Expansions superstables du groupe des entiers

Quentin Lambotte

Institut de Mathématique
Université de Mons

24 mars 2016

1 Motivations

- Le groupe libre
- Pourquoi est-ce un objet important ?
- Le problème de Tarski
- Un sous-groupe de $\mathbf{F}(a, b)$ particulier...

2 Position du problème

- Expansions d'un groupe
- Groupe abélien superstable
- Expansions superstables de $(\mathbf{Z}, +, 0)$

Rappel : définition d'un groupe

Definition

Un groupe est un ensemble G muni d'une opération $\cdot$ et d'un élément e, appelé l'élément *neutre*, de sorte que les propriétés suivantes soient vraies :

Rappel : définition d'un groupe

Definition

Un groupe est un ensemble G muni d'une opération $\cdot$ et d'un élément e, appelé l'élément *neutre*, de sorte que les propriétés suivantes soient vraies :

1. $\forall x \in G, e \cdot x = x \cdot e = x$;

Rappel : définition d'un groupe

Definition

Un groupe est un ensemble G muni d'une opération $\cdot$ et d'un élément e, appelé l'élément *neutre*, de sorte que les propriétés suivantes soient vraies :

1. $\forall x \in G, e \cdot x = x \cdot e = x$;
2. $\forall x \in G, \exists y \in G, x \cdot y = y \cdot x = e$;

Rappel : définition d'un groupe

Definition

Un groupe est un ensemble G muni d'une opération $\cdot$ et d'un élément e, appelé l'élément *neutre*, de sorte que les propriétés suivantes soient vraies :

1. $\forall x \in G, e \cdot x = x \cdot e = x$;
2. $\forall x \in G, \exists y \in G, x \cdot y = y \cdot x = e$;
3. $\forall x, y, z \in G \ (x \cdot y) \cdot z = x \cdot (y \cdot z)$.

$\mathbf{F}(a, b)$

$\mathbf{F}(a, b)$ est l'ensemble des *mots* de l'alphabet $\{a, b, a^{-1}, b^{-1}\}$ muni de l'opération de *concaténation*, notée $\frown$.

$\mathbf{F}(a, b)$

$\mathbf{F}(a, b)$ est l'ensemble des *mots* de l'alphabet $\{a, b, a^{-1}, b^{-1}\}$ muni de l'opération de *concaténation*, notée $\frown$.
Avec plus de détails :

$\mathbf{F}(a, b)$

$\mathbf{F}(a, b)$ est l'ensemble des *mots* de l'alphabet $\{a, b, a^{-1}, b^{-1}\}$ muni de l'opération de *concaténation*, notée $\frown$.

Avec plus de détails :

1. un mot est une chaîne finie de caractères, où chaque caractère est dans $\{a, b, a^{-1}, b^{-1}\}$.

$\mathbf{F}(a, b)$

$\mathbf{F}(a, b)$ est l'ensemble des *mots* de l'alphabet $\{a, b, a^{-1}, b^{-1}\}$ muni de l'opération de *concaténation*, notée $\frown$.
Avec plus de détails :

1. un mot est une chaîne finie de caractères, où chaque caractère est dans $\{a, b, a^{-1}, b^{-1}\}$.

Exemple

e (mot vide), *baba*, $abbab^{-1}$, etc.

$\mathbf{F}(a, b)$

$\mathbf{F}(a, b)$ est l'ensemble des *mots* de l'alphabet $\{a, b, a^{-1}, b^{-1}\}$ muni de l'opération de *concaténation*, notée $\frown$.

Avec plus de détails :

1. un mot est une chaîne finie de caractères, où chaque caractère est dans $\{a, b, a^{-1}, b^{-1}\}$.

Exemple

e (mot vide), $baba$, $abbab^{-1}$, etc.

2. $abba \frown babb = abbababb$.

$\mathbf{F}(a, b)$

$\mathbf{F}(a, b)$ est l'ensemble des *mots* de l'alphabet $\{a, b, a^{-1}, b^{-1}\}$ muni de l'opération de *concaténation*, notée $\frown$.
Avec plus de détails :

1. un mot est une chaîne finie de caractères, où chaque caractère est dans $\{a, b, a^{-1}, b^{-1}\}$.

Exemple

e (mot vide), $baba$, $abbab^{-1}$, etc.

2. $abba \frown babb = abbababb$.

Remarques

$\mathbf{F}(a, b)$

$\mathbf{F}(a, b)$ est l'ensemble des *mots* de l'alphabet $\{a, b, a^{-1}, b^{-1}\}$ muni de l'opération de *concaténation*, notée $\frown$.

Avec plus de détails :

1. un mot est une chaîne finie de caractères, où chaque caractère est dans $\{a, b, a^{-1}, b^{-1}\}$.

Exemple

e (mot vide), $baba$, $abbab^{-1}$, etc.

2. $abba \frown babb = abbababb$.

Remarques

1. $aa^{-1} = a^{-1}a = e$ et $bb^{-1} = b^{-1}b = e$;

$\mathbf{F}(a, b)$

$\mathbf{F}(a, b)$ est l'ensemble des *mots* de l'alphabet $\{a, b, a^{-1}, b^{-1}\}$ muni de l'opération de *concaténation*, notée $\frown$.

Avec plus de détails :

1. un mot est une chaîne finie de caractères, où chaque caractère est dans $\{a, b, a^{-1}, b^{-1}\}$.

Exemple

e (mot vide), $baba$, $abbab^{-1}$, etc.

2. $abba \frown babb = abbababb$.

Remarques

1. $aa^{-1} = a^{-1}a = e$ et $bb^{-1} = b^{-1}b = e$;
2. dans le groupe libre les mots $babb^{-1}a$ et baa sont les mêmes mots.

Pourquoi est-ce un objet important ?

Cet ensemble, muni de l'opération de concaténation est un *groupe*. Parmi les propriétés que $\mathbf{F}(a,b)$ vérifie, citons :

Théorème

Tout groupe dénombrable est contenu dans un quotient de $\mathbf{F}(a,b)$*. Autrement dit, si* G *est un groupe dénombrable, il existe un sous-groupe* H *de* $\mathbf{F}(a,b)$ *et un morphisme de groupe surjectif* $H \to G$*.*

De plus, $\mathbf{F}(a, b)$ est un objet qui apparaît dans d'autres domaines des mathématiques, comme la topologie algébrique (groupe fondamental d'un bouquet de deux cercles) ou la théorie des catégories (généralisation du groupe libre).

Une remarque sur le groupe libre

La construction du groupe $\mathbf{F}(a, b)$ peut être généralisée à n'importe quel alphabet A. Le groupe que l'on obtient est appelé *groupe libre* engendré par A et est noté $\mathbf{F}(A)$.

Quelques rappels de logique

Quelques rappels de logique

1. Une formule est une phrase écrite avec les symboles $\frown$, e, les connecteurs logiques, la négation et les quantificateurs universels et existentiels.

Quelques rappels de logique

1. Une formule est une phrase écrite avec les symboles $\frown$, e, les connecteurs logiques, la négation et les quantificateurs universels et existentiels.

Exemple

$\exists x, x \frown y = y \frown x = x$

Quelques rappels de logique

1. Une formule est une phrase écrite avec les symboles $\frown$, e, les connecteurs logiques, la négation et les quantificateurs universels et existentiels.

Exemple

$\exists x, x \frown y = y \frown x = x$

2. Un énoncé est une formule où toutes les variables sont quantifiées.

Quelques rappels de logique

1. Une formule est une phrase écrite avec les symboles $\frown$, e, les connecteurs logiques, la négation et les quantificateurs universels et existentiels.

Exemple

$\exists x, x \frown y = y \frown x = x$

2. Un énoncé est une formule où toutes les variables sont quantifiées.

Exemple

$\forall x \exists y, x \frown y = y \frown x = e$

Quelques rappels de logique

1. Une formule est une phrase écrite avec les symboles $\frown$, e, les connecteurs logiques, la négation et les quantificateurs universels et existentiels.

Exemple

$\exists x, x \frown y = y \frown x = x$

2. Un énoncé est une formule où toutes les variables sont quantifiées.

Exemple

$\forall x \exists y, x \frown y = y \frown x = e$

3. Un sous-ensemble X du groupe libre est *définissable* s'il correspond aux mots du groupe libre qui vérifient une formule.

Le problème de Tarski

Chaque groupe libre $\mathbf{F}(A)$ est associé à sa *théorie*, notée T_A, qui est l'ensemble des *énoncés* (formule où toutes les variables sont quantifiées) que vérifie $\mathbf{F}(A)$.

FIGURE – Alfred Tarski

Le problème de Tarski est la question suivante, posée en 1945.

Question

Si A a plus de deux éléments, a-t-on que $T_A = T_{\{a,b\}}$?

La réponse à cette question est positive et a été fournie par trois mathématiciens : Kharlampovich et Myasnikov d'une part et Sela d'autre part. Les deux preuves sont très techniques, longues (plus de 600 pages pour la preuve de Sela) et certains morceaux sont toujours en cours de vérification...

Un résultat inattendu

Une conséquence des techniques développées par Sela pour sa réponse au problème de Tarski est le théorème suivant :

Théorème

$\mathbf{F}(a, b)$ *est un groupe stable : on ne peut pas définir un ordre sur ce groupe à partir d'une formule.*

Un résultat inattendu

Une conséquence des techniques développées par Sela pour sa réponse au problème de Tarski est le théorème suivant :

Théorème

$\mathbf{F}(a,b)$ *est un groupe stable : on ne peut pas définir un ordre sur ce groupe à partir d'une formule.*

Exemple

Dans la structure $(\mathbf{N}, +, 0)$, il est possible de définir l'ordre habituel :
$n \leq m$ si et seulement si $\exists x \in \mathbf{N}, m = n + x$.

Un résultat inattendu

Une conséquence des techniques développées par Sela pour sa réponse au problème de Tarski est le théorème suivant :

Théorème

$\mathbf{F}(a, b)$ *est un groupe stable : on ne peut pas définir un ordre sur ce groupe à partir d'une formule.*

Exemple

Dans la structure $(\mathbf{N}, +, 0)$, il est possible de définir l'ordre habituel :
$n \leq m$ si et seulement si $\exists x \in \mathbf{N}, m = n + x$.

Question

Est-ce que certains sous-groupes ont aussi cette propriété de stabilité ?

Un sous-groupe de $\mathbf{F}(a, b)$ particulier...

Parmi les sous-groupes de $\mathbf{F}(a, b)$, on retrouve le groupe des entiers $(\mathbf{Z}, +, 0)$. Comment ?

Un sous-groupe de $\mathbf{F}(a, b)$ particulier...

Parmi les sous-groupes de $\mathbf{F}(a, b)$, on retrouve le groupe des entiers $(\mathbf{Z}, +, 0)$. Comment ?

1. Le sous-groupe engendré par a est isomorphe au groupe des entiers :

$$\langle a \rangle = \{a^z | z \in \mathbf{Z}\};$$

Un sous-groupe de $\mathbf{F}(a, b)$ particulier...

Parmi les sous-groupes de $\mathbf{F}(a, b)$, on retrouve le groupe des entiers $(\mathbf{Z}, +, 0)$. Comment ?

1. Le sous-groupe engendré par a est isomorphe au groupe des entiers :

$$\langle a \rangle = \{a^z | z \in \mathbf{Z}\};$$

2. de plus, c'est un ensemble définissable : il correspond aux mots qui vérifient la formule $x \frown a = a \frown x$;

Un sous-groupe de $\mathbf{F}(a, b)$ particulier...

Parmi les sous-groupes de $\mathbf{F}(a, b)$, on retrouve le groupe des entiers $(\mathbf{Z}, +, 0)$. Comment ?

1. Le sous-groupe engendré par a est isomorphe au groupe des entiers :
$$\langle a \rangle = \{a^z | z \in \mathbf{Z}\};$$
2. de plus, c'est un ensemble définissable : il correspond aux mots qui vérifient la formule $x \frown a = a \frown x$;
3. preuve ? Par induction sur la longeur (nombre de lettres) du mot x ;

Un sous-groupe de $\mathbf{F}(a, b)$ particulier...

Parmi les sous-groupes de $\mathbf{F}(a, b)$, on retrouve le groupe des entiers $(\mathbf{Z}, +, 0)$. Comment ?

1. Le sous-groupe engendré par a est isomorphe au groupe des entiers :

$$\langle a \rangle = \{a^z | z \in \mathbf{Z}\};$$

2. de plus, c'est un ensemble définissable : il correspond aux mots qui vérifient la formule $x \frown a = a \frown x$;
3. preuve ? Par induction sur la longeur (nombre de lettres) du mot x ;
4. de manière plus générale, tous les sous-groupes définissables infinis du groupe libre sont isomorphes à $(\mathbf{Z}, +, 0)$.

En résumé

En résumé

1. $\mathbf{F}(a, b)$ a une bonne propriété du point de vue du logicien : ce groupe est stable.

En résumé

1. $\mathbf{F}(a, b)$ a une bonne propriété du point de vue du logicien : ce groupe est stable.
2. un de ces sous-groupes est le groupe des entiers (d'ailleurs, tous les sous-groupes définissables et infinis du groupe libre sont isomorphes à $(\mathbf{Z}, +, 0)$).

En résumé

1. $\mathbf{F}(a, b)$ a une bonne propriété du point de vue du logicien : ce groupe est stable.
2. un de ces sous-groupes est le groupe des entiers (d'ailleurs, tous les sous-groupes définissables et infinis du groupe libre sont isomorphes à $(\mathbf{Z}, +, 0)$).
3. quels sont les liens entre les bonnes propriétés vérifées par le groupe libre et $(\mathbf{Z}, +, 0)$? Est-ce que les propriétés vérifiées par $(\mathbf{Z}, +, 0)$ permettent de mieux comprendre le groupe libre ?

Expansions d'un groupe

Lorsqu'un logicien étudie un groupe G, ce qui l'intéresse, c'est sa théorie T_G, c'est-à-dire l'ensemble des énoncés que G vérifie.

Expansions d'un groupe

Lorsqu'un logicien étudie un groupe G, ce qui l'intéresse, c'est sa théorie T_G, c'est-à-dire l'ensemble des énoncés que G vérifie.
Malheureusement, ce point de vue peut avoir quelques limitations.

Expansions d'un groupe

Lorsqu'un logicien étudie un groupe G, ce qui l'intéresse, c'est sa théorie T_G, c'est-à-dire l'ensemble des énoncés que G vérifie.
Malheureusement, ce point de vue peut avoir quelques limitations.

Exemple

Travaillons avec le groupe $(\mathbf{Z}, +, 0)$. Alors, dans la théorie de ce groupe $(T_{\mathbf{Z}})$ on ne peut pas parler des ensembles suivants :

Expansions d'un groupe

Lorsqu'un logicien étudie un groupe G, ce qui l'intéresse, c'est sa théorie T_G, c'est-à-dire l'ensemble des énoncés que G vérifie.
Malheureusement, ce point de vue peut avoir quelques limitations.

Exemple

Travaillons avec le groupe $(\mathbf{Z}, +, 0)$. Alors, dans la théorie de ce groupe ($T_{\mathbf{Z}}$) on ne peut pas parler des ensembles suivants :

1. les nombres premiers ;

Expansions d'un groupe

Lorsqu'un logicien étudie un groupe G, ce qui l'intéresse, c'est sa théorie T_G, c'est-à-dire l'ensemble des énoncés que G vérifie.
Malheureusement, ce point de vue peut avoir quelques limitations.

Exemple

Travaillons avec le groupe $(\mathbf{Z}, +, 0)$. Alors, dans la théorie de ce groupe ($T_{\mathbf{Z}}$) on ne peut pas parler des ensembles suivants :

1. les nombres premiers ;
2. les puissances de 2 ;

Expansions d'un groupe

Lorsqu'un logicien étudie un groupe G, ce qui l'intéresse, c'est sa théorie T_G, c'est-à-dire l'ensemble des énoncés que G vérifie.
Malheureusement, ce point de vue peut avoir quelques limitations.

Exemple

Travaillons avec le groupe $(\mathbf{Z}, +, 0)$. Alors, dans la théorie de ce groupe ($T_{\mathbf{Z}}$) on ne peut pas parler des ensembles suivants :

1. les nombres premiers ;
2. les puissances de 2 ;
3. la suite de Fibonacci ($x_0 = 1$, $x_1 = 2$, $x_{n+1} = x_n + x_{n-1}$).

Expansions d'un groupe

Pour dépasser ces limitations, les logiciens ajoutent de la structure aux groupes avec lesquels ils travaillent : pour pouvoir parler, par exemple, des nombres premiers dans $(\mathbf{Z}, +, 0)$ on ajoute un nouveau symbole $P(x)$ dans notre langage : $P(x)$ est vrai si et seulement si x est un nombre premier. Ainsi, les formules sont maintenant construite à partir de $+$, 0, $P(x)$, des connecteurs logiques et des quantificateurs.
La nouvelle structure que l'on obtient est notée $\mathbf{Z}_P = (\mathbf{Z}, +, 0, P)$ et est appelée *expansion* du groupe $(\mathbf{Z}, +, 0)$ par le symbole P.

Expansions d'un groupe

Pour dépasser ces limitations, les logiciens ajoutent de la structure aux groupes avec lesquels ils travaillent : pour pouvoir parler, par exemple, des nombres premiers dans $(\mathbf{Z}, +, 0)$ on ajoute un nouveau symbole $P(x)$ dans notre langage : $P(x)$ est vrai si et seulement si x est un nombre premier. Ainsi, les formules sont maintenant construite à partir de $+$, 0, $P(x)$, des connecteurs logiques et des quantificateurs.
La nouvelle structure que l'on obtient est notée $\mathbf{Z}_P = (\mathbf{Z}, +, 0, P)$ et est appelée *expansion* du groupe $(\mathbf{Z}, +, 0)$ par le symbole P.
En résumé : travailler avec une expansion d'un groupe revient à ajouter de la structure.

Groupe abélien superstable

La notion de superstabilité est une notion difficile à définir de manière générale...
L'idée derrière cette notion est de donner du sens, pour de nombreuses structures, à l'expression « a est indépendant de b au dessus de A ». Cette notion d'indépendance devrait ensuite fournir une notion de dimension permettant de classer plus facilement les objets étudiés. De plus, la notion de superstabilité a pour exemples les espaces vectoriels sur un corps et les corps algébriquement clos, où l'on retrouve l'indépendance linéaire et l'indépendance algébrique.

Groupe abélien superstable

Heureusement, dans le cas des groupes abéliens, la superstabilité est caractérisable algébriquement.

Groupe abélien superstable

Heureusement, dans le cas des groupes abéliens, la superstabilité est caractérisable algébriquement.

Théorème

Soit G un groupe abélien infini. Alors G est superstable si et seulement s'il n'existe pas une suite $(H_i)_{i \in \mathbf{N}}$ de sous-groupes définissables de G telle que

Groupe abélien superstable

Heureusement, dans le cas des groupes abéliens, la superstabilité est caractérisable algébriquement.

Théorème

Soit G un groupe abélien infini. Alors G est superstable si et seulement s'il n'existe pas une suite $(H_i)_{i \in \mathbf{N}}$ de sous-groupes définissables de G telle que

1. $H_0 > H_1 > H_2 > \ldots > H_n > \ldots;$

Groupe abélien superstable

Heureusement, dans le cas des groupes abéliens, la superstabilité est caractérisable algébriquement.

Théorème

Soit G un groupe abélien infini. Alors G est superstable si et seulement s'il n'existe pas une suite $(H_i)_{i \in \mathbf{N}}$ de sous-groupes définissables de G telle que

1. $H_0 > H_1 > H_2 > \ldots > H_n > \ldots;$
2. $[H_{i+1} : H_i] = \infty.$

Groupe abélien superstable

Heureusement, dans le cas des groupes abéliens, la superstabilité est caractérisable algébriquement.

Théorème

Soit G un groupe abélien infini. Alors G est superstable si et seulement s'il n'existe pas une suite $(H_i)_{i \in \mathbf{N}}$ de sous-groupes définissables de G telle que

1. $H_0 > H_1 > H_2 > \ldots > H_n > \ldots;$
2. $[H_{i+1} : H_i] = \infty.$

Remarque

Ce théorème est faux pour les expansions de G.

Le groupe $(\mathbf{Z}, +, 0)$ est superstable

Ce n'est pas très difficile d'appliquer le précédent théorème pour montrer que le groupe des entiers est superstable :

Théorème

Le groupe $(\mathbf{Z}, +, 0)$ est superstable

Ce n'est pas très difficile d'appliquer le précédent théorème pour montrer que le groupe des entiers est superstable :

Théorème

1. *Si H est un sous-groupe de $\mathbf{Z}$, alors $H = n\mathbf{Z}$, pour un certain $n \in \mathbf{Z}$.*

Le groupe $(\mathbf{Z}, +, 0)$ est superstable

Ce n'est pas très difficile d'appliquer le précédent théorème pour montrer que le groupe des entiers est superstable :

Théorème

1. *Si H est un sous-groupe de $\mathbf{Z}$, alors $H = n\mathbf{Z}$, pour un certain $n \in \mathbf{Z}$.*
2. *Soient $n, m \in \mathbf{Z}$. Alors $n\mathbf{Z} > m\mathbf{Z}$ si et seulement si n divise m.*

Le groupe $(\mathbf{Z}, +, 0)$ est superstable

Ce n'est pas très difficile d'appliquer le précédent théorème pour montrer que le groupe des entiers est superstable :

Théorème

1. *Si H est un sous-groupe de $\mathbf{Z}$, alors $H = n\mathbf{Z}$, pour un certain $n \in \mathbf{Z}$.*
2. *Soient $n, m \in \mathbf{Z}$. Alors $n\mathbf{Z} > m\mathbf{Z}$ si et seulement si n divise m.*
3. *Si n divise m, alors $[m\mathbf{Z} : n\mathbf{Z}]$ est fini.*

Le groupe $(\mathbf{Z}, +, 0)$ est superstable

Ce n'est pas très difficile d'appliquer le précédent théorème pour montrer que le groupe des entiers est superstable :

Théorème

1. *Si H est un sous-groupe de $\mathbf{Z}$, alors $H = n\mathbf{Z}$, pour un certain $n \in \mathbf{Z}$.*
2. *Soient $n, m \in \mathbf{Z}$. Alors $n\mathbf{Z} > m\mathbf{Z}$ si et seulement si n divise m.*
3. *Si n divise m, alors $[m\mathbf{Z} : n\mathbf{Z}]$ est fini.*

En conséquence, $(\mathbf{Z}, +, 0)$ est un groupe superstable.

Expansions superstables de $(\mathbf{Z}, +, 0)$

Question

Quelles sont les expansions de $\mathbf{Z}$ qui sont superstables ?

Ce qui a déjà été démontré

1. $(\mathbf{Z}, +, 0, P)$, où P représente les nombres premiers et leurs inverses, n'est pas superstable ;
2. $(\mathbf{Z}, +, 0, 2^{\mathbf{N}})$ est superstable ;
3. $(\mathbf{Z}, +, 0, \mathrm{Fac})$ est superstable.

Généralisation

On considère les expansions de $\mathbf{Z}$ par un symbole $P(x)$ qui interprète une suite (x_n) strictement croissante de naturels.

Résultat attendu

Si (x_n) vérifie l'une des deux conditions suivantes, alors $\mathbf{Z}_P$ est superstable.

1. (x_n) *est ultimement périodique modulo m, pour tout* $m > 1$, *et* $\lim_{n\to\infty} x_{n+1}/x_n = \infty$;
2. (x_n) *est définie par récurrence et il existe* $\theta > 0$ *tel que* $\lim_{n\to\infty} x_n/\theta^n \in \mathbf{R}\backslash\{0\}$.