Le problème du mot

Olivier Geneste

Journée des Jeunes Chercheurs - 28 mars 2014

Table des matières

- Le problème du mot
 - Groupes & Exemples
 - Groupes définis par une présentation
 - Le problème du mot
- 2 Dans les groupes de Coxeter
 - Définition & Exemples
 - Problème du mot dans les groupes de Coxeter
 - Groupes de Coxeter finis
- Oans les groupes d'Artin
 - Définition & Exemples
 - Relation avec les groupes de Coxeter
 - Problème du mot dans certains groupes d'Artin



Définition d'un groupe

Définition : Groupe

Un **groupe** est un ensemble G muni d'une loi de composition, notée *, telle que l'on ait :

- associativité : $\forall a, b, c \in G$, (a * b) * c = a * (b * c)
- élément neutre : $\exists 1 \in G \ \forall a \in G$, a * 1 = 1 * a = 1
- inversibilité : $\forall a \in G \ \exists b \in G, \ a * b = b * a = 1$

Premier exemple : Groupe symétrique

L'ensemble des permutations de l'ensemble $\{1,2,3\}$ muni de la loi de composition usuelle est un groupe contenant 6 éléments, appelé groupe symétrique d'ordre 3.

$$\mathfrak{S}_3 = \{id, (12), (13), (23), (123), (132)\}$$

Premier exemple : Groupe symétrique

L'ensemble des permutations de l'ensemble $\{1,2,3\}$ muni de la loi de composition usuelle est un groupe contenant 6 éléments, appelé groupe symétrique d'ordre 3.

$$\mathfrak{S}_3 = \{id, (12), (13), (23), (123), (132)\}$$

Deuxième exemple : Groupe libre

L'ensemble des mots que l'on peut former avec les lettres a,b,a^{-1} et b^{-1} muni de la loi de concaténation est un groupe, appelé groupe libre à 2 générateurs, noté F_2 .

NB: On sous-entend que aa^{-1} et bb^{-1} sont le mot vide. Il contient par exemple les éléments aba, bab ou encore $a^{-1}b^7a^{-1}$.

Troisième exemple : Groupe d'Artin

L'ensemble des mots que l'on peut former avec les lettres a, b, a^{-1} et b^{-1} muni de la loi de concaténation, où l'on identifie les mots aba et bab est un groupe d'Artin.

NB: On sous-entend que aa^{-1} et bb^{-1} sont le mot vide.

Dans ce groupe, par exemple, *bbbab*, *bbaba* et *babab* sont trois mots qui représentent le même élément.

Troisième exemple : Groupe d'Artin

L'ensemble des mots que l'on peut former avec les lettres a, b, a^{-1} et b^{-1} muni de la loi de concaténation, où l'on identifie les mots aba et bab est un groupe d'Artin.

NB: On sous-entend que aa^{-1} et bb^{-1} sont le mot vide.

Dans ce groupe, par exemple, *bbbab*, *bbaba* et *babab* sont trois mots qui représentent le même élément.

Troisième exemple : Notation

On désigne le groupe de l'exemple ci-dessus par $\langle a, b \mid aba = bab \rangle$.

Présentation d'un groupe

Définition : Présentation d'un groupe

Soit S un ensemble fini et R un ensemble constitué de certains mots formés à partir les lettres de S (et leurs inverses).

L'ensemble des mots que l'on peut former avec les lettres de S muni de la loi de concaténation, où l'on identifie les mots de R ainsi que les mots du type aa^{-1} au mot vide est un groupe. On dit que $\langle S|R\rangle$ est une **présentation** de ce groupe.

Exemple : Présentations de groupes

- ⟨a, b | ⟩
- $\langle a, b \mid abab^{-1}a^{-1}b^{-1} \rangle$
- $\langle a \mid a^n = 1 \rangle$

Présentation d'un groupe

Définition : Présentation d'un groupe

Soit S un ensemble fini et R un ensemble constitué de certains mots formés à partir les lettres de S (et leurs inverses).

L'ensemble des mots que l'on peut former avec les lettres de S muni de la loi de concaténation, où l'on identifie les mots de R ainsi que les mots du type aa^{-1} au mot vide est un groupe. On dit que $\langle S|R\rangle$ est une **présentation** de ce groupe.

Exemple : Présentations de groupes

- $\langle a, b \mid \rangle = F_2$
- $\langle a, b \mid abab^{-1}a^{-1}b^{-1} \rangle$ = groupe d'Artin de l'exemple

Le problème du mot sur un exemple

Soit un groupe donné par une présentation $\langle S|R\rangle$. Le problème du mot consiste à, étant donnés deux mots quelconques formés de lettres de S, savoir si l'on peut passer de l'un à l'autre en utilisant un nombre fini de relations de R.

Le problème du mot sur un exemple

Soit un groupe donné par une présentation $\langle S|R\rangle$. Le problème du mot consiste à, étant donnés deux mots quelconques formés de lettres de S, savoir si l'on peut passer de l'un à l'autre en utilisant un nombre fini de relations de R.

Exemple : problème de mot

Dans le groupe d'Artin $\langle a,b \mid abab^{-1}a^{-1}b^{-1}\rangle$, les mots bbbab et abaaa représentent le même élément du groupe.

En effet, bbbab = bbaba en utilisant la relation aba = bab,

= babaa de même.

= abaaa

Table des matières

- 1 Le problème du mot
 - Groupes & Exemples
 - Groupes définis par une présentation
 - Le problème du mot
- 2 Dans les groupes de Coxeter
 - Définition & Exemples
 - Problème du mot dans les groupes de Coxeter
 - Groupes de Coxeter finis
- Dans les groupes d'Artin
 - Définition & Exemples
 - Relation avec les groupes de Coxeter
 - Problème du mot dans certains groupes d'Artin



Groupes de Coxeter - Définition

Définition : Groupe de Coxeter

On dit que (W, S) est un système de Coxeter si

- W est un groupe,
- $S \subset W$ est un ensemble d'éléments d'ordre 2 qui engendre W,
- $W = \langle S \mid \forall s \in S, s^2 = 1 \text{ et } \forall s, t \in S, (st)^{\text{ordre de } st} = 1 \rangle$.

En pratique, on parle de *groupe de Coxeter*, et l'on donne uniquement la présentation de *W* correspondante.

Groupes de Coxeter - Exemples

Premier exemple:

$$W = \langle s, t \mid s^2 = t^2 = 1, (st)^3 = 1 \rangle = D_3$$
 est un groupe de Coxeter.

Groupes de Coxeter - Exemples

Premier exemple:

 $W = \langle s, t \mid s^2 = t^2 = 1, (st)^3 = 1 \rangle = D_3$ est un groupe de Coxeter.

Deuxième exemple :

$$W = \langle s, t \mid s^2 = t^2 = 1, (st)^2 = 1 \rangle = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$
 est un groupe de Coxeter.

Groupes de Coxeter - Exemples

Premier exemple:

 $W = \langle s, t \mid s^2 = t^2 = 1, (st)^3 = 1 \rangle = D_3$ est un groupe de Coxeter.

Deuxième exemple :

$$W = \langle s, t \mid s^2 = t^2 = 1, (st)^2 = 1 \rangle = \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$$
 est un groupe de Coxeter.

Troisième exemple :

$$W = \langle s, t \mid s^2 = t^2 = 1 \rangle = D_{\infty}$$
 est un groupe de Coxeter.

Longueur d'un élément

Désormais, on désigne par (W, S) un système de Coxeter.

Définition : Longueur d'un élément

Soit $w \in W$. On appelle **longueur** de w le plus petit entier $n \in \mathbb{N}$ tel que $w = s_1 s_2 \dots s_n$ où $s_i \in S$. On note l(w) = n. Dans ce cas, (s_1, \dots, s_n) est une **écriture réduite** de w.

Longueur d'un élément

Désormais, on désigne par (W, S) un système de Coxeter.

Définition : Longueur d'un élément

Soit $w \in W$. On appelle **longueur** de w le plus petit entier $n \in \mathbb{N}$ tel que $w = s_1 s_2 \dots s_n$ où $s_i \in S$. On note l(w) = n. Dans ce cas, (s_1, \dots, s_n) est une **écriture réduite** de w.

Exemples : Longueurs d'éléments

Dans $D_3 = \langle s, t | s^2 = t^2 = 1, (st)^3 = 1 \rangle$, on a :

- $l(s^2) = 0$
- l(sts) = 3
- l(tsts) = 2

Théorème fondamental

Théorème : Combinatoire dans les groupes de Coxeter

Soit $s \in S$, $w \in W$ et (s_1, \ldots, s_n) une écriture réduite de w.

- Soit $(s, s_1, ..., s_n)$ est une écriture réduite : l(sw) = l(w) + 1.
- Soit (s, s_1, \ldots, s_n) n'est pas une écriture réduite, il existe alors $j \in [|1, n|]$ tel que $(s_1, \ldots, s_{j-1}, s_{j+1}, \ldots, s_n)$ soit une écriture réduite de sw et l'on a l(sw) = l(w) 1.

Théorème fondamental

Théorème : Combinatoire dans les groupes de Coxeter

Soit $s \in S$, $w \in W$ et (s_1, \ldots, s_n) une écriture réduite de w.

- Soit (s, s_1, \ldots, s_n) est une écriture réduite : l(sw) = l(w) + 1.
- Soit (s, s_1, \ldots, s_n) n'est pas une écriture réduite, il existe alors $j \in [|1, n|]$ tel que $(s_1, \ldots, s_{j-1}, s_{j+1}, \ldots, s_n)$ soit une écriture réduite de sw et l'on a l(sw) = l(w) 1.

Exemple:

Dans
$$D_3$$
, $I(s.ts) = I(ts) + 1 = 3$
 $I(s.tst) = I(tst) - 1 = 2$ et $stst = tst .

Solution au problème du mot

Notons
$$a(s,t) = \begin{cases} 1 & \text{si} & \text{st d'ordre infini} \\ \langle st \rangle^n & \text{si} & \text{st est d'ordre n} \end{cases}$$
 où la notation $\langle st \rangle^n$ désigne l'élément $\underbrace{stst \dots}_{n \text{ termes}}$.

Solution au problème du mot (J.Tits)

- Deux écritures réduites (s_1, \ldots, s_p) et (t_1, \ldots, t_p) représentent le même élément de W si et seulement si on peut passer de l'un à l'autre par une suite finie de mouvements du type $a(s,t) \leftrightarrow a(t,s)$.
- Une écriture (s₁,..., s_p) n'est pas réduite si et seulement si on arrive à faire apparaître une suite ayant deux termes consécutifs égaux par une suite finie de a(s, t) ↔ a(t, s).

Classification des groupes de Coxeter finis

Définition : Groupe de Coxeter

On dit que (W, S) est un système de Coxeter si

- W est un groupe,
- S ⊂ W est un ensemble d'éléments d'ordre 2 qui engendre W,
- $W = \langle S \mid \forall s \in S, s^2 = 1 \text{ et } \forall s, t \in S, (st)^{\text{ordre de } st} = 1 \rangle$.

Théorème de classification :

On connaît toutes les présentations pour lesquelles les groupes de Coxeter associés sont des groupes finis.

Table des matières

- Le problème du mot
 - Groupes & Exemples
 - Groupes définis par une présentation
 - Le problème du mot
- 2 Dans les groupes de Coxeter
 - Définition & Exemples
 - Problème du mot dans les groupes de Coxeter
 - Groupes de Coxeter finis
- Dans les groupes d'Artin
 - Définition & Exemples
 - Relation avec les groupes de Coxeter
 - Problème du mot dans certains groupes d'Artin



Groupes d'Artin - Définition

Soit S un ensemble, notons $\Sigma = \{\sigma_s, s \in S\}$.

Définition : Groupe d'Artin

On dit que (A, Σ) est un système d'Artin si A est un groupe qui admet une présentation de la forme suivante :

$$A = \langle \Sigma \mid \forall s, t \in S, \langle \sigma_s \sigma_t \rangle^{m_{s,t}} = \langle \sigma_t \sigma_s \rangle^{m_{t,s}} \rangle$$

où
$$m_{s,t} = m_{t,s} \in \mathbb{N}^* \cup \{\infty\}.$$

Groupes d'Artin - Exemples

Premier exemple: Groupe d'Artin

Le groupe associé à la présentation

$$A = \langle \sigma_s, \sigma_t \mid \sigma_s \sigma_t \sigma_s = \sigma_t \sigma_s \sigma_t \rangle = B_3$$

est un groupe d'Artin, appelé groupe de tresses à 3 brins.

Groupes d'Artin - Exemples

Premier exemple : Groupe d'Artin

Le groupe associé à la présentation

$$A = \langle \sigma_s, \sigma_t \mid \sigma_s \sigma_t \sigma_s = \sigma_t \sigma_s \sigma_t \rangle = B_3$$

est un groupe d'Artin, appelé groupe de tresses à 3 brins.

Deuxième exemple : Groupe d'Artin

Le groupe associé à la présentation

$$A = \langle \sigma_s, \sigma_t \mid \rangle = F_2$$

est un groupe d'Artin, appelé groupe libre à 2 générateurs.



Groupes d'Artin & Groupes de Coxeter

A un groupe d'Artin donné, on associe un groupe de Coxeter de manière naturelle en rajoutant les relations du type $s^2 = 1$.

Premier exemple:

$$W = \langle s, t \mid sts = tst, t^2 = s^2 = 1 \rangle = D_3$$
$$A = \langle \sigma_s, \sigma_t \mid \sigma_s \sigma_t \sigma_s = \sigma_t \sigma_s \sigma_t \rangle = B_3$$

Deuxième exemple :

$$W = \langle s, t \mid s^2 = t^2 = 1 \rangle = \mathbb{Z}/2\mathbb{Z} * \mathbb{Z}/2\mathbb{Z}$$

$$A = \langle \sigma_s, \sigma_t \mid \rangle = F_2$$

Une section ensembliste

Soient W un groupe de Coxeter et A un groupe d'Artin associés. On commence par définir le morphisme de groupes suivant :

$$p\colon \left\{ \begin{array}{l} A \longrightarrow W \\ \sigma_s \longmapsto s \end{array} \right.$$

Une section ensembliste

Soient W un groupe de Coxeter et A un groupe d'Artin associés. On commence par définir le morphisme de groupes suivant :

$$p\colon \left\{ \begin{array}{l} A \longrightarrow W \\ \sigma_s \longmapsto s \end{array} \right.$$

On définit ensuite l'application τ telle que $\forall w \in W, p \circ \tau(w) = w$ de la manière suivante :

$$\tau \colon \left\{ \begin{array}{ccc} W \longrightarrow & A \\ w = \underbrace{s_1 \dots s_n}_{\text{\'ecriture r\'eduite}} & \mapsto & \sigma_{s_1} \dots \sigma_{s_n} \end{array} \right.$$

Une section ensembliste

Propriété:

L'application au est bien définie.

On notera $\tau(W) = A_{\text{red}}^+$ l'image de W par l'application τ .

Exemple:

Considérons l'exemple où $W=D_3$ et $A=B_3$, alors

•
$$\tau(st) = \sigma_s \sigma_t \in A^+_{red}$$

•
$$\tau(sts) = \tau(tst) = \sigma_s \sigma_t \sigma_s = \sigma_t \sigma_s \sigma_t \in A^+_{red}$$

•
$$\tau(stst) = \tau(ts) = \sigma_t \sigma_s \in A_{red}^+$$

Monoïdes d'Artin - Définition

Soit S un ensemble, notons $\Sigma = \{\sigma_s, s \in S\}$.

Définition : Monoïde d'Artin

Soit (A, Σ) est un système d'Artin de présentation :

$$A = \langle \Sigma \mid \forall s, t \in S, \langle \sigma_s \sigma_t \rangle^{m_{s,t}} = \langle \sigma_t \sigma_s \rangle^{m_{t,s}} \rangle$$

On appelle **monoïde d'Artin** l'ensemble des mots que l'on peut former à partir des lettres de Σ (en n'utilisant *pas* les inverses), muni de la loi de concaténation. On le note A^+ .

Exemple: Monoïde d'Artin

L'élément $\sigma_s \sigma_t$ est dans B_3^+ . L'élément $\sigma_s^{-1} \sigma_t^2 \sigma_s$ n'y est pas.



Divisibilité dans les monoïdes

On écrit, pour $u, v \in A^+$, que $u \prec v \iff \exists w \in A^+, uw = v$.

Proposition:

Un ensemble fini d'éléments de A+

- possède toujours un plus grand diviseur commun
- soit possède un plus petit multiple commun, soit ne possède aucun multiple commun.

Pour $J \subset \Sigma$, ppcm (σ_s) , s'il existe, est noté $\Delta_J \in A^+_{red}$.

Premier exemple : Élément fondamental

Dans B_3 , l'élément fondamental est $\Delta_{\Sigma} = \sigma_s \sigma_t \sigma_s = \Delta$.

Divisibilité dans les monoïdes

Second exemple : Élément fondamental

Dans le groupe d'Artin suivant (groupe de tresses à 4 brins),

$$B_{4} = \left\langle \sigma_{s}, \sigma_{t}, \sigma_{u} \middle| \begin{array}{l} \sigma_{s}\sigma_{t}\sigma_{s} = \sigma_{t}\sigma_{s}\sigma_{t} \\ \sigma_{t}\sigma_{u}\sigma_{t} = \sigma_{u}\sigma_{t}\sigma_{u} \end{array} \right\rangle$$
$$\sigma_{s}\sigma_{u} = \sigma_{u}\sigma_{s}$$

l'élément fondamental est $\Delta = \sigma_s.\sigma_t\sigma_u\sigma_s\sigma_t\sigma_s$ $= \sigma_t.\sigma_s\sigma_t\sigma_u\sigma_t\sigma_s$ $= \sigma_u.\sigma_t\sigma_u\sigma_s\sigma_t\sigma_u \in B_{\mathsf{tred}}^+$

Existence de l'élément fondamental

Théorème :

Les assertions suivantes sont équivalentes :

- Il existe un élément fondamental Δ_{Σ} dans A^+ .
- Tout sous-ensemble fini de A⁺ possède un ppcm.
- Le groupe de Coxeter associé, W, est fini. On dit alors que le groupe d'Artin A est de **type sphérique**.

Désormais, on se place dans le cas où A est de type sphérique pour y résoudre le problème du mot.

Solution au problème du mot dans le monoïde

On considère un élément du monoïde $w \in A_{red}^+$.

Solution au problème du mot dans le monoïde

On considère un élément du monoïde $w \in A_{red}^+$.

• On calcule $J_1 = \{s \in S \mid \sigma_s \prec w\}$, et l'on écrit $w = \Delta_{J_1} w'$.

On considère un élément du monoïde $w \in A_{red}^+$.

- On calcule $J_1 = \{s \in S \mid \sigma_s \prec w\}$, et l'on écrit $w = \Delta_{J_1} w'$.
- On calcule $J_2 = \{s \in S \mid \sigma_s \prec w'\}$, et l'on a $w = \Delta_{J_1} \Delta_{J_2} w''$.

On considère un élément du monoïde $w \in A_{red}^+$.

- On calcule $J_1 = \{s \in S \mid \sigma_s \prec w\}$, et l'on écrit $w = \Delta_{J_1} w'$.
- On calcule $J_2 = \{s \in S \mid \sigma_s \prec w'\}$, et l'on a $w = \Delta_{J_1} \Delta_{J_2} w''$.
- ... et ainsi de suite ...

On considère un élément du monoïde $w \in A_{red}^+$.

- On calcule $J_1 = \{ s \in S \mid \sigma_s \prec w \}$, et l'on écrit $w = \Delta_{J_1} w'$.
- On calcule $J_2 = \{s \in S \mid \sigma_s \prec w'\}$, et l'on a $w = \Delta_{J_1} \Delta_{J_2} w''$.
- ... et ainsi de suite ...
- On récupère $w = \Delta_{J_1} \Delta_{J_2} \dots \Delta_{J_n}$. On dit alors que w est sous forme normale positive.

On considère un élément du monoïde $w \in A_{red}^+$.

- On calcule $J_1 = \{s \in S \mid \sigma_s \prec w\}$, et l'on écrit $w = \Delta_{J_1} w'$.
- On calcule $J_2 = \{s \in S \mid \sigma_s \prec w'\}$, et l'on a $w = \Delta_{J_1} \Delta_{J_2} w''$.
- ... et ainsi de suite ...
- On récupère $w = \Delta_{J_1} \Delta_{J_2} \dots \Delta_{J_n}$. On dit alors que w est sous forme normale positive.

Propriété:

Cette écriture est unique : $\Delta_{J_1}\Delta_{J_2}\dots\Delta_{J_n}=\Delta_{I_1}\Delta_{I_2}\dots\Delta_{I_m}$ implique m=n et pour tout $k\in[|1,n|],\ I_k=J_k$.

L'élément fondamental - Propriété

Proposition:

Si Δ existe, alors l'élément Δ^2 commute avec tous les éléments du groupe d'Artin A.

Par conséquent, tout élément $w \in A$ peut s'écrire sous la forme $w = \Delta^m w^+$ où $m \in \mathbb{Z}$ et $w \in A^+$.

L'élément fondamental - Propriété

Proposition:

Si Δ existe, alors l'élément Δ^2 commute avec tous les éléments du groupe d'Artin A.

Par conséquent, tout élément $w \in A$ peut s'écrire sous la forme $w = \Delta^m w^+$ où $m \in \mathbb{Z}$ et $w \in A^+$.

Exemple:

Dans le groupe d'Artin B_3 , considérons l'élément $w = \sigma_s^{-2} \sigma_t^{-2} \sigma_s^{-1}$.

On écrit
$$w^+ = \underbrace{\sigma_s^{-1} \Delta^2}_{\in A^+} \underbrace{\sigma_s^{-1} \Delta^2}_{\in A^+} \underbrace{\sigma_t^{-1} \Delta^2}_{\in A^+} \underbrace{\sigma_t^{-1} \Delta^2}_{\in A^+} \underbrace{\sigma_s^{-1} \Delta^2}_{\in A^+} = \Delta^{10} w.$$

D'où l'écriture $w = \Delta^{-10} w^+$, où $w^+ \in A^+$.

On considère un élément du groupe $w \in A$.

On considère un élément du groupe $w \in A$.

• On écrit $w = \Delta^m w^+$ où m est maximal.

On considère un élément du groupe $w \in A$.

- On écrit $w = \Delta^m w^+$ où m est maximal.
- On calcule $w^+ = \Delta_{J_1} \Delta_{J_2} \dots \Delta_{J_n}$ la forme normale positive de l'élément w^+ du monoïde.

On considère un élément du groupe $w \in A$.

- On écrit $w = \Delta^m w^+$ où m est maximal.
- On calcule $w^+ = \Delta_{J_1} \Delta_{J_2} \dots \Delta_{J_n}$ la forme normale positive de l'élément w^+ du monoïde.
- On récupère $w^+ = \Delta^m \Delta_{J_1} \Delta_{J_2} \dots \Delta_{J_n}$. On dit alors que w est sous **forme normale**.

On considère un élément du groupe $w \in A$.

- On écrit $w = \Delta^m w^+$ où m est maximal.
- On calcule $w^+ = \Delta_{J_1} \Delta_{J_2} \dots \Delta_{J_n}$ la forme normale positive de l'élément w^+ du monoïde.
- On récupère $w^+ = \Delta^m \Delta_{J_1} \Delta_{J_2} \dots \Delta_{J_n}$. On dit alors que w est sous **forme normale**.

Propriété:

Cette écriture est unique : $\Delta^p \Delta_{J_1} \Delta_{J_2} \dots \Delta_{J_n} = \Delta^q \Delta_{I_1} \Delta_{I_2} \dots \Delta_{I_m}$ implique p = q, m = n et pour tout $k \in [|1, n|]$, $I_k = J_k$.

Bibliographie

- Nicolas Bourbaki : Groupes et Algèbres de Lie, Chapitres 4,5 et 6. Masson, 1981.
- Egbert Brieskorn, Kyoji Saito : Artin groups and Coxeter groups. Article original : 1972. Traduction anglaise : 1996.