda e^{i\theta/2}\\
&= \delta+i\nu e^{i\theta/2}+\mu e^{i\theta/2}+i\nu e^{i\theta/2}+\lambda e^{i\theta/2}\\
&= \delta+(\lambda+\mu)e^{i\theta/2}+2\nu ie^{i\theta/2}.
\end{aligned}$$

Le vecteur de la translation $u\circ v$ est donc égal à $(\lambda+\mu)e^{i\theta/2}+2\nu ie^{i\theta/2}$. Sa composante parallèle aux axes Δ_u et Δ_v est ainsi la somme des vecteurs de glissement de u et v ; sa composante orthogonale à ces axes est quant à elle égale à 2ω.

(6.11) Interprétation concrète. Soient Δ_u et Δ_v deux droites de $\mathbb{C}$. Les faits suivants résultent de 6.10.1 et 6.10.2 :

(A) Si Δ_u et Δ_v ne sont pas parallèles et si z_0 désigne leur point d'intersection alors $\Sigma_{\Delta_u}\circ\Sigma_{\Delta_v}$ est la rotation de centre z_0 et d'angle $2(\widehat{\Delta_u,\Delta_v})$.

(B) Si Si Δ_u et Δ_v sont parallèles et si ω désigne le vecteur orthogonal à leur direction commune tel que $\Delta_u = T_\omega(\Delta_v)$ alors $\Sigma_{\Delta_u}\circ\Sigma_{\Delta_v}$ est la translation de vecteur 2ω.

Nous allons maintenant mentionner de ≪vrais≫ phénomènes qui peuvent s'interpréter comme des conséquences de (A) et (B) – nous vous laissons comprendre vous-mêmes comment.

(6.11.1) *Conséquence concrète de* (A). Si vous regardez votre image dans un miroir puis que vous faites basculer celui-ci en arrière d'un angle θ, l'image bascule de l'angle 2θ.

(6.11.2) *Conséquence concrète de* (B). Si vous regardez votre image dans un miroir puis que vous faites reculer celui-ci d'une distance D, l'image recule de la distance $2D$.

(6.12) Quelques calculs explicites.

(6.12.1) L'application $u\colon z \mapsto iz - 3$ est, par son écriture même et en vertu de 6.6.1, une rotation d'angle $\pi/2$. On détermine son centre z_0 en caractérisant celui-ci comme son unique point fixe, c'est-à-dire comme l'unique solution de l'équation $z = iz - 3$. Il vient

$$z_0 = \frac{-3}{1-i} = \frac{-3(1+i)}{2} = -\frac{3}{2} - \frac{3i}{2}.$$

L'isométrie u est donc la rotation de centre $-\frac{3}{2} - \frac{3i}{2}$ et d'angle $\pi/2$.

(6.12.2) L'application $v\colon z \mapsto -\overline{z}+1+i$ est, par son écriture même et en vertu de 6.6.2, une symétrie glissée. On trouve son vecteur de glissement en calculant v^2. On a pour tout $z \in \mathbb{C}$ les égalités

$$\begin{aligned} v(v(z)) &= -\overline{v(z)} + 1 + i \\ &= -(\overline{-\overline{z} + 1 + i}) + 1 + i \\ &= -(-z + 1 - i) + 1 + i \\ &= z - 1 + i + 1 + i \\ &= z + 2i. \end{aligned}$$

On a donc $v^2 = T_{2i}$, si bien que le vecteur de glissement de v est égal à $(2i)/2 = i$. L'axe de v est alors égal à l'ensemble des points fixes de $T_{-i} \circ v = z \mapsto -\overline{z} + 1$. Soit $z \in \mathbb{C}$. On a les équivalences

$$\begin{aligned} z = -\overline{z} + 1 \quad &\iff \quad z + \overline{z} = 1 \\ &\iff \quad 2 \cdot \mathrm{Re}(z) = 1. \end{aligned}$$

Ainsi v est la symétrie glissée d'axe la droite verticale d'équation $\mathrm{Re}(z) = 1/2$ et de vecteur de glissement i.

(6.13) Soit n un entier $\geqslant 3$. Un *polygone régulier à n sommets* de $\mathbb{C}$ est un sous-ensemble de $\mathbb{C}$ de la forme

$$\{z_0 + ae^{2ik\pi/n}\}_{k\in\mathbb{Z}}$$

où $z_0 \in \mathbb{C}$ et $a \in \mathbb{C}^\times$.

(6.14) Soit n un entier $\geqslant 3$ et soit P un polygone régulier à n sommets. Soient $z_0 \in \mathbb{C}$ et $a \in \mathbb{C}^\times$ tels que $P = \{z_0 + ae^{2ik\pi/n}\}_{k\in\mathbb{Z}}$.

(6.14.1) Comme $e^{2ik\pi/n} = e^{2i\ell\pi/n}$ si et seulement si k et ℓ sont égaux modulo n, les éléments $z_0 + a, z_0 + ae^{2i\pi/n}, \ldots, z_0 + ae^{2i(n-1)\pi/n}$ de P sont deux à deux distincts, et

$$P = \{z_0 + a, z_0 + ae^{2i\pi/n}, \ldots, z_0 + ae^{2i(n-1)\pi/n}\}.$$

Par conséquent, P comprend exactement n éléments, qu'on appelle parfois ses *sommets*.

(6.14.2) On a les égalités

$$\begin{aligned}\frac{1}{n}\sum_{z\in P} z &= \frac{1}{n}\sum_{k=0}^{n-1} z_0 + ae^{2ik\pi/n}\\ &= \frac{1}{n}\left(nz_0 + a\sum_{k=0}^{n-1}(e^{2i\pi/n})^k\right)\\ &= \frac{1}{n}\left(nz_0 + a\frac{(e^{2i\pi/n})^n - 1}{e^{2i\pi/n}-1}\right)\\ &= \frac{1}{n}\cdot nz_0\\ &= z_0.\end{aligned}$$

Ainsi z_0 est uniquement déterminé par P ; on l'appelle son *centre*. Notons que comme $a \neq 0$, tout sommet de P est de la forme $z_0 + b$ avec $b \neq 0$.

(6.14.3) Nous allons maintenant décrire P en termes de théorie des groupes. On a défini plus haut (6.8.3) un isomorphisme h du groupe $\mathbb{U}$ sur le stabilisateur $\mathsf{I}^+_{z_0}$ de z_0 dans le groupe des isométries directes ; cet isomorphisme envoie un élément a de $\mathbb{U}$ sur la rotation $z \mapsto z_0 + a(z - z_0)$. Soit μ_n le sous-groupe de $\mathbb{U}$ engendré par $e^{2i\pi/n}$. Par définition, μ_n est l'ensemble des nombres complexes de la forme $e^{2ik\pi/n}$ avec $k \in \mathbb{Z}$, c'est-à-dire l'ensemble des racines n-ièmes de l'unité ; comme $e^{2i\pi/n}$ est d'ordre n, le groupe μ_n est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

L'image G de $h(\mu_n)$ est un sous-groupe de $\mathsf{I}^+_{z_0}$, isomorphe à μ_n (car h est injective) et donc $\mathbb{Z}/n\mathbb{Z}$. Par définition, G est constitué des rotations de la forme $R_{z_0,2k\pi+n} = R^k_{z_0,2\pi/n}$ avec $k \in \mathbb{Z}$; on peut également le décrire comme le sous-groupe de $\mathsf{I}^+_{z_0}$ engendré par $R_{(z_0,2\pi/n)}$.

Le polygone P est égal à

$$\{z_0 + ae^{2ik\pi/n}\}_{k\in\mathbb{Z}},$$

c'est-à-dire encore à $\{R_{z_0,2k\pi/n}(z_0 + a)\}_{k\in\mathbb{Z}}$, ou encore à $\{g(z_0 + a)\}_{g\in G}$. Autrement dit, P est l'orbite de $z_0 + a$ sous G. Mais on sait alors que P est également l'orbite sous G de n'importe lequel de ses sommets (lemme 4.6.4). Cela signifie qu'on a pour tout $b \in \mathbb{C}$ tel que $z_0 + b \in P$ les égalités

$$P = \{g(z_0 + b)\}_{g\in G} = \{z_0 + be^{2ik\pi/n}\}_{k\in\mathbb{Z}}$$

(vous pouvez aussi le vérifier directement, sans faire appel aux résultats généraux sur les orbites).

(6.15) Groupe des isométries d'un polygone. Soit n un entier $\geqslant 3$ et soit P un polygone régulier à n sommets de $\mathbb{C}$. Soit Γ (resp. Γ^+) l'ensemble des isométries (resp. isométries directes) g de $\mathbb{C}$ que $g(P) = P$.

(6.15.1) Montrons que Γ est un sous-groupe de I. Il est clair que $\mathrm{Id} \in \Gamma$. Si g et h sont deux éléments de Γ on a alors $(gh)(P) = g(h(P)) = g(P) = P$, et gh appartient donc à Γ. Enfin si $g \in \Gamma$ alors comme $P = g(P)$ il vient $g^{-1}(P) = g^{-1}(g(P)) = (g^{-1}g)(P) = P$, et $g^{-1} \in \Gamma$. Ainsi Γ est bien un sous-groupe de I, qu'on appelle en général le *groupe des isométries de P*. Par définition, $\Gamma^+ = \Gamma \cap \mathsf{I}^+$; c'est donc un sous-groupe de I^+, appelé *groupe des isométries directes de P*.

(6.15.2) Soit $g \in \mathsf{I}$. Par définition, g appartient à Γ si et seulement si $g(P) = P$; mais il suffit en fait que $g(P)$ soit *contenu* dans P : en effet si c'est le cas alors $g(P)$ est un sous-ensemble de P de cardinal n (car g est injective) et est donc égal à P tout entier.

(6.16) Groupe des isométries d'un polygone : description explicite. Soit n un entier $\geqslant 3$ et soit P un polygone régulier à n sommets. On note Γ (resp. Γ^+) le groupe des isométries (resp. isométries directes) de P. Le but de ce qui suit est de décrire explicitement les groupes Γ et Γ^+ ; on note z_0 le centre de P.

(6.16.1) Soit g une isométrie appartenant à Γ. Écrivons $g = z \mapsto \alpha\Sigma^m(z) + \beta$ avec $\alpha \in \mathbb{U}$, $m \in \mathbb{Z}$ et $\beta \in \mathbb{C}$. On a

$$\begin{aligned}
g(z_0) &= g\left(\frac{1}{n}\sum_{z\in P} z\right) \\
&= \alpha\Sigma^m\left(\frac{1}{n}\sum_{z\in P} z\right) + \beta \\
&= \frac{1}{n}\sum_{z\in P} \alpha\Sigma^m(z) + \beta \\
&= \frac{1}{n}\left(\sum_{z\in P} \alpha\Sigma^m(z) + n\beta\right) \\
&= \frac{1}{n}\sum_{z\in P} (\alpha\Sigma^m(z) + \beta) \\
&= \frac{1}{n}\sum_{z\in P} g(z) \\
&= \frac{1}{n}\sum_{z\in g(P)} z \\
&= \frac{1}{n}\sum_{z\in P} z \\
&= z_0.
\end{aligned}$$

Ainsi, Γ est contenu dans le stabilisateur I_{z_0} de z_0, qui consiste précisément en les rotations de centre z_0 et les symétries orthogonales dont l'axe passe par z_0 (6.8.4).

(6.16.2) *Description de* Γ^+. Soit G le sous-groupe de $\mathsf{I}^+_{z_0}$ constitué des rotations dont l'angle est de la forme $2k\pi/n$ avec $k \in \mathbb{Z}$. On sait que pour tout $z \in P$ le polygone P est l'orbite de z sous G (6.14.3) ; en particulier, $g(z) \in P$ pour tout $g \in G$. Ainsi $g(P) \subset P$ pour tout $g \in G$, et G est par conséquent contenu dans Γ^+ (en vertu de 6.15.2).

Réciproquement, soit g un élément de Γ^+. Il résulte de 6.16.1 que g est une rotation de centre z_0, donc de la forme $z \mapsto z_0 + \alpha(z - z_0)$ pour un certain $\alpha \in \mathbb{U}$. Choisissons un élément de P, que nous écrivons sous la forme $z_0 + a$ avec $a \neq 0$. On a $g(z_0 + a) = z_0 + a\alpha$. Mais $g(z_0 + a)$ appartient à P (car g appartient à Γ^+) ; puisque P est l'orbite de $z_0 + a$ sous G (6.14.3), cela signifie

que $g(z_0+a)=z_0+ae^{2ik\pi/n}$ pour un certain entier k. Il vient

$$z_0+a\alpha=z_0+ae^{2ik\pi/n}$$

et partant $\alpha=e^{2ik\pi/n}$ car $a\neq 0$. En conséquence g appartient à G, d'où l'inclusion $\Gamma^+\subset G$, et finalement l'égalité $\Gamma^+=G$. Le groupe des isométries directes de P est donc le groupe des rotations de centre z_0 dont l'angle est un multiple entier de $2\pi/n$, ou encore le sous-groupe de $\mathsf{I}^+_{z_0}$ engendré par $R_{(z_0,2\pi/n)}$; il est isomorphe à $\mathbb{Z}/n\mathbb{Z}$.

(6.16.3) *Description des autres éléments* Γ. Pour décrire complètement Γ, il reste à comprendre son sous-ensemble Γ^- constitué des isométries indirectes. Comme $\Gamma\subset\mathsf{I}_{z_0}$, il résulte de 6.8.4 que Γ^- est constitué de symétries orthogonales dont l'axe passe par z_0. Soit g une telle symétrie et soit θ l'angle que fait son axe avec l'axe réel. Nous allons déterminer pour quelles valeurs de θ la symétrie g appartient à Γ^-.

Fixons un sommetde P, que nous écrivons $z_0+re^{i\varphi}$ avec $r\in\mathbb{R}_+^\times$ et $\varphi\in\mathbb{R}$. Pour tout entier relatif k on pose $w_k=z_0+re^{i(\varphi+k\pi/n)}$. Notre sommet initial est w_0, et le polygone P est l'ensemble des w_k pour k pair, qui est en fait réduit à $\{w_0,w_2,\dots,w_{2n-2}\}$; notons également que pour tout k, la droite (z_0w_k) est la droite passant par z_0 et dirigée par $e^{i(\varphi+k\pi/n)}$, ou encore la droite passant par z_0 et d'angle $\varphi+k\pi/n$ avec l'horizontale.

L'isométrie g appartient à Γ^- si et seulement si $g(w_{2k})$ appartient à P pour tout k, c'est-à-dire si et seulement si pour tout entier k, il existe un entier ℓ tel que $g(w_{2k})=w_{2\ell}$.

Soit $k\in\mathbb{Z}$. On a en vertu de 6.5.3 les égalités

$$g(w_{2k})=g(z_0+e^{i(\varphi+2k\pi+n)})=z_0+re^{i(2\theta-\varphi-2k\pi/n)}.$$

Il s'ensuit que $g(w_{2k})$ appartient à P si et seulement si il existe un entier ℓ tel que

$$\begin{array}{rcc} & z_0+re^{i(2\theta-\varphi-2k\pi/n)} & = & z_0+re^{i(\varphi+2\ell\pi/n)} \\ \iff & e^{i(2\theta-\varphi-2k\pi/n)} & = & e^{i(\varphi+2\ell\pi/n)} \\ \iff & 2\theta-\varphi-2k\pi & = & \varphi+2\ell\pi/n \mod 2\pi \\ \iff & 2\theta & = & 2\varphi+2\ell\pi/n+2k\pi/n \mod 2\pi \\ \iff & \theta & = & \varphi+\ell\pi/n+k\pi/n \mod \pi \end{array}$$

Puisque π est multiple entier de π/n, cela revient simplement à demander que θ soit égal à $\varphi+k\pi/n$ modulo π/n, ou encore tout simplement que θ soit égal à φ modulo π/n ; cette condition ne dépend alors plus de k.

On voit ainsi que g appartient à Γ^- si et seulement si θ est égal à φ modulo π/n. L'ensemble Γ^- est donc constitué des symétries orthogonales dont l'axe passe par z_0 et fait avec l'axe réel un angle de la forme $\varphi+\ell\pi/n$ avec $\ell\in\mathbb{Z}$; c'est également l'ensemble des symétries orthogonales dont l'axe est de la forme (z_0w_ℓ) avec $\ell\in\mathbb{Z}$. Si ℓ et ℓ' sont deux entiers, les droites (z_0w_ℓ) et $(z_0w_{\ell'})$ coïncident si et seulement si leurs vecteurs directeurs $e^{i(\varphi+\ell\pi/n)}$ et $e^{i(\varphi+\ell'\pi/n)}$ sont $\mathbb{R}$-colinéaires, c'est-à-dire si et seulement si $\varphi+\ell\pi/n=\varphi+\ell'\pi/n$ modulo π, ce qui se produit si et seulement si ℓ et ℓ' sont égaux modulo n. On en déduit que les symétries orthogonales

$$\Sigma_{(z_0w_0)},\dots,\Sigma_{(z_0w_{n-1})}$$

sont deux à deux distinctes, et que $\Gamma^- = \{\Sigma_{(z_0 w_0)}, \ldots, \Sigma_{(z_0 w_{n-1})}\}$; l'ensemble Γ^- comporte donc n éléments, et $\Gamma = \Gamma^+ \coprod \Gamma^-$ est en conséquence de cardinal $n + n = 2n$.

Remarquons pour terminer que pour tout sommet z de P, la symétrie orthogonale $\Sigma_{(z_0 z)}$ appartient à Γ^- puisque z est égal à w_{2k} pour un certain entier k.

(6.16.4) *Supposons que n est impair.* Écrivons $n = 2m + 1$ avec $m \in \mathbb{Z}$, et soit $k \in \mathbb{Z}$. On a alors $k = k(n - 2m) = nk - 2km$ et partant

$$\frac{k\pi}{n} = k\pi - \frac{2km\pi}{n}.$$

Il s'ensuit que $e^{i(\varphi + k\pi/n)} = e^{ik\pi} e^{i(\varphi - 2km\pi/n)}$. Par conséquent, les vecteurs $e^{i(\varphi+k\pi/n)}$ et $e^{i(\varphi-2km\pi/n)}$ sont $\mathbb{R}$-colinéaires, et la droite $(z_0 w_k)$ est donc égale à $(z_0 w_{-2km})$ (ainsi qu'à $(w_{2k} w_{-2km})$). Or w_{-2km} est un sommet de P ; on vient ainsi de démontrer que tout élément Γ^- est de la forme $\Sigma_{(z_0 w)}$ avec $w \in P$. On sait par ailleurs que pour tout sommet w de P la symétrie $\Sigma_{(z_0 w)}$ appartient à Γ^-, et que Γ^- et P sont tous deux de cardinal n. En conséquence, lorsque w parcourt P les symétries $\Sigma_{(z_0 w)}$ sont deux à deux distinctes (ce qui veut dire que les droites $(z_0 w)$ sont deux à deux distinctes), et $\Gamma^- = \{\Sigma_{(z_0 w)}\}_{w \in P}$.

(6.16.5) *Supposons que n est pair.* Écrivons $n = 2m$ avec $m \in \mathbb{Z}$. Soit $k \in \mathbb{Z}$. On a

$$\frac{2k\pi}{n} + \pi = \frac{(2k+n)\pi}{n} = \frac{2(k+m)\pi}{n},$$

d'où l'égalité $e^{i(\varphi + 2(k+m)\pi/n)} = -e^{i(\varphi + k\pi/n)}$. Par conséquent $w_{2(k+m)}$ (qui est un sommet de P) est le symétrique du sommet w_{2k} de P par rapport à z_0, et les droites $(z_0 w_{2k})$ et $(z_0 w_{2(k+m)})$ coïncident. Par ailleurs une droite passant par z_0 contient au plus 2 points de la forme w_ℓ (et en particulier au plus deux sommets de P) car ces points sont tous situés à la même distance de z_0 (à savoir r).

On a ainsi établi que pour tout sommet w de P, le symétrique w' de w par rapport à z_0 appartient à P aussi, et que la droite $(z_0 w) = (z_0 w') = (w w')$ ne contient aucun point de la forme w_k à part w et w' (c'est-à-dire aucun autre sommet de P, ni aucun w_k pour k impair). Le sous-ensemble $\{\Sigma_{(z_0 w)}\}_{w \in P}$ de Γ^- comprend donc $m = n/2$ éléments. Les m autres éléments de Γ^- sont les symétries de la forme $\Sigma_{(z_0 w_{2k+1})}$ pour $k \in \mathbb{Z}$ (on peut se limiter aux entiers k tels que $0 < 2k+1 < n$). Remarquons que pour tout k, l'axe $(z_0 w_{2k+1})$ de $\Sigma_{(z_0 w_{2k+1})}$ est la bissectrice de l'angle formé par les deux droites $(z_0 w_{2k})$ et $(z_0 w_{2k+2})$, ou encore la médiatrice du segment $[w_{2k} w_{2k+2}]$.

(6.17) Exemples : le triangle et le carré.

(6.17.1) *Le cas du triangle.* Posons $a = 1, b = e^{2i\pi/3}$ et $c = e^{4i\pi/3}$. L'ensemble $P := \{a, b, c\}$ est alors un polygone régulier à 3 sommets – ce qu'on appelle le plus souvent un triangle équilatéral ; son centre est l'origine. Le groupe des isométries directes de P est égal à $\{\mathrm{Id}, R_{(0,2\pi/3)}, R_{(0,4\pi/3)}\}$. Les isométries indirectes de P sont les symétries orthogonales par rapport aux droites joignant respectivement l'origine à a, à b et à c (qui sont les médiatrices du triangle).

(6.17.2) *Le cas du carré.* Posons $a = 1, b = i, c = -i$ et $d = -1$. L'ensemble $P := \{a, b, c, d\}$ est alors un polygone régulier à 4 sommets – ce qu'on appelle le plus souvent un carré ; son centre est l'origine. Le groupe des isométries directes

de P est égal à $\{\mathrm{Id}, R_{(0,\pi/2)}, R_{(0,\pi)}, R_{(0,3\pi/2)}\}$. Les isométries indirectes de P sont d'une part les symétries orthogonales par rapport aux droites (ac) et (bd) (qui sont les diagonales du carré), et d'autre part les symétries orthogonales par rapport aux droites joignant respectivement l'origine à $e^{i\pi/4}$ et $e^{3i\pi/4}$ (ce sont les deux médiatrices du carré).

(6.18) Isométries d'un polygone et permutation des sommets. Soit n un entier supérieur ou égal à 3 et soit P un polygone régulier à n côtés ; soit z_0 le centre de P et soit Γ le groupe d'isométries de P. Tout élément g de Γ induit par restriction une bijection de P dans lui-même, c'est-à-dire une permutation de P ; on définit ainsi une application ρ de Γ dans S_P qui est en fait un morphisme de groupes (la restriction de la composée est la composée des restrictions).

(6.18.1) *Le morphisme ρ est injectif.* En effet, soit g un élément de $\mathrm{Ker}\ \rho$. Par définition, g est un élément de Γ tel que $g(w) = w$ pour tout $w \in P$.

Si g est une isométrie indirecte alors g est une symétrie othogonale dont l'axe Δ passe par z_0. L'ensemble des points fixes de g est égal à Δ, et $\Delta \cap P$ contient au plus deux sommets ; on aboutit ainsi à une contradiction avec le fait que g fixe les n sommets de P (rappelons que $n \geqslant 3$).

Par conséquent g est une isométrie directe. C'est donc une rotation de centre z_0, et elle au moins un point fixe en plus de z_0 (puisque tous les sommets de P sont fixes) ; il vient $g = \mathrm{Id}$, et ρ est injectif.

(6.18.2) Supposons que $n = 3$. Le groupe Γ est alors de cardinal $2 \times 3 = 6$, et S_P est de cardinal $3! = 6$. Comme Γ et S_P ont même cardinal, le morphisme injectif ρ est alors un isomorphisme. Plaçons-nous dans le cas où P est le triangle $\{a, b, c\}$ décrit au 6.17.1, et décrivons complètement l'isomorphisme ρ dans ce cas.

- On a $\rho(\mathrm{Id}_{\mathbb{C}}) = \mathrm{Id}_P$.
- La rotation $R_{(0,2\pi/3)}$ envoie a sur b, b sur c et c sur a. Son image par ρ est donc le 3-cycle (abc).
- La rotation $R_{(0,4\pi/3)}$ envoie a sur c, c sur b et b sur a. Son image par ρ est donc le 3-cycle (acb).
- La symétrie orthogonale $\Sigma_{(0a)}$ fixe a et échange b et c ; son image par ρ est donc la transposition (bc).
- La symétrie orthogonale $\Sigma_{(0b)}$ fixe b et échange a et c ; son image par ρ est donc la transposition (ac).
- La symétrie orthogonale $\Sigma_{(0c)}$ fixe c et échange a et b ; son image par ρ est donc la transposition (ab).