Université Claude Bernard–Lyon I
Agrégation de Mathématiques : Algèbre & géométrie
Année 2008–2009

Présentations de groupes

Références

- Josette Calais, *Éléments de théorie des groupes*, PUF, chap. IX.
- Jean-Yves Mérindol, *Nombres et algèbre*, EDP Sciences, lieux divers.
- Nathan Jacobson, *Basic Algebra II.*

I Introduction au problème

1° Deux exemples

(a) Groupes cycliques d'ordre 12 On s'intéresse aux groupes engendrés par un élément x satisfaisant la relation $x^{12} = 1$. Certes, $\mathbb{Z}/12\mathbb{Z}$ convient (avec $x = 1$ ou $x = 7$), mais $\mathbb{Z}/6\mathbb{Z}$ (avec $x = 5$ par exemple) et $\mathbb{Z}/3\mathbb{Z}$ aussi (avec $x = \pm 1$).
Décrivons-les tous lourdement. Soit donc G un groupe muni d'un générateur x tel que $x^{12} = 1$. On a un morphisme $\mathbb{Z} \to G$, $n \mapsto x^n$. L'hypothèse que x engendre G exprime que ce morphisme est surjectif. Comme par ailleurs, $x^{12} = 1$, le noyau contient $12\mathbb{Z}$, donc le morphisme se factorise sous la forme : $\mathbb{Z} \to \mathbb{Z}/12\mathbb{Z} \to G$. En d'autres termes, G est un quotient de $\mathbb{Z}/12\mathbb{Z}$. On dira que le groupe présenté par générateur x et relation $x^{12} = 1$ est $\mathbb{Z}/12\mathbb{Z}$.
(b) Groupes diédraux Dans ce paragraphe, on fixe $n \geq 2$. Il existe une action, non triviale dès que $n \geq 3$, de $\mathbb{Z}/2\mathbb{Z}$ sur $\mathbb{Z}/n\mathbb{Z}$: si $\delta \in \mathbb{Z}/2\mathbb{Z}$ et $k \in \mathbb{Z}/n\mathbb{Z}$, $\delta \cdot k = (-1)^\delta k$. Le groupe diédral d'indice n est le produit semi-direct correspondant, $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z}$. Concrètement, ses éléments sont les couples $(k, \delta) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ et le produit est définie par :

$$\forall (k,\delta), (k',\delta') \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}, \quad (k,\delta)(k',\delta') = (k + (-1)^\delta k', \delta + \delta').$$

(Remarque : pour $n = 2$, le produit est direct et D_2 est le groupe de Klein $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.)
Autre réalisation –à connaître– du groupe diédral. Dans le plan complexe $\mathbb{C}$, considéré comme plan euclidien, soit P_n le polygone régulier formé des racines de l'unité :

$$P_n = \{p \in \mathbb{C},\ p^n = 1\}.$$

Soit D_n le groupe des isométries du plan complexe qui stabilisent P_n. Notons qu'une isométrie affine qui stabilise P_n fixe son isobarycentre, qui est 0. Il y a donc au plus deux types d'éléments dans D_n, des rotations et des réflexions.
Soit D_n^+ le sous-groupe de D_n formé des rotations. Une rotation qui fixe P_n est déterminée par l'image d'un sommet : il y en a donc au plus n. Or la rotation ρ (de centre 0 et) d'angle $2\pi/n$ stabilise P_n et elle est d'ordre n, donc toutes les rotations qui fixent P_n sont de la forme ρ^k, $k \in \{0, \ldots, n-1\}$.
Il existe une réflexion σ qui stabilise P, c'est la conjugaison complexe. Mais alors, l'application $D_n \to D_n$, $\varphi \mapsto \varphi\sigma$ est une involution qui échange D_n^+ et son complémentaire. Par suite, il y a exactement n réflexions dans D_n, et ce sont les $\rho^k\sigma$, $k \in \{0, \ldots, n-1\}$.
On vérifie que

$$\sigma^2 = \mathrm{Id} = \rho^n \quad \text{et} \quad \sigma\rho\sigma^{-1} = \rho^{-1}.$$

On en déduit facilement que l'application $\mathbb{Z}/n\mathbb{Z} \rtimes \mathbb{Z}/2\mathbb{Z} \to D_n$, $(k, \delta) \mapsto \rho^k\sigma^\delta$ est un isomorphisme du groupe diédral sur le groupe des isométries du polygone régulier P_n. Montrons à présent que le groupe diédral est "le groupe le plus général" engendré par deux éléments satisfaisant les relations ci-dessus.

Proposition *Soit G un groupe engendré par deux éléments a et b tels que*

$$a^2 = 1 = b^n \quad et \quad aba^{-1} = b^{-1}.$$

Alors il existe un morphisme surjectif $D_n \to G$, $\sigma \mapsto a$, $\rho \mapsto b$.

Pour commencer, exhibons une "forme normale" pour les éléments de G.

Lemme *Sous les hypothèses de la proposition :*

$$\forall g \in G, \quad \exists k \in \mathbb{Z}, \quad g = b^k \ ou \ g = b^k a.$$

Démonstration du lemme. Par hypothèse, tout élément g de G est le produit d'éléments de la forme a, a^{-1}, b et b^{-1}. En regroupant ensemble les lettres identiques et en notant que $a^{-1} = a$ et $b^n = 1$, on obtient une expression de g comme produits d'éléments de la forme a et b^k, $k \in \{0, \dots, n-1\}$. Si on trouve strictement plus d'une occurrence de a, on en choisit deux consécutives. Elles sont séparées par un élément b^k ($k \in \{0, \dots, n-1\}$). Or on a :

$$ab^k a = b^{-k} = b^{n-k},$$

si bien qu'on peut trouver une expression avec strictement moins d'occurrences de a que la précédentes. On peut donc trouver une expression avec zéro ou une occurrence de a. S'il n'y en a pas, c'est gagné. S'il y en a une, c'est que g est de la forme $b^k a b^\ell$. Comme on a :

$$ab^\ell = b^{-\ell} a,$$

on a bien : $g = b^{k-\ell} a$.

Démonstration de la proposition. Notons que le lemme s'applique en particulier à D_n... Comme on sait que le cardinal de D_n est $2n$, les éléments sont tous distincts. On peut établir les tables de multiplication de G et de D_n. (Dans la table, on calcule le produit xy.)

$x \backslash y$	b^ℓ	$b^\ell a$
b^k	$b^{k+\ell}$	$b^{k+\ell}a$
$b^k a$	$b^{k-\ell}a$	$b^{k-\ell}$

$x \backslash y$	ρ^ℓ	$\rho^\ell \sigma$
ρ^k	$\rho^{k+\ell}$	$\rho^{k+\ell}\sigma$
$\rho^k \sigma$	$\rho^{k-\ell}\sigma$	$\rho^{k-\ell}$

On constate que quitte à remplacer ρ par a et σ par b, les tables sont identiques. Cela signifie précisément que l'application

$$\begin{array}{rccc} \varphi : & D_n & \longrightarrow & G \\ & \rho^k & \longmapsto & b^k \\ & \rho^k \sigma & \longmapsto & b^k a \end{array}$$

est un morphisme, et il est surjectif car son image contient a et b, qui engendrent G.

Application : morphismes $D_n \to \mathbb{C}^*$

À titre d'application, on détermine tous les morphismes de D_n vers $\mathbb{C}^*$. Soit χ un tel morphisme, $a = \chi(\sigma)$ et $b = \chi(\rho)$. On a nécessairement, vu les relations satisfaites par σ et ρ :

$$a^2 = 1 = b^n \quad \text{et} \quad aba = b^{-1}.$$

Cette dernière relation s'écrit $b^2 = 1$, c'est-à-dire $b = \pm 1$. En prenant en compte l'égalité $b^n = 1$, on voit que $b = 1$ si n est impair.

Inversement, fixons $a \in \{-1, 1\}$ et $b \in \{-1, 1\}$ (si n est pair) ou $b = 1$ (si n est impair). Le sous-groupe de $\mathbb{C}^*$ engendré par a et b satisfait les hypothèses de la proposition, donc il existe un morphisme $\chi : D_n \to \mathbb{C}^*$ tel que $\chi(\sigma) = a$ et $\chi(\rho) = b$. On reviendra plus loin sur cet exemple pour donner une "explication géométrique" de la différence n pair/n impair.

Bilan : On a en fait obtenu une présentation par générateurs et relations du groupe diédral D_n. Les générateurs sont ρ et σ et les relations sont $\sigma^2 = \rho^n = \sigma\rho\sigma\rho = 1$. On a vu que le groupe diédral est "le groupe le plus général" engendré par deux éléments satisfaisant ces relations, et comment en déduire facilement les morphismes $D_n \to \mathbb{C}^*$.
Le but de ce texte est de donner un formalisme pour étendre ces constructions à d'autres systèmes de relations. Etant donné un ensemble de générateurs et un ensemble de relations, il y a en fait deux problèmes :

- existe-t-il un "groupe le plus général" satisfaisant ces relations ? on le construira comme solution à un problème universel ;
- comment reconnaître, travailler avec un tel groupe : à ce problème difficile, on ne donnera qu'un seul exemple, celui du groupe symétrique.

2° Exemples de problèmes universels

(a) Bases d'un espace vectoriel

Partons de la propriété bien connue suivante :

Proposition *Etant donné deux espaces vectoriels V et W sur $\mathbb{K}$, une base $B = (e_i)_{i\in I}$ d'éléments de V et une famille $(f_i)_{i\in I}$ d'éléments de W [donnée équivalente à une fonction $f : B \to W$, $e_i \mapsto f_i$], il existe une unique application linéaire $\varphi : V \to W$ telle que $\varphi(e_i) = f_i$ pour tout $i \in I$.*

Problème *Soit $\mathbb{K}$ un corps, V un espace vectoriel sur $\mathbb{K}$, B une base de V. À quelle condition, portant sur B, a-t-on la propriété suivante : pour tout espace vectoriel W, toute application $f : B \to W$ se prolonge en une unique application linéaire $\varphi : V \to W$ (telle que $f = \varphi \circ i$, où $i : B \hookrightarrow V$ est l'injection canonique) ?*

Réponse Une condition nécessaire et suffisante est que B soit une base de V, et c'est une façon de reformuler la propriété précédente.
En effet, prenons pour W un espace vectoriel de dimension $\dim W \geq |B|$. Lorsque $f(B)$ est une famille libre de W, l'existence de φ impose que B soit elle-même libre. Par ailleurs, si B n'est pas génératrice, on complète de deux façons différentes B (supposée libre) en deux bases $B \cup C$ et $B \cup C'$ de V ; alors, une bijection de C sur C' induit une application linéaire $\varphi : V \to V$ différente de l'identité, et on a donc deux applications qui répondent au problème.

À présent, nous allons reformuler les choses de sorte à "mutifier" V.

Problème *Soit $\mathbb{K}$ un corps et X un ensemble. On cherche un espace vectoriel V et une application $i : X \to V$ tels que pour tout espace vectoriel W et toute application $f : B \to W$, il existe une unique application linéaire $\varphi : V \to W$ telle que $f = \varphi \circ i$.*

D'après ce qui précède, $i(X)$ doit être une base de V. Etant donné l'ensemble X, on connaît un espace vectoriel dont une base est (en bijection avec) X : c'est $\mathbb{K}^{(X)}$. Ses éléments sont les familles de scalaires presque nulles, i.e. les applications $X \to \mathbb{K}$ à support fini :

$$\mathbb{K}^{(X)} = \{\lambda : X \to \mathbb{K},\ |\operatorname{Supp}\lambda| < +\infty\}, \quad \text{où, pour } \lambda : X \to \mathbb{K}, \quad \operatorname{Supp}\lambda = \{x \in X,\ \lambda(x) \neq 0\}.$$

Remarque : unicité de la solution à isomorphisme près. Soit V, $i : X \to V$ et V', $i' : X \to V'$ deux solutions de ce problème. Comme (V, i) est une solution, il existe une application linéaire $\varphi : V \to V'$ telle que $\varphi \circ i = i'$. De même, comme (V', i') est une solution, il existe une application linéaire $\varphi' : V' \to V$ telle que $\varphi' \circ i' = i$. Mais alors, $\varphi' \circ \varphi$ et $\mathrm{Id}_V : V \to V$ sont deux applications qui prolonge i : $\varphi' \circ \varphi \circ i = i$. Par unicité de l'application dans le problème universel de (V, i), c'est que $\varphi' \circ \varphi = \mathrm{Id}_V$. De même, on montre que $\varphi \circ \varphi' = \mathrm{Id}_{V'}$. Ainsi, V et V' sont isomorphes.

(b) Groupes abéliens libres

Relire le paragraphe précedent en remplaçant $\mathbb{K}$ par $\mathbb{Z}$, "espace vectoriel" par "groupe abélien".

(c) Polynômes

Problème *Soit $\mathbb{K}$ un corps et X un ensemble. On cherche un anneau, noté $\mathbb{K}[X]$, tel que pour tout $\mathbb{K}$-algèbre commutative unitaire A et toute application $f : X \to A$, il existe un unique morphisme d'algèbres $\varphi : \mathbb{K}[X] \to A$ tel que $f = \varphi \circ i$.*

Par exemple, si X est un singleton, l'anneau des polynômes à une indéterminée est une (la) réponse à ce problème.

II Groupes libres

1° Énoncé du problème universel

L'idée du "groupe le plus général" engendré par un ensemble se formalise de la façon suivante.

Problème *Etant donné un ensemble X, on cherche un groupe $F(X)$ et une application $i : X \to F(X)$ tels que pour tout groupe G et toute application $f : X \to G$, il existe un unique morphisme de groupes $\varphi : F(X) \to G$ qui "prolonge" f, i.e. tel que $f = \varphi \circ i$.*

Un tel couple $(F(X), i)$ formé d'un groupe $F(X)$ et d'une application $i : X \to F(X)$ (que l'on sous-entendra assez souvent), est appelé *groupe libre sur X*. Notons deux conséquences simples de la définition.

Lemme *Soit X un ensemble. S'il existe un groupe libre (F, i) sur X, alors il est unique à isomorphisme près, et l'application $i : X \to F(X)$ est injective.*

La première partie se démontre comme pour les espaces vectoriels. En effet, si (F, i) et (F', i') sont deux groupes libres sur X, soit $\varphi : F \to F'$ et $\varphi' : F' \to F$ les morphismes obtenus en utilisant la propriété universelle avec F et $f = i' : X \to F'$ d'une part, avec F et $f' = i : X \to F$ d'autre part. Alors, $\varphi' \circ \varphi$ et Id_F sont deux "prolongements" de i : $\varphi' \circ \varphi \circ i = i = \mathrm{Id}_F \circ i : X \to F$. Par unicité du morphisme dans la propriété universelle, on a : $\varphi' \circ \varphi = \mathrm{Id}_F$. De même, on a : $\varphi \circ \varphi' = i'$. Ainsi, φ et φ' sont des isomorphismes inverses l'un de l'autre.
Pour montrer le deuxième point, fixons $x_0 \in X$. Soit $f : X \to \{-1, 1\}$ l'application définie par : $f(x_0) = -1$, $f(x) = 1$ si $x \neq x_0$. Soit $\varphi : F(X) \to \{-1, 1\}$ le morphisme associé. Alors $\varphi \circ i(x_0) = f(x_0) = -1$ et $\varphi \circ i(x) = f(x) = 1$ si $x \neq x_0$. Par suite, $i(x_0) \neq i(x)$ dès que $x \neq x_0$. Ceci exprime que i est injective.

2° Mots

Idée *Admettons pour l'instant qu'il existe un groupe libre sur X. Comme i est injective, on identifie X et $i(X)$. Si un groupe contient les éléments $x \in X$, il contient aussi leurs inverses x^{-1}, $x \in X$, et les produits $x_1^{\pm 1} \cdots x_n^{\pm 1}$. On peut concaténer deux suites de symboles. En termes plus sophistiqués, on travaille avec le monoïde des mots, i.e. les suites finies à valeurs dans $X \cup X^{-1}$, pour la concaténation.*
L'étape suivante consiste à tenir compte des simplifications de la forme $xx^{-1} \to 1$. On va identifier deux mots si on peut passer de l'un à l'autre par des simplifications de cette forme (dans un sens ou dans l'autre). Le monoïde quotient ainsi construit est un groupe, et c'est en fait un groupe libre.

Pour chaque élément $x \in X$, on forme un nouveau symbole x^{-1}, ce qui donne un nouvel ensemble X^{-1} disjoint de X.[1]

[1] Si on veut formaliser à outrance, $X \cup X^{-1}$ est $X \times \{+, -\}$, où, pour $x \in X$, on identifie x à l'élément $(x, +) \in X \times \{+\}$ et on note x^{-1} l'élément $(x, -) \in X \times \{-\}$. Pour $x \in X$, on note aussi $(x^{-1})^{-1} = x$, d'où une involution $y \mapsto y^{-1}$ sur $X \cup X^{-1}$.

On note $W(X)$ l'ensemble des suites finies d'éléments de $X \cup X^{-1}$: ses éléments sont des n-listes $(a_1, \dots, a_n)$, avec $n \in \mathbb{N}$ et $a_1, \dots, a_n \in X \cup X^{-1}$. On appelle n la longueur d'une telle liste. Il y a exactement une suite de longueur 0, qu'on appelle suite vide, et qu'on note ε. On appelle généralement les éléments de $W(X)$ des mots sur l'alphabet $X \cup X^{-1}$ (d'où le W de *words*).

On définit le produit de concaténation de deux mot $u, v \in W(X)$. Si $v = \varepsilon$, on pose $u\varepsilon = \varepsilon u = u$, et si $u = (a_1, \dots, a_n)$ et $v = (b_1, \dots, b_p)$, on pose $uv = (a_1, \dots, a_n, b_1, \dots, b_p)$. La concaténation est manifestement associative, et ε et neutre : ainsi, $W(X)$ est un monoïde, appelé monoïde libre sur $X \cup X^{-1}$.

On dit qu'un mot $(a_1, \dots, a_n) \in W(X)$ est réduit si pour tout $i \in \{0, \dots, n-1\}$, $a_{i+1} \neq a_i^{-1}$. Le mot vide est réduit. On note $\mathrm{Red}(X)$ l'ensemble des mots réduits de $W(X)$. Le but de ce paragraphe est le résultat suivant.

Théorème *Soit X un ensemble. Il existe un groupe, unique à isomorphisme près, noté $F(X)$ ou $\langle X \rangle$, et une application $i : X \to F(X)$, tel que pour tout groupe G et toute application $f : X \to G$, il existe un unique morphisme $\varphi : F(X) \to G$ tel que $f = \varphi \circ i$.*
Ses éléments sont en bijection avec $\mathrm{Red}(X)$ et le produit dans $F(X)$ s'obtient par "concaténation et simplification". De plus, $i : X \to F(X)$ est injective et $i(X)$ engendre $F(X)$.

3° Construction de $F(X) = W(X)/\sim$

Etant donné $w, w' \in W(X)$, on dit que w et w' sont adjacents et on note[2] $w \asymp w'$ s'il existe $u, v \in W(X)$ et $a \in X \cup X^{-1}$ tels que

$$\begin{cases} w = uaa^{-1}v \\ w' = uv \end{cases} \quad \text{ou} \quad \begin{cases} w = uv \\ w' = uaa^{-1}v. \end{cases}$$

Par exemple, si $X = \{x, y\}$, on a : $x^{-1}xyy^{-1} \asymp yy^{-1}$ et $x^{-1}xyy^{-1} \asymp x^{-1}x$; en revanche, on n'a pas $x^{-1}x \asymp yy^{-1}$.
On considère la clôture transitive de cette relation symétrique. Plus concrètement, pour $w, w' \in W(X)$, on écrit $w \sim w'$ s'il existe des mots $w_1 = w$, w_2,..., $w_k = w' \in W(X)$ tels que

$$\forall i \in \{1, \dots, k-1\}, \quad w_i \asymp w_{i+1}.$$

Lemme (i) *La relation $\sim$ est une relation d'équivalence.*
(ii) *La relation $\asymp$ est compatible à la concaténation :*

$$\forall v, w, w' \in W(X), \quad w \asymp w' \implies vw \asymp vw' \text{ et } wv \asymp w'v.$$

(iii) *La relation $\sim$ est compatible à la concaténation :*

$$\forall v, v', w, w' \in W(X), \quad \begin{cases} v \sim v' \\ w \sim w' \end{cases} \implies vw \sim v'w'.$$

Le point (i) est laissé au lecteur. D'ailleurs, le point (ii), aussi. Pour le point (iii), on remarque que si $v = v_1 \asymp v_2 \asymp \cdots \asymp v_k = v'$ et $w = w_1 \asymp \cdots \asymp w_\ell = w'$, on a : $vw = v_1w_1 \asymp v_2w_1 \asymp \cdots \asymp v_kw_1 \asymp v_kw_2 \cdots \asymp v_kw_\ell = v'w'$.

Proposition *Soit X un ensemble.*
(i) *Soit $F(X) = W(X)/\sim$ le quotient de $W(X)$ par la relation d'équivalence $\sim$. La concaténation sur $W(X)$ induit une loi de groupe sur $F(X)$.*
(ii) *Le groupe $F(X)$ est un groupe libre sur X.*

[2]Notation prise dans [Mérindol]. La notation de [Calais] est : $w\mathcal{A}w'$.

(i) D'après le point (iii) du lemme précédent, on peut définir une loi sur $F(X)$, naturellement associative et munie d'un neutre (la classe du mot vide). Or il est clair que pour $w = a_1 \cdots a_n \in W(X)$, on a : $a_n^{-1} \cdots a_1^{-1} a_1 \cdots a_n \sim \varepsilon$, ce qui montre que (la classe de) $a_n^{-1} \cdots a_1^{-1}$ est un inverse de (la classe de) w dans $F(X)$.
(ii) Soit G un groupe et $f : X \to G$ une application. On définit un morphisme de monoïdes $\varphi_0 : W(X) \to G$ par : $\varphi_0(\varepsilon) = 1$ (le neutre de G) et, pour $(x_1, \ldots, x_n) \in X^n$ et $(\varepsilon_1, \ldots, \varepsilon_n) \in \{-1, 1\}^n$: $\varphi_0(x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n}) = f(x_1)^{\varepsilon_1} \cdots f(x_n)^{\varepsilon_n}$.
Il est immédiat que si $w, w' \in W(X)$ sont deux mots adjacents, alors $\varphi_0(w) = \varphi_0(w')$. Il en résulte que si $w \sim w'$, on a encore : $\varphi_0(w) = \varphi_0(w')$. Par suite, φ_0 passe au quotient par $\sim$ et induit une application $\varphi : F(X) \to G$. Cette application est bien le morphisme cherché dans le problème universel.

4° Description de $F(X)$ par les mots réduits

Un tour de magie ! C'est ce qui vous attend dans ce petit paragraphe, inspiré de Jacobson. Rappelons que $\mathrm{Red}(X)$ désigne les mots réduits de X, c'est une partie de $W(X)$.

Proposition *L'application naturelle* $\mathrm{Red}(X) \to F(X)$*, restriction de la projection naturelle* $W(X) \to F(X) = W(X)/\!\sim$*, est une bijection.*

En simplifiant petit à petit une écriture quelconque d'un élément de $F(X)$, on se convainc que l'application est surjective. La magie, c'est pour l'injectivité.
Pour $a \in X \cup X^{-1}$, on note

$$\begin{array}{rccl} T_a : & \mathrm{Red}(X) & \longrightarrow & \mathrm{Red}(X) \\ & a_1 \cdots a_n & \longmapsto & \left\{ \begin{array}{ll} a a_1 \cdots a_n & \text{si } a_1 \neq a^{-1}, \\ a_2 \cdots a_n & \text{si } a_1 = a^{-1}. \end{array} \right. \end{array}$$

C'est bien une application de $\mathrm{Red}(X)$ dans lui-même, et on a sans peine : $T_a^{-1} = T_{a^{-1}}$. On peut donc prolonger l'application $f : x \mapsto T_x$, de X vers le groupe $\mathfrak{S}_{\mathrm{Red}(X)}$ des bijections de $\mathrm{Red}(X)$ dans lui-même, en un morphisme $\varphi : F(X) \to \mathfrak{S}_{\mathrm{Red}(X)}$. Supposons qu'un élément $g \in F(X)$ ait deux écritures réduites, i.e. qu'il existe deux suites $(a_1, \ldots, a_m), (b_1, \ldots, b_n) \in \mathrm{Red}(X)$ telles que $a_1 \ldots a_m = g = b_1 \ldots b_n$. Alors, comme $\varphi(g) = \varphi(a_1) \cdots \varphi(a_m) = T_{a_1} \cdots T_{a_m}$, on a :

$$a_1 \cdots a_m = T_{a_1} \cdots T_{a_m}(\varepsilon) = \varphi(g)(\varepsilon) = T_{b_1} \cdots T_{b_n}(\varepsilon) = b_1 \cdots b_n \in \mathrm{Red}(X).$$

Ceci prouve l'injectivité !

5° Groupes libres dans "la vraie vie"

(a) Deux homographies

Référence : premier chapitre du livre d'Alessandri, *Groupes en situation géométrique.*
Rappelons que $SL_2(\mathbb{Z})$ est le groupe des matrices 2×2 à coefficients entiers de déterminant 1. Il opère sur la sphère de Riemann $\mathbb{P}^1(\mathbb{C})$ par homographies : à une matrice $A \in SL_2(\mathbb{Z})$ on associe l'homographie h_A définie, avec les conventions usuelles sur ∞, par :

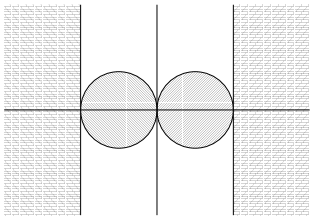
$$\forall z \in \mathbb{P}^1 = \mathbb{C} \cup \{\infty\}, \quad h_A(z) = \frac{az + b}{cz + d}, \qquad \text{lorsque } A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

.
Si Γ est le groupe des homographies, l'action est un morphisme $SL_2(\mathbb{Z}) \to \Gamma$. Son noyau est $\{\pm \mathrm{Id}\} \subset SL_2(\mathbb{Z})$, et $PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm \mathrm{Id}\}$.

Proposition *Le groupe engendré dans* $PSL_2(\mathbb{Z})$ *par les classes de*

$$U = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix} \quad \textit{et} \quad V = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}$$

est (isomorphe au groupe) libre (sur deux générateurs).



Notons $u = h_U : z \mapsto z+2$ et $v = h_V : z \mapsto z/(2z+1)$. Notons

$$D_u = \{z \in \mathbb{C},\ \mathrm{Re}\, z \geq 2\} \cup \{\infty\}, \quad D_{u^{-1}} = \{z \in \mathbb{C},\ \mathrm{Re}\, z \leq -2\} \cup \{\infty\}.$$

On a immédiatement : $u(\mathbb{P}^1 \setminus D_{u^{-1}}) \subset D_u$ et $u(\mathbb{P}^1 \setminus D_u) \subset D_{u^{-1}}$.
Si on note $i : z \mapsto 1/z$, on a : $v = i \circ u \circ i^{-1}$. Posons alors $D_v = i(D_u)$ et $D_{v^{-1}} = i(D_v)$. (Il est facile de voir que $D_{v^{\pm 1}}$ est le disque de centre $\pm 1/2$ et de rayon $1/2$.) On a donc : $v(\mathbb{P}^1 \setminus D_{v^{-1}}) \subset D_v$ et $v(\mathbb{P}^1 \setminus D_v) \subset D_{v^{-1}}$.
Par suite, si E désigne le complémentaire des quatre disques $D_u \cup D_{u^{-1}} \cup D_v \cup D_{v^{-1}}$, on constate qu'un mot réduit sur $X = \{u, v\}$, quand on l'interprète comme une homographie, envoie E dans l'un des quatre disques. En d'autres termes, un tel mot réduit n'est jamais l'identité, ou encore : l'application $\mathrm{Red}(X) \to F(X) \to \Gamma$ est injective. Comme elle est une surjection sur $\langle u, v\rangle$, ce dernier groupe est isomorphe au groupe libre.

Exercice. Montrer que le groupe engendré par U et V est le noyau de la projection $\pi : SL_2(\mathbb{Z}) \to SL_2(\mathbb{Z}/2\mathbb{Z})$. En déduire l'indice de $\langle U, V\rangle$ dans $SL_2(\mathbb{Z})$. (Indication : pour montrer qu'une matrice $A \in \mathrm{Ker}\, \pi$ comme ci-dessus est dans $\langle U, V\rangle$, procéder par récurrence sur $|a|+|c|$.)
(b) Paradoxe de Banach-Tarski Référence : Marc Guinot, *Le paradoxe de Banach-Tarski*, éditions Aléas ou la deuxième épreuve du CAPES 2004.

Théorème *La sphère unité de $\mathbb{R}^3$ est équidécomposable.*

Le sens de l'assertion est le suivant : il existe une *partition* de la sphère S^2 en un nombre fini de parties

$$S^2 = A_1 \cup \cdots \cup A_p \cup B_1 \cup \cdots B_q$$

et des parties $A'_1, \ldots, A'_p$ et $B'_1, \ldots, B'_q$ *isométriques* aux précédentes (c'est-à-dire qu'il existe des isométries φ_i et ψ_j telles que $A'_i = \varphi_i(A_i)$ $B'_j = \psi_j(B_j)$) telles que

$$S^2 = A'_1 \cup \cdots \cup A'_p \quad \text{et} \quad S^2 = B'_1 \cup \cdots B'_q$$

L'idée de la preuve consiste à

1. exhiber un sous-groupe libre à deux générateurs $F(2) = \langle A, B\rangle$ dans $\mathrm{SO}_3(\mathbb{R})$,
2. équidécomposer ce groupe libre $F(2)$,
3. appliquer à la sphère.

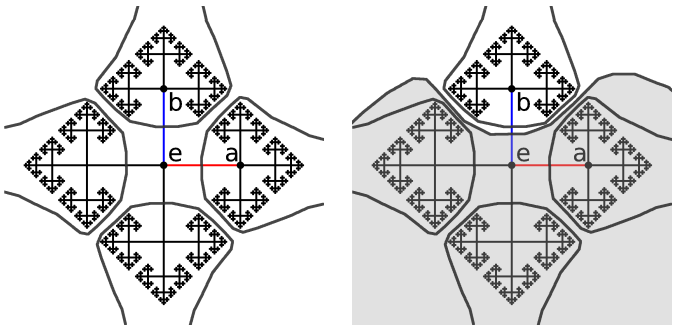
Pour le premier point, on utilise les deux matrices du CAPES 2004 :

$$A = \begin{pmatrix} 3/5 & -4/5 & 0 \\ 4/5 & 3/5 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \qquad B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 3/5 & -4/5 \\ 0 & 4/5 & 3/5 \end{pmatrix}.$$

Il s'agit de montrer que pour tous les entiers $n_1, p_1, \ldots, n_r, p_r$ avec $r \geq 1$ et $n_1 + p_1 > 0$, on a : $A^{n_1} B^{p_1} \cdots A^{n_r} B^{n_r} \neq \mathrm{Id}$.
Une deuxième méthode plus radicale consiste à montrer que l'ensemble des couples $(A, B) \in \mathrm{SO}_3 \times \mathrm{SO}_3$ qui n'engendrent pas un groupe libre est de mesure nulle dans $\mathrm{SO}_3 \times \mathrm{SO}_3$.

Le point-clé est le deuxième. Pour $x \in \{A^{\pm 1}, B^{\pm 1}\}$, on note $S(x)$ les éléments de $\langle A, B\rangle$ dont l'écriture réduite commence par x.
On a les décompositions suivantes, illustrées par les figures ci-dessous (où a= A et b= B, e= e est le neutre) :

$$\begin{aligned}\langle A,B\rangle &= \{e\} \cup \underbrace{S(A)\cup S(A^{-1})}_{\clubsuit} \cup \underbrace{S(B)\cup S(B^{-1})}_{\heartsuit}\\ \langle A,B\rangle &= \underbrace{S(A)\cup AS(A^{-1})}_{\clubsuit} = \underbrace{S(B)\cup BS(B^{-1})}_{\heartsuit}.\end{aligned}$$



Sur la première figure, les lobes représentent (dans le sens trigonométrique en partant du haut) $S(B)$, $S(A^{-1})$, $S(B)$, $S(A)$. La deuxième figure montre, en grisé, la partie $BS(B^{-1})$.
Négligeons la partie $\{e\}$: on a décomposé le groupe libre en quatre parties qui, à translation près, se recomposent en deux copies du groupe libre.
Pour le troisième point, voir les références.

III Groupes présentés par générateurs et relations

1° Relations

On veut dire ce qu'est une relation entre des éléments d'une partie X d'un groupe. Prenons une relation typique (penser à une réflexion a et à une rotation b) : $aba^{-1} = b^{-1}$. Comme on travaille dans des groupes, on peut récrire une relation équivalente à celle-ci en regroupant tout dans le même membre, par exemple : $aba^{-1}b = 1$. Et bien sûr, on peut oublier "$= 1$" pour ne retenir que $aba^{-1}b$. Ainsi, une relation entre les éléments de X, c'est un élément de $W(X)$. Quitte à faire des simplifications, on ne perd rien à supposer ces éléments réduits. Finalement, une relation sur X n'est autre qu'un élément de $\mathrm{Red}(X)$.

2° Générateurs et relations

Etant donné un ensemble de générateurs X et un ensemble de relations, c'est-à-dire une partie $\mathcal{R} \subset W(X)$, on définit le groupe présenté par générateurs X et relations $\mathcal{R}$ comme[3]

$$\langle X|\mathcal{R}\rangle = F(X)/\langle\langle \mathcal{R}\rangle\rangle,$$

où $F(X)$ est le groupe libre sur X défini précédemment, et $\langle\langle \mathcal{R}\rangle\rangle$ est le sous-groupe normal engendré par $\mathcal{R}$, i.e. l'intersection des sous-groupes normaux de $F(X)$ qui contiennent $\mathcal{R}$.
Il existe une application naturelle $\kappa : X \to \langle X|\mathcal{R}\rangle$, composée de $\iota : X \to F(X)$ et de la projection naturelle $F(X) \to F(X)\langle\langle \mathcal{R}\rangle\rangle$.
On a bien défini "le groupe le plus général engendré par X, satisfaisant les relations $\mathcal{R}$" en vertu de la proposition suivante :

[3]La notation $\langle X|\mathcal{R}\rangle$ est (seulement) presque standard.

Lemme *On fixe X un ensemble, $\mathcal{R} \subset F(X)$. Etant donné un groupe G et une application $\psi : X \to G$ telle que pour tout $r \in \mathcal{R}$, $r = (a_1, \dots, a_n)$, on ait*

$$\psi(a_1) \cdots \psi(a_n) = 1 \in G,$$

il existe un unique morphisme $\Psi : \langle X|\mathcal{R}\rangle \to G$ tel que $\Psi \circ \kappa = \psi$.
En particulier, si G est engendré par $\psi(X)$, alors G est isomorphe à un quotient de $\langle X|\mathcal{R}\rangle$.

Démonstration. Evident ! Pour l'unicité, remarquer que, pour $u = (a_1, \dots, a_n) \in \langle X|\mathcal{R}\rangle$:

$$\Psi\Big((a_1, \dots, a_n)\Big) = \Psi\Big((a_1) \cdots (a_n)\Big) = \Psi\Big((a_1)\Big) \cdots \Psi\Big((a_n)\Big) = \psi(a_1) \cdots \psi(a_n).$$

Quant à l'existence de Ψ, on considère le morphisme $\Phi : F(X) \to G$ tel que $\Phi \circ \iota = \psi$. Comme, par hypothèse et par construction de Φ, les éléments de $\mathcal{R}$ sont dans le noyau, Φ "passe au quotient", i.e. induit un morphisme $\Psi : F(X)/\langle\mathcal{R}\rangle \to G$, qui satisfait la propriété requise.□

Remarque. La proposition montre comment construire très facilement des morphismes d'un groupe présenté par générateurs et relations vers un autre groupe : choisir l'image des générateurs, et vérifier que les relations sont satisfaites. Cela dit, il est difficile en général de décrire un tel groupe. Par exemple, on montre qu'il n'est (même) pas possible de programmer un ordinateur qui prend en entrée une présentation (c'est-à-dire un alphabet X et une partie $\mathcal{R} \subset W(X)$) qui détermine si le groupe correspondant $\langle X|\mathcal{R}\rangle$ est isomorphe au groupe trivial ou pas.

3° Le groupe diédral

(a) Deux présentations

On fixe $n \in \mathbb{N}^*$ et on considère le groupe D_n défini par générateurs $\{a, b\}$ et relations

$$a^2 = b^2 = (ab)^n = 1.$$

Introduisons aussi le groupe D'_n présenté par générateurs $\{a, c\}$ et relations

$$a^2 = c^n = 1, \quad aca = c^{-1}.$$

Montrons que ces deux présentations définissent le même groupe. Les éléments $a' = a$ et $c' = ab$ de D_n satisfont les relations de D'_n :

$$a'^2 = 1, \quad c'^n = (ab)^n = 1, \quad a'c'a' = a(ab)a = ba = c'^{-1}.$$

Ainsi, il existe un unique morphisme $\psi : D'_n \to D_n$, tel que $\psi(a) = a$ et $\psi(c) = ab$. On définit de façon analogue un morphisme $\varphi : D_n \to D'_n$ en posant : $\varphi(a) = a$, $\varphi(b) = ac$. Ces deux morphismes sont des isomorphismes réciproques, d'où : $D_n \simeq D'_n$. Désormais, on identifiera ces deux groupes, via la relation : $c = ab$.

(b) Forme normale et majoration du cardinal

Lemme *Tout élément de D_n peut s'écrire sous la forme ac^k ou c^k pour $k \in \{0, \dots, n-1\}$ convenable.*

Démonstration. On a dans D_n : $a^{-1}ca = c^{-1}$, d'où $a^{-1}c^k a = c^{-k}$, puis $c^k a = ac^{-k}$ pour tout $k \in \mathbb{Z}$. Par suite, $D = \{ac^k : k \in \mathbb{Z}\} \cup \{c^k : k \in \mathbb{Z}\}$ est stable par produit et inverse :

$$\forall k, \ell \in \mathbb{Z}, \quad (a)c^k\, c^\ell = (a)c^{k+\ell}, \quad c^k ac^\ell = ac^{-k+\ell}, \quad ac^k\, ac^\ell = c^{-k+\ell}, \quad (ac^k)^{-1} = ac^k.$$

Ainsi, D est un sous-groupe de D_n. Comme D contient a et c, c'est que $D = D_n$.□

Il résultera de la suite qu'une telle écriture est unique, d'où le terme de forme normale. Cependant, c'est sans doute faisable, mais pas trivial, de montrer directement que ces $2n$ éléments sont distincts. On peut quand même dire :

Corollaire *Le cardinal de D_n est au plus $2n$.*

(c) Réalisation géométrique et minoration du cardinal

Dans un plan vectoriel euclidien, on fixe une rotation ρ d'ordre n et une réflexion σ. On vérifie sans peine que $\sigma^2 = \rho^n = 1$ et $\sigma\rho\sigma = \rho^{-1}$, d'où l'existence d'un morphisme de D_n vers le groupe engendré par σ et ρ dans le groupe des isométries du plan.
Pour $k = 0, \dots, n-1$, $\rho^k \sigma \rho^{-k}$ est la réflexion d'axe $\rho^k(\Delta)$, où $\Delta = \mathrm{Ker}(\sigma - \mathrm{Id})$. On obtient ainsi n éléments distincts, distincts aussi des n éléments $\rho, \rho^2, \dots, \rho^n$. Par suite, le groupe engendré par σ et ρ contient au moins $2n$ éléments.

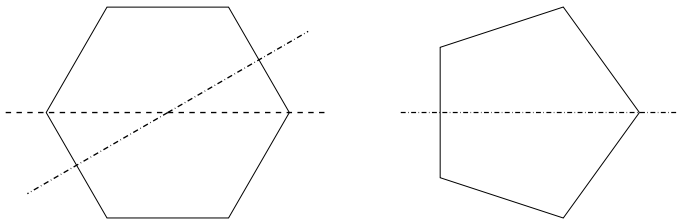
Corollaire *Le cardinal de D_n est au moins $2n$.*

Remarque. Fixons un point de l'axe de σ, distinct de l'origine. Son orbite sous le groupe engendré par σ et ρ est un polygone régulier à n côtés.

(d) Application : morphismes $D_n \to \mathbb{C}^*$

On veut déterminer tous les morphismes $D_n \to \mathbb{C}^*$. Si φ en est un, il est déterminé par $\varphi(a)$ et $\varphi(b)$, et on a nécessairement : $\varphi(a)^2 = \varphi(b)^2 = 1$. Il y a donc au plus 4 morphismes.
En vertu du lemme de **??**2°, et en utilisant la première présentation de D_n, on définit bien un morphisme en posant $\varphi(a) = \varphi(b) = \varepsilon$ pour $\varepsilon \in \{-1, 1\}$. En effet, on a alors : $\varphi(a)^2 = \varphi(b)^2 = (\varphi(a)\varphi(b))^n = 1$. Dans la réalisation géométrique de D_n, les morphismes sont le morphisme trivial et le déterminant.
Voyons si on peut prendre $\varphi(a) = -\varphi(b)$. La seule relation à vérifier est : $(\varphi(a)\varphi(b))^n = 1$, ce qui donne $(-1)^n = 1$: c'est possible si et seulement si n est pair.
Ainsi, pour n pair, il existe exactement quatre morphismes $\varphi : D_n \to \mathbb{C}^*$, caractérisés par des valeurs arbitraires de $\varphi(a)$ et de $\varphi(b)$ dans $\{-1, 1\}$. Pour n impair, il n'y en a que deux, caractérisés par une valeur arbitraire de $\varphi(a) = \varphi(b)$ dans $\{-1, 1\}$.

Interprétations de la différence pair/impair. Sur un dessin, on voit qu'il y a deux "types" de réflexions si n est pair, mais un seul "type" si n est impair.



Plus formellement, on constate que si n est impair, alors a et b sont conjugués, si bien que tout morphismes vers un groupe abélien prend la même valeur en a et b :

$$\underbrace{ab\cdots ab}_{n-1 \text{ lettres}}\ a\ \underbrace{ba\cdots ba}_{n-1 \text{ lettres}}\ b = (ab)^n = 1 \quad \Longrightarrow \quad (ab)^{n-1}\, a\, (ab)^{-n+1} = b.$$

En revanche, si n est pair, a et b ne sont pas conjugués, donc la contrainte $\varphi(a) = \varphi(b)$ semble pouvoir tomber –et on a constaté que c'est bien le cas. En effet, dans la réalisation géométrique, on constate que l'axe de $b = \sigma\rho$ ne contient aucun sommet du polygone régulier introduit ci-dessus, au contraire de l'axe de $a = \sigma$.

4° Plus délicat : présentation de Coxeter de $\mathfrak{S}_n$

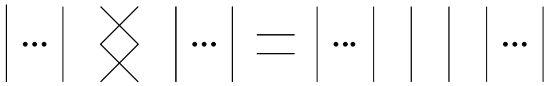
Proposition *Pour $n \geq 2$, le groupe symétrique $\mathfrak{S}_n$ est présenté par générateurs $s_1, \dots, s_{n-1}$ et relations*

$$\begin{cases} \forall i = 1, \dots, n-1, & s_i^2 = 1 \\ \forall i = 1, \dots, n-1, & s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}, \\ \forall i, j = 1, \dots, n-1,\ |i-j| \geq 2, & s_i s_j = s_j s_i. \end{cases}$$

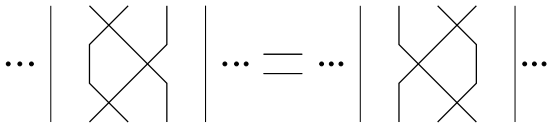
Réf. : J.-Y. Mérindol, *Nombres et algèbre*, EDP Sciences, 2006.

Preuve : Soit G_n le groupe présenté par les générateurs et relations de la proposition. On montre que les éléments $(i, i+1)$ de $\mathfrak{S}_n$ satisfont les relations de G_n. Il est d'ailleurs intéressant de le faire graphiquement :

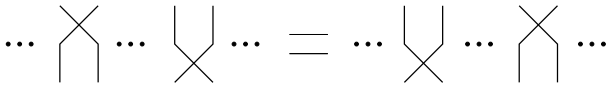
$s_i^2 = 1$



$s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}$



$s_i s_j = s_j s_i$



Ceci prouve (seulement) que $\mathfrak{S}_n$ est un quotient du groupe cherché. Comme pour le groupe diédral, on majore le cardinal de notre groupe en utilisant une "forme normale". Voici la clé :

Lemme *Tout élément $w \in G_n$ peut s'écrire sous la forme :*

$$w = \underbrace{s_{i_{n-1}} s_{i_{n-1}+1} \cdots s_{n-2} s_{n-1}}\ \underbrace{s_{i_{n-2}} s_{i_{n-2}+1} \cdots s_{n-3} s_{n-2}}\ \cdots \underbrace{s_{i_k} s_{i_k+1} \cdots s_{k-1} s_k}\ \cdots$$

où $1 \leq i_k \leq k+1$ pour $k = 1, \ldots, n-1$, avec la convention que si $i_k = k+1$, on n'écrit pas le "paquet" correspondant.

Sens du lemme : Tout élément s'obtient en supprimant les premières lettres de chaque paquet à partir de la décomposition suivante de l'élément le plus long :

$$w_0 = \underbrace{s_1 s_2 \cdots s_{n-2} s_{n-1}}\ \underbrace{s_1 s_2 \cdots s_{n-3} s_{n-2}}\ \cdots\ \underbrace{s_1 s_2 s_3}\ \underbrace{s_1 s_2}\ \underbrace{s_1}\ .$$

Preuve du lemme. On procède par récurrence sur n (trivial pour $n \leq 2$). On suppose l'assertion vraie pour le groupe G_n engendré par $s_1, \ldots, s_{n-1}$, et on la prouve pour G_{n+1}.
Premier pas : Tout élément $w \in G_{n+1}$ peut s'écrire avec au plus une occurrence de s_n.
En effet, considérons une écriture de w comme produit des s_i $(i = 1, \ldots, n)$ contenant un nombre minimal d'occurrences de s_n, et supposons qu'il y en ait au moins deux. Il existe donc w' dans le groupe engendré par $s_1, \ldots, s_{n-1}$ et $x, y \in G_n$ tels que

$$w = x\ s_n\ w'\ s_n\ y.$$

Par hypothèse de récurrence, w' s'écrit sous la forme $s_i s_{i+1} \cdots s_{n-1} w''$, avec $i \leq n-1$, ou alors $w = w''$, où w'' est un produit des éléments $s_1, \ldots, s_{n-2}$: w'' commute à s_n. Dans le premier cas, on a :

$$w = x s_n s_i s_{i+1} \cdots s_{n-1} w'' s_n y = x s_i s_{i+1} \cdots s_{n-2} s_n s_{n-1} s_n y = x s_i s_{i+1} \cdots s_{n-2} s_{n-1} s_n s_{n-1} y.$$

Dans le deuxième cas :

$$w = x s_n w'' s_n y = x w'' s_n^2 y = x w'' y.$$

Dans les deux cas, l'écriture obtenue contredit la minimalité du nombre d'occurrences de s_n dans l'écriture initiale, ce qui prouve le premier pas.

Deuxième pas : On prouve le lemme.
Soit $w \in G_n$. Si w peut s'écrire sans s_n, l'hypothèse de récurrence s'applique et donne une écriture de w qui convient. Sinon, d'après le premier pas, w peut s'écrire sous la forme

$$w = x s_n y,$$

où x et y sont des produits de $s_1, \ldots, s_{n-1}$. Par hypothèse de récurrence, x s'écrit $s_i s_{i+1} \cdots s_{n-1} z$ ou $x = z$, où z est un produit de $s_1, \ldots, s_{n-2}$, i.e. z commute à s_n. Dans le premier cas, on a :

$$x = s_i s_{i+1} \cdots s_{n-1} s_n \; zy,$$

et dans le deuxième cas :

$$x = zy.$$

Dans chaque cas, l'hypothèse de récurrence appliquée à zy permet de conclure.□

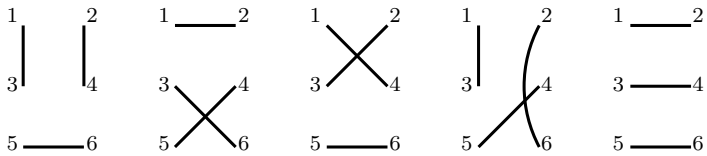
Fin de la preuve de la proposition. D'après le lemme, le cardinal du groupe G_n est au plus $n \times (n-1) \times \cdots \times 2 = n!$. Or, on a mis en évidence une surjection $G_n \to \mathfrak{S}_n$, et le cardinal de $\mathfrak{S}_n$ est $n!$. Il en résulte que notre surjection est un isomorphisme, et, de plus, que l'écriture dans le lemme est *unique*.□

5° Application : automorphisme extérieur de $\mathfrak{S}_6$

On utilise la présentation précédente pour exhiber un automorphisme extérieur de $\mathfrak{S}_6$. Dans ce qui précède (i.e. dans le livre de Perrin...), on a vu qu'un automorphisme qui envoie les transpositions sur des transpositions est intérieur. (Exercice : le reprouver en utilisant la présentation précédente.) Or, les transpositions de $\mathfrak{S}_n$ sont l'unique classe de conjugaison de leur cardinal, sauf pour $n = 6$, où les produits de trois transpositions constituent une classe de conjugaison de même cardinal. Le miracle numérique, ici, c'est que :

$$\binom{6}{2} = 15 = \frac{1}{3!}\binom{6}{2}\binom{4}{2}\binom{2}{2}.$$

Calculons avec les triples transpositions : si deux triples transpositions ont une transposition en commun (par exemple, (12)(34)(56) et (13)(24)(56)), alors elles commutent : en effet, la transposition commune est élevée au carré, et le reste du calcul se passe dans le groupe de Klein (les doubles transpositions dans $\mathfrak{S}_4$), qui est abélien. Si ce n'est pas le cas, alors elles satisfont une relation de tresse de la forme $sts = tst$. (On n'a pas besoin de le démontrer en général, il suffira de le vérifier pour les éléments qu'on exhibera ci-dessous.)
Pour trouver un automorphisme de $\mathfrak{S}_6$, il suffit de définir l'image des cinq générateurs (12), (23),..., (56). Il suffit donc de trouver cinq triples transpositions telles que deux consécutives n'aient pas de transposition commune et deux non consécutives en aient un. Voici une façon de procéder :



En d'autres termes, les triples transpositions

$$t_1 = (13)(24)(56),\ t_2 = (12)(36)(45),\ t_3 = (14)(23)(56),\ t_4 = (13)(26)(45),\ t_5 = (12)(34)(56)$$

satisfont les mêmes relations que $s_1 = (12), \ldots, s_5 = (56)$. Finalement, l'application $s_i \mapsto t_i$ ($i = 1, \ldots, 5$) s'étend en un automorphisme de $\mathfrak{S}_6$, qui est extérieur puisque l'image d'une transposition n'est pas une transposition.

Réf. : Sans doute inexistante sous cette forme.