Application de l'algorithme de Todd-Coxeter dans le calcul de la théorie des groupes

Moumouni **DJASSIB0 WOBA**
moumouniabdoulwoba@gmail.com
Université de Ouahigouya
(BURKINA FASO)

Résumé
Dans cet article, nous avons décrit l'algorithme de Todd-Coxeter. En effet, l'algorithme de Todd-Coxeter est un outil mathématique utilisé dans le domaine de la théorie des groupes. Il permet de déterminer différentes présentations possibles d'un groupe, c'est-à-dire différentes façons d'exprimer ses éléments et ses opérations. Nous avons par ailleurs appliqué cet algorithme sur un sous-groupe engendré H par G ; où on a obtenu une table du sous- groupe, trois tables de relateurs dont : Table du relateur aaaa ; Table du relateur abab ; Table du relateur bbb et une table de multiplication aa'bb'. Une fois l'algorithme terminé, l'unité de H dans G est 6. On a obtenu explicitement un homomorphisme de G dans le groupe des permutations de H/G qui est isomorphe à $\mathbb{G}_6$; où nous avons remarqué qu'il est injectif : en effet un élément du noyau appartient à l'intersection des xHx^{-1} pour $x \in G$, en particulier, il appartient à H ; d'autre part, l'image de H dans $\mathbb{G}_6$ est d'ordre 4, donc le noyau est réduit à l'élément neutre.
Mots clés *: Algorithme de Todd-Coxeter, Sous-groupe, Semi-direct, Groupe opérant, Homomorphisme.*

Application of the Todd-Coxeter algorithm in the calculation of group theory

Summary
In this article, we describe the Todd-Coxeter algorithm. The Todd-Coxeter algorithm is a mathematical tool used in the field of group theory. It allows us to determine different possible presentations of a group, i.e. different ways of expressing its elements and operations. We have applied this algorithm to a subgroup generated H by G, where we obtained a subgroup table and three relator tables, including : Relator table aaaa; Relator table abab; Relator table bbb and a multiplication table aa'bb'. Once the algorithm is completed, the unit of H in G is 6. We explicitly obtained a homomorphism of G in the group of permutations of H/G which is isomorphic to G_6; where we noticed that it is injective: indeed an element of the kernel belongs to the intersection of xHx^(-1) for x∈G, in particular, it belongs to H; on the other hand, the image of H in G_6 is of order 4, so the kernel is reduced to the neutral element.
Keywords*: Todd-Coxeter algorithm, Subgroup, Semi-direct, Operating group, Homomorphism.*

Introduction

Le concept de groupe fit son apparition dans l'étude des équations polynomiales. En effet, c'est Evariste Galois qui, durant les années 1830, utilisa pour la première fois le terme « groupe » dans un sens technique similaire à ce qui est utilisé de nos jours, faisant de lui un des fondateurs de la théorie des groupes. A la suite de contributions d'autres domaines des mathématiques, comme la théorie des nombres et la géométrie, la notion de groupe fut généralisée et plus fermement établie autour des années 1870. La théorie des groupes moderne, une branche des mathématiques toujours active, se concentre donc sur la structure de groupes abstraits, indépendamment de leur utilisation extra-mathématique. Ce faisant, les mathématiciens ont défini, au fil des années, plusieurs notions permettant de fragmenter des groupes en des objets plus petits et plus compréhensibles, les sous-groupes, groupes quotient, sous-groupes normaux et les groupes simples en sont quelques exemples**.** En plus d'étudier ces types de structures, les théoriciens de groupes s'intéressent aussi aux déférentes façons dont un groupe peut être exprimé concrètement, autant du point de vue de la théorie des représentations que du point de computationnel. La théorie des groupes finis fut développée avec, comme point culminant, la classification de groupes finis, achevée en 2004. Depuis le milieu des années 1980, la théorie géométrique des groupes, qui s'intéresse aux groupes de type fini en tant qu'objets géométriques, est devenue un champ particulièrement actif de la théorie des groupes. Cet article nous permettra de « réviser » quelques notions théoriques sur les groupes. Nous y manipulerons les groupes de permutations et les groupes définis par générateurs et relations. Il faut dire ici que d'autres logiciels comme par exemple GAP sont beaucoup plus adaptés aux calculs en théorie des groupes. Cependant, nous exploiterons l'algorithme de Todd-Coxeter pour le calcul de la théorie des groupes.

1. Sous-groupe distingué, Groupe quotient

Dans la suite, G est un groupe et H un sous-groupe de G. On appelle classe à droite (resp. à gauche) de G modulo H un sous-ensemble de G du type H_g

(resp. $_gH$) pour un g ϵ G. L'ensemble des classes à droite (resp. à gauche) est noté H\G (resp. G\H) et s'appelle l'ensemble quotient (à droite, resp. à gauche) de G par H. La surjection canonique G → H \G (resp. G\H) défini par g⟼H_g (resp. g⟼$_g$ H) est appelée projection canonique modulo H à droite (resp. à gauche).

H est dit distingué ou normal dans G si pour tout g ϵ G, on a $_{,g}\, H_{g^{-1}} \subset$H, ou encore si pour tout g ϵ G et pour h ϵ H,$_g\, h_{g^{-1}}$ ϵ H. Si H est distingué, on a gH = Hg et les classes à droite ont les mêmes que les classes à gauche.

Le sous-groupe H est distingué dans G si et seulement s'il existe une structure de groupe sur G/H telle que la projection canonique G→G\H soit un homomorphisme de groupe. La loi est alors unique et

G/H = H\G est appelé le groupe-quotient.

2. Groupe de permutations.

On note $\mathfrak{G}_n$ le groupe symétrique de degré n, c'est-à-dire le groupe des bijections de l'ensemble à n éléments {1,…,n} dans lui-même muni de la loi de composition. Une permutation de degré n est un élément de $\mathfrak{G}_n$. On appelle groupe de permutations (de degré n) un sous-groupe de $\mathfrak{G}_n$. Rappelons qu'il existe un unique homomorphisme de groupes $\mathfrak{G}_n$ → {±1}tel que l'image d'une transposition soit -1. C'est la signature. Le noyau est le groupe alterné $\mathfrak{U}_n$.

U_n r-cycle (ou cycle de longueur r) est noté $(a_1a_2.....a_r)$. C'est la permutation qui envoie a_1 sur a_2,.....,a_r sur a_1. L'ensemble $(a_1.....a_r)$ est appelé support du cycle $(a_1a_2.....a_r)$.

Le groupe $\mathfrak{G}_n$ est engendré par (1 2) et (1 2...n). Le groupe $\mathfrak{U}_n$ est engendré pour

n > 3 par (1 2 3) et (3....n) si n est impair et par (1 2 3) et (1 2)(3...n) si n est pair.
Le premier énoncé est classique. Pour le second, on rappelle que $\mathfrak{U}_n$ est engendré par les 3-cycles

- (1 2 i) pour i ϵ {3....n}. Si c = (1 2 3) et σ = (1 2) (3... n) ou σ = (3… n) selon la parité de n, on a $\sigma^i c\sigma^{-1}$ = (1 2 3 + i) ou (2 1 3 + i) = $(1\ 2\ 3 + i)^2$. On en déduit aisément la proposition précédente.

2.1. Groupe opérant sur un ensemble

Soit X un ensemble. Un groupe G opérant (à gauche) sur X est un groupe muni d'une application
G×X → X : (g, x) ↦ g. x vérifiant (gg'). x = g.(g'x) pour tout g, g' ϵ G et x ϵ X et e. x = x si e est un élément neutre de G. Il revient au même de se donner un homomorphisme de groupes G→S(X) où S(X) désigne le groupe des permutations de X.
On dit que G opère transitivement sur X si pour tous x et y ϵ X, il existe g ϵ G tel que g x = y. Il revient au même de dire que l'orbite de n'importe quel x ϵ X, c'est-à-dire l'ensemble des g. x pour g ϵ G, est égale à X. Si G est défini comme un groupe de permutations de degré n et que son action naturelle sur {1,....,n}est transitive, G est dit transitif.
On dit que G opère 2-transitivement sur X si pour tout (x, y) ϵ X×X avec $x \neq y$ et pour (x', y') ϵ X×X avec $x \neq y$, il existe g ϵ G tel que g x = x' et gy = y'. En particulier, G opère transitivement sur X et G opère 2-transitivement si et seulement si l'action diagonale de G sur X×X : g. (x, y) = (g. x, g. y) a exactement deux orbites : la diagonale de X×X et le complément. Un groupe de permutations de degré n opérant 2-transitivement sur {1,....,n}est dit 2-transitif.

2.2. Groupe opérant sur lui-même par conjugaison

Un groupe G opère sur lui-même par conjugaison : (g, x) ↦ g x g^{-1}. Deux éléments a et b ϵ G sont dits conjugués s'il existe g ϵ G tel que b = gag^{-1}. L'équation aux classes est la formule
card (G) = $\sum_i card(C_i)$
où C_i parcourt l'ensemble des classes de conjugaison. Il est facile de calculer les classes de conjugaison de $\mathfrak{G}_n$. Si σ est une permutation, on peut l'écrire de manière unique comme produit de cycles à support disjoints.
Deux éléments de $\mathfrak{G}_n$ sont conjugués si et seulement si leurs décompositions en cycles disjoints comportent pour tout i le même nombre de cycle de longueur i.
Un groupe G opère sur lui-même par translation (à gauche) : (g, x) ⟼ g. x. Si H est un sous-groupe de G, le groupe G opère aussi sur l'ensemble G/H par translations, ce qui permet de définir un homomorphisme de groupes ρ : G→S(G/H) par ρ(g)(C) = gC pour g ϵ G et C un élément de G/H. En particulier, une fois numérotées ces classes de 1 à n si n est l'indice de H dans G, on obtient un homomorphisme ρ' de G dans $\mathfrak{G}_n$. Remarquons que ρ'(G) est un groupe de permutations transitif de degré n, quotient de G.

2.3. Définition supplémentaires : sous-groupe dérivé, produit semi-direct

Soit G un groupe. On appelle commutateur un élément d G de la forme $xyx^{-1}y^{-1}$. On appelle groupe dérivé de G (et on note G'ou D(G)) le sous-groupe engendré par les commutateurs de G.
D(G) est un sous-groupe distingué de G. Le quotient G/D(G) est un groupe abélien et même le plus grand groupe-quotient abélien de G au sens suivant : notons π : G→G/D(G) ; si G_1 est un groupe abélien et f : G→G_1 un homomorphisme de groupes, il existe un unique homomorphisme $\overline{f}$:G/D(G)→G_1 tel que $\overline{f}$ ∘ π = f. Ainsi, l'ordre de G/D(G) est maximal parmi l'ordre des quotients de G

qui sont abéliens. On appelle suite dérivée d'un groupe G la suite $G_0 = G$, $G_1=D(G_0),....,G_k=D(G_{k-1}),..$

Le groupe dérivé de $\mathfrak{G}_n$ est $\mathfrak{U}_n$. Le groupe dérivé de $\mathfrak{U}_n$ est $\mathfrak{U}_n$ pour $n \geq 5$. Pour $n = 4$, demander plus tard à MAPLE ce qu'il en pense.

Soient H et K deux groupes et $T : K \rightarrow Aut(H)$ un homomorphisme de groupe (ici, Auto(H) est le groupe des homomorphismes bijectifs de H dans lui-même). On appelle produit semi-direct (abstrait) de H par K relativement à T l'ensemble $H\times K$ muni de la loi suivante

$(h, k) * (h',k')=(hT(k)(h'),kk')$.

Cette loi est une loi de groupe, notons G ce groupe. Lorsque T est l'homomorphisme trivial, on retrouve le produit direct. Il est facile de montrer que les ensembles $H' = H\times \{1\}$et $K' = \{1\} \times K$ sont les sous-groupes de G, que H' est distingué dans G et que $K'\cap H' = \{1\}$.

Soit G un groupe et soient H et K deux sous-groupes de G. On dit que G est le produit semi-droit de H par K si H est distingué dans G, si $G = HK$ et si $H \cap G = \{1\}$.

Sous les conditions précédentes, prenons $T : K \rightarrow Aut(H)$ donne par $k\longmapsto(h\longmapsto khk^{-1})$. Alors G est isomorphe au produit semi-direct (abstrait) de H par K relativement à T.

2.4. Groupes libres, groupes définis par générateurs et relations

Soit V un ensemble. Le monoïde libre de base V est l'ensemble note V*, des suites finies d'éléments de V. On notes ces suites en juxtaposant les éléments, par exemple la suite $(\upsilon_1,...,\upsilon_r)$ avec $\upsilon_i \in V$ est notée $\upsilon_1,...,\upsilon_r$. On appelle les éléments de V^* des chaînes d'éléments de V ou mots sur V.

Si $\upsilon = \upsilon_1,...,\upsilon_r \in V^*$, avec $\upsilon_i \in V$, la longueur de la chaîne υ est r. On note ρ l'application naturelle $V\rightarrow V^*$ qui à υ associe la chaîne de longueur 1 formée de υ. Si υ_1 et υ_2 sont des mots, le mot formé en

les juxtaposant est noté $\upsilon_1\upsilon_2$ et est appel concaténation de υ_1 et de υ_2.

La concaténation définit une loi de composition interne sur V^* qui est associative et admet un élément neutre ε qui est la chaîne vide.

Pour tout monoïde M et toute application f : V → M, il existe un unique morphisme de monoïde

$f^* : V^* \to M$ tel que $f = f^* \circ \rho$.

Remarquons que V^* est caractérisé par la propriété universelle qui précède à isomorphisme unique près. Soit V' une copie de V. Si υ un élément de V, on note υ' le même élément vu dans V'.

Soit $\overline{V} = V \sqcup V'$ la réunion disjointe de V et V'. Soit $\overline{V}^*$ le monoïde libre de base V'. Si $\alpha = \alpha_1 ... \alpha_r$, on pose $\alpha' = \alpha_r' ... \alpha_1'$.

Deux éléments de $\overline{V}^*$ sont dits équivalents s'il existe $n \in N$ et $\alpha_0, \alpha_1, ..., \alpha_n$ appartiennent à $\overline{V}^*$ tels que

$\alpha_0 = \alpha_1$, $\alpha_n = \beta$ et tels que si $0 \leq i < n$, α_i et α_{i+1} soient contigus. La relation ainsi définie est une relation d'équivalence. La parité de la longueur est conservée par cette relation.

Le groupe libre F(V) de base V est l'ensemble des classes d'équivalence de la relation d'équivalence précédente. On vérifie que la concaténation respecte la relation d'équivalence. Ce qui permet de définir une loi de composition interne sur F(V).

Muni de la concaténation, F(V) est un groupe. Pour $\alpha \in V$, l'inverse de (la classe) de α est

(La classe de) α_0. Pour cette raison, on note aussi $\alpha_0 = \alpha^{-1}$ pour $\alpha \in V$. On a encore une application

$\bar{\rho} : V \to F(V)$

Pour tout groupe G et toute application f : V → G, il existe un unique homomorphisme de groupe

$\bar{f}$: F(V)→G tel que $f = \bar{f} \circ \rho$. De nouveau, F(V) muni de l'application $\bar{\rho} : V \to F(V)$ est caractérisé à isomorphisme uniqueprès par la propriété universelle ci-dessus.

1. Si V est l'ensemble vide, le groupe libre de base V est le groupe trivial {1} ;

2. Si V ={α} est réduit à un élément, F(V) est isomorphe à ℤ. En effet, on commence à énumérer les éléments de F(V) en les « réduisant » : ce sont les α...α (n fois) = α^n et les α'...α' (n fois) = $\alpha'^n = \alpha^{-n}$ pour n ϵ ℕ. On remarque que ℤ vérifie la propriété universelle : si G est un groupe, une application
f :{α}→ G est déterminée par l'image b = f (α) ϵ G; il existe alors un unique homomorphisme de groupe de ℤ dans G donné par n → b^n. Par unicité de l'objet universel, on en déduit que F(V) est isomorphe à ℤ ;
3. Si V a deux éléments α et β, F(V) est très gros : il contient par exemple αb, αbα, $\alpha b\alpha^{-1}b$, $\alpha^5b^2\alpha b\alpha b\alpha b$, etc. qui sont tous distincts.
Soit un groupe et A une partie de G. On appelle sous-groupe distingué de G engendré par A l'intersection de tous les sous-groupes distingués de G contenant A. C'est aussi le plus petit sous-groupe distingué de G contenant A. Il est formé des produits finis d'éléments de A et de tous leurs conjugués par un élément de G.

Une présentation de groupe est un couple (X, R) où X est un ensemble et R une partie de F(X). On note G = ⟨X/R⟩ le quotient du groupe libre F(X) par le sous-groupe distingué de F(X) engendré par R. On dit que (X, R) est une présentation de G ou encore que c'est une définition de G par générateurs et relations. Les éléments de X sont appelés les générateurs, les éléments de R sont appelés les relateurs. Si r est un relateur, r =1 est appelé une relation. On note aussi ⟨X/R⟩ = ⟨X|ω = 1 pour ω ϵ R⟩.
Par exemple
$\langle x, y | x^2, y^2, xyx^{-1}y^{-1} \rangle$ ou $\langle x, y | x^2 = 1, y^2 = 1, xy = yx \rangle$, $\langle x, y | x^n, y^2, yxy^{-1}x \rangle$ ou $\langle x, y | x^n = 1, y^2 = 1, yxy^{-1} = x^{-1} \rangle$.
Pour tout groupe G et toute application f :X→G tel que $\bar{f}$(r) =1 pour r ϵ R, il existe un unique homomorphisme de groupe f' : ⟨X/R⟩→G tel que f =f'∘π∘$\bar{\rho}$ ou π est la projection de F(X) sur ⟨X/R⟩.
1. Si R est l'ensemble vide, le sous-groupe de F(X) engendré par R est réduit à 1. Donc ⟨H/R⟩ = F(X). 2. G = $\langle a/a^5 \rangle$ est isomorphe à

$\mathbb{Z}/5\mathbb{Z}$. En en effet, on a F({a}) = $a^{\mathbb{Z}}$, le sous-groupe distingué engendré par a^5 est $a^{5\mathbb{Z}}$.

3. G = $\langle a, b/a^3, b^2, aba^{-1}b^{-1}\rangle$ est isomorphe à $\mathbb{Z}/6\mathbb{Z}$. En effet, dans $\bar{X}^*$

ab~aba^{-1}a~$aba^{-1}b^{-1}$ba~ba. On énumère les éléments de G : on trouve 1, a, a^2, b, ba, ba^2. Donc |G| ≤ 6. D'autre part, le groupe $\mathbb{Z}/6\mathbb{Z}$ a deux générateurs x = 2 et y = 3 vérifiant (notation additive)

1 x = 0, 2 y = 0, $x + y - x - y$ = 0. On en en déduit par la propriété universelle qu'il existe un homomorphisme de groupe G→ $\mathbb{Z}/6\mathbb{Z}$ qui envoie a sur x = 2 et b sur y = 3. Il est surjectif. D'où

|G| ≥ 6. Donc |G| = 6 et G est isomorphe à Z/6Z.

4. Reconnaître les groupes $\langle x/x^n = 1\rangle, \langle x, y|x^2 = 1, y^2 = 1, xy = yx\rangle$

2.5. Familiarisation avec group

La bibliothèque group concerne deux types de groupes : les groupes de permutations de degré n, qui sont donnés par une liste de générateurs et l'entier n, et les groupes définis par les générateurs et relations. On remarquera tout de suite que certaines commandes sont utilisables pour les deux types de groupes comme cosets, cosrep, isnormal, d'autres uniquement avec un groupe de permutations comme areconjugate, center, centralizer, issubgroup d'autres enfin uniquement avec un groupe défini par générateurs et relations comme permrep, pres.

La commande pour définir un groupe de permutations est permgroup. Il est important de se familiariser avec les deux manières dont MAPLE représente une permutation σ. On peut se donner une permutation list, c'est-à-dire la liste [σ(1), ...σ(n)]. Ainsi, [1,3,4,5,2] désigne pour MAPLE la permutation $\begin{pmatrix}1 & 2 & 3 & 4 & 5\\ 1 & 3 & 4 & 5 & 2\end{pmatrix}$.

On peut aussi se donner la permutation σ comme la liste des cycles à support disjoint dont le produit est σ : [[1,2,3], [4,5]] désigne la

permutation (123)(45). On passe de l'un à l'autre par couvert (('*permlist*', n) et ouvert ('*disjcyc*').
Exemple :
> couvert ([1,3,4,5,2],'*disjcyc*') ;
> couvert ([[1,2,3], [4,5]],'*permlist*',5) ;
> couvert ([[1,2,3], [4,5]],'*permlist*',9) ;
Dans la deuxième commande, la permutation est vue comme un élément de $\mathfrak{G}_5$, dans la troisième comme un élément de $\mathfrak{G}_9$. Les opérations sur les permutations sont données par *invperm*, *mulperms*. Vérifier sur un exemple que MAPLE fait opérer à droite les permutations : $\sigma_2.\sigma_1 = \sigma_1 \circ \sigma_2$, en notant
σ (i) = i^{σ} (notation exponentielle), on a alors $i^{\sigma_1 \cdot \sigma_2} = (i^{\sigma_1})^{\sigma_2}$. Du coup, MAPLE calcule plutôt les classes à droites sur lesquelles G opère à droite. Certaines commandes ne donnent pas de résultats lorsqu'on a nommé les générateurs. Si l'on rencontre ce problème, on peut utiliser la procédure suivante pour enlever ces noms :

```
> gr: = pro(G) local a,b,L,c ;
> a=op (1, G); b: = op(2, G) ;
> L: {};
> for c in b do
> if type (c, '=') then c: =op (2, c) fi;
> L: ={op(L), c};
> od;
> permgroup (a,L) ;
> end;
```

2.5.1. Appendice. Algorithme de Told-Coxeter

Soit G un groupe défini par générateurs et relations : G=⟨H/ R⟩ avec X fini et H un sous-groupe de G engendré par l'image d'un sous-ensemble fini S de mots de $\bar{X}$ = X⊔X. L'algorithme de Todd-Coxeter que l'on va décrire permet, lorsque l'indice de H dans G est fini, de calculer cet indice et de donner l'action de G par translation à droite sur l'ensemble des classes H\G.

Description de l'algorithme

Il s'agit de donner à toutes les classes un numéro et un seul, la classe H ayant par exemple le numéro 1 (à ne pas confondre avec l'élément neutre). Pour cela, on va construire un certain nombre de tableaux selon les règles suivantes (on conseille de faire en même temps l'exemple qui suit)

1. A chaque mot $\alpha = a_{i1}...a_{ir}$ de S, on associe une table $M_{gen}(\alpha)$ à une seule ligne et r+1 colonnes dont le premier élément est 1. On remplira ultérieurement la deuxième colonne en mettant le numéro de la classe de $H_{a_{i1}}$ que l'on note aussi 1. a_{i1}, puis la troisième colonne avec le numéro de $1.a_{i1}.a_{i2}$, etc.

Premier principe : Le dernier élément de la ligne est 1. En effet, si $\alpha \in S$, on a $H\alpha = H$. On appelle ces tables *les tables du sous-groupe H*. Les tables sont ici présentées l'état initial :

1				1
	$ai1$	...	...	air

2. A chaque relateur $\beta = b_{j1}...b_{js}$, élément de R, on associe une table $M_{rel}(\beta)$ à s+1 colonnes et un nombre de lignes non limité.

Dans la première colonne, on mettra successivement les numéros introduits 1,2, 3, ..., numéros de classes. De nouveau, sur une même ligne, on passe de la colonne k à la colonne k+1 par « multiplication à droite » par b_{jk}.

Second principe : Sur une même ligne, le premier élément et le dernier sont identiques. En effet, si $\beta \in R$, $(Hx)\ \beta = Hx$ pour tout $x \in G$. On appelle cette table *la table du relateur β*.

	b_{j1}	…	…	b_{js}
1				1

3. Enfin, on construit une table de type différent, semblable à une table de loi de groupe (appelée table de multiplication). Les lignes sont indexées par les numéros des classes obtenus, les colonnes par les éléments de X et leurs inverses. A la place (i, g) se trouve le numéro de i. g.

	x	x'	…	$\mathcal{Z}$	$\mathcal{Z}$'
1					

4. On construit petit à petit les tableaux. Dès que l'on définit un nouveau numéro, on rajoute une ligne aux tableaux des relateurs et à la table de multiplication. Dès que l'on donne un numéro à une classe, on le reporte partout où l'on peut. Si $\mathcal{k} = \mathcal{j}.x$, on en déduit que $\mathcal{j} = \mathcal{k}.x$'. Si les principes 1 et 2 permettent de faire des déductions, on les utilise. Si l'on tombe sur une coïncidence, par exemple si une classe a à la fois le numéro 3 et 6, on remplace partout le numéro 6 par le numéro 3. Une fois faites toutes les déductions possibles, et s'il reste une case vide dans la table de multiplication, on attribue un nouveau numéro à une case vide de cette table. Sinon, l'algorithme est terminé.

Application de l'algorithme de Todd-Coxeter

Prenons G = $\langle a, b | a^4 = (ab)^2 = b^3 = 1 \rangle$.

On a donc $X = \{a, b\}, R = \{aaa, abab, bbb\}$

Prenons pour H le sous-groupe engendré par a. Il y a donc une table du sous-groupe, trois tables de relateurs et une table de multiplication.

Au début, elles sont de la forme suivante :

Table du sous-groupe :

	a
1	1

Table du relateur $aaaaa$:

a	a	a	a	
1	1	1	1	1

Table du relateur $abab$:

a	b	a	b	
1	1			1

Table du relateur bbb :

			b	b	b
1			1		

Table de « multiplication » :

	a	a'	b	b'
1	1	1		

La table du sous-groupe ne bougera plus. Nous ne la réécrirons plus.

On prend $2 = 1.b$. Les tables deviennent

a	a	a	a	
1 2	1	1	1	1 2

	a	b	a	b
1 2	1	2 1	1	1 2

1 2	2		1 2
		1	
b	b	b	

	a	a'	b	b'
1 2	1	1	2	 1

On prend $3=2.a$. Les tables deviennent

1	1	1	1	1

. .....

2	3			2
3			2	3

$a \quad a \quad a \quad a \qquad a \quad b \quad a \quad b$

1	1	2	3	1
2	3	1	1	2
3			2	3

$b \quad b \quad b$

1	2	3	1
2	3	1	2
3	1	2	3

	a	a'	b	b'
1	1	1	2	3
2	3		3	1
3		2	1	2

On a trouvé au passage comme déduction que $3.b = 1\ et\ 2.b = 3$.
On prend ensuite 4=3.a. Les tables deviennent

$a \quad a \quad a \quad a \qquad a \quad b \quad a \quad b$

1	1	1	1	1
2	3	4		2
3	4		2	3
4		2	3	4

1	2	3	1
2	3	1	2
3	1	2	3
4			4

$b \quad b \quad b$

1	1	2	3	1
2	3	1	1	2
3	4	5	2	3
4	5	2	3	4

	a	a'	b	b'
1	1	1	2	3
2	3		3	1
3	4	2	1	2
4		3		

On prend 5= 4.a. Les tables deviennent

$a \quad a \quad a \quad a \qquad a \quad b \quad a \quad b$

1	1	1	1	1
2	3	4	5	2
3	4	5	2	3
4	5	2	3	4
5	2	3	4	5

1	1	2	3	1
2	3	1	1	2
3	4	5	2	3
4	5	2	3	4
5	2	3	4	5

b b b

1	2	3	1
2	3	1	2
3	1	2	3
4	5		4
5		4	5

	a	*a'*	*b*	*b'*
1	1	1	2	3
2	3	5	3	1
3	4	2	1	2
4	5	3	5	
5	2	4		4

Au passage, on a fait les déductions 5.*a* =2 et 4.*b*=5.
Enfin, on pend 6=5.*b*. Les tables deviennent

a a a a

1	1	1	1	1
2	3	4	5	2
3	4	5	2	3
4	5	2	3	4
5	2	3	4	5
6	6	6	6	6

a b a b

1	1	2	3	1
2	3	1	1	2
3	4	5	2	3
4	5	2	3	4
5	2	3	4	5
6	6	4	5	6

b b b

1	2	3	1
2	3	1	2
3	1	2	3
4	5		4
5	6	4	5
6	4		6

	a	*a'*	*b*	*b'*
1	1	1	2	3
2	3	5	3	1
3	4	2	1	2
4	5	3	5	6
5	2	4	6	4
6	6	6	4	5

L'algorithme est terminé. L'indice de H dans G est 6. Montrons que a est d'ordre 4 dans G. Comme a^4 =1, il est d'ordre divisant 4. On remarque que l'image de a dans S(H\G) est le cycle (2 3 4 5) qui est d'ordre 4. Ainsi, a est d'ordre 4 et G est d'ordre 24. De même, l'image de b est la permutation (1 2 3)(4 5 6) qui est d'ordre 3.

On a obtenu explicitement un homomorphisme de G dans le groupe des permutations de H\G qui est isomorphe à $\mathfrak{G}_6$. Remarquons qu'il est injectif : en effet un élément du noyau appartient à l'intersection des xHx^{-1} pour $x \in$ G, en particulier, il appartient à H ; d'autre part, l'image de H dans $\mathfrak{G}_6$ est d'ordre 4, donc le noyau est réduit à l'élément neutre.

Conclusion

Si est un G un groupe défini par générateurs et relations tel que : G = $\langle X|R\rangle$ avec X fini et H un sous-groupe de G engendré par l'image d'un sous-ensemble fini S de mots de $\bar{X}$ = X⊔X.

L'algorithme de Todd-Coxeter permet, lorsque l'indice de H dans G est fini, de calculer cet indice et de donner l'action de G par translation à droite sur l'ensemble des classes H\G. La bibliothèque group concerne deux types de groupes : les groupes de permutations de degré n, qui sont donnés par une liste de générateurs et l'entier n, et les groupes définis par les générateurs et relations.

MAPLE calcule les classes à droites sur lesquelles G opère à droite. Certaines commandes ne donnent pas de résultats lorsqu'on a nommé les générateurs. Si l'on rencontre ce problème, on peut utiliser la procédure suivante pour enlever ces noms :

```
> gr: =pro(G) local a,b,L,c ;
> a=op (1, G); b: =op (2, G);
> L: {};
```

```
> for c in b do
> if type (c, '=') then c: =op (2, c) fi;
> L: ={op(L), c};
> od;
> permgroup (a,L) ;
 > end ;
```

Références bibliographie

A. Bouvier et D. Richard, Groupe, Actualités scientifiques et industrielles, Hermann, Paris 1974.

D. Perrin, 1996, *Cours d'algèbre*, Paris, Ellipses,.

Deschamps et J. Odoux, Paris, Masson, 1976 M. Artin, Algebra, Prentice Hall, New Jersey, 1991.

E. Ramis, C., 2005, Le journal Mathématical Reviews, La classification des finis.

J.D.Dixon et B. Mortimer, 1996, *Permutation groups*, GTM 163, Springer, New York.

P. Mazet, 1996, Algèbre et géométrie pour le capes et l'agrégation, Ellipses, Paris.

P.J Cameron, 1999, *Permutation g*roups, London Math. Soc. Student Texts 45, Cambridge Univ. Press.